Diplomarbeit: An Isabelle Formalization of the Universe Type System

Martin Klebermass

01.10.2006

Background: The Universe Type System [1] allows to structure the heap memory into universes. Those universes together with the owner-as-modifier Property make it easier to reason about the structure of the heap. Featherweight Java [2] is a very small subset for Java, just like the lambda calculus is for ML. Isabelle/HOL [3] is a generic theorem prover developed at Cambridge University and TU Munich.

Goal of this diploma's project is to formalize the Universe Type System using a Featherweight Java like Syntax, extended with Field Updates. The formalization has to be proved using the theorem prover Isabelle/HOL.

The main parts of this project are:

1. Extract information out of the GUT-Paper [4] and UJ - Paper [5].
2. describe the Syntax, and a Heap model for the Formalization of Featherweight Java
3. describe the Type System, the Well Formed Class Property and the Well Formed Program Property using inference rules
4. describe the Well Formed Heap Property and the Big Step Semantics using inference rules
5. describe how to prove type safety and the owner-as-modifier Property
6. formalize the Syntax and the Heap model using Isabelle/HOL
7. formalize the Type System using Isabelle/HOL
8. formalize the Big Step Semantic using Isabelle/HOL
9. prove type Safety and the owner-as-modifier Property using Isabelle/HOL

Possible Extensions of this project are:

1. add generics to the Model
2. extend featherweight java with some other constructs
3. Arrays
4. Exceptions

A written report, an oral presentation in the middle and an oral report at the end will complete the project. The presentation is presented in zurich and munich.

Schedule

The Schedule for the Project is the following:

- till 31.12.06: Finish Description Part of the Proof
- First Presentation will be done after Finishing the Description Part
- till 28.02.07:Finish the formalization and the proofs in Isabelle/HOL
- till 15.03.07: Finish the Report
- Final Presentation is planned to be around the end of March.

Aufgabensteller

Aufgabensteller: Prof. Tobias Nipkow, TU Muenchen
Betreuer: Prof. Peter Müller, ETH Zurich; Werner M. Dietl, ETH Zurich

References

1 W. Dietl and P. M?uller. Universes: Lightweight ownership for JML. Journal of Object Technology (JOT), 4(8):5Ð32, October 2005.

2 A. Igarashi, B. C. Pierce, and P. Wadler. Featherweight Java: A mini- mal core calculus for Java and GJ. ACM Transactions on Programming Languages and Systems, 23(3):396Ð450, 2001.

3 T. Nipkow, L. Paulson, and M. Wenzel. Isabel le/HOL Ñ A Proof As- sistant for Higher-Order Logic, volume 2283. 2002. http://www.in.tum. de/?nipkow/LNCS2283/.

4 W. Dietl,S. Drossopoulou and P. M?uller. Generic Universe Types

5 D. Cunningham, W. Dietl,S. Drossopoulou, A. Francalanza and P. M?uller. UJ: Soundness for Universe Types