Proof complexity (11w5103)

Samuel Buss (University of California, San Diego)
Stephen Cook (University of Toronto)
Antonina Kolokolova (Memorial University of Newfoundland)
Toni Pitassi (University of Toronto)
Pavel Pudlák (Institute of Mathematics, Prague)

October 2 – October 7, 2011

1 Overview of the Field

Proof complexity is a research area that studies the concept of complexity from the point of view of logic. In proof complexity, an important question is: "how difficult is it to prove a theorem?" There are various ways that one can measure the complexity of a theorem. We can ask what is the length of the shortest proof of a theorem in a given formal system (size of the proofs) or how strong a theory is needed to prove the theorem (that is, how complex are the concepts involved in the proof). The former is studied in the context of proof systems (in particular, propositional proof systems), the latter in bounded arithmetic.

Naturally, the length of a shortest proof of a theorem very much depends on the type of proof system in which it is being proved. For a proof system, we also would like to know if there is an efficient algorithm that would produce a proof of any tautology, and whether it would produce a shortest such proof. These questions, besides their mathematical and philosophical significance, have practical applications in automated theorem proving.

From the computational point of view, the question of proving tautologies is a co-NP question: that is, a counterexample to a formula which is not a tautology would be short and easily verifiable. Moreover, it is known that the existence of a propositional proof system in which all tautologies have short proofs is equivalent to proving that NP is closed under complementation. This establishes an important link between proof complexity and a major open problem in computational complexity theory. There are other connections between computational and proof complexity (for example, circuit lower bounds and proof system lower bounds), although in some cases the proof complexity counterparts of computational complexity results are still unresolved.

A related, uniform side of proof complexity is the study of weak systems of arithmetic (in particular, bounded arithmetic). Here the complexity of a proof of a theorem is defined in terms of the complexity of concepts involved in that proof. For example, the weaker systems of arithmetic cannot operate with concepts such as the Pigeonhole Principle. A recent subarea of proof complexity, called bounded reverse mathematics, studies the complexity of reasoning needed to prove a given theorem: that is, what is the weakest theory in which a given mathematical theorem can be proven.

Proof complexity historically was developed during the 1960's and 1970's, as an outgrowth of research on computer-based theorem provers. At first, researchers in proof complexity concentrated primarily on lower bounds on proof size, and targeted lower bounds on computational complexity (for instance, Cook's characterization of the NP=?coNP problem in terms of proof complexity) and independence results in formal

theories such as bounded arithmetic (the theories $I\Delta_0$ and PV at first, and later fragments such as S^i_2 and T^i_2.) More recently, especially in the past 10-15 years, proof complexity has become increasingly concerned with problems in computer-based proof search again. This aspect was well-represented at the BIRS workshop, with talks on resolution, on SAT solvers, on linear programming, and on semi-definite programming. This renewed interest by the proof complexity community in practical computer-based theorem provers is a welcome development. Indeed, it is hoped that significant future developments will arise from these two strands of proof complexity, namely from the interplay between the lower bounds on proof complexity and computational complexity, and the upper bounds of improved algorithms for theorem proving.

2 Recent Developments

Proof complexity is an active field of research. This interdisciplinary area is recognized as a respectable field both in computational complexity and in proof theory. The number of papers published, as well as the number of researchers working in proof complexity steadily increases. The present workshop documented the viability of this field.

There are many directions of research in proof complexity. A large part of these directions was represented in the workshop. Due to space limitations we mention only a few of them in this report.

2.1 Resolution and SAT-solvers

SAT solvers, or "satisfiability solvers" represent the state of the art in *practical* algorithms for determining the satisfiability of propositional formulas (usually given as sets of clauses). The solvers have been quite successful (indeed, unexpectedly successful) in solving large instances of SAT that arise in applications for software verification, hardware verification, and many other areas. The most successful solvers to date for these kinds of applications are based on the DPLL (Davis-Putnam-Logemann-Loveland) search procedures that use the clause learning method of Marques-Silva and Sakallah.

Resolution proof system was introduced in automated theorem proving. Thus the study of this system is motivated by practical problems. However, it is also a basic proof system in the theoretical study of proof systems. Resolution is also tightly connected with SAT-solvers. Namely, DPLL, the most commonly used tool in solving SAT is just one facet of the tree-like proofs based on Resolution. Recent advances in the study of Resolution were mostly motivated by connections with SAT-solvers. Lower bounds and trade-offs between various parameters of resolution proofs can explain why certain SAT-solvers are not efficient in certain situations. One set of such results was presented in the lecture of Jakob Nordström. These results are described in the section Highlights.

2.1.1 Presentation highlights

The main highlight of this topic of the workshop was a talk by Jakob Nordstrom (KTH) on "Understanding the Hardness of Proving Formulas in Propositional Logic". This was a survey talk, covering both the Resolution proof system and SAT solvers, and emphasizing the interplay between them. In particular, some new results on formula space complexity in the Resolution setting and their relation to SAT solver performance were discussed. The full description of the talk is below:

Jakob Nordstrom, *Understanding the Hardness of Proving Formulas in Propositional Logic*.

Abstract: Proving formulas in propositional logic is believed to be theoretically intractable in general, and the importance of deciding whether this is so has been widely recognized, e.g., by this being listed as one of the famous million dollar Millennium Problems. On the practical side, however, these days SAT solvers are routinely used to solve large-scale real-world SAT instances with millions of variables. This is in contrast to that there are also known small example formulas with just hundreds of variables that cause even state-of-the-art SAT solvers to stumble.

What lies behind the spectacular success of SAT solvers, and how can one determine whether a particular formula is hard or tractable? In this talk, we will discuss if proof complexity can say anything interesting about these questions.

In particular, we propose that the space complexity of a formula could be a good measure of its hardness. We prove that this would have drastic implications for the impossibility of simultaneously optimizing time and memory consumption, the two main resources of SAT solvers. Somewhat surprisingly, our results are obtained by relatively elementary means from combinatorial pebble games on graphs, studied extensively in the 70s and 80s.

Joint work with Eli Ben-Sasson.

2.1.2 Some other notable talks in this area[1]

Another problem recently studied in proof complexity concerns various modifications of DPLL that are used in SAT-solvers. In order to prove bounds on these proof system it is necessary to find corresponding modifications of Resolution. The most successful SAT-solvers use clause learning. Advantages and limits of this method were presented in two talks devoted to the analysis of clause learning:

Jan Johannsen, *Lower Bounds for Width-restricted Clause Learning*

Abstract: Clause learning is a technique used by propositional satisfiability solvers where some clauses obtained by an analysis of conflicts are added to the formula during backtracking. It has been observed empirically that clause learning does not significantly improve the performance of a solver when restricted to learning clauses of small width only. We survey several lower bound theorems supporting this experience.

Sam Buss, *An Improved Separation of Regular Resolution from Proof Resolution and Clause Learning*.

Abstract: We prove that the graph tautology principles of Alekhnovich, Johannsen, Pitassi and Urquhart have polynomial size pool resolution refutations using only input lemmas as learned clauses and without degenerate resolution inferences. Consequently, these can be shown unsatisfiable by polynomial size DPLL proofs with clause learning.

2.2 Subsystems of Bounded Arithmetic

In Bounded Arithmetic first order theories are studied that have close connection with complexity classes in computational complexity and proof systems in propositional logic. The research in this subarea focuses on the following problems:

- finding the weakest theory in which a given theorem from computational complexity can be proven,
- separating theories corresponding to complexity classes,
- characterizing low complexity theorems of a given theory.

There is a lot of interaction going on between bounded arithmetic and computational complexity. For instance, in recent years several characterizations of $\forall\Sigma^b_1$ theorems of the theories T^n_2 of the bounded arithmetic hierarchy have been found. These results introduced new classes of total polynomial search problems that were not known before.

2.2.1 Presentation highlights

In a videotaped lecture Stephen Cook presented a survey of first order theories associated with complexity classes. In the second part of the lecture he talked about formalizing matching algorithms.

Stephen Cook, *Formalizing Randomized Matching Algorithms*

Abstract: Using Jeřábek's framework for probabilistic reasoning, we formalize the correctness of two fundamental RNC2 algorithms for bipartite perfect matching within the theory VPV for polytime reasoning. The first algorithm is for testing if a bipartite graph has a perfect matching, and is based on the Schwartz-Zippel Lemma for polynomial identity testing applied to the Edmonds polynomial of the graph. The second algorithm, due to Mulmuley, Vazirani and Vazirani, is for finding a perfect matching, where the key ingredient of this algorithm is the Isolating Lemma.

Joint work with Dai Tri Man Le.

[1] Due to space limitation we mention only two talks. The abstracts of other high quality talks can be found in the materials of the workshop. The same applies to the following sections.

2.2.2 Some other notable talks in this area

Theories for approximate counting appeared also in another lecture. Leszek Kolodziejczyk talked about the problem of separating these theories from theories T_2^n.

Leszek Kolodziejczyk, *Fragments of approximate counting*.

Abstract: We study the low-complexity consequences of Jerabek's theory of approximate counting, that is, T_2^1 plus the surjective weak pigeonhole principle for $P^N P$ functions, with the goal of showing that it does not prove all the Σ_1^b sentences provable in full bounded arithmetic. This is inspired by the question of whether the levels of the bounded arithmetic hierarchy can be separated by a sentence of fixed low complexity, and the related question of whether the CNFs provable in constant depth Frege systems form a hierarchy with depth. We give some partial results. Joint work with Sam Buss and Neil Thapen.

Emil Jeřábek talked about a problem that apparently does not have much to do with proof complexity. But in fact the problem is highly motivated by proof complexity and has an interesting consequence for first order theories studied in bounded arithmetic.

Emil Jeřábek, *Root finding in TC^0*.

Abstract: We show that for any constant d, there is a uniform TC^0 algorithm computing approximations of complex zeros of degree-d univariate rational polynomials (given by a list of coefficients in binary). Equivalently, the theory VTC^0 + the set of all true $\forall\Sigma_0^B$ sentences includes $IOpen$ (for the string sort).

2.3 Proof systems for integer linear programing

Another important subarea of proof complexity is the study methods used in integer linear programing by means of propositional proof systems. For example, using a machinery developed in proof complexity it has been shown that there are instances of integer linear programing that cannot be solved in subexponential time by the well-known method of cutting planes. For most methods such lower bounds are not known yet, but some partial results have been obtained.

2.3.1 Presentation highlights

The most impressive lecture on this topic was given by Albert Atserias. He showed how to combine methods of finite model theory and integer linear programing to prove results about the graph isomorphism problem. Here is a more detailed description of the lecture.

Albert Atserias, *Sherali-Adams Relaxations and Indistinguishability in Counting Logics*.

Abstract: Two graphs with adjacency matrices $\mathbf{A}$ and $\mathbf{B}$ are isomorphic if there exists a permutation matrix $\mathbf{P}$ for which the identity $\mathbf{P}^{\mathrm{T}}\mathbf{A}\mathbf{P} = \mathbf{B}$ holds. Multiplying through by $\mathbf{P}$ and relaxing the permutation matrix to a doubly stochastic matrix leads to the linear programming relaxation known as fractional isomorphism. We show that the levels of the Sherali-Adams (SA) hierarchy of linear programming relaxations applied to fractional isomorphism interleave in power with the levels of a well-known color-refinement heuristic for graph isomorphism called the Weisfeiler-Lehman algorithm, or equivalently, with the levels of indistinguishability in a logic with counting quantifiers and a bounded number of variables. This tight connection has quite striking consequences. For example, it follows immediately from a deep result of Grohe in the context of logics with counting quantifiers, that a fixed number of levels of SA suffice to determine isomorphism of planar and minor-free graphs. We also offer applications both in finite model theory and polyhedral combinatorics. First, we show that certain properties of graphs, such as that of having a flow-circulation of a prescribed value, are definable in the infinitary logic with counting with a bounded number of variables. Second, we exploit a lower bound construction due to Cai, Fürer and Immerman in the context of counting logics to give simple explicit instances that show that the SA relaxations of the vertex-cover and cut polytopes do not reach their integer hulls for up to $\Omega(n)$ levels, where n is the number of vertices in the graph.

Joint work with Elitza Maneva.

This was the other of the two videotaped lectures.

2.3.2 Another notable talk in this area

The study of the constraint satisfaction problem is a very active area in theoretical computer science. This is because many practical problems can be represented as a particular type of the constraint satisfaction problem. Therefore it is important to understand the computational complexity of constraint satisfaction problems for natural classes. Konstantinos Georgiou studied a particular form of the problem from the point of view of the Sherali-Adams method.

Konstantinos Georgiou, *Refuting CSPs require Sherali-Adams SDPs of Exponential Size, due to Pairwise Independence*.

Abstract: This work considers the problem of approximating fixed predicate constraint satisfaction problems (MAX k-CSP(P)). We show that if the set of assignments accepted by P contains the support of a balanced pairwise independent distribution over the domain of the inputs, then such a problem on n variables cannot be approximated better than the trivial (random) approximation, even after augmenting the natural semidefinite relaxation with $\Omega(n)$ levels of the Sherali-Adams hierarchy. It was recently shown that under the Unique Game Conjecture, CSPs for predicates satisfying this condition cannot be approximated better than the trivial approximation. Our results can be viewed as an unconditional analogue of this result in a restricted computational model. Alternatively, viewing the Sherali-Adams SDP system as a proof system, our result states that a proof of exponential size is required in order to refute highly unsatisfiable instances. For our result we introduce a new generalization of techniques to define consistent local distributions over partial assignments to variables in the problem, which is often the crux of proving lower bounds for such hierarchies.

This is joint work with Siavosh Benabbas, Avner Magen and Madhur Tulsiani.

2.4 Other topics

A very interesting lecture was given by a leading expert in computational and proof complexity Alexander Razborov. He developed a theory, which he calls *flag algebras*, for proving results in extremal combinatorics. His aim his to solve problems of the type of Turán's Conjecture from 1941 and the Cacceta-Häggkvist Conjecture. He did not prove any of these two conjectures, but made a substantial progress towards the solution. What is the most interesting aspect of his approach is that it is completely new. Here is the abstract of his talk.

Alexander Razborov (University of Chicago), *Flag algebras*.

Abstract: A substantial part of extremal combinatorics studies relations existing between densities with which given combinatorial structures (fixed size "templates") may appear in unknown (and presumably very large) structures of the same type. Using basic tools and concepts from algebra, analysis and measure theory, we develop a general framework that allows to treat all problems of this sort in an uniform way and reveal mathematical structure that is common for most known arguments in the area. The backbone of this structure is made by commutative algebras defined in terms of finite models of the associated first-order theory.

In this talk I will give a general impression of how things work in this framework, and we will pay a special attention to concrete applications of our methods.

3 Panel discussion

During the workshop we had a panel discussion on the future of proof complexity. Due to the presence of most of the leading experts in the field it was a unique opportunity to discuss such strategic problems, and the panel discussion proved to be highly stimulating. Many participants proposed research directions for the field, as well as suggested open problems (see below). The panel discussion was viewed by most participants very positively — interesting and informative.

4 Problems

During the workshop many open problems were suggested in the talks, as well during the panel discussion. Thus, we decided to make a compendium of open problems suggested by the participants and include it here in the report.

List of problems

1. Separate levels of $T_2^k[R]$ hierarchy: We don't know a k such that sentences $\forall\Sigma_k^b$ would separate levels. This corresponds to separating levels of bounded-depth Frege systems (a well-known problem). During the panel discussion Pavel Pudlák pointed out that, although the problem is hard, we probably do have means to solve it.

2. (Antonina Kolokolova, panel discussion) More connections between finite model theory and proof complexity, in the spirit of Albert Atserias and Yijia Chen's work.

3. (Oliver Kullmann, panel discussion) Look at single instances for SAT.

4. (Sam Buss, panel discussion) Look at SMT solvers and higher order setting: relax conditions at SMT setting, analyze counterexample guided abstraction refinement.

5. (Paul Beame, panel discussion) How to do an analog of clause learning in the integer programming setting (e.g., learning an equation)? What are the limitations of integer linear programming?

6. (Jan Johannsen, panel discussion) Algorithms vs proof systems question, e.g., DLL vs. tree resolution, DLL+CL vs. WRTC.

7. (Russell Impagliazzo, panel discussion)

   (a) Dynamic programming analysis similar to resolution.

   (b) Proof complexity of satisfiable instances. E.g., myopic searches. We can bound the time needed on unsatisfiable formulas, but can we do it also for satisfiable?

   (c) Find problem solvable in B-ODI, but not in backtracking trees.

8. (Toni Pitassi, panel discussion) Lower bounds for stronger proof systems. Also, approximation algorithms vs. LS, Lasserre, etc.

9. (Alasdair Urquhart) What is the complexity of determining the minimum regular width of a set of clauses? (Conjecture: PSPACE-complete).

10. (Moshe Vardi via Alasdair Urquhart) What is the complexity of determining the resolution width of a set of clauses? (Conjecture: EXPTIME-complete).

11. (Alasdair Urquhart) Prove or disprove: The Tseitin graph tautologies always have a regular proof with minimal size. Same question for the pigeonhole principle.

12. (Alexander Razborov) Unconditional size lower bounds for "simple" proof systems like Cutting Planes (combinatorial, without interpolation) or Lovasz-Schrijver.

13. (Albert Atserias and Alexander Razborov) Prove that the integrality gap of 2 for Vertex Cover problem survives $\Omega(n)$ rounds of Sherali-Adams without Unique Games conjecture.

14. (Toni Pitassi and Alexander Razborov) Remove restrictions in Pitassi/Patrascu's upper bound being close to optimal.

15. (Jakob Nordström and Alexander Razborov) Is there a tautology with superlinear lower bounds on (total) variable space? This problem was listed in 2002 paper by M. Alekhnovich, E. Ben-Sasson, A. Razborov and A. Wigderson "Space complexity in propositional calculus". In particular, are there polynomial-size k-CNF formulas with total refutation space $\Omega((sizeof)F)^2$ in resolution?

16. (Jakob Nordström and Alexander Razborov) Prove superconstant clause space lower bounds for PCR or Cutting Planes proofs for any bounded fan-in tautology. (The question for PCR also appears in ABRW'02 paper).

17. (Jakob Nordström) Is tractability captured by space complexity? That is, do theoretical trade-offs show up in real life for state-of-the-art SAT solvers run on pebbling contradictions?

18. (Jakob Nordström) Can the Substitution Theorem be proven for, say, Cutting Planes or Propositional Calculus (with or without Resolutions), thus yielding time-space trade-offs for these proof systems as well?

19. (Jakob Nordström) Are there superpolynomial trade-offs in resolution for formulas refutable in constant space? Can every proof be carried out in at most linear space?

20. (Stephen Cook) Use Emil Jerabek's techniques to formalize constructive aspects of fundamental theorems that require probabilistic reasoning. This includes theorems in cryptography, such as the Goldreich-Levin Theorem, and construction of pseudo-random number generators from one-way functions.

21. (Stephen Cook) A very recent paper by Pavel Hrubes and Iddo Tzameret proves that the 'hard matrix identities' (such as AB = I implies BA = I) over certain rings have quasi-polynomial size Frege proofs. The big open question here is: does this result have a uniform version? This would involve formalizing these identities in a suitable theory such as those introduced by Stephen Cook and Lila Fontes: "Formalizing Linear Algebra", CSL 2010.

22. (Edward Hirsch) Devise an "interesting" heuristic proof system, i.e., a heuristic proof system that makes an advantage over classical proof systems for a problem that possesses no known polynomially bounded heuristic acceptor.

23. (Leszek Kolodziejczyk) Can Jerabek's theory for approximate counting, i.e. $T^1_2(\alpha)$ plus the surjective WPHP for $PV_2(\alpha)$ functions, be separated from full $S_2(\alpha)$ by an NP search problem?

24. (Leszek Kolodziejczyk) Is there a sequence $\{A_n : n \geq 1\}$ of narrow (polylog width) CNFs, with $size(A_n) = poly(n)$, that does have short constant-depth refutations, but does not have quasipolynomial-size treelike "random Res(log) refutations". More precisely, this means that there should be no quasipolynomial-size treelike Res(log) refutations of $A_n \wedge B_n$, where B_n is any narrow CNF true under at least a $1 - (1/n)$ fraction of all truth assignments.

5 Scientific Progress Made

Participants of the workshop reported on many opportunities for collaborations, some just starting and some for which the resulting papers are already in preparation. In particular, Jan Johannsen and Sam Buss have obtained during the workshop new results about the provability of the obfuscated Stone tautologies in reg-WRTI and in DPLL with clause learning; a planned paper is in preparation. Albert Atserias and Moritz Müller reported that they made a significant progress on their joint work on general lower bounds for daglike $Res(k)$ system during the workshop (in preparation). There was a discussion between Stephen Cook, Russell Impagliazzo, Valentine Kabanets and Antonina Kolokolova after Stephen Cook's talk which is leading to an ongoing collaboration on formalizing a more general version of Schwartz-Zippel lemma. Alasdair Urquhart said he made plans to continue collaboration with Oliver Kullmann; he also reported that his conversations with Toni Pitassi about clause learning should result in a joint publication. Another collaboration project was between Sebastian Müller, Jan Johannsen, Moritz Müller and Iddo Tzameret; they have arranged follow-up research visits. Many results presented at the workshop were work in progress and papers in preparations; participants commented on obtaining helpful feedback.

A solution to one of the problems suggested during the panel discussion was solved by a person who was not able to attend, Jan Krajíček, when student participants from the same research group recounted to him the workshop events. A note on this is written and available from Krajíček's website.

References

[1] S. Benabbas, K. Georgiou, A. Magen, M. Tulsiani, Optimal Sherali-Adams Gaps from Pairwise Independence, *APPROX* (2009), 185-194

[2] S. Benabbas, K. Georgiou, A. Magen, M. Tulsiani, SDP Gaps from Pairwise Independence, *(in preparation)*

[3] S. Cook and P. Nguyen, *Logical Foundations of Proof Complexity*, Cambridge University Press, Cambridge, 2010.

[4] Dai Tri Man Le and S. Cook, Formalizing Randomized Matching Algorithms. *LICS* (2011), 185-194

[5] P. Pudlák, Twelve problems in proof complexity, Proc. 3rd International Computer Science Symposium in Russia, CSR (2008), pp.13-27

[6] A. Razborov, Flag algebras, *Journal of Symbolic Logic*, **Vol. 72**, No 4 (2007), pp 1239-1282

[7] A. Urquhart, Width and Size of Regular Resolution Proofs , *(in preparation)*.

[8] Beame, P.; Beck, C., Impagliazzo, R. (2011), Time-Space Tradeoffs in Resolution: Superpolynomial Lower Bounds for Superlinear Space., *Electronic Colloquium on Computational Complexity (ECCC)* **Vol.18** (2011), p.149 .

[9] S.R. Buss, J. Hoffmann, J. Johannsen. Resolution Trees with Lemmas: Resolution Refinements that Characterize DLL-Algorithms with Clause Learning. *Logical Methods in Computer Science* **4** (2008), pp.4–13.

[10] J. Johannsen. An exponential lower bound for width-restricted clause learning, in: Oliver Kullmann (ed.), Theory and Applications of Satisfiability Testing, *12th International Conference SAT 2009*, Springer LNCS **5584** (2009), pp. 128–140

[11] E. Ben-Sasson, J. Johannsen. Lower Bounds for width-restricted clause learning on small width formulas, in: *Ofer Strichman and Stefan Szeider (eds.), Theory and Applications of Satisfiability Testing, 13th International Conference SAT 2010*, Springer LNCS **6175** (2010), pp. 16–29

[12] E. A. Hirsch, D. Itsykson, I. Monakhov, A. Smal. On optimal heuristic randomized semidecision procedures, with applications to proof complexity and cryptography. *Theory of Computing Systems*, 2011 (to appear), DOI 10.1007/s00224-011-9354-3.

[13] E. A. Hirsch, D. Itsykson, V. Nikolaenko, A. Smal. Optimal heuristic algorithms for the image of an injective function. *Notes of Mathematical Seminars of PDMI*, (2012), to appear. Preliminary version appears as *ECCC* TR11-091.

[14] E. A. Hirsch, D. Itsykson. On an optimal randomized acceptor for graph nonisomorphism. *Information Processing Letters* (2011), to appear.

[15] C. Polett, On the Finite Axiomatizability of Prenex R_2^1, *in preparation*

[16] S.R. Buss, L. Kolodziejczyk, N. Thapen, Fragments of approximate counting, *in preparation*

[17] S. Müller and I. Tzameret, Short Propositional Refutations for Dense Random 3CNF formulas, Preliminary version in *Electronic Colloquium on Computational Complexity (ECCC)* **18:6** (2011).

[18] P. Nguyen, Proving soundness for the quantified propositional calculus G_i^*, *submitted*.

[19] E. Ben-Sasson, J. Nordström, Understanding Space in Proof Complexity: Separations and Trade-offs via Substitutions, *Electronic Colloquium on Computational Complexity (ECCC)* **17:125** (2010).

[20] J. Nordström, Pebble Games, Proof Complexity, and Time-Space Trade-offs. *Logical Methods in Computer Science* (2011), to appear.