

Verfahren zur automatischen Verifikation

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

3. Hausaufgabe

Abgabe am Donnerstag, den 26.05.2009, in der Übung

Hinweis Alle Verweise in den Aufgaben beziehen sich auf das Skriptum. Für diese Hausaufgabe gibt es **20 Punkte**.

Hausaufgabe 3.1 (Relationenbeschreibungen von Prozeduren) 5 Punkte

Gegeben sei die Prozedur

```
function remove(n:nat, k:list):list <=  
  if k=empty  
  then empty  
  else if n=hd(k)  
    then remove(n,tl(k))  
    else add(hd(k),remove(n,tl(k)))  
  fi  
fi .
```

- (i) Bestimmen Sie die Relationenbeschreibung B_{remove} gemäß Definition 4.18.
- (ii) Bestimmen Sie alle range-Generalisierungen von B_{remove} gemäß Definition 4.21, und geben Sie die resultierenden Relationenbeschreibungen explizit an. Welche dieser range-Generalisierungen sind range maximal?
- (iii) Bestimmen Sie alle domain-Generalisierungen der range maximalen Relationenbeschreibungen aus Teilaufgabe (ii) gemäß Definition 4.23, und geben Sie die resultierenden Relationenbeschreibungen explizit an. Welche dieser domain-Generalisierungen sind domain maximal und welche sind maximal?
- (iv) Bestimmen Sie alle optimalen Relationenbeschreibungen der Relationenbeschreibungen aus Teilaufgabe (iii) gemäß Definition 4.25.
- (v) Bestimmen Sie $\text{grd-set}(\text{remove})$, so daß diese Menge optimal ist (vgl. Skript Seite 38).

Hausaufgabe 3.2 (Relationenbeschreibungen von Prozeduren) 5 Punkte

Gegeben sei die Prozedur

```
function nth-tl(k:list, n:nat):list <=  
  if n=0  
  then k  
  else if k=empty  
    then empty  
    else nth-tl(tl(k),pred(n))  
  fi  
fi .
```

- (i) Bestimmen Sie die Relationenbeschreibung $B_{\text{nth-tl}}$ gemäß Definition 4.18.
- (ii) Bestimmen Sie alle range-Generalisierungen von $B_{\text{nth-tl}}$ gemäß Definition 4.21, und geben Sie die resultierenden Relationenbeschreibungen explizit an. Welche dieser range-Generalisierungen sind range maximal?

(iii) Bestimmen Sie alle domain-Generalisierungen der range maximalen Relationenbeschreibungen aus Teilaufgabe (ii) gemäß Definition 4.23, und geben Sie die resultierenden Relationenbeschreibungen explizit an. Welche dieser domain-Generalisierungen sind domain maximal und welche sind maximal?

(iv) Bestimmen Sie alle optimalen Relationenbeschreibungen der Relationenbeschreibungen aus Teilaufgabe (iii) gemäß Definition 4.25.

(v) Bestimmen Sie $grd\text{-}set(\mathit{nth}\text{-}\mathit{t1})$, so daß diese Menge optimal ist (vgl. Skript Seite 38).

Hausaufgabe 3.3 (Subsumption von Relationenbeschreibungen) 2 Punkte

Vergleichen Sie alle Relationenbeschreibungen aus $grd\text{-}set(\mathit{remove})$, $grd\text{-}set(\mathit{nth}\text{-}\mathit{t1})$ und aus $\{B_{\mathit{nat}}, B_{\mathit{list}}\}$ bzgl. Subsumption \sqsubseteq (vgl. Definition 4.27) miteinander, wobei Variablennamen keine Rolle spielen (d. h. Variablen dürfen konsistent umbenannt werden).

Hausaufgabe 3.4 (Aussagenlogik, Symbolische Auswertung) 6 Punkte

(i) Formulieren Sie die aussagenlogische Formel $(a \rightarrow b) \rightarrow ((a \rightarrow c) \rightarrow (b \rightarrow c))$ als booleschen Term t und werten Sie t mit den Auswertungsregeln aus Abschnitt 5.3.1 symbolisch aus. Geben Sie Ihre symbolische Auswertung so wie im Beispiel am Ende von Abschnitt 5.3.1 an. Was schließen Sie über die Formel aus dem Ergebnis der symbolischen Auswertung?

(ii) Formulieren Sie die aussagenlogische Formel $(a \rightarrow b) \rightarrow ((c \vee a) \rightarrow (c \vee b))$ als booleschen Term t und werten Sie t mit den Auswertungsregeln aus Abschnitt 5.3.1 symbolisch aus. Geben Sie Ihre symbolische Auswertung so wie im Beispiel am Ende von Abschnitt 5.3.1 an. Was schließen Sie über die Formel aus dem Ergebnis der symbolischen Auswertung?

Hausaufgabe 3.5 (Markierung von Prozedurrümpfen) 2 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
```

mit

$$grd\text{-}set(\mathit{find}) = \{ \{ \langle \{ j > i \}, \{ \{ i/i, j/pred(plus(i, half(minus(j, i)))) \}, \{ i/succ(plus(i, half(minus(j, i)))) \}, j/j \} \} \} \} .$$

Markieren Sie den Prozedurrumpf von find so, wie in Definition 5.1 angegeben. (Dazu können Sie dieses Blatt kopieren und Ihre Markierungen darauf – nicht in schwarz, blau oder rot – eintragen).