Automatic Verification of Heap-Manipulating Programs Using Separation Logic

Hongseok Yang

Queen Mary University of London, UK

Abstract. The incorrect use of pointers, such as null pointer dereference and memory leak, is one of the most common sources of program errors. In this talk, I will describe our techniques for automatically verifying the absence of such pointer errors, which we have been developing for the past three years, based on a new program logic called separation logic.

This talk has two goals. The first is to show, by demo, the current status of techniques for automatically verifying pointer safety. The second is to present interesting instances of the interplay between automatic verification and program logic. In order to reduce the complexity of formal (manual) verification of programs, separation logic has unusual proof rules that exploit programming disciplines used by skilled software developers. I will explain how such rules have been used to improve the performance of our automatic verification techniques. Regarding the influence of automatic verification on program logic, I will describe new types of theorem proving questions on separation logic that were motivated by automatic verification.

A. Frid et al. (Eds.): CSR 2009, LNCS 5675, p. 25, 2009.