FACULTY
OF MATHEMATICS
AND PHYSICS
Charles University

To whom it may concern

Prague, September 6, 2024

Doctoral thesis of Vlastimil Dort – Supervisor's report

The doctoral thesis describes extensions of the core type system of the Scala programming language, which is based on the Dependent Object Types (DOT) calculus. Two key extensions developed by the author of this thesis add support for read-only references (also called reference immutability) and method purity, enabling programmers to write more robust and safe code. The author started working on this research topic during his stay at the University of Waterloo, Canada, in 2018 under the supervision of prof. Ondřej Lhoták, and continued up to now.

Text of the thesis is organized as follows. In Chapter 1, the author introduces the whole research topic, providing the motivation and context for his work. Chapter 2 defines important concepts and terminology related to the field of type systems, and presents basics of the DOT calculus, including syntax, semantics, type soundness and mechanization.

Then, Chapter 3 describes the first major contribution - the roDOT calculus. It is an extension of the baseline DOT calculus with reference immutability and read-only references. Author summarizes previous work on reference immutability in the context of other programming languages, discusses requirements on the type system extension and key design decisions, formal definition of the roDOT calculus in the form of typing rules, and finally states and proves important properties, including soundness and immutability

Department of Distributed and Dependable Systems
Malostranské nám. 2/25, 118 00 Praha 1, Czech Republic
info@d3s.mff.cuni.cz
+420 951554245

guarantee. Main contributions have been published in the proceedings of the conference ECOOP 2020.

Chapter 4 builds upon the previous chapter, and presents the second major contribution of this work - support for method purity. Author discusses the concept of pure methods from several perspectives, focusing on the property of side-effect freedom (SEF). Then follow core parts of this chapter, (1) description of necessary changes to the type system and its soundness proof, motivated by the need to recognize read-only types, and (2) the SEF guarantee that allows us to identify pure methods without runtime side effects just based on static type information. A proof of the SEF guarantee is included too. In addition, the chapter describes one application of method purity - safe transformations of program code - and selected technical aspects of mechanization in Coq. Main contributions of this chapter have been published in the proceedings of the conference ECOOP 2024.

Author has also worked on mechanization of the roDOT calculus and type system extensions for method purity in the Coq proof assistant, capturing all the definitions and proofs.

Chapter 5 describes the prototype implementation of the presented type system extensions in the Dotty compiler for Scala, together with a case study done on Scala collections library. The sixth chapter concludes and outlines possible future work.

Throughout his work, the author demonstrated his ability to perform very solid research, at the levels of theory as well as implementation, and make significant contributions. Results of his work presented in the doctoral thesis were published at ECOOP 2020 and ECOOP 2024, respectively, which is a top international conference in the field of programming languages. He has focused mainly on theory, that means definitions of typing rules and soundness proofs, but he has also dedicated a lot of time to work on the mechanization in Coq and preparation of artifacts. In addition, the candidate also participated in the development of Checker Framework, a state-of-the-art bug finding and prevention tool, where he worked on a type system for detecting out-of-bounds array accesses. Results were published in the proceedings of ISSTA 2018, a top international conference in the field of software testing and analysis.

To conclude my report, I strongly recommend to accept the thesis for defense and to grant a PhD degree to Vlastimil Dort.

Pavel Parízek
(supervisor)