DAGSTUHL
REPORTS

Volume 5, Issue 9, September 2015

ISSN 2192-5283

Published online and open access by
Schloss Dagstuhl – Leibniz-Zentrum für Informatik GmbH, Dagstuhl Publishing, Saarbrücken/Wadern, Germany. Online available at http://www.dagstuhl.de/dagpub/2192-5283

Publication date
January, 2016

Bibliographic information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at `http://dnb.d-nb.de`.

Digital Object Identifier: 10.4230/DagRep.5.9.i

Aims and Scope
The periodical *Dagstuhl Reports* documents the program and the results of Dagstuhl Seminars and Dagstuhl Perspectives Workshops.
In principal, for each Dagstuhl Seminar or Dagstuhl Perspectives Workshop a report is published that contains the following:

- an executive summary of the seminar program and the fundamental results,
- an overview of the talks given during the seminar (summarized as talk abstracts), and
- summaries from working groups (if applicable).

This basic framework can be extended by suitable contributions that are related to the program of the seminar, e. g. summaries from panel discussions or open problem sessions.

Contact
Schloss Dagstuhl – Leibniz-Zentrum für Informatik
Dagstuhl Reports, Editorial Office
Oktavie-Allee, 66687 Wadern, Germany
reports@dagstuhl.de
http://www.dagstuhl.de/dagrep

Report from Dagstuhl Seminar 15371

Quantum Cryptanalysis

Edited by

Michele Mosca[1], Martin Roetteler[2], Nicolas Sendrier[3], and Rainer Steinwandt[4]

1 **University of Waterloo, CA,** mmosca@iqc.ca
2 **Microsoft Corporation – Redmond, US,** martinro@microsoft.com
3 **INRIA – Le Chesnay, FR,** nicolas.sendrier@inria.fr
4 **Florida Atlantic University – Boca Raton, US,** rsteinwa@fau.edu

Abstract

This report documents the program and the outcomes of Dagstuhl Seminar 15371 "Quantum Cryptanalysis". In this seminar, participants explored the impact that quantum algorithms will have on cryptology once a large-scale quantum computer becomes available. Research highlights in this seminar included both computational resource requirement and availability estimates for meaningful quantum cryptanalytic attacks against conventional cryptography, as well as the security of proposed quantum-safe cryptosystems against emerging quantum cryptanalytic attacks.

Seminar September 6–11, 2015 – http://www.dagstuhl.de/15371
1998 ACM Subject Classification E.3 Data Encryption, F.2 Analysis of Algorithms and Problem Complexity, G.2 Discrete Mathematics, G.3 Probability and Statistics
Keywords and phrases Cryptography, Quantum computing, Post-quantum cryptography, Quantum algorithms, Cryptanalysis, Computational algebra, Quantum circuit complexity, Quantum hardware and resource estimation
Digital Object Identifier 10.4230/DagRep.5.9.1
Edited in cooperation with Jennifer Katherine Fernick

1 Executive Summary

Jennifer Katherine Fernick

It is known that quantum algorithms exist that jeopardize the security of most of our widely-deployed cryptosystems, including RSA and Elliptic Curve Cryptography. It is also known that advances in quantum hardware implementations are making it increasingly likely that large-scale quantum computers will be built in the near future that can implement these algorithms and devastate most of the world's cryptographic infrastructure. What is not known is an estimate of the resources that will be required to carry out these attacks – or even whether other quantum attacks exist that have not yet been accounted for in our security estimates. In this seminar, we examined both computational resource estimates for meaningful quantum cryptanalytic attacks against classical (i.e.: conventional) cryptography, as well as the security of proposed quantum-safe cryptosystems against emerging quantum cryptanalytic attacks.

This seminar had a number of research highlights spanning the areas of implementations of quantum hardware and software, quantum algorithms, and post-quantum cryptography.

Implementations of quantum information processing were outlined to help contextualize the current state of quantum computation. Recent advances in the synthesis of efficient quantum circuits were presented, as well as an update on implementations – particularly in the domain of superconducting integrated circuits. Seminar participants were warned that traditional approaches to the modeling of quantum processors may be reaching an end, while the LIQUi|> software architecture for control of quantum hardware and simulation of quantum algorithms was unveiled. Challenges involving practical costs for error correction in systems with specific types of quantum memory (particularly quantum bucket brigade RAM architectures) were articulated.

In the domain of algorithmic advances, seminar participants demonstrated quantum improvements on the gapped group testing problem, as well as improvements on lattice sieving using nearest neighbour search algorithms. A discussion of how quantum computers can sometimes provide quadratic speedup for the differential cryptanalysis of symmetric-key cryptosystems was also presented. A quantum version of the unique-SVP algorithm was discussed, but it was found to have slightly worse performance than its' classical counterpart. For the purposes of improving our understanding quantum algorithms before large-scale quantum computers become available, a technique involving trapdoor simulation of quantum algorithms was proposed.

Seminar participants also gave a number of recent results in the domain of quantum-safe cryptography. These included a provably-secure form of Authenticated Key Exchange based on the Ring-Learning with Errors problem, a proposal for a quantum-safe method to prevent key leakage during key agreement failure stemming from invalid public keys, and updates on hash-based digital signatures. The EU PQCRYPTO project also presented some preliminary recommendations for post-quantum cryptography.

In the domain of code-based cryptography, it was demonstrated that assuming hardness of Niederreiter problem, CFS signatures are strongly existentially unforgeable in the random oracle model. A number of results related to lattice reduction were also presented, including an improvement on the BKZ lattice reduction algorithm, some lattice enumeration work involving factoring integers by CVP algorithms for the prime number lattice, and a reduction of gapped uSVP to the Hidden Subgroup Problem in dihedral groups. A LIQUi|> implementation of a quantum algorithm to extract hidden shift was also presented, as well as demonstration of instances of HSPs over dihedral group which can be efficiently solved on a quantum computer. Seminar participants also proposed alternative ways of thinking about the dihedral coset problem, including some hardness reductions. A very new result on finding a generator of a principal ideal was also debuted at this seminar and provoked lively and ongoing discussion among participants.

Other talks were presented on diverse and compelling topics including quantum-mechanical means for program obfuscation, and a means for quantum indistinguishability of some types of ciphertext messages. A presentation was also made about how standardization bodies and industry deal with information security and risk, and many discussions – both formal and informal – among participants began to deal with the applied challenges of developing and deploying quantum-safe information security standards and tools.

Overall, the success of this seminar can be observed not only through the quantity of new results, but also in their diversity and interdisciplinarity. While there exist venues for cryptography and cryptanalysis, for quantum algorithms, and for implementations of quantum information processing, it remains critical that these communities continue to come together to ensure rigorous and broad cryptanalysis of proposed quantum-safe cryptographic algorithms, and to share a well-defined mutual understanding of the quantum-computational

resource requirements – and their present availability – for attacking both public and symmetric key cryptography. The security of the world's information depends on it.

The organizers (Michele Mosca, Martin Roetteler, Nicolas Sendrier, and Rainer Steinwandt) are grateful to the participants of this seminar and the team of Schloss Dagstuhl for an inspiring and productive third edition of this seminar series.

2 Table of Contents

3 Overview of Talks

3.1 Obfuscation and Quantum Encryption

Gorjan Alagic (University of Copenhagen, DK)

Joint work of Broadbent, Anne; Fefferman, Bill; Gagliardoni, Tommaso; Schaffner, Christian; St. Jules, Michael

Encryption of data is fundamental to secure communication. Beyond encryption of data lies obfuscation, i.e., encryption of functionality. It has been known for some time that the most powerful form of classical obfuscation (black-box obfuscation) is impossible. In this talk, we discuss the potential of obfuscating programs via quantum-mechanical means. As a starting point, we will mention some quantum analogues of several foundational results in obfuscation, including the aforementioned impossibility result (joint work with B. Fefferman). Our proof involves a novel technical idea: chosen-ciphertext-secure encryption for quantum states. We will thus also discuss what it means to encrypt quantum states with computational assumptions (joint work with A. Broadbent, B. Fefferman, T. Gagliardoni, C. Schaffner and M. St. Jules.)

3.2 A Trapdoor Simulation of Quantum Algorithms

Daniel J. Bernstein (University of Illinois – Chicago, US)

State-of-the-art algorithms to attack hard cryptanalytic problems never have complete proofs of their correctness and performance conjectures.The only reason for confidence in these conjectures is experiments showing that the algorithms work for many inputs. Trapdoor simulation builds the same confidence as experiment and is often much faster. Tung Chou and I have successfully simulated, e.g., the latest online Childs–Eisenberg distinctness algorithm and shown that it does notwork. This is a quantum algorithm using many qubits, with no other verification strategy.

3.3 Gapped Group Testing with Applications

Aleksandrs Belovs (University of Latvia, LV)

Joint work of Ambainis, Andris; Belovs, Aleksandrs; Regev, Oded; de Wolf, Ronald
Main reference A. Ambainis, A. Belovs, O. Regev, R. de Wolf, "Efficient Quantum Algorithms for (Gapped) Group Testing and Junta Testing," arXiv:1507.03126v1 [cs.CC], 2015.
URL http://arxiv.org/abs/1507.03126v1

In the group testing problem, given an oracle access to a function f on n variables that is promised to be the disjunction of some set S of at most k variables, the task is to identify S. We study the gapped version of this problem, where the task is to distinguish whether the set S is of size at most k or at least $k+d$ for some parameters k and d. We show the following. The randomized complexity of this problem is $\min\{k, (1+k/d)^2\}$ up to logarithmic

factors. The quantum complexity of this problem is $\Theta(\sqrt{1+k/d})$. Note that this constitutes a quartic improvement for $d \geq \sqrt{k}$. We demonstrate an application of this subroutine in a quantum algorithm for testing k-juntas.

3.4 Finding a Generator of a Principal Ideal

Jean-François Biasse (University of South Florida – Tampa, US)

Some recent cryptosystems, including the multilinear maps of Garg, Gentryand Halevi and the fully homomorphic encryption scheme of Smart and Vercauteren, are based on the hardness of finding a short generator of an principal ideal (short-PIP) in a number field (typically in cyclotomic fields). However, the assumption that short-PIP is hard has been challenged recently by Campbel et al. They proposed an approach for solving short-PIP that proceeds in two steps: first they sketched a quantum algorithm for finding an arbitrary generator (not necessarily short) of the input principal ideal. Then they suggested that it is feasible to compute a short generator efficiently from the generator in Step 1. Campbel et al. conjectured that this attack could run in polynomial time, which drew a lot attention. Since then, the conjectured run-time for Step 1 has been retracted while Cramer et al. validated Step2 of the approach by giving a detailed analysis. Whether the first step could be salvaged remains an open question.

In this paper we investigate the first step of the attack of Campbel et al. formally. We first observe that their quantum algorithm for finding a generator essentially falls into a framework of quantum algorithms for the hidden subgroup problem described by Hallgren. Hence, it suffers from similar limits, and we can show that, according to the same line of analysis of Hallgren, the algorithm has running time exponential in the degree of the number field. It has been an open question whether one can improve the analysis of Hallgren. Therefore it indicates that it is at least difficult to prove that the quantum algorithm of Campbel et al. is efficient.

On the positive side, we show that if we adapt one component of the algorithm of Campbel et al. and combine it with techniques in a recent work by Eisentrager et al., then we can essentially use the quantum algorithm for computing the unit group described in Eisentrager at al. to compute the a generator of a principal ideal, thus efficiently solving the problem of Step 1.

3.5 Synthesis of Efficient Quantum Circuits

Alexei Bocharov (Microsoft Corporation – Redmond, US)

The talk offers a high-level overview of recent advances in number theoretic methods for synthesis of efficient quantum circuit. The disruptive move from circuits of nearly quartic complexity (obtained by generic Solovay-Kitaev algorithm) to circuits of linear complexity (known to exist over any specific universal quantum basis of interest) is summarized and analyzed. Examples for popular universal binary quantum bases are provided and a newer

universal ternary basis is discussed in more detail. Many of the binary cases are now explained in the general framework developed in arXiv:1504.04350 and arXiv:1510.03888. Distinction between asymptotic optimality and practical optimality of efficient circuits is also explained in the talk.

3.6 A Simple and Provably Secure (Authenticated) Key Exchange based on the Learning Eith Errors Problems

Jintai Ding (University of Cincinnati, US)

Joint work of Ding, Jintai; Xie, Xiang; Lin, Xiaodong; Zhang, Jiang; Zhang, Zhenfeng; Snook, Michael; Dagdelen, Özgür
Main reference J. Ding, "A Simple Provably Secure Key Exchange Scheme Based on the Learning with Errors Problem," IACR Cryptology ePrint Archive, Report 2012/688, 2012.
URL http://eprint.iacr.org/2012/688

Public key cryptosystems (PKC) are critical part of the foundation of modern communication systems, in particular, Internet. However Shor's algorithm shows that the existing PKC like Diffie-Hellmann key exhange, RSA and ECC can be broken by a quantum computer. To prepare for the coming age of quantum computing, we need to build new public key cryptosystems that could resist quantum computer attacks. In this lecture, we present a practical and provably secure (authenticated) key exchange protocol based on the learing with errors problems, which is conceptually simple and has strong provable security properties. Several concrete choices of parameters are provided, and a proof-of-concept implementation shows that our protocols are indeed practical.

3.7 Semantic Security and Indistinguishability in the Quantum World

Tommaso Gagliardoni (TU Darmstadt, DE)

Joint work of Gagliardoni, Tommaso; Hülsing, Andreas; Schaffner, Christian
Main reference T. Gagliaordoni, A. Hülsing, C. Schaffner, "Semantic Security and Indistinguishability in the Quantum World," arXiv:1504.05255v2 [cs.CR], 2015.
URL http://arxiv.org/abs/1504.05255v2

At CRYPTO 2013, Boneh and Zhandry initiated the study of quantum-secure encryption. They proposed first indistinguishability definitions for the quantum world where the actual indistinguishability only holds for classical messages, and they provide arguments why it might be hard to achieve a stronger notion. In this work, we show that stronger notions are achievable, where the indistinguishability holds for quantum superpositions of messages. We investigate exhaustively the possibilities and subtle differences in defining such a quantum indistinguishability notion for symmetric-key encryption schemes. We justify our stronger definition by showing its equivalence to novel quantum semantic-security notions that we introduce. Furthermore, we show that our new security definitions cannot be achieved by a large class of ciphers – those which are quasi-preserving the message length. On the other hand, we provide asecure construction based on quantum-resistant pseudo random permutations; this construction can be used as a generic transformation for turning a large class of encryption schemes into quantum indistinguishable and hence quantum semantically secure ones.

3.8 How Hard is Deciding Trivial versus Nontrivial in the Dihedral Coset Problem?

Sean Hallgren (Pennsylvania State University – University Park, US)

We revisit the dihedral coset problem and relax the problem to a decision problem where we only ask if the subgroup is order two, or trivial. The relaxed problem turns out to be as hard computationally. The decision problem asks if a given vector is in the span of all coset states. We approach this by first computing an explicit basis for the coset space and the perpendicular space. We then show that if this subspace membership problem can be efficiently solved by some restricted unitaries using the basis, then the random subset sum problem with density a constant greater than 1 can also be solved by using the same unitaries.

3.9 An Update on Hash-based Signatures.

Andreas Hülsing (TU Eindhoven, NL)

This talk will discuss recent developments in the field of hash-based signatures. On the one hand, it will give an overview of recent standardization efforts in IETF. The most recent draft describes a variant of XMSS which will be discussed, including design decisions and security reasoning. On the other hand, it will cover SPHINCS, the first practical stateless scheme solely based on hash functions and recent follow-up work.

3.10 Combining Lattice Sieving Algorithms with (Quantum) Nearest Neighbor Searching

Thijs Laarhoven (TU Eindhoven, NL)

Main reference T. Laarhoven, "Sieving for shortest vectors in lattices using angular locality-sensitive hashing," in Proc. of the 35th Annual Cryptology Conf. (CRYPTO'15), LNCS, Vol. 9215, pp. 3–22, Springer, 2015.
URL http://dx.doi.org/10.1007/978-3-662-47989-6_1

To deploy lattice-based cryptographic primitives in practice and to choose parameters for these schemes, it is critical to understand the (quantum) hardness of hard lattice problems such as the shortest vector problem (SVP): given a basis of a lattice, how long would it take a classical or quantum computer to find a shortest non-zero vector in this lattice? Various algorithms for solving SVP have been proposed over the years, and while enumeration has long stood as the main candidate for solving SVP in high dimensions, lattice sieving algorithms are closing in. In particular, the recent connection between lattice sieving and nearest neighbor searching has significantly reduced both the theoretical and practical complexities of sieving, making it competitive with enumeration.

In this talk we take a look at the main ideas behind these recent improvements to sieving using nearest neighbor search algorithms, and how quantum searching can lead to further reduced complexities when combined with classical nearest neighbor search methods for

sieving. We conclude with an interesting direction for future research: Can quantum nearest neighbor methods be designed which can find nearby vectors even faster than by simply combining the best classical nearest neighbor algorithm with quantum searching?

3.11 Danger of Failure in Post-quantum Key Agreements

Bradley Lackey (University of Maryland – College Park, US)

Key agreement failure stemming from invalid public keys can lead to key leakage. We propose a method to block this, indirect public key validation, which is suitable for post-quantum key agreements.

3.12 Initial Recommendations of Long-term Secure Post-quantum Systems

Tanja Lange (TU Eindhoven, NL)

Joint work of Augot, Daniel; Batina, Lejla; Bernstein, Daniel J.; Bos, Joppe; Buchmann, Johannes; Castryck, Wouter; Dunkelman, Orr; Gueneysu, Tim; Gueron, Shay; Huelsing, Andreas; Lange, Tanja; Saied Emam Mohamed, Mohamed; Rechberger, Christian; Schwabe, Peter; Sendrier, Nicolas; Vercauteren, Frederik; Yang, Bo-Yin
URL http://pqcrypto.eu.org/

I will present the PQCRYPTO project's initial recommendations forpost-quantum cryptographic algorithms for symmetric encryption,symmetric authentication, public-key encryption, and public-keysignatures. These recommendations are chosen for confidence in theirlong-term security, rather than for efficiency (speed, bandwidth,etc.). Most of the talk slot is reserved for feedback and discussion on the proposal.

3.13 Quantum Differential Cryptanalysis

Anthony Leverrier (INRIA Rocquencourt, FR)

Joint work of Kaplan, Marc; Leurent, Gaëtan; Leverrier, Anthony; Naya-Plasencia, Maria

Quantum computers pose a serious threat to many cryptosystems. It is generally acknowledged that symmetric cryptography would be less impacted by quantum computing than public-key cryptography: indeed, in many cases, it seems that the best attack relies on Grover's search algorithm and therefore doubling the keysize essentially suffices to make a cryptosystem quantum resistant. Over the years, the symmetric cryptography community has come up with many cryptanalysis tools to test the security of symmetric cryptosystems, including for instance differential cryptanalysis. In this talk, we study the impact of quantum computing on this technique. In particular, while a quadratic speedup can be achieved sometimes, it turns out that the speedup is only sub quadratic in several cases of interest.

3.14 On the Possibility of a Quantum uSVP Algorithm

Alexander May (Ruhr-Universität Bochum, DE)

Joint work of Kirshanova, Elena; May, Alexander

We show how to turn Regev's reduction from uSVP to DCP into an algorithm. The basic idea is to use block reduction in order to compute a good basis, and to make Kuperberg's algorithm somewhat error-tolerant.Given a classical 2^{sn}-SVP algorithm, this leads to a quantum algorithm for $(n^{\frac{1}{2}+c})$-uSVP with time $2^{\sqrt{\frac{s}{c}}n}$ having constant success probability.

Unfortunately, it is not hard to show that for n^c-uSVP there is a classical algorithm with time $2^{\frac{s}{c}n}$ (having success probability 1). This also includes the special case where $c = \frac{n}{\log n}$, in which one solves $\exp(n)$-uSVP in polynomial time (by just using LLL).

So the quantum reduction achieves $\sqrt{\frac{s}{c}}$ as opposed to $\frac{s}{c}$.Unfortunately, this does not improve, since $\frac{s}{c} < 1$. Notice that $s \leq 1$ (even provably) and $c \geq 1$ (at least for the quantum algorithm, since we do not know how to completely avoid errors in Regev's reduction).

So the resulting quantum algorithm is (just) slightly worse than the classical one. Maybe with some additional tricks, this approach might eventually lead to a real improvement.

3.15 On Security of the Courtois-Finiasz-Sendrier Signature

Kirill Morozov (Kyushu University – Fukuoka, JP)

We show that the code-based Courtois-Finiasz-Sendrier (CFS) signature is strongly existentially unforgeable (SEUF-CMA) in the random oracle model, assuming hardness of the Niederreiter problem.

3.16 On the Robustness of Bucket Brigade Quantum RAM

Michele Mosca (University of Waterloo, CA)

Joint work of Arunachalam, Srinivasan; Gheorghiu, Vlad; Jochym-O'Connor, Tomas; Mosca, Michele; Srinivasan, Priyaa Varshinee
Main reference S. Arunachalam, V. Gheorghiu, T. Jochym-O'Connor, M. Mosca, P. V. Srinivasan, "On the robustness of bucket brigade quantum RAM," to appear in New Journal of Physics; pre-print available as arXiv:1502.03450v4 [quant-ph], 2015.
URL http://arxiv.org/abs/1502.03450v4

The practical cost of quantumly accessible classical memory will play a central role in the practical efficiency of some important quantum algorithms, including some algorithms relevant to quantum cryptanalysis. Will the cost be comparable to a similar amount of regular classical memory, or closer to the cost of a similar amount of general purpose fault-tolerant computational qubits?

I discussed the robustness of the bucket brigade quantum random access memory model introduced by Giovannetti, Lloyd, and Maccone. Their error analysis applies to algorithms

that make few queries to the qRAM, however it does not extend to algorithms that require superpolynomially many queries. A result of Regev and Schiff [ICALP '08] implies that for a class of error models a non-trivial error rate per gate in the bucket brigade quantum memory nullifies the speed-up of the quantum searching algorithm. This motivates the need for quantum error correction within the quantum RAM, and we argue that quantum error correction for the circuit causes the quantum bucket brigade architecture to lose its primary advantages.

The practical cost of quantumly accessible classical memory remains an important open question.

References

1 Srinivasan Arunachalam, Vlad Gheorghiu, Tomas Jochym-O'Connor, Michele Mosca, Priyaa Varshinee Srinivasan. *On the robustness of bucket brigade quantum RAM*, in Proceedings of the 10th Conf. on the Theory of Quantum Computation, Communication and Cryptography (TQC'15), Leibniz International Proceedings in Informatics (LIPIcs), Vol. 44, pp. 226–244, Schloss Dagstuhl, 2015, http://dx.doi.org/10.4230/LIPIcs.TQC.2015.226.

2 Srinivasan Arunachalam, Vlad Gheorghiu, Tomas Jochym-O'Connor, Michele Mosca, Priyaa Varshinee Srinivasan. *On the robustness of bucket brigade quantum RAM*, to appear in *New Journal of Physics*.

3.17 Continuous Permutations and Entropy Power Inequalities

Maris Ozols (University of Cambridge, GB)

Joint work of Audenaert, Koenraad; Datta, Nilanjana

I described a unitary version of Cayley's theorem which allows to embed any finite group in a continuous subgroup of the unitary group. When applied to the symmetric group, this construction can be used to permute quantum systems in a continuous fashion. For the case of two systems, the resulting continuous swap operation obeys a discrete version of the entropy power inequality. My talk is based on [ADO] and [Oz].

References

1 Koenraad Audenaert, Nilanjana Datta, Maris Ozols.*Entropy power inequalities for qudits.* arXiv:1503.04213, 2015

2 Maris Ozols.*How to combine three quantum states.* arXiv:1508.00860, 2015

3.18 Dihedral HSP and Hidden Shifts: On Efficiently Solvable Instances and Small Scale LIQUi|> Simulations

Martin Roetteler (Microsoft Corporation – Redmond, US)

It has been known for some time [2] that gapped instances of the unique-shortest vector problem can be reduced to a hidden subgroup problem (HSP) in the dihedral groups D_N.

The standard approach to solving this problem is by considering coset states, however, this ignores some of the information that might be available from the hiding function $f : D_N \to S$, in particular, it ignores that values of the function. The talk is on work in progress that attempts to use the target values. I consider the equivalent formulation to this HS this HSP as a hidden shift problem over the cyclic (or more generally, abelian) group.

Starting from an already known case, namely the hidden shift problem over the hypercube where a class of efficiently solvable instances is known to correspond to so-called bent functions, I then present a simple quantum algorithm to extract the shift. The algorithm was implemented in the quantum programming LIQUi|> that is developed by the Microsoft group at Redmond [WS:2014] and a short demo of the implementation was given.

Finally, I showed that there are instances of HSPs over the dihedral group that can be solved fully efficiently—in terms of queries, time, and space complexity, as well as classical post-processing—on a quantum computer. These instances are constructed from so-called difference sets and are well-known in combinatorics. We show that the quantum algorithms for hidden shifts of the Legrende symbol [1] and of bent functions [3] can be recovered as special cases of shifted difference sets. Regarding difference sets in the cyclic group, which correspond to dihedral HSP instance, we show that a trace zero hyperplane in a finite geometry $\mathrm{PG}(n, GF(q))$ gives rise to instances of hidden shifts in the group generated by a Singer cycle, hence, providing a new class of dihedral HSP instances that can be efficiently solved.

References

1 Wim van Dam, Sean Hallgren, and Lawrence Ip. Quantum algorithms for some hidden shift problems. *SIAM Journal on Computing*, 36(3):763–778, 2006.
2 Oded Regev. Quantum computation and lattice problems. *SIAM Journal on Computing*, 33(3):738–760, 2004.
3 Martin Roetteler. Quantum algorithms for highly non-linear Boolean functions. In *Proceedings of the 21st Annual ACM-SIAM Symposium on Discrete Algorithms (SODA'10)*, pages 448–457, 2010.
4 Dave Wecker and Krysta M. Svore. LIQUi|>: A software design architecture and domain-specific language for quantum computing. arXiv.org preprint arXiv:1402.4467, February 2014.

3.19 Factoring Integers by CVP Algorithms for the Prime Number Lattice

Claus-Peter Schnorr (Goethe-Universität Frankfurt am Main, DE)

Main reference C-P. Schnorr, "Factoring Integers by CVP Algorithms," in M. Fischlin, S. Katzenbach (eds.). "Number Theory and Cryptography – Papers in Honor of Johannes Buchmann on the Occasion of His 60th Birthday," LNCS, Vol. 8260, pp. 73–93, Springer, 2013.
URL http://dx.doi.org/10.1007/978-3-642-42001-6_6

1. Under reasonable heuristic assumptions it is shown that SVP and CVP of any lattice L of dimension n is solvable in polynomial time if the relative density $rd(L)$ of L is polynomially smaller than 1, essentially it is sufficient that $rd(L) = o(e\pi/2n)^{(1/4)}$. By definition $rd(L)$ is $\lambda_1(L)/max\lambda_1(L')$ for all lattices L' that have the same dimension and

the same determinant as L.Here $\lambda_1(L)$ denote the minimal length of non zero vectors of L.

2. The prime number lattice that is used for factoring large integers has a sufficiently small relative density.
3. There is a very practical speed up for the enumeration of short – resp. close – lattice vectors. The stages of the enumeration are performed according to their success probability to lead to a shorter – resp. closer – lattice vector. Stages with high success probability are done first.
4. For factoring the integer N we generate lattice vectors of the prime number lattice that are very close to the target vector $\mathbf{N}$ that represents N. For a sufficiently large prime base $p_1, ..., p_n$ such close vectors most likely yield a relation $\prod_{i=1}^{n} p_i^{e_i} = \pm \prod_{i=1}^{n} p_i^{e_i'} \mod N$ with small $e_i, e_i' \in \mathbb{N}$. We can easily factor N when given about n such independent $\mod N$ relations. Now an algorithm implemented by C. Morgan, A. Schickedanz, N. Hahn generates for $N = \Theta(10^{14})$ one $\mod N$ relation every 2 seconds on the average. This factors $N = \Theta(10^{14})$ in about 3 minutes. The method generates particular relations given by p_n-smooth integers u, v such that $|u - vN|$ is p_n-smooth too. (By definition u is p_n-smooth if it has no prime-factor larger than p_n. Here are some recent improvements).
5. We perform the stages in enumerating lattice vectors close to $\mathbf{N}$ according to their success rate to provide a $\mod N$ relation. Stages with high success rates are done first and stages with low success rate are put back to be performed later or they are even cut of if the success rate is extremely small. The success rate depends on the consumed distance to the target vector at the current stage and on the probability that the consumed distance can be extended to a new minimal distance of a lattice vectors to the target vector. This probability is based on the Gaussian volume heuristics for lattices.
6. In each round we randomly scale the basis vectors of a BKZ-reduced basis of the prime number lattice. The scaling fines each prime p_i randomly with probability 1/2. The scaling produces independent $\mod N$ relations each round.
7. We extremely prune the enumeration of lattice vectors close to $\mathbf{N}$ so that a very small fraction of these vectors can be efficiently generated still providing at least n $\mod N$ relations.

3.20 LIQUi|>: A Software Design Architecture and Domain-Specific Language for Quantum Computing

Krysta Svore (Microsoft Corporation – Redmond, US)

Joint work of Svore, Krysta; Wecker, Dave
Main reference D. Wecker, K. M. Svore, "LIQUi|>: A Software Design Architecture and Domain-Specific Language for Quantum Computing," arXiv:1402.4467v1 [quant-ph], 2014.
URL http://arxiv.org/abs/1402.4467v1

Languages, compilers, and computer-aided design tools will be essential for sscalable quantum computing, which promises an exponential leap in our ability to execute complex tasks. LIQUi|> is a modular software architecture designed tto control quantum hardware. It enables easy programming, compilation, and simulation of quantum algorithms and circuits, and is independent of a specific quantum architecture. LIQUi|> contains an embedded, domain specific language designed for programming quantum algorithms, with $F\#$ as the host language. It also allows the extraction of a circuit data structure that can be used

for optimization, rendering, or translation. The circuit can also be exported to external hardware and software environments. Two different simulation environments are available to the user which allow a trade-off between number of qubits and class of operations. LIQUi|> has been implemented on a wide range of runtimes as back-ends with a single user front-end. We describe the significant components of the design architecture and how to express any given quantum algorithm.

3.21 Improvement on BKZ Lattice Reduction Algorithm

Tsuyoshi Takagi (Kyushu University – Fukuoka, JP)

Joint work of Wang, Yuntao; Aono, Yoshinori; Hayashi, Takuya

The security of lattice-based cryptography is based on the hardness of finding a short vector in the underlying lattice. Currently the most efficient algorithms for solving this problem in random lattices of large dimensions are perhaps the BKZ algorithm and its modifications. In this talk, we investigate a variant of BKZ algorithm, called progressive BKZ, which performs the BKZ reduction starting from the small block size and switches to larger ones so that the total cost used for the local enumeration algorithm is minimized. We discuss how to accelerate the speed of the progressive BKZ algorithm for optimizing the parameters: the block size, the search radius and probability of the local enumeration algorithm, and the successive sizes of Gram-Schmidt orthogonal basis known as geometric series assumption. Using our improved progressive BKZ we have solved the ideal lattice challenge from Darmstadt in $2^{20.7}$ and $2^{24.0}$ seconds on a standard PC for 600 and 650 dimensions, respectively.

3.22 How to Address Post-quantum in Economy

Enrico Thomae (Operational Services GmbH – Zwickau, DE)

This talk gives a brief overview on how information security is addressed in economy by national and international standards (e.g. ISO27001) and big companies (e.g. Volkswagen). Using the case study of broken RFID technology, we show the limitations of this process. The main part of the talk should be a discussion on how we could overcome those limitations for Post-Quantum Cryptography. We will encourage to participate in generating an open access risk analysis.

3.23 Progress Towards Quantum Processors and Quantum Interfaces: Why Experimentalists Start Listening to Computer Science

Frank K. Wilhelm (Universität des Saarlandes, DE)

As a peripheral guest to the event, I reported on the status of the implementation of quantum computers with a heavy focus on superconducting integrated circuits. There is a clear sign for

optimism and the threshold at which a quantum processor outperforms a classical computer at least in simulating itself is imminent. While this is not a useful milestone, it shows that traditional approaches to modeling quantum processor experiments are reaching an end and experimentalists should work with computer scientists on topics like validation.

Participants

- Gorjan Alagic
University of Copenhagen, DK
- Aleksandrs Belovs
University of Latvia, LV
- Daniel J. Bernstein
Univ. of Illinois – Chicago, US
- Jean-François Biasse
University of South Florida – Tampa, US
- Alexei Bocharov
Microsoft Corporation – Redmond, US
- Harry Buhrman
CWI – Amsterdam, NL
- André Chailloux
INRIA Rocquencourt, FR
- Jintai Ding
University of Cincinnati, US
- Hang Dinh
Indiana Univ. South Bend, US
- Jürgen Eschner
Universität des Saarlandes, DE
- Jennifer Katherine Fernick
University of Waterloo, CA
- Tommaso Gagliardoni
TU Darmstadt, DE
- Markus Grassl
Univ. Erlangen-Nürnberg, DE
- Sean Hallgren
Pennsylvania State University – University Park, US
- Peter Hoyer
University of Calgary, CA
- Andreas Hülsing
TU Eindhoven, NL
- Stacey Jeffery
CalTech – Pasadena, US
- Stavros Kousidis
BSI – Bonn, DE
- Thijs Laarhoven
TU Eindhoven, NL
- Bradley Lackey
University of Maryland – College Park, US
- Tanja Lange
TU Eindhoven, NL
- Anthony Leverrier
INRIA Rocquencourt, FR
- Yi-Kai Liu
NIST – Gaithersburg, US
- Alexander May
Ruhr-Universität Bochum, DE
- Kirill Morozov
Kyushu Univ. – Fukuoka, JP
- Michele Mosca
University of Waterloo, CA
- Michael Naehrig
Microsoft Res. – Redmond, US
- Maris Ozols
University of Cambridge, GB
- Ray Perlner
NIST – Gaithersburg, US
- Martin Roetteler
Microsoft Corporation – Redmond, US
- Christian Schaffner
University of Amsterdam, NL
- John M. Schanck
University of Waterloo, CA
- Claus-Peter Schnorr
Goethe-Universität Frankfurt am Main, DE
- Nicolas Sendrier
INRIA – Le Chesnay, FR
- Dan J. Shepherd
CESG – Cheltenham, GB
- Daniel Smith-Tone
University of Louisville, US
- Fang Song
University of Waterloo, CA
- Rainer Steinwandt
Florida Atlantic University – Boca Raton, US
- Krysta Svore
Microsoft Corporation – Redmond, US
- Tsuyoshi Takagi
Kyushu Univ. – Fukuoka, JP
- Enrico Thomae
operational services GmbH – Zwickau, DE
- Jean-Pierre Tillich
INRIA – Le Chesnay, FR
- Joop van de Pol
University of Bristol, GB
- Frank K. Wilhelm
Universität des Saarlandes, DE
- Bo-Yin Yang
Academica Sinica – Taipei, TW

Report from Dagstuhl Seminar 15381

Information from Deduction: Models and Proofs

Edited by

Nikolaj S. Bjørner[1], Jasmin Christian Blanchette[2], Viorica Sofronie-Stokkermans[3], and Christoph Weidenbach[4]

1 **Microsoft Corporation – Redmond, US,** nbjorner@microsoft.com
2 **INRIA Lorraine – Nancy, FR,** jasmin.blanchette@inria.fr
3 **Universität Koblenz-Landau, DE,** sofronie@uni-koblenz.de
4 **MPI für Informatik – Saarbrücken, DE,** weidenbach@mpi-inf.mpg.de

Abstract

This report documents the program and the outcomes of Dagstuhl Seminar 15381 "Information from Deduction: Models and Proofs". The aim of the seminar was to bring together researchers working in deduction and applications that rely on models and proofs produced by deduction tools. Proofs and models serve two main purposes: (1) as an upcoming paradigm towards the next generation of automated deduction tools where search relies on (partial) proofs and models; (2) as the actual result of an automated deduction tool, which is increasingly integrated into application tools. Applications are rarely well served by a simple yes/no answer from a deduction tool. Many use models as certificates for satisfiability to extract feasible program executions; others use proof objects as certificates for unsatisfiability in the context of high-integrity systems development. Models and proofs even play an integral role within deductive tools as major methods for efficient proof search rely on refining a simultaneous search for a model or a proof. The topic is in a sense evergreen: models and proofs will always be an integral part of deduction. Nonetheless, the seminar was especially timely given recent activities in deduction and applications, and it enabled researchers from different subcommunities to communicate with each other towards exploiting synergies.

Seminar September 13–18, 2015 – http://www.dagstuhl.de/15381
1998 ACM Subject Classification D.2.4 Software/Program Verification, F.2.2 Nonnumerical Algorithms and Problems, F.3.1 Specifying and Verifying and Reasoning about Programs, F.4.1 Mathematical Logic, F.4.2 Grammars and Other Rewriting Systems, G.1.6 Optimization, I.2.3 Deduction and Theorem Proving
Keywords and phrases Automated Deduction, Program Verification, Certification
Digital Object Identifier 10.4230/DagRep.5.9.18
Edited in cooperation with Carsten Fuhs

1 Executive Summary

Nikolaj S. Bjørner
Jasmin Christian Blanchette
Viorica Sofronie-Stokkermans
Christoph Weidenbach

Models and proofs are the quintessence of logical analysis and argumentation. Many applications of deduction tools need more than a simple answer whether a conjecture holds;

often additional information – for instance proofs or models – can be extremely useful. For example, proofs are used by high-integrity systems as part of certifying results obtained from automated deduction tools, and models are used by program analysis tools to represent bug traces. Most modern deductive tools may be trusted to also produce a proof or a model when answering whether a conjecture is a theorem or whether a certain problem formalized in logic has a solution. Moreover, major progress has been obtained recently by procedures that rely on refining a simultaneous search for a model and a proof. Thus, proofs and models help producing models and proofs, and applications use proofs and models in many crucial ways.

Below, we point out several directions of work related to models and proofs in which there are challenging open questions:

- *Extracting proofs from derivations.* An important use of proof objects from derivations is for applications that require certification. But although the format for proof objects and algorithms for producing and checking them has received widespread attention in the research community, the current situation is not satisfactory from a consumer's point of view.
- *Extracting models from derivations.* Many applications rely on models, and models are as important to certify non-derivability. Extracting models from first-order saturation calculi is a challenging problem: the well-known completeness proofs of superposition calculi produce perfect models from a saturated set of clauses. The method is highly non-constructive, so extracting useful information, such as "whether a given predicate evaluates to true or false under the given saturated clauses," is challenging. The question of representation is not yet well addressed for infinite models.
- *Using models to guide the search for proofs and vice versa.* An upcoming next generation of reasoning procedures employ (partial) models/proofs for proof search. They range from SAT to first-order to arithmetic reasoning and combinations thereof. It remains an open question what properties of models are crucial for successful proof search, how the models should be dynamically adapted to the actual problem, and how the interplay between the models and proof search progress through deduction should be designed.
- *External applications of models and proofs.* Models and proofs are used in various ways in applications. So far application logics and automated proof search logics have been developed widely independently. In order to get more of a coupling, efforts of bringing logics closer together or the search for adequate translations are needed.

This Dagstuhl seminar allowed to bring together experts for these topics and invited discussion about the production and consumption of proofs and models. The research questions pursued and answered include:

- To what extent is it possible to design common exchange formats for theories, proofs, and models, despite the diversity of provers, calculi, and formalisms?
- How can we generate, process, and check proofs and models efficiently?
- How can we search for, represent, and certify infinite models?
- How can we use models to guide proof search and proofs to guide model finding?
- How can we make proofs and models more intelligible, yet at the same time provide the level of detail required by certification processes?

2 Table of Contents

3 Overview of Talks

3.1 Formal Verification of Pastry Using TLA+

Noran Azmy (MPI für Informatik – Saarbrücken, DE)

Peer-to-peer protocols for maintaining distributed hash tables, such as Pastry or Chord, have become popular for certain Internet applications. While such protocols promise certain properties concerning correctness and performance, verification attempts using formal methods invariably discover border cases that violate some of those guarantees. For example, Zave discovered that no previously published version of Chord maintains the invariants claimed of the protocol. In his PhD thesis, Tianxiang Lu discovered similar correctness problems for Pastry and also developed a model, which he called LuPastry, for which he provided a partial proof of correct delivery assuming no node departures, mechanized in the TLA+ Proof System. We present the first complete proof of correct delivery for LuPastry, which we call LuPastry+.

3.2 CDCL as Saturation

Peter Baumgartner (NICTA – Canberra, AU)

Conflict driven clause learning (CDCL) is the main paradigm for building propositional logic SAT solvers. Saturation based theorem proving is the main paradigm for building first-order logic theorem provers. A natural research question is to investigate the relationships between these paradigms for, e.g., exploiting successful techniques from CDCL in first-order logic theorem proving. To this end, techniques like splitting, dependency-directed backtracking and lemma-learning techniques have been considered for integration in first-order logic resolution calculi and instance-based methods.

The paper revisits this topic from a different point of view. Instead of *integrating* its concepts, it shows how CDCL can be *simulated* by a saturation based resolution calculus. This is not trivial, as CDCL's splitting and backjumping operations are not compatible with saturation. One could, of course, add an explicit splitting rule to resolution, as mentioned above, but this would work in very restricted cases only. In contrast, our calculus approach allows for straightforward lifting to first-order logic. Moreover, in contrast to, e.g., model evolution calculi, it separates model representation from calculus. This supports the modular design of theorem provers, which, this way, e.g., may arbitrarily trade-off representational power versus efficiency, without compromising refutational completeness.

The main result for now is a refutational completeness result in presence of redundancy criteria and deletion rules. The latter are needed for a faithful simulation of CDCL.

3.3 Higher-Order Proofs and Models – Examples from Meta-Logical Reasoning and Metaphysics

Christoph Benzmueller (FU Berlin, DE)

Joint work of Benzmüller, Christoph; Woltzenlogel-Paleo, Bruno; Paulson, Lawrence; Brown, Chad; Claus, Maximilian; Sutcliffe, Geoff; Sultana, Nik; Blanchette, Jasmin
Main reference C. Benzmüller, B. Woltzenlogel Paleo, "Automating Gödel's Ontological Proof of God's Existence with Higher-order Automated Theorem Provers," in Proc. of the 21st Europ. Conf. on Artificial Intelligence (ECAI'14), Frontiers in Artificial Intelligence and Applications, Vol. 263, pp. 93–98, IOS Press, 2014.
URL http://dx.doi.org/10.3233/978-1-61499-419-0-93

Extraction and utilization of information (by hand) from higher-order logic proofs and countermodels has played an important role in my recent research. Two examples are presented, one from meta-logical reasoning and one from metaphysics.

In the first example countermodels from Nitpick were utilized in a schematic process to verify the independence of prominent modal logic axioms in Isabelle/HOL. In addition, minimality aspects of these models were proved. The independence results constituted the key steps in the verification of the well known modal logic cube.

In the second example, the higher-order prover LEO-II detected an inconsistency in Kurt Gödel's original variant of ontological argument for the existence of God. While LEO-II's (extensional higher-order RUE-resolution) proof object in fact contains the information needed for the reconstruction of a human-intuitive explanation, I failed for a long time to identify the relevant puzzle pieces. Only recently, I was able to extract (and verify) a surprisingly easily accessible abstract-level proof. It is as in many fields in mathematics: once a beautiful structure has been revealed, it can't be missed anymore. Unmated low-level formal proofs, in contrast, are lacking persuasive power.

References

1 Christoph Benzmüller and Bruno Woltzenlogel Paleo. *Automating Gödel's Ontological Proof of God's Existence with Higher- order Automated Theorem Provers*, In ECAI 2014, IOS Press, Frontiers in Artificial Intelligence and Applications, volume 263, pp. 93–98, 2014. http://dx.doi.org/10.3233/978-1-61499-419-0-93

2 Christoph Benzmüller and Bruno Woltzenlogel Paleo. *Higher-Order Modal Logics: Automation and Applications*, In Reasoning Web 2015, Springer, LNCS, number 9203, pp. 1–43, 2015. http://dx.doi.org/10.1007/978-3-319-21768-0_2

3 Christoph Benzmüller and Lawrence Paulson. *Quantified Multimodal Logics in Simple Type Theory*, In Logica Universalis, volume 7, number 1, pp. 7–20, 2013. http://dx.doi.org/10.1007/s11787-012-0052-y

4 Christoph Benzmüller. *Invited Talk: On a (Quite) Universal Theorem Proving Approach and Its Application in Metaphysics*, In TABLEAUX 2015, Springer, LNAI, volume 9323, pp. 209–216, 2015. http://dx.doi.org/10.1007/978-3-319-24312-2_15

5 Christoph Benzmüller, Maximilian Claus, and Nik Sultana. *Systematic Verification of the Modal Logic Cube in Isabelle/HOL*, In PxTP 2015, EPTCS, volume 186, pp. 27–41, 2015. http://dx.doi.org/10.4204/EPTCS.186.5

3.4 Semi-intelligible Isar Proofs from Machine-Generated Proofs

Jasmin Christian Blanchette (INRIA Lorraine – Nancy, FR)

Main reference J. C. Blanchette, S. Böhme, M. Fleury, S. J. Smolka, A. Steckermeier, "Semi-intelligible Isar Proofs from Machine-Generated Proofs," to appear in Journal of Automated Reasoning.

Sledgehammer is a component of the Isabelle/HOL proof assistant that integrates external automatic theorem provers (ATPs) to discharge interactive proof obligations. As a safeguard against bugs, the proofs found by the external provers are reconstructed in Isabelle. Reconstructing complex arguments involves translating them to Isabelle's Isar format, supplying suitable justifications for each step. Sledgehammer transforms the proofs by contradiction into direct proofs; it iteratively tests and compresses the output, resulting in simpler and faster proofs; and it supports a wide range of ATPs, including E, LEO- II, Satallax, SPASS, Vampire, veriT, Waldmeister, and Z3.

3.5 Tips and Tricks in LIA constraint solving

Martin Bromberger (MPI für Informatik – Saarbrücken, DE)

Joint work of Bromberger, Martin; Sturm, Thomas; Weidenbach, Christoph

We present tips and tricks for constraint solving in the theory of linear integer arithmetic. These tricks are sound, efficient, heuristic methods that find solutions for a large number of problems. While most complete methods search on the problem surface for a solution, these heuristics use balls and cubes to explore the interior of the problems. The heuristic methods are especially efficient for problems with a large number of integer solutions. Although it might seem that problems with a large number of integer solutions should be trivial for complete solvers, we will show the opposite by comparing state-of-the-art SMT solvers with our own solver that contains those heuristic methods.

3.6 Formally verified constraint solvers

Catherine Dubois (ENSIIE – Evry, FR)

Do you trust your solver ? In this talk, we focus on finite domains (FD) constraint solvers. We have developed a family of formally verified solvers through a generic and modular solver developed within the Coq proof assistant and proved sound and complete [CDD12]. Local consistency property, labeling strategy are parameters of this formal development. In the talk we present the main features and the current status of the development. Work in progress concerns the Coq formalization and verification of the well-known filtering algorithm [Reg94] for the alldiff constraint.

References

1 Carlier M., Dubois C., Gotlieb A. *A Certified Constraint Solver over Finite Domains*. FM 2012:116–131

2 Régin J.-C., *A Filtering Algorithm for Constraints of Difference in CSPs*. AAAI 1994:362–367

3.7 Overview of Models in Yices

Bruno Dutertre (SRI – Menlo Park, US)

We present a form of model-based theory combination recently implemented in Yices, algorithms for exists/forall solving and model generalization.

3.8 Automatic Proofs of Termination and Memory Safety for Programs with Pointer Arithmetic

Carsten Fuhs (Birkbeck, University of London, GB)

Joint work of Ströder, Thomas; Giesl, Jürgen; Brockschmidt, Marc; Frohn, Florian; Fuhs, Carsten; Hensel, Jera; Schneider-Kamp, Peter; Aschermann, Cornelius
Main reference T. Ströder, J. Giesl, M. Brockschmidt, F. Frohn, C. Fuhs, J. Hensel, P. Schneider-Kamp, "Proving Termination and Memory Safety for Programs with Pointer Arithmetic," in Proc. of the 7th Int'l Joint Conf. on Automated Reasoning (IJCAR'14), LNAI, Vol. 8562, pp. 208–223, Springer, 2014.
URL http://dx.doi.org/10.1007/978-3-319-08587-6_15

While automated verification of imperative programs has been studied intensively, proving termination of programs with explicit pointer arithmetic fully automatically was still an open problem. To close this gap, we introduce a novel abstract domain that can track allocated memory in detail. Automating our abstract domain with the help of SMT-based entailment proofs, we construct a symbolic execution graph that over-approximates all possible runs of the program and that can be used to prove memory safety. This graph is then transformed into an integer transition system, whose termination can be proved by standard techniques, e.g., based on models found by SMT solvers. We have implemented this approach in the automated termination prover AProVE and demonstrate its capability of analyzing C programs with pointer arithmetic that existing tools cannot handle.

3.9 Quantified Array Fragments: Decision Results and Applications

Silvio Ghilardi (University of Milan, IT)

Joint work of Alberti, Francesco; Ghilardi, Silvio; Sharygina, Natasha

The theory of arrays is one of the most relevant theories for software verification, this is the reason why current research in automated reasoning dedicated so much effort in

establishing decision and complexity results for it. As soon as quantified formulae are concerned, however, satisfiability becomes intractable when free unary function symbols are added to mild fragments of arithmetic [6]. Nevertheless, since applications require the use of quantifiers, e.g. in order to express invariants of program loops, it becomes crucial to identify sufficiently expressive tractable quantified fragments of the theory.

In this talk we first compare and discuss some state-of-the-art literature on the subject [4], [5], [2], [3] and then we show how the results can be applied to model-checking problems in array-based systems. We finally report the status of the implementation in our tools MCMT and BOOSTER [1].

The original contributions of this talk come from joint work with F. Alberti and N. Sharygina.

References

1 F. Alberti, S. Ghilardi, and N. Sharygina. Booster : an acceleration-based verification framework for array programs. In *ATVA*, pages 18–23, 2014.
2 F. Alberti, S. Ghilardi, and N. Sharygina. Decision procedures for flat array properties. In *TACAS*, pages 15–30, 2014.
3 F. Alberti, S. Ghilardi, and N. Sharygina. A new acceleration-based combination framework for array properties. In *FroCoS*, 2015.
4 A.R. Bradley, Z. Manna, and H.B. Sipma. What's decidable about arrays? In *VMCAI*, pages 427–442, 2006.
5 P. Habermehl, R. Iosif, and T. Vojnar. A logic of singly indexed arrays. In *LPAR*, pages 558–573, 2008.
6 J.Y. Halpern. Presburger arithmetic with unary predicates is Π^1_1 complete. *J. Symbolic Logic*, 56(2):637–642, 1991.

3.10 Using Information from Deduction for Complexity Analysis

Juergen Giesl (RWTH Aachen University, DE)

Joint work of Frohn, Florian; Giesl, Jürgen; Hensel, Jera; Aschermann, Cornelius; Ströder, Thomas
Main reference F. Frohn, J. Giesl, J. Hensel, C. Aschermann, T. Ströder, "Inferring Lower Bounds for Runtime Complexity," in Proc. of the 26th Int'l Conf. on Rewriting Techniques and Applications (RTA'15), LIPIcs, Vol. 36, pp. 334–349, Schloss Dagstuhl, 2015.
URL http://dx.doi.org/10.4230/LIPIcs.RTA.2015.334

Several techniques and tools have been developed to prove termination and to verify inductive properties of programs automatically. We report on our recent work to use information from such automatically generated proofs in order to analyze complexity of programs. More precisely, from automated termination proofs, one can infer upper bounds on a program's runtime and on the values of its variables. Moreover, from automated induction proofs, one can infer lower bounds on the runtime of a program.

3.11 SAT-based techniques for parameter synthesis and optimization

Alberto Griggio (Bruno Kessler Foundation – Trento, IT)

Joint work of Bittner, Benjamin; Bozzano, Marco; Cimatti, Alessandro; Gario, Marco; Griggio, Alberto; Mattarei, Cristian
Main reference M. Bozzano, A. Cimatti, A. Griggio, C. Mattarei, "Efficient Anytime Techniques for Model-Based Safety Analysis," in Proc. of the 27th Int'l Conf. on Computer Aided Verification (CAV'15), LNCS, Vol. 9206, pp. 603–621, Springer, 2015.
URL http://dx.doi.org/10.1007/978-3-319-21690-4_41

Many application domains can be described in terms of parameterized systems, where parameters are variables whose value is invariant over time, but is only partially constrained. A key challenge in this context is the estimation of the parameter valuations that guarantee the correct behavior of the system. Manual estimation of these values is time consuming and does not find optimal solutions for specific design problems. Therefore, a fundamental problem is to automatically synthesize the maximal region of parameter valuations for which the system satisfies some properties, or to find the best/most appropriate valuation with respect to a given cost function.

In this talk, we present a technique for parameter synthesis and optimization that exploits the efficiency of state-of-the art model checking algorithms based on SAT solvers. We will start from a general solution applicable in various settings, and then show how to improve the effectiveness of our procedure by exploiting domain knowledge. We demonstrate the usefulness of our technique with a set of case studies taken from the domains of diagnosability and safety analysis.

3.12 Exploit Generation for Information Flow Leaks in Object-Oriented Programs

Reiner Haehnle (TU Darmstadt, DE)

Joint work of Do, Quoc Huy; Bubel, Richard; Haehnle, Reiner
Main reference Q. H. Do, R. Bubel, R. Hähnle, "Exploit Generation for Information Flow Leaks in Object-Oriented Programs," in Proc. of the 30th IFIP TC 11 Int'l Conf. on ICT Systems Security and Privacy Protection (SEC'15), IFIP Advances in Information and Communication Technology, Vol. 455, pp. 401–415, Springer, 2015.
URL http://dx.doi.org/10.1007/978-3-319-18467-8_27

We present a method for automated generation of exploits for information flow leaks in object-oriented programs. Given a flow policy and a security level specification, our approach combines self-composition, symbolic execution, computation of an insecurity formula, and model generation to produce a test input that witnesses a security leak (if one exists). The method is one instance of a general framework for generating test data that witnesses a given relational program property, for example, faults, regressions, etc. A prototypic tool called KEG implementing our method for Java target programs is available. It generates security exploits in the form of executable JUnit tests.

3.13 Saturation Theorem Proving for Herbrand Models

Matthias Horbach (MPI für Informatik – Saarbrücken, DE)

In system verification, we are often interested in analyzing specific models, usually Herbrand models over a given domain. The use of efficient first-order methods like superposition in such a setting is unsound, because the introduction of Skolem constants for existential variables changes the Herbrand domain.

I will present superposition calculi that can explicitly represent existentially quantified variables in computations with respect to a given fixed domain. They give rise to new decision procedures for minimal model validity and I will demonstrate how to employ them for counter model generation in the analysis of Petri nets and LTL formulas, as well as in local reasoning.

3.14 SMT-based Reactive Synthesis

Swen Jacobs (Universität des Saarlandes, DE)

We consider reductions of the synthesis problem for distributed and parameterized reactive systems to problems in satisfiability modulo theories (SMT). Given a (possibly parametric) system architecture and an LTL specification, we use automata theory (and possibly cutoff results from parameterized verification) to reduce the synthesis problem for implementations that satisfy the specification to a set of first-order constraints. The problem is encoded such that a model of the constraints represents both the desired implementation and an additional annotation that witnesses correctness. Our experimental results with different approaches to solve such constraints suggest that this is a very hard problem for existing SMT solvers.

3.15 Interpolation Synthesis for Quadratic Polynomial Inequalities and Combination with EUF

Deepak Kapur (University of New Mexico – Albuquerque, US)

Joint work of Gan, Ting; Dai, Liyun; Xia, Bican; Zhan, Naijun; Chen, Mingshuai

An algorithm for generating interpolants for formulas which are conjunctions of quadratic polynomial inequalities (both strict and nonstrict) is proposed. The algorithm is based on a key observation that quadratic polynomial inequalities can be linearized if they are concave. A generalization of Motzkin's transposition theorem is proved, which is used to generate an interpolant between two mutually contradictory conjunctions of polynomial inequalities, in a way similar to the linear inequalities case. This can be done efficiently using semi-definite programming but forsaking completeness. A combination algorithm is given for the combined theory of concave quadratic polynomial inequalities and the equality theory over uninterpreted functions symbols using a hierarchical framework for combining interpolation algorithms for quantifier-free theories. A preliminary implementation has been explored.

3.16 Obtaining Inductive Invariants with Formula Slicing

George Karpenkov (VERIMAG – Gières, FR)

Program analysis by abstract interpretation finds inductive invariants in a given abstract domain, over-approximating the reachable state-space. This over-approximation at every program location may lead to weak invariants, insufficient for proving a desired property. *Path focusing* and *large block encoding* alleviate this problem by requiring abstractions only at loop heads; at other control points, candidate invariants are expressed as first-order formulas within a decidable theory, precisely describing possible executions from the last loop head. This significantly improves the precision.

Our *formula slicing* approach goes further, by propagating first-order formulas *through* loop heads: formulas are weakened until they become inductive by replacing atomic predicates with "true".

We show that the problem of deciding the existence of a non-trivial weakening is Σ_2^p-complete. we propose the over-approximation approaches based on the existing algorithms from the literature.

The produced inductive weakenings can be conjoined to the invariant candidates expressed in the abstract domain, improving the analysis precision, as we demonstrate on a range of programs from the International Competition on Software Verification (SV-COMP).

3.17 Optimization modulo quantified linear rational arithmetic

Zachary Kincaid (University of Toronto, CA)

Joint work of Kincaid, Zachary; Farzan, Azadeh

The optimization modulo theories (OMT) problem is to compute the supremum of the value of some given objective term over all models of a given (satisfiable) formula. Recently, techniques have been developed for optimization modulo the theories of quantifier-free linear rational (and integer) arithmetic. In principle, these techniques can be also be applied to formulas with quantifiers, since linear rational (integer) arithmetic admits quantifier elimination. However, quantifier elimination is computationally expensive, and it may be possible to avoid it. I will present an algorithm for optimization modulo quantified linear rational arithmetic that works directly on quantified linear rational arithmetic formulas.

3.18 EPR-based BMC and k-induction with Counterexample Guided Abstraction Refinement

Konstantin Korovin (University of Manchester, GB)

Joint work of Khasidashvili, Zurab; Korovin, Konstantin; Tsarkov, Dmitry
Main reference Z. Khasidashvili, K. Korovin, D. Tsarkov, "EPR-based k-induction with Counterexample Guided Abstraction Refinement," in Proc. of the 2015 Global Conf. on Artificial Intelligence (GCAI'15), EPiC Series, Vol. 36, pp. 137–150, EasyChair, 2015.
URL http://www.easychair.org/publications/paper/EPR-based_k-induction_with_Counterexample_Guided_Abstraction_Refinement

In recent years it was proposed to encode bounded model checking (BMC) into the effectively propositional fragment of first-order logic (EPR). The EPR fragment can provide for a succinct representation of the problem and facilitate reasoning at a higher level. In this talk we present a novel abstraction-refinement approach based on unsatisfiable cores and models (UCM) for BMC and k-induction in the EPR setting. We have implemented UCM refinements for EPR-based BMC and k-induction in a first-order automated theorem prover iProver [1]. We also extended iProver with the AIGER format and evaluated it over the HWMCC'14 competition benchmarks. The experimental results are encouraging. We show that a number of AIG problems can be verified until deeper bounds with the EPR-based model checking.

This talk is based on [2].

References

1 K. Korovin. *Inst-Gen – a modular approach to instantiation-based automated reasoning*. In Programming Logics, ser. LNCS, A. Voronkov and C. Weidenbach, Eds., vol. 7797. Springer, pp. 239–270, 2013.
2 Z. Khasidashvili, K. Korovin, D. Tsarkov. *EPR-based k-induction with Counterexample Guided Abstraction Refinement*. EPiC Series, EasyChair, 2015.

3.19 Hyperresolution modulo Horn Clauses – generating infinite models

Christopher Lynch (Clarkson University – Potsdam, US)

When Ordered Resolution terminates on a satisfiable set of clauses, it is not always possible to constructively find a model. On the other hand, in Hyperresolution a model can be easily computed, but Hyperresolution rarely halts.

We present a method to identify some Horn clauses that lead to nontermination, and remove them from the Hyperresolution process. Instead of resolving these clauses, unification will be performed modulo those clauses. In many cases, this will force Hyperresolution to halt, and the result will determine an infinite Herbrand model with nice properties, e.g, closed under intersection.

We first apply this result to Cryptographic Protocol Analysis, where Horn clauses used to represent Intruder Abilities cause nontermination. If Hyperresolution modulo Intruder Abilities halts then the infinite Herbrand model gives all the messages an intruder could learn.

We extend this result to a more general class of Horn clauses, which may be useful for program analysis where it is difficult or impossible to find a finite model.

The work on Cryptographic Protocol Analysis is joint with Erin Hanna, David Myers and Corey Richardson.

3.20 Confluence and Certification

Aart Middeldorp (Universität Innsbruck, AT)

Joint work of Nagele, Julian; Felgenhauer, Bertram; Middeldorp, Aart
Main reference J. Nagele, B. Felgenhauer, A. Middeldorp, "Improving Automatic Confluence Analysis of Rewrite Systems by Redundant Rules," in Proc. of the 16th Int'l Conf. on Rewriting Techniques and Applications (RTA'15), LIPIcs, Vol. 36, pp. 257–268, Schloss Dagstuhl, 2015.
URL http://dx.doi.org/10.4230/LIPIcs.RTA.2015.257

We discuss the importance of certification for confluence. A simple technique is presented that increases the power of modern (certified) confluence tools considerably.

3.21 Mining the Archive of Formal Proofs

Tobias Nipkow (TU München, DE)

Joint work of Blanchette, Jasmin C.; Haslbeck, Maximilian; Matichuk, Daniel; Nipkow, Tobias
Main reference J. C. Blanchette, M. Haslbeck, D. Matichuk, T. Nipkow, "Mining the Archive of Formal Proofs," in Proc. of the 2015 Int'l Conf. on Intelligent Computer Mathematics (CICM'15), LNCS, Vol. 9150, pp. 3–17, Springer, 2015.
URL https://doi.org/10.1007/978-3-319-20615-8_1

The Archive of Formal Proofs is a vast collection of computer-checked proofs developed using the proof assistant Isabelle. We perform an in-depth analysis of the archive, looking at various properties of the proof developments, including size, dependencies, and proof style. This gives some insights into the nature of formal proofs.

3.22 SMT-Based Methods for Difference Logic Invariant Generation

Albert Oliveras (UPC – Barcelona, ES)

Joint work of Candeago, Lorenzo; Oliveras, Albert; Rodríguez-Carbonell, Enric

We consider the problem of synthesizing difference logic invariants for a restricted class of imperative programs: the ones whose transitions can be described as conjunctions of difference logic inequalities.

Our methodology is based on the so-called constraint-based method: we consider a template for each location as a candidate invariant, to which initiation and consecution conditions are imposed. Unlike in the general case, where Farkas' lemma is used to convert these conditions into formulas over non-linear arithmetic, in our particular case we show how we can use more efficient SMT-based techniques using only difference logic arithmetic.

3.23 How to avoid proving the absence of integer overflows

Andrei Paskevich (University Paris-Sud, FR)

Joint work of Clochard, Martin; Filliâtre, Jean-Christophe; Paskevich, Andrei
Main reference M. Clochard, J.-C. Filliâtre, A. Paskevich, "How to avoid proving the absence of integer overflows," to appear in Proc. of the 7th Int'l Conf. on Verified Software: Theories, Tools, and Experiments (VSTTE'15), as volume 9593 of LNCS; pre-print available as hal-01162661, 2016.
URL https://hal.inria.fr/hal-01162661

When proving safety of programs, we must show, in particular, the absence of integer overflows. Unfortunately, there are lots of situations where performing such a proof is extremely difficult, because the appropriate restrictions on function arguments are invasive and may be hard to infer. Yet, in certain cases, we can relax the desired property and only require the absence of overflow during the first n steps of execution, n being large enough for all practical purposes. It turns out that this relaxed property can be easily ensured for large classes of algorithms, so that only a minimal amount of proof is needed, if at all. The idea is to restrict the set of allowed arithmetic operations on the integer values in question, imposing a "speed limit" on their growth. For example, if we repeatedly increment a 64-bit integer, starting from zero, then we will need at least 2 to the power of 64 steps to reach an overflow; on current hardware, this takes several hundred years. When we do not expect any single execution of our program to run that long, we have effectively proved its safety against overflows of all variables with controlled growth speed. In this talk, we give a formal explanation of this approach and show how it is implemented in the context of deductive verification.

3.24 Compositional Program Analysis using Max-SMT

Albert Rubio (UPC – Barcelona, ES)

Joint work of Brockschmidt, Marc; Larraz, Daniel; Oliveras, Albert; Rodríguez-Carbonell, Enric; Rubio, Albert
Main reference M. Brockschmidt, D. Larraz, A. Oliveras, E. Rodríguez-Carbonell, A. Rubio, "Compositional Safety Verification with Max-SMT," to appear in Proc. of the 2015 Conf. on Formal Methods in Computer-Aided Design (FMCAD'15); pre-print available as arXiv:1507.03851v3 [cs.LO], 2015.
URL http://arxiv.org/abs/1507.03851v3

An automated compositional program verification technique for safety properties based on conditional inductive invariants is presented. For a given program part (e.g., a single loop) and a postcondition, we show how to, using a Max-SMT solver, an inductive invariant together with a precondition can be synthesized so that the precondition ensures the validity of the invariant and that the invariant implies the postcondition. From this, we build a bottom-up program verification framework that propagates preconditions of small program parts as postconditions for preceding program parts. The method recovers from failures to prove the validity of a precondition, using the obtained intermediate results to restrict the search space for further proof attempts.

Currently we are extending the framework to prove reachability properties by using conditional termination.

3.25 Exploiting Locality in Parametric Verification

Viorica Sofronie-Stokkermans (Universität Koblenz-Landau, DE)

Joint work of Damm, Werner; Horbach, Matthias; Sofronie-Stokkermans, Viorica
Main reference W. Damm, M. Horbach, V. Sofronie-Stokkermans, "Decidability of Verification of Safety Properties of Spatial Families of Linear Hybrid Automata," in Proc. of the 10th Int'l Symp. on Frontiers of Combining Systems (FroCoS'15), LNAI, Vol. 9322, pp. 186–202, Springer, 2015.
URL http://dx.doi.org/10.1007/978-3-319-24246-0_12

We show how hierarchical reasoning, quantifier elimination and model generation can be used to automatically provide guarantees that given parametric systems satisfy certain safety or invariance conditions. Such guarantees can be for instance expressed as constraints on parameters. Alternatively, hierarchical reasoning combined with techniques for model generation allows us to construct counterexamples which show how unsafe states can be reached.

In this talk we focus on the case of systems composed of an unbounded number of similar components (modeled as linear hybrid automata), whose dynamic behavior is determined by their relation to neighboring systems. We present a class of such systems and a class of safety properties whose verification can be reduced to the verification of (small) families of neighboring systems of bounded size, and identify situations in which such verification problems are decidable, resp. fixed parameter tractable. We illustrate the approach with an example from coordinated vehicle guidance.

3.26 Verified AC-Equivalence Checking in Isabelle/HOL

Christian Sternagel (Universität Innsbruck, AT)

Joint work of Bertram, Felgenhauer; Sternagel, Christian

We present an algebraic correctness proof of an executable AC-equivalence check that we formalized in Isabelle/HOL. This work constitutes the basis for extending our Isabelle/HOL Formalization of Rewriting (IsaFoR) with results on rewriting modulo associativity and commutativity.

3.27 Thousands of Models for Theorem Provers – The TMTP Model Library

Geoff Sutcliffe (University of Miami, US)

The TPTP World is a well established infrastructure that supports research, development, and deployment of Automated Theorem Proving (ATP) systems for classical logics. The TPTP World includes the TPTP problem library, the TSTP solution library, standards for writing ATP problems and reporting ATP solutions, tools and services for processing ATP problems and solutions, and it supports the CADE ATP System Competition (CASC).

This work describes a new component of the TPTP World – the Thousands of Models for Theorem Provers (TMTP) Model Library. This will be a corpus of models for identified sets of axioms in the TPTP, along with tools for interpreting formulae wrt models, tools for translating from from model form to another, interfaces for visualizing models, etc. The TMTP will support the development of semantically guided theorem proving ATP systems, provide examples for developers of model finding ATP systems, and provide insights into the semantic structure of axiom sets.

3.28 Conflict-based Quantifier Instantiation for SMT

Cesare Tinelli (University of Iowa – Iowa City, US)

Joint work of Reynolds, Andrew; Tinelli, Cesare; de Moura, Leonardo
Main reference A. Reynolds, C. Tinelli, L. de Moura, "Finding conflicting instances of quantified formulas in SMT," in Proc. of the 2014 Conf. on Formal Methods in Computer-Aided Design (FMCAD'14), pp. 195–202, IEEE, 2014.
URL http://dx.doi.org/10.1109/FMCAD.2014.6987613

Satisfiability Modulo Theories (SMT) solvers have been used successfully in a variety of applications including verification, automated theorem proving, and synthesis. While such solvers are highly adept at handling ground constraints in several decidable background theories, they primarily rely on heuristic quantifier instantiation methods such as E-matching to process quantified formulas. The success of these methods is often hindered by an overproduction of instances, which makes ground level reasoning difficult. This talk introduces a new technique that alleviates this shortcoming by first discovering instances of the quantified formulas that are in conflict with the current state of the solver. The solver only resorts to traditional heuristic methods when such instances cannot be found, thus decreasing its dependence upon E-matching. Extensive experimental results show that this technique significantly reduces the number of instantiations required by an SMT solver to answer "unsatisfiable" for several benchmark libraries, and consequently leads to improvements over state-of-the-art implementations.

3.29 Learn Fresh: Model-Guided Inferences

Christoph Weidenbach (MPI für Informatik – Saarbrücken, DE)

Joint work of Alagi, Gabor; Teucke, Andreas; Weidenbach, Christoph
Main reference C. Weidenbach, "Automated Reasoning Building Blocks," in R. Meyer, A. Platzer, H. Wehrheim (eds.), "Correct System Design – Symposium in Honor of Ernst-Rüdiger Olderog on the Occasion of His 60th Birthday", LNCS, Vol. 9360, pp. 172–188, Springer, 2015.
URL http://dx.doi.org/10.1007/978-3-319-23506-6_12

I investigate the relationship between candidate models, inferences and redundancy. It turns out that clauses learned by the CDCL calculus correspond to the result of superposition inferences and are not redundant. The result can be lifted to the Bernays Schoenfinkel class but it is open how it can be lifted to first-order logic, in general. For-first order logic abstraction mechanisms are needed that result in effective model representations enabling decision procedures for clause validity.

References

1 Gabor Alagi and Christoph Weidenbach. NRCL – a model building approach to the Bernays-Schönfinkel fragment. In Carsten Lutz and Silvio Ranise, editors, *Frontiers of Combining Systems, 10th International Symposium, FroCoS 2015, Wroslav, Poland, 2015. Proceedings*, volume 9322 of *LNCS*, pages 69–84. Springer, 2015.

2 Peter Baumgartner, Alexander Fuchs, and Cesare Tinelli. Lemma learning in the model evolution calculus. In *LPAR*, volume 4246 of *Lecture Notes in Computer Science*, pages 572–586. Springer, 2006.

3 Harald Ganzinger and Konstantin Korovin. New directions in instatiation–based theorem proving. In Samson Abramsky, editor, *18th Annual IEEE Symposium on Logic in Computer Science, LICS'03*, LICS'03, pages 55–64. IEEE Computer Society, 2003.

4 Robert Nieuwenhuis, Albert Oliveras, and Cesare Tinelli. Solving sat and sat modulo theories: From an abstract davis–putnam–logemann–loveland procedure to dpll(t). *Journal of the ACM*, 53:937–977, November 2006.

5 Ruzica Piskac, Leonardo Mendonça de Moura, and Nikolaj Bjørner. Deciding effectively propositional logic using DPLL and substitution sets. *Journal of Automated Reasoning*, 44(4):401–424, 2010.

6 Andreas Teucke and Christoph Weidenbach. First-order logic theorem proving and model building via approximation and instantiation. In Carsten Lutz and Silvio Ranise, editors, *Frontiers of Combining Systems, 10th International Symposium, FroCoS 2015, Wroslav, Poland, 2015. Proceedings*, volume 9322 of *LNCS*, pages 85–100. Springer, 2015.

7 Christoph Weidenbach. Automated reasoning building blocks. In Roland Meyer, André Platzer, and Heike Wehrheim, editors, *Correct System Design – Symposium in Honor of Ernst-Rüdiger Olderog on the Occasion of His 60th Birthday, Oldenburg, Germany, September 8-9, 2015. Proceedings*, volume 9360 of *Lecture Notes in Computer Science*, pages 172–188. Springer, 2015.

3.30 Partial Models for More Proofs

Sarah Winkler (Microsoft Research UK – Cambridge, GB)

Joint work of Sato, Haruhiko; Winkler, Sarah
Main reference H. Sato. S. Winkler, "Encoding Dependency Pair Techniques and Control Strategies for Maximal Completion," in Proc. of the 25th Int'l Conf. on Automated Deduction (CADE'15), LNAI, Vol. 9195, pp. 152–162, Springer, 2015.
URL http://dx.doi.org/10.1007/978-3-319-21401-6_10

Maximal completion constitutes a powerful and fast Knuth-Bendix completion procedure based on MaxSAT/MaxSMT solving. Recent advancements let Maxcomp improve over other automatic completion tools, and produce novel complete systems [1]: (1) Termination techniques using the dependency pair framework are encoded as satisfiability problems, including dependency graph and reduction pair processors. (2) Instead of relying on pure maximal completion, different SAT-encoded control strategies are exploited.

Maximal completion can also produce complete systems for subtheories (partial models): This is done by encoding control strategies which, for instance, give preference to rewrite systems where the number of non-joinable critical pairs is minimal.

Exploiting this feature, we use maximal completion to guide equational proof search. More precisely, we investigate how the addition of a partial model R (and a reduction order to prove it terminating) to unit equality problems from TPTP influences the behavior of

provers on these problems. When restricting to reduction orders which are total on ground terms, there always exists a ground complete system extending R, hence completeness is not compromised. Experiments with the theorem prover SPASS show that supplying complete systems for subtheories is indeed beneficial, though adding the respective reduction order has more effect than the additional rewrite rules.

References

1 H. Sato and S. Winkler. Encoding Dependency Pair Techniques and Control Strategies for Maximal Completion. In *CADE*, volume 9195 of *LNCS*, pages 152–162, 2 2015.

Participants

- Noran Azmy
MPI für Informatik – Saarbrücken, DE
- Franz Baader
TU Dresden, DE
- Peter Baumgartner
NICTA – Canberra, AU
- Christoph Benzmüller
FU Berlin, DE
- Nikolaj S. Bjørner
Microsoft Corporation – Redmond, US
- Jasmin Christian Blanchette
INRIA Lorraine – Nancy, FR
- Martin Bromberger
MPI für Informatik – Saarbrücken, DE
- Catherine Dubois
ENSIIE – Evry, FR
- Bruno Dutertre
SRI – Menlo Park, US
- Carsten Fuhs
Birkbeck, Univ. of London, GB
- Silvio Ghilardi
University of Milan, IT
- Jürgen Giesl
RWTH Aachen University, DE
- Alberto Griggio
Bruno Kessler Foundation – Trento, IT
- Arie Gurfinkel
Carnegie Mellon University – Pittsburgh, US
- Liana Hadarean
University of Oxford, GB
- Reiner Hähnle
TU Darmstadt, DE
- Matthias Horbach
MPI für Informatik – Saarbrücken, DE
- Swen Jacobs
Universität des Saarlandes, DE
- Dejan Jovanovic
SRI – Menlo Park, US
- Deepak Kapur
University of New Mexico – Albuquerque, US
- George Karpenkov
VERIMAG – Gières, FR
- Zachary Kincaid
University of Toronto, CA
- Konstantin Korovin
University of Manchester, GB
- Christopher Lynch
Clarkson Univ. – Potsdam, US
- Aart Middeldorp
Universität Innsbruck, AT
- Tobias Nipkow
TU München, DE
- Albert Oliveras
UPC – Barcelona, ES
- Andrei Paskevich
University Paris-Sud, FR
- Alexander Rabinovich
Tel Aviv University, IL
- Giles Reger
University of Manchester, GB
- Albert Rubio
UPC – Barcelona, ES
- Andrey Rybalchenko
Microsoft Research UK – Cambridge, GB
- Stephan Schulz
Duale Hochschule Baden-Württemberg – Stuttgart, DE
- Viorica Sofronie-Stokkermans
Universität Koblenz-Landau, DE
- Christian Sternagel
Universität Innsbruck, AT
- Geoff Sutcliffe
University of Miami, US
- Cesare Tinelli
Univ. of Iowa – Iowa City, US
- Andrei Voronkov
University of Manchester, GB
- Christoph Weidenbach
MPI für Informatik – Saarbrücken, DE
- Sarah Winkler
Microsoft Research UK – Cambridge, GB
- Burkhart Wolff
University Paris-Sud, FR
- Jian Zhang
Chinese Academy of Sciences – Beijing, CN

Report from Dagstuhl Seminar 15382

Modeling and Simulation of Sport Games, Sport Movements, and Adaptations to Training

Edited by

Ricardo Duarte[1], Björn Eskofier[2], Martin Rumpf[3], and Josef Wiemeyer[4]

1 **University of Lisbon, PT,** rduarte@fmh.ulisboa.pt
2 **Universität Erlangen-Nürnberg, DE,** bjoern.eskofier@fau.de
3 **Universität Bonn, DE,** martin.rumpf@ins.uni-bonn.de
4 **TU Darmstadt, DE,** wiemeyer@sport.tu-darmstadt.de

Abstract

This report documents the program and the outcomes of Dagstuhl Seminar 15382 "Modeling and Simulation of Sport Games, Sport Movements, and Adaptations to Training". The primary goal of the seminar was the continuation of the interdisciplinary and transdisciplinarity research in sports and computer science with the emphasis on modeling and simulation technologies. In this seminar, experts on modeling and simulation from computer science, sport science, and industry were invited to discuss recent developments, problems and future tasks in these fields. For instance, computational models are applied in motor control and learning, biomechanics, game analysis, training science, sport psychology, and sport sociology. However, for these models to be adequate, accurate and fully utilized to their potential, major inputs from both computer and sports scientists are required. To bridge the potential disconnect between the skill sets of both sets of experts, the major challenge is to equip both computer and sports scientists with a common language and skill sets where both parties can communicate effectively. The seminar focused on three application areas: sport games, sport movements, and adaptations to training. In conclusion, the seminar showed that the different application areas face closely related problems. The disciplines could mutually benefit from each other combing the knowledge of domain experts in e.g. computer vision, biomechanics, and match theory.

Seminar September 13–16, 2015 – http://www.dagstuhl.de/15382
1998 ACM Subject Classification I.6.3 Simulation and Modeling – Applications
Keywords and phrases Modeling, Simulation, Machine Learning, Sports Science, Biomechanics, Sport Games, Training Adaptation
Digital Object Identifier 10.4230/DagRep.5.9.38
Edited in cooperation with Eva Dorschky

1 Executive Summary

Josef Wiemeyer
Ricardo Duarte
Björn Eskofier
Martin Rumpf

Computational modeling and simulation are essential to analyze human motion and interaction in sport science, sport practice and sport industry. Applications range from game analysis,

issues in exercising like training load-adaptation relationship, motor control and learning, to biomechanical analysis. New challenges appear due to the rapid development of information and communication technologies (ICT) as well as the enormous amount of data being captured within training and competition domains. The motivation of this seminar was to enable an interdisciplinary exchange between sports and computer scientists as well as sport practice and industry to advance modeling and simulation technologies in selected fields of applications: sport games, sport movements and adaptations to training.

From September 13 to September 16, 2015 about 29 representatives of science, practice and industry met at the Leibniz-Zentrum für Informatik in Schloss Dagstuhl to discuss selected issues of modelling and simulation in the application fields of sport games, sport movements and adaptation to training. This seminar was the fifth in a series of seminars addressing computer science in sport, starting in 2006. Based on previously selected issues, four main streams were identified:

- Validation and model selection
- Sensing and tracking
- Subject-specific modelling
- Training and sport games

The talks addressing these four topics are summarized in this report. They have been arranged according to the three main application fields: sport games, sport movements, and adaptations to training. In addition, generic comments on modeling in industry and science are presented. Moreover, the final discussion is summarized and a conclusion of the seminar is drawn.

2 Table of Contents

3 Overview of Talks: Sport Games

3.1 On the Use of Tracking Data to Support Coaches in Professional Football

John Komar (Prozone Sports Ltd. – Leeds, GB)

A new era in sports sciences is emerging with the advent of new digital tools for the analysis of athletes' training, performance and health. However, massive technological changes emerging over the past few years have led to a new issue, captured in the term Big Data. A clear challenge for sports scientists and practitioners is to understand which data matter and how to interpret them. The real challenge for the professional world is now to move from data-driven decisions to data-informed decisions. From this perspective, my talk addresses the question of investigating tracking data in football (i.e. both events data and players position in x,y,t coordinate) in order to derive meaningful and functional metrics. Broadly speaking, the idea is to overcome traditional generic statistics (e.g., number of passes done, number of shots, number of tackles, percentage of ball possession) by combining them into meaningful items for coaches and practitioners (i.e. information that can help them to make informed choices for recruitment, injury prevention or match analysis). More specifically, part of the work presented looked at the number of goals one could expect from a player, based on the location of the shots he took [1]. A model of expected goals per field position was derived from previous seasons and then compared to the actual number of goals scored by a specific player. This comparison can thus inform about the ability of this player to under- or overachieve in shots success. Looking at probability of scoring goals during a season, coaches can then be informed about conversion rate of a player, but rather than a raw goals/shots ratio, this goal expectancy metrics gives more context to the conversion ability (e.g., it can take into account the position of the shot, the defensive density during the shots). Combined to other measures like ball movement effectiveness, this kind of metrics can feed models of offensive contribution in professional football.

References

1 H. Ruiz, P.J. Lisboa, P.J. Neilson, and W. Gregson, "Measuring scoring efficiency through goal expectancy estimation," in *Proc. ESANN'15*, Bruges, 2015.

3.2 The "Practical Impact Debate" in Performance Analysis

Martin Lames (TU München, DE)

Problem

Mainstream research in Performance Analysis (PA) applies traditional linear methods to data analysis, e.g. ANOVA. In this context, complex interactions in game sports are modelled quite poorly, e.g. quality of opponent is introduced as another static variable in a linear model: rank in final table of league [8, 9]. Fluctuations in behaviour, typically a constitutive pattern of game sports, are treated as measurement error and sought to be controlled by

enlarging sample size [3]. On the other hand, practical support is considered to be the main purpose of PA [6]. McGarry (2009) sees advancing the understanding of sports mainly with regard to improving future outcomes. In this situation, a review of Drust and Green (2013) gave rise to the "Practical Impact Debate". The authors stated: "... it can be suggested that the influence of the scientific information that is available has a relatively small influence on the day-to-day activities within the "real world" of football." (p. 1382).

The "Practical Impact Debate"

This statement was supported by a review of Mackenzie and Cushion (2013). They analysed existing PA-research and found widespread methodological problems as well as a missing research strategy for practical support. Carling et al. (2014) replied to this paper and – among other issues – defended analysts working in practice against some methodological criticism by the demands of conducting research in practical settings. He frequently referred to his earlier paper with the telling header: "Should we be more pragmatic in our approach?" [1].

Remarks on the "Practical Impact Debate"

The problem addressed has its root in a lacking distinction between applied and basic research. This issue is mentioned by Mackenzie and Cushion (2013) without drawing consequences for research strategies to be applied. In the eyes of the author it is helpful to distinguish between practical PA (PPA) and theoretical PA (TPA) [5]. TPA aims at clarifying the general structure of sports. It looks for general rules, appropriate models (dynamical systems modelling) and needs large, representative samples. PPA is in some respects the opposite. It may be defined as PA activities conducted in practice, i.e. analysing training and competition to support a team or a player. PPA is interested in any information that provides practical support and typically works with and for a single case, the own team or player. Moreover, practical consequences for training may not be found algorithmically from data collected but need a thorough interpretation with a background of in-depth knowledge from the many sources of information available in a professional football club (medical, physiotherapy, fitness, training are only the most important ones). So, in PPA – whether with or without methodological awareness – qualitative research methodology is used, which may be considered as a typical feature as well. With a basic distinction between TPA and PPA researchers analysing the general structure of performances are relieved from demonstrating an immediate practical use of their results, and analysts working in practice shouldn't feel obliged any more to refute criticism from the point of view of basic research on their pragmatic solutions. Nevertheless, there is a tight connection between both areas. Measures in practice should be in agreement with general findings about the nature of the game, and in the other direction, findings in practice can give rise to new hypotheses on its structure.

Agenda for computer science in PA

What are consequences of the "Practical Impact Debate" for the interdisciplinary research field of computer science in sports? It becomes clear that there are different agendas for it working in either TPA or PPA. Nevertheless, both areas depend on data on the matches meaning that there remains a general agenda including the detection of positions and actions. The automatisation of action detection will be a prominent future task as well as drawing inferences on higher level from action and position data, like analysing constructs not available before like availability or more complex tactical behaviours like passing style or pressing. Specifically for TPA the introduction of more appropriate models will determine a future

agenda. As interaction and dynamics are constitutive for game sports these features should be included in any future approach. What PPA is concerned challenges lie in improving informational service for coaches and athletes. We will see information systems that combine the different sources of information by machine learning technologies to arrive at advanced versions of automated data mining, for example driven by assumptions on the nature of information needed and driven by query habits of the user. All in all, there is a challenging but also promising future for computer science in PA to be expected.

References

1 C. Carling, C. Wright, L.N. Nelson, and P.S. Bradley, "Comment on ?Performance analysis in football: A critical review and implications for future research," *J Sport Sci*, vol. 32, pp. 2–7, 2014.
2 B. Drust and M. Green, "Science and football: evaluating the influence of science on performance," *J Sport Sci*, vol. 31, pp. 1377–1382, 2013.
3 M. Hughes, S. Evans, and J. Wells, "Establishing normative profiles in performance analysis," *Int J Perform Anal Sport*, vol. 1, pp. 4–27, 2001.
4 M. Lames and G. Hansen, "Designing observational systems to support top-level teams in game sports," *Int J Perform Anal Sport*, vol. 1, pp. 85–91, 2001.
5 M. Lames and T. McGarry, "On the search for reliable performance indicators in game sports," *Int J Perform Anal Sport*, vol. 7, no. 1, pp. 62–79, 2007.
6 R. Mackenzie and C. Cushion, "Performance analysis in football: A critical review and implications for future research," *J Sport Sci*, vol. 31, pp. 639–676, 2013.
7 T. McGarry, D.I. Anderson, S.A. Wallace, M.D. Hughes, and I.M. Franks, "Sport competition as a dynamical self-organizing system," *J Sport Sci*, vol. 20, pp. 771–781, 2002.
8 P. O'Donoghue, "Interacting Performances Theory," *Int J Perform Anal Sport*, vol. 9, pp. 26–46, 2009.
9 A. Tenga and E. Sigmundstad, "Characteristics of goal-scoring possessions in open-play: Comparing the top, in-between and bottom teams from professional soccer league," *Int J Perform Anal Sport*, vol. 11, pp. 545–552, 2011.

3.3 Performance Analysis in Soccer Based on Knowledge Discovery Approach

Roland Leser (Universität Wien, AT)

Joint work of Leser, Roland; Moser, Bernhard; Hoch, Thomas; Baca, Arnold

The contribution addresses the development of explanation models for key performance indices extracted from position and tracking data. The goal is to come up with an explanation rather than a black box model which allows the explanation of the performance by means of behavioral patterns. For this purpose, a knowledge discovery approach for extracting behavioral patterns from position measurement data in small-sided soccer games is outlined. The resulting kinematic feature space of spatial-temporal variables is high-dimensional. In order to maintain interpretability for coaches, therefore, the reduction to a reasonable amount of variables is needed. To this end, the Laplacian Score method is introduced which yields promising results. This method aims at reducing the dimensionality while keeping the structure of the data. In a further step clusters in this reduced feature space are induced by taking key performance indicators into account. Promisingly, for small-sided games this

approach leads to expressive linguistically interpretable explanation models. Our contribution aims at discussing the potential of this approach also for more complex scenarios.

3.4 Individual Ball Possession in Soccer

Daniel Link (TU München, DE)

This paper describes models for detecting individual and team ball possession in soccer based on position data. The types of ball possession are classified as Individual Ball Possession (IBC), Individual Ball Action (IBA), Individual Ball Control (IBC), Team Ball Possession (TBP), Team Ball Control (TBC) und Team Playmaking (TPM) according to the type of ball control involved. The machine learning approach used is able to determine how long the ball spends in the sphere of influence of a player based on the distance between the players and the ball together with their direction of motion, speed and the acceleration of the ball. The degree of ball control exhibited during this phase is classified based on the spatio-temporal configuration of the player controlling the ball, the ball itself and opposing players using a Bayesian network.The evaluation and illustrative application of this approach uses data taken from a game in a top European league. When applied to error-corrected raw data, the algorithm showed an accuracy of 92 % (IBA), 86 % (IBP), and 92 % (IBC) using a tolerance of 0.6 s. This is well above the accuracy achieved manually by the competition information providers of 52 % (TBC). There were 1291 phases involving ball control (IBC) totalling 29:39 min with a gross game time of 90:12 min and a net game time of 57:56 min. This initial analysis of ball possession at the player level indicates IBC times of between 0:22 and 3:18 min. The shortest ball control times are observed for the centre forwards of each team (0.9 s) and the full backs of the losing team (0.7 s) and the longest for the losing team's goalkeeper (2.9 s). This can be interpreted as a tendency for the defenders to try and clear the ball as quickly as possible and the goalkeeper attempting to slow the pace of game.

3.5 Understanding Actions in a Sports Context

Jim Little (University of British Columbia – Vancouver, CA)

Understanding human action is critical to surveillance, monitoring, and situation understanding. Sports present events where the types of actions are limited and depend on roles, locations, and situations. Understanding the actions, activity and performance of the players interests many. Action understanding in broadcast video has led to progress in tracking, recognition, camera rectification, pose, and multi-view action recognition.

3.6 Performance Analysis in Soccer Based on Knowledge Discovery Approach

Bernhard Moser (Software Competence Center – Hagenberg, AT)

The contribution addresses the development of explanation models for key performance indices extracted from position and tracking data. The goal is to come up with an explanation rather than a black box model which allows the explanation of the performance by means of behavioral patterns. For this purpose, a knowledge discovery approach for extracting behavioral patterns from position measurement data in small-sided soccer games is outlined. The resulting kinematic feature space of spatial-temporal variables is high-dimensional. In order to maintain interpretability for coaches, therefore, the reduction to a reasonable amount of variables is needed. To this end, the Laplacian Score method is introduced which yields promising results. This method aims at reducing the dimensionality while keeping the structure of the data. In a further step clusters in this reduced feature space are induced by taking key performance indicators into account. Promisingly, for small-sided games this approach leads to expressive linguistically interpretable explanation models. Our contribution aims at discussing the potential of this approach also for more complex scenarios.

3.7 Covered Distances of Handball Players Obtained by an Automatic Tracking Method

Tiago Guedes Russomanno (University of Brasilia, BR)

Joint work of Russomanno, Tiago Guedes; Misuta, Milton Shoiti; Menezes, Rafael Pombo; Brandão, Bruno Cedraz; Figueroa, Pascual Jovino; Leite, Neucimar Jeronimo; Goldenstein, Siome Klein; Barros, Ricardo Machado Leite

Main reference T. G. Russomanno, M. S. Misuta, R. P.Menezes, B. C. Brandão, P. J. Figueroa, N. J. Leite, S. K. Goldstein, R. M. L. Barros, "Covered distances of handball players obtained by an automatic tracking method," in Proc. of the 25th Int'l Symp. on Biomechanics in Sports (ISBS'07), pp. 324–327, University of Konstanz, 2007.

URL https://ojs.ub.uni-konstanz.de/cpa/article/view/473

Tracking players in sports events is still a topic of discussion in sport science and the data provided by this tracking is useful for team staff to evaluate team performance. Therefore, the aim of this work was to obtain the distances covered by handball players and their velocities during a match using a new approach based on automatic tracking method described in Figueroa et. al. [1, 2] and the Adaboost detector [5]. A whole game of a Brazilian regional handball championship for players under age of 21 was recorded. Applying the mentioned automatic tracking, the accumulated covered distances and the velocities were calculated for all the players. The results of average covered distances (±SD) in the 1st and 2nd halves were 2199 (±230) and 2453 (±214). The results of covered distances and the velocities allow individual and collective analyses of the players by the team staff. The proposed method revealed to be a powerful tool to improve physical analysis of the handball players.

References

1 P. J. Figueroa, N. J. Leite, and R. M. L. Barros, "Tracking soccer players aiming their kinematical motion analysis," *Comput Vis Image Underst*, vol. 101, no. 2, pp. 122-135, 2006.

2 P. J. Figueroa, N. J. Leite, and R. M. L. Barros, "Background recovering in outdoor image sequences: An example of soccer players segmentation," *Image Vision Comput*, vol. 24, no. 4, pp. 363-374, 2006.
3 M. Kristan, J. Pers, J., M. Perse, M. Bon, and S. Kovacic, "Multiple interacting targets tracking with application to team sports," in *Proc. ISAP*, Zagreb, 2005, pp. 322-327.
4 M. S. Misuta, R. P. Menezes, P. J. Figueroa, S. A. Cunha, and R. M. L. Barros, "Representation and analysis of soccer player trajectories," in *Proc. ISB*, Cleveland, 2005, vol. 415.
5 K. Okuma, A. Taleghani, N. de Freitas, J. Little, and D. Lowe "A boosted particle filter: multitarget detection and tracking," in *Proc. ECCV*, Prague, 2004, pp. 28-38.
6 P. Viola and M. J. Jones, "Rapid Object Detection using a Boosted Cascade of Simple Features," in *Proc. CVPR*, Kauai, 2001, vol. 1, pp. 511-518.

3.8 Data Requirements in the Sports Data Industry

Malte Siegle (Sportradar AG – St. Gallen, CH)

Different markets do have different requirements concerning data depth, data delivery speed and data quality. Here is a short overview about three markets: (1) Professional Sports, (2) Media, and (3) Bookmakers / Betting.

1. Professional Sports (Teams, Clubs, Leagues)
   - Strong need for deep data
   - Delivery speed not too important, as most teams use the data post-match. Moreover, live-match analyses are sometimes prohibited.
   - Data quality is important. Performance analysis based on imprecise data could cause wrong conclusions.
2. Media
   - Strong need for deep data (e.g. for story telling)
   - Delivery speed Not too important as there is a broadcasting latency anyways
   - Data quality is not important.
3. Bookmakers / Betting
   - Data depth is not important, as there is a market limit anyways. If you would offer too many bets, you would cannibalize your own market.
   - Delivery speed is a must have and very important
   - Just as data quality is. Wrong data could cause a of lot trouble and punters would claim their right to get their money back

Consequently, for a company like Sportradar it is very important to fulfill all different requirements. This results in the claim to be able to provide fast, highly accurate, and deep data.

3.9 Factors that Influence Scoring Dynamics in Low-Scoring and High-Scoring Team Games

Anna Volossovitch (University of Lisbon, PT)

Joint work of Volossovitch, Anna; Pratas, José; Dumangane, Montezuma; Rosati, Nicoletta
Main reference M. Dumangane, N. Rosati, A. Volossovitch, "Departure from independence and stationarity in a handball match," Journal of Applied Statistics, 36(7):723–741, 2009.
URL http://dx.doi.org/10.1080/02664760802499329

Research in match analysis frequently attempts to establish causal relationships between isolated performance variables and goal scoring or game outcome. This approach reduces the complexity of performance by presenting it in overly descriptive and regular ways, which do not reflect properly the curse of the game. The purpose of the presentation was to discuss two examples of the analysis of factors, which could influence the scoring dynamic during a match in handball and in football. In the first example, the influence of teams past performance on the present teams performance was evaluated throughout the handball match using the model with time-varying parameters. This model estimates the probability of scoring as a function of the past performance of the opposing team and the current match result. This assessment considers the specific context of the game situation, the teams rankings, the match equilibrium and the number of ball possessions per match. In the second example the performance indicators, which had a significant effect on the time of the first goal scoring in football has been identified using Cox time-dependent proportional hazard model. The survival analysis is suggested to be a suitable tool to identify which and how performance indicators influence the time of the first ball is scored in different competitive context.

References

1 J. Pratas, A.Volossovitch, and A. I. Carita, "What performance indicators influence the time of the first goal in the match?," In *Proc. World Congress of Performance Analysis of Sport X*, Opatija, 2014, p. 102.
2 A. Volossovitch, M. Dumangane, and N. Rosati, "The influence of the pace of match on the dynamic of handball game," *Int. J Sports Psychol*, vol. 41, no. 4, pp. 117–118, 2010.
3 M. Dumangane, N. Rosati, and A. Volossovitch, "Departure from independence and stationarity in a handball match," *J Appl Stat*, vol. 36, no. 7, pp. 723–741, 2009.

4 Overview of Talks: Sport Movement

4.1 Predicting Human Responses to Environmental Changes

Eva Dorschky (Universität Erlangen – Nürnberg, DE)

Joint work of Dorschky, Eva; van den Bogert, Antonie J.; Schlarb, Heiko; Eskofier, Björn
Main reference E. Dorschky, et al., "Predictive Musculoskeletal Simulation of Uphill and Downhill Running," in *Proc. ECSS*, Malmö, 2015, p. 126.

Predicting human responses to environmental changes is necessary for biomechanical analysis and sports product design. If case studies, environmental conditions or prototypes cannot be realized, modeling and simulation can be used instead. The aim of this work was to evaluate a method of predictive musculoskeletal simulation [1] for uphill and downhill running. A

study was simulated by randomizing the model's muscle parameters. The predicted energy costs for running at different slopes were compared to literature [2]. Future work includes a personalization of biomechanical models to represent individual athletes as well as population groups. The sensitivity of simulation results to model parameters will be studied to ensure robust simulation results.

References

1 A. J. van den Bogert, M. Hupperets, H. Schlarb, and B. Krabbe,"Predictive musculoskeletal simulation using optimal control: effects of added limb mass on energy cost and kinematics of walking and running," in *Proc. Inst Mech Eng, Part P: J Sports Eng Technol*, vol. 226, pp. 123-133, 2012.

2 A. E. Minetti, C. Moia, G. S. Roi, D. Susta, and G. Ferretti, "Energy cost of walking and running at extreme uphill and downhill slopes," *J Appl Physiol*, vol. 93, no. 3, pp. 1039-1046, 2002.

4.2 Wearable Computing Systems for Recreational and Elite Sports

Björn Eskofier (Universität Erlangen-Nürnberg, DE)

Wearable computing systems play an increasingly important role in recreational and elite sports. They comprise of two important parts. The first are sensors embedded into clothes and equipment that are used for physiological (ECG, EMG) and biomechanical (accelerometer, gyroscope) data recording. The second are signal processing and data mining algorithms implemented on wearable computers (smartphones, watches) that are used for analysis of the recorded data. Wearable computing systems can provide support, real-time feedback and coaching advice to sportsmen of all performance levels. In order to implement these systems, several challenges have to be addressed. Our work focusses on four of the most prevalent of these:

- Integration: sensors and microprocessors have to be embedded unobtrusively and have to record a variety of signals.
- Communication: sensors and microprocessors have to communicate in body-area-networks in a secure, safe and energy-saving manner.
- Interpretation: physiological and biomechanical data have to be interpreted using signal processing and machine learning methods.
- Simulation and modeling: understanding of sensor data is needed to model processes in sports more accurately, simulation methodologies help here to provide basic information to drive those models.

4.3 What is the Right Model?

Karen Roemer (Central Washington University – Ellensburg, US)

Investigating human movements requires using biomechanical models to perform kinematic and kinetic analyses. Depending on the available motion analysis system or software packages, anthropometric models, tracking models, joint models etc. are applied to quantify kinematic and kinetic variables. Two standard biomechanical models (OpenSim and Visual3D) were used to analyze a simple stepping task. Similarities and differences of kinematic and kinetic results for both models were discussed.

4.4 Model-Based Tracking of Human Motion

Antonie van den Bogert (Cleveland State University – Cleveland, US)

Two sensing modalities are in use for field studies of human movement: inertial sensing and video. While both are suitable for analysis of human movement during sports events, data quality is usually far inferior to those encountered during laboratory conditions. Inspired by the classical Kalman filtering concept, we consider using a dynamic model to improve the estimates of the state trajectory of the system. This approach presents the estimation problem as an optimal control problem: find state and control trajectories that satisfy system dynamics and minimize a cost function. For tracking of sensor data, the cost function consists of the sum of squared errors between simulated and measured sensor signals. When using a musculoskeletal model, an extra term, representing muscular effort, must be added to ensure a unique solution. This is due to the classical load sharing redundancy: humans have more muscles than strictly necessary to produce movement.

Efficient solution methods have been developed to solve this optimal control problem, and the approach was successfully used to obtain a detailed analysis of a landing movement during skiing, based on low-quality video data [1]. The same approach was used to perform a full dynamic gait analysis, including muscle force estimation, with body-mounted accelerometers [2]. The accelerometer-based analysis was not good enough for clinical applications, because it was too sensitive to the unmodeled dynamics (damped vibrations) of the accelerometer attachments. Improvement is expected when the instrumentation is supplemented by gyroscopic angular velocity sensors.

Model-based state estimation will reduce the sensitivity to measurement error, and there are additional advantages. The estimation process includes estimation of the full state of the system, including variables such as muscle forces which could not be directly obtained from sensor signals. The raw data is then not only filtered, but also enriched by the dynamic model. A second advantage is that a dynamically consistent simulation is obtained as an additional result. Such simulations can be useful to explore "what if" scenarios, such as sports injuries that are caused by unfavorable landing postures [3].

References

1 A. J. van den Bogert, D. Blana and D. Heinrich, "Implicit methods for efficient musculoskeletal simulation and optimal control," *Procedia IUTAM*, vol. 2, pp. 297-316, 2011.

2 O. Nwanna, "Validation of an Accelerometry Based Method of Human Gait Analysis," M.S. thesis, Cleveland State University, 2014, http://rave.ohiolink.edu/etdc/view?acc_num=csu1400424346
3 D. Heinrich, A. J. van den Bogert, and W. Nachbauer, "Relationship between jump landing kinematics and peak ACL force during a jump in downhill skiing: A simulation study," *Scand J Med Sci Sports*, vol. 24, no. 3, pp. 180-187, 2013.

5 Overview of Talks: Adaptions to Training

5.1 Modelling Speed-HR Relation using PerPot

Stefan Endler (Universität Mainz, DE)

Joint work of Endler, Stefan; Perl, Jürgen
Main reference S. Endler, J. Perl, "Optimizing practice and competition in marathon running by means of the meta-model", in Proc. of 2012 pre-Olympic Congress on Sports Science and Computer Science in Sport (IACSS'12), pp. 127–131, World Academic Union, 2012.

A model, which represents the heart rate (HR) process based on a speed process has to model three apects:

1. Increasing HR after increasing speed.
2. Decreasing HR after decreasing speed.
3. Break down after exhaustion.

The performance potential metamodell (PerPot) models all these behaviors. It was adapted to the environment of endurance running. Once, the model is calibrated to the individual athlete by a graded incremental test, it can be used for simulation of e.g. competitions. Simulations can help unexperienced athletes particularly to avoid overloading and underperforming.

5.2 Performance Adaptions to Football Training: Is More Always Better?

Hugo Folgado (University of Evora, PT)

Joint work of Folgado, Hugo; Sampaio, Jaime

Traditionally, performance in sports is measured by magnitude based indicators, summed up by the Olympic moto – Citius, Altius Fortius – Faster, Higher, Stronger. However, in several sport domains, and particularly in team sports, this idea has been challenged by recent research. In football, the physical analysis of matches in different competitive leagues have showed that players in higher level contexts tend to run less and at lower intensities than players involved in lower leagues [1]. In other approach studying the effects of congested fixtures in players physical performance showed no differences in the amount of distance covered and distance covered at different displacement intensities [2]. So, it may be speculated that the amount of displacement is not related to greater levels of performance in football. Based in these approaches, we measured players physical and tactical performance development during the preseason, evaluated during sided-games. Our results showed that players tend to reduce the amount of distance covered during these situation has the preseason

progresses. However, their tactical performance, measured as the amount of time players are displacing in synchronized manner, was higher as the preseason progressed. These findings lead to a need for shifting to a more holistic approach, were performance indicators need to be understood within the different interpersonal relations established during the match.

References

1 P. S. Bradley, C. Carling, A. G. Diaz, P. Hood, C. Barnes, J. Ade, M. Boddy, P. Krustrup, and M. Mohr, "Match performance and physical capacity of players in the top three competitive standards of English professional soccer," *Hum Movement Sci*, vol. 32, no. 4, pp. 808-821, 2013.

2 A. Dellal, C. Lago-Penas, E. Rey, K. Chamari, and E. Orhant, "The effects of a congested fixtures period on physical performance, technical activity and injury rate during matches in a professional soccer team," *Br J Sports Med*, vol. 49, no. 6, 2013.

5.3 Modeling Individual HR Dynamics to the Change of Load

Katrin Hoffmann (TU Darmstadt, DE)

The success of training in sports and, in particular, in the application of Exergames, is dependent on setting an appropriate training load. Modeling the individual HR dynamics to the change of load in the sub maximal range provides an effective and efficient prediction of the individual strain in the human body. This enables systematic load control and is essential for an individually optimal training. This task is not simple. Beside the final steady state HR corresponding to the load, the slope of the curve is also essential for a reliable modeling. However, research has shown that this slope can vary in humans, depending on a great amount of influencing factors, i.e. age, body weight, sex, training and resting level and many more. Additionally, it can also vary in the same human under apparently similar conditions. Further research is needed to improve the modeling of HR dynamics inside Exergames:

1. Additional influencing factors on the HR, i.e. emotion or diseases, need to be identified.
2. Additional load on the human body caused by game control, i.e. body movements, need to be identified and controlled.
3. The formula for modeling the human HR responses need to be improvement and dynamically adapted.

5.4 Model Design and Validation for Oxygen Dynamics

Dietmar Saupe (Universität Konstanz, DE)

Joint work of Artiga Gonzalez, A.; Bertschinger, R.; Brosda, F.; Dahmen, T.; Thumm, P.; Saupe, D.
Main reference A. A. Gonzalez, eR. Bertschinger, F. Brosda, T. Dahmen, P. Thumm, D. Saupe, "Modeling Oxygen Dynamics under Variable Work Rate," in Proc. of the 3rd Int'l Congress on Sport Sciences Research and Technology Support (icSPORTS'15), pp. 198–207, ScitePress, 2015; pre-print available from author's webpage.
URL http://dx.doi.org/10.5220/0005607701980207
URL https://www.uni-konstanz.de/mmsp/pubsys/publishedFiles/ArBeBr15.pdf

Measurements of oxygen uptake and blood lactate content are central to methods for assessment of physical fitness and endurance capabilities in athletes. Two important parameters extracted from such data of incremental exercise tests are the maximal oxygen uptake and the critical power. A commonly accepted model of the dynamics of oxygen uptake during exercise at constant work rate comprises a constant baseline oxygen uptake, an exponential fast component, and another exponential slow component for heavy and severe work rates. We generalized this model to variable load protocols by differential equations that naturally correspond to the standard model for constant work rate. This provides the means for prediction of oxygen uptake response to variable load profiles including phases of recovery. The model parameters were fitted for individual subjects from a cycle ergometer test. The model predictions were validated by data collected in separate tests. Our findings indicate that oxygen kinetics for variable exercise load can be predicted using the generalized mathematical standard model, however, with an overestimation of the slow component. Such models allow for applications in the field where the constant work rate assumption generally is not valid.

6 Comments

6.1 Research Perspective

Anne Danielle Koelewijn (Cleveland State University – Cleveland, US)

The Dagstuhl seminar was a very interesting and inspiring event for me. There were many opportunities and a good environment to discuss research. I would recommend to keep talks short also in future events to encourage this even more. Also, the different disciplines that were brought together was insightful, as well as the different backgrounds of the participants. It showed in what ways human modelling could be used in other fields of research and also how this could be helpful in commercial applications. A lot of work is still to be done before this can happen, for example in personalization of models for specific sports or even specific athletes.

6.2 Industry Perspective

Malte Siegle (Sportradar AG – St. Gallen, CH)

For a company it is very important to know about the latest research activities. The Dagstuhl seminar is a great opportunity to get the latest insights and discuss with prestigious representatives from different areas. Besides the important fact to extend the network it can result in concrete research collaborations and even in funded projects. I highly recommend to open Dagstuhl even more towards the industry, as science needs to be applied in concrete projects or products. Moreover, knowing about the requirements of the industry can also help scientists and universities to improve their research programs.

7 Discussion

In the seminar, the term "model" was not exactly defined to allow for a broad discussion. During the discussions, a different understanding of "models" became apparent depending on the background of each participant. In sport science, models are used to understand and predict the behaviour of e.g. sport games, human movement or physical performance of athletes. Models are commonly physically motivated and based on specialist knowledge. However, such models reach their limits when the underlying process is complex and the real world cannot be adequately represented. In machine learning, a model refers to an algorithm describing the dependency of input and output variables. Models are commonly data-driven rather than physics-based. Their application as black boxes conceals risks: How do we know that the results are accurate? How can we optimize our results? What causes problems? How to interpret the model structure physically? As a result from the seminar, computer scientist should provide more support and expertise to allow for insights into the behaviour of the model. Contrarily, the model structure depends on the chosen input and output variables. Therefore, it is essential that sports scientists and industry provide useful information: What are meaningful performance indicators i.e., model input, related to the problem? What output variables are of interest, e.g. to give useful feedback to a coach or the athlete?

In the seminar, the term "sensemakeing" was mentioned in this context. As the amount of collected data is increasing, machine learning methods like unsupervised learning, offer new opportunities for joint collaboration. The combination of knowledge-based and data-driven models would be another advance. For example, position data of players during sport games is already available using computer vision or local positioning technologies. The position data itself might not offer enough insight to the course of the game. In terms of "sensemaking", a pose estimation of the players would lead to a better behavioral understanding of the athletes. This could be done by tracking a biomechanical model with recorded video or inertial sensor data. Moreover, physical models, like biomechanical models, could be used to synthesise training data for training neural networks to improve activity recognition based on noisy sensor data. Finally, new methodologies like agent-based modelling and simulation should be applied to sports related problems. This implies a close cooperation between computer and sports scientists.

8 Conclusion

The seminar enabled fruitful interdisciplinary discussions concerning the core problems of modeling and simulation starting with the acquisition and preprocessing of data, the selection of the appropriate model(s) and ending with the verification and validation of models. The seminar also uncovered the different perspectives of science, practice and industry on modeling and simulation as well as the necessity of all parties to communicate about their views and mutual expectations. Furthermore, the discussions revealed the ambivalence of applying ICT to modeling and simulations in sports. On the one hand, added values like accuracy, speed, and complexity as well as convenience were emphasized. On the other hand, numerous issues including error identification and correction in the data, data quality in general, classification problems, and knowledge discovery in "big data" were addressed. Due to the "spirit of Dagstuhl" the schedule was finalized and flexibly adapted during the seminar. Some guidelines were suggested to the presenters to establish overarching aspects for discussion, e.g., how models were selected and applied to the problem at hand and which advantages and disadvantages appeared in the process of modeling.

There was a broad agreement that the series of Dagstuhl seminars on computer science in sport should be continued. The positive results of the seminar evaluation confirmed the high quality of the seminar. However, some things need to be improved concerning the structure of the seminar as well as the commitment of the participants, e.g., talks more structured and focused on fundamental issues rather than specific aspects, fostering more discussions by shortening the talks as well as a better preparation of the seminar by collecting main topics in advance (e.g., three basic issues per participant). The organizers are sure that the next Dagstuhl seminar will be successful in improving the quality beyond the high level already established by this seminar.

Participants

- Arnold Baca
Universität Wien, AT
- Eva Dorschky
Univ. Erlangen – Nürnberg, DE
- Ricardo Duarte
University of Lisbon, PT
- Stefan Endler
Universität Mainz, DE
- Björn Eskofier
Univ. Erlangen-Nürnberg, DE
- Irfan A. Essa
Georgia Institute of Technology – Atlanta, US
- Hugo Folgado
University of Evora, PT
- Katrin Hoffmann
TU Darmstadt, DE
- Anne Danielle Koelewijn
Cleveland State University – Cleveland, US
- John Komar
Prozone Sports Ltd. – Leeds & University of Rouen
- Martin Lames
TU München, DE
- Roland Leser
Universität Wien, AT
- Daniel Link
TU München, DE
- Jim Little
University of British Columbia – Vancouver, CA
- Stuart Morgan
Australian Institute of Sport – Bruce, AU
- Bernhard Moser
Software Competence Center – Hagenberg, AT
- Jürgen Perl
Universität Mainz, DE
- Robert Rein
Deutsche Sporthochschule Köln, DE
- Karen Roemer
Central Washington University – Ellensburg, US
- Martin Rumpf
Universität Bonn, DE
- Tiago Guedes Russomanno
University of Brasilia, BR
- Dietmar Saupe
Universität Konstanz, DE
- Heiko Schlarb
adidas AG – Herzogenaurach, DE
- Malte Siegle
Sportradar AG – St. Gallen, CH
- Michael Stöckl
Universität Wien, AT
- Antonie van den Bogert
Cleveland State University – Cleveland, US
- Anna Volossovitch
University of Lisbon, PT
- Hendrik Weber
DFL GmbH - Frankfurt, DE
- Josef Wiemeyer
TU Darmstadt, DE

Report from Dagstuhl Seminar 15391

Algorithms and Complexity for Continuous Problems

Edited by

Aicke Hinrichs[1], Joseph F. Traub[*2], Henryk Woźniakowski[3], and Larisa Yaroslavtseva[4]

1 **Universität Linz, AT,** aicke.hinrichs@jku.at
2 **Columbia University – New York, US**
3 **Columbia University – New York, US**
4 **Universität Passau, DE,** larisa.yaroslavtseva@uni-passau.de

Abstract

From 20.09.15 to 25.09.15, the Dagstuhl Seminar 15391 Algorithms and Complexity for Continuous Problems was held in the International Conference and Research Center (IBFI), Schloss Dagstuhl. During the seminar, participants presented their current research, and ongoing work and open problems were discussed. Abstracts or the presentations given during the seminar can be found in this report. The first section describes the seminar topics and goals in general. Links to extended abstracts or full papers are provided, if available.

Seminar September 20–25, 2015 – http://www.dagstuhl.de/15391
1998 ACM Subject Classification E.1 Data Structures, F.2 Analysis of Algorithms and Problem Complexity
Keywords and phrases High Dimensional Problems, Tractability, Random coefficients, Multilevel algorithms, computational stochastic processes, Compressed sensing, Learning theory
Digital Object Identifier 10.4230/DagRep.5.9.57
Edited in cooperation with Daniel Rudolf

1 Executive Summary

Aicke Hinrichs
Henryk Woźniakowski
Larisa Yaroslavtseva

This was already the 12th Dagstuhl Seminar on Algorithms and Complexity for Continuous Problems over a period of 24 years. It brought together researchers from different communities working on computational aspects of continuous problems, including computer scientists, numerical analysts, applied and pure mathematicians. Although the seminar title has remained the same, many of the topics and participants change with each seminar and each seminar in this series is of a very interdisciplinary nature.

Continuous computational problems arise in diverse areas of science and engineering. Examples include path and multivariate integration, approximation, optimization, as well as operator equations. Typically, only partial and/or noisy information is available, and the aim is to solve the problem within a given error tolerance using the minimal amount

[*] Joseph F. Traub (June 24, 1932 – August 24, 2015): http://www.cs.columbia.edu/~traub/.

of computational resources. For example, in high-dimensional integration one wants to compute an ϵ-approximation to the integral with the minimal number of function evaluations. Here it is crucial to identify first the relevant variables of the function. Understanding the complexity of such problems and construction of efficient algorithms is both important and challenging. The current seminar attracted 35 participants from nine different countries all over the world. About 30 % of them were young researchers including PhD students. There were 25 presentations covering in particular the following topics:

- High-dimensional problems
- Tractability
- Computational stochastic processes
- Compressive sensing
- Random media
- Computational finance
- Noisy data
- Learning theory
- Biomedical learning problems
- Markov chains

There were three introductory talks to recent developments in PDE with random coefficients, learning theory and compressive sensing. A joint session with the Dagstuhl Seminar 15392 "Measuring the Complexity of Computational Content: Weihrauch Reducibility and Reverse Analysis" stimulated the transfer of ideas between the two different groups present in Dagstuhl.

The work of the attendants was supported by a variety of funding agencies. This includes the Deutsche Forschungsgemeinschaft, the Austrian Science Fund, the National Science Foundation (USA), and the Australian Research Council.

As always, the excellent working conditions and friendly atmosphere provided by the Dagstuhl team have led to a rich exchange of ideas as well as a number of new collaborations. Selected papers related to this seminar will be published in a special issue of the Journal of Complexity.

2 Table of Contents

3 Overview of Talks

3.1 Maximum Improvement Algorithm for Global Optimization of Brownian Motion

James M. Calvin (NJIT – Newark, US)

Two common approaches to optimizing an unkown random function are to choose the next point to maximize the conditional probability that the function value is less than some amount below the current record minimum, and to choose the next point to maximize the expected decrease below the current record minimum. We construct algorithms based on each approach, and describe error bounds.

3.2 On lattice rules, approximation and Lebesgue constants

Ronald Cools (KU Leuven, BE)

Joint work of Cools, Ronald; Nuyens, Dirk; Suryanarayana, Gowri

In this talk I start with introducing lattice rules for numerical integration with the trigonometric degree as quality criterion. I focus on Fibonacci lattice rules and lattice rules with minimal number of points for the trigonometric degree. Then I consider the points of these lattice rules for approximation and introduce the trigonometric approximation degree. This approximation degree is calculated for the lattices used throughout this talk.

To investigate the quality of point sets for approximation the Lebesgue constant is often used. The Lebesgue constant for trigonometric approximation for 1- and 2-dimensional lattices is investigated. We reveal some nice structures and make the link between the Dirichlet kernel and the reproducing kernel that was used to obtain minimal lattice rules in two dimensions.

3.3 Weak convergence for semi-linear SPDEs

Sonja Cox (University of Amsterdam, NL)

Joint work of Cox, Sonja; Jentzen, Arnulf; Kuniawan, Ryan
Main reference A. Jentzen, R. Kurniawan, "Weak convergence rates for Euler-type approximations of semilinear stochastic evolution equations with nonlinear diffusion coefficients," arXiv:1501.03539v1 [math.PR], 2015.
URL http://arxiv.org/abs/1501.03539v1

In recent work by Jentzen and Kurniawan weak convergence of both spatial and temporal discretizations for semi-linear SPDEs was proven. Their approach required the non-linear terms in the SPDE to be four times Fréchet differentiable as operators on a Hilbert space. In particular, their results can not be applied to non-linear terms arising from Nemytskii operators. In my talk I will explain how this problem can be overcome by working the more general Banach space setting.

3.4 General multilevel adaptations for stochastic approximation algorithms

Steffen Dereich (Universität Münster, DE)

Joint work of Dereich, Steffen; Müller-Gronbach, Thomas
Main reference S. Dereich, T. Müller-Gronbach, "General multilevel adaptations for stochastic approximation algorithms," arXiv:1506.05482v1 [math.PR], 2015.
URL http://arxiv.org/abs/1506.05482v1

We analyse multilevel adaptations of stochastic approximation algorithms. In contrast to the classical multilevel Monte Carlo algorithm of Mike Giles one now deals with a parameterised family of expectations and the aim is to compute parameters for which the expectation is zero. We propose a new algorithm and provide an upper bound for its error. Under similar assumptions as in [2] we recover the same order of convergence in the computation of zeroes as the ones originally derived in the computation of single expectations.

References

1 S. Dereich and T. Müller-Gronbach. *General multilevel adaptations for stochastic approximation algorithms*, arXiv:1506.05482.
2 M. B. Giles. *Multi-level Monte Carlo path simulation.* Operations Research, 56(3):607–617, 2008.

3.5 On exit times of diffusions from a domain

Stefan Geiss (University of Jyväskylä, FI)

Joint work of Bouchard, Bruno; Geiss, Stefan; Gobet, Emmanuel
Main reference B. Bouchard, S. Geiss, E. Gobet, "First time to exit of a continuous Itô process: general moment estimates and $\mathbf{L}_1$-convergence rate for discrete time approximations," arXiv:1307.4247v2 [math.PR], 2014.
URL http://arxiv.org/abs/1307.4247v2

We establish general moment estimates for the discrete and continuous exit times of a general Itô process in terms of the distance to the boundary. These estimates serve as intermediate steps to obtain strong convergence results for the approximation of a continuous exit time by a discrete counterpart, computed on a grid. In particular, we prove that the discrete exit time of the Euler scheme of a diffusion converges in the $\mathbf{L}_1$ norm with an order $1/2$ with respect to the mesh size. This rate is optimal. The talk is based on [1].

References

1 B. Bouchard, S. Geiss, and E. Gobet: *First time to exit of a continuous Itô process: general moment estimates and $\mathbf{L}_1$-convergence rate for discrete time approximations*, In revision for *Bernoulli*.
2 B. Bouchard and S. Menozzi. *Strong approximations of BSDEs in a domain. Bernoulli*, 15(4):1117–1147, 2009.
3 D. J. Higham, X. Mao, M. Roj, Q. Song, and G. Yin. *Mean exit times and the multilevel Monte Carlo method. SIAM/ASA J. Uncertain. Quantif.* 1(1):2–18, 2013.

3.6 Universality of Weighted Anchored and ANOVA Spaces

Michael Gnewuch (Universität Kiel, DE)

Joint work of Gnewuch, Michael; Hefter, Mario; Hinrichs, Aicke; Ritter, Klaus

We present upper and lower error bounds for high- and infinite-dimensional integration. We study spaces of integrands with weighted norms and consider deterministic and randomized algorithms. Interesting examples of norms are norms induced by an anchored function space decomposition or the ANOVA decomposition.

In some settings (depending on the class of integrands we consider, the weighted norm, the class of algorithms we admit and the way we account for the computational cost) one can derive good or even optimal error bounds directly. If one changes the weighted norm, a correspondent direct error analysis can be much more involved and complicated. The focus of the talk is to discuss new results on function space embeddings of weighted spaces which allow for an easy transfer of error bounds.

3.7 Optimal Strong Approximation of the One-dimensional Squared Bessel Process

Mario Hefter (TU Kaiserslautern, DE)

Joint work of Hefter, Mario; Calvin, James M.; Herzwurm, André

We consider the one-dimensional squared Bessel processes given by the stochastic differential equation (SDE)

$$dX_t = 1\,dt + 2\sqrt{X_t}\,dW_t, \quad X_0 = x_0, \quad t \in [0,1], \tag{1}$$

and study strong (pathwise) approximation of the solution X at the final time point $t = 1$. This SDE is a particular instance of a Cox-Ingersoll-Ross (CIR) process where the boundary point zero is accessible. We consider numerical methods that have access to values of the driving Brownian motion W at a finite number of time points. We show that the polynomial convergence rate of the n-th minimal errors for the class of adaptive algorithms as well as for the class of algorithms that rely on equidistant grids are equal to infinity and $1/2$, respectively. As a consequence, we obtain that the parameters appearing in the CIR process affect the convergence rate of strong approximation.

A key step in the proofs consists of identifying the pathwise solution of (1) and link this problem to global optimization under the Wiener measure.

3.8 Complexity of parametric SDEs

Stefan Heinrich (TU Kaiserslautern, DE)

We consider the problem of strong solution of scalar stochastic differential equations depending on a parameter. We seek to find numerical approximations for all parameter values simultaneously.

The problem is approached within a general scheme of solving parameter-dependent numerical problems by multilevel methods, developed previously by T. Daun and the author in a series of papers. First we obtain suitable convergence results for the Banach space valued Euler-Maruyama scheme in spaces of martingale type 2. Then we develop a multilevel scheme involving two embedded Banach spaces, where discretization is balanced with approximation of the embedding. Finally, the parametric problem is cast into this embedded Banach space setup, from which a multilevel method for the strong solution of parametric stochastic differential equations results.

We obtain convergence rates for various smoothness classes of input functions. Furthermore, the optimality of these rates is established by proving matching lower bounds. Thus, the complexity of this problem is established in the sense of information-based complexity theory.

3.9 Quasi-Monte Carlo conquers the Rendering Industry

Alexander Keller (NVIDIA GmbH – Berlin, DE)

Quasi-Monte Carlo methods for image synthesis have been under investigation for over 20 years. Although the deterministic approach has been shown to be superior to corresponding Monte Carlo methods, adoption had been rare for a long time. However, coincident with the rendering industry changing to path tracing algorithms for light transport simulation, recently there is a huge interest and growing adoption of quasi-Monte Carlo methods.

We point out how Dagstuhl seminars brought about this change that even influenced standard textbooks, review the state of the art in the rendering industry, and discuss current algorithmic and mathematical questions in light transport simulation.

3.10 Efficient truncation for integration in weighted anchored and ANOVA spaces

Peter Kritzer (Universität Linz, AT)

Joint work of Kritzer, Peter; Pillichshammer, Friedrich, Wasilkowski, Greg W.
Main reference P. Kritzer, F. Pillichshammer, G. W. Wasilkowski, "Very low truncation dimension for high dimensional integration under modest error demand," arXiv:1506.02458v2 [math.NA], 2015.
URL http://arxiv.org/abs/1506.02458v2

We consider the problem of numerical integration for weighted anchored and ANOVA Sobolev spaces of s-variate functions, where s is large. Under the assumption of sufficiently fast decaying weights, we show in a constructive way that such integrals can be approximated by

quadratures for functions f_k with only k variables, where $k = k(\varepsilon)$ depends solely on the error demand ε. Moreover $k(\varepsilon)$ does not depend on the function being integrated, i.e., is the same for all functions from the unit ball of the space.

3.11 Approximation in multivariate periodic Gevrey spaces

Thomas Kühn (Universität Leipzig, DE)

Joint work of Kühn, Thomas; Petersen, Martin

The classical Gevrey classes, already introduced in 1918, play an important role in analysis, especially in the context of PDEs. They consist of C^∞-functions on $\mathbb{R}^d$ whose derivatives satisfy certain growth conditions. All Gevrey classes contain non-analytic functions. For periodic functions f , these growth conditions on the derivatives can be expressed equivalently by decay conditions on the Fourier coefficients of f. Using this approach, we define periodic Gevrey spaces $G^{s,c}(\mathbb{T}^d)$ on the d-dimensional torus $\mathbb{T}^d$, where $s \in (0,1)$ is a smoothness parameter and $c > 0$ a fine parameter.

There is a rich literature on approximation of functions of *finite smoothness*, as well as for classes of *analytic functions*, but only quite few results are available for C^∞-functions. The talk is devoted to this "intermediate" case, more precisely to estimates for approximation numbers a_n of the embeddings $G^{s,c}(\mathbb{T}^d) \hookrightarrow L_2(\mathbb{T}^d)$. In particular, we determine the exact asymptotic rate of a_n as $n \to \infty$. Not surprisingly, this rate is sub-exponential and faster than polynomial. Moreover, we give two-sided preasymptotic estimates, i.e. for small n, with special emphasis on the dependence of the hidden constants on the dimension d. These results allow an interpretation in the language of IBC, concerning different notions of tractability.

3.12 Minimax signal detection in statistical inverse problems

Peter Mathè (Weierstraß Institut – Berlin, DE)

Joint work of Mathé, Peter; Clèment Marteau
Main reference C. Marteau, P. Mathé, "General regularization schemes for signal detection in inverse problems," Mathematical Methods of Statistics, 23(3):176–200, 2014.
URL http://dx.doi.org/10.3103/S1066530714030028

We shall consider inverse problems in Hilbert space under Gaussian white noise. Usually, the problem of reconstructing the unknown signal, say f, from the noisy observation $Y = Tf + \sigma\xi$ is considered. Instead, we are interested in the nonparametric test problem, and we ask $f = f_0$ for some given function. We shall exhibit how optimality for such test problem can be defined. Lower bounds have been established, previously. We emphasize that many of the common regularization schemes, both with and/or without discretization can be used to yield order optimal tests. This is joint work with Clèment Marteau, Univ. Toulouse, [1].

References

1 C. Marteau, and P. Mathé, *General regularization schemes for signal detection in inverse problems*, Mathematical Methods of Statistics, 23 (2014) pp. 176–200.

3.13 On tough quadrature problems for SDEs with bounded smooth coefficients

Thomas Müller-Gronbach (Universität Passau, DE)

Joint work of Müller-Gronbach, Thomas; Yaroslavtseva, Larisa

We study the problem of approximating the expected value $E(f(X(1)))$ of a function f of the solution $X(1)$ of a SDE at time 1 based on a finite number of evaluations of f and the coefficients of the SDE. We present classes of SDEs with bounded smooth coefficients such that this problem can not be solved with a polynomial error rate in the worst case sense.

3.14 Optimal approximation of SDEs driven by fractional Brownian motion – An overview

Andreas Neuenkirch (Universität Mannheim, DE)

In this talk I give an overview on recent results concerning the optimal approximation of stochastic differential equations (SDEs) driven by fractional Brownian motion (fBm) with Hurst parameter $H > 1/4$. More precisely, I will consider the approximation of the solution at a fixed time point with respect to the root mean square error given an equidistant discretisation of the driving fBm.

While the scalar case has been analysed in detail [1] for $H > 1/2$ in 2008, in recent years several error bounds have been established in the multi-dimensional case. The picture is now as follows: Up to sub-polynomial terms the optimal convergence order is at least $\min\{2H - 1/2, 1\}$, due to results of Bayer et al. [2] and Hu et al. [3]. In the case of the fractional Lévy area, which corresponds to a particular two-dimensional SDE, the optimal convergence order is $2H - 1/2$ for $H > 1/2$, see [4].

I strongly suppose that as long the diffusion coefficients do not commute, the optimal convergence order is $2H - 1/2$.

References

1 A. Neuenkirch (2008). *Optimal pointwise approximation of stochastic differential equations driven by fractional Brownian motion.* Stochastic Processes and their Applications 118 (12), 2294–2333

2 C. Bayer, P. K. Friz, S. Riedel, J. Schoenmakers (2013+). *From rough path estimates to multilevel Monte Carlo.* Working Paper

3 Y. Hu, Y. Lui, D. Nualart (2015+). *Rate of convergence and asymptotic error distribution of Euler approximation schemes for fractional diffusions.* Annals of Applied Probability. To appear

4 A. Neuenkirch, T. Shalaiko (2015+). *The maximum rate of convergence for the approximation of the fractional Lévy area at a single point.* Journal of Complexity. To appear

3.15 Multivariate integration over the Euclidean space for analytic functions and r-smooth functions

Dong Nguyen (KU Leuven, BE)

Joint work of Nuyens, Dirk

In this talk we study multivariate integration over $\mathbb{R}^s$ for weighted analytic functions, whose Fourier transform decays exponentially fast. We prove that the exponential convergence rate can be achieved by using a classical quasi-Monte Carlo method. More specific, we prove two convergence rates of $\mathcal{O}(\exp(-N^{\frac{1}{D(s)+B(s)}}))$ and $\mathcal{O}(\exp(-N^{\frac{1}{B(s)}}(\ln N)^{-\frac{D(s)}{B(s)}}))$, where $D(s)$ and $B(s)$ are respectively defined by the exponential decay of the Fourier transform and of the integrand, for two different function classes. We discuss work in progress to obtain a stronger convergence rate with less dependence on the dimension. Some numerical results demonstrate the theory.

3.16 A Universal Algorithm for Multivariate Integration

Erich Novak (Universität Jena, DE)

Main reference D. Krieg, E. Novak, "A Universal Algorithm for Multivariate Integration," arXiv:1507.06853v1 [math.NA], 2015.
URL http://arxiv.org/abs/1507.06853v1

We present an algorithm for multivariate integration over cubes that is unbiased and has optimal order of convergence (in the randomized sense as well as in the worst case setting) for all Sobolev spaces $H^{r,\mathrm{mix}}([0,1]^d)$ and $H^s([0,1]^d)$ for $s > d/2$.

3.17 Approximation with lattice points

Dirk Nuyens (KU Leuven, BE)

Joint work of Nuyens, Dirk; Gowri, Suryanarayana; Ronald, Cools; Frances Y., Kuo

We analyse the asymptotic worst case error of using tent transformed lattice points for approximation of functions in the half period cosine space. This space is the unanchored Sobolev space of smoothness one for a certain choice of parameters. This is a continuation of [1].

References

1 G. Suryanarayana, D. Nuyens, and R. Cools. *Reconstruction and collocation of a class of non-periodic functions by sampling along tent-transformed rank-1 lattices.* Journal of Fourier Analysis and Applications, pp. 1–28, 2015.

3.18 Tensor product approximation of analytic functions

Jens Oettershagen (Universität Bonn, DE)

Joint work of Oettershagen, Jens; Griebel, Michael
Main reference M. Griebel, J. Oettershagen, "On tensor product approximation of analytic functions," INS Preprint, No. 1512, 2015.
URL http://wissrech.ins.uni-bonn.de/research/pub/oettershagen/INSPreprint1512.pdf

We prove sharp, two-sided bounds on sums of the form $\sum_{\mathbf{k}\in\mathbb{N}_0^d\setminus\mathcal{D}_{\mathbf{a}}(T)} \exp(-\sum_{j=1}^d a_j k_j)$, where $\mathcal{D}_{\mathbf{a}}(T) := \{\mathbf{k}\in\mathbb{N}_0^d : \sum_{j=1}^d a_j k_j \le T\}$ and $\mathbf{a}\in\mathbb{R}_+^d$. These sums appear in the error analysis of tensor product approximation, interpolation and integration of d-variate analytic functions. Examples are tensor products of univariate Fourier-Legendre expansions or interpolation and integration rules at Leja points . Moreover, we discuss the limit $d\to\infty$, where we prove both, algebraic and sub-exponential upper bounds. As an application we consider tensor products of Hardy spaces, where we study convergence rates of a certain truncated Taylor series, as well as of interpolation and integration using Leja points.

3.19 A linear functional strategy for regularized ranking

Sergei Pereverzyev (RICAM – Linz, AT)

Main reference G. Kriukova, O. Panasiuk, S. V. Pereverzyev, P. Tkachenko, "A Linear Functional Strategy for Regularized Ranking," RICAM Report 2015-13, 2015.
URL http://www.ricam.oeaw.ac.at/publications/reports/15/rep15-13.pdf

Regularization schemes are frequently used for performing ranking tasks. This topic has been intensively studied in recent years. However, to be effective a regularization scheme should be equipped with a suitable strategy for choosing a regularization parameter. In the present study we discuss an approach, which is based on the idea of a linear combination of regularized rankers corresponding to different values of the regularization parameter. The coefficients of the linear combination are estimated by means of the so-called linear functional strategy. We provide a theoretical justification of the proposed approach and illustrate them by numerical experiments. Some of them are related with ranking the risk of nocturnal hypoglycemia of diabetes patients.

3.20 Linear versus nonlinear approximation in the average case setting

Leszek Plaskota (University of Warsaw, PL)

We compare the average errors of linear and nonlinear approximations assuming that the coefficients in an orthogonal expansion are scaled i.i.d. random variables. We show that generally the n-term nonlinear approximation can be much better than linear approximation. On the other hand, if the scaling parameters decrease no faster than polynomially then the average error of nonlinear approximations does not converge to zero faster than that of linear approximations, as n goes to infinity.

References

1 A. Cohen and J.-P. D'Ales, *Nonlinear approximation of random functions*. SIAM J. Appl. Math. 57 (1997) pp. 518–540.
2 J. Creutzig, T. Müller-Gronbach, K. Ritter, *Freer-knot spline approximation of stochastic processes*. J. Complexity 23 (1997) pp. 867–889.
3 R. A. DeVore, *Nonlinear approximation*. Acta Numerica 8 (1998) pp. 51–150.
4 R. A. DeVore and B. Jawerth, *Optimal nonlinear approximation*, Manuscripta Math. 63 (1992) pp. 469–478.
5 M. A. Kon and L. Plaskota, *Information-based nonlinear approximation: an average case setting*. J. Complexity 21 (2005), pp. 211–229.
6 J. Vybiral, *Average best m-term approximation*, Constr. Approx. 36 (2012), pp. 83–115.

3.21 Optimal adaptive solution of piecewise smooth systems of IVPs with unknown switching hypersurface

Pawel Przybylowicz (AGH Univ. of Science & Technology-Krakow, PL)

Joint work of Kacewicz, Boleslaw; Przybylowicz, Pawel
Main reference B. Kacewicz, Boleslaw, P. Przybylowicz, "Complexity of the derivative-free solution of systems of IVPs with unknown singularity hypersurface," Journal of Complexity, 31(1):75–91, 2015.
URL http://dx.doi.org/10.1016/j.jco.2014.07.002

We present results concerning optimal approximation of solutions of piecewise regular systems of IVPs. We assume that a right-hand side function is smooth everywhere except for an unknown smooth hypersurface, defined by zeros of an 'event' function h. We do not assume the knowledge of h, even in the weak sense of computing certain discrete information on h. We restrict ourselves to information defined only by values of the right-hand side function (computation of partial derivatives is not allowed).We show how to construct optimal algorithm that is rigorous (it is not based on heuristic arguments), it does not use information on the event function, and preserves the optimal error known for regular systems. The complexity of piecewise regular problems is consequently asymptotically the same as that for globally regular problems.

3.22 Compressive sensing and function reconstruction in high dimensions

Holger Rauhut (RWTH Aachen, DE)

Main reference S. Foucart, H. Rauhut, "A Mathematical Introduction to Compressive Sensing," ISBN 978-0-8176-4947-0, Applied and Numerical Harmonic Analysis, Birkhäuser/Springer, 2013.
URL http://www.springer.com/de/book/9780817649470

Compressive sensing is a recent field originating from mathematical signal processing which predicts that sparse or compressible vectors can be reconstructed from a few linear and non-adaptive measurements via efficient algorithms such as l1-minimization. It is a remarkable fact that uptodate all provably optimal measurement matrices are based on randomness. An important special case is the reconstruction of sparse signals from randomly selected Fourier

coefficients. Extensions of this principle can be applied to the reconstruction of functions of many variables. Under standard smoothness assumptions this problem faces the curse of dimensionality. Introducing some non-standard smoothness spaces allowing for efficient sparse approximations, one may avoid the curse of dimension by using compressive sensing techniques for the reconstruction. This principle has applications for the numerical solution of high-dimensional parametric operator equations. The talk gives an overview on these topics.

3.23 Perturbation theory of Markov chains

Daniel Rudolf (Universität Jena, DE)

Joint work of Rudolf, Daniel; Schweizer, Nikolaus
Main reference D. Rudolf, N. Schweizer, "Perturbation theory for Markov chains via Wasserstein distance," arXiv:1503.04123v2 [stat.CO], 2015.
URL http://arxiv.org/abs/1503.04123v2

Perturbation theory for Markov chains addresses the question how small differences in the transitions of Markov chains are reflected in differences between their distributions. We show bounds on the distance of the nth step distributions of two Markov chains when one of them satisfies a Wasserstein ergodicity condition. Our work is motivated by the recent interest in approximate Markov chain Monte Carlo (MCMC) methods in the analysis of big data sets. We illustrate our theory by showing quantitative estimates for an autoregressive model and an approximate version of the Metropolis-Hastings algorithm.

3.24 Generalized solution operators and topology

Pawel Siedlecki (University of Warsaw, PL)

It is known that a solution operator $S : F \times [0, \infty) \to \mathcal{P}(G)$ induces a certain type of a topological structure on a set G, i.e., a family of pseudometrics such that the sets of ε-approximations of solutions (i.e., $S(f, \varepsilon)$) are, almost, closed balls in these pseudometrics. We generalize this result to the case of solution operators $S : F \times P \to \mathcal{P}(G)$, where P is a partially ordered set with some additional structure. We investigate what types of metric-like and topological structures are induced on a set G in such a case, and how $S(f, \varepsilon)$ may be interpreted.

3.25 PDE with random coefficients – a survey

Ian H. Sloan (University of New South Wales – Sydney, AU)

This invited survey described recent algorithmic developments in partial differential equations with random coefficients treated as a high-dimensional problem. The prototype of such problems is the underground flow of water or oil through a porous medium, with the permeability of the material treated as a random field. (The stochastic dimension of the problem is high if the random field needs a large number of random variables for its effective description.). The talk introduced the problem, then explained different approaches to the problem, ranging from the polynomial chaos method initiated by Norbert Wiener to the Monte Carlo and Quasi-Monte Carlo methods. In recent years there have been significant progress in the development and analysis of algorithms in these areas. The talk aimed to encourage further interest and activity, especially from younger researchers.

3.26 Multi-Level Monte Carlo for Parametric Integration of a Discontinuous Function

Jeremy Staum (Northwestern University – Evanston, US)

Joint work of Rosenbaum, Imry; Staum, Jeremy

We consider parametric integration of a discontinuous function, focusing on the stochastic setting of random fields. We explore sets of assumptions under which the Multi-Level Monte Carlo method can be shown to improve computational complexity of parametric integration.

3.27 Analysis of Kernel-Based Learning Methods

Ingo Steinwart (Universität Stuttgart, DE)

The last decade has witnessed an explosion of data collected from various sources. Since in many cases these sources do not obey the assumptions of classical statistical approaches, new automated methods for interpreting such data have been developed in the machine learning community. Statistical learning theory tries to understand the statistical principles and mechanisms these methods are based on.

This talk begins by introducing some central questions considered in statistical learning. Then various theoretical aspects of a popular class of learning algorithms, which include support vector machines, are discussed. In particular, I will describe how classical concepts from approximation theory such as interpolation spaces and entropy numbers are used in the analysis of these methods. The last part of the talk considers more practical aspects including the choice of the involved loss function and some implementation strategies. In addition, I will present a data splitting strategy that enjoys the same theoretical guarantees as the standard approach but reduces the training time significantly.

References

1 Caponnetto, A. and De Vito, E. (2007). *Optimal rates for regularized least squares algorithm. Found. Comput. Math.*, 7:331–368.
2 Eberts, M. and Steinwart, I. (2013). *Optimal regression rates for SVMs using Gaussian kernels. Electron. J. Stat.*, 7:1–42.
3 Eberts, M. and Steinwart, I. (2014). *Optimal learning rates for localized SVMs.* Technical Report 2014-002, Fakultät für Mathematik und Physik, Universität Stuttgart.
4 Mammen, E. and Tsybakov, A. (1999). *Smooth discrimination analysis. Ann. Statist.*, 27:1808–1829.
5 Mendelson, S. and Neeman, J. (2010). *Regularization in kernel learning. Ann. Statist.*, 38:526–565.
6 Platt, J. (1999). *Fast training of support vector machines using sequential minimal optimization.* In *Advances in Kernel Methods–Support Vector Learning*, pages 185–208. MIT Press, Cambridge, MA.
7 Rahimi, A. and Recht, B. (2008). *Random features for large-scale kernel machines.* In Platt, J., Koller, D., Singer, Y., and Roweis, S., editors, *Advances in Neural Information Processing Systems 20*, pages 1177–1184.
8 Smale, S. and Zhou, D.-X. (2003). *Estimating the approximation error in learning theory. Anal. Appl.*, 1:17–41.
9 Smale, S. and Zhou, D.-X. (2007). *Learning theory estimates via integral operators and their approximations. Constr. Approx.*, 26:153–172.
10 Steinwart, I. (2009). *Oracle inequalities for SVMs that are based on random entropy numbers. J. Complexity*, 25:437–454.
11 Steinwart, I., Hush, D., and Scovel, C. (2009). *Optimal rates for regularized least squares regression.* In Dasgupta, S. and Klivans, A., editors, *Proceedings of the 22nd Annual Conference on Learning Theory*, pages 79–93.
12 Steinwart, I., Hush, D., and Scovel, C. (2011). *Training SVMs without offset. J. Mach. Learn. Res.*, 12:141–202.
13 Steinwart, I. and Scovel, C. (2007). *Fast rates for support vector machines using Gaussian kernels. Ann. Statist.*, 35:575–607.
14 Steinwart, I. and Scovel, C. (2012). *Mercer's theorem on general domains: on the interaction between measures, kernels, and RKHSs. Constr. Approx.*, 35:363–417.
15 Urner, R., Wulff, S., and Ben-David, S. (2013). *PLAL: cluster-based active learning.* In Shalev-Shwartz, S. and Steinwart, I., editors, *COLT 2013 – The 26th Annual Conference on Learning Theory*, pages 376–397.
16 Williams, C. K. I. and Seeger, M. (2001). *Using the Nyström method to speed up kernel machines.* In Leen, T., Dietterich, T., and Tresp, V., editors, *Advances in Neural Information Processing Systems 13*, pages 682–688. MIT Press.
17 Yao, Y., Rosasco, L., and Caponnetto, A. (2007). *On early stopping in gradient descent learning. Constr. Approx.*, 26:289–315.

3.28 On numerical integration of functions with mixed smoothness

Mario Ullrich (Universität Linz, AT)

Joint work of Ullrich, Mario; Ullrich, Tino
Main reference M. Ullrich, T. Ullrich, "The role of Frolov's cubature formula for functions with bounded mixed derivative," arXiv:1503.08846v1 [math.NA], 2015.
URL http://arxiv.org/abs/1503.08846v1

We prove upper bounds on the order of convergence of Frolov's cubature formula for numerical integration in function spaces of dominating mixed smoothness on the unit cube with homogeneous boundary condition. More precisely, we study worst-case integration errors for Besov $\mathbf{B}^s_{p,\theta}$ and Triebel-Lizorkin spaces $\mathbf{F}^s_{p,\theta}$ and our results treat the whole range of admissible parameters ($s \geq 1/p$). In particular, we treat the case of small smoothness which is given for Triebel-Lizorkin spaces $\mathbf{F}^s_{p,\theta}$ in case $1 < \theta < p < \infty$ with $1/p < s \leq 1/\theta$. The presented upper bounds on the worst-case error show a completely different behavior compared to "large" smoothness $s > 1/\theta$. In the latter case the presented upper bounds are optimal, i.e., they can not be improved by any other cubature formula. The optimality for "small" smoothness is open. Moreover, we present a modification of the algorithm which leads to the same bounds also for the larger spaces of periodic functions, and we discuss a randomized version of the algorithm. All results come with supporting numerical results.

3.29 Preasymptotic error bounds for multivariate approximation problems

Tino Ullrich (Universität Bonn, DE)

Joint work of Ullrich, Tino; Kühn, Thomas; Mayer, Sebastian
Main reference T. Kühn, S. Mayer, T. Ullrich, "Counting via entropy: new preasymptotics for the approximation numbers of Sobolev embeddings," arXiv:1505.00631v1 [math.NA], 2015.
URL http://arxiv.org/abs/1505.00631v1

We study the classical problem of finding the rate of convergence of the approximation numbers of isotropic and dominating mixed multivariate periodic Sobolev embeddings. Our particular focus is on so-called preasymptotic estimates, i.e., error estimates for rather small n. By pointing out an interesting relation to entropy numbers in finite dimensional spaces, we can precisely determine the preasymptotic rate of convergence for a family of isotropic norms defined through an additional "compressibility" parameter p which enters the (sharp) preasymptotic error estimate as well as the asymptotic constant which is also determined exactly.

3.30 (s,t)-Weak tractability

Markus Weimar (Universität Marburg, DE)

Joint work of Siedlecki, Pawel; Weimar, Markus
Main reference P. Siedlecki, M. Weimarm "Notes on (s,t)-weak tractability: A refined classification of problems with (sub)exponential information complexity," Journal of Approximation Theory, Vol. 200, pp. 227–258, 2015.
URL http://dx.doi.org/10.1016/j.jat.2015.07.007

In the last 20 years a whole hierarchy of notions of tractability was proposed and analyzed by several authors. These notions are used to describe the computational hardness of continuous numerical problems in terms of the behavior of their information complexity $n(\epsilon, d)$ as a function of the accuracy ϵ and the dimension d; see [3]. In this talk we present the new notion of (s,t)-*weak tractability* defined by

$$\lim_{\epsilon^{-1}+d\to\infty} \frac{\ln n(\epsilon,d)}{\epsilon^{-s}+d^{\,t}} = 0 \quad \text{for fixed} \quad s,t \geq 0$$

which allows a refined classification of problems with (sub-/super-)exponentially growing information complexity. For compact linear Hilbert space problems $S = (S_d \colon H_d \to G_d)_{d\in\mathbb{N}}$ we provide characterizations of (s,t)-weak tractability in terms of the asymptotic decay of the sequence of singular values $(\lambda_{d,j})_{j\in\mathbb{N}}$ of S_d. In addition, the advantages of our new notion is illustrated by the example of embedding problems of periodic Sobolev spaces with hybrid smoothness $H^{a,b}(p,\mathbb{T}^d)$ which collect all $f \in L_2(\mathbb{T}^d)$ for which the norm

$$\left[\sum_{\mathbf{k}\in\mathbb{Z}^d} |c_{\mathbf{k}}|^2 \big(1+\sum_{j=1}^{d} |k_j|^p\big)^{2a/p} \prod_{j=1}^{d} (1+|k_j|^2)^b\right]^{1/2}$$

is finite; see [1]. In detail, we complement some conclusions drawn in [2] by showing the following complete tractability characterization:

▶ **Theorem 1.** *Let $\gamma,\beta\in\mathbb{R}$, $p\in(0,\infty]$, $\alpha>0$, and $s,t\in[0,\infty)$. Consider* $\mathrm{id} = (\mathrm{id}_d)_{d\in\mathbb{N}}$ *given by*

$$\mathrm{id}_d \colon H^{\gamma+\alpha,\beta}(p,\mathbb{T}^d) \to H^{\gamma,\beta}(p,\mathbb{T}^d), \quad f \mapsto \mathrm{id}_d(f) = f,$$

w.r.t. the worst case setting and Λ^{all}. Then we have (s,t)-weak tractability if and only if

$$s > \frac{p}{\alpha} \ \text{ and } \ t>0 \qquad \text{or} \qquad s>0 \ \text{ and } \ t>1.$$

In particular,

- *UWT, QPT, PT, or SPT never holds,*
- *classical weak tractability holds if and only if $\alpha > p$.*

Finally, we have the curse of dimensionality if and only if $p=\infty$.

References

1 M. Griebel and S. Knapek. *Optimized tensor-product approximation spaces. Constr. Approx.*, 16(4):525–540, 2000.
2 T. Kühn, S. Mayer, and T. Ullrich. *Counting via entropy: new preasymptotics for the approximation numbers of Sobolev embeddings.* arXiv:1505.00631, 2015.
3 E. Novak and H. Woźniakowski. *Tractability of Multivariate Problems. Vol. I–III.* EMS, Zürich, 2008–2012.

3.31 On SDEs with arbitrary slow convergence rate at the final time

Larisa Yaroslavtseva (Universität Passau, DE)

Joint work of Yaroslavtseva, Larisa; Jentzen, Arnulf; Müller-Gronbach, Thomas
Main reference A. Jentzen, T. Müller-Gronbach, L. Yaroslavtseva, "On stochastic differential equations with arbitrary slow convergence rates for strong approximation," arXiv:1506.02828v1 [math.NA], 2015.
URL http://arxiv.org/abs/1506.02828v1

In the recent article [Hairer, M., Hutzenthaler, M., & Jentzen, A., Loss of regularity for Kolmogorov equations, To appear in Ann. Probab. (2015)] it has been shown that there exist stochastic differential equations (SDEs) with infinitely often differentiable and bounded coefficients such that the Euler scheme converges to the solution in the strong sense but with no polynomial rate. Hairer et al.'s result naturally leads to the question whether this slow convergence phenomenon can be overcome by using a more sophisticated approximation method than the simple Euler scheme. In this talk we answer this question to the negative. We prove that there exist SDEs with infinitely often differentiable and bounded coefficients such that no approximation method based on finitely many observations of the driving Brownian motion converges in absolute mean to the solution with a polynomial rate. Even worse, we prove that for every arbitrarily slow convergence speed there exist SDEs with infinitely often differentiable and bounded coefficients such that no approximation method based on finitely many observations of the driving Brownian motion can converge in absolute mean to the solution faster than the given speed of convergence.

Participants

- James M. Calvin
NJIT – Newark, US
- Ronald Cools
KU Leuven, BE
- Sonja Cox
University of Amsterdam, NL
- Steffen Dereich
Universität Münster, DE
- Stefan Geiss
University of Jyväskylä, FI
- Michael Gnewuch
Universität Kiel, DE
- Mario Hefter
TU Kaiserslautern, DE
- Stefan Heinrich
TU Kaiserslautern, DE
- Aicke Hinrichs
Universität Linz, AT
- Alexander Keller
NVIDIA GmbH – Berlin, DE
- Peter Kritzer
Universität Linz, AT
- Thomas Kühn
Universität Leipzig, DE
- Peter Mathé
Weierstraß Institut – Berlin, DE
- Thomas Müller-Gronbach
Universität Passau, DE
- Andreas Neuenkirch
Universität Mannheim, DE
- Dong Nguyen
KU Leuven, BE
- Erich Novak
Universität Jena, DE
- Dirk Nuyens
KU Leuven, BE
- Jens Oettershagen
Universität Bonn, DE
- Sergei Pereverzyev
RICAM – Linz, AT
- Leszek Plaskota
University of Warsaw, PL
- Pawel Przybylowicz
AGH Univ. of Science & Technology-Krakow, PL
- Holger Rauhut
RWTH Aachen, DE
- Klaus Ritter
TU Kaiserslautern, DE
- Daniel Rudolf
Universität Jena, DE
- Winfried Sickel
Universität Jena, DE
- Pawel Siedlecki
University of Warsaw, PL
- Ian H. Sloan
University of New South Wales – Sydney, AU
- Jeremy Staum
Northwestern University – Evanston, US
- Ingo Steinwart
Universität Stuttgart, DE
- Mario Ullrich
Universität Linz, AT
- Tino Ullrich
Universität Bonn, DE
- Markus Weimar
Universität Marburg, DE
- Larisa Yaroslavtseva
Universität Passau, DE
- Marguerite Zani
Université d'Orléans, FR

Report from Dagstuhl Seminar 15392

Measuring the Complexity of Computational Content: Weihrauch Reducibility and Reverse Analysis

Edited by

Vasco Brattka[1], Akitoshi Kawamura[2], Alberto Marcone[3], and Arno Pauly[4]

1 **Universität der Bundeswehr – München, DE,** Vasco.Brattka@unibw.de
2 **University of Tokyo, JP,** kawamura@graco.c.u-tokyo.ac.jp
3 **University of Udine, IT,** alberto.marcone@uniud.it
4 **University of Cambridge, GB,** Arno.Pauly@cl.cam.ac.uk

Abstract

This report documents the program and the outcomes of Dagstuhl Seminar 15392 "Measuring the Complexity of Computational Content: Weihrauch Reducibility and Reverse Analysis." It includes abstracts on most talks presented during the seminar, a list of open problems that were discussed and partially solved during the meeting as well as a bibliography on the seminar topic that we compiled during the seminar.

Seminar September 20–25, 2015 – http://www.dagstuhl.de/15392
1998 ACM Subject Classification F.1.1 Models of Computation, F.1.3 Complexity Measures and Classes, F.2.1 Numerical Algorithms and Problems, F.4.1 Mathematical Logic
Keywords and phrases Computability and complexity in analysis, computations on real numbers, reducibilities, descriptive complexity, computational complexity, reverse and constructive mathematics
Digital Object Identifier 10.4230/DagRep.5.9.77
Edited in cooperation with Rupert Hölzl

1 Executive Summary

Vasco Brattka
Akitoshi Kawamura
Alberto Marcone
Arno Pauly

Reducibilities such as many-one, Turing or polynomial-time reducibility have been an extraordinarily important tool in theoretical computer science from its very beginning. In recent years these reducibilites have been transferred to the continuous setting, where they allow to classify computational problems on real numbers and other (continuous) data types.

On the one hand, Klaus Weihrauch's school of computable analysis and several further researchers have studied a concept of reducibility that can be seen as an analogue of many-one reducibility for functions on such data. The resulting structure is a lattice that yields a refinement of the Borel hierarchy and embeds the Medvedev lattice. Theorems of for-all-exists form can be easily classified in this structure.

Measuring the Complexity of Computational Content: Weihrauch Reducibility and Reverse Analysis,
Dagstuhl Reports, Vol. 5, Issue 9, pp. 77–104
Editors: Vasco Brattka, Akitoshi Kawamura, Alberto Marcone, and Arno Pauly

Dagstuhl Reports
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

On the other hand, Stephen Cook and Akitoshi Kawamura have independently introduced a polynomial-time analogue of Weihrauch's reducibility, which has been used to classify the computational complexity of problems on real numbers and other objects. The resulting theory can be seen as a uniform version of the complexity theory on real numbers as developed by Ker-I Ko and Harvey Friedman.

The classification results obtained with Weihrauch reducibility are in striking correspondence to results in reverse mathematics. This field was initiated by Harvey Friedman and Stephen Simpson and its goal is to study which comprehension axioms are needed in order to prove certain theorems in second-order arithmetic. The results obtained so far indicate that Weihrauch reducibility leads to a finer uniform structure that is yet in basic agreement with the non-uniform results of reverse mathematics, despite some subtle differences.

Likewise one could expect relations between weak complexity theoretic versions of arithmetic as studied by Fernando Ferreira et al., on the one hand, and the polynomial-analogue of Weihrauch reducibility studied by Cook, Kawamura et al., on the other hand.

While the close relations between all these approaches are obvious, the exact situation has not yet been fully understood. One goal of our seminar was to bring researchers from the respective communities together in order to discuss the relations between these research topics and to create a common forum for future interactions.

We believe that this seminar has worked extraordinarily well. We had an inspiring meeting with many excellent presentations of hot new results and innovative work in progress, centred around the core topic of our seminar. In an Open Problem Session many challenging current research questions have been addressed and several of them have been solved either during the seminar or soon afterwards, which underlines the unusually productive atmosphere of this meeting.

A bibliography that we have compiled during the seminar witnesses the substantial amount of research that has already been completed on this hot new research topic up to today.

This report includes abstracts of many talks that were presented during the seminar, it includes a list of some of the open problems that were discussed, as well as the bibliography.

Altogether, this report reflects the extraordinary success of our seminar and we would like to use this opportunity to thank all participants for their valuable contributions and the Dagstuhl staff for their excellent support!

2 Table of Contents

3 Overview of Talks

3.1 Preliminary investigations into Eilenberg-Moore algebras arising in descriptive set theory

Matthew de Brecht (NICT – Osaka, JP)

Recently we proposed an abstract notion of a "jump-operator" to unify characterizations of limit-computability and other topological and recursion-theoretic complexity classes given by V. Brattka, M. Ziegler, and others. These operators determine functors on the category of (Baire-) represented spaces, are closely related to (strong) Weihrauch reducibility, and can be used to represent the major complexity hierarchies in descriptive set theory. In particular, sets of a given level of the Borel hierarchy correspond to realizable maps into particular "jumps" of the Sierpinski-space.

In a different context, P. Taylor has been developing a re-axiomatization of topology inspired by M. Stone's celebrated duality theorem between topology and algebra. Within this paradigm, P. Taylor showed that many important concepts from topology can be described using the exponential object of maps into an object playing the role of the Sierpinski-space. In particular, fundamental aspects of Stone duality can be expressed in terms of Eilenberg-Moore algebras of a monad defined using the Sierpinski-space object. The resulting theory is quite general, and much can be expressed with very little assumptions on the Sierpinski-space object.

In this talk, we present preliminary investigations into interpreting some parts of P. Taylor's theory using "jumps" of the Sierpinski-space as the basic Sierpinski-space object, and look at some examples of the resulting Eilenberg-Moore algebras. As a case study, we make some connections with the Jayne-Rogers theorem by applying recent results on that theorem by A. Pauly and myself.

This work was supported by JSPS Core-to-Core Program, A. Advanced Research Networks and by JSPS KAKENHI Grant Number 15K15940.

3.2 The mathematics and metamathematics of weak analysis

Fernando Ferreira (University of Lisboa, PT)

In this survey talk, we start by remarking that it is well-known that the provably total functions of the base theory RCA_0 of reverse mathematics are the primitive recursive functions. We show how to set up a similar theory (called BTFA, an acronym for 'base theory for feasible analysis') whose provably total functions are (in an appropriate sense) the polytime computable functions. As with RCA_0, one can add to this theory weak König's lemma without proving new Π^0_2-consequences. We draw attention to the pivotal rôle of the bounded collection scheme in defining BTFA and in the proof of the above conservation result, and also to some differences with the usual setting of reverse mathematics (weak König's lemma can be formulated in BTFA not only for set trees but, more generally, for trees defined by bounded formulas).

We describe how to introduce the real numbers in the theory BTFA. Continuous functions can also be introduced, following the usual blueprint of reverse mathematics. The intermediate value theorem can be proved and, in particular, the real numbers form a real closed ordered field (but are more than just that). We discuss the rôle of (several forms of) weak König's lemma in the setting of BTFA in relation to the Heine-Borel theorem, the uniform continuity theorem and the attainament of maximum for continuous real functions defined on a closed bounded interval.

We also briefly describe two other theories of weak analysis: one related to Vaillant's class $\#P$ of counting functions and the other related to polyspace computability. We show how to introduce Riemann integration in the former theory and argue that, in a sense (namely, for continuous functions defined *à la* Simpson with a modulus of uniform continuity) this is the weaker theory in which integration can be done.

References

1 F. Ferreira, A feasible theory for analysis. The Journal of Symbolic Logic 59, 1001–1011 (1994).

2 A. Fernandes & F. Ferreira, Groundwork for weak analysis. The Journal of Symbolic Logic 67, 557–578 (2002).

3 A. Fernandes & F. Ferreira, Basic applications of weak König's lemma in feasible analysis. In: *Reverse Mathematics 2001*, S. Simpson (editor), Association for Symbolic Logic / A K Peters 2005, 175–188.

4 F. Ferreira & Gilda Ferreira, Counting as integration in feasible analysis. Mathematical Logic Quarterly 52, 315–320 (2006).

5 A. Fernandes, F. Ferreira & G. Ferreira, Techniques in weak analysis for conservation results. In: *New Studies in Weak Arithmetics*, P. Cégielski, Ch. Cornaros and C. Dimitracopoulos (eds.), CSLI Publications (Stanford) and Presses Universitaires (Paris 12) 2013, 115–147.

6 F. Ferreira & G. Ferreira, The Riemann integral in weak systems of analysis. Journal of Universal Computer Science 14, 908–937 (2008).

3.3 The Weihrauch degrees of conditional distributions

Cameron Freer (MIT – Cambridge, US)

Joint work of Ackerman, Nathanael L.; Freer, Cameron; Roy, Daniel
Main reference N. L. Ackerman, C. Freer, D. Roy, "On computability and disintegration," arXiv:1509.02992v1 [math.LO], 2015.
URL http://arxiv.org/abs/1509.02992v1

We show that the disintegration operator on a complete separable metric space along a projection map, restricted to measures having a unique continuous disintegration, is strongly Weihrauch equivalent to the limit operator Lim. When a measure does not have a unique continuous disintegration, we may still obtain a disintegration when some basis of continuity sets has the Vitali covering property with respect to the measure; the disintegration, however, may depend on the choice of sets. We show that, when the basis is computable, the resulting disintegration is strongly Weihrauch reducible to Lim, and further exhibit a single distribution realizing this upper bound.

3.4 Probabilistic computability and the Vitali Covering Theorem

Guido Gherardi (Universität der Bundeswehr – München, DE)

Joint work of Brattka, Vasco; Gherardi, Guido; Hölzl, Rupert

Our recent work [3] has developed our investigation on probabilistic and Las Vegas computability for sequences of infinite length, already introduced and studied in [1] and [2].

Las Vegas computable (multi-valued) functions are those (multi-valued) functions on represented spaces that can be computed with positive success probability by *non deterministic TTE Turing machines*. Such devices constitute a more powerful variation of TTE Turing machines: they are allowed to integrate the information contained in the input by accessing auxiliary information contained in a *randomly selected* binary string ("*oracle*"). If such randomly accessed information is useful to solve the task, then a correct output is produced. Otherwise, after finitely many steps, the machine recognizes the failure and outputs in fact a failure message. If a (multi-valued) function $f :\subseteq X \rightrightarrows Y$ over represented spaces can be computed by a non deterministic TTE Turing machine under the condition that for every possible input the set of successful oracles has positive measure in the Cantor space, then f is said to be *Las Vegas computable*.

We also consider functions that can be simulated on non deterministic Turing machines that replace the oracle space $2^{\mathbb{N}}$ by $\mathbb{N} \times 2^{\mathbb{N}}$. In reality, such functions can also be computed by non deterministic Turing machines that maintain $2^{\mathbb{N}}$ as oracle space but that are allowed to do finitely many corrections on the output tape. For this reason we call such functions *Las Vegas computable with finitely many mind changes*. This new class of functions extends the previous one, and both classes are contained in the wider class of *probabilistic functions*, that is, the class of those functions computed by selecting the Baire space $\mathbb{N}^{\mathbb{N}}$ as oracle space and without demanding for failure messages in case of unsuccess.

As a very significant study case we have investigated the classical *Vitali covering theorem*: every sequence $\mathcal{I}$ of open intervals that *Vitali covers* a Lebesgue measurable subset $A \subseteq [0,1]$ (i.e., $\mathcal{I}$ is such that every point of A is contained in arbitrarily small elements of $\mathcal{I}$) includes a countable sequence $\mathcal{J}$ *eliminating* A (i.e., the elements of $\mathcal{J}$ are pairwise disjoint and cover A up to measure 0). Several classically equivalent versions of the statement are of course possible. We have analyzed three natural versions for $A := [0,1]$ that we are going to formulate after having introduced the following terminology. For every sequence of open intervals $\mathcal{I}$, a point x is *captured* by $\mathcal{I}$ if it is contained in elements of $\mathcal{I}$ of arbitrarily small diameter. Moreover $\mathcal{I}$ is called *saturated* if every point covered by some element in $\mathcal{I}$ is even captured by $\mathcal{I}$ (therefore, every Vitaly cover is a saturated sequence). We have then the following versions of the theorem:

1. For every Vitali cover $\mathcal{I}$ of $[0,1]$ there exists a countable subsequence $\mathcal{J}$ of $\mathcal{I}$ that eliminates $[0,1]$.
2. For every saturated sequence $\mathcal{I}$ of open intervals that does not admit a countable subsequence eliminating $[0,1]$ there exists a point $x \in [0,1]$ that is not covered by $\mathcal{I}$.
3. For every sequence $\mathcal{I}$ of open intervals that does not admit a countable subsequence eliminating $[0,1]$ there exists a point $x \in [0,1]$ that is not captured by $\mathcal{I}$.

These three classically equivalent versions define three different operators defined on Int, the set of all sequences of open rational intervals in $\mathbb{R}$:

1. $\mathrm{VCT}_0 :\subseteq \mathrm{Int} \rightrightarrows \mathrm{Int}$ with

$$\mathrm{VCT}_0(\mathcal{I}) := \{\mathcal{J} : \mathcal{J} \text{ is a countable subsequence of } \mathcal{I} \text{ eliminating } [0,1]\}$$

for $\mathcal{I}$ a Vitali cover of $[0,1]$;

2. $\mathrm{VCT}_1 :\subseteq \mathrm{Int} \rightrightarrows [0,1]$ with

$$\mathrm{VCT}_1(\mathcal{I}) := \{x \in [0,1] : x \text{ is not covered by } \mathcal{I}\}$$

for $\mathcal{I}$ saturated with no countable subsequence eliminating $[0,1]$;
3. $\mathrm{VCT}_2 :\subseteq \mathrm{Int} \rightrightarrows [0,1]$ with

$$\mathrm{VCT}_2(\mathcal{I}) := \{x \in [0,1] : x \text{ is not captured by } \mathcal{I}\}$$

for $\mathcal{I}$ with no countable subsequence eliminating $[0,1]$.

It turns out that these operators are computationally very significant, in particular to characterize the notion of Las Vegas computability. In fact the following theorems hold:

▶ **Theorem 1.** VCT_0 *is computable.*

▶ **Theorem 2.** VCT_1 *is Weihrauch complete with respect to the class of Las Vegas computable functions.*

▶ **Theorem 3.** VCT_2 *is Weihrauch complete with respect to the class of Las Vegas computable functions with finitely many mind changes.*

Theorem 2 is proved by showing that $\mathrm{VCT}_1 \equiv_{\mathrm{W}} \mathrm{PC}_{[0,1]}$, where $\mathrm{PC}_{[0,1]}$ is the operator selecting points from closed subsets of $[0,1]$ of positive Lebesgue measure. It was indeed proved in [2] that this operator is Weihrauch complete with respect to the class of Las Vegas computable functions. Analogously, Theorem 3 is proved by showing that $\mathrm{VCT}_2 \equiv_{\mathrm{W}} \mathrm{PC}_{\mathbb{R}}$, where $\mathrm{PC}_{\mathbb{R}}$ is the extension of the previous positive choice operator over $[0,1]$ to the whole real line (one direction of the equivalence has been proved by Arno Pauly).

We point out that the Vitali Covering Theorem has been proved to be equivalent to the principle WWKL_0 in Reverse Mathematics ([4]). In fact, in computable anlysis $\mathrm{WWKL} \equiv_{\mathrm{W}} \mathrm{PC}_{[0,1]}$ holds, where WWKL is the natural operational interpretation of the proof theoretic principle WWKL_0: every infinite binary tree of positive measure contains an infinite path. Nevertheless the situation in our framework is, as we have seen, more finely structured and at the same time particularly interesting, since the same theorem can be used to characterize three important different computational classes.

References

1 Vasco Brattka, Guido Gherardi, Rupert Hölzl. Las Vegas computability and algorithmic randomness. *STACS 2015.* Dagstuhl Publishing. 130–142. 2015
2 Vasco Brattka, Guido Gherardi, Rupert Hölzl. Probabilistic computability and choice. *Information and Computation.* 242:249–286. 2015
3 Vasco Brattka, Guido Gherardi, Rupert Hölzl, Arno Pauly: Vitali Covering Theorem and Las Vegas Computability. Unpublished notes.
4 Stephen Simpson: *Subsystems of Second Order Arithmetic.* Springer Verlag. 2009

3.5 Topological Complexity and Topological Weihrauch Degrees

Peter Hertling (Universität der Bundeswehr – München, DE)

We describe the relation between various ways for measuring the topological complexity of computation problems: either by counting the number of comparison nodes that a

computation tree for the problem needs to have, or by the level of discontinuity of the problem or by the topological Weihrauch degree of the problem. The hierarchies defined via continuous Weihrauch reductions refine the hierarchy defined by the level. Examples from algebraic complexity theory, from information-based complexity and from algebraic topology are presented. Furthermore, we show that an initial segment of the topological Weihrauch degrees of computation problems given by relations with finite discrete range can be described by classes of labeled forests under suitable reducibility relations on the class of labeled forests.

3.6 Reverse Mathematics and Computability-Theoretic Reduction

Denis R. Hirschfeldt (University of Chicago, US)

Reverse mathematics is a research program that aims to calibrate the strength of theorems of ordinary mathematics in the context of subsystems of second-order arithmetic. Typically, one performs this calibration over the weak base theory RCA_0, which roughly corresponds to the level of computable mathematics. This practice has been quite successful in many respects, but its very success has led to a desire for more fine-grained tools than implication over RCA_0. This talk will introduce a few notions of computability-theoretic reduction between principles of a certain form, one of which is equivalent to Weihrauch reducibility.

3.7 Formalized reducibility

Jeffry L. Hirst (Appalachian State University – Boone, US)

Joint work of Hirst, Jeffry L.; Mummert, Carl; Gura, Kirill
Main reference K. Gura, J. L. Hirst, C. Mummert, "On the existence of a connected component of a graph," Computability, 4(2):103–117, 2015.
URL http://dx.doi.org/10.3233/COM-150039

Some forms of reduciblity can be formalized in higher order reverse mathematics, as axiomatized by Professor Kohlenbach [1]. Proving strong Weihrauch reductions in the higher order reverse mathematics setting yields both the usual reduction results and associated sequential reverse mathematics results as easy corollaries.

Several natural questions arise from considering these formal proofs. For what portions of type-2 constuctable analysis would this sort of formalization be fruitful? What is the comparative logical strength of the various functional existence axioms generated in this way? What foundational insights can be gained here? What about other reducibilities?

References

1 Ulrich Kohlenbach, *Higher order reverse mathematics* In: Reverse mathematics 2001, Lecture Notes in Logic, vol. 21, Assoc. Symbol. Logic, La Jolla, CA, (2005) 281–295.

3.8 Universality, optimality, and randomness deficiency

Rupert Hölzl (Universität Heidelberg, DE)

Joint work of Hölzl, Rupert; Paul Shafer
Main reference R. Hölzl, P. Shafer, "Universality, optimality, and randomness deficiency," Annals of Pure and Applied Logic, 166(10):1049–1069, 2015.
URL http://dx.doi.org/10.1016/j.apal.2015.05.006

A Martin-Löf test $\mathcal{U}$ is universal if it captures all non-Martin-Löf random sequences, and it is optimal if for every Martin-Löf test $\mathcal{V}$ there is a constant c such that for all n the set $\mathcal{V}_{n+c}$ is contained $\mathcal{U}_n$.

We study the computational differences between universal and optimal Martin-Löf tests as well as the effects that these differences have on both the notion of layerwise computability and the Weihrauch degree of LAY, the function that produces a bound for a given Martin-Löf random sequence's randomness deficiency. We prove several robustness results concerning the Weihrauch degree of LAY. Along similar lines we also study the principle RD, a variant of LAY outputting the precise randomness deficiency of sequences instead of only an upper bound as LAY.

References

1 Rupert Hölzl, Paul Shafer. *Universality, optimality, and randomness deficiency*. Annals of Pure and Applied Logic, 166(10):1049–1069, Elsevier, 2015.

3.9 Constructive reverse mathematics: an introduction

Hajime Ishihara (JAIST – Ishikawa, JP)

Main reference H. Ishihara, "Constructive reverse mathematics: compactness properties," in L. Crosilla, P. Schuster (eds.), "From Sets and Types to Analysis and Topology," Oxford Logic Guides, Vol. 48, pp. 245–267, Oxford University Press, 2005.
URL global.oup.com/uk/isbn/0-19-856651-4

A mathematical theory consists of axioms describing mathematical objects in the theory, and logic being used to derive theorems from the axioms.

Intuitionistic logic is obtained from minimal logic by adding the intuitionistic absurdity rule (ex falso quodlibet), and classical logic is obtained from intuitionistic logic by strengthening the absurdity rule to the classical absurdity rule (reductio ad absurdum).

Intuitionistic mathematics has axioms: the weak continuity for numbers (WCN) and the fan theorem (FAN), and constructive recursive mathematics has axioms: extended Church's thesis (ECT) and Markov's principle (MP). A common consequence of intuitionistic mathematics and constructive recursive mathematics is the Kreisel-Lacombe-Shoenfield-Tsejtin theorem (KLST) which is inconsistent with classical mathematics:

> Every mapping from a complete separable metric space into a metric space is continuous.

The Friedman-Simpson-program (classical reverse mathematics) [2] is a formal mathematics using classical logic with a very weak set existence axiom. Its main question is "Which set existence axioms are needed to prove the theorems of ordinary mathematics?", and many

classical theorems have been classified by set existence axioms of various strengths. Since classical reverse mathematics is formalized with classical logic, we cannot classify theorems in intuitionistic mathematics nor in constructive recursive mathematics which are inconsistent with classical mathematics such as KLST.

The purpose of constructive reverse mathematics [1] is to classify various theorems in intuitionistic, constructive recursive and classical mathematics by logical principles, function existence axioms and their combinations.

References

1 Hajime Ishihara, *Constructive reverse mathematics: compactness properties*, In: L. Crosilla and P. Schuster eds., *From Sets and Types to Analysis and Topology*, Oxford Logic Guides 48, Oxford Univ. Press, 2005, 245–267.
2 Stephen G. Simpson, *Subsystems of Second Order Arithmetic*, Springer, Berlin, 1999.

3.10 Decomposing Borel functions and generalized Turing degree theory

Takayuki Kihara (University of California – Berkeley, US)

The Jayne-Rogers Theorem states that a function from an absolutely Souslin-F set into a separable metrizable space is first-level Borel measurable (that is, the preimage of each F_σ set under the function is again F_σ) if and only if it is decomposable into countably many continuous functions with Δ^0_2 domains. Recently, Gregoriades, K., and Ng [1, 2] used the Louveau separation theorem and the Shore-Slaman join theorem to show that if the preimage of a Σ^0_α set under a function from an analytic space into a Polish space is again $\Sigma^0_{\beta+1}$ then the function is decomposable into countably many functions each of which is $\Sigma^0_{\gamma+1}$-measurable for some γ with $\gamma + \alpha \leq \beta$. As shown by K. and Pauly [3], by combining other computability-theoretic methods, this theorem can be used to construct a family of continuum many infinite dimensional Cantor manifolds with property C in the sense of Haver/Addis-Gresham whose Borel structures at an arbitrary finite rank are mutually non-isomorphic.

Now we discuss possible extensions of this decomposition theorem of Borel functions. Is there a generalization of the theorem in higher measurabillity levels such as Nikodym's hierarchy of Selivanovskii's C-sets, Kolmogorov's R-sets and beyond? Is there a generalization in a wider category of topological spaces? We mainly focus on the latter problem, and give a few results on separation axioms and quasi-minimal enumeration degrees.

References

1 Vassilios Gregoriades and Takayuki Kihara, Recursion and effectivity in the decomposability conjecture, submitted.
2 Takayuki Kihara, Decomposing Borel functions using the Shore-Slaman join theorem, Fundamenta Mathematicae 230 (2015), pp. 1–13.
3 Takayuki Kihara and Arno Pauly, Point degree spectra of represented spaces, submitted.

3.11 Convergence Theorems in Mathematics: Reverse Mathematics and Weihrauch degrees versus Proof Mining

Ulrich Kohlenbach (TU Darmstadt, DE)

We discuss the issue of how to formulate the computational content of convergence statements and compare the information provided by reverse mathematics, Weihrauch degrees and proof mining.

'Proof Mining' emerged as a systematic program during the last two decades as a new applied form of proof theory and has successfully been applied to a number of areas of core mathematics (see [3] for a book treatment of this paradigm covering the development up to 2008). This program has its roots in Georg Kreisel's pioneering ideas of 'unwinding of proofs' going back to the 1950's who asked for a 'shift of emphasis' in proof theory away from issues of mere consistency of mathematical theories ('Hilbert's program') to the question 'What more do we know if we have proved a theorem by restricted means than if we merely know that it is true?' Proof Mining is concerned with the extraction of hidden finitary and combinatorial content from proofs that make use of infinitary noneffective principles. The main logical tools for this are so-called proof interpretations. Logical metatheorems based on such interpretations have been applied with particular success in the context of nonlinear analysis including fixed point theory (e.g. [8]), ergodic theory (e.g. [4, 11]), continuous optimization (e.g. [9, 5] and abstract Cauchy problems ([6]). The combinatorial content can manifest itself both in explicit effective bounds as well as in the form of uniformity results.

In this talk we focus on convergence theorems. In many cases one can show that a computable rate of convergence cannot exist (see e.g. [12]). In terms of (intuitionistic) reverse mathematics this usually corresponds to the fact that the Cauchy statement for the sequence (x_n) at hand implies the law-of-excluded-middle-principle for Σ^0_1-formulas (Σ^0_1-LEM which is also called LPO, see [16, 10]) and that the existence of a limit requires arithmetical comprehension ACA. In terms of Weihrauch degrees one often has, corresponding to this, that $\lim \equiv_W \lim(x_n)$ (see [12]). We show that Proof Mining provides more detailed information on noneffective convergence statements by extracting explicit and highly uniform subrecursive bounds on the so-called metastable (in the sense of Tao [14, 15]) reformulation of the Cauchy property. These bounds also allow for a detailed analysis of the convergence statements in terms of the algorithmic learnability of a rate of convergence which under certain conditions may result in oscillation bounds (see [10, 2]). In some cases this can be converted into full rates of convergence. We exemplify this with strong convergence results that are based on Fejér monotonicity of sequences defined by suitable iterations of nonlinear functions ([9]). We give applications of this in the context of the proximal point algorithm in Hilbert spaces ([9]) and to recent results ([1]) of convex feasibility problems in CAT(κ)-spaces ([5]). We also discuss a recent asymptotic regularity result of a general alternated iteration procedure in CAT(0)-spaces which applies to the resolvents of lower semi-continuous convex functions ([1]). From the prima facie highly noneffective convergence proof in [1] a simple exponential rate of convergence could be extracted using the logical machinery ([13]). In all these cases already the proof of the Cauchy property prima facie made use of ACA which, however, gets eliminated in the course of the extraction procedure.

We also briefly mention an explicit bound extracted recently in the context of nonlinear semigroups from a proof based on the weak ('binary') König's lemma WKL ([7]).

References

1 David Ariza-Ruiz, Genaro López-Acedo, Adriana Nicolae. *The asymptotic behavior of the composition of firmly nonexpansive mappings*. J. Optim. Theory Appl. vol. 167, pp. 409-429 (2015), DOI: 10.1007/s10957-015-0710-3.

2 Jeremy Avigad, Jason Rute. *Oscillation and the mean ergodic theorem for uniformly convex Banach spaces*. Ergodic Theory and Dynamical Systems 35, pp. 1009–1027 (2015).

3 Ulrich Kohlenbach. *Applied Proof Theory: Proof Interpretations and their Use in Mathematics*. Springer Monograph in Mathematics, xx+536pp., 2008.

4 Ulrich Kohlenbach *A uniform quantitative form of sequential weak compactness and Baillon's nonlinear ergodic theorem*. Communications in Contemporary Mathematics 14, 20pp. (2012).

5 Ulrich Kohlenbach. *On the quantitative asymptotic behavior of strongly nonexpansive mappings in Banach and geodesic spaces*. To appear in: Israel Journal of Mathematics.

6 Ulrich Kohlenbach, Angeliki Koutsoukou-Argyraki. *Rates of convergence and metastability for abstract Cauchy problems generated by accretive operators*, J. Math. Anal. Appl. 423, pp. 1089–1112 (2015).

7 Ulrich Kohlenbach, Angeliki Koutsoukou-Argyraki. *Effective asymptotic regularity for one-parameter nonexpansive semigroups*. J. Math. Anal. Appl. 433, pp. 1883–1903 (2016).

8 Ulrich Kohlenbach, Laurenţiu Leuştean. *Asymptotically nonexpansive mappings in uniformly convex hyperbolic spaces*. Journal of the European Mathematical Society 12, pp. 71–92 (2010).

9 Ulrich Kohlenbach, Laurenţiu Leuştean, Adriana Nicolae. *Quantitative results of Fejér monotone sequences*. Preprint 2014, arXiv:1412.5563, submitted.

10 Ulrich Kohlenbach, Pavol Safarik. *Fluctuations, effective learnability and metastability in analysis*, Ann. Pure Appl. Logic 165, pp. 266–304 (2014).

11 Laurenţiu Leuştean, Adriana Nicolae. *Effective results on nonlinear ergodic averages in CAT(k) spaces*. Ergodic Theory and Dynamical Systems, DOI: 10.1017/etds.2015.31, 2015

12 Eike Neumann. *Computational problems in metric fixed point theory and their Weihrauch degrees*. To appear in: Logical Methods in Computer Science.

13 Adriana Nicolae, Ulrich Kohlenbach, Genaro López-Acedo. *Asymptotic regularity results for the composition of two mappings*, Preprint in preparation.

14 Terence Tao. *Soft analysis, hard analysis, and the finite convergence principle*. Essay posted May 23, 2007. Appeared in: 'T. Tao, Structure and Randomness: Pages from Year One of a Mathematical Blog. AMS, 298pp., 2008.

15 Terence Tao. *Norm convergence of multiple ergodic averages for commuting transformations*. Ergodic Theory and Dynamical Systems 28, pp. 657–688 (2008).

16 Michael Toftdal. *A calibration of ineffective theorems of analysis in a hierachy of semi-classical logical principles*. In: J. Diaz et al. (eds.), ICALP 2004, Springer LNCS 3142, pp. 1188–1200, 2004.

3.12 On the Uniform Computational Content of the Baire Category Theorem

Alexander P Kreuzer (National University of Singapore, SG)

Joint work of Brattka, Vasco; Hendtlass Matthew; Kreuzer, Alexander P.
Main reference V. Brattka, M. Hendtlass, A. P. Kreuzer, "On the Uniform Computational Content of the Baire Category Theorem," arXiv:1510.01913v1 [math.LO], 2015.
URL http://arxiv.org/abs/1510.01913v1

We study the uniform computational content of different versions of the Baire Category Theorem in the Weihrauch lattice. The Baire Category Theorem can be seen as a pigeonhole principle that states that a complete (i.e., "large") metric space cannot be decomposed into countably many nowhere dense (i.e., "small") pieces. The Baire Category Theorem is an illuminating example of a theorem that can be used to demonstrate that one classical theorem can have several different computational interpretations. For one, we distinguish two different logical versions of the theorem, where one can be seen as the contrapositive form of the other one. The first version aims to find an uncovered point in the space, given a sequence of nowhere dense closed sets. The second version aims to find the index of a closed set that is somewhere dense, given a sequence of closed sets that cover the space. Even though the two statements behind these versions are equivalent to each other in classical logic, they are not equivalent in intuitionistic logic and likewise they exhibit different computational behavior in the Weihrauch lattice. Besides this logical distinction, we also consider different ways how the sequence of closed sets is "given". Essentially, we can distinguish between positive and negative information on closed sets. We discuss all the four resulting versions of the Baire Category Theorem. Somewhat surprisingly it turns out that the difference in providing the input information can also be expressed with the jump operation. Finally, we also relate the Baire Category Theorem to notions of genericity and computably comeager sets.

3.13 From Well-Quasi-Orders to Noetherian Spaces: Reverse Mathematics results and Weihrauch lattice questions

Alberto Marcone (University of Udine, IT)

Joint work of Frittaion, Emanuele; Hendtlass, Matthew; Marcone, Alberto; Shafer, Paul; Van der Meeren, Jeroen
Main reference E. Frittaion, M. Hendtlass, A. Marcone, P. Shafer, J. Van der Meeren, "Reverse mathematics, well-quasi-orders, and Noetherian spaces," arXiv:1504.07452v2 [math.LO], 2015.
URL http://arxiv.org/abs/1504.07452v2

We study some theorems by Goubalt-Larrecq from the viewpoint of reverse mathematics. These theorems deal with the relationship between well-quasi-orders and Noetherian spaces. The main result is the following:

▶ **Theorem 1** (RCA_0). *The following are equivalent:*
1. ACA_0;
2. *if $\mathcal{Q}$ is wqo then $\mathcal{A}(\mathcal{P}^\flat_f(\mathcal{Q}))$ is Noetherian;*
3. *if $\mathcal{Q}$ is wqo then $\mathcal{U}(\mathcal{P}^\flat_f(\mathcal{Q}))$ is Noetherian;*
4. *if $\mathcal{Q}$ is wqo then $\mathcal{U}(\mathcal{P}^\sharp_f(\mathcal{Q}))$ is Noetherian;*
5. *if $\mathcal{Q}$ is wqo then $\mathcal{U}(\mathcal{P}^\flat(\mathcal{Q}))$ is Noetherian;*
6. *if $\mathcal{Q}$ is wqo then $\mathcal{U}(\mathcal{P}^\sharp(\mathcal{Q}))$ is Noetherian.*

These statements are of the form:

$$\forall X(\forall Z\, \Phi(X,Z) \implies \forall Y\, \Psi(X,Y))$$

with Φ and Ψ arithmetical (because both "$\mathcal{Q}$ is wqo" and "$\mathcal{U}(\mathcal{Q})$ is Noetherian" are $\mathbf{\Pi}^1_1$). Thus, even if they are $\mathbf{\Pi}^1_2$, they do not fit nicely in the problem/solution pattern usually used to translate $\mathbf{\Pi}^1_2$ statements into multi-valued functions analyzed in the Weihrauch lattice setting.

We suggest to rewrite

$$\forall X(\forall Z\, \Phi(X,Z) \implies \forall Y\, \Psi(X,Y))$$

as

$$\forall X\, \forall Y(\neg\Psi(X,Y) \implies \exists Z\, \neg\Phi(X,Z)).$$

Now a problem is a pair consisting of a quasi-order $\mathcal{Q}$ and a witness to the fact that $\mathcal{U}(\mathcal{P}^\sharp(\mathcal{Q}))$ is not Noetherian. Its solutions are the sequences witnessing that $\mathcal{Q}$ is not wqo.

In fact the proofs of both directions of the reverse mathematics results actually work with

if $\mathcal{U}(\mathcal{P}^\sharp(\mathcal{Q}))$ is not Noetherian then $\mathcal{Q}$ is not wqo

so the above translation in problem/solution form is quite faithful.

3.14 Separation of randomnes notions in Weihrauch degrees

Kenshi Miyabe (Meiji University – Kawasaki, JP)

Joint work of Hölzl, Rupert; Miyabe, Kenshi

We consider randomness notions in the Weihrauch degrees. Let WR, SR, CR, MLR, W2R, DiffR, and 2R be the classes of Kurtz random sets, Schnorr random sets, computably random sets, ML-random sets, weakly 2-random sets, difference random sets, and 2-random sets, respectively. These notions naturally induce operations in the Weihrauch degrees, that we denote by the same notations. In particular, MLR has been studied in the literature. Here, we only consider the usual Turing relativization.

We have the following reductions:

$$\mathrm{WR} <_W \mathrm{SR} \leq_W \mathrm{CR} <_W \mathrm{MLR} <_W \mathrm{W2R} <_W \mathrm{2R}.$$

The strictness of the inequalities above can be proved by looking at hyperimmune degrees, high degrees, and minimal degrees.

In contrast, we need to make use of uniformity to prove the separation between MLR and DiffR.

Whether the Weihrauch degrees of SR and CR can be separated remains an open question.

3.15 On the existence of a connected component of a graph

Carl Mummert (Marshall University – Huntington, US)

Joint work of Gura, Kirill; Hirst, Jeffry L.; Mummert, Carl
Main reference K. Gura, J. L. Hirst, C. Mummert, "On the existence of a connected component of a graph," Computability, 4(2):103–17, 2015.
URL http://dx.doi.org/10.3233/COM-150039

We study the reverse mathematics and computable analysis properties of countable graph theory. We focus on two problems. The first is to construct a single connected component of a countable graph, while the second is to decompose a countable graph into connected components. We show that each of these problems is strongly Weihrauch equivalent to its parallelized form and to the parallelized form of LPO. We also study problems relating to countable graphs in which each connected component is finite, and countable graphs with a finite number of connected components.

3.16 Closed choice and ATR

Arno Pauly (University of Cambridge, GB)

The concept of "iterating taking a limit over some countable ordinal" can be formalized as a Weihrauch degree, and this Weihrauch degree is shown to be equivalent to $\mathrm{UC}_{\mathbb{N}^{\mathbb{N}}}$ (unique choice on Baire space). $\mathrm{UC}_{\mathbb{N}^{\mathbb{N}}}$ is strictly below $\mathrm{C}_{\mathbb{N}^{\mathbb{N}}}$ (choice on Baire space), which is another candidate for a Weihrauch degree corresponding to ATR_0.

Looking at determinacy principles, in reverse math Δ^0_1-determinacy on Cantor space, Δ^0_0-determinacy on Baire space and Σ^0_1-determinacy on Baire space are all equivalent to ATR_0. For Weihrauch degrees, the two former are equivalent to $\mathrm{UC}_{\mathbb{N}^{\mathbb{N}}}$, whereas the latter is at least as hard as $\mathrm{C}_{\mathbb{N}^{\mathbb{N}}}$.

3.17 On Weihrauch Degrees of k-Partitions of the Baire Space

Victor Selivanov (A. P. Ershov Institute – Novosibirsk, RU)

In [7] K. Weihrauch introduced some notions of reducibility for functions on topological spaces turned out useful for understanding the non-computability and non-continuity of decision problems in computable analysis and constructive mathematics. In particular, the following three notions of reducibility between functions $f, g : X \to Y$ on topological spaces were introduced: $f \leq_0 g$ (resp. $f \leq_1 g$, resp. $f \leq_2 g$) iff $f = g \circ H$ for some continuous function $H : X \to X$ (resp. $f = F \circ g \circ H$ for some continuous functions $H : X \to X$, resp. $F : Y \to Y$, $f(x) = F(x, g(H(x)))$ for some continuous functions $H : X \to X$ and $F : X \times Y \to Y$). In this way we obtain preorders $(Y^X; \leq_i)$, $i \leq 2$, on the set Y^X of all functions from X to Y.

The notions are nontrivial even for the case of discrete spaces $Y = k = \{0, \dots, k-1\}$ with $k < \omega$ points (we call functions $A : X \to k$ *k-partitions of X* because they are in a natural bijective correspondence with the partitions $(A_0, \dots, A_{k-1})$ of X where $A_j = f^{-1}(j)$). E.g., for $k = 2$ the relation $\leq_0$ coincides with the classical Wadge reducibility [3].

In [1, 2] P. Hertling gave useful "combinatorial" characterizations of initial segments of the degree structures under Weihrauch reducibilities on k-partitions of the Baire space $\mathcal{N} = \omega^\omega$ whose components are finite boolean combinations of open sets. The Baire space is important in this context because it is commonly used in computable analysis [8] for representing many other spaces of interest. In particular, the structure $(k^{\mathcal{N}}; \leq_0)$ induces (via total admissible representations) the fine hierarchies of k-partitions of quasi-Polish spaces discussed in [6].

In this work we attempt to extend the characterizations from [1, 2] to as large segments of Weihrauch degrees of k-partitions as possible. In particular, for any countable ordinal $\alpha \geq 2$ we try to characterize the quotient-posets of the preorders $((\mathbf{\Delta}^0_\alpha)_k; \leq_i)$ for any $i \leq 2$, where $(\mathbf{\Delta}^0_\alpha)_k$ is the class of k-partitions of $\mathcal{N}$ with components in $\mathbf{\Delta}^0_\alpha$. It is easy to see that $(\mathbf{\Delta}^0_\alpha)_k$ is an initial segment of $(k^{\mathcal{N}}; \leq_i)$ for each $i \leq 2$, i.e. $A \leq_i B \in (\mathbf{\Delta}^0_\alpha)_k$ implies $A \in (\mathbf{\Delta}^0_\alpha)_k$.

By a *forest* we mean a poset without infinite chains in which every upper cone $\{y \mid x \leq y\}$ is a chain. A *k-forest* is a triple $(F; \leq, c)$ consisting of a forest $(F; \leq)$ and a labeling $c : F \to k$. Let $\widetilde{\mathcal{F}}_k$ denote the class of countable k-forests without infinite chains. Note that we use tilde in our notation in order to distinguish $\widetilde{\mathcal{F}}_k$ from the class $\mathcal{F}_k$ of finite k-forests considered in a series of previous publications.

A *0-morphism (resp. 1-morphism, resp. 2-morphism)* $f : (P; \leq, c) \to (P'; \leq', c')$ between k-forests is a monotone function $f : (P; \leq) \to (P'; \leq')$ satisfying $c = c' \circ f$ (resp. satisfying $\forall p, q \in P(c(p) \neq c(q) \to c'(f(p)) \neq c'(f(q)))$, resp. satisfying $\forall p, q \in P(p \leq q \wedge c(p) \neq c(q) \to c'(f(p)) \neq c'(f(q)))$).

For $i \leq 2$, the i-preorder on $\widetilde{\mathcal{F}}_k$ is defined as follows: $(P, \leq, c) \leq_i (P', \leq', c')$, if there is an i-morphism from $(P, \leq, c)$ to $(P', \leq', c')$. Obviously, $\leq_0$ implies $\leq_1$ and $\leq_1$ implies $\leq_2$.

A basic result of this work is the following:

▶ **Theorem 1.** *For all $2 \leq k < \omega$ and $0 \leq i \leq 2$, the quotient-posets of $(\widetilde{\mathcal{F}}_k; \leq_i)$ and $((\mathbf{\Delta}^0_2)_k; \leq_i)$ are isomorphic.*

This results extends the mentioned characterizations from [1, 2]. For $\leq_0$ the result was in fact established in [4, 5]. Although for $i = 1, 2$ the isomorphism is induced by the same function from $\widetilde{\mathcal{F}}_k$ to $(\mathbf{\Delta}^0_\alpha)_k$ as in [4, 5], the proof requires some additional considerations. We believe that the result may be extended to a characterization of $((\mathbf{\Delta}^0_\alpha)_k; \leq_i)$ for any $\alpha \geq 3$, although the proof becomes technically much more involved. So far we succeeded with the proof only for $i = 0$.

References

1 P. Hertling. Topologische Komplexitätsgrade von Funktionen mit endlichem Bild. Informatik-Berichte 152, 34 pages, Fernuniversität Hagen, December 1993.

2 P. Hertling. *Unstetigkeitsgrade von Funktionen in der effektiven Analysis*. Dissertation, Fachbereich Informatik, FernUniversität Hagen, 1996.

3 A. S. Kechris. *Classical Descriptive Set Theory.*, Springer, New York, 1994.

4 V. L. Selivanov. The quotient algebra of labeled forests modulo h-equivalence. *Algebra and Logic*, 46, N 2 (2007), 120–133.

5 V. L. Selivanov. Hierarchies of $\mathbf{\Delta}^0_2$-measurable k-partitions. *Math. Logic Quarterly*, 53 (2007), 446–461.

6 V. L. Selivanov. Towards a descriptive theory of cb_0-spaces. Accepted for publication by *Mathematical Structures in Computer Science*, Arxive: 1406.3942v1.

7 K. Weihrauch. The degrees of discontinuity of some translators between representations of the real numbers. Technical Report TR-92-050, International Computer Science Institute, Berkeley, 1992.
8 K. Weihrauch. *Computable Analysis*. Springer Verlag, Berlin, 2000.

3.18 A simple conservation proof for ADS

Keita Yokoyama (JAIST – Ishikawa, JP)

It is known that the first-order part of infinite Ramsey's theorem can be approximated by a version of Paris/Harrington Principle. In this talk, I will give a simple proof of a partial conservation result for ADS based on this idea.

3.19 Evaluating separations in the Weihrauch lattice

Kazuto Yoshimura (JAIST – Ishikawa, JP)

This research aims to develop a method of evaluating separation results in the Weihrauch lattice. Two multi-valued functions, or their degrees, are said to be *separated* if and only if they are not Weihrauch equivalent, i.e. at least one direction of the mutual reducibilities fails. A number of separation results are already established by existing researches, though, the *strengths* of those separations have never been discussed.

Our proposal is to use a suitable ideal notion for evaluating the strengths of separations. Say a non-empty downward closed subset of the pointed Weihrauch lattice is a *stable ideal* if it is closed under the compositional product. Given a stable ideal $\mathcal{I}$ and two degrees $\mathcal{F}$ and $\mathcal{G}$, if we define $\mathcal{F} \leq_{\mathcal{I}} \mathcal{G}$ by the existence of an $I \in \mathcal{I}$ for which $\mathcal{F} \leq_W I \cdot \mathcal{G} \cdot I$, the relation $\leq_{\mathcal{I}}$ turns out to be a preorder. We shall then ask an appropriate $\mathcal{I}$, for separated degrees, such that they are still separated with respect to $\leq_{\mathcal{I}}$. The strength of the separation will approximately be evaluated by such an $\mathcal{I}$. In what follows we list some concrete examples of stable ideals.

The most primary example is given by *continuous degrees*. A continuous degree is the degree of a multi-valued function having a continuous choice function. The class of continuous degrees is indeed a stable ideal, and the induced partial order is characterized by the continuous Weihrauch reducibility.

Next let us introduce an ideal which captures the *rigidness* of the hierarchy of LLPO_n's [1]. A multi-valued function F is said to be *properly discontinuous* if its restriction to $\{\lim \alpha_i,\ \alpha_i \mid i \in \omega\}$ does not have a continuous choice function for some converging sequence $\{\alpha_i\}_{\alpha \in \omega}$ on $\mathrm{dom}(F)$ whose limit is still in $\mathrm{dom}(F)$, and to be *improperly discontinuous* otherwise. All LLPO_n's and LPO are properly discontinuous. Accordingly a degree is *proper* and *improper* in cases that its arbitrary representative is properly and improperly discontinuous, respectively. The class $\mathcal{L}$ of improper pointed degrees turns out to be a stable ideal while that of proper degrees is a filter of the Weihrauch lattice. If we say, given a reduction $\mathcal{F} \leq_W \mathcal{G}$, that $\mathcal{G}$ is *rigidly separated* from $\mathcal{F}$ in case $\mathcal{G} \leq_W \mathcal{G}/\mathcal{F}$, where $(-/-)$ is the

residual implication of the compositional product, then rigid separations never happen in above LPO since $\mathsf{LPO} \leq \mathcal{F}, \mathcal{G}$ implies $\mathcal{G}/\mathcal{F} \in \mathcal{L}$; while the following hierarchy can be shown via rigid separations.

$$\cdots <_{\mathcal{L}} \mathsf{LLPO}_{n+1} <_{\mathcal{L}} \mathsf{LLPO}_n <_{\mathcal{L}} \cdots <_{\mathcal{L}} \mathsf{LLPO}_2 <_{\mathcal{L}} \mathsf{LPO}$$

In particular LPO is the top with respect to $\leq_{\mathcal{L}}$. Hence the above *earliest* hierarchy found by K. Weihrauch in 1990s has a remarkable rigidness, which, for example, the classifications of closed choices (see [2]) do not have. We also remark to the fact that every improper degree is ω*-indiscriminative*. Hence for instance ω-indiscriminativeness of the *cohesiveness* COH is automatically derived from its implicational presentation $\mathsf{COH} \equiv_W \mathsf{WKL}'/\lim$ [1].

For further variations of stable ideals, let us consider on analogs of the big five systems in reverse mathematics [4]. As usual, we interpret a *conditional* Π^1_2*-formula*, i.e. a formula of the form $\varphi \equiv \forall X.(\varphi_0(X) \to \exists Y.\varphi_1(X,Y))$ where φ_0 and φ_1 are arithmetical, as the multi-valued function $\alpha \mapsto \{\beta \mid (\omega, \mathrm{Pow}(\omega)) \models \varphi_0(\alpha) \wedge \varphi_1(\alpha,\beta)\}$. If we say a multi-valued function F is a *uniformity* when $F[\alpha]$ contains an α-computable point for every $\alpha \in \mathrm{dom}(F)$, and say a degree is a uniformity degree when its arbitrary representative is a uniformity, then all conditional Π^1_2-theorems of RCA are interpreted as uniformities. Moreover the reducibility $\leq_{\mathcal{U}}$, where $\mathcal{U}$ is the stable ideal of pointed uniformity degrees, is characterized by computable reducibility proposed in [3]. It would not go too far to say that this ideal $\mathcal{U}$ is the most natural one among all thinkable analogs of RCA. Also etting $\mathcal{U}(\mathsf{WKL})$ and $\mathcal{U}(\lim)$ be the smallest stable ideals containing $\mathcal{U} \cup \{\mathsf{WKL}\}$ and $\mathcal{U} \cup \{\lim\}$, respectively, we obtain the similar *soundness* works for WKL and ACA. In particular $\mathcal{U}(\lim)$ can be obtained as the downward closure of $\{\lim^i \cdot \mathcal{F} \mid i \in \omega, \mathcal{F} \in \mathcal{U}\}$. As expected, the three ideals $\mathcal{U}$, $\mathcal{U}(\mathsf{WKL})$ and $\mathcal{U}(\lim)$ behaves as good *steps* for evaluating separation results.

It is very likely that natural analogs of ATR and Π^1_1-CA can also be found, according to the characterizations of their ω-models. However, on another front, most pre-known separations in the Weihrauch lattice do not have the strengths of above ATR, and the above three ideals suffice.

As future directions, we suggest the following three. Firstly it would be significant to have a general result which enable us to convert a separation to a stronger separation; namely a pair of a stable ideal $\mathcal{I}$, probably one of the above listed examples, and a mapping $(F,G) \mapsto (F_{\mathcal{I}}, G_{\mathcal{I}})$ such that $F \not\equiv_W G$ implies $F_{\mathcal{I}} \not\equiv_{\mathcal{I}} G_{\mathcal{I}}$. Secondly the *correctness* of the analogs for the big five systems should be concerned; in particular it is natural to ask if the provability of a conditional Π^1_2-sentence in $\mathrm{RCA}_{(0)}$ is equivalent to the condition that its interpretation is a uniformity in every model of $\mathrm{RCA}_{(0)}$. The similar questions should be asked for $\mathrm{WKL}_{(0)}$, $\mathrm{ACA}_{(0)}$ and possibly also for the rest two. Finally a deep result on the relationship of the induced reducibility $\leq_{\mathcal{U}}$ and the *computable entailment* (see [3]) is strongly desirable. Such a result would show a formal connection of reverse mathematics and the classification of Weihrauch degrees.

References

1 Vasco Brattka, Matthew Hendtlass and Alexander P. Kreuzer: On the Uniform Computational Content of Computability Theory. http://arxiv.org/abs/1501.00433 (2015)

2 Vasco Brattka, Matthew de Brecht and Arno Pauly: Closed choice and a Uniform Low Basis Theorem. Ann. Pure Appl. Logic. Vol.163(8): pp. 986–1008 (2012)

3 Denis R. Hirschfeldt and Carl G. Jockusch, Jr: On notions of computably theoretic reduction between Π^1_2-principles. to appear

4 Stephen G Simpson: Subsystems of second order arithmetic. Perspectives in Logic (2nd ed.). Cambridge University Press (2009)

3.20 Hyper-degrees of 2nd-order polynomial-time reductions

Martin Ziegler (KAIST – Daejeon, KR)

Ko, Friedman, and Kawamura et al. have shown common operators in analysis to map polynomial-time computable arguments to $\mathcal{NP}$-hard ones, thus gauging their non-uniform complexity. 2nd-order polynomial-time reductions compare the uniform computational complexity of operators in analysis, that is, functionals on Baire space $\mathbb{N}^{\mathbb{N}}$, respectively; cmp. [2]. They (have to) grant more runtime on 'long' arguments, expressed by 2nd-order polynomials, that is, terms $P(n, \mu)$ over $+, \cdot, 1$ and 1st and 2nd-order variables $n \in \mathbb{N}$ and $\mu \in \mathbb{N}^{\mathbb{N}}$, respectively; cmp. Mehlhorn (1976) – but are criticized for permitting, on arguments of exponential length, runtimes bounded by any constant-height exponential tower. We suggest a refined analysis in terms of the *hyper*degree of the 2nd-order polynomial bounds according to the following

▶ **Lemma 1.** *Let P denote a 2nd-order polynomial.*

(a) *For every integer d, $P(n, n \mapsto n^d)$ is an ordinary integer polynomial.*

(b) *The (thus well-defined) mapping $\mathbb{N} \ni d \mapsto \mathrm{DEG}\big(P\big)(d) := \deg\big(P(n, n \mapsto n^d)\big)$ is in turn an integer polynomial in d.*

(c) *For every fixed ordinary polynomial μ it holds $\deg(P(n, \mu)) = \mathrm{DEG}\big(P\big)(\deg \mu)$.*

(d) *It holds $\mathrm{DEG}\big(P(Q, \cdot)\big) = \mathrm{DEG}(P) \cdot \mathrm{DEG}(Q)$.*

(e) *It holds $\mathrm{DEG}\big(P(\cdot, Q)\big) = \mathrm{DEG}\big(P\big)\big(\mathrm{DEG}(Q)\big)$.*

(f) *The integer $\deg\big(\mathrm{DEG}(P)\big)$ coincides with the* depth *of P as defined in* [1].

In particular 2nd-order polynomials of hyperdegree one are closed under composition. This suggests to try to refine recent reductions [3, 6, 5].

References

1 B.M. Kapron, S. A. Cook. A New Characterization of Type-2 Feasibility. *SIAM Journal on Computing*, 25:1 (1996), 117–132.

2 A. Kawamura, S. A. Cook. Complexity theory for operators in analysis. *Proceedings of the 42nd ACM symposium on Theory of computing*, ACM STOC (2010), 495–502.

3 A. Kawamura, H. Ota, C. Rösnick, M. Ziegler. Computational Complexity of Smooth Differential Equations. *Logical Methods in Computer Science* 10:1 (2014).

4 A. Kawamura, A. Pauly. Function spaces for second-order polynomial time. *Proc. 10th Conf. on Computability in Europe* (2014), LNCS 8493, 245–254.

5 A. Kawamura, F. Steinberg, M. Ziegler. On the Computational Complexity of the Dirichlet Problem for Poisson's Equation. *Bulletin of Symbolic Logic* 20:2 (2014), p. 231; full version to appear in *Mathematical Structures in Computer Science*.

6 A. Pauly, M. Ziegler. Relative computability and uniform continuity of relations. *Logic and Analysis*, 5:7 (2013).

4 Open Problems

- **Question (Ackerman, Freer, Pauly, Roy).** "Does currying give rise to an interesting operator?"
  Suppose $f\colon X \times Y \to Z$ is such that for all x, the map $f(x, \cdot)\colon Y \to Z$ is continuous.
  One could instead consider the "curried" version $F\colon X \to \mathcal{C}(Y, Z)$, defined by $x \mapsto f(x, \cdot)$.

Clearly $f \leq_W F$. If $Y = \mathbb{N}$ then $F \leq_W \widehat{f}$. In general, can $f \mapsto F$ be seen as an interesting operator? What can one say about this map in general?
Background: For continuous f, the currying map is computable; see [8, Prop. 3, part 2]. In probability theory and elsewhere, often both the curried and uncurried functions are of interest; see, e.g., the discussion of disintegration and conditional distributions in [1, Def. 2.1].

- **Question (Brattka).** Does strong Weihrauch reducibility induce a lattice structure? It is clear that the sum operation induces an infimum and that the coproduct, which induces the supremum with respect to ordinary Weihrauch reducibility, does not yield a supremum for strong Weihrauch reducibility. But currently it is not known whether there is some other way to obtain a supremum for strong Weihrauch reducibility.
- **Question (Brattka).** How do different combinations of the stable version of Ramsey's Theorem for pairs and the cohesiveness problem compare to Ramsey's Theorem for pairs? We have

$$\mathrm{SRT}^2_2 \sqcup \mathrm{COH} \leq_{\mathrm{W}} \mathrm{SRT}^2_2 \times \mathrm{COH} \leq_{\mathrm{W}} \mathrm{SRT}^2_2 * \mathrm{COH}$$

and

$$\mathrm{SRT}^2_2 \sqcup \mathrm{COH} \leq_{\mathrm{W}} \mathrm{RT}^2_2 \leq_{\mathrm{W}} \mathrm{SRT}^2_2 * \mathrm{COH}.$$

What else can be said?
In an upcoming paper initiated during the seminar, Damir Dzhafarov, Denis Hirschfeldt and Ludovic Patey establish several negative results about some of the remaining reductions.

- **Problem (Fernandes, Ferreira and Ferreira [2])** Define a notion of integration within BTFA that works well for a sufficiently robust class of continuous functions (e.g., a class that contains many analytical functions).
- **Conjecture (Fernandes, Ferreira and Ferreira [2])** Show that over BTFA (and within the framework of [3]), Weierstrass approximation theorem is equivalent to the totality of the exponential function.
- **Question (Fouché).** Complexity of Fourier dimension: Write $M_+[0,1]$ for the Radon probability measures on the unit interval. An s-Fourier measure on the unit interval is a Radon measure μ such that its Fourier transform satisfies

$$|\hat{\mu}(\xi)|^2 \leq \frac{1}{(1+|\xi|)^s},$$

for all real ξ. Define

$$\mathrm{Fourm} :\subseteq \mathcal{A}[0,1] \times [0,1] \rightrightarrows M_+[0,1]$$

by

$$\mu \in \mathrm{Fourm}(A,s) \leftrightarrow \mu \text{ is an } s\text{-Fourier measure and } \mathrm{supp}\mu \subseteq A.$$

Determine the Weihrauch degree of Fourm.

- **Conjecture (Hölzl and Shafer [4]).** There exist universal tests $\mathcal{U}$ and $\mathcal{V}$ such that

$$\mathrm{RD}_{\mathcal{U}} \not\leq_{\mathrm{sW}} \mathrm{RD}_{\mathcal{V}}.$$

- **Question (Le Roux & Pauly [5])** Is there some $k \in \mathbb{N}$ such that $\mathrm{XC}_{[0,1]} \star \mathrm{XC}_{[0,1]} \leq_W \mathrm{XC}^k_{[0,1]}$?
Here $\mathrm{XC}_{[0,1]}$ is the restriction of closed choice on the unit interval to convex sets, i.e. intervals. $\star$ denotes the sequential composition of Weihrauch degrees.
After the seminar, this question has been answered in the negative by Takayuki Kihara.

- **Question (Marcone)** "What do the Weihrauch hierarchies look like once we go to very high levels of reverse mathematics strength?"
  So far the Weihrauch hierarchies have been used to obtain a finer picture of the relationships between statements that are provable in ACA_0. Yet the reverse mathematics picture of the relationships between mathematical statements goes well beyond ACA_0. Can we use the Weihrauch hierarchies to obtain information about the relationships between statements that are equivalent to ATR_0 or to Π^1_1-CA_0? One could start by looking at different forms of the perfect tree theorem.
- **Question (Pauly [7])** Is there some $k \in \mathbb{N}$ such that $\mathrm{AoUC}_{[0,1]} \star \mathrm{AoUC}_{[0,1]} \leq_W \mathrm{AoUC}^k_{[0,1]}$?
  Here $\mathrm{AoUC}_{[0,1]}$ is the restriction of closed choice on the unit interval to sets that are either the entire unit interval or singletons. $\star$ denotes the sequential composition of Weihrauch degrees.
  After the seminar, this question has been answered in the negative by Takayuki Kihara.
- **Question (Yokoyama)** For given a coloring $P : [\mathbb{N}]^2 \to 2$, a *grouping for* P is an infinite family of ω-large finite sets $\{F_0 < F_1 < \dots\}$ such that

$$\forall i_1 < \dots < i_n \, \exists c < k \, \forall x_1 \in F_{i_1}, \dots, \forall x_n \in F_{i_n} \, P(x_1, \dots, x_n) = c$$

  Now GP (grouping principle for ω-largeness) asserts that for any coloring $P : [\mathbb{N}]^2 \to 2$, there exists an infinite grouping for P. Then, what is the reverse mathematical strength of GP? Trivially, it is a consequence of RT^2_2.
  Ludovic Patey answered this question as follows. He showed that GP does not imply ADS, and it implies RRT^2_2. Also, he showed that there exists an ω-model of $\mathsf{RCA}_0 + \mathrm{SGP}$ with only low sets, where SGP is a grouping principle for stable colorings. The second result give a good information to calibrate the proof theoretic strength of RT^2_2. See [6].

References

1 Nathanael Ackerman, Cameron Freer, Daniel Roy. *On computability and disintegration*. arXiv 1509.02992v1, 2015.
2 António M. Fernandes, Fernando Ferreira, Gilda Ferreira. *Techniques in weak analysis for conservation results*. In P. Cégielski, C. Cornaros and C. Dimitracopoulos, editors, *New Studies in Weak Arithmetics*, volume 211 of *CSLI Lecture Notes*, pages 115–147. CSLI Publications and Presses universitaires du Pôle de Recherche et d'Enseignement Supérieur de Paris-Est, 2013.
3 António M. Fernandes and Fernando Ferreira. *Groundwork for weak analysis*. The Journal of Symbolic Logic, 67(2):557–578, 2002.
4 Rupert Hölzl, Paul Shafer. *Universality, optimality, and randomness deficiency*. Annals of Pure and Applied Logic, 166(10):1049–1069, Elsevier, 2015.
5 Stéphane Le Roux and Arno Pauly. Finite choice, convex choice and finding roots. *Logical Methods in Computer Science*, 2015.
6 Ludovic Patey and Keita Yokoyama, The strength of Ramsey's theorem for pairs and two colors, in preparation.
7 Arno Pauly. *Computable Metamathematics and its Application to Game Theory*. PhD thesis, University of Cambridge, 2012.
8 Arno Pauly. *On the topological aspects of the theory of represented spaces*. arXiv 1204.3763v3, 2015.

5 Bibliography on Weihrauch Complexity

For an always up-to-date version of this bibliography see

http://cca-net.de/publications/weibib.php

References

1 Nathanael L. Ackerman, Cameron E. Freer, and Daniel M. Roy. On computability and disintegration. *arXiv*, 1509.02992, 2015.
2 Vasco Brattka. *Grade der Nichtstetigkeit in der Analysis*. Fachbereich Informatik, FernUniversität Hagen, 1993. Diplomarbeit.
3 Vasco Brattka. Computable invariance. In Tao Jiang and D.T. Lee, editors, *Computing and Combinatorics*, volume 1276 of *Lecture Notes in Computer Science*, pages 146–155, Berlin, 1997. Springer. Third Annual Conference, COCOON'97, Shanghai, China, August 1997.
4 Vasco Brattka. Computable invariance. *Theoretical Computer Science*, 210:3–20, 1999.
5 Vasco Brattka. Effective Borel measurability and reducibility of functions. *Mathematical Logic Quarterly*, 51(1):19–44, 2005.
6 Vasco Brattka, Matthew de Brecht, and Arno Pauly. Closed choice and a uniform low basis theorem. *Annals of Pure and Applied Logic*, 163:986–1008, 2012.
7 Vasco Brattka and Guido Gherardi. Borel complexity of topological operations on computable metric spaces. *Journal of Logic and Computation*, 19(1):45–76, 2009.
8 Vasco Brattka and Guido Gherardi. Effective choice and boundedness principles in computable analysis. In Andrej Bauer, Peter Hertling, and Ker-I Ko, editors, *CCA 2009, Proceedings of the Sixth International Conference on Computability and Complexity in Analysis*, pages 95–106, Schloss Dagstuhl, Germany, 2009. Leibniz-Zentrum für Informatik.
9 Vasco Brattka and Guido Gherardi. Weihrauch degrees, omniscience principles and weak computability. In Andrej Bauer, Peter Hertling, and Ker-I Ko, editors, *CCA 2009, Proceedings of the Sixth International Conference on Computability and Complexity in Analysis*, pages 83–94, Schloss Dagstuhl, Germany, 2009. Leibniz-Zentrum für Informatik.
10 Vasco Brattka and Guido Gherardi. Effective choice and boundedness principles in computable analysis. *The Bulletin of Symbolic Logic*, 17(1):73–117, 2011.
11 Vasco Brattka and Guido Gherardi. Weihrauch degrees, omniscience principles and weak computability. *The Journal of Symbolic Logic*, 76(1):143–176, 2011.
12 Vasco Brattka, Guido Gherardi, and Rupert Hölzl. Las Vegas computability and algorithmic randomness. In Ernst W. Mayr and Nicolas Ollinger, editors, *32nd International Symposium on Theoretical Aspects of Computer Science (STACS 2015)*, volume 30 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 130–142, Dagstuhl, Germany, 2015. Schloss Dagstuhl–Leibniz-Zentrum für Informatik.
13 Vasco Brattka, Guido Gherardi, and Rupert Hölzl. Probabilistic computability and choice. *Information and Computation*, 242:249–286, 2015.
14 Vasco Brattka, Guido Gherardi, and Alberto Marcone. The Bolzano-Weierstrass theorem is the jump of weak Kőnig's lemma. *Annals of Pure and Applied Logic*, 163:623–655, 2012.
15 Vasco Brattka, Matthew Hendtlass, and Alexander P. Kreuzer. On the uniform computational content of computability theory. *arXiv*, 1501.00433, 2015.
16 Vasco Brattka, Matthew Hendtlass, and Alexander P. Kreuzer. On the uniform computational content of the Baire category theorem. *arXiv*, 1510.01913, 2015.
17 Vasco Brattka, Stéphane Le Roux, and Arno Pauly. Connected choice and the Brouwer fixed point theorem. *arXiv*, 1206.4809, June 2012.

18 Vasco Brattka, Stéphane Le Roux, and Arno Pauly. On the computational content of the Brouwer Fixed Point Theorem. In S. Barry Cooper, Anuj Dawar, and Benedikt Löwe, editors, *How the World Computes*, volume 7318 of *Lecture Notes in Computer Science*, pages 57–67, Berlin, 2012. Springer. Turing Centenary Conference and 8th Conference on Computability in Europe, CiE 2012, Cambridge, UK, June 2012.

19 Vasco Brattka and Arno Pauly. Computation with advice. In Xizhong Zheng and Ning Zhong, editors, *CCA 2010, Proceedings of the Seventh International Conference on Computability and Complexity in Analysis*, Electronic Proceedings in Theoretical Computer Science, pages 41–55, 2010.

20 Vasco Brattka and Arno Pauly. On the algebraic structure of Weihrauch degrees. *Unpublished draft*, 2014.

21 Vasco Brattka and Tahina Rakotoniaina. On the uniform computational content of Ramsey's theorem. *arXiv*, 1508.00471, 2015.

22 Raphaël Carroy. *Functions of the first Baire class.* PhD thesis, University of Lausanne and University Paris 7, 2013.

23 Raphaël Carroy. A quasi-order on continuous functions. *Journal of Symbolic Logic*, 78(2):663–648, 2013.

24 Matthew de Brecht. Levels of discontinuity, limit-computability, and jump operators. In Vasco Brattka, Hannes Diener, and Dieter Spreen, editors, *Logic, Computation, Hierarchies*, Ontos Mathematical Logic, pages 93–122. Walter de Gruyter, Boston, 2014.

25 François G. Dorais, Damir D. Dzhafarov, Jeffry L. Hirst, Joseph R. Mileti, and Paul Shafer. On uniform relationships between combinatorial problems. *Trans. Amer. Math. Soc.*, 368(2):1321–1359, 2016.

26 Damir D. Dzhafarov. Cohesive avoidance and strong reductions. *Proc. Amer. Math. Soc.*, 143(2):869–876, 2015.

27 Damir D. Dzhafarov. Strong reductions between combinatorial principles. *arXiv*, 1504.01405, 2015.

28 Makoto Fujiwara, Kojiro Higuchi, and Takayuki Kihara. On the strength of marriage theorems and uniformity. *Mathematical Logic Quarterly*, 60(3):136–153, 2014.

29 Guido Gherardi. An analysis of the lemmas of Urysohn and Urysohn-Tietze according to effective Borel measurability. In A. Beckmann, U. Berger, B. Löwe, and J.V. Tucker, editors, *Logical Approaches to Computational Barriers*, volume 3988 of *Lecture Notes in Computer Science*, pages 199–208, Berlin, 2006. Springer. Second Conference on Computability in Europe, CiE 2006, Swansea, UK, June 30-July 5, 2006.

30 Guido Gherardi. Effective Borel degrees of some topological functions. *Mathematical Logic Quarterly*, 52(6):625–642, 2006.

31 Guido Gherardi. *Some Results in Computable Analysis and Effective Borel Measurability.* PhD thesis, University of Siena, Department of Mathematics and Computer Science, Siena, 2006.

32 Guido Gherardi and Alberto Marcone. How incomputable is the separable Hahn-Banach theorem? In Vasco Brattka, Ruth Dillhage, Tanja Grubba, and Angela Klutsch, editors, *CCA 2008, Fifth International Conference on Computability and Complexity in Analysis*, volume 221 of *Electronic Notes in Theoretical Computer Science*, pages 85–102. Elsevier, 2008. CCA 2008, Fifth International Conference, Hagen, Germany, August 21–24, 2008.

33 Guido Gherardi and Alberto Marcone. How incomputable is the separable Hahn-Banach theorem? *Notre Dame Journal of Formal Logic*, 50(4):393–425, 2009.

34 Kirill Gura, Jeffry L. Hirst, and Carl Mummert. On the existence of a connected component of a graph. *Computability*, 4(2):103–117, 2015.

35 Peter Hertling. Stetige Reduzierbarkeit auf Σ^ω von Funktionen mit zweielementigem Bild und von zweistetigen Funktionen mit diskretem Bild. Informatik Berichte 153, FernUniversität Hagen, Hagen, December 1993.

36 Peter Hertling. A topological complexity hierarchy of functions with finite range. Technical Report 223, Centre de recerca matematica, Institut d'estudis catalans, Barcelona, Barcelona, October 1993. Workshop on Continuous Algorithms and Complexity, Barcelona, October, 1993.

37 Peter Hertling. Topologische Komplexitätsgrade von Funktionen mit endlichem Bild. Informatik Berichte 152, FernUniversität Hagen, Hagen, December 1993.

38 Peter Hertling. *Unstetigkeitsgrade von Funktionen in der effektiven Analysis*. PhD thesis, Fachbereich Informatik, FernUniversität Hagen, 1996.

39 Peter Hertling and Victor Selivanov. Complexity issues for preorders on finite labeled forests. In Benedikt Löwe, Dag Normann, Ivan Soskov, and Alexandra Soskova, editors, *Models of computation in context*, volume 6735 of *Lecture Notes in Computer Science*, pages 112–121, Heidelberg, 2011. Springer. 7th Conference on Computability in Europe, CiE 2011, Sofia, Bulgaria, June 27–July 2, 2011.

40 Peter Hertling and Victor Selivanov. Complexity issues for preorders on finite labeled forests. In Vasco Brattka, Hannes Diener, and Dieter Spreen, editors, *Logic, Computation, Hierarchies*, Ontos Mathematical Logic, pages 165–190. Walter de Gruyter, Boston, 2014.

41 Peter Hertling and Klaus Weihrauch. Levels of degeneracy and exact lower complexity bounds for geometric algorithms. In *Proceedings of the Sixth Canadian Conference on Computational Geometry*, pages 237–242, 1994. Saskatoon, Saskatchewan, August 2–6, 1994.

42 Peter Hertling and Klaus Weihrauch. On the topological classification of degeneracies. Informatik Berichte 154, FernUniversität Hagen, Hagen, February 1994.

43 Kojiro Higuchi. *Degree Structures of Mass Problems and Choice Functions*. PhD thesis, Mathematical Institute, Tohoku University, Sendai, Japan, January 2012.

44 Kojiro Higuchi and Takayuki Kihara. Inside the Muchnik degrees I: Discontinuity, learnability and constructivism. *Annals of Pure and Applied Logic*, 165(5):1058–1114, 2014.

45 Kojiro Higuchi and Takayuki Kihara. Inside the Muchnik degrees II: The degree structures induced by the arithmetical hierarchy of countably continuous functions. *Annals of Pure and Applied Logic*, 165(6):1201–1241, 2014.

46 Kojiro Higuchi and Arno Pauly. The degree structure of Weihrauch reducibility. *Log. Methods Comput. Sci.*, 9(2):2:02, 17, 2013.

47 Denis R. Hirschfeldt. *Slicing the Truth, On the Computable and Reverse Mathematics of Combinatorial Principles*, volume 28 of *Lecture Notes Series, Institute for Mathematical Sciences, National University of Singapore*. World Scientific, Singapore, 2015.

48 Denis R. Hirschfeldt and Carl G. Jockusch. On notions of computability theoretic reductions between Π^1_2 principles. *submitted*, 2015.

49 Rupert Hölzl and Paul Shafer. Universality, optimality, and randomness deficiency. *Annals of Pure and Applied Logic*, 166(10):1049–1069, 2015.

50 Mathieu Hoyrup, Cristóbal Rojas, and Klaus Weihrauch. Computability of the Radon-Nikodym derivative. In *Models of computation in context*, volume 6735 of *Lecture Notes in Comput. Sci.*, pages 132–141, Heidelberg, 2011. Springer.

51 Mathieu Hoyrup, Cristóbal Rojas, and Klaus Weihrauch. Computability of the Radon-Nikodym derivative. *Computability*, 1(1):3–13, 2012.

52 Akitoshi Kawamura. Lipschitz continuous ordinary differential equations are polynomial-space complete. In *24th Annual IEEE Conference on Computational Complexity*, pages 149–160. IEEE Computer Soc., Los Alamitos, CA, 2009.

53 Akitoshi Kawamura. Lipschitz continuous ordinary differential equations are polynomial-space complete. *Computational Complexity*, 19(2):305–332, 2010.

54 Akitoshi Kawamura and Stephen Cook. Complexity theory for operators in analysis. In *Proceedings of the 42nd ACM symposium on Theory of computing*, STOC '10, pages 495–502, New York, 2010. ACM.

55 Akitoshi Kawamura and Hiroyuki Ota. Small complexity classes for computable analysis. In *Mathematical foundations of computer science 2014. Part II*, volume 8635 of *Lecture Notes in Comput. Sci.*, pages 432–444. Springer, Heidelberg, 2014.

56 Akitoshi Kawamura, Hiroyuki Ota, Carsten Rösnick, and Martin Ziegler. Computational complexity of smooth differential equations. In *Mathematical foundations of computer science 2012*, volume 7464 of *Lecture Notes in Comput. Sci.*, pages 578–589. Springer, Heidelberg, 2012.

57 Akitoshi Kawamura, Hiroyuki Ota, Carsten Rösnick, and Martin Ziegler. Computational complexity of smooth differential equations. *Logical Methods in Computer Science*, 10:1:6,15, 2014.

58 Akitoshi Kawamura and Arno Pauly. Function spaces for second-order polynomial time. In *Language, life, limits*, volume 8493 of *Lecture Notes in Comput. Sci.*, pages 245–254. Springer, Cham, 2014.

59 Alexander P. Kreuzer. On the strength of weak compactness. *Computability*, 1(2):171–179, 2012.

60 Alexander P. Kreuzer. Bounded variation and the strength of Helly's selection theorem. *Logical Methods in Computer Science*, 10(4:16):1–23, 2014.

61 Alexander P. Kreuzer. From Bolzano-Weierstraß to Arzelà-Ascoli. *Mathematical Logic Quarterly*, 60(3):177–183, 2014.

62 Oleg V. Kudinov, Victor L. Selivanov, and Anton V. Zhukov. Undecidability in Weihrauch degrees. In Fernando Ferreira, Benedikt Löwe, Elvira Mayordomo, and Luís Mendes Gomes, editors, *Programs, Proofs, Processes*, volume 6158 of *Lecture Notes in Computer Science*, pages 256–265, Berlin, 2010. Springer. 6th Conference on Computability in Europe, CiE 2010, Ponta Delgada, Azores, Portugal, June/July 2010.

63 Stéphane Le Roux and Arno Pauly. Closed choice for finite and for convex sets. In Paola Bonizzoni, Vasco Brattka, and Benedikt Löwe, editors, *The Nature of Computation. Logic, Algorithms, Applications*, volume 7921 of *Lecture Notes in Computer Science*, pages 294–305, Berlin, 2013. Springer. 9th Conference on Computability in Europe, CiE 2013, Milan, Italy, July 1-5, 2013.

64 Stéphane Le Roux and Arno Pauly. Finite choice, convex choice and finding roots. *Logical Methods in Computer Science*, 11(4):4:6, 31, 2015.

65 Stéphane Le Roux and Arno Pauly. Weihrauch degrees of finding equilibria in sequential games (extended abstract). In Arnold Beckmann, Victor Mitrana, and Mariya Soskova, editors, *Evolving Computability*, volume 9136 of *Lecture Notes in Computer Science*, pages 246–257, Cham, 2015. Springer. 11th Conference on Computability in Europe, CiE 2015, Bucharest, Romania, June 29–July 3, 2015.

66 Uwe Mylatz. *Vergleich unstetiger Funktionen in der Analysis*. PhD thesis, Fachbereich Informatik, FernUniversität Hagen, 1992. Diplomarbeit.

67 Uwe Mylatz. *Vergleich unstetiger Funktionen: "Principle of Omniscience" und Vollständigkeit in der C–Hierarchie*. PhD thesis, Faculty for Mathematics and Computer Science, University Hagen, Hagen, Germany, 2006.

68 Eike Neumann. *Computational Problems in Metric Fixed Point Theory and their Weihrauch Degrees*. PhD thesis, Department of Mathematics, Universität Darmstadt, 2014. MSc thesis.

69 Eike Neumann. Computational problems in metric fixed point theory and their Weihrauch degrees. *arXiv*, 1506.05127, 2015.

70 Arno Pauly. *Methoden zum Vergleich der Unstetigkeit von Funktionen*. PhD thesis, FernUniversität Hagen, 2007. MSc thesis.

71 Arno Pauly. How discontinuous is computing Nash equilibria? (Extended abstract). In Andrej Bauer, Peter Hertling, and Ker-I Ko, editors, *6th International Conference on Computability and Complexity in Analysis (CCA'09)*, volume 11 of *OpenAccess Series in Informatics (OASIcs)*, Dagstuhl, Germany, 2009. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

72 Arno Pauly. How incomputable is finding Nash equilibria? *Journal of Universal Computer Science*, 16(18):2686–2710, 2010.

73 Arno Pauly. On the (semi)lattices induced by continuous reducibilities. *Mathematical Logic Quarterly*, 56(5):488–502, 2010.

74 Arno Pauly. *Computable Metamathematics and its Application to Game Theory*. PhD thesis, University of Cambridge, Computer Laboratory, Clare College, Cambridge, 2011.

75 Arno Pauly. Computability on the countable ordinals and the Hausdorff-Kuratowski theorem. *arXiv*, 1501.00386, 2015.

76 Arno Pauly. Many-one reductions and the category of multivalued functions. *Mathematical Structures in Computer Science*, 2015.

77 Arno Pauly, George Davie, and Willem Fouché. Weihrauch-completeness for layerwise computability. *arXiv*, 1505.02091, 2015.

78 Arno Pauly and Matthew de Brecht. Towards synthetic descriptive set theory: An instantiation with represented spaces. *arXiv*, 1307.1850, 2013.

79 Arno Pauly and Matthew de Brecht. Non-deterministic computation and the Jayne-Rogers theorem. In Benedikt Löwe and Glynn Winskel, editors, *Proceedings 8th International Workshop on Developments in Computational Models, DCM 2012, Cambridge, United Kingdom, 17 June 2012.*, volume 143 of *Electronic Proceedings in Theoretical Computer Science*, pages 87–96, 2014.

80 Arno Pauly and Matthew de Brecht. Descriptive set theory in the category of represented spaces. In *30th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*, pages 438–449, 2015.

81 Arno Pauly and Willem L. Fouché. How constructive is constructing measures? *arXiv*, 1409.3428, 2014.

82 Tahina Rakotoniaina. *On the Computational Strength of Ramsey's Theorem*. PhD thesis, Department of Mathematics and Applied Mathematics, University of Cape Town, Rondebosch, South Africa, 2015.

83 Victor Selivanov. Total representations. *Logical Methods in Computer Science*, 9:2:5, 30, 2013.

84 Thorsten von Stein. *Vergleich nicht konstruktiv lösbarer Probleme in der Analysis*. PhD thesis, Fachbereich Informatik, FernUniversität Hagen, 1989. Diplomarbeit.

85 Nazanin R. Tavana and Klaus Weihrauch. Turing machines on represented sets, a model of computation for analysis. *Log. Methods Comput. Sci.*, 7(2):2:19, 21, 2011.

86 Klaus Weihrauch. The degrees of discontinuity of some translators between representations of the real numbers. Technical Report TR-92-050, International Computer Science Institute, Berkeley, July 1992.

87 Klaus Weihrauch. The degrees of discontinuity of some translators between representations of the real numbers. Informatik Berichte 129, FernUniversität Hagen, Hagen, July 1992.

88 Klaus Weihrauch. The TTE-interpretation of three hierarchies of omniscience principles. Informatik Berichte 130, FernUniversität Hagen, Hagen, September 1992.

89 Klaus Weihrauch. *Computable Analysis*. Springer, Berlin, 2000.

Participants

- Vasco Brattka
Universität der Bundeswehr – München, DE
- Matthew de Brecht
NICT – Osaka, JP
- Damir D. Dzhafarov
University of Connecticut – Storrs, US
- Fernando Ferreira
University of Lisboa, PT
- Willem L. Fouché
UNISA – Pretoria, ZA
- Cameron Freer
MIT – Cambridge, US
- Guido Gherardi
Universität der Bundeswehr – München, DE
- Peter Hertling
Universität der Bundeswehr – München, DE
- Denis R. Hirschfeldt
University of Chicago, US
- Jeffry L. Hirst
Appalachian State University – Boone, US
- Rupert Hölzl
Universität Heidelberg, DE
- Hajime Ishihara
JAIST – Ishikawa, JP
- Akitoshi Kawamura
University of Tokyo, JP
- Takayuki Kihara
University of California – Berkeley, US
- Ulrich Kohlenbach
TU Darmstadt, DE
- Alexander P. Kreuzer
National Univ. of Singapore, SG
- Stéphane Le Roux
University of Brussels, BE
- Alberto Marcone
University of Udine, IT
- Kenshi Miyabe
Meiji University – Kawasaki, JP
- Antonio Montalbán
University of California – Berkeley, US
- Carl Mummert
Marshall University – Huntington, US
- Eike Neumann
Aston Univ. – Birmingham, GB
- Paulo Oliva
Queen Mary University of London, GB
- Ludovic Patey
University Paris-Diderot, FR
- Arno Pauly
University of Cambridge, GB
- Matthias Schröder
TU Darmstadt, DE
- Victor Selivanov
A. P. Ershov Institute – Novosibirsk, RU
- Paul Shafer
Ghent University, BE
- Dieter Spreen
Universität Siegen, DE
- Klaus Weihrauch
FernUniversität in Hagen, DE
- Keita Yokoyama
JAIST – Ishikawa, JP
- Kazuto Yoshimura
JAIST – Ishikawa, JP
- Martin Ziegler
KAIST – Daejeon, KR

Report from Dagstuhl Seminar 15401

Circuits, Logic and Games

Edited by

Mikołaj Bojańczyk[1], Meena Mahajan[2], Thomas Schwentick[3], and Heribert Vollmer[4]

1 **University of Warsaw, PL,** bojan@mimuw.edu.pl
2 **The Institute of Mathematical Sciences, IN,** meena@imsc.res.in
3 **TU Dortmund, DE,** thomas.schwentick@udo.edu
4 **Leibniz Universität Hannover, DE,** vollmer@thi.uni-hannover.de

Abstract

Over the years, there has been a lot of interplay between circuit complexity and logic. There are tight connections between small-depth circuit classes and fragments and extensions of first-order logic, and ideas from games and finite model theory have provided powerful lower bound techniques for circuits.

In recent years, there has been an impressive and sustained growth of interest and activity in the intersection of finite model theory and Boolean circuit complexity. The central aim of the seminar was to bring together researchers from these two areas to further strengthen the mutual fertilisation. The seminar focussed on the following specific topics:

- The algebraic approach to circuit complexity with its applications to finite model theory
- The logic-circuit connection, with a particular emphasis on circuit lower bounds that trigger results in finite model theory like separations between logics
- New connections between uniformity conditions on circuit families and logical predicates
- Structural complexity and circuit lower bounds inherently using methods from logic and algebra
- Proof systems with low circuit complexity
- Dynamic complexity: understanding the dynamic expressive power of small depth circuit classes

The seminar had 43 participants from 11 countries and was very successful with respect to the exchange of recent results, ideas and methodological approaches.

Seminar September 27 to October 2, 2015 – http://www.dagstuhl.de/15401
1998 ACM Subject Classification F.1.1 Models of Computation, F.1.3 Complexity Measures and Classes, F.2.2 Non-Numerical Algorithms and Problems, F.4.1 Mathematical Logic
Keywords and phrases computational complexity theory, finite model theory, Boolean circuits, regular languages, finite monoids, Ehrenfeucht-Fraïssé-games
Digital Object Identifier 10.4230/DagRep.5.9.105
Edited in cooperation with Nils Vortmeier

Circuits, Logic and Games, *Dagstuhl Reports*, Vol. 5, Issue 9, pp. 105–124
Editors: Mikołaj Bojańczyk, Meena Mahajan, Thomas Schwentick, and Heribert Vollmer

Dagstuhl Reports
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

1 Executive Summary

Mikołaj Bojańczyk
Meena Mahajan
Thomas Schwentick
Heribert Vollmer

This report documents the programme and outcomes of Dagstuhl Seminar 15401 "Circuits, Logic and Games". This seminar was the third in this series, the earlier two being Dagstuhl Seminars 06451 in November 2006 and 10061 in February 2010.

Goals of the Seminar

Over the years, there has been a lot of interplay between circuit complexity and logic. There are tight connections between small-depth circuit classes and fragments and extensions of first-order logic, and ideas from games and finite model theory have provided powerful lower bound techniques for circuits.

In recent years, there has been an impressive and sustained growth of interest and activity in the intersection of finite model theory and Boolean circuit complexity. The central aim of the seminar was to bring together researchers from these two areas to further strengthen the mutual fertilisation. Given the ubiquitousness of algebraic techniques in circuit complexity, the seminar also included arithmetic circuit complexity in its ambit.

The seminar focussed on the following specific topics:

- The algebraic approach to circuit complexity with its applications to finite model theory
- The logic-circuit connection, with a particular emphasis on circuit lower bounds that trigger results in finite model theory like separations between logics
- New connections between uniformity conditions on circuit families and logical predicates
- Structural complexity and circuit lower bounds inherently using methods from logic and algebra
- Proof systems with low circuit complexity
- Dynamic complexity: understanding the dynamic expressive power of small depth circuit classes

Organization of the Seminar and Activities

The seminar had the participation of 43 members from 11 countries.

The organisers attempted to create a schedule with a judicious mix of survey talks, focussed talks, and free time for unstructured discussions. Participants were invited to present their work and to communicate state-of-the-art advances. Since the participants came from diverse communities, the organisers invited some of them to give long survey-style talks in specific sub-areas. There were five such talks, listed below.

1. Olaf Beyersdorff. Lower bounds: from circuits to QBF proof systems.
   This talk surveyed the relatively new area of proof systems for establishing falseness of fully quantified Boolean formulas. It demonstrated techniques by which lower bounds in ciruit complexity can be tranferred to lower bounds on the sizes of such proofs.

2. Thomas Colcombet. Combinatorial Expressions and Lower Bounds.
   This talk described an elegant formalism, combinatorial expressions, that captures bounded depth circuits manipulating infinite data in specified restrictive ways, and showed how one may obtain indefinability results in this model.
3. Anuj Dawar. Lower Bounds for Symmetric Circuits.
   This talk described the recently formalised circuit model of symmetric circuits, its connections with logical definability, and a lower bound technique using games.
4. Martin Grohe. Color Refinement: A Simple Partitioning Algorithm with Applications From Graph Isomorphism Testing to Machine Learning.
   This talk described exciting connections between higher-dimensional generalisations of the extremely simple colour refinement aglorithm and a linear programming approach to testing isomorphism.
5. Nutan Limaye. Arithmetic Circuit Lower Bounds.
   This talk surveyed the recent explosion of results concerning size lower bounds in restricted models of algebraic computation, using techniques which seem essentially combinatorial in nature.

In addition, 20 other participants gave short talks on some of their recent work relevant to the seminar theme. These talks covered results in two-variable first-order logic; dynamic complexity; graph colouring; database theory; circuit lower bounds; logics on words; and semigroup techniques. There was also a short session on Thursday devoted to discussing interesting open problems.

Concluding Remarks and Future Plans

The organizers regard the seminar as being quite successful. Most participants felt that they learnt new things from other areas, and were hopeful of using such ideas to make progress in their own research areas.

One aspect noted by the organizers was that a lot of the work discussed at the seminar used techniques from algebra. In fact, there was even a suggestion that if there is a future seminar in this series, it could be called “Circuits, Logic, and Algebra” instead of “Circuits, Logic, and Games”.

The organizers are grateful to the Scientific Directorate of the Center for its support of this seminar.

2 Table of Contents

3 Overview of Talks

3.1 Crane Beach conjecture and modulo counting quantifiers

Sreejith Ajithkumar (University of Paris VII, FR)

Joint work of Krebs, Andreas; Sreejith, A. V.
Main reference Andreas Krebs, A. V. Sreejith: Non-definability of Languages by Generalized First-order Formulas over (N, +). LICS 2012: 451-460
URL http://dx.doi.org/10.1109/LICS.2012.55

We show that the crane beach conjecture holds for first order logic with modulo counting quantifiers (or group quantifiers) in the presence of less than and addition relation.

3.2 Limitations of Algebraic Approaches to Graph Isomorphism Testing

Christoph Berkholz (HU Berlin, DE)

Joint work of Berkholz, Christoph; Grohe, Martin
Main reference C. Berkholz, M. Grohe, "Limitations of Algebraic Approaches to Graph Isomorphism Testing," in Proc. of the 42nd Int'l Colloquium on Automata, Languages and Programming (ICALP'15), pp. 451–460, IEEE, 2015.
URL http://dx.doi.org/10.1007/978-3-662-47672-7_13

We investigate the power of graph isomorphism algorithms based on algebraic reasoning techniques like Gröbner basis computation. The idea of these algorithms is to encode two graphs into a system of multivariate polynomial equations that is satisfiable if and only if the graphs are isomorphic, and then to (try to) decide satisfiability of the system using, for example, the Gröbner basis algorithm. In some cases this can be done in polynomial time, in particular, if the equations admit a bounded degree refutation in an algebraic proof systems such as Nullstellensatz or polynomial calculus.

We show that the strength of this algebraic approach is closely related to the Weisfeiler-Lehman algorithm or, equivalently, to the equivalence problem for the k-variable fragment of first-order counting logic. This shows that logical methods can be used to understand the strength of algebraic approaches for graph isomorphism testing, complementing previous connections of logic and linear programming approaches.

3.3 Lower bounds: from circuits to QBF proof systems

Olaf Beyersdorff (University of Leeds, GB)

Joint work of Beyersdorff, Olaf; Bonacina, Ilario; Chew, Leroy
Main reference O. Beyersdorff, I. Bonacina, L. Chew, "Lower bounds: from circuits to QBF proof systems," in Proc. of the 7th ACM Conf. on Innovations in Theoretical Computer Science (ITCS'16)), pp. 249–260, ACM, 2016; pre-print available ECCC TR15-133, 2015.
URL http://dx.doi.org/10.1145/2840728.2840740
URL http://eccc.hpi-web.de/report/2015/133

The main aim in proof complexity is to understand the complexity of theorem proving. Arguably, what is even more important is to establish techniques for lower bounds, and

the recent history of computational complexity speaks volumes on how difficult it is to develop general lower bound techniques. Understanding the size of proofs is important for at least two reasons. The first is its tight relation to the separation of complexity classes: NP vs. coNP for propositional proofs, and NP vs. PSPACE in the case of proof systems for quantified boolean formulas (QBF). The second reason to study lower bounds for proofs is the analysis of SAT and QBF solvers: powerful algorithms that efficiently solve the classically hard problems of SAT and QBF for large classes of practically relevant formulas.

In this talk we give an overview of the relatively young field of QBF proof complexity. We explain the main resolution-based proof systems for QBF, modelling CDCL and expansion-based solving. In the main part of the talk we will give an overview of current lower bound techniques (and their limitations) for QBF systems. In particular, we exhibit a new and elegant proof technique for showing lower bounds in QBF proof systems based on strategy extraction. This technique provides a direct transfer of circuit lower bounds to lengths of proofs lower bounds.

By using the full spectrum of state-of-the-art circuit lower bounds, our new lower bound method leads to very strong lower bounds for QBF Frege systems:

1. exponential lower bounds and separations for $\mathrm{AC}^0[p]$-Frege+$\forall$red for all primes p;
2. an exponential separation of $\mathrm{AC}^0[p]$-Frege+$\forall$red from TC^0-Frege+$\forall$red;
3. an exponential separation of the hierarchy of constant-depth systems AC^0_d-Frege+$\forall$red by formulas of depth independent of d.

In the propositional case, all these results correspond to major open problems.

3.4 Transductions: From circuits to continuity

Michaël Cadilhac (Universität Tübingen, DE)

Joint work of Cadilhac, Michaël; Krebs, Andreas; Ludwig, Michael; Paperman, Charles
Main reference M. Cadilhac, A. Krebs, M. Ludwig, C. Paperman, "A Circuit Complexity Approach to Transductions," in Proc. of the 40th Int'l Symp. on Mathematical Foundations of Computer Science (MFCS'15), LNCS, Vol. 9234, pp. 141–153, Springer, 2015.
URL http://dx.doi.org/10.1007/978-3-662-48057-1_11

Low circuit complexity classes and regular languages exhibit very tight interactions that shade light on their respective expressiveness. We propose to study these interactions at a functional level, by investigating the deterministic rational transductions computable by constant-depth, polysize circuits. To this end, a circuit framework of independent interest that allows variable output length is introduced. Relying on it, there is a general characterization of the set of transductions realizable by circuits. It is then decidable whether a transduction is definable in AC^0 and, assuming a well-established conjecture, the same for ACC^0. This study unveils a crucial property of the functions at hand: the preservation under inverse image of classes of languages. More precisely, with C a class of languages, a function f is C-continuous if every language of C is mapped by f^{-1} to another language in C. In this talk, an emphasis is put on the pervasiveness of this notion, and the key problems that arise, in particular deciding C-continuity of deterministic transductions.

3.5 Combinatorial Expressions and Lower Bounds

Thomas Colcombet (CNRS / University Paris-Diderot, FR)

Joint work of Colcombet, Thomas; Manuel, Amaldev

In this talk, I present a new paradigm, combinatorial expressions, for computing functions expressing properties over an infinite domain. The main result is a generic technique, for showing indefinability of certain functions by the expressions. It is based the Hales-Jewett theorem, from Ramsey theory. I also show how this formalims is a conveninent tool for separating logics over data words.

These results are based on a joint works with Amaldev Manuel, and received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 259454.

References

1 Thomas Colcombet and Amaldev Manuel. *Fragments of Fixpoint Logic on Data Words*. FSTTCS 2015, pp. 98–111, http://dx.doi.org/10.4230/LIPIcs.FSTTCS.2015.98.
2 Thomas Colcombet and Amaldev Manuel. *Combinatorial Expressions and Lower Bounds*. STACS 2015, pp. 249–261, http://dx.doi.org/10.4230/LIPIcs.STACS.2015.249.

3.6 Model checking distributed algorithms against propositional dynamic logic with data

Aiswarya Cyriac (Uppsala University, SE)

Joint work of Aiswarya, C.; Bollig, Benedikt; Gastin, Paul
Main reference C. Aiswarya, B. Bollig P. Gastin, "An Automata-Theoretic Approach to the Verification of Distributed Algorithms," in Proc. of the 26th Int'l Conf. on Concurrency Theory (CONCUR'15), LIPIcs, Vol. 42, pp. 340–353, Schloss Dagstuhl, 2015.
URL http://dx.doi.org/10.4230/LIPIcs.CONCUR.2015.340

In a distributed algorithm, an arbitrary number of processes cooperate to achieve a common goal (e.g., elect a leader). Processes have unique identifiers (pids) from an infinite, totally ordered domain. An algorithm proceeds in synchronous rounds, each round allowing a process to perform a bounded sequence of actions such as send or receive a pid, store it in some register, and compare register contents wrt. the associated total order. An algorithm is supposed to be correct independently of the number of processes. We introduce a logic to specify correctness of distributed algorithms. This logic is inspired by data logics, and can reason about processes and pids. The model checking problem is undecidable in general; we will see some ideas to regain decidability for distributed algorithms over ring topologies. Since the verification of distributed algorithms is undecidable, we propose an underapproximation technique, which bounds the number of rounds. This is an appealing approach, as the number of rounds needed by a distributed algorithm to conclude is often exponentially smaller than the number of processes. We show that round-bounded verification of distributed algorithms over rings is PSPACE-complete.

3.7 Lower Bounds for Symmetric Circuits

Anuj Dawar (University of Cambridge, GB)

Joint work of Anderson, Matthew; Dawar, Anuj
Main reference M. Anderson, A. Dawar, "On Symmetric Circuits and Fixed-Point Logics," in Proc. of the 31st Int'l Symp. on Theoretical Aspects of Computer Science (STACS'14), LIPIcs, Vol. 25, pp. 41–52, Schloss Dagstuhl, 2014.
URL http://dx.doi.org/10.4230/LIPIcs.STACS.2014.41

Symmetric Circuits provide a natural model for studying the complexity of problems on graphs and similar relational structures. Recent work by Anderson and Dawar establishes a close link between families of symmetric circuits and definability in fixed-point logics. This link can be used to show lower bounds on families of symmetric circuits, using methods from finite model theory. In this talk, we show how this can be done, without reference to logical definability by combining the support theorem of Anderson-Dawar with the bijection games of Hella.

3.8 Canonizing Graphs of Bounded Tree Width in Logspace

Michael Elberfeld (RWTH Aachen, DE)

Joint work of Elberfeld, Michael; Schweitzer, Pascal
Main reference M. Elberfeld, P. Schweitzer, "Canonizing Graphs of Bounded Tree Width in Logspace," arXiv:1506.07810v1 [cs.CC], 2015.
URL http://arxiv.org/abs/1506.07810v1

Graph canonization is the problem of computing a unique representative, a canon, from the isomorphism class of a given graph. This implies that two graphs are isomorphic exactly if their canons are equal. We show that graphs of bounded tree width can be canonized by logarithmic-space (logspace) algorithms. This implies that the isomorphism problem for graphs of bounded tree width can be decided in logspace. In the light of isomorphism for trees being hard for the complexity class logspace, this makes the ubiquitous class of graphs of bounded tree width one of the few classes of graphs for which the complexity of the isomorphism problem has been exactly determined.

3.9 Colour Refinement: A Simple Partitioning Algorithm with Applications From Graph Isomorphism Testing to Machine Learning

Martin Grohe (RWTH Aachen, DE)

Colour refinement is a simple algorithm that partitions the vertices of a graph according their "iterated degree sequences". It has very efficient implementations, running in quasilinear time, and a surprisingly wide range of applications. The algorithm has been designed in the context of graph isomorphism testing, and it is used as important subroutine in almost all

practical graph isomorphism tools. Somewhat surprisingly, other applications in machine learning, probabilistic inference, and linear programming have surfaced recently.

In my talk, I introduce the basic algorithm as well as higher dimensional extensions known as the k-dimensional Weisfeiler-Lehman algorithm. Then I discuss an unexpected connection between colour refinement and a natural linear programming approach to graph isomorphism testing and an application of colour refinement as a pre-processing routine for linear progarmming.

3.10 Bipartite Matching is in Quasi-NC

Rohit Gurjar (Universität Ulm, DE)

The bipartite matching problem is known to be in P but not in NC. However, it has a randomized NC algorithm using the famous isolation lemma of Mulmuley, Vazirani and Vazirani, 1987. The isolation lemma states that assigning random weights (polynomially bounded) to the edges of a graph ensures that there is a unique minimum weight perfect matching with a good probability. Derandomizing the isolation lemma, that is constructing such a weight assignment deterministically, would give an NC algorithm for matching. We make a step towards this. We construct such a weight assignment for bipartite graphs with quasi-polynomially bounded weights. This implies that bipartite matching is in Quasi-NC (circuits with polylog depth and quasi-poly size).

3.11 Backdoors into Two Occurrences

Jan Johannsen (LMU München, DE)

Backdoor sets for the class CNF(2) of CNF-formulas in which every variable has at most two occurrences are studied in terms of parameterized complexity. The question whether there exist a CNF(2)-backdoor set size k is hard for the class W[2], for both weak and strong backdoors, and in both cases it becomes fixed-parameter tractable when restricted to inputs in d-CNF for a fixed d. Besides that, upper bounds in the W-hierarchy are given for a problem related to the existence of weak backdoor sets, for CNF(2) and other tractable cases of SAT. These imply the first W[2]-completeness results for the problem of finding weak backdoor sets for any tractable cases.

3.12 Quantifying over tuples with Algebra – the multidimensional blockproduct

Klaus-Jörn Lange (Universität Tübingen, DE)

The close connections between polynomially sized circuits of constant depth and first-order logic have been mirrored by algebraic constructions using the blockproduct. This algebraic view had been restricted up to now by only allowing for unary quantifiers using single variables. In this talk the multidimensional blockproduct is introduced which provides a way for the algebraic simulation of first-order quantifiers over tuples of variables.

3.13 Arithmetic circuit complexity and lower bounds

Nutan Limaye (Indian Institute of Technology – Mumbai, IN)

In this talk we will start with a brief introduction to the area of arithmetic circuit complexity. We will then discuss the history of the field and motivation behind some of the important questions being studied in this area.

We will then closely look at the frontier of the current knowledge and discuss some interesting open problems. If time permits, we will discuss some of the recent results.

3.14 Unary temporal and two-variable FO logic with threshold

Kamal Lodaya (The Institute of Mathematical Sciences, IN)

Joint work of Krebs, Andreas; Lodaya, Kamal; Pandya, Paritosh; Straubing, Howard

On words, two-variable logic $\mathrm{FO}^2[<]$ is well mapped out (Schutzenberger, Therien-Wilke, Etessami-Vardi-Wilke, Schwentick-Therien-Vollmer, Lodaya-Pandya-Shah). Its quantifier structure has also been recently studied (Kufleitner-Weil, Krebs-Straubing). Extensions $\mathrm{FO}^2[\mathrm{Num}]$, $\mathrm{FO}^2[\mathrm{Reg}]$ and $\mathrm{Maj}^2[<]$, the last one going out of first order logic, were studied in the complexity context (Koucky-Pudlak-Therien, Behle-Krebs-Refferscheid).

At the level of alphabet letters we look at an extension $\mathrm{FO}^2[<,\mathrm{Th}]$ with binary predicates $a(x,y)$ which stand for the letter a occurring during the "open" interval (x,y) (Pratt, Segerberg). Alternately we can think of a subalphabet B occurring invariantly during the interval (Manna-Moszkowski).

The definable languages include dot depth two and the logic can define several standard languages above $\mathrm{FO}^2[<]$ which occur in the literature, for example $c^*(ac^*bc^*)^*$, for which it is open whether they can be defined in AC^0 circuits with a linear number of gates. As far as we are aware this is the smallest logic which can express these languages. In fact the logic intersects every level of the until and dot depth hierarchies.

So the question of interest is, where is this logic placed?

3.15 QBF Resolution: How important is width?

Meena Mahajan (The Institute of Mathematical Sciences, IN)

Joint work of Beyersdorff, Olaf; Chew, Leroy; Mahajan, Meena; Shukla, Anil
Main reference O. Beyersdorff,L. Chew, M. Mahajan, A. Shukla, "Are Short Proofs Narrow? QBF Resolution is not Simple," ECCC TR15-152, 2015.
URL http://eccc.hpi-web.de/report/2015/152/

One of the main techniques for proving size and space lower bounds in classical resolution proceeds via width: the results of Ben-Sasson and Wigderson (JACM 2001) and of Atserias and Dalmau (JCSS 2008) show that lower bounds on width imply lower bounds on size and space respectively. We assess the effectiveness of such a technique for the QRes system (used to prove QBFs false). We show through a series of examples that

1. The size-width and space-width relations fail to hold in QRes.
   However the failure is due to wide clauses with many universal variables. So we define existential-width (e-width), counting only the number of existential variables in a clause.
2. The tree-size-vs-e-width and tree-space-vs-e-width relations fail to hold in QRes.
3. The size-vs-e-width relation also fails to hold in QRes.
   Examples 2 and 3 have poly-size proofs but need linear e-width.
4. The QParity formula needs exponential-size proofs, and independently, needs linear e-width.

We also provide a direct and efficient (in size, space and e-width) simulation of tree-like QRes proofs by tree-like proofs in the expansion-based system ∀Exp+Res. Further, we show that the expansion-based systems ∀Exp+Res and IR-calc, provably separate in general, have the same power when restricted to tree-like proofs.

3.16 A Strongly Exponential Separation of DNNFs from CNF Formulas

Stefan Mengel (Artois University – Lens, FR)

Joint work of Bova, Simone; Capelli, Florent; Mengel, Stefan; Slivovsky, Friedrich
Main reference S. Bova, F. Capelli, S. Mengel, F. Slivovsky, "A Strongly Exponential Separation of DNNFs from CNF Formulas," arXiv:1411.1995v3 [cs.CC], 2015.
URL http://arxiv.org/abs/1411.1995v3

Decomposable Negation Normal Forms (DNNFs) are Boolean circuits in negation normal form where the subcircuits leading into each AND gate are defined on disjoint sets of variables. We prove a strongly exponential lower bound on the size of DNNFs for a class of CNF formulas built from expander graphs. As a corollary, we obtain a strongly exponential separation between DNNFs and CNF formulas in prime implicates form. This settles an open problem in the area of knowledge compilation (Darwiche and Marquis, 2002).

3.17 Dynamic Complexity of Reachability and Related Problems

Anish Mukherjee (Chennai Mathematical Institute, IN)

Joint work of Datta, Samir; Kulkarni, Raghav; Mukherjee, Anish; Schwentick, Thomas; Zeume, Thomas
Main reference S. Datta, R. Kulkarni, A. Mukherjee, T. Schwentick, T. Zeume, "Reachability is in DynFO," in Proc. of the 42nd International Colloquium on Automata, Languages, and Programming (ICALP'15) – Part 2, LNCS, Vol. 9135, pp. 159–170, Springer, 2015; pre-print available as arXiv:1502.07467v2 [cs.LO], 2015.
URL http://arxiv.org/abs/1502.07467

In most real-life databases data changes frequently and thus makes efficient query answering challenging. Auxiliary data might help to avoid computing query answers from scratch all the time. One way to study this incremental maintenance scenario is from the perspective of dynamic algorithms with the goal of reducing (re-)computation time. Another option is to investigate it from the perspective of low-level parallel computational complexity.

As the "lowest" complexity class AC^0 (with a suitable uniformity condition) and the core of the standard database query language SQL both coincide with first-order predicate logic, one naturally arrives at the question which queries can be maintained dynamically with first-order predicate logic (DynFO). The dynamic complexity framework introduced by Patnaik and Immerman models this setting.

Very recently we have shown that the Reachability query can be maintained in DynFO, confirming a two decade old conjecture of Patnaik and Immerman. After surveying previous known upper bounds for the Reachability query and related problems briefly, I will present the main ideas of the proof of this result.

The talk is based on joint work with Samir Datta, Raghav Kulkarni, Thomas Schwentick and Thomas Zeume.

3.18 Word transducers: from 2-way to 1-way

Anca Muscholl (University of Bordeaux, FR)

Joint work of Baschenis, Felix; Gauwin, Olivier; Muscholl, Anca; Puppis, Gabriele
Main reference F. Baschenis, O. Gauwin, A. Muscholl, G. Puppis, "One-way Definability of Sweeping Transducer.," in Proc. of the 35th IARCS Annual Conf. on Foundation of Software Technology and Theoretical Computer Science (FSTTCS'15), LIPIcs, Vol. 45, pp. 178–191, Schloss Dagstuhl, 2015.
URL http://dx.doi.org/10.4230/LIPIcs.FSTTCS.2015.178

Two-way finite-state transducers on words are strictly more expressive than one-way transducers. It has been shown recently how to decide if a two-way functional transducer has an equivalent one-way transducer, but the complexity of the algorithm is non-elementary. We propose an alternative and simpler characterization for sweeping functional transducers, namely, for transducers that can only reverse their head direction at the extremities of the input. Our algorithm works in 2ExpSpace and, in the positive case, produces an equivalent one-way transducer of doubly exponential size. We also show that the bound on the size of the transducer is tight, and that the one-way definability problem is undecidable for (sweeping) non-functional transducers.

3.19 Finite-Degree Predicates and Two-Variable First-Order Logic

Charles Paperman (University of Warsaw, PL)

Main reference C. Paperman, "Finite-Degree Predicates and Two-Variable First-Order Logic," in Proc. of the 24th EACSL Annual Conf. on Computer Science Logic (CSL'15), LIPIcs, Vol. 41, pp. 616–630, Schloss Dagstuhl, 2015.
URL http://dx.doi.org/10.4230/LIPIcs.CSL.2015.616

We consider two-variable first-order logic on finite words with a fixed number of quantifier alternations. In this talk, we will present results about definability of languages with a neutral letter definable using the order and finite-degree predicates. From these results we derive the strictness of the alternation hierarchy of two-variable logic over this signature as well as a "uniform" lower bounds for the function of addition.

3.20 AC^0 and first order logic, a new approach based on ultrafilters on words

Jean-Eric Pin (University of Paris VII, FR)

Joint work of Gehrke, Mai; Krebs, Andreas; Pin, Jean-Eric
Main reference M. Gehrke, A. Krebs, J.-E. Pin, "Ultrafilters on words for a fragment of logic," Theoretical Computer Science, Vol. 610, Part A, pp. 37–58, 2016.
URL http://dx.doi.org/10.1016/j.tcs.2015.08.007

We give a method for specifying ultrafilter equations and identify their projections on the set of profinite words. Let B be the set of languages captured by first-order sentences using unary predicates for each letter, arbitrary uniform unary numerical predicates and a predicate for the length of a word. We illustrate our methods by giving ultrafilter equations characterising B and then projecting these to obtain profinite equations characterising $B \cap \mathrm{Reg}$. This suffices to establish the decidability of the membership problem for $B \cap \mathrm{Reg}$.

3.21 An exponential lower bound for the sum of products of read once formulas

B. V. Raghavendra Rao (Indian Institute of Techology – Madras, IN)

Joint work of Ramya, C.; Rao, B. V. Raghavendra

Read once arithmetic formulas are formulas where every variable is read at most once. We study limitations of polynomials computed by depth two circuits built over read-once formulas of unbounded depth where the total leaf fan-in for + gates is sub- linear. We prove an exponential lower bound on the size of depth-2 arithmetic circuits with sub- linear product fan-in built over ROPs computing the permanent. Our results demonstrate a class of formulas of unbounded depth with exponential size lower bound against the permanent and can be seen as an exponential improvement over the multilinear formula size lower bounds given by Raz [2] for a sub-class of multilinear and non-multilinear formulas. Our proof techniques are

built on the one developed by Raz [2] and later extended by Kumar et al. [1]. Our proofs exploit the structural weakness of CF-ROPs against random partitions

This is a joint work with C. Ramya.

References

1 Mrinal Kumar, Gaurav Maheshwari, and Jayalal Sarma. *Arithmetic circuit lower bounds via MaxRank*. In Automata, Languages, and Programming – 40th International Colloquium, ICALP 2013, Riga, Latvia, July 8-12, 2013, Proceedings, Part I, pages 661–672, 2013.

2 Ran Raz. *Multi-linear formulas for permanent and determinant are of super-polynomial size*. In Proceedings of the 36th Annual ACM Symposium on Theory of Computing, Chicago, IL, USA, June 13-16, 2004, pages 633–641, 2004.

3.22 On the generalised colouring numbers of graphs that exclude a fixed minor

Sebastian Siebertz (TU Berlin, DE)

Joint work of van den Heuvel, Jan; Ossona de Mendez, Patrice; Rabinovich, Roman; Siebertz, Sebastian
Main reference J. van den Heuvel, P. Ossona de Mendez, R. Rabinovich, S. Siebertz, "On the generalised colouring numbers of graphs that exclude a fixed minor," Electronic Notes in Discrete Mathematics, Vol. 49, pp. 523–530, 2015.
URL http://dx.doi.org/10.1016/j.endm.2015.06.072
URL http://eurocomb2015.b.uib.no/files/2015/08/endm1950.pdf

The colouring number $\mathrm{col}(G)$ of a graph G is the minimum integer k such that there exists a linear ordering of the vertices of G in which each vertex v has back-degree at most k, i.e., v has at most k neighbours u with $u < v$. The colouring number is a structural measure that measures the edge density of subgraphs of G. For $r \geq 1$, the numbers $\mathrm{col}_r(G)$ and $\mathrm{wcol}_r(G)$ generalise the colouring number, where $\mathrm{col}_1(G)$ and $\mathrm{wcol}_1(G)$ are equivalent to $\mathrm{col}(G)$. For increasing values of r these measures converge to the well-known structural measures tree-width and tree-depth. For an n-vertex graph, $\mathrm{col}_n(G)$ is equal to the tree-width of G and $\mathrm{wcol}_n(G)$ is equal to the tree-depth of G.

We show that if G excludes K_t as a minor, then $\mathrm{col}_r(G) \leq 3\binom{t-1}{2} \cdot (2r+1)$ and $\mathrm{wcol}_r(G) \leq (r+1)^{3\binom{t-1}{2}} \cdot (2r+1)$. These results improve earlier results published in [1].

References

1 Jan van den Heuvel, and Patrice Ossona de Mendez, and Roman Rabinovich, and Sebastian Siebertz *On the generalised colouring numbers of graphs that exclude a fixed minor*. Electronic Notes in Discrete Mathematics, 2015

3.23 Converse elimination in the algebra of binary relations

Dimitri Surinx (Hasselt University – Diepenbeek, BE)

Joint work of Surinx, Dimitri; Fletcher, George H. L.; Gyssens, Marc; Leinders, Dirk; Van den Bussche, Jan; Van Gucht, Dirk; Wu, Yuqing
Main reference D. Surinx, G. H. L. Fletcher, M. Gyssens, D. Leinders, J. Van den Bussche, D. Van Gucht, S. Vansummeren, Y. Wu, "Relative expressive power of navigational query on graphs using transitive closure," Logic Journal of the IGPL, 23(5):759–788, 2015.
URL http://dx.doi.org/10.1093/jigpal/jzv028

The algebra of binary relations has a long history, going back to Peirce and Schröder, and was greatly developed by Tarski and his collaborators. The simplest language has only the two operators union and composition, together with the identity relation. We can enrich this basic algebra by adding any of the following operators: converse; intersection; set difference; projection; coprojection; transitive closure; and the diversity relation. Boolean queries on relational structures are expressed in terms of the nonemptiness of an algebraic expression. The algebra without intersection, difference and transitive closure, but with projection, admits converse elimination: every expressible boolean query can already be expressed without using the converse operator. We show an exponential lower bound on the degree of the converse-free expression. Furthermore, we show that converse elimination fails in the presence of transitive closure.

3.24 Static Analysis for Logic-Based Dynamic Programs

Nils Vortmeier (TU Dortmund, DE)

Joint work of Schwentick, Thomas; Vortmeier, Nils; Zeume, Thomas
Main reference T. Schwentick, N. Vortmeier, T. Zeume, "Static Analysis for Logic-based Dynamic Programs," in Proc. of the 24th EACSL Annual Conf. on Computer Science Logic (CSL'15), LIPIcs, Vol. 41, pp. 308–324, Schloss Dagstuhl, 2015.
URL http://dx.doi.org/10.4230/LIPIcs.CSL.2015.308

A dynamic program, as introduced by Patnaik and Immerman (1994), maintains the result of a fixed query for an input database which is subject to tuple insertions and deletions. It can use an auxiliary database whose relations are updated via first-order formulas upon modifications of the input database.

This talk discusses static analysis problems for dynamic programs and investigates, more specifically, the decidability of the following three questions. Is the answer relation of a given dynamic program always empty? Does a program actually maintain a query? Is the content of auxiliary relations independent of the modification sequence that lead to an input database?

In general, all these problems can easily be seen to be undecidable for full first-order programs. Therefore we aim at pinpointing the exact decidability borderline for programs.

3.25 Small Dynamic Complexity Classes

Thomas Zeume (TU Dortmund, DE)

Joint work of Datta, Samir; Kulkarni, Raghav; Anish, Mukherjee; Schwentick, Thomas; Zeume, Thomas

In modern data management scenarios, data is subject to frequent changes. In order to avoid costly re-computations from scratch after each small update, one can try to (re-)use auxiliary data structures that have been already computed before to keep the information about the data up-to-date. However, the auxiliary data structures need to be updated dynamically whenever the data changes.

The descriptive dynamic complexity framework (short: dynamic complexity) introduced by Patnaik and Immerman models this setting. It was mainly inspired by relational databases. For a relational database subject to change, auxiliary relations are maintained with the intention to help answering a query Q. When an update to the database, i.e. an insertion or a deletion of a tuple, occurs, every auxiliary relation is updated through a first-order query that can refer to the database as well as to the auxiliary relations.

In this talk I introduced the dynamic complexity framework and discussed recent work on understanding the limits of expressive power of small dynamic complexity classes.

References

1 Samir Datta, Raghav Kulkarni, Anish Mukherjee, Thomas Schwentick, and Thomas Zeume. *Reachability is in DynFO*. ICALP 2015. Springer, 2015.
2 Thomas Zeume and Thomas Schwentick. *Dynamic conjunctive queries*. Proc. 17th International Conference on Database Theory (ICDT) 2014. OpenProceedings.org, 2014.
3 Thomas Zeume and Thomas Schwentick. *On the quantifier-free dynamic complexity of reachability*. Inf. Comput., 240:108-129, 2015.

4 Open Problems

4.1 Perfect matchings for grid graphs and AC^0

Kristoffer Arnsfelt Hansen (Aarhus University, DK)

The width w and length ℓ *full grid* is the graph with vertices $\{(i,j) \mid i \in \{1,\ldots,\ell\}, j \in \{1,\ldots,w\}\}$ and edges between vertices (i,j) and (i',j') whenever $|i-i'|+|j-j'|=1$. A width w and length ℓ *grid graph* G is simply a subgraph of the width w and length ℓ full grid. In [1] it was shown that deciding whether a perfect matching exists for *constant width* grid graphs can be decided in ACC^0. We will now describe an open question originating from that paper, although not appearing there explicitly. Resolving the question in the positive would imply improving the ACC^0 bound to AC^0.

Let G be a width w length ℓ grid graph where ℓ is odd. The left-end vertices $L(G)$ is the set of vertices of G of the form $(1,j)$ and similarly the right-end vertices $R(G)$ is the set of vertices of G of the form $\ell, j)$. If $L(G) = R(G)$ we can form the width w infinite grid graph G^∞ by an infinite concatenation of G identifying the left-end and right-end vertices of consecutive copies of G.

Assume now that G^∞ has a perfect matching M. Let M' be the perfect matching in G^∞ obtained from M by shifting it by one length of G to the right. We can now ask the question: Is it the case that a graph of the form $M \cup M'$ can never have an infinite path?

References

1 Kristoffer Arnsfelt Hansen, Balagopal Komarath, Jayalal Sarma, Sven Skyum and Navid Talebanfard: *Circuit Complexity of Properties of Graphs with Constant Planar Cutwidth*. MFCS 2014:336–347.

4.2 AC^0 on trees

Mikołaj Bojańczyk (University of Warsaw, PL)

Normally, AC^0 circuits are indexed by lengths of their input. A family of circuits is then viewed as a set of words of arbitrary lengths, and the logical complexity of such word languages can then be studied. In my open problem, I propose to index circuits by unlabelled binary trees (other ideas, like unranked trees or maybe even graphs could also make sense). If the index of a circuit is a tree t, then each gate represents a node of t, and therefore a valuation of the gates represents a labelling of the tree with the alphabet $\{0, 1\}$. A family of circuits, indexed by all possible finite unlabelled binary trees, defines a language of trees labelled by $\{0, 1\}$. The question is: which languages of finite binary trees labelled by $\{0, 1\}$ are simultaneously regular and can be defined in AC^0? One conjecture is that these are exactly those languages which can be defined in first-order logic with the following predicates:

- $0(x)$, which says that position x has label 0;
- $x < y$, which says that y is a descendant of x;
- $\varphi(x)$ for every mso formula φ which only uses the left and right child predicates, and which cannot talk about labels.

This conjecture would be a natural generalisation of a characterisation for finite words, where the logic has modular predicates instead of the mso formulas, as shown in [1].

References

1 David A. Mix Barrington, Kevin J. Compton, Howard Straubing, Denis Thérien: *Regular Languages in NC^1*. J. Comput. Syst. Sci. 44(3):478–499 (1992)

4.3 Prefix diversity

Michaël Cadilhac (Universität Tübingen, DE)

Let L be a language over Σ. Its *prefix diversity* is the function $\mathsf{pd}_L \colon \mathbb{N} \to \mathbb{N}$ defined by:

$$\mathsf{pd}_L(n) = \max_{v_1,\dots,v_n \in \Sigma^*} |\{(v_1 v, v_2 v, \dots, v_n v) \mid v \in \Sigma^*\}| \ .$$

In words, for a given n, this is the maximum different number of behaviors one obtains by reading a word v in n different quotients of L.

This notion was used in different terms by Paz [1] and Turakainen [2] in link with probabilistic automata. They show in particular that any so-called $\mathbb{Q}$-stochastic language has a prefix diversity bounded by a polynomial.

Open questions: What is the entire class of languages of poly-bounded prefix diversity? Same question with linear? How does it relate to other notions, such as subword complexity?

References

1 Azaria Paz. *Introduction to probabilistic automata*. Academic Press, 1971.
2 Paavo Turakainen. *On nonstochastic languages and homomorphic images of stochastic languages*. Information Sciences, 24(3):229–253, 1981.

4.4 Proof systems computed by NC^0 circuit families.

Karteek Sreenivasaiah (MPI für Informatik – Saarbrücken, DE)

Main reference K. Sreenivasaiah, "On verifying proofs in constant depth, and polynomial identity testing," Ph. D. Thesis, Institute of Mathematical Sciences (IMSc), India, 2014.
URL http://www.imsc.res.in/xmlui/handle/123456789/361

A computable function f is called a proof system for a language L if and only if $\text{Range}(f) = L$. We study proof systems computable by NC^0 circuit families. A circuit family $\{C_n\}$ is in NC^0 if C_n has bounded fanin gates and constant depth. We say such a family computes a proof system for L if $\text{Range}(C_n) = L \cap \{0,1\}^n$.

The main goal of this line of work is to characterize languages that have proof systems computable in NC^0. However, a list of realistic goals are as follows:

- Characterize regular languages that have NC^0 computable proof systems.
- Does the language of all directed graphs on n vertices with a path from vertex 0 to vertex n have an NC^0 proof system?

All related results and open problems can be found in the PhD Thesis available here: http://www.imsc.res.in/xmlui/handle/123456789/361.

Participants

- Sreejith Ajithkumar
University of Paris VII, FR
- Christoph Berkholz
HU Berlin, DE
- Olaf Beyersdorff
University of Leeds, GB
- Mikołaj Bojańczyk
University of Warsaw, PL
- Michaël Cadilhac
Universität Tübingen, DE
- Thomas Colcombet
CNRS / University Paris-Diderot, FR
- Aiswarya Cyriac
Uppsala University, SE
- Samir Datta
Chennai Mathematical Inst., IN
- Anuj Dawar
University of Cambridge, GB
- Michael Elberfeld
RWTH Aachen, DE
- Martin Grohe
RWTH Aachen, DE
- Rohit Gurjar
Universität Ulm, DE
- Anselm Haak
Leibniz Univ. Hannover, DE
- Kristoffer Arnsfelt Hansen
Aarhus University, DK
- Jan Johannsen
LMU München, DE
- Juha Kontinen
University of Helsinki, FI
- Andreas Krebs
Universität Tübingen, DE
- Klaus-Jörn Lange
Universität Tübingen, DE
- Nutan Limaye
Indian Institute of Technology – Mumbai, IN
- Kamal Lodaya
The Institute of Mathematical Sciences, IN
- Meena Mahajan
The Institute of Mathematical Sciences, IN
- Pierre McKenzie
University of Montréal, CA
- Arne Meier
Leibniz Univ. Hannover, DE
- Stefan Mengel
Artois University – Lens, FR
- David A. Mix Barrington
University of Massachusetts – Amherst, US
- Anish Mukherjee
Chennai Mathematical Inst., IN
- Anca Muscholl
University of Bordeaux, FR
- Charles Paperman
University of Warsaw, PL
- Jean-Eric Pin
University of Paris VII, FR
- B. V. Raghavendra Rao
Indian Institute of Techology – Madras, IN
- Thomas Schwentick
TU Dortmund, DE
- Luc Segoufin
ENS – Cachan, FR
- Sebastian Siebertz
TU Berlin, DE
- Karteek Sreenivasaiah
MPI für Informatik – Saarbrücken, DE
- Howard Straubing
Boston College, US
- Dimitri Surinx
Hasselt Univ. – Diepenbeek, BE
- Thomas Thierauf
Hochschule Aalen, DE
- Jacobo Torán
Universität Ulm, DE
- Jan Van den Bussche
Hasselt Univ. – Diepenbeek, BE
- Jonni Virtema
Leibniz Univ. – Hannover
- Heribert Vollmer
Leibniz Univ. Hannover, DE
- Nils Vortmeier
TU Dortmund, DE
- Thomas Zeume
TU Dortmund, DE

Report from Dagstuhl Seminar 15402

Self-assembly and Self-organization in Computer Science and Biology

Edited by

Vincent Danos[1] and Heinz Koeppl[2]

1 University of Edinburgh, GB, `vdanos@inf.ed.ac.uk`
2 TU Darmstadt, DE, `heinz.koeppl@bcs.tu-darmstadt.de`

Abstract

This report documents the program and the outcomes of Dagstuhl Seminar 15402 "Self-assembly and Self-organization in Computer Science and Biology". With the trend of technological systems to become more distributed they tend to resemble closer biological systems. Biological systems on all scale are distributed and most often operate without central coordination. Taking the morphogenesis as an example, it is clear that the complexity and precision of distributed mechanisms in biology supersedes our current design attempts to distributed systems. The seminar assembled together researchers from computer science, engineering, physics and molecular biology working on the problem of decentralized coordination of distributed systems. Within every domain different terms have been coined, different analysis methods have been developed and applied and the seminar aims to foster the exchange of methods and the instantiation and alignment of important problem statements that can span across the disciplines. A representative example for a problem that is studied across domains through different methods is self-assembly. For example, computer scientists consider abstract self-assembly models such as Wang tiles to bound shape complexities while polymer physicists and biologists use molecular dynamics simulations to characterize self-assembly by means of energy and entropy. Because of its well-definedness, we deliberately placed emphasis on self-assembly that is otherwise entailed in the more general term self-organization. Within the domain of self-organization various research threads were represented at the seminar and a certain convergence of underlying concepts was possible. The seminar helped to exchange techniques from different domains and to agree on certain problem statements for future collaborations.

Seminar September 27 to October 2, 2015 – http://www.dagstuhl.de/15402
1998 ACM Subject Classification F.1.2 Modes of Computation, F.3.2 Semantics of Programming Languages, G.1.2 Approximation, G.2.2 Graph Theory, I.6.1 Simulation Theory
Keywords and phrases Self-assembly, molecular modeling, molecular dynamics, graph-rewriting grammars, self-organization, self-* systems, concurrency
Digital Object Identifier 10.4230/DagRep.5.9.125

1 Executive Summary

Heinz Koeppl

The Seminar brought together researchers from molecular biology, molecular modeling and theoretical computer scientists with interest in formal models of molecular computation and self-organization. Molecular biology provides a rich substrate to implement molecular computation and complex self-assembly algorithms. The Seminar featured several talks

Self-assembly and Self-organization in Computer Science and Biology, *Dagstuhl Reports*, Vol. 5, Issue 9, pp. 125–138
Editors: Vincent Danos and Heinz Koeppl
Dagstuhl Reports
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

on DNA-assembly systems, that to-date represents the most advanced molecular substrate for self-assembly. The increase in the achieveable complexity of such molecular structures asks for a formal description and analysis of those systems using methods from theoretical computer science. The Seminar was successful in identifying common problem statements and in establishing a common scientific language. Apart from self-assembly, the broader term self-organization was mostly represented by research on swarming or self-propelled particle (SPP) models. The common feature of SPP systems and self-assembly is the emergence of global structures through local interaction rules (self-assembled structure vs swarms or flocks). One contribution also featured the combination of swarming and self-assembly system in terms of nucleation studies. Moreover, novel methodological overlap between simulation algorithms for molecular self-assembly and simulation algorithms for SPP systems were identified and elaborated during the workshop.

The seminar was structured as a regular workshop with morning and afternoon sessions but plenty of time was allocated for discussions after each talk. For the first such Dagstuhl Seminar no working groups were defined. For follow-up Seminars on the same topic we aim to additionally define working groups that may also deliver preliminary research results and initiation of new collaborations.

Although the workshop was very interdisciplinary we were able to arrange the presentations into sessions of a coherent theme. The feedback of participants was extremely positive, stating that they could really profit from the technical discussions that accompanied every presentation and that were performed in the free time. Correspondingly, several new collaborations across disciplines were initiated at the seminar.

2 Table of Contents

3 Overview of Talks

3.1 Engineering Self-Organization: From Networking to Synthetic Biology

Jacob Beal (BBN Technologies – Cambridge, US)

Emerging methods for aggregate programming can greatly simplify the engineering of complex self-organizing systems. The foundation of this approach is field calculus, which provides guaranteed local-to-global mapping and encapsulation of distributed processes. Building on this foundation, composable "building block" algorithms provide resilience guarantees, and are then packaged into accessible APIs that can make the engineering of complex self-organizing systems are simple as the engineering of single-machine programs.These methods are already being applied into electronic networked systems. In order to effectively engineer complex self-organization behaviors with biological organisms, however, the performance and predictability of cellular information processing must be improved. Toward this end, I will review key recent advances in the enabling technologies of biological design automation, CRISPR-based repressor families, and device modeling based on calibrated flow cytometry.

3.2 Self-Organized Actin Patterns in Motile Amoeboid Cells

Carsten Beta (Universität Potsdam, DE)

Joint work of Beta, Carsten; Gerhardt, Matthias; Nagel, Oliver; Walz, Michael; Ecke, Mary; Stengl, Andreas; Gerisch, Günther
Main reference M. Gerhardt, M. Ecke, M. Walz, A. Stengl, C. Beta, G. Gerisch, "Actin and PIP3 waves in giant cells reveal the inherent length scale of an excited state'', Journal of Cell Science, Vol. 127, pp. 4507–4517, 2014.
URL http://dx.doi.org/10.1242/jcs.156000
Main reference M. Gerhardt, M. Walz, C. Beta, "Signaling in chemotactic amoebae remains spatially confined to stimulated membrane regions," Journal of Cell Science, Vol. 127, pp. 5115–5125, 2014.
URL http://dx.doi.org/10.1242/jcs.161133

Numerous cellular functions like cell motility, phagocytosis, and division depend on the coordinated formation of functional cytoskeletal structures that exhibit characteristic length and time scales. Here, we focus on self-organized wave patterns that emerge in the substrate-attached actin cortex of motile cells of the social amoeba Dictyostelium discoideum. We use electric pulse-induced cell fusion to generate giant polynuclear Dictyostelium cells that allow us to observe the wave patterns in a large spatially extended actin cortex, independent of confinement due to limited cell size. We found that waves consist of a PIP3-rich band enclosed by an actin-rich border, i.e., they are composite structures involving both the actin cortex and the composition of the adjacent membrane. They travel across the substrate-attached membrane with a constant speed and display a self-organized width on the order of m that remains constant independent of the cell size. Also the formation of rotating spiral waves was observed. Upon head-on collision, they mutually annihilate and, thus, show all the typical properties of an excitable system. To investigate whether localized receptor stimuli can induce the spreading of excitable waves, we delivered spatially confined stimuli of the chemoattractant cAMP to the cell membrane. To generate localized cAMP stimuli, either

particles coated with covalently bound cAMP molecules were brought into contact with the cell membrane or a patch of the membrane was aspirated into a glass micropipette to shield this patch against freely diffusing cAMP molecules in the surrounding medium. By imaging the spatiotemporal dynamics of fluorescent markers for PIP3, PTEN and filamentous actin, we observed that the signaling activity remained spatially confined to the stimulated membrane region. Neighboring parts of the membrane that were not exposed to cAMP did not show any sign of excitation, i.e., no receptor-initiated spatial spreading of excitation waves was observed. Finally, we showed data on the transport of micron-sized objects by Dictyostelium cells, demonstrating that motile amoeboid cells can function as small trucks that transport micro-cargo to a desired location.

3.3 Optimizing the Assembly of Stacked Rings

Koan Briggs (University of Kansas, US)

Joint work of Briggs, Koan; Deeds, Eric

Many macromolecular machines inside the cell exhibit a stacked ring architecture, with multiple uniform-length rings of protein subunits bound to one another. The majority of these machines must adopt their fully assembled quaternary structure in order to function, making the assembly process vital for cellular function and survival. The assembly of protein complexes containing stable substructures has been shown to suffer from a type of kinetic trapping that we term assembly deadlock, which occurs when smaller intermediates are exhausted from the system before all of the fully functional structures have formed. Deadlock can result in plateaus in the assembly dynamics, leading to delays in reaching maximum complex assembly and a reduced final complex concentration. While these plateaus have been extensively studied for simple rings, the effect of assembly deadlock on more general structures like stacked rings remains to be fully investigated. In this work, we focused on the case of a stacked homotrimer; this structure contains both three- and four-member rings as substructures, but is simple enough to allow for extensive investigation. Our mathematical models revealed that this structure could suffer from extreme deadlock that significantly reduces the efficiency of assembly. Using a computationally efficient deterministic simulation approach, we exhaustively analyzed the parameter space of self-assembly for this case, and found that the number and duration of plateaus in the assembly dynamics depended strongly on the pattern of affinities in this structure. Since these complexes are generally only functional when fully assembled, we hypothesized that existing stacked ring architectures would evolve to utilize the most efficient assembly pathways predicted by our models. Analysis of interfaces in solved crystal structures of stacked homotrimers confirmed this prediction. Our findings have important implications for understanding how assembly dynamics have influenced the structural evolution of large macromolecular machines.

3.4 Swarming Models with Repulsive-Attractive Effects

Jose Antonio Carillo (Imperial College London, GB)

I gave an overview of the different levels of description of collective behaviormodels highlighting some of the interesting mathematical open problems in thesubject. Calculus of variations, dynamical systems, mean-field limits for PDEs, kinetic and aggregation-diffusion equations naturally show up as necessary tools to solve some of these questions.

3.5 Three-Dimensional Swarming States Induced by Hydrodynamic Interactions

Maria Rita D'Orsogna (California State University – Northridge, US)

Swarming patterns arising from self-propelled particles have been extensively studied,particularly in two-dimensions and in the absence of an embedding medium. We consider the dynamics of more realistic three dimensional self-propelled particles interacting in a fluid medium. The fluid interaction terms generated by direct short-ranged pairwise interactions may impart much longer-ranged hydrodynamic forces, eff ectively amplifying the coupling between individuals. We consider two limiting cases of fluid interactions, a "clear fluid" where particles have direct knowledge of their own velocity, that of others and of the fluid, and an "opaque fluid" where particles are able to determine their velocity only in relation to the surrounding fluid flow. We discuss emergent patterns that are unstable in fluid-free environments and that become stabilized by opaque fluid couplings such as rotating mills.

3.6 If I had a Hammer ...

Hanno Hildmann (NEC Laboratories Europe – Heidelberg, DE)

My talk is about the proverbial hammer with which one would like to address allproverbial nails, and specifically and in the context of this seminar, about the nature inspired mechanisms used to design self-organization into the solutions we have worked on at NEC and at BT's EBTIC. I will talk about a variety of projects which have all been approached with ai few different techniques. I will also discuss these techniques and highlight their common elements as well as the parts in which they differ. The "if" part of the title refers to the fact that the aim of this seminar is to discuss a variety of techniques and that I am interested to engage in a discussion with the other participants about other / new techniques I could learn.

3.7 Porphyrins, Pyrazinacenes and Oxoporphyrinogens: Supramolecular (and other) Effects

Jonathan P. Hill (National Institute for Materials Science – Ibaraki, JP)

Self-assembly of molecules implies intermolecular processes that can involvehydrogen bonding, van der Waals interactions (e. g. pi-pi stacking),amphiphilicity, coordination chemistry and combinations of these. Here, we willdiscuss assembly processes of porphyrins, pyrazinacenes and oxoporphyrinogens(amongst others) including how their structures affect the final self-assembly form and any dynamic processes occurring in the structures. These includeinvestigations of supramolecular activity at surfaces and in solutions. Forinstance, charge transfer within a supramolecular manifold, surface assembly ofporphyrin trimers and chiral processes at surfaces and in solution will bepresented.

3.8 Statistical Inference of Cellular Behaviour from Heterogeneous Single-Cell Data

Heinz Koeppl (TU Darmstadt, DE)

Modeling and inferring stochastic biomolecular processes based on single-cell data requires an extension of the traditional Markov chain description to account for the random molecular environment into which the process of interest is embedded. In particular, we seek an isolated process model that behaves as if the process was still embedded into the molecular environment. Based on that novel process model we develop a Bayesian inference framework that resorts to traditional MCMC schemes in combination with sequential Monte Carlo techniques. We apply the framework to live-cell imaging data of a inducible gene expression system in budding yeast and show that it allows to separate intrinsic from extrinsic noise components from single measurements without the need for dedicated dual-color constructs.

3.9 Self-propelled Chimeras

Nikita Kruk (TU Darmstadt, DE)

Joint work of Kruk, Nikita; Maistrenko, Yuri; Wenzel, Nicolas; Koeppl, Heinz
Main reference N. Kruk, Y. Maistrenko, N. Wenzel, H. Koeppl, "Self-propelled Chimeras," arXiv:1511.04738v1 [nlin.AO], 2015.
URL http://arxiv.org/abs/1511.04738v1

The appearance of chimera states in a minimal extension of the classical Vicsek model for collective motion of self-propelled particle systems is presented. Inspired by earlier works on chimera states in the Kuramoto model, a phase lag parameter in the particle alignment dynamics is introduced. Compared to the oscillatory networks with fixed site positions, the self-propelled particle systems can give rise to distinct forms of chimeras resembling moving flocks through an incoherent surrounding, for which their parameter domains are

characterized. More specifically, localized directional one-headed and multi-headed chimera states, as well as scattered directional chimeras without space localization are detected. Canonical generalizations of the elementary Vicsek model are discussed and chimera states for them indicating the universality of this novel behavior are shown. A continuum limit of the particle system is derived that preserves the chimeric behavior.

3.10 Principles of Protein Self-Assembly in the Cell

Emmanuel Levy (Weizmann Institute of Science – Rehovot, IL)

A single yeast cell is a few microns in diameter and yet contains about a hundred million proteins. Interactions between these proteins are crucial for the self-organization of the cell and its ability to perform cellular functions. While much information exists on the identity of protein interactions and complexes, little is known about their higher-order organization in living cells. We will present work that aims to better understand this high-order organization. First, we will describe a strategy that we have been developing to probe the local environment of proteins in cells (functional interactions). Second, we will present an analysis where we assess the potential of single point mutations to trigger unwanted interactions, leading to uncontrolled protein super-assembly (dysfunctional interactions). Finally, we will present a minimal protein system that we engineered to model and better understand principles protein self-assembly at the micron scale.

3.11 Chimera State: A Novel Paradigm of Nonlinear Science

Yuri Maistrenko (National Academy of Sciences of Ukraine – Kiev, UA)

Joint work of Larger, L.; Penkovsky, B.; Sudakov, O.; Osiv, O.; Maistrenko, V.
Main reference L. Larger, B. Penkovsky, Y. Maistrenko, "Laser chimeras as a paradigm for multistable patterns in complex systems," Nature Communications, Vol. 6, Article No. 7752, 2015.
URL http://dx.doi.org/10.1038/ncomms8752
Main reference Y. Maistrenko, O. Sudakov, O. Osiv, V. Maistrenko, "Chimera states in three dimensions," New Journal of Physics, Vol. 17, 073037, 2015.
URL http://dx.doi.org/10.1088/1367-2630/17/7/073037

Chimera is a rich class of self-organized solutions developed spontaneously in high dimensional networks with non-local and symmetry breaking coupling features, in which synchronous and asynchronous oscillations co-exist. Its accurate understanding is expected to bring important insight in many complex spatiotemporal phenomena, from living and mechanical systems to optics and turbulence. Chimera state was discovered in 2002 by Kuramoto and Battogtock for the complex Ginzburg-Landau equation and its phase approximation, the Kuramoto model. Currently, this is an area of intense theoretical and experimental research, for now, chimeras have been found in many systems from various fields.In the lecture, different aspects of chimera state in one-, two- and three-dimensions have been discussed. The main attention was paid on a highly controllable experiment based on optoelectronic delayed feedback applied to a wavelength tunable semiconductor laser and modelled by a modified Ikeda equation. For the system, a wide variety of chimera patterns of different modality is found and interpreted.

The model simulations generate behavior in an excellent qualitative agreement with that exhibited in the experiment. The presentation is illustrated by 3-Dim videos of the complex spatiotemporal chimera dynamics.

3.12 Cell-Free Transcription-Translation: From Gene Circuits to Self-Assembly in a Test Tube

Vincent Noireaux (University of Minnesota – Minneapolis, US)

Joint work of Noireaux, Vincent; Shin, Jonghyeon; Caschera, Filippo
Main reference J. Shin, V. Noireaux, "An E. coli Cell-Free Expression Toolbox: Application to Synthetic Gene Circuits and Artificial Cells," ACS Synthetic Biology, 1(1):29–53, 2012.
URL http://dx.doi.org/10.1021/sb200016s

Cell-free transcription-translation (TX-TL) systems are becoming powerful platforms to construct biochemical systems in vitro through the expression of synthetic gene circuits. In the past decade, considerable efforts have been made to expand the capabilities of those systems.My lab has worked on expanding the transcription repertoire of cell-free expression systems, traditionally based on the T7 RNA polymerase and promoter, to go beyond just in vitro protein production. We developed an all E. coli platform so as to use 10s or 100s of regulatory parts for the construction, execution and characterization of gene circuits outside living cells in either test tube reactions, microfluidics or liposomes. New metabolisms energize gene expression for 8-10 hours to reconstruct complex active biological systems. For example, the phages T7 and phix174 are synthesized in cell-free TX-TL reactions from their genomes. Both phages serve as model systems to study the relationship information to self-assembly. Encapsulated inside cell-sized phospholipid liposomes, the cell-free TX-TL system is used to construct a minimal cell using a bottom-up approach. I will present this cell-free synthetic biology platform and our last experiments.

3.13 Theoretical Modeling of Algorithmic Self-Assembling Systems

Matthew J. Patitz (University of Arkansas – Fayetteville, US)

An introduction to tile-based algorithmic self-assembly will be presented, starting with Winfree's abstract Tile Assembly Model (aTAM). A series of aTAM results are surveyed, followed by a description of derivative models, such as the 2-Handed Assembly Model, along with related results. Special emphasis is given to results relating to computational universality and intrinsic universality.

3.14 DNA-Based Programmable Molecular Devices

John H. Reif (Duke University – Durham, US)

My talk overviews the use of self-assembly techniques for the construction of DNA nanostructures from strands of synthetic DNA, and the use of chemical reactions on DNA (such as strand-displacement reactions) to allow for molecular devices to operate in a programmable manner.First we overview our prior work:- The self-assembly of DNA lattices from DNA tiles and it's use for executing molecular computations is described.- Also, our experimental demonstrations of autonomous DNA devices that walk on DNA nanostructures are described.Then various techniques for executing molecular computations currently being developed in my lab will be overviewed, including:- Activatable tiles: which are initial inactive, and then can be activated when needed.- Time-responsive see-saw gates: which can be reset to be reused for multiple computations, – Analog gates: which compute (with inputs and outputs encoded as reactant concentrations) arithmetic operations over the reals.- DNA origami Transformers: which allow DNA origami to be transformed via strand-displacement reactions.

3.15 Thermostat Methods for Canonical Sampling

Matthias Sachs (University of Edinburgh, GB)

Joint work of Leimkuhler, Benjamin; Matthews, Charles; Sachs, Matthias

The talk comprises a general introduction to stochastic thermostat methods for canonical sampling in molecular dynamics and beyond. I will introduce stochastic thermostats as ergodic extensions of Newtons equations. A particular focus will be on so called adaptive thermostats i.e. thermostats which still maintain ergodicity with respect to the Gibbs-Boltzmann distribution even if the dynamics of the system are perturbed by external noise.

3.16 Models and Algorithms for Programmable Matter

Christian Scheideler (Universität Paderborn, DE)

Joint work of Derakhshandeh, Zahra; Gmyr, Robert; Strothmann, Thim; Bazzi, Rida; Richa, Andrea; Scheideler, Christian

Consider programmable matter consisting of simple computational elements, calledparticles, that can establish and release bonds and can actively move in aself-organized way. I will present a basic model and first results concerningthe feasibility of solving basic problems relevant for such programmable matter.As a model, I will use a general form of the amoebot model first proposed inSPAA 2014. Based on that model, efficient local-control algorithms for leaderelection and line formation requiring only particles with constant size memoryare presented, and the limitations of solving these problems within the amoebotmodel are discussed.The details of this talk can be found in [1].

References

1 Zahra Derakhshandeh, Robert Gmyr, Thim Strothmann, Rida Bazzi,Andrea Richa, and Christian Scheideler. Leader Election and Shape Formation withSelf-organizing Programmable Matter. In *21st International Conference on DNA Computing and Molecular Programming*, pp. 117–132, Cambridge, MA, USA, 2015.

3.17 Inverse Reinforcement Learning in Swarm Systems

Adrian Sosic (TU Darmstadt, DE)

Inverse reinforcement learning (IRL) is the problem of recovering a system's latent reward function from observed system behavior. In this paper, weconcentrate on IRL in homogeneous large-scale systems, which we refer to asswarms. We show that, by exploiting the inherent homogeneity of these systems,the IRL objective can be reduced to an equivalent single-agent problem ofconstant complexity, allowing us to decompose a global system objective intolocal subgoals at the agent-level. Based on this, we reformulate thecorresponding optimal control problem as a fix-point problem pointing towards asymmetric Nash equilibrium, which we solve using a novel heterogeneous learningscheme particularly tailored to the swarm setting. Results on the Vicsek modeland the Ising model demonstrate that the proposed framework is able to producemeaningful reward models from which we can learn near-optimal local policiesthat replicate the observed system dynamics.

3.18 Rule-Based Modeling of Graph-Like Systems

Sandro Stucki (EPFL – Lausanne, CH)

Joint work of Danos, Vincent; Heindel, Tobias; Honorato-Zimmer, Ricardo; Jaramillo-Riveri, Sebastian; Stucki, Sandro

Rule-based modeling (RBM) is a paradigm for describing combinatoriallycomplex stochastic processes with an underlying network structurethrough a finite set of rewrite rules. In this talk, I will give anoverview of RBM – illustrating how it can been used to modelbiological process in particular – and present some recent work ongenerating rate-equations and ODEs tracking higher-order statisticsfrom a large class of rule-based systems, as well as an extension of theformalism for modeling steric constraints in molecular self-assembly.

3.19 Coarse-Grained Modelling for Self-Assembly

Petr Šulc (Rockefeller University – New York, US)

Joint work of Šulc, Petr; Romano, Flavio; Ouldridge, Thomas; Louis, Ard; Doye, Jonathan; Matek, Christian; Rovigatti, Lorenzo
Main reference P. Šulc, F. Romano, T. E. Ouldridge, L. Rovigatti, J. P. K. Doye, A. A. Louis, "Sequence-dependent thermodynamics of a coarse-grained DNA model," Journal of Chemical Physics, Vol. 137, 135101, 2012.
URL http://dx.doi.org/10.1063/1.4754132
Main reference P. Šulc, F. Romano, T. E. Ouldridge, J. P. K. Doye, A. A., Louis, "A nucleotide-level coarse-grained model of RNA," Journal of Chemical Physics, Vol. 137, 235102, 2014.
URL http://dx.doi.org/10.1063/1.4881424

We introduce coarse-grained models of DNA and RNA. The models are developed tocapture the basic thermodynamics, mechanics and structural properties of DNA andRNA, including the formation of duplex from two single strands. The models areprimarily developed for applications in DNA and RNA nanotechnology, but can beused as well for biophysical properties of the molecules.We describe the model development and parametrization, and provide estimates ofcomputational efficiency.We further provide examples of applications of the models, including stranddisplacement reactions with DNA and RNA, DNA hybridization, the effects ofsecondary structure on duplex formation, RNA supercoiling, unzipping of an RNAhairpin and RNA pseudoknot folding thermodynamics.

3.20 Effects of Time-delays and Plasticity in Neural Networks

Serhiy Yanchuk (Weierstraß Institut – Berlin, DE)

Joint work of Yanchuk, Serhiy; Popovych, Oleksandr; Tass, Peter
Main reference O. V. Popovych, S. Yanchuk, P. A. Tass, "Self-organized noise resistance of oscillatory neural networks with spike timing-dependent plasticity," Science Reports, Vol. 3, Article No. 2926, 2013.
URL http://dx.doi.org/10.1038/srep02926

I split my talk into two parts. Part 1. I firstly review basic properties of systems with time-delays and theirimplementation with delay-differential equations. In large neural networks,delays can be important for determining spiking patterns and play crucial role for informationprocessing. With the use of time-shift transformation, one can reduce the number of time-delays in the network to the number of independent cycles. In such a situation,the "effective delays", which determine the dynamics, are given by the sums oftime-delaysalong any independent closed cycle [1]. Part 2. The second topic, which I mention in my talk is the effect of STDP – spike timing-dependent plasticity on the dynamics of noisyneuronal networks. In particular, STDP may produce the resistance to noise. In such a situation, the network with STDP reacts to an application of noise byadjustingthe average level of the coupling weights so that the necessary level ofsynchronizationis maintained [2].

References

1 L. Lücken, J. P. Pade, K. Knauer, S. Yanchuk,*Reduction of interaction delays in networks*, EPL (Europhys. Lett.) 103, 10006 (2013).
2 O. V. Popovych, S. Yanchuk, P. A. Tass, *Self-organized noise resistance of oscillatory neural networks withspike timing-dependent plasticity*, Sci. Rep. 3, 2926 (2013).

Participants

- Jacob Beal
BBN Technologies – Cambridge, US
- Carsten Beta
Universität Potsdam, DE
- Koan Briggs
University of Kansas, US
- José Antonio Carillo
Imperial College London, GB
- Matthew Cook
Universität Zürich & ETH Zürich, CH
- Maria Rita D'Orsogna
California State University – Northridge, US
- Vincent Danos
University of Edinburgh, GB
- Hanno Hildmann
NEC Laboratories Europe – Heidelberg, DE
- Jonathan P. Hill
National Institute for Materials Science – Ibaraki, JP
- Heinz Koeppl
TU Darmstadt, DE
- Nikita Kruk
TU Darmstadt, DE
- Emmanuel Levy
Weizmann Institute of Science – Rehovot, IL
- Yuri Maistrenko
National Academy of Sciences of Ukraine – Kiev, UA
- Vincent Noireaux
University of Minnesota – Minneapolis, US
- Matthew J. Patitz
University of Arkansas – Fayetteville, US
- John H. Reif
Duke University – Durham, US
- Matthias Sachs
University of Edinburgh, GB
- Christian Scheideler
Universität Paderborn, DE
- Rebecca Schulman
Johns Hopkins University – Baltimore, US
- Friedrich Simmel
TU München, DE
- Adrian Sosic
TU Darmstadt, DE
- Sandro Stucki
EPFL – Lausanne, CH
- Petr Šulc
Rockefeller University – New York, US
- Serhiy Yanchuk
Weierstraß Institut – Berlin, DE