Title: Complexity Theory in Feasible Mathematics

Author: Ján Pich

Department: Department of Algebra

Supervisor: Prof. RNDr. Jan Krajíček, DrSc., MAE

Abstract: We study the provability of statements and conjectures from Complexity Theory in Bounded Arithmetic. First, modulo a hardness assumption, we show that theories weaker in terms of provably total functions than Buss's theory S^1_2 cannot prove n^k-size circuit lower bounds for SAT formalized as a Σ^b_2-formula $LB(SAT, n^k)$. In particular, the true universal first-order theory in the language containing names for all uniform NC^1 algorithms denoted T_{NC^1} does not prove $LB(SAT, n^{4kc})$ where $k \geq 1, c \geq 2$ unless each function $f \in SIZE(n^k)$ can be approximated by formulas F_n of subexponential size $2^{O(n^{1/c})}$ with subexponential advantage: $P_{x\in\{0,1\}^n}[F_n(x) = f(x)] \geq 1/2 + 1/2^{O(n^{1/c})}$. Unconditionally, V^0 does not prove quasipolynomial $n^{\log n}$-size circuit lower bounds for SAT. Considering upper bounds, we prove the PCP theorem in Cook's theory PV_1. This includes a formalization of the (n, d, λ)-graphs in PV_1. A consequence of the result is that Extended Frege proof system admits p-size proofs of tautologies encoding the PCP theorem.

Keywords: Circuit Lower Bounds, Bounded Arithmetic, The PCP theorem