Institute of Mathematics of the AS CR, v.v.i.
Žitná 25, 115 67 Praha 1
Czech Republic

Prague, October 6, 2023

Report of the advisor on Erfan Khaniki's thesis *(Im)possibility results in Proof Complexity and Arithmetic.*

Erfan Khaniki contacted me already during his master studies in Tehran. He briefly visited our institute and he worked on problems that I suggested to him. None of these results are covered in his PhD thesis, although the thesis is mostly from the same area of research. After graduating he came to Prague to doctoral studies and was partially supported from one of our department grants. During his doctoral studies we communicated a lot, and it was a pleasure to talk to him, but he was one of the ideal doctoral students who essentially do not need any help; he used to come up with his own problems and often solved them.

The thesis is based on four papers of him, all are single author papers. The first three papers are in the area of proof complexity, the fourth paper is in the model theory of intuitionistic logic.

The aim of Paper A is to extend the current lower-bound techniques beyond the current state of art. To this end Khaniki studied the proof system which combines two standard proof systems Resolution and Polynomial Calculus into, what is called, Resolution over Polynomial Calculus. He was able to generalize the famous width-size relation of Ben Sasson and Wigderson to this calculus. This is an interesting result of its own right, but it also enabled him to prove new lower bound. For instance, his nearly quadratic lower bounds on DAG-like proofs in Resolution over Polynomial Calculus of bounded degree imply the first nontrivial lower bound on $Res(\oplus)$ DAG-like proofs.

In Paper B Khaniki proved a version of a conjecture proposed by Jan Krajíček about tautologies defined using Nisan-Wigderson pseudorandom generators. He proved that for certain formalization, these tautologies require exponential size bounded depth Frege proofs.

Paper C has two parts. I will comment only on the second one. It contains a remarkable theorem about jump operators in the lattice of all propositional proof systems. It says, roughly speaking, that the existence of a computable jump operator implies that the particular operator based on consistency statements is a jump operator. This supports the validity of a conjecture about finite consistency statements stated by me in the 1980's.

Paper D gave a rather surprising answer to an important and well-known problem in intuitionistic logic. He proved that there exist a Kripke models of Heyting Arithmetic, the intuitionistic version of classical Peano Arithmetic, such that not all "worlds" in them are models of Peano Arithmetic.

This is an exceptionally strong thesis. It contains new interesting and nontrivial results that Erfan Khaniki obtained with very little advice of mine. Furthermore, these results only comprise part of the work that he has done during his PhD studies. Therefore I strongly recommend the thesis for giving him the PhD title.

Prof. Pavel Pudlák