Verification of Software Product Lines by Proof Reuse

Master Project Proposal

Motivation and Context

A *software product line* is a set of systems with well-defined commonalities and variabilities that are developed by managed reuse. Because of the high configurability, it is important to ensure that safety-critical requirements are satisfied by all products. Formal verification has been proven useful in order to establish that software systems satisfy critical properties. However, it is not feasible to verify each product of the product line in isolation. Instead, efficient verification techniques are necessary that allow reusing proofs between the implementations of different products.

Project Goals

The goal of this master thesis project is a case study for proof reuse for verifying software product lines. The KeY System (http://www.key-project.org) already contains mechanisms for proof reuse. The case study comprises the following tasks:

- Design and implementation of an example software product line using Δ-Modelling [1] and Frame Technology to facilitate automated derivation of product implementations
- Specification of product properties in JML: Analysis of the differences between properties of different products, automatic generation of product specifications
- Verification of product properties using the KeY System by reusing proofs between products, Analysis of the reuse potential dependent on the differences between products

Prerequistes

Knowledge of Formal Methods ("Software Engineering using Formal Methods TDA292/DIT270").
Programming Experience in Java

Contact

Ina Schaefer
`http://www.cse.chalmers.se/~schaefer/`
Software Engineering using Formal Methods Group
`http://www.chalmers.se/cse/EN/research/research-groups/formal-methods/`
Phone: +46 - 31 - 772 - 1072
Email: schaefer@chalmers.se

Literature

[1] I. Schaefer, A. Worret, and A. Poetzsch-Heffter. A model-based framework for automated product derivation. In *Workshop on Model-based Approaches in Product Line Engineering (MAPLE)*, 2009.