David M. Cerna, Ph.D.

Office 324 Computational Mathematics

Pod Vodárenskou věží 271/2
182 07 Prague, Czechia

Phone: +420 266 05 3104

Email: dcerna@cs.cas.cz

Opponent's diploma thesis Bc. Jachym Šimon

" Automated proof-checking of the Rose-Rosser's proof of completeness of Łukasiewicz propositional logic"

In the presented work, the student provides a lean formalizaion of an extensive part of a particularly important proof of the completeness of Łukasiewicz propositional logic. This proof was recently modernized as part of a bachelor thesis. A daunting feature of this proof of completeness is the large number of syntactic and tedious lemmata, thus making verification of correctness difficult without the aid of interactive theorem provers. This feature motivated the investigation carried out in the thesis. Certain features of the lean prover aided this formalization effort. For example the use of the simplifier to carry-out tedious syntactic manipulation, and the development of new tactics that cover proof techniques used through-out the formalization. While a complete formalization of the completeness proof is not presented, a large portion has been completed and the current state of formalization is of high enough quality to be used and completed by anyone well versed in the lean prover.

In individual chapters, the student first presents propositional Łukasiewicz logic through there lean formalism together with important properties such as *proofs with cut*. They also provide a discussion of the proof structure which will be used throughout the formalism and within their proof_verifier tactic that greatly simplifies complex syntactic proofs. Additionally, in chapter one, the student discusses adding notions of congruence to the simplifier. They provide an important discussion concerning providing the simplifier with too much information and the inefficiency this entails. After presenting a how to deal with these issues, they move on the the main result of this chapter, the *proof by cases theorem*. In Chapter 2, the student starts by presenting an example of what can be achieved so far with the formalism presented in Chapter 1. Essentially, complex syntactic proofs can be completed using a call to the proof_verifier. A large portion of Chapter 2 is dedicated to the construction and use of the formalization of polynomial formulas. What is interesting about this formalism is the use of dependent types and some of the complexities associated with them. This is discussed in the paragraph on the apply_PF tactic where the student discusses how certains types are considered different from Lean's perspective even though they are intuitively equivalent. The example they gave is PF (f-g) and PF (-g+f). They solve this issue by developing a tactic for conversion purposes.

At the end of the thesis the student summarizes, their contributation as the completion of the first 2 parts of the completeness of Łukasiewicz propositional logic which they seperate into three parts.

They also emphasize the development of the proof_verifier tactic which significantly simplifies part 2 of the completeness of Łukasiewicz propositional logic, that is proving syntactic properties and theorems associated with polynomial formulas. The 3rd part of the formalization effort requires formalizing Farkas' Lemma and theorems connecting polynomial formulas and provability. The last step is of course the completeness theorem itself. The student plans to finish the formalism in the near future.

The student (no?) Fulfilled the assignment of DP, I believe the student has done excellent work and has done more than enough to fulfill the assignment of the DP.

I have these questions for the student, 1) If I wanted to formalize other syntactically heavy completeness proofs of propositional logics how much of these formalism can be repurposed? Is there a way to parameter the proof verifier tactic for reuse? 2) Concerning the conversion issues discussed in the paragraph **apply_PF tactic,** one could imagine a general conversion which equates two polynomial formula if they syntactically equal modulo an equational theory. Is there a reason not to take this route? 3) For part 3, is there more to be done foundationally, or is the majority of the work left finding formal proofs using the developed (and built-in) tactics? Do you know the rough structure of the final formalization push already?

Given the above, I clearly propose to evaluate this thesis with an grade of A-excellent and I recommend it to defend an engineering degree.

In Prague on 18. May 2022

Prof . Name, Ph.D signature