Contract Specification and Checking: Application to .NET and C

Shuvendu Lahiri and Francesco Logozzo

RiSE, Microsoft Research
Redmond, WA (USA)
{shuvendu, logozzo}@microsoft.com
http://research.microsoft.com/~{shuvendu, logozzo}

In this tutorial, we will present some of the recent advances in the theory and application of contract checking for industrial strength software. The tutorial will focus on two application domains:

1. Contract checking for .NET programs (using Clousot and runtime techniques)
2. Contract checking for C programs (using HAVOC)

In the first part we will present the language agnostic contracts for .NET. We will introduce the: (1) language agnostic specification of contracts; (2) the runtime checking enforced via binary rewriting; and (3) the design and the implementation of a static contract checker based on abstract interpretation. We will provide the necessary background on abstract interpretation, and we will explore the most important issues in the design of a precise yet scalable and generic static analyzer to be used for code checking.

In the second part, we will discuss the challenges and progress in verifying C programs with high precision, coverage and automation in the context of the HAVOC project. We will address the basic challenges in specifying and verifying low-level systems software with regards to the lack of type-unsafety, use of linked data structures and inferring contracts for modules several thousand lines of code. We will present relevant background information on verification condition generation, Satisfiability Modulo Theories (SMT) solvers, which underlies the approach.

References

1. Managed Contracts. http://research.microsoft.com/en-us/projects/contracts/
2. Havoc. http://research.microsoft.com/en-us/projects/HAVOC/