



Praktikum

Formale Entwicklung objektorientierter Software

Übungsblatt 3

Aufgabe 1

Beweisen Sie mit Hilfe des KeY-Systems den Hilfssatz *Is-Asg-List-Conc1*

$$\forall x: \text{Var } (\forall y: \text{Var } (\forall vs: \text{Vars } (\forall tli: \text{Tlist} \\ (\neg \text{In}(x, \text{vcons}(y, vs)) \wedge \text{Is-Asg-List}(x, tli) \rightarrow \text{Is-Asg-List}(x, \text{conc}_1(tli, \text{mk-rasg}(x, x, y)))))))$$

Hinweise

1. Das Archiv „aufgabe1.tar.gz“ enthält die Problemdatei „asg-list-conc1.key“ und in „korrekt-defs.key“ die Definitionen.
2. Die Festlegung, wann eine mit conc_1 erzeugte Folge von Zuweisungen in Zweiadressform eine korrekte Asg-Liste ist, drückt das Tactlet *Conc1_AsgListDef* aus.
3. Sie können diesen Beweis auch bei der Bearbeitung von Aufgabe 4 führen.

Aufgabe 2

Beweisen Sie mit Hilfe des KeY-Systems den Hilfssatz *Wf-Exp-Nicht-tleer*

$$\forall x: \text{Var } \forall vs: \text{Vars } \neg vs = v_\varepsilon \wedge \neg \text{In}(x, vs) \rightarrow \text{Wf-Exp}(f(x, vs, t_\varepsilon))$$

unter Verwendung der Hilfsaussage *Wf-Exp-Vs*

$$\forall x: \text{Var } (\forall vs: \text{Vars } (\forall tli: \text{Tlist} \\ (vs \neq v_\varepsilon \wedge \neg \text{In}(x, vs) \wedge \text{Is-Asg-List}(x, tli) \rightarrow \text{Wf-Exp}(f(x, vs, tli))))),$$

die mit Hilfe der Schnittregel während des Beweises einzuführen ist.

Hinweise

1. Das Beweisziel, das KeY mit der Überschrift „CUT: X FALSE“ kennzeichnet (X dabei die Schnittformel) müssen Sie nicht bearbeiten.
2. Die für die Bearbeitung dieser Aufgabe notwendigen Dateien finden Sie in „aufgabe2.tar.gz“.

Aufgabe 3

Führen Sie beim Nachweis von *Wf-Exp-Vs* die Aussage

$$\forall x: \text{Var } (\forall vs: \text{Vars } (\forall tli: \text{Tlist} \\ (\text{lg}(vs) = n \wedge n \geq 0 \rightarrow (\neg \text{In}(x, vs) \wedge \text{Is-Asg-List}(x, tli) \rightarrow \text{Wf-Exp}(f(x, vs, tli))))))$$

als eine ein, die durch Induktion bewiesen wird. Bearbeiten Sie mit Hilfe des KeY-Systems den Induktionsanfang und den Anwendungsfall.

Die zur Bearbeitung dieser Aufgabe notwendigen Dateien finden Sie in „aufgabe3.tar.gz“.

Aufgabe 4

Beweisen Sie mit Hilfe des KeY-Systems die Aussage

$\forall vs: Vars$

$$\begin{aligned} & (\forall x: Var (\forall tli: Tlist (\neg In(x, vs) \wedge Is-Asg-List(x, tli) \rightarrow Wf-Exp(f(x, vs, tli)))))) \\ & \rightarrow \forall x: Var (\forall y: Var (\forall tli: Tlist \\ & \quad (\neg In(x, vcons(y, vs)) \wedge Is-Asg-List(x, tli) \rightarrow Wf-Exp(f(x, vcons(y, vs), tli)))))) \end{aligned}$$

also den Induktionsschritt, der beim Nachweis von *Wf-Exp-Vs* mit Hilfe struktureller Induktion notwendig ist. Verwenden Sie dabei den Hilfssatz *Is-Asg-List-Conc1*, siehe Aufgabe 1. (Einführung des Hilfsatz mit Hilfe der Schnittregel.)

Hinweise

1. „aufgabe4.tar.gz“ enthält die notwendigen Dateien.
2. Sie können den Hilfssatz *Is-Asg-List-Conc1* (siehe Aufgabe 1 auch hier beweisen. Dazu müssen Sie das Ziel „CUT X FALSE“ (*X* die Schnittformel) bearbeiten.

Aufgabe 5

Beim Nachweis von *Wf-Exp-Vs* haben wir den Induktionsschritt mit struktureller Induktion durchgeführt. Geben Sie mit Hilfe des KeY-Systems einen Beweis, bei dem Sie im Induktionsschritt die Länge von *vs* verwenden. (Sie können dazu das in Aufgabe 3 nicht behandelte Ziel „Induktionsschritt“ bearbeiten.)

Hinweis. Die Aufgabe muß nicht abgegeben werden.

Abgabe bis 21.11.2007

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 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://i12www.ira.uka.de/~engelc/lehre/keypraktWS0708/>

Dr. Thomas Käufel: Zi. 207, Tel. 608-6286, E-Mail: kaeufl@ira.uka.de
Christian Engel: Zi. 106, Tel. 608-4338, E-Mail: engelc@ira.uka.de
Benjamin Weiß: Zi. 309, Tel. 608-4324, E-Mail: bweiss@ira.uka.de