Proceedings Paper:
Beyersdorff, O and Mueller, S (2010) Different Approaches to Proof Systems. In: Kratochvil, J, Li, A, Fiala, J and Kolman, P, (eds.) Theory and Applications of Models of Computation, 7th Annual Conference, TAMC 2010, Proceedings. 7th Annual Conference, TAMC 2010, 07-11 Jun 2010, Prague, Czech Republic. Springer Verlag , 50 - 59 . ISBN 978-3-642-13561-3

https://doi.org/10.1007/978-3-642-13562-0_6

Different Approaches to Proof Systems

Olaf Beyersdorff[1]* and Sebastian Müller[2]**

[1] Institute of Computer Science, Humboldt University Berlin, Germany
[2] Faculty of Mathematics and Physics, Charles University Prague, Czech Republic
{beyersdo,smueller}@informatik.hu-berlin.de

Abstract. The classical approach to proof complexity perceives proof systems as deterministic, uniform, surjective, polynomial-time computable functions that map strings to (propositional) tautologies. This approach has been intensively studied since the late 70's and a lot of progress has been made. During the last years research was started investigating alternative notions of proof systems. There are interesting results stemming from dropping the uniformity requirement, allowing oracle access, using quantum computations, or employing probabilism. These lead to different notions of proof systems for which we survey recent results in this paper.

1 Introduction

In their seminal paper [CR79], Cook and Reckhow defined the notion of a *proof system* for an arbitrary language L as a polynomial-time computable function f with range L. A string w with $f(w) = x$ is called an *f-proof* for $x \in L$. All classical proof systems like Resolution, Cutting Planes, or Frege systems fall under this general concept, and in the last thirty years there has been great progress in understanding the complexity of proofs in this model (cf. [Seg07] for a recent survey).

While the Cook-Reckhow approach is certainly the most useful setting for practical applications, it is nevertheless interesting to ask what happens if we allow alternative computational resources for the verification of proofs. This approach is very common in complexity theory where besides (non-)deterministic polynomial time a number of other models like randomisation, non-uniformity, oracle access, or new paradigms as quantum computing are studied.

In proof complexity these considerations were started recently by several researchers. In this paper we mainly survey results on proof systems with advice which were introduced by Cook and Krajíček [CK07], but also mention randomised systems investigated by Hirsch and Itsykson [HI10,Hir10] and quantum proof systems introduced by Pudlák [Pud09]. The common idea in these approaches is that verification of proofs can be performed with additional resources,

* This paper was written while the first author was visiting Sapienza University of Rome under support of DFG grant KO 1053/5-2.
** Supported by the Marie Curie FP7 Initial Training Network MALOA (no. 238381).

not just polynomial time. The results show a number of new phenomena such as the existence of optimal proof systems with advice or under weak oracles. Such results are not known in the classical setting. We also address other interesting questions such as the existence of polynomially bounded proof systems—which receives a different characterization in the advice model—and whether proofs can be shortened by using quantum rules.

2 Proof Systems Using Advice

Our first non-classical model will be proof systems that use advice. Like in the classical setting of Karp and Lipton [KL80] this will allow the proof systems to use a specified amount of non-uniform information. Proof systems with advice were recently introduced by Cook and Krajíček [CK07] and further developed by Beyersdorff, Köbler, and Müller [BKM09, BM09, BM].

2.1 Setting the Stage

Our general model of computation for proof systems f with advice is a polynomial-time Turing transducer with several tapes: an input tape containing the proof π, possibly several work tapes for the computation of the machine, an output tape where we output the proven element $f(\pi)$, and an advice tape containing the advice. We start with a quite flexible definition of proof systems with advice for arbitrary languages, generalizing the notion of propositional proof systems with advice from [CK07].

Definition 1 ([BKM09]). *For a function $k : \mathbb{N} \to \mathbb{N}$, a proof system f for L is a* proof system with k bits of advice*, if there exist a polynomial-time Turing transducer M, an advice function $h : \mathbb{N} \to \Sigma^*$, and an advice selector function $\ell : \Sigma^* \to 1^*$ such that*

1. *ℓ is computable in polynomial time,*
2. *M computes the proof system f with the help of the advice h, i.e., for all $\pi \in \Sigma^*$, $f(\pi) = M(\pi, h(|\ell(\pi)|))$, and*
3. *for all $n \in \mathbb{N}$, the length of the advice $h(n)$ is bounded by $k(n)$.*

For a class F of functions, we denote by ps/F the class of all ps/k with $k \in F$.

We say that f *uses k bits of input advice* if ℓ has the special form $\ell(\pi) = 1^{|\pi|}$. On the other hand, in case $\ell(\pi) = 1^{|f(\pi)|}$ for all π in the domain of f, then f is said to *use k bits of output advice*. By this definition, proof systems with input advice use non-uniform information depending on the length of the proof, while proof systems with output advice use non-uniform information depending on the length of the proven formula.

We note that proof systems with advice are a quite powerful concept, as for every language $L \subseteq \Sigma^*$ there exists a proof system for L with only one bit of advice. In contrast, the class of all languages for which proof systems without advice exist coincides with the class of all recursively enumerable languages.

2.2 Polynomially Bounded Proof Systems with Advice

The classical Cook-Reckhow Theorem states that $\mathsf{NP} = \mathsf{coNP}$ if and only if the set of all tautologies TAUT has a polynomially bounded proof system, i.e., there exists a polynomial p such that every tautology φ has a proof of size $\leq p(|\varphi|)$ in the system. Consequently, showing super-polynomial lower bounds to the proof size in propositional proof systems of increasing strength provides one way to attack the P/NP problem. This approach, also known as the Cook-Reckhow program, has lead to a very fruitful research on the length of propositional proofs.

What happens if the proof systems may use advice? Which languages admit polynomially bounded proof systems in this new model? In [BKM09] a complete characterization of this question was given. In particular, there is a tight connection of this problem to the notion of nondeterministic instance complexity. Similarly as Kolmogorov complexity, instance complexity measures the complexity of individual instances of a language [OKSW94]. We now give the definition of nondeterministic instance complexity from [AKMT00].

Definition 2 (Arvind et al. [AKMT00]). *For a set L and a time bound t, the t-time-bounded* nondeterministic instance complexity *of x with respect to L is defined as $nic^t(x : L) = \min\{\, |M| \,:\, M$ is a t-time-bounded nondeterministic machine, $L(M) \subseteq L$, and M decides correctly on $x\,\}$.*

We collect all languages with prescribed upper bounds on the running time and nondeterministic instance complexity in a complexity class.

Definition 3 ([BKM09]). *The complexity class $\mathsf{NIC}[\mathsf{log}, \mathsf{poly}]$ contains all languages L for which there exists a polynomial p such that $nic^p(x : L) \leq O(\log |x|)$ holds for all $x \in \Sigma^*$.*

This class can be strictly placed between familiar non-uniform complexity classes:

Theorem 4 ([BKM09]). $\mathsf{NP} \subsetneq \mathsf{NP}/1 \subsetneq \mathsf{NP}/\mathsf{log} \subsetneq \mathsf{NIC}[\mathsf{log}, \mathsf{poly}] \subsetneq \mathsf{NP}/\mathsf{poly}$.

The classes in Theorem 4 are exactly the classes which in appear in the characterization of polynomially bounded proof systems with advice, as given in Table 1. Quite unusually in complexity theory, all complexity classes appearing in this table are distinct by Theorem 4.

Table 1. Languages with polynomially bounded proof systems

	input advice	output advice	reference
ps/poly	$\mathsf{NP}/\mathsf{poly}$	$\mathsf{NP}/\mathsf{poly}$	[BKM09]
ps/log	$\mathsf{NIC}[\mathsf{log}, \mathsf{poly}]$	NP/log	[BKM09]
$ps/1$	$\mathsf{NIC}[\mathsf{log}, \mathsf{poly}]$	$\mathsf{NP}/1$	[BKM09]
$ps/0$	NP		[CR79]

Concentrating on propositional proof systems (or more generally, on languages from coNP), the picture simplifies a bit because it was shown in [BKM09] that for a language $L \in \mathsf{coNP}$, $L \in \mathsf{NP/log}$ if and only if $L \in \mathsf{NIC}[\mathsf{log}, \mathsf{poly}]$.

It is also natural to ask, how likely these assumptions actually are, i.e., what consequences follow from the assumption that such proof systems exist. For TAUT we obtain a series of collapse consequences of presumably different strength as shown in Table 2.

Table 2. Consequences of the existence of polynomially bounded proof systems (results are from [BKM09])

Assumption *if* TAUT *has a polynomially bounded ...*		**Consequence** *then* PH *collapses to ...*
ps/poly	(input or output advice)	$\mathsf{S}_2^{\mathsf{NP}} \subseteq \Sigma_3^{\mathsf{p}}$
ps/log	(input or output advice)	$\mathsf{P}^{\mathsf{NP}[\mathsf{log}]}$
$ps/O(1)$	(input advice)	$\mathsf{P}^{\mathsf{NP}[\mathsf{log}]}$
$ps/O(1)$	(output advice)	$\mathsf{P}^{\mathsf{NP}[O(1)]} = \mathsf{BH}$
$ps/0$	(no advice)	NP

2.3 Optimal Proof Systems with Advice

Proof systems are compared according to their strength by simulations as introduced in [CR79] and [KP89]. If f and g are proof systems for L, we say that g *simulates* f if there exists a polynomial p such that for all $x \in L$ and f-proofs w of x there is a g-proof w' of x with $|w'| \leq p(|w|)$. If such a proof w' can even be computed from w in polynomial time, we say that g *p-simulates* f. Proof systems f, g which mutually (p-)simulate each other are called *(p-)equivalent*.

A prominent open question posed in [KP89] is whether there exists a strongest proof system, called a *(p-)optimal* proof system, which (p-)simulates all proof systems for L. This question has interesting consequences such as existence of complete languages for promise classes [KMT03, BS09]. Despite a considerable research effort the existence of optimal proof systems is still open (cf. [Hir10] in this volume). Surprisingly, Cook and Krajíček [CK07] have shown that there exists a propositional proof system with one bit of input advice which simulates all classical Cook-Reckhow proof systems. The proof of this result easily generalizes to arbitrary languages L, thus yielding:

Theorem 5 (Cook, Krajíček [CK07], [BKM09]). *For every language L there exists a proof system P with one bit of input advice such that P simulates all ps/log for L. Moreover, P p-simulates all advice-free proof systems for L.*

In contrast, it seems unlikely that we can obtain a similar result for output advice by current techniques (cf. [BM08] were we investigated this problem

for propositional proof systems). The question whether this optimality result can be strengthened to p-optimality (where the simulations are replaced by p-simulations) was also studied in detail in [BM08], with both negative and positive results providing partial answers to the question.

We remark that optimal proof systems are known to imply complete sets for various promise classes [KMT03], and this relation also holds in the presence of advice [BS09]. A related line of research has shown strong time and space hierarchy theorems for randomised and other semantic classes which use advice [FS04, FST05, vMP07, KvM08]. All these results are not known to hold in the classical advice-free setting.

2.4 Proof Systems with Advice and Bounded Arithmetic

Propositional proof systems enjoy a very close relationship to weak arithmetic theories, so-called bounded arithmetic, which in particular yields insight into strong proof systems as Frege systems and their extensions [Kra95]. This connection also holds in the presence of advice, and this, in fact, was the motivation for their introduction in [CK07]. There, Cook and Krajíček investigate Karp-Lipton collapse consequences of the assumption $\mathsf{NP} \subseteq \mathsf{P/poly}$. 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 [KL80]. Subsequently, these collapse consequences have been improved by Köbler and Watanabe [KW98] to $\mathsf{ZPP}^{\mathsf{NP}}$ and by Sengupta and Cai to $\mathsf{S}_2^{\mathsf{p}}$ (cf. [Cai07]). Making the stronger assumption that $\mathsf{NP} \subseteq \mathsf{P/poly}$ is provable in some weak arithmetic theory, Cook and Krajíček obtained stronger collapse consequences, namely to the Boolean hierarchy if the theory is PV (cf. also [Jeř09, BM]).

One important intermediate step towards this result is a surprising trade-off between advice and nondeterminism (which is unlikely to hold without reference to bounded arithmetic):

Theorem 6 (Cook, Krajíček [CK07]). *PV proves $\mathsf{NP} \subseteq \mathsf{P/poly}$ if and only if PV proves $\mathsf{coNP} \subseteq \mathsf{NP}/O(1)$.*

The latter condition can be interpreted as saying that there exists a polynomially bounded proof system using constant advice (and, moreover, the polynomial boundedness in provable in PV). In fact, Cook and Krajíček even exhibit a natural proof system P with advice that is polynomially bounded if PV proves $\mathsf{NP} \subseteq \mathsf{P/poly}$: the system P is an extended Frege system with constant advice.

2.5 Simplifying the Advice

From a practical point of view, proof systems with advice are susceptive to criticism: advice can be arbitrarily complex (even non-recursive) and thus verifying proofs with the help of advice does not form a feasible model to use in practice. The next result shows that for propositional proof systems, logarithmic advice can be replaced by a sparse NP-oracle without increasing the proof length.

Theorem 7 ([BM09]).

1. *Every propositional proof system with logarithmic advice is simulated by a propositional proof system computable in polynomial time with access to a sparse* NP*-oracle.*
2. *Conversely, every propositional proof system computable in polynomial time with access to a sparse* NP*-oracle is simulated by a propositional proof system with logarithmic advice.*

We remark that sparse NP-sets indeed seem to be very weak if used as oracles. For instance, TAUT $\notin \mathsf{NP}^S$ with a sparse NP-oracle S, unless the polynomial hierarchy collapses to its second level [Kad89].

Another simplification of advice was investigated in [BM09]. As we have seen, there are two natural ways to enhance proof systems with advice by either supplying non-uniform information to the proof (input advice) or to the proven formula (output advice). Intuitively, input advice is the stronger model: proofs can be quite long and formulas of the same size typically require proofs of different size. Hence, supplying advice depending on the proof size is not only more flexible, but also results in more advice per formula.

Therefore, shifting the advice from the proof to the formula will result in a simplification of advice. In this direction in was shown in [BM09] that if there exists a proof system with advice with nontrivial upper bounds on the proof lengths, then there is such a proof system with output advice.

3 Probabilistic Proof Systems

We will now turn to the use of probabilism to compute proof systems. Usually, the term "probabilistic proofs" is associated with interactive proof systems like IP or Babai's Arthur-Merlin classes MA and AM. Besides from randomisation, the power of these proof systems stems from using interaction between a powerful prover and a polynomial-time verifier.

A non-interactive model of randomized proofs was very recently introduced by Hirsch and Itsykson [HI10]. They define two concepts: heuristic acceptors and heuristic proof systems. Acceptors are not really proof systems, but algorithms which accept all elements from the language and do not stop on other inputs. There is, however, a close relationship between acceptors and proof systems (cf. [KP89]). As there is a nice survey on optimal acceptors and optimal proof systems in this volume [Hir10], we will be very brief on this randomized model.

For the randomized approach, we have to consider a probability distribution. A distribution D is concentrated on some set A, if $\mu_D(A) = 1$.

Definition 8 (Hirsch, Itsykson [HI10]). *A pair (D, L) is a* distributional proving problem *if D is a family of probability distributions D_n concentrated on $\overline{L} \cap \{0,1\}^n$.*

Hirsch and Itsykson define a *heuristic acceptor* for a distributional proving problem (D, L) as a randomized algorithm which always accepts inputs from L

and accepts inputs from $\bar{L}$ only with small probability (see [Hir10] for the exact definition). For this model they show an optimality result:

Theorem 9 (Hirsch, Itsykson [HI10]). *Let L be recursively enumerable and D be a polynomial-time samplable distribution. Then there exists an optimal automatizer for (D, L).*

The authors also consider heuristic proof systems and show interesting results on these systems with respect to automatizability, i. e., the problem to construct proofs for given formulas (see [Hir10]).

4 Quantum Proof Systems

As our last model we briefly mention quantum proof systems as introduced by Pudlák [Pud09]. Since Shor's polynomial-time quantum algorithm for factoring [Sho97], quantum computations are a computational model which has attracted an enormous amount of research. Recently, Pudlák investigated the usage of quantum rules in propositional proof systems [Pud09].

Pudlák first introduces a general model of quantum proof systems and then focuses on quantum Frege systems. Let us start with the general concept.

Definition 10 (Pudlák [Pud09]). *A* quantum proof system *consists of a set $A \subseteq \Sigma^*$ (the set of valid proofs) and a family of circuits C_n (the proof system) such that*

1. *A is decidable in polynomial time and C_n is* P*-uniform* (Efficiency)*;*
2. *for any proof $\pi \in A$, $C_{|\pi|}(\pi)$ produces a superposition of strings of tautologies* (Correctness)*;*
3. *for every tautology φ there exists $\pi \in A$ such that φ occurs in the superposition of $C_{|\pi|}(\pi)$* (Completeness)*.*

Regarding the completeness condition, it is also important that by measuring $C_{|\pi|}(\pi)$ we can obtain φ with a probability which is not too small. Hence quantum proof systems also have probabilistic aspects.

The next concept which Pudlák introduces are *quantum rules* which are based on unitary transformations. Using a finite set of quantum rules, Pudlák arrives at the notion of *quantum Frege systems*. Comparing quantum Frege with classical Frege systems, Pudlák obtains the surprising result that quantum Frege systems do not have shorter proofs, i. e., every quantum Frege system is simulated by a classical Frege system. On the other hand, it does not seem possible to extract classical proofs from quantum Frege proofs, i. e., under cryptographic assumptions quantum Frege systems are not p-simulated by classical Frege systems.

5 Conclusion

We conclude by mentioning that there are more interesting approaches which we did not cover in this survey. For instance, *space complexity* for proof systems was

intensively investigated in the context of Resolution [ET01, ABSRW02, BSN08]. Here the minimal space to refute a set of clauses is of particular interest as it corresponds to the memory consumption of modern SAT solvers which often combine DPLL algorithms with clause learning. Therefore, both lower bounds for Resolution space [ABSRW02,BSG03,EGM04,ET03] as well as optimal trade-offs between space and length, i. e., between memory and run-time consumption, have been intensively studied [Nor06, NH08, BSN08, BSN09].

Another approach is to provide a finer analysis of proof lengths in the model of *parameterized proof complexity*. Parameterized resolution and, moreover, a general framework for parameterized proof complexity was recently introduced by Dantchev, Martin, and Szeider [DMS07]. In that paper, Dantchev et al. show a complexity gap in parameterized tree-like resolution for propositional formulas arising from translations of first-order principles. A purely combinatorial approach to obtain lower bounds to the proof size in parameterized tree-like resolution was developed in [BGL10].

Of course, non-classical proof complexity is still a relatively young area of research and many problems are still open. In particular, it is interesting to determine the relationship between the different approaches (e. g. with respect to simulations as in Theorem 7). We believe that further research into non-classical measures of proofs will both strengthen the connections between computational and proof complexity and lead to new insights for classical proof systems.

References

[ABSRW02] Michael Alekhnovich, Eli Ben-Sasson, Alexander A. Razborov, and Avi Wigderson. Space complexity in propositional calculus. *SIAM Journal on Computing*, 31(4):1184–1211, 2002.

[AKMT00] V. Arvind, Johannes Köbler, Martin Mundhenk, and Jacobo Torán. Nondeterministic instance complexity and hard-to-prove tautologies. In *Proc. 17th Symposium on Theoretical Aspects of Computer Science*, volume 1770 of *Lecture Notes in Computer Science*, pages 314–323. Springer-Verlag, Berlin Heidelberg, 2000.

[BGL10] Olaf Beyersdorff, Nicola Galesi, and Massimo Lauria. The strength of parameterized tree-like resolution. Preprint, 2010.

[BKM09] Olaf Beyersdorff, Johannes Köbler, and Sebastian Müller. Nondeterministic instance complexity and proof systems with advice. In *Proc. 3rd International Conference on Language and Automata Theory and Applications*, volume 5457 of *Lecture Notes in Computer Science*, pages 164 – 175. Springer-Verlag, Berlin Heidelberg, 2009.

[BM] Olaf Beyersdorff and Sebastian Müller. A tight Karp-Lipton collapse result in bounded arithmetic. *ACM Transactions on Computational Logic*. To appear.

[BM08] Olaf Beyersdorff and Sebastian Müller. A tight Karp-Lipton collapse result in bounded arithmetic. In *Proc. 17th Annual Conference on Computer Science Logic*, volume 5213 of *Lecture Notes in Computer Science*, pages 199 – 214. Springer-Verlag, Berlin Heidelberg, 2008.

[BM09] Olaf Beyersdorff and Sebastian Müller. Does advice help to prove propositional tautologies? In *Proc. 12th International Conference on Theory and Applications of Satisfiability Testing*, volume 5584 of *Lecture Notes in Computer Science*, pages 65 – 72. Springer-Verlag, Berlin Heidelberg, 2009.

[BS09] Olaf Beyersdorff and Zenon Sadowski. Characterizing the existence of optimal proof systems and complete sets for promise classes. In *Proc. 4th International Computer Science Symposium in Russia*, volume 5675 of *Lecture Notes in Computer Science*, pages 47 – 58. Springer-Verlag, Berlin Heidelberg, 2009.

[BSG03] Eli Ben-Sasson and Nicola Galesi. Space complexity of random formulae in resolution. *Random Structures and Algorithms*, 23(1):92–109, 2003.

[BSN08] Eli Ben-Sasson and Jakob Nordström. Short proofs may be spacious: An optimal separation of space and length in resolution. In *Proc. 49th IEEE Symposium on the Foundations of Computer Science*, pages 709–718, 2008.

[BSN09] Eli Ben-Sasson and Jakob Nordström. Understanding space in resolution: Optimal lower bounds and exponential trade-offs. Technical Report TR09-034, Electronic Colloquium on Computational Complexity, 2009.

[Cai07] Jin-Yi Cai. $S_2^p \subseteq ZPP^{NP}$. *Journal of Computer and System Sciences*, 73(1):25–35, 2007.

[CK07] Stephen A. Cook and Jan Krajíček. Consequences of the provability of NP $\subseteq$ P/poly. *The Journal of Symbolic Logic*, 72(4):1353–1371, 2007.

[CR79] Stephen A. Cook and Robert A. Reckhow. The relative efficiency of propositional proof systems. *The Journal of Symbolic Logic*, 44(1):36–50, 1979.

[DMS07] Stefan S. Dantchev, Barnaby Martin, and Stefan Szeider. Parameterized proof complexity. In *Proc. 48th IEEE Symposium on the Foundations of Computer Science*, pages 150–160, 2007.

[EGM04] Juan Luis Esteban, Nicola Galesi, and Jochen Messner. On the complexity of resolution with bounded conjunctions. *Theoretical Computer Science*, 321(2–3):347–370, 2004.

[ET01] Juan Luis Esteban and Jacobo Torán. Space bounds for resolution. *Information and Computation*, 171(1):84–97, 2001.

[ET03] Juan Luis Esteban and Jacobo Torán. A combinatorial characterization of treelike resolution space. *Information Processing Letters*, 87(6):295–300, 2003.

[FS04] Lance Fortnow and Rahul Santhanam. Hierarchy theorems for probabilistic polynomial time. In *Proc. 45th IEEE Symposium on the Foundations of Computer Science*, pages 316–324, 2004.

[FST05] Lance Fortnow, Rahul Santhanam, and Luca Trevisan. Hierarchies for semantic classes. In *Proc. 37th ACM Symposium on Theory of Computing*, pages 348–355, 2005.

[GMR89] O. Goldreich, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof systems. *SIAM Journal on Computing*, 18(2):186–208, 1989.

[HI10] Edward A. Hirsch and Dmitry Itsykson. On optimal heuristic randomized semidecision procedures, with application to proof complexity. In *Proc. 27th Symposium on Theoretical Aspects of Computer Science*, pages 453–464, 2010.

[Hir10] Edward A. Hirsch. Optimal acceptors and optimal proof systems. In *Proc. 7th Conference on Theory and Applications of Models of Computation*. Springer-Verlag, Berlin Heidelberg, 2010.

[Jeř09] Emil Jeřábek. Approximate counting by hashing in bounded arithmetic. *Journal of Symbolic Logic*, 74(3):829–860, 2009.

[Kad89] J. Kadin. $P^{NP[\log n]}$ and sparse Turing-complete sets for NP. *Journal of Computer and System Sciences*, 39:282–298, 1989.

[KL80] Richard M. Karp and Richard J. Lipton. Some connections between nonuniform and uniform complexity classes. In *Proc. 12th ACM Symposium on Theory of Computing*, pages 302–309. ACM Press, 1980.

[KMT03] Johannes Köbler, Jochen Messner, and Jacobo Torán. Optimal proof systems imply complete sets for promise classes. *Information and Computation*, 184(1):71–92, 2003.

[KP89] Jan Krajíček and Pavel Pudlák. Propositional proof systems, the consistency of first order theories and the complexity of computations. *The Journal of Symbolic Logic*, 54(3):1063–1079, 1989.

[Kra95] Jan Krajíček. *Bounded Arithmetic, Propositional Logic, and Complexity Theory*, volume 60 of *Encyclopedia of Mathematics and Its Applications*. Cambridge University Press, Cambridge, 1995.

[KvM08] Jeff Kinne and Dieter van Melkebeek. Space hierarchy results for randomized models. In *Proc. 25th Symposium on Theoretical Aspects of Computer Science*, pages 433–444, 2008.

[KW98] Johannes Köbler and Osamu Watanabe. New collapse consequences of NP having small circuits. *SIAM Journal on Computing*, 28(1):311–324, 1998.

[NH08] Jakob Nordström and Johan Håstad. Towards an optimal separation of space and length in resolution. In *Proc. 40th ACM Symposium on Theory of Computing*, pages 701–710, 2008.

[Nor06] Jakob Nordström. Narrow proofs may be spacious: separating space and width in resolution. In *Proc. 38th ACM Symposium on Theory of Computing*, pages 507–516, 2006.

[OKSW94] P. Orponen, K. Ko, U. Schöning, and O. Watanabe. Instance complexity. *Journal of the ACM*, 41(1):96–121, 1994.

[Pud09] Pavel Pudlák. Quantum deduction rules. *Annals of Pure and Applied Logic*, 157(1):16–29, 2009.

[Seg07] Nathan Segerlind. The complexity of propositional proofs. *Bulletin of Symbolic Logic*, 13(4):417–481, 2007.

[Sho97] Peter Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997.

[vMP07] Dieter van Melkebeek and Konstantin Pervyshev. A generic time hierarchy with one bit of advice. *Computational Complexity*, 16(2):139–179, 2007.