Spec#: A .NET Language for Software Contracts

Mike Barnett, Rob DeLine, Manuel Fähndrich, K. Rustan M. Leino, Wolfram Schulte, and Herman Venter

Microsoft Research, Redmond, WA, USA

The Spec# Programming System

Spec# is the latest in a long line of work on programming languages and systems aimed at improving the development of correct software. The Spec# programming system consists of the object-oriented Spec# programming language, the Spec# compiler, and the Spec# static program verifier. The language includes constructs for writing specifications that capture programmer intentions about how methods and data are to be used, the compiler emits run-time checks to enforce these specifications, and the verifier can check the consistency between a program and its specifications. The Spec# programming system is currently under development at Microsoft Research.

Besides pre- and postconditions, Spec# provides a sound modular treatment of object invariants. It also provides a sound modular system for multithreaded programs which allows for sequential reasoning even in the presence of concurrency. It is integrated into the Visual Studio development environment.

Acknowledgments

Peter Müller (ETH) and David Naumann (Stevens Institute of Technology) are external collaborators with the Spec# project. We have also had several interns who have contributed to the project: Bor-Yuh Evan Chang, Bart Jacobs, Xinming Ou, and Qi Sun.