

Proving Program Properties as First-Order Satisfiability*

Salvador Lucas

DSIC, Universitat Politècnica de València, Spain
<http://slucas.webs.upv.es/>

Abstract

Program semantics can often be expressed as a (many-sorted) first-order theory \mathcal{S} , and program properties as sentences φ which are intended to hold in the *canonical model* of such a theory, which is often incomputable. Recently, we have shown that properties φ expressed as the existential closure of a boolean combination of atoms can be *disproved* by just finding a model of \mathcal{S} and the *negation* $\neg\varphi$ of φ . Furthermore, this idea works quite well in practice due to the existence of powerful tools for the automatic generation of models for (many-sorted) first-order theories. In this paper we extend our previous results to *arbitrary* properties, expressed as sentences without any special restriction. Consequently, one can prove a program property φ by just *finding a model* of an appropriate theory (including \mathcal{S} and possibly something else) and an appropriate first-order formula related to φ . Beyond its possible theoretical interest, we show that our results can also be of practical use in several respects.

Keywords: First-Order Logic, Logical models, Program analysis.

References

- [1] S. Lucas. Proving Program Properties as First-Order Satisfiability. In F. Mesnard and P.J. Stuckey, editors, *Revised Selected papers from the 28th International Symposium on Logic-Based Program Synthesis and Transformation, LOPSTR 2018*, LNCS 11408:3-21, 2019. *LOPSTR 2018 best paper award*

*Partially supported by the EU (FEDER), and projects TIN2015-69175-C4-1-R, RTI2018-094403-B-C32, PROMETEO/2019/098, and SP20180225.