Developing Verified Programs with Dafny

K. Rustan M. Leino

Microsoft Research, Redmond, WA, USA
leino@microsoft.com

Abstract. Dafny [2] is a programming language and program verifier. The language is type-safe and sequential, and it includes common imperative features, dynamic object allocation, and inductive datatypes. It also includes specification constructs like pre- and postconditions, which let a programmer record the intended behavior of the program along with the executable code that is supposed to cause that behavior. Because the Dafny verifier runs continuously in the background, the consistency of a program and its specifications is always enforced.

Dafny has been used to verify a number of challenging algorithms, including Schorr-Waite graph marking, Floyd's "tortoise and hare" cycle-detection algorithm, and snapshotable trees with iterators. Dafny is also being used in teaching and it was a popular choice in the VSTTE 2012 program verification competition. Its open-source implementation has also been used as a foundation for other verification tools.

In this tutorial, I will give a taste of how to use Dafny in program development. This will include an overview of Dafny, basics of writing specifications, how to debug verification attempts, how to formulate and prove lemmas, and some newer features for staged program development.

References

1. Leino, K.R.M.: Specification and verification of object-oriented software. In: Broy, M., Sitou, W., Hoare, T. (eds.) Engineering Methods and Tools for Software Safety and Security. NATO Science for Peace and Security Series D: Information and Communication Security, vol. 22, pp. 231–266. IOS Press (2009); Summer School Marktoberdorf 2008 Lecture Notes
2. Leino, K.R.M.: Dafny: An Automatic Program Verifier for Functional Correctness. In: Clarke, E.M., Voronkov, A. (eds.) LPAR-16 2010. LNCS, vol. 6355, pp. 348–370. Springer, Heidelberg (2010)
3. Leino, K.R.M.: Automating induction with an SMT solver. In: VMCAI (to appear, 2012)

R. Joshi, P. Müller, and A. Podelski (Eds.): VSTTE 2012, LNCS 7152, p. 82, 2012.
© Springer-Verlag Berlin Heidelberg 2012