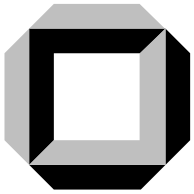

Universität Karlsruhe
Institut für Theoretische Informatik
Prof. Dr. P. H. Schmitt
C. Engel, B. Weiß

04. Februar 2009

Praktikum
Formale Entwicklung objektorientierter Software
Übungsblatt 10 – Gruppe 3

Vorbemerkung

Sie haben eine Version Ihres Milliardenbankprojekts zugesandt bekommen oder werden es noch bekommen. Im Wesentlichen haben wir die GUI-Klassen entfernt, `System.out.println` Anweisungen auskommentiert, und evtl. kleine Syntaxfehler in der Spezifikation behoben. Insbesondere haben wir keine Fehler in die Implementierung eingebaut, die nicht schon vorher vorhanden waren.

Außerdem haben wir einzelne Methodenspezifikationen verändert oder eingefügt. Es kann sein, dass eine solche Spezifikation die Aufgabe der Methode nicht richtig beschreibt. Sollten Sie feststellen, dass ein Beweis nicht schließbar ist, kann der "Fehler" in der Spezifikation, der Implementierung oder in beidem liegen. Die Ursache sollte dann beseitigt und die Verifikation erfolgreich abgeschlossen werden. Nähere Hinweise finden Sie in der gruppenspezifischen Aufgabenbeschreibung unten.

Schalten Sie bitte vor dem Beweisen im KeY-System unter "Taclet libraries" den Punkt "stringRules.key" an.

Aufgabe 19 (Gruppe 3)

Zur Methode `keyprkt3.model.Zentralrechner::getKonto(int)` haben wir 3 Verträge hinzugefügt. Beweisen Sie jeweils die "EnsuresPost"-Beweisverpflichtung für jeden dieser Verträge. Dazu folgende Hinweise:

- Für die Schleife in getKonto müssen Sie eine Invariante, Variante und assignable-Klausel schreiben.
- Code und Methodenspezifikation sollen nicht verändert werden. Sie dürfen allerdings Klasseninvarianten zu den verwendeten Klassen hinzufügen. Das ist auch nötig, um auszuschließen, daß z.B. NullPointerExceptions in getKonto auftreten.
- Entsprechend dürfen Sie auch beliebige Invarianten im Vorzustand von getKonto annehmen (über "Assumed Invariants" im "Contract Configurator" auswählbar). Es ist aber nicht ratsam Invarianten anzunehmen, die man zum Schließen des Beweises gar nicht braucht, da das nur zu unübersichtlicheren Sequenzen führt (Sie werden interaktiv einige Quantoren instanziieren müssen, was bei übersichtlich kleinen Sequenzen deutlich einfacher ist).
- Benutzen Sie für die Beweissuchstrategie die Einstellungen "Method treatment: Expand" und "Query treatment: Expand".

Geben Sie sowohl die geänderten .java-Dateien als auch die Beweise selbst ab.
Rückfragen zu diesen Aufgaben bitte an Christian Engel.

Abgabe bis 31.03.

Es braucht pro Gruppe nur *eine* Lösung abgegeben werden.
Die Abgabe der Übungsblätter erfolgt mit dem SVN System. Dazu legen Sie die abzugebenden Dateien im SVN ab und kopieren sie mit SVN in den Unterordner *abgabe/<nr>* wie in Aufgabe 2 auf Blatt 1 beschrieben.
Einige Aufgaben verlangen eine schriftliche Bearbeitung, diese ist dann je nach Komplexität als ASCII, html, ps- oder pdf-Dokument abzugeben. Auf *keinen* Fall im MS Word `doc`-Format.

Praktikums-Webseite: `http://lfm.iti.uni-karlsruhe.de/keyprakt0809.php`

Christian Engel: R. 106, Tel. 608-4338, E-Mail: `engelc@ira.uka.de`
Benjamin Weiß: R. 309, Tel. 608-4324, E-Mail: `bweiss@ira.uka.de`