DEPARTMENT OF INFORMATICS

TECHNISCHE UNIVERSITÄT MÜNCHEN

Bachelor's Thesis in Informatics

Combatting the Precision Loss of Partial Contexts in Abstract Interpretation

Felix Sebastian Krayer

DEPARTMENT OF INFORMATICS

TECHNISCHE UNIVERSITÄT MÜNCHEN

Bachelor's Thesis in Informatics

Combatting the Precision Loss of Partial Contexts in Abstract Interpretation

Bekämpfung des Präzisionsverlust durch partielle Kontexte in Abstrakter Interpretation

Author:	Felix Sebastian Krayer
Supervisor:	Supervisor
Advisor:	Advisor
Submission Date:	15th of February 2023

I confirm that this bachelor's thesis in informatics is my own work and I have documented all sources and material used.

Munich, 15th of February 2023 Felix Sebastian Krayer

Acknowledgments

Abstract

Contents

1 Introduction

```
1  int function (int a) {
2    //a = [0, 12]; y = [1, 2]
3    a = a * 2;
4    return a; //x_f = [0, 24]; y = [1, 2]
5  }
6
7  int y; //global
8
9  int main() {
10   int x; //local
11   x = 0;
12
13   y = 1;
14   x = function(0); // a = x = [0, 0]; y = [1, 1]
15   // x = [0, 24], y = [1, 1]
16
17   //...
18
19   y = 2;
20   x = function(12); // a = x = [12, 12]; y = [2, 2]
21   // x = [0, 24], y = [2, 2]
22 }
```

2 Background

2.1 Related Work

3 Main Contributions

3.1 Taint analysis

3.1.1 Fromal description

3.1.2 Implementation

3.2 Benefiting other Analyses

In this section we will use the new <TODO Name> analysis to improve a context insensitive analysis. For this let's choose an analysis that maps Lvalues to Rvalues. When combining the contexts of the caller before the call with the one returned by the callee there a few aspects to keep in mind:

- All mappings of Lvalues, which are not tracked in the caller (i.e. map to top), but have a concrete value within the callee need to be added to the combined context. This is for Lvalues which are newly initialized inside the caller.
- (All mappings which are not in the callee context but have been in the caller context need to be removed. This can happen in multithreaded programs, if in the caller a mutex was held, that then was unlocked by the callee, deleting the information protected by the mutex)
- for all other Lvalues present in both contexts, the Rvalues mapped to by Lvalues not in the tainted set can be kept. We are sure that these variables are unchanged, even if they have a less precise record in the callee's context. For Lvalues present in the tainted set, it is necessary to take the Rvalue from the callee context, as the old Rvalue mapped to by the caller is incorrect.

4 Evaluation

4.1 Testing

4.2 Benchmarking

5 Conclusion

List of Figures

List of Tables