

► JAN KRAJÍČEK,

Towards hard tautologies.

Faculty of Mathematics and Physics, Charles University, Sokolovská 83, Prague, 186 75, Czech Republic.

E-mail: krajicek@karlin.mff.cuni.cz.

A proof system for propositional logic is a polynomial time map P whose range is exactly the set of propositional tautologies (Cook and Reckhow [1]). Any string w for which $P(w) = \tau$ is called a P -proof of formula τ . A proof system P is p -bounded if all tautologies admit a P -proof of the length bounded by a fixed polynomial in the length of the tautology. Cook and Reckhow [1] noted that a p -bounded proof system exists if and only if the class NP is closed under complementation.

It is expected that no p -bounded proof system exists and it is a fundamental problem to prove this conjecture. This amounts to demonstrating super-polynomial lengths-of-proofs lower bounds for all proof systems. Such lower bounds were established for a variety of proof systems but all of them are weaker than the usual text-book propositional calculus based on a finite number of axiom schemes and inference rules, cf.[2].

A key issue in any lower bound proof is to come up with plausible candidate hard tautologies. For weaker systems such hard tautologies encode various combinatorial principles (e.g. the pigeonhole principle) but for stronger systems no combinatorial constructions were proposed. I shall expose a recent theory of proof complexity generators describing a class of possibly hard tautologies, cf. [3, Chpts.29 and 30].

[1] S. A. COOK and R. A. RECKHOW, *The relative efficiency of propositional proof systems* **Journal of Symbolic Logic**, vol. 44, no. 1, 1979, pp. 36–50.

[2] J. KRAJÍČEK, *Proof complexity*, **European congress of mathematics**(Stockholm), (Ari Laptev editor), European Mathematical Society, 2005, pp. 221–231.

[3] ———, **Forcing with random variables and proof complexity**, London Mathematical Society Lecture Notes, Cambridge University Press, to appear.