Abstract

Stacking-based Context-sensitive Points-to Analysis for Java

Xin Li[†1] and Mizuhito Ogawa[†1]

A points-to analysis is a prerequiste to context-sensitive program analyses for Java, in which difficulty lies in mutual dependency between a call graph generation and a points-to analysis result. Existing practical context-sensitive points-to analyses are mostly cloning-based, which have an inherent limit to handle recursive procedure calls and are hard to scale under deep cloning. We present a stacking-based context-sensitive points-to analysis for Java, by encoding the analysis as weighted pushdown model checking. Sound abstraction and proper modeling of a Java program are proposed. Further, localizing each analysis at an iteration on a partial program brings a substantial acceleration, which finally leads to an incremental algorithm. Our empirical study shows that, the incremental analysis scales well to Java benchmarks of significant size, whereas some of them cannot be handled by non-incremental ones.

(Presented October 30, 2009)

†1 Japan Advanced Institute of Science and Technology