

Research Statement

Sebastian Müller
Faculty of Mathematics and Physics
Charles University, Prague
muller@karlin.mff.cuni.cz

I am mainly interested in the development of methods from pure mathematics and their application to applied fields, especially computer science. This, in particular, comprises an interest in Proof Complexity, Bounded Arithmetic, Complexity Theory and their interconnection. This connection is manifold and lead to some classical areas, such as arithmetic and parts of model theory, more and more becoming focal points of investigation with respect to efficiency in computation.

One of the main reasons for the success of mathematical logic in the early 20th century probably was the rising interest, not least due to Hilbert's Program, in whether mathematics is sound, i.e. whether a mathematical proof only proves true statements. Since Kurt Gödel's seminal work "Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I" [12] it is well known that we cannot reason about this question in any strong enough formal system of mathematics. This was a serious setback for Hilbert's program. However we know that for certain weak fragments of mathematics we can define a sound reasoning system. One of which is a propositional proof system, as introduced by Cook and Reckhow [9], which is any polynomial-time computable function P on binary strings that has TAUT, the set of all propositional tautologies, as its range. A P -proof of a given tautology φ is simply any element of the domain that is mapped via P to φ . Via well known translations this means that we are able to prove mathematical statements that talk about elements which are bounded by some polynomial. Once we know that everything is provable in such a setting a natural question is: How efficient is such a proof? Things may well be provable, but the proof might be so long that it will be unlikely to be found. This is one of the main questions in Proof Complexity and has close connections to the famous $P = NP$ problem in Computational Complexity.

More precisely it relates to the question, whether coNP equals NP , that is, whether every problem that can efficiently be solved by a Turing machine that perfectly guesses witnesses can also efficiently be solved by a Turing machine that perfectly guesses counterexamples, and vice versa. It is well known that the set TAUT of all propositional tautologies is coNP -complete. Thus, the question whether there exists a propositional proof system P in which short proofs for all tautologies can be found is equivalent to whether $\text{NP} = \text{coNP}$.

Past Research In [8] Cook and Krajíček proposed propositional proof systems that have access to nonuniform information, so called advice. This is a natural concept if one assumes a proof system not being computed by a Turing machine, but by circuits, and corresponds to these circuits being nonuniformly constructed. They showed that some resulting proof systems are very strong in comparison to standard ones, as they simulate every existing standard proof system. They explicitly showed that if such a system is polynomially bounded, i.e. has short proofs for all tautologies, and this property is provable in a weak arithmetic, then the polynomial hierarchy PH collapses, provably in the same theory. In [5] Olaf Beyersdorff and I showed that actually equivalence holds between a provable collapse of the hierarchy and the provable existence of polynomially bounded nonuniform proof systems. We did this by exploiting that a trade-off between nondeterminism and nonuniformity exists with respect to provability in weak arithmetic. This trade-off is unlikely to hold in the general case but allowed us to use a result by Buhrmann, Chang and Fortnow [7] to conclude the equivalence of a collapse of the polynomial hierarchy and having short nonuniform

propositional proofs. This is interesting as it shows that the close connection between propositional proof systems and the $P = NP$ problem is not entirely lost, when we allow ourselves stronger variants of proof systems. This might also be a path of proving a collapse of PH to a higher level, yet being able to use stronger tools for creating algorithms.

In a series of subsequent papers (see [4] for a synopsis) together with Johannes Köbler we pinpointed the computational strength that corresponds to such proof systems with different strengths of nonuniformity. To investigate this question we deviated from the classical definition of propositional proof system and considered any language L as a possible range. As an interesting special case we obtained for propositional proofs that, no matter how strong we choose the nonuniformity to be (up to polynomial size), we still got nontrivial collapse consequences for the polynomial hierarchy.

Current Research Recently I took a stronger focus on very weak arithmetic theories and provability in that framework. Together with Iddo Tzameret, in [15] we transferred a recent spectral argument of Feige, Kim and Ofek [10] to \mathbf{VTC}^0 , an arithmetic theory that only allows for very weak arithmetic computations and includes a parity predicate for bounded sets. This theory is in close connection to the circuit class \mathbf{TC}^0 of constant depth polynomial circuits with parity gates. With this argument at hand we could conclude that certain random 3DNF's are efficiently provable in a proof system that comprises some parity predicate. It implied a separation between Resolution, probably the most used proof system, and \mathbf{TC}^0 -Frege, which is still weaker than Frege, on a random set of instances. This result was a little surprising as reasoning about eigenvalues in matrices is perceived as being only doable in \mathbf{NC}^1 a provably stronger class of circuits. We exploited some nondeterminism in the construction of the circuits to provide the additional information needed to carry out the argument of Feige, Kim and Ofek. This, presumably, will not be possible with all spectral arguments.

I am currently working on a model-theoretic approach to reason about simulations between propositional proof systems. In [14] I took a model of a weak arithmetic theory T and focussed on an initial segment of it. Intuitively this segment, if small enough, should be model of a stronger theory than T , as the arithmetic allows for stronger induction on its small elements. I was able to verify this intuition for certain T by proving a version of Nepomnjascij's Theorem [16] in the initial segment. That theorem connects computability with definability in the model and so, using a standard evaluation algorithm for formulas, it showed that evaluations of such formulas existed in the initial segment. It is known that these do not exist for all formulas in the big model. This generalized a result by Paris and Wilkie [17],[18] and implied a recent result by Filmus, Pitassi and Santhanam [11]. It also implies that the separation result from [15] extends, in a weaker form, to bounded depth Frege systems. Additionally, this creates a very interesting perspective of how to view simulations between propositional proof systems which I am investigating further.

Future Research As just mentioned, I aim to extend the results of [14]. An interesting start would be to have the big structure model a weaker base theory. Depending on the strength of the theory in the initial segment this yields different simulation properties between weak proof systems, ultimately getting results for a stronger version of Resolution. The next step I would like to do is to prove the correctness of the Diffie-Hellman Key Exchange protocol in such a cut. Applying results from Atserias and Bonnet [2] and arguing as Krajíček and Pudlák in [13] or Bonnet, Pitassi, Raz [6] this would allow the conclusion that Resolution is not essentially automatizable, i.e. that there is no efficient algorithm producing proofs for this or any stronger proof system. This would be a very interesting result as Resolution seems to be the weakest reasonable propositional proof system and its non-automatizability is so far only known under strong complexity theoretic assumptions (see Aleknovich and Razborov [1]) and this result does not generalize to stronger systems.

Another line of research I have an interest in, is the connection between games on structures and their descriptive complexity. I visited Stephan Kreutzer in Berlin this Summer and we started to work on such games and their connection to various graph properties. There is an interesting connection between Σ_1^B - and Δ_1^B -definability in weak arithmetics and computability in NP and P, respectively. That is, if the methods used to prove that some language is in $\text{coNP} \cap \text{NP}$ can be formalized in weak arithmetic, then the language is already in P. Moreover this is provable in the weak theory. I would be interested to apply that sort of reasoning to parity games, a class of games played on graphs that are of central interest in model checking and in finite model theory in general. There has been work by Beckmann and Moller [3] in this direction, but unfortunately it fell short of achieving its main goal. We want to try to understand Parity Games from a parameterized point of view. Therefore, I would like to develop a theory, building on Sam Buss' S_2^1 , that coincides with FPT, and we then would like to apply arguments similar to those in [3] to parameterized Parity Games, once we come up with a promising characterization.

Finally, on the long run, I would like to investigate the influence of probability to the verification or construction of proofs in propositional proof systems. This could be very interesting, as there are strong trade-offs between probability and nondeterminism, as for example is observed in the famous PCP Theorem, and so far there has been not much research in that direction, but I think it might well be worth investigating it.

REFERENCES

1. M. Alekhovich and A. A. Razborov Resolution is Not Automatizable Unless $W[P]$ is Tractable *Proceedings of the 42nd IEEE Symposium on FOCS*, 2001, pp. 210-219.
2. A. Atserias and M. L. Bonet. On the Automatizability of Resolution and Related Propositional Proof Systems. *Information and Computation*, Vol. **189**(2), 2004, pp. 182-201.
3. A. Beckmann and F. Moller On the Complexity of Parity Games. *Proceedings of Visions of Computer Science*, 2008, pp. 237-247.
4. O. Beyersdorff, J. Köbler and S. Müller. Proof Systems that take Advice. *Information and Computation*, Vol. **209**(3), 2011, pp. 320-332.
5. O. Beyersdorff and S. Müller. A Tight Karp-Lipton Collapse Result in Bounded Arithmetic. *Transactions of Computational Logic*, Vol. **11**(4), 2010.
6. M.L. Bonet, T. Pitassi, and R. Raz. On interpolation and automatization for Frege systems. *SIAM Journal of Computing*, Vol. **29** (6), 2000, pp. 1939-1967.
7. H. Buhrman, R. Chang, and L. Fortnow. One bit of advice. In *Proc. 20th Symposium on Theoretical Aspects of Computer Science*, 2003, pp. 547-558.
8. S. A. Cook and J. Krajíček. Consequences of the provability of $NP \subseteq P/poly$. *The Journal of Symbolic Logic*, Vol. **72**(4), 2007, pp. 1353-1371.
9. S. Cook and R. Reckhow. The Relative Efficiency of Propositional Proof Systems. *Journal of Symbolic Logic*, Vol. **44**(1), 1979, pp.36-50.
10. U. Feige, J. H. Kim, and E. Ofek. Witnesses for non-satisfiability of dense random 3CNF formulas. *Proceedings of the IEEE 47th Annual Symposium on Foundations of Computer Science*, 2006.
11. Y. Filmus, T. Pitassi, and R. Santhanam. Exponential Lower Bounds for AC-Frege Imply Superpolynomial Frege Lower Bounds. *Proceedings ICALP*, Vol. **1**, 2011, pp.618-629.
12. K. Gödel. Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I. *Monatshefte für Mathematik und Physik*, Vol. **38**, 1931, pp. 173-198.
13. J. Krajíček and P. Pudlák. Some Consequences of Cryptographical Conjectures for S_2^1 and EF. *Information and Computation*, Vol. **140** (1), 1998, pp.82-94.
14. S. Müller. Polylogarithmic Cuts in Models of V^0 . Manuscript, 2012.
15. S. Müller and I. Tzameret. Short Propositional Refutations for Dense Random 3CNF Formulas. Manuscript, 2011.
16. V.A. Nepomnjascij. Rudimentary Predicates and Turing Calculations. *Doklady AN SSSR*, Vol. **195**, 1970.
17. J. Paris and A. Wilkie. Counting Problems in Bounded Arithmetic. *Methods in Mathematical Logic*, LNM **1130**, 1985, pp.317-340.
18. J. Paris and A. Wilkie. Counting Δ_0 Sets. *Fundamenta Mathematica*, Vol. **127**, 1987, pp.67-76.