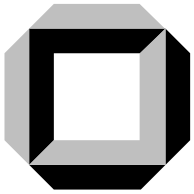

Universität Karlsruhe
Institut für Theoretische Informatik
Prof. Dr. P. H. Schmitt
C. Engel, B. Weiß

04. Februar 2009

Praktikum
Formale Entwicklung objektorientierter Software
Übungsblatt 10 – Gruppe 1

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 1)

(a) Methode `myutil.Map::getKeyPos()`. Beweisen Sie für den von uns geschriebenen Vertrag die "EnsuresPost"-Beweisverpflichtung.

- Wie üblich müssen Sie für die Behandlung der Schleife zunächst eine passende Schleifeninvariante, -variante und `assignable`-Klausel angeben.
- Die Methode erfüllt den Vertrag nur unter der Voraussetzung, dass die betroffenen Objekte einige naheliegende Konsistenzeigenschaften erfüllen. Formalisieren sie diese Eigenschaften als Klasseninvarianten der Klassen `Map` und `List`, und aktivieren Sie sie beim Starten des Beweises im "Contract Configurator" unter "assumed invariants", um sie für die Verifikation verwenden zu können. Falls Sie die notwendigen Invarianten nicht gleich sehen, können Sie versuchen, den Vertrag zu verifizieren, und sich den offenen Beweis anschauen.
- Für die Automatisierung der Beweise ist es vorteilhaft, auf die Verwendung von Methodenaufrufen in Spezifikationen zu verzichten (wie es im gegebenen Vertrag geschehen ist).
- Benutzen Sie für die Beweissuchstrategie die Einstellungen "Method treatment: expand" und "Query treatment: Expand".

(b) Methode `myutil.Map::get()`. Beweisen Sie auch hier für den von uns geschriebenen Vertrag die "EnsuresPost"-Beweisverpflichtung. Verwenden Sie dazu die Verträge der aufgerufenen Methoden (Einstellung "Method treatment: contracts").

(c) Methode `myutil.Map::put()`. Beweisen Sie wieder "EnsuresPost" für den gegebenen (recht einfachen und unvollständigen) Vertrag. Benutzen Sie wieder die Verträge der aufgerufenen Methoden, soweit vorhanden.

- Für den Beweis benötigen Sie die folgende zusätzliche Klasseninvariante in der Klasse `List`:

  ```
  \typeof(data) == \type(Object[])
  ```

  Was besagt diese Invariante, und warum ist sie notwendig?
- Sie benötigen außerdem noch weitere Klasseninvarianten in `Map`, die für die bisherigen Beweise nicht gebraucht wurden, da dort nur lesend auf die beteiligten Objekte zugegriffen wird. Diese Invarianten dienen dazu, unerwünschtes *Aliasing* zu verbieten.

(d) *(Ohne Abgabe)* Betrachten Sie noch einmal Ihre Implementierung der zentralen Methode `ServerImpl::receiveInternalTransfer`. Inwiefern tut dieser Code nicht das, was wir von ihm erwarten? Würden wir dieses Problem finden, wenn wir die Korrektheit Ihres Vertrags zu verifizieren versuchen würden? Warum oder warum nicht?

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

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`