

Übungen zur Vorlesung
 Programmanalyse
 Blatt 11

Abgabe bis 24.01.2024

Aufgabe 11.1 (Abstraktionsverfeinerung)

Betrachten Sie das folgende Programm. Dieses berechnet für $x, y \in \mathbb{N}$ das Produkt $z = x \cdot y$. Zeigen Sie mittels CEGAR-loop, dass Block 8 nicht erreichbar ist.

```

[z := 0]1
if [x > 0]2 then
  if [y > 0]3 then
    while [x > 0]4 do
      [z := z + y]5
      [x := x - 1]6
    if [z = 0]7 then
      [skip]8
    else
      [skip]9
  else
    [skip]10
else
  [skip]11

```

Aufgabe 11.2 (Echte Gegenbeispiele)

Beweisen Sie folgendes Lemma aus der Vorlesung:

Sei $c = (c_0, q_0) \Rightarrow \dots \Rightarrow (c_k, q_k)$ ein Gegenbeispiel, wobei $q_0 \models true$. Ferner sei $r = r_1; \dots; r_k$ der zu c assoziierte Ablauf. Dann gilt:

Gegenbeispiel c ist unecht genau dann, wenn $\models \{true\} r \{false\}$.

Gehen Sie dazu wie folgt vor.

- a) Zeigen Sie zuerst die Richtung " \Leftarrow " per Kontraposition: Wenn c echt ist, dann ist das Hoare Tripel $\models \{true\} r \{false\}$ nicht gültig. Sie dürfen dabei annehmen, dass folgende Aussage gilt.

Wenn $(c_0, \sigma_0) \rightarrow \dots \rightarrow (c_k, \sigma_k)$, dann $(r_1; \dots; r_k, \sigma_0) \rightarrow \dots \rightarrow (r_k, \sigma_{k-1}) \rightarrow \sigma_k$.

- b) Zeigen Sie nun die Richtung " \Rightarrow " per Kontraposition: Wenn $\not\models \{true\} r \{false\}$, dann ist c echt. Dafür zeigen Sie zuerst (unter Annahme $\not\models \{true\} r \{false\}$), dass $\sigma_0, \sigma_1, \dots, \sigma_k \in State$ existieren mit $\sigma_0 \models true$ und $\sigma_k \not\models false$, so dass

$(r_1; \dots; r_k, \sigma_0) \rightarrow \dots \rightarrow (r_k, \sigma_{k-1}) \rightarrow \sigma_k$

eine valide Ableitung in Small-Step Semantik ist.

- c) Um den Beweis abzuschließen, zeigen Sie per Induktion, dass $\sigma_i \models q_i$. Nutzen Sie folgende Einsicht: Es gilt $(r_{i+1}, \sigma_i) \rightarrow \sigma_{i+1}$, falls $(r_{i+1}; \dots; r_k, \sigma_i) \rightarrow (r_{i+2}; \dots; r_k, \sigma_{i+1})$ und r ein Ablauf ist.