Verfahren zur automatischen Verifikation

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

5. Übungsblatt

Übung am Dienstag, 02.06.2009

Hinweis Alle Verweise in den Aufgaben beziehen sich auf das Skriptum.

Aufgabe 5.1 (Assumption-Menge, Assumptionregeln)
Gegeben seien die Prozeduren

```
function smaller(n:nat, k:list):list <=
if k=empty
  then empty
  else if hd(k)>n
         then smaller(n,tl(k))
         else add(hd(k),smaller(n,tl(k)))
         fi
fi
function larger(n:nat, k:list):list <=
if k=empty
  then empty
  else if hd(k)>n
         then add(hd(k),larger(n,tl(k)))
         else larger(n,tl(k))
       fi
fi
function qsort(k:list):list <=
if k=empty
 then empty
 else app(qsort(smaller(hd(k),tl(k))),add(hd(k),qsort(larger(hd(k),tl(k)))))
fi
```

sowie die Prozedur app aus dem Skriptum. Des weiteren sind folgende verifizierte Lemmata

```
lemma larger_lower_bound <= all n:nat, k:list lower_bound(n,larger(n,k))
lemma lower_bound_hd <= all k:list, n:nat
 if(k=empty,true,if(lower_bound(n,k),if(n>hd(k),false,true),true))
lemma lower_bound_qsort <= all k:list, n:nat
 if(lower_bound(n,k),lower_bound(n,qsort(k)),true)
lemma ordered_append_add <= all k,l:list, n:nat
 if(ordered(k),
    if(upper_bound(k,n),
       if(n>hd(l),true,if(ordered(l),ordered(app(k,add(n,l))),true)),
       true),
    true)
lemma ordered_append_add_empty* <= all l,k:list, n:nat
 if(l=empty,
    if(ordered(k),if(upper_bound(k,n),ordered(app(k,add(n,l))),true),true),
    true)
lemma smaller_upper_bound <= all k:list, n:nat upper_bound(smaller(n,k),n)
lemma upper_bound_qsort <= all n:nat, k:list
 if(upper_bound(k,n),upper_bound(qsort(k),n),true)
```

gegeben. Zu beweisen ist das Lemma

```
lemma qsort_sorts <= all k:list ordered(qsort(k))
```

durch Induktion über die Relationenbeschreibung von `qsort`.

(i) Berechnen Sie für den Schrittfall des Beweises die verfügbare Assumption-Menge wie im Skript angegeben.

(ii) Beweisen Sie den Schrittfall durch symbolische Auswertung und notieren Sie dabei die Anwendung der Execute- und Assumptionregeln. Folgen von einfachen Beweisschritten dürfen Sie dabei abkürzen.