Verfahren zur automatischen Verifikation

Prof. Dr. Christoph Walther • Markus Aderhold
FG Programmiermethodik • FB Informatik • TU Darmstadt
Sommersemester 2009

4. Hausaufgabe

Abgabe am Dienstag, den 02.06.2009, in der Übung

Hinweis Alle Verweise in den Aufgaben beziehen sich auf das Skriptum. Für diese Hausaufgabe gibt es **11 Punkte**.

Hausaufgabe 4.1 (Execution Guard) **4 Punkte**

Gegeben sei die Prozedur

```
function find(key:nat, a:list, i:nat, j:nat):bool <=
if length(a)>j
  then if j>i
         then if element(a,plus(i,half(minus(j,i))))>key
                then find(key,a,i,pred(plus(i,half(minus(j,i)))))
                else if key>element(a,plus(i,half(minus(j,i))))
                       then find(key,a,succ(plus(i,half(minus(j,i)))),j)
                       else true
                     fi
              fi
         else if j=i
                then key=element(a,i)
                else false
              fi
       fi
  else false
fi .
```

Berechnen Sie den Execution Guard $exec_{\texttt{find}}$, wie in Definition 5.2 angegeben. Bei der symbolischen Auswertung brauchen Sie nur den ersten Schritt sowie das Endergebnis anzugeben.

Hausaufgabe 4.2 (Symbolische Auswertung von Induktionsformeln) **7 Punkte**

Gegeben sei ein funktionales Program Pr mit den Prozeduren `plus` und `dbl` aus Abschnitt 11, sowie das Lemma `lemma dbl_plus <= all x,y:nat dbl(plus(x,y))=plus(dbl(x),dbl(y))`.

(i) Bestimmen Sie die optimalen Mengen für *grd-set*(*plus*) und *grd-set*(*dbl*).

(ii) Wählen Sie eine Relationenbeschreibung $B \in \textit{grd-set}(\textit{plus}) \cup \textit{grd-set}(\textit{dbl})$ und bilden Sie $\mathcal{IND}(B, \textit{goal}[x, y])$ mit $\textit{goal}[x, y] = \textit{dbl}(\textit{plus}(x, y)) = \textit{plus}(\textit{dbl}(x), \textit{dbl}(y))$ gem. Definition 4.13.

(iii) Geben Sie $\textit{goal}_{\perp_{\langle Pr, H, \varnothing, \{\otimes\}, \varnothing\rangle}}$ durch Angabe der symbolischen Auswertung von *goal* unter den Kontrollparametern $\langle Pr, H, \varnothing, \{\otimes\}, \varnothing\rangle$ für jede Sequenz $\langle H, IH, \textit{goal}\rangle \in \mathcal{IND}(B, \textit{goal}[x, y])$ an. Notieren Sie dabei wie im Skript, welche Auswertungsregeln Sie bei jedem Schritt verwendet haben, und insbesondere, welche der Anwendungsbedingungen von Regel 5.19 *Execute procedure call* bei Verwendung dieser Auswertungsregel jeweils erfüllt ist.

(iv) Vergleichen Sie $\textit{goal}_{\perp_{\langle Pr, H, \varnothing, \{\otimes\}, \varnothing\rangle}}$ für jede Sequenz $\langle H, IH, \textit{goal}\rangle \in \mathcal{IND}(B, \textit{goal}[x, y])$, für die $IH \neq \varnothing$ gilt, mit den Elementen von IH und interpretieren Sie das Ergebnis Ihres Vergleichs.