POLYLOGARITHMIC CUTS IN MODELS OF WEAK ARITHMETIC

SEBASTIAN MÜLLER

In Proof Complexity one regards propositional proof systems, such as propositional Frege systems or Resolution, in a general concept as poly-time functions P that map any string π (the P-proof) to a tautology φ (the proven formula), such that for every tautology there is a proof (i.e. the system is complete). The main question is, whether there exists such a function P, such that for every tautology φ there exists a short (i.e. polynomial in $|\varphi|$) proof in P for it. As the set of propositional tautologies is NP-complete, this is equivalent to whether coNP = NP.

After a brief introduction into Proof Complexity, Bounded Arithmetic and their interconnection I intend to discuss a model-theoretic approach to answer some open questions in this field. To this end, I will introduce the notion of a polylogarithmic cut, a model that only contains a small fragment of a larger model of arithmetic. Intuitively, such cuts are models of a stronger theory. This intuition is at least sometimes justified as we will see the following

Theorem 1. *Let $N \models \mathbf{V^0}$ and $M \subseteq N$ be the polylogarithmic cut. Then $M \models \mathbf{VNC^1}$.*

From this result various results in Proof Complexity straightforwardly follow. For example the following recent simulation result by Filmus, Pitassi and Santhanam follows directly from Theorem 1 by a simple calculation and the application of the Reflection Principle for Frege.

Theorem 2 ([2])**.** *Every Frege system is sub exponentially simulated by AC^0-Frege systems.*

Also, from a recent result of Tzameret and me, we can straightforwardly conclude the following separation theorem between Resolution and AC^0-Frege. To this end first observe that by a result from Chvátal and Szemerédi [1] Resolution does not admit subexponential proofs of random 3CNF with a variable density below $n^{1.5-\epsilon}$. The separation then follows from the following theorem, which is an easy corollary of the main result from [3] and Theorem 1.

Theorem 3. *For almost every random 3CNF A with n variables and $m = c \cdot n^{1,4}$ clauses, where c is a large constant, $\neg A$ has subexponentially bounded AC^0-Frege proofs.*

I will try to motivate these results and then discuss some interesting lines for further research. One such direction might be to consider oth[illegible]