06451 Abstracts Collection
Circuits, Logic, and Games
— Dagstuhl Seminar —

Thomas Schwentick[1], Denis Thérien[2] and Heribert Vollmer[3]

[1] Univ. Dortmund, DE
thomas.schwentick@udo.edu
[2] McGill Univ. - Montreal, CA
[3] Univ. Hannover, DE
vollmer@thi.uni-hannover.de

Abstract. From 08.11.06 to 10.11.06, the Dagstuhl Seminar 06451 "Circuits, Logic, and Games" was held in the International Conference and Research Center (IBFI), Schloss Dagstuhl. During the seminar, several participants presented their current research, and ongoing work and open problems were discussed. Abstracts of the presentations given during the seminar as well as abstracts of seminar results and ideas are put together in this paper. The first section describes the seminar topics and goals in general. Links to extended abstracts or full papers are provided, if available.

Keywords. Computational complexity theory, finite model theory, Boolean circuits, regular languages, finite monoids, Ehrenfeucht-Fraïssé games

06451 Summary – Circuits, Logic, and Games

In this document we describe the original motivation and goals of the seminar as well as the sequence of talks given during the seminar.

Keywords: Circuits, Logics, Games

Joint work of: Schwentick, Thomas; Thérien, Denis; Vollmer, Heribert

Extended Abstract: http://drops.dagstuhl.de/opus/volltexte/2007/977

Some Recent and Not-So-Recent Upper and Lower Bounds in Arithmetic Circuit Complexity

Eric Allender (Rutgers Univ. - Piscataway, USA)

Arithmetic circuit complexity is the object of intense study in four different subareas of theoretical computer science:

Dagstuhl Seminar Proceedings 06451
Circuits, Logic, and Games
http://drops.dagstuhl.de/opus/volltexte/2007/978

1. Derandomization. The problem of determining if two arithmetic circuits compute the same function is known as ACIT (arithmetic circuit identity testing). ACIT is the canonical example of a problem in BPP that is not known to have a deterministic polynomial-time algorithm. Kabanets and Impagliazzo showed that the question of whether or not ACIT is in P very tightly linked to the question of proving circuit size lower bounds.

2. Counting Classes (such as #P and #L) can be characterized using arithmetic circuits.

3. Computation over the Reals. The Blum-Shub-Smale model of computation over the reals is an algebraic model that has received wide attention.

4. Valiant's Classes VP and VNP. Valiant characterized the complexity of the permanent in two different ways. Viewed as a function mapping n-bit strings to binary encodings of Natural numbers, the permanent is complete for the class #P. Viewed as an n-variate polynomial, the permanent is complete for the class VNP.

The general thrust of these four subareas has been in four different directions, and the questions addressed seem quite different from those addressed by work in the numerical analysis community, such as that surveyed by Demmel and Koev.

This talk will survey some recent work that ties all of these areas together in surprising ways. Most of the results that will be discussed can be found in [ABKM, Bu] but I will also discuss some more recent progress.

[Al] Eric Allender Arithmetic Circuits and Counting Complexity Classes.

In Complexity of Computations and Proofs, edited by Jan Krajíček, Quaderni di Matematica Vol. 13, Seconda Universita di Napoli, 2004, pp. 33-72.

[ABKM] E. Allender and P. Buergisser and Johann Kjeldgaard-Pedersen and Peter Bro Miltersen, On the Complexity of Numerical Analysis, Proc. 21st Ann. IEEE Conf. on Computational Complexity (CCC '06), 2006, 331–339.

[Bu] P. Buergisser, On defining integers in the counting hierarchy and proving lower bounds in algebraic complexity, TR06-113, ECCC, 2006.

[DK] J. Demmel and P. Koev, Accurate and efficient algorithms for floating point computation, Proceedings of the 2003 International Congress of Industrial and Applied Mathematics, 2003

[KI] V. Kabanets and R. Impagliazzo, Derandomizing polynomial identity tests means proving circuit lower bounds, STOC 2003, 355–364.

Keywords: Arithmetic Circuit Complexity

FO[<] Uniformity

Christoph Behle (Universität Tübingen, D)

Uniformity notions more restrictive than the usual FO[<,+,*]-uniformity = FO[<,Bit]-uniformity are introduced.

It is shown that the general framework exhibited by Barrington et al. still holds if the fan-in of the gates in the corresponding circuits is considered, if one restricts just to FO[<]-uniformity.

Joint work of: Behle, Christoph; Lange, Klaus-Joern

Non Uniform Reductions

Harry Buhrman (CWI Amsterdam, NL)

We show how to sometimes make non-uniform reductions uniform. In particular we show that every $\leq_m^{P/1}$-complete set for EXP is $\leq_T^P$-complete. Our result does not relativize and in particular setteling the question whether these sets are in fact $\leq_{tt}^P$-complete will separate complexity classes.

Joint work of: Buhrmann, Harry; Hescott, Ben; Homer, Steve; Torenvliet, Leen

Model Theory on Well-Behaved Classes of Finite Structures

Anuj Dawar (Cambridge University, GB)

The early days of finite model theory saw a variety of results establishing that the model theory of the class of finite structures is not well-behaved. Recent work has shown that considering subclasses of the class of finite structures allows us to recover some good model-theoretic behaviour. This appears to be especially true of some classes that are known to be algorithmically well-behaved. I will review some results in this area and explore the connection between logic and algorithms.

Keywords: Fintie model theory, bounded treewidth, planar graphs, excluded minors, preservation theorems

A Game for Lower Bounds on Formula Size

Lauri Hella (University of Tampere, FIN)

We define an Ehrenfeucht-Fraïssé game that characterizes definability of classes of structures with first order formuals of given size. The game $\mathrm{EF}_r(A, B)$ is defined for two classes A and B of structures; r is the upper bound for formula size. The main theorem states that Spoiler has a winning strategy in $\mathrm{EF}_r(A, B)$ if and only if there is a formula φ of size at most r such that $\mathbb{A}$

Some Algebraic Problems with Connections to Circuit Complexity of Dynamic Data Structures

William Hesse (Clarkson University - Potsdam, USA)

While researching dynamic data structures of polynomial size that are updated by extremely simple circuits, we have come across many interesting algebraic problems. Some of these simple questions about small sums and products in an algebra would give lower bounds on the complexity of dynamic data structures.

Keywords: Boolean Functions, auxiliary data, circuit complexity, lower bounds

Extended Abstract: http://drops.dagstuhl.de/opus/volltexte/2007/974

Structure Theorem and Strict Alternation Hierarchy for $\mathbf{FO^2}$ on Words

Neil Immerman (Univ. of Massachusetts - Amherst, USA)

It is well-known that every first-order property on words is expressible using at most three variables. The subclass of properties expressible with only two variables is also quite interesting and well-studied. We prove precise structure theorems that characterize the exact expressive power of first-order logic with two variables on words. Our results apply to $\mathrm{FO}^2[<]$ and $\mathrm{FO}^2[<, \mathrm{suc}]$, the latter of which includes the binary successor relation in addition to the linear ordering on string positions.

For both languages, our structure theorems show exactly what is expressible using a given quantifier depth, n, and using m blocks of alternating quantifiers, for any $m \leq n$. Using these characterizations, we prove, among other results, that there is a strict hierarchy of alternating quantifiers for both languages. The question whether there was such a hierarchy had been completely open since it was asked in [Etessami, Vardi, and Wilke 1997].

Keywords: Descriptive complexity, finite model theory, alternation hierarchy, Ehrenfeucht-Fraïssé games

Joint work of: Weis, Philipp; Immerman, Neil

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2007/975

Integer Addition, Circuits, Logic and Games

Michal Koucky (Academy of Sciences - Prague, CZ)

We discuse the problem of the circuit complexity of Integer Addition.

We review what is known and we point out that the size of bounded-depth circuits that compute Integer Addition is still not known accurately. We relate this problem to the classification of regular languages with respect to their circuit size. We report on our approach of proving required lower bounds via Ehrenfeucht-Fraïssé game type arguments. In particular we show a proof of Parity not being in AC^0 via Ehrenfeucht-Fraïssé games.

Keywords: Circuit lower-bounds, Ehrenfeucht-Fraïssé game

Joint work of: Latemann, Clemens; Poloczek, Sebastian; Thérien, Denis; Koucky, Michal

Algebraic Characterisation of TC^0

Andreas Krebs (Universität Tübingen, D)

We show that the well-known equivalences between logic, circuits and algebra, have their analogies for TC^0 resp. Maj-Logic.

For the algebraic part we characterize the languages in TC^0 as inverse morphic images of certain groups. Necessarily these are infinite, since nonregular sets are concerned. To limit the power of these infinite algebraic objects, we equip them with a finite type set and introduce the notion of a finitely typed (infinite) monoid.

For this algebraic characterisations we can show that there is a tight correspondences between the algebraic subvareties to subclasses of TC^0 and subfamilies of logic formulas.

Keywords: TC0, Maj Logic, Finitely Typed Groups

A rank technique for formula size lower bounds

Troy Lee (Université Paris Sud, F)

We introduce a new technique for proving formula size lower bounds based on matrix rank. A simple form of this technique already gives bounds at least as large as those given by the method of Khrapchenko, originally used to prove an n^2 lower bound on the parity function. We also apply our method to the parity function, and give an exact expression for the formula size of parity: if $n = 2^\ell + k$, where $0 \leq k < 2^\ell$, then the formula size of parity on n bits is exactly $2^\ell(2^\ell + 3k) = n^2 + k2^\ell - k^2$. Such a bound cannot be proven by any of the lower bound techniques of Khrapchenko, Nečiporuk, Koutsoupias, or the quantum adversary method, which are limited by n^2.

Keywords: Formula size, communication complexity, lower bound

Some classes between NC1 and LogCFL

Meena Mahajan (IMSc - Chennai, IND)

We consider two new kinds of classes lying between NC^1 and LogCFL. By imposing a restriction of polynomial degree on polylog-width circuits (SC), we obtain a hierarchy of classes between NC^1 and LogCFL. We explore the power of these classes and their arithmetizations.

Visibly pushdown languages (VPLs) are a subclass of DCFLs properly generalizing regular languages, and are known to be in NC^1. We explore how much further we can go beyond VPLs while staying within NC^1. The framework of synchronised PDA, developed by Caucal, turns out to be quite useful. We also consider arithmetizations of the generalizations.

Joint work of: Raghavendra Rao, B.V.; Limaye, Nutan; Meyer, Antoine; Mahajan, Meena

Keywords: NC, SC, LogCFL, pshdown-automata

Characterization of Ehrenfeucht-Fraïsé equivalence for two classes of finite graphe

Malika More (Université Clermont 1, F)

We present a complete analysis of Ehrenfeucht-Fraïsé equivalence for the class of equivalence relations and the class of bijections. We deduce some information about the asymptotic behavior of the corresponding Ash counting functions.

Joint work of: More, Malika; Chateau, Annie

Counting results in weak formalisms

Malika More (Université Clermont 1, F)

The counting ability of weak formalisms is of interest as a measure of their expressive power. The question was investigated in the 1980's in several papers in complexity theory and in weak arithmetic. In each case, the considered formalism (AC^0–circuits, first–order logic, Δ_0, respectively) was shown to be able to count precisely up to a polylogarithmic number. An essential part of each of the proofs is the construction of a 1–1 mapping from a small subset of $\{0, \ldots, N-1\}$ into a small initial segment. In each case the expressibility of such a mapping depends on some strong argument (group theoretic device or prime number theorem) or intricate construction. We present a coding device based on a collision-free hashing technique, leading to a completely elementary proof for the polylog counting capability of first–order logic (with built–in arithmetic), AC^0–circuits, rudimentary arithmetic, the Linear Hierarchy, and monadic–second order logic with addition.

Keywords: Small complexity classes, logic, polylog counting

Joint work of: Durand, Arnaud; Lautemann, Clemens; More, Malika

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2007/976

Games and Search Problems

Pavel Pudlak (Czech Academy of Sciences, CZ)

We consider finite combinatorial two-player games. We show a way how to combine several games into one for which we know that B has a winning strategy. Then we consider the search problem: given a strategy for A find moves for B that beat the strategy. If A's strategy is given by a circuit, this is a total NP search problem (TFNP). We consider a version of the game in which the game and A's strategy is given by an oracle and ask how many queries are needed to beat the alleged strategy. Our result shows that for such games there is a hierarchy with respect to the length of the games used in the construction. If the length is k then the number of queries needed is roughly k-times iterated exponential.

Keywords: Combinatorial games, search problems

Branching Programs: Complexity Lower Bounds by Communication Games

Martin Sauerhoff (Universität Dortmund, D)

In the first part of the talk, state-of-the-art time-space tradeoff lower bounds for unrestricted branching programs (or, equivalently, RAM algorithms) have been surveyed and some remarks about proof techniques have been made. In the second part, a lower bound on the size of randomized read-k BPs of order $2^{-\Omega(k^{-2}2^{-13k}n}$ for the function $\mathrm{cl}_{3,n}$ testing whether a graph on n nodes has a 3-clique has been presented that works if the error probability is bounded by $O(2^{-4k})$. The best previous bound for this function (Sauerhoff, 2003) was of order $2^{-\Omega(k^{-2}2^{4k}\sqrt{n}}$ and required an upper bound on the error of $2^{-\Theta(2^{-2k})}$. The function can be trivially computed even by nondeterministic OBDDs of size $O(n^3)$ by a straightforward guess-and-verify approach.

Keywords: Branching programs, communication complexity, information complexity

The expressive power of numerical predicates

Nicole Schweikardt (HU Berlin, D)

This 2 hour lecture gives a survey on the expressive power of numerical predicates. In particular, the following logics are considered:

(1) First-order logic with Bit-predicate (FO[Bit], for short):

It is well-known that the linear order can be expressed in FO[Bit] and that FO[Bit] is exactly as expressive as, e.g., first-order logic with addition and multiplication or, equivalently, first-order logic with addition and a "square numbers" predicate.

In this talk I will also sketch the proof of a not so well-known result stating that there are 5 particular linear ordering relations such that FO[Bit] is exactly as expressive as first-order logic with these five linear orders.

(2) First-order logic and monadic logics with addition (FO[+], MLFP[+], MSO[+]):

I will present an Ehrenfeucht-Fraïssé game proof of the Theorem of Ginsburg and Spanier, stating that FO[+]-sentences have semi-linear spectra. Concerning extensions of FO[+] which allow quantification of monadic relations, it is known that on strings with built-in addition, monadic second-order logic MSO(+)-sentences can describe exactly those languages that belong to the linear time hierarchy. Furthermore, it is known that monadic least fixed-point logic MLFP(+) can describe at least all problems in Grandjean's linear time complexity class DLIN. This, in particular, leads to a result stating that a separation between the expressive power of addition-invariant MLFP(+) and addition-invariant MSO(+) on strings would imply a separation between the complexity class DLIN and the linear time hierarchy.

Apart from these topics, I will also survey results on

(3) first-order logic with counting quantifiers and various numerical predicates

and

(4) the Crane Beach conjecture.

FO-definable tree languages

Luc Segoufin (INRIA Futurs - Orsay, F)

Given a regular tree language is there a recursive algorithm saying whether it is definable in FO[+1]? In this talk we solve positively this question.

Definability of Languages by Generalized First-order Formulas over (N,+)

Howard Straubing (Boston College, USA)

We study an extension of first-order logic by modular quantifiers of a fixed modulus q. Drawing on collapse results from finite model theory and techniques of finite semigroup theory, we show that if the only available numerical predicate is addition, then sentences in this logic cannot define the set of bit strings in which the number of 1's is divisible by a prime p that does not divide q. More generally, we give an effective algebraic characterization of all the regular languages definable in this logic.

The same statement with addition replaced by arbitrary numerical predicates is equivalent to the conjectured separation of the circuit complexity classes ACC and NC^1. Thus our theorem can be viewed as proving a highly uniform version of this conjecture.

A preliminary version of this paper appeared in the proceedings of the 2006 STACS conference. The full paper has been accepted for publication in *SIAM Journal on Computing.*

Keywords: Finite model theory, circuit complexity

Joint work of: Roy, Amitabha; Straubing, Howard

Finite monoids, regular languages, circuit complexity and logic

Pascal Tesson (Laval University - Quebec, CA)

Finite monoids provide a crucial tool in the study of finite automata. This algebraic point of view has been particularly successful to obtain effective characterizations of regular languages defined by various logical fragments.

The program over finite monoid formalism provides a way of applying these ideas to obtain algebraic characterizations of circuit complexity classes.

This introductory talk surevys the imoprtant results in this direction and discusses the current state of our understanding of these methods.

Keywords: Finite monoids, circuit complexity, programs over monoids

On the size of Craig's Interpolant

Jacobo Toran (Universität Ulm, D)

Mundici considered the question of whether the interpolant of two propositional formulas of the form $F \rightarrow G$ can always have a short circuit description, and showed that if this is the case then every problem in NP $\cap$ co-NP would have polynomial size circuits.

In this talk we observe further consequences of the interpolant having short circuit descriptions, namely that UP $\subseteq$ P/poly, and that every single valued NP function has a total extension in FP/poly. We also relate this question with other Complexity Theory assumptions and with the Graph Isomorphism problem.

A note on the size of Craig Interpolants

Jacobo Toran (Universität Ulm, D)

Mundici considered the question of whether the interpolant of two propositional formulas of the form $F \rightarrow G$ can always have a short circuit description, and showed that if this is the case then every problem in NP $\cap$ co-NP would have polynomial size circuits.

In this note we observe further consequences of the interpolant having short circuit descriptions, namely that UP $\subseteq$ P/poly, and that every single valued NP function has a total extension in FP/poly. We also relate this question with other Complexity Theory assumptions.

Keywords: Interpolant, non-uniform complexity

Joint work of: Schöning, Uwe; Toran, Jacobo

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2007/973