

Logical strength of complexity theory and a formalization of the PCP theorem in bounded arithmetic

Ján Pich

Department of Algebra, Faculty of Mathematics and Physics, Charles University in Prague, Sokolovská 83, Prague, CZ-186 75, The Czech Republic

Abstract. The aim of this presentation is to show that a lot of complexity theory can be formalized in low fragments of arithmetic like Cook's theory PV_1 .

Our motivation is to demonstrate the power of bounded arithmetic as a counterpart to the unprovability results we already have or want to obtain, and generally to find out how complexity theory behaves in different worlds of bounded arithmetic.

Concerning the unprovability results, in [8] it is proven that under certain hardness assumptions theory T_{NC^1} , the true universal first-order theory in the language containing names for all uniform NC^1 algorithms, cannot prove polynomial circuit lower bounds on SAT formalized as a sentence $LB(SAT, n^k)$. In fact, the result generalizes basically to any theory weaker than PV_1 in terms of provably total functions.

The question whether PV_1 proves $LB(SAT, n^k)$ remains open even if we allow standard complexity-theoretic assumptions and it can be seen as a weaker form of Razborov's proof complexity conjecture about NW-generators, cf. [9].

Generally, it would be interesting to arrive at a complexity-theoretic statement, not necessarily circuit lower bounds, whose provability in PV_1 unexpectedly breaks some natural hypothesis. To understand better what are plausible candidates for such statements it might help to investigate the theorems provable in low fragments of arithmetic.

Many classical theorems from complexity theory have been already formalized in bounded arithmetic. In the table closing this abstract we tried to list some representative results but it should be understood that they come with a lot of other theorems that are formalizable too in a similar fashion. In fact, some of the formalizations are so evident that they are used without a proof as a folklore, e.g. Cook-Levin's theorem in PV_1 .

The technical contribution of our presentation is a formalization of the exponential PCP theorem in the theory APC_1 and the PCP theorem in the theory $PV_1 + \Pi_1^b$ -LLIND. Perhaps the most challenging part here was to formalize properties of (n, d, λ) -graphs needed to derive the PCP theorem in $PV_1 + \Pi_1^b$ -LLIND. These are usually obtained using algebraic techniques involving norms over real vector spaces coming all the way down to the fundamental theorem of algebra etc. In order to avoid formalization of this machinery, we employ certain approximations to derive

slightly weaker properties of (n, d, λ) -graphs which, however, suffice to derive the PCP theorem.

Theory	Theorem	Reference
PV_1	Cook-Levin's theorem	*
$PV_1 + \Pi_1^b$ -LLIND	the PCP theorem	*
	(n, d, λ) -graphs	*
$PV_1 + WPHP(PV_1)$	$\text{PARITY} \notin AC^0$	[7]
APC_1	BPP, ZPP, AM,...	[5]
	Goldreich-Levin's theorem	[2]
	the exponential PCP theorem	*
$HARD_\epsilon$	Impagliazzo-Wigderson derandomiz.	[4]
$HARD^A$	Nisan-Wigderson's derandomization	[3]
$T_2^1 + rWPHP(PV_2)$	$S_2^P \subseteq ZPP^{NP}$	[6]
APC_2	Graph isomorphism in coAM	[6]
$APC_2^{\oplus p^P}$	Toda's theorem	[1]

* means that the result is shown in this presentation.

References

1. Buss S.R., Kolodziejczyk L.A., Zdanowski K.; Collapsing Modular Counting in Bounded Arithmetic and Constant Depth Propositional Proofs, preprint, 2012.
2. Dai Tri Man Le; Bounded arithmetic and formalizing probabilistic proofs, Ph.D. thesis, University of Toronto, 2014.
3. Jeřábek E.; Dual weak pigeonhole principle, Boolean complexity and derandomization, Annals of Pure and Applied Logic, pp. 1-37, 2004.
4. Jeřábek E.; Weak pigeonhole principle, and randomized computation; Ph.D. thesis, Faculty of Mathematics and Physics, Charles University, Prague, 2005.
5. Jeřábek E.; Approximate counting in bounded arithmetic, Journal of Symbolic Logic, pp. 959-993, 2007.
6. Jeřábek E.; Approximate counting by hashing in bounded arithmetic, Journal of Symbolic Logic, pp. 829-860, 2009.
7. Krajíček J.; Bounded arithmetic, propositional logic, and complexity theory, Cambridge University Press, 1995.
8. Pich J., Circuit lower bounds in bounded arithmetics, preprint, 2013.
9. Razborov A., Pseudorandom Generators Hard for k-DNF Resolution and Polynomial Calculus, people.cs.uchicago.edu/~razborov/files/res_k.pdf, 2002-2003.