## Contents

1 Introduction .......................................................... 1
   1.1 Semantic-based program certification .............................. 5
   1.1.1 Proof-Carrying Code (PCC) ................................... 6
   1.1.2 Model Carrying Code (MCC) ................................... 18
   1.1.3 Certified components for FPCC ................................. 21
   1.1.4 PCC with certifier authorities ................................. 22
   1.1.5 Code synthesis and certification ............................... 22
   1.2 Thesis publications ............................................... 27

2 Preliminaries ............................................................ 31
   2.1 Rewriting Logic and Maude ....................................... 31
   2.2 Abstract Interpretation ............................................ 36

3 The Java Rewriting Logic Semantics .................................. 45
   3.1 The Java state ..................................................... 46
   3.2 Continuation-based semantics ..................................... 49
   3.3 Java execution ..................................................... 53

4 Certifying Java programs ................................................. 57
   4.1 The Java Modeling Language JML ................................. 58
   4.1.1 JML tools ..................................................... 59
   4.2 Full certificates ................................................... 63
   4.3 Reduced certificates ............................................... 64
   4.4 Certificate checking vs. generation ............................... 66

5 Analyzing Arithmetic Properties of Java Programs .................. 71
   5.1 Introduction ....................................................... 71
   5.2 The abstract RL semantics of Java for the arithmetic domain .... 76
   5.2.1 Abstract rewriting formalization .............................. 80
   5.2.2 Extending the approach to relational domains .............. 87
   5.3 Experimental Evaluation .......................................... 93
## Contents

6 Analyzing Confidentiality of Java Programs  
6.1 Introduction .......................... 95  
6.2 Non-interference policies .................. 96  
6.3 The extended Rewriting Logic semantics of Java for non-interference  
   6.3.1 Proving non-interference as a safety property .......... 103  
6.4 The extended abstract Rewriting Logic semantics of Java  
6.5 Experimental evaluation .................. 126

7 Analyzing Erasure with or without Non-Interference of Java Programs  
7.1 Introduction .......................... 129  
7.2 Erasure policies ........................ 130  
   7.2.1 Erasure and non-interference .................. 134  
7.3 The extended Rewriting Logic semantics of Java for erasure  
   7.3.1 Proving erasure as a safety property ............... 140  
7.4 The extended abstract Rewriting Logic semantics of Java for erasure  
7.5 Experimental evaluation .................. 152

8 The JavaPCC certification environment  

9 Conclusions  

Bibliography  

A Related work: a comparison  

B Code of Chapter 5 example programs  

C Code of Chapter 6 example programs  

D Code of Chapter 7 example programs  

129  
155  
161  
165  
189  
201  
203  
209
### List of Figures

1. Overview of our JavaPCC framework. ......................... 2
2. Overview of the typical PCC framework. .................... 7

2.1 Maude TIMER example. ........................................ 35
2.2 Abstract lattice on Int values regarding their parity. .... 41
2.3 Abstract post increment ++ integer operator. ............. 44

3.1 Java program state. ........................................... 47
3.2 Sequential Java program state. .............................. 48
3.3 Continuation-based equations for Java addition operator on integers. .................................. 49
3.4 Evaluation of "2+3" Java expression. ....................... 50
3.5 Continuation-based equations for Java less-or-equal operator on integers. .......................... 50
3.6 Continuation-based equations for building the environment. ............................... 50
3.7 Continuation-based equations for variable content retrieval. ...................................... 50
3.8 Continuation-based equations for the Java assignment operator. .............................. 51
3.9 Continuation-based equations for the if-then-else statement. .................................. 51
3.10 Continuation-based equations for the while statement. ........................................ 51
3.11 Continuation-based equations for the while-break statement. .................................. 51
3.12 Continuation-based equations for the instance method call statement. ........................................ 52
3.13 Continuation-based equations for the return statement. ........................................ 52

4.1 JML method specification. ..................................... 58
4.2 JML assert statement. .......................................... 59
4.3 JML specification clauses for a class with a model field. ........................................ 59
4.4 Time differences with a simple condition. .................. 68
4.5 Time differences with a simple condition and a costly computation. .......................... 68
4.6 Time differences with a simple condition and a more costly computation. .................. 68

5.1 Lattice of integers for the mod2 and mod4 abstractions. .... 77
List of Figures

5.2 Abstract domain and association of abstract domain to variable name. 78
5.3 Modified continuation-based equations for building environments and Java assignment. 78
5.4 Abstract definition and equations for the abstract Java addition operator with EvenOdd values. 79
5.5 Continuation-based equations for Java less-or-equal abstract operator on EvenOdd and Mod4 abstract integers. 80
5.6 Concretization function $\text{mod2}^\#$ . 82
5.7 Concretization function $\text{mod4}^\#$ . 82
5.8 Java less-or-equal operator on integers. 88
5.9 Continuation-based equations for Java less-or-equal operator on integers. 88
5.10 Specification of Java post- and pre-increment operator on integers. 89
5.11 Continuation-based equations for Java post- and pre-increment operator for $\text{leq}^#$ values: Case 1) if the value of $\text{Var}$ is not equal to $\text{Val}$. 89
5.12 Continuation-based equations for Java post- and pre-increment operator for $\text{leq}^#$ values: Case 2) if the value of $\text{Var}$ is equal to $\text{Val}$. 90
5.13 Continuation-based equations for Java pre- and post-increment operator for $\text{gt}^#$ values. 90
6.1 Sets of sets of Java program traces. 104
6.2 Sets of Java program traces. 105
6.3 Extended equations for constant evaluation. 106
6.4 Extended equations for variable content retrieval. 107
6.5 Specification of the $\text{join}$ operator. 107
6.6 Continuation-based equations for building the extended environment. 107
6.7 Continuation-based equations for setting the initial variable confidentiality level. 107
6.8 Equations of extended Java + operator. 108
6.9 Equations of extended Java $<=$ operator. 108
6.10 Equations of extended Java ++ post-increment operator. 108
6.11 Extended equations for the Java assignment operator. 108
6.12 Updating memory locations. 108
6.13 Extended equations for the if-then-else statement. 110
6.14 Extended equations for the while statement. 110
6.15 Extended abstract equations for constant evaluation. 119
6.16 Extended abstract equations for variable content retrieval. 119
6.17 Abstract equations of extended Java + operator. 119
6.18 Abstract equations of extended Java <= operator. 119
6.19 Abstract equations of extended Java ++ post-increment operator. 119
6.20 Continuation-based equations for setting initial variable confidentiality level. 120
6.21 Abstract equations for the Java assignment operator. 120
6.22 Abstract rules for the if-then-else statement. 120

7.1 Updating memory locations for Erasure. 136
7.2 Joining over erasure labels. 136
7.3 Binary expression evaluation. 137
7.4 Equations of extended constant evaluation with erasure labels. 137
7.5 Equations of extended variable content retrieval with erasure labels. 137
7.6 Continuation-based equations for setting the initial variable confidentiality level. 138
7.7 Equations of extended Java + operator. 138
7.8 Equations of extended Java <= operator. 138
7.9 Equations of extended Java ++ post-increment operator. 138
7.10 Equations of extended Java assignment operator. 138
7.11 Equations of extended if-then-else with erasure labels. 139
7.12 Java and Maude eraseT operator equations. 140
7.13 Abstract rules for the if-then-else statement. 147

8.1 Web interface snapshot 156
8.2 JavaPCC main page snapshot 157
8.3 Full and reduced rules certificate snapshots 158