Chair of Programming Methodology

Semester Thesis

Translating Java bytecode to a simple language

Roman Scheidegger

1.10.2009

Introduction

The Java bytecode language is composed by more than 200 statements. Intuitively, it is an intermediate language between source and machine code. Thus the most part of statements is specific for a given type (e.g. sum operators of integers, floats, etc.) as they are intended to optimize the execution (e.g. loading from and storing to the first local variable, the second one, etc.). In addition, Java bytecode is not structured, i.e. it contains goto and conditional jumps. Finally, values are passed through an operand stack. E.g. in order to add two integer numbers, they are pushed on the operand stack, and a sum operator adds them pushing on the top of the stack the resulting value.

We want to build up a static analyzer for Java programs at bytecode level. In order to achieve this goal, we want to deal with a simpler language, as tuning the analysis at bytecode level would require to formalize and implement the semantics of more than 200 statements. In addition, tuning a static analyzer at bytecode level without performing any reconstruction of the information contained in it produces too much approximated results.

Goal

The goal of this semester project is to develop and implement a translation from Java bytecode programs to a particular language composed by a small set of statements (i.e. assignments, variable declarations, throws of exceptions, method calls, and field accesses), and to represent programs through control flow graphs. This language and the control flow graph structure have already been developed and implemented. The student has to translate Java bytecode programs into such a language using the control flow graph structure. The main issues will be to

- abstract away the operand stack
- build up the control flow graph starting from unstructured code
- inject the information contained in the bytecode (e.g. type information) into its simplified representation

Contact Information

	Prof. Dr. Peter Müller	Dr. Pietro Ferrara
Room:	RZ F2	RZ F1
Phone:	(01) 63-22868	(01) 63-29439
Email:	peter.mueller@inf.ethz.ch	pietro.ferrara@inf.ethz.ch
WWW:	http://www.pm.inf.ethz.ch/education/theses/semester_ongoing	