ulm university universität
uulm

Institut für Theoretische Informatik

56. Workshop über Komplexitätstheorie, Datenstrukturen und Effiziente Algorithmen

Programm
Ulm, den 18. Februar 2009, Universität Ulm, Hörsaal H21/O28

10:00-10:30	*Kaffeepause und Begrüßung*
10:30-11:00	Olaf Beyersdorff
	A tight Karp-Lipton Collapse Result in Bounded Arithmetic
11:10-11:40	Michael Huber
	Combinatorial Configurations and Cryptography
11:50-12:20	Henning Wunderlich
	Ist in der Kommunikationskomplexität die Polynomielle Hierarchie PH(cc) eine echte Teilmenge von PSPACE(cc) ?
12:20-13:30	*Mittagspause*
13:30-14:00	Nadja Betzler
	Parametrisierte Komplexität von Wahlsystemen
14:10-14:40	Arne Meier
	The complexity of reasoning for fragments of default logic
14:50-15:20	Peter Lohmann
	Large Fragments of Temporal Logic and Formal Languages
15:20-15:50	*Kaffeepause*
15:50-16:20	Tatjana Schmidt
	On some SAT-Variants over linear formulas
16:30-17:00	Fabian Wagner
	Planar Graph Isomorphism is in Log-space

Weitere Informationen zum TheorieTag und Abstracts zu den Beiträgen finden Sie unter `http://www.uni-ulm.de/in/theo/tt56.html`.

A Tight Karp-Lipton Collapse Result in Bounded Arithmetic

Olaf Beyersdorff

Institut für Theoretische Informatik, Leibniz-Universität Hannover, Germany
beyersdorff@thi.uni-hannover.de

The classical Karp-Lipton Theorem states that $\mathsf{NP} \subseteq \mathsf{P}/poly$ implies a collapse of the polynomial hierarchy PH to its second level. Subsequently, these collapse consequences have been improved by Köbler and Watanabe to $\mathsf{ZPP}^{\mathsf{NP}}$ and by Sengupta and Cai to $\mathsf{S}_2^{\mathsf{p}}$. This currently forms the strongest known collapse result of this kind.

Recently, Cook and Krajíček [2] have considered the question which collapse consequences can be obtained if the assumption $\mathsf{NP} \subseteq \mathsf{P}/poly$ is provable in some weak arithmetic theory. This assumption seems to be stronger than in the classical Karp-Lipton results, because in addition to the inclusion $\mathsf{NP} \subseteq \mathsf{P}/poly$ we require an easy proof for it. In particular, Cook and Krajíček showed that if $\mathsf{NP} \subseteq \mathsf{P}/poly$ is provable in PV, then PH collapses to the Boolean hierarchy BH, and this collapse is provable in PV. For stronger theories, the collapse consequences become weaker. Namely, if PV is replaced by S_2^1, then $\mathsf{PH} \subseteq \mathsf{P}^{\mathsf{NP}[O(\log n)]}$, and for S_2^2 one gets $\mathsf{PH} \subseteq \mathsf{P}^{\mathsf{NP}}$ [2]. Still all these consequences are presumably stronger than in Sengupta's result above, because $\mathsf{P}^{\mathsf{NP}} \subseteq \mathsf{S}_2^{\mathsf{p}}$.

In [2] Cook and Krajíček ask whether under the above assumptions, their collapse consequences for PH are optimal in the sense that also the converse implications hold. Here we give an affirmative answer to this question for the theory PV. Thus PV proves $\mathsf{NP} \subseteq \mathsf{P}/poly$ if and only if PV proves $\mathsf{PH} \subseteq \mathsf{BH}$. To show this result we use the assertion $\mathsf{coNP} \subseteq \mathsf{NP}/O(1)$ as an intermediate assumption. Surprisingly, Cook and Krajíček [2] have shown that provability of this assumption in PV is equivalent to the provability of $\mathsf{NP} \subseteq \mathsf{P}/poly$ in PV. While such a trade-off between nondeterminism and advice seems rather unlikely to hold unconditionally, Buhrman, Chang, and Fortnow [1] proved that $\mathsf{coNP} \subseteq \mathsf{NP}/O(1)$ holds if and only if PH collapses to BH. Their proof in [1] refines the hard/easy argument of Kadin. We formalize this technique in PV and thus obtain that $\mathsf{coNP} \subseteq \mathsf{NP}/O(1)$ is provable in PV if and only if PV proves $\mathsf{PH} \subseteq \mathsf{BH}$. Combined with the mentioned results from [2], this implies that $PV \vdash \mathsf{PH} \subseteq \mathsf{BH}$ is equivalent to $PV \vdash \mathsf{NP} \subseteq \mathsf{P}/poly$.

Results described in the talk are joint work with Sebastian Müller (Humboldt University Berlin).

References

1. H. Buhrman, R. Chang, and L. Fortnow. One bit of advice. In *Proc. 20th Symposium on Theoretical Aspects of Computer Science*, pages 547–558, 2003.
2. S. A. Cook and J. Krajíček. Consequences of the provability of $NP \subseteq P/poly$. *The Journal of Symbolic Logic*, 72(4):1353–1371, 2007.

Combinatorial Configurations and Cryptography

Michael Huber

Wilhelm-Schickard-Institut für Informatik, Universität Tübingen
michael.huber@uni-tuebingen.de

The construction of authentication codes is an important topic in cryptography, and has been considered by many researchers over the last few decades. The first construction of such codes go back to Gilbert, MacWilliams and Sloane (1974), using finite projective planes.

In this talk, we consider combinatorial constructions for codes providing authentication and secrecy for equiprobable source probability distributions. For general authentication codes without any secrecy requirements, there exist various constructions for a long time, regardless of the source distribution. However, if we wish that the authentication codes simultaneously provide for secrecy, then there are only a few constructions known. These constructions are mostly of combinatorial nature. In particular, Stinson constructed in 1990 optimal authentication codes that are one-fold secure against spoofing and achieve perfect secrecy. His constructions rely on Steiner 2-designs and assume that the source states are equiprobable distributed.

We will extend Stinson's constructions to obtain optimal codes which are multi-fold secure against spoofing and provide perfect secrecy. This can be achieved by means of Steiner t-designs for larger t. Using Möbius planes, and more generally spherical geometries, we will particularly construct a new infinite class of optimal codes which are two-fold secure against spoofing and achieve perfect secrecy. Several further new optimal codes satisfying these properties will be illustrated. Almost all of these appear to be the first authentication codes with these properties.

Research supported by the Deutsche Forschungsgemeinschaft (DFG) via a Heisenberg grant (Hu954/4).

Ist in der Kommunikationskomplexität die Polynomielle Hierarchie PH(cc) eine echte Teilmenge von PSPACE(cc)?

Henning Wunderlich

Institut für Theoretische Informatik, Universität Ulm,
Oberer Eselsberg, D-89069 Ulm, Germany
henning.wunderlich@uni-ulm.de

Zu jedem Berechnungsmodell existiert eine Strukturelle Komplexitätstheorie. Eine solche wurde für Yao's Kommunikationsmodell vor 20 Jahren von Babai, Frankl und Simon entwickelt und untersucht. Eine wichtige offene Frage, nämlich die „PH vs. PSPACE"-Frage, ist, ob man mit einer konstanten Anzahl von Alternierungen genauso viele Probleme lösen kann, wie mit einer effizienten Anzahl von Alternierungen. Wir wollen diese Frage im Kontext der Strukturellen Kommunikationskomplexität untersuchen.

Parametrisierte Komplexität von Wahlsystemen

Nadja Betzler

Universität Jena
betzler@minet.uni-jena.de

Wahlsysteme nehmen in der modernen Informationsgesellschaft eine immer wichtigere Rolle ein. Sie sind nicht nur zentrales Werkzeug der Demokratie sondern spielen beispielsweise auch bei der Koordination in Multiagentensystemen eine tragende Rolle. Es gibt eine Vielzahl von Wahlsystemen – mit jeweiligen Vor- und Nachteilen – verknüpft mit einer Vielzahl von damit einhergehenden Fragestellungen. Angefangen bei der Auswertung einer Wahl reichen diese bis zu Fragen nach der Manipulierbarkeit, der Wahlkontrolle und vielem mehr. Ab etwa Ende der achtziger Jahre des letzten Jahrhunderts wurde damit begonnen, Fragen der Berechnungskomplexität bei Wahlsystemen intensiv zu studieren. Seither gibt es eine große Anzahl insbesondere auch komplexitätstheoretischer Ergebnisse, die zeigen, dass viele interessante Wahlfragen zu NP-schweren Problemen führen.

Nach einer allgemeinen Einleitung zum Thema Wahlsysteme wird die Nützlichkeit der parametrisierten Algorithmik im Kontext von Wahlsystemen anhand des vielstudierten Kemeny-Rankings vorgestellt. Die Eingabe besteht aus Präferenzlisten über eine Menge von Kandidaten. Eine Präferenzliste ist hierbei eine Permutation der Kandidaten. An der ersten Position einer Präferenzliste steht der jeweilige Favorit, wogegen am Listenende der jeweils am schlechtesten bewertete Kandidat steht. Das Ziel ist eine "Konsensliste" zu finden, die die Summe der "Abstände" zu den Einzellisten minimiert. Der Abstand zweier Präferenzlisten ist hierbei die Anzahl der Inversionen, auch Kendall-Tau Distanz genannt. Das zugehörige Entscheidungsproblem "Kemeny Score" ist NP-hart. Im Vortrag werden nun Ergebnisse präsentiert, die auf einer "multivariaten" Problemanalyse beruhen. Dazu werden werden insbesondere die Parameter

- Kemeny score
- Anzahl Kandidaten,
- durchschnittliche Kendall-Tau-Distanz der Eingabepräferenzlisten, und
- maximaler und durchschnittlicher "Range" eines Kandidaten in den gegebenen Präferenzlisten betrachtet.

Dieser Vortrag beruht im Wesentlichen auf folgenden Arbeiten:

Nadja Betzler, Michael R. Fellows, Jiong Guo, Rolf Niedermeier, and Frances A. Rosamond: Computing Kemeny rankings, parameterized by the average KT-distance.
In Proceedings of the 2nd International Workshop on Computational Social Choice (COMSOC'08), Liverpool, September 2008.

Nadja Betzler, Michael R. Fellows, Jiong Guo, Rolf Niedermeier, and Frances A. Rosamond: Fixed-parameter algorithms for Kemeny scores.
In Proceedings of the 4th International Conference on Algorithmic Aspects in Information and Management (AAIM'08), Shanghai, China. June 2008. Volume 5034 in Lecture Notes in Computer Science, pages 60-71, Springer

The Complexity of Reasoning for Fragments of Default Logic

Olaf Beyersdorff, Arne Meier, Michael Thomas, and Heribert Vollmer

Theoretische Informatik, Universität Hannover
Appelstr. 4, 30167 Hannover, Germany
{beyersdorff,meier,thomas,vollmer}@thi.uni-hannover.de

Default logic was introduced by Reiter in 1980. In 1992, Gottlob classified the complexity of the extension existence problem for propositional default logic as Σ_2^{p}-complete, and the complexity of the credulous and skeptical reasoning problem as Σ_2^{p}-complete, resp. Π_2^{p}-complete. Additionally, he investigated restrictions on the default rules, i. e., semi-normal default rules. Selman made in 1992 a similar approach with disjunction-free and unary default rules. In this paper we systematically restrict the set of allowed propositional connectives. We give a complete complexity classification for all sets of Boolean functions in the meaning of Post's lattice for all three common decision problems for propositional default logic. We show that the complexity is a trichotomy (Σ_2^{p}-, NP-complete, trivial) for the extension existence problem, whereas for the credulous and sceptical reasoning problem we get a finer classification down to NL-complete cases.

Fragments of Temporal Logic and Formal Languages

Peter Lohmann

Theoretische Informatik, Universität Hannover
Appelstr. 4, 30167 Hannover, Germany
lohmann@thi.uni-hannover.de

Linear temporal logic can be used as a formalism to describe formal languages. In 1965 Kamp showed that the class of languages describable by a linear temporal logic formula using future as well as past temporal operators is exactly the subclass of regular languages which can be described by a first order formula with $<$ and succ as the only binary relation symbols and without any function symbols. Etessami, Vardi and Wilke showed in 1997 that restricting the first order perspective to only using two different variables corresponds to only using unary temporal operators in the temporal logic perspective and that the correspondence can easily be held up if further restricting the first order part by not using succ anymore. Several other characterizations by algebraical and combinatorial means exist for the afore-mentioned language classes.

We show that, in the case of only two different variables, only using succ instead of only using $<$ corresponds to using only $\mathbf{X}$, $\mathbf{Y}$ and the newly introduced $\mathbf{D}$ operator and give a combinatorial characerization of the resulting language class as the class of languages which are locally threshold testable with threshold two. Local threshold testability was already used to characterize the class of languages obtained by using first order formulas with only succ but with arbitrary many different variables, as showed by Straubing in 1994.

On Some SAT-Variants over Linear Formulas

Stefan Porschen and Tatjana Schmidt

Institut für Informatik, Universität zu Köln,
Pohligstr. 1, D-50969 Köln, Germany.
{porschen,schmidt}@informatik.uni-koeln.de

We investigate the computational complexity of some prominent variants of the propositional satisfiability problem (SAT), namely not-all-equal SAT (NAE-SAT) and exact SAT (XSAT) restricted to the class of *linear* conjunctive normal form (CNF) formulas. Clauses of a linear formula pairwise have at most one variable in common. We prove that NAE-SAT and XSAT both remain NP-complete when restricted to linear formulas. Since the corresponding reduction is not valid when input formulas are not allowed to have 2-clauses, we also prove that NAE-SAT and XSAT still behave NP-complete on formulas only containing clauses of length at least k, for each fixed integer $k \geq 4$. Moreover, NP-completeness proofs for NAE-SAT and XSAT restricted to *monotone* linear formulas are presented. We also discuss the length restricted monotone linear formula classes regarding NP-completeness where a difficulty arises for NAE-SAT, when all clauses are k-uniform, for $k \geq 5$. Finally, we show that NAE-SAT is polynomial-time decidable on *exact* linear formulas, where each pair of distinct clauses has *exactly* one variable in common. And, we give some hints regarding the complexity of XSAT on the exact linear class.

Planar Graph Isomorphism is in Log-space

Fabian Wagner

Insitut für Theoretische Informatik, Universität Ulm
fabian.wagner@uni-ulm.de

Graph Isomorphism is the prime example of a computational problem with a wide difference between the best known lower and upper bounds on its complexity. We bridge this gap for a natural and important special case, planar graph isomorphism, by presenting an upper bound that matches the known logspace hardness of Lindell. In fact, we show the formally stronger result that planar graph canonization is in logspace. This improves the previously known upper bound of AC^1 of Miller and Reif.

Our algorithm first constructs the biconnected component tree of a connected planar graph and then refines each biconnected component into a triconnected component tree. The next step is to logspace reduce the biconnected planar graph isomorphism and canonization problems to those for 3-connected planar graphs, which are known to be in logspace by Datta, Limaye and Nimbhorkar. This is achieved by using the above decomposition, and by making significant modifications to Lindell's algorithm for tree canonization, along with changes in the space complexity analysis.

The reduction from the connected case to the biconnected case requires further new ideas, including a non-trivial case analysis and a group theoretic lemma to bound the number of automorphisms of a colored 3-connected planar graph. This lemma is crucial for the reduction to work in logspace.