Forcing with random variables and proof complexity

Jan Krajíček

[1] Mathematical Institute, Academy of Sciences, Prague
[2] Faculty of Mathematics and Physics, Charles University, Prague

A fundamental problem about the strength of non-deterministic computations is the problem whether the complexity class $\mathcal{NP}$ is closed under complementation. The set $TAUT$ (w.l.o.g. a subset of $\{0,1\}^*$) of propositional tautologies (in some fixed, complete language, e.g. DeMorgan language) is co$\mathcal{NP}$-complete. The above problem is therefore equivalent to asking if there is a non-deterministic polynomial-time algorithm accepting exactly $TAUT$.

Cook and Reckhow (1979) realized that there is a suitably general definition of propositional proof systems that encompasses traditional propositional calculi but links naturally with computational complexity theory. Namely, a propositional proof system is defined to be a binary relation (on $\{0,1\}^*$) $P(x,y)$ decidable in polynomial time such that $x \in TAUT$ iff $\exists y, P(x,y)$. Any y such that $P(x,y)$ is called a P-proof of x.

It is easy to see (viz Cook and Reckhow (1979)) that the fundamental problem becomes a lengths-of-proofs question: Is there a propositional proof system in which every tautology admits a proof whose length is bounded above by a polynomial in the length of the tautology?

Proving lower bounds for particular propositional proof systems appears rather difficult. For example, no non-trivial lower bounds are known even for the ordinary text-book calculus based on a finite number of axiom schemes and inference rules (a Frege system in the terminology of Cook and Reckhow (1979)).

Proof complexity applies methods from logic, from finite combinatorics, from complexity theory (in particular, from circuit complexity, communication complexity, cryptography, or derandomization), from classical algebra (field theory or representation theory of groups), and even borrows abstract geometrical concepts like Euler characteristic or Grothendieck ring.

However, the most stimulating for proof complexity are its multiple connections to bounded arithmetic. In particular, the task of proving lower bounds (for any particular proof system) is equivalent to the task of constructing suitably non-elementary extensions of models of a bounded arithmetic theory (the theory in question depends on the proof system we want lower bounds for). Most lower bounds can be explained very naturally as constructions of such extensions (and some of the most treasured ones were discovered in this way).

In particular, models M to be extended are cuts in models of true arithmetic (they can be "explicitly" obtained as bounded ultrapowers of $\mathbf{N}$). Extensions N of M we are after should preserve polynomial-time properties but should not be elementary w.r.t. $\mathcal{NP}$-properties. There are two things going against each other: Under how fast functions is M closed and how strong theory model N satisfies.

The former issue influences the rate of the lower bound deduced, the latter one the strength of the proof system for which it is proved.

I shall describe a new method for constructing these extensions. The models are Boolean-valued and are formed by random variables.

References

1. Cook, S. A., and Reckhow, R. A.: The relative efficiency of propositional proof systems. J. Symbolic Logic **44(1)** (1979) 36–50
2. Krajíček, J.: *Bounded arithmetic, propositional logic, and complexity theory.* Encyclopedia of Mathematics and Its Applications, Vol. **60**, Cambridge University Press, (1995)
3. Krajíček, J.: Forcing with random variables. A draft of lecture notes available at `http://www.math.cas.cz/~krajicek`