

Deductive Program Verification

Jean-Christophe Filliâtre^{1,2}

¹ Lab. de Recherche en Informatique, Univ. Paris-Sud, CNRS, Orsay, F-91405

² Inria Saclay – Île-de-France, Orsay, F-91893

`Jean-Christophe.Filliatre@lri.fr`

Abstract. Among formal methods, the deductive verification approach consists in first building verification conditions and then resorting to traditional theorem proving. Most deductive verification tools involve a high degree of proof automation through the use of SMT solvers. Yet there may be a substantial part of interactive theorem proving in program verification, such as inserting logical cuts, ghost code, or inductive proofs via lemma functions. In this talk, I will show how the Why3 tool for deductive verification resembles more and more a traditional ITP, while stressing key differences between the two.

Keywords: Deductive Verification · Theorem Proving.