WS 2017/2018 17.01.2018

Übungen zur Vorlesung
Programmanalyse
Blatt 11

Prof. Dr. Roland Meyer,
M. Sc. Sebastian Wolff
M. Sc. Elisabeth Neumann Abgabe bis 24.01.2018 um 12 Uhr

Aufgabe 11.1 (Prädikatenabstraktion)
Betrachten Sie das folgende Programm:

$[x := 1]^1$
$[y := 0]^2$
while $[x > 0]^3$ **do**
  $[x := x - 1]^4$
  $[y := y + 1]^5$
if $[y = 0]^6$ **then**
  $[x := 1]^7$

Zeigen Sie mittels Prädikatenabstraktion, dass die Anweisung $[x := 1]^7$ nicht erreichbar ist. Wählen Sie dafür geeignete Prädikate und geben Sie die abstrakte Transitionsrelation ausgehend vom Startzustand true an.

Aufgabe 11.2 (Control-State-Reachability)
Eine *Safety-Eigenschaft* oder *Invariante* eines Programms ist eine Menge **Safe** $\subseteq$ **Prog** $\times$ **State** von Konfigurationen. Man sagt, die Eigenschaft ist *erfüllt*, falls alle erreichbaren Konfigurationen in **Safe** liegen, anderenfalls ist sie *verletzt*. Beispiele für Safety-Eigenschaften sind z.B.: „Es gibt keine Divisionen durch 0“ oder „Die Variable x ist immer positiv“.
Erklären Sie, wie man die Überprüfung von Safety-Eigenschaften eines Programms auf einen Erreichbarkeitscheck für einen Kontrollzustand c_{bad} reduzieren kann. Machen Sie Ihre Vorgehensweise an einem der obigen Beispiele deutlich.

Aufgabe 11.3 (Echte Gegenbeispiele)
Machen Sie sich mit dem Begriff des Ablaufs (Line-Program) vertraut. Lesen Sie dazu die zugehörige Bemerkung und das Beispiel auf Seite 2 der handschriftlichen Notizen zu der Abstraktionsverfeinerung. Danach beweisen Sie folgendes Lemma:

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

Gegenbeispiel c ist unecht (spurious) *gdw.* $\models \{\text{true}\}\ r\ \{\text{false}\}$

Gehen Sie dazu wie folgt vor.

a) Zeigen Sie zuerst die Richtung $''\Leftarrow''$ mit Kontraposition:

Wenn c echt ist, dann gilt $\not\models \{\text{true}\}\ r\ \{\text{false}\}$.

Sie dürfen dabei annehmen dass folgende Aussage gilt.

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

b) Zeigen Sie nun die Richtung $''\Rightarrow''$ per Kontraposition, also:

Wenn $\not\models \{\text{true}\}\ r\ \{\text{false}\}$, dann ist c echt.

Dafür zeigen Sie zuerst (unter Annahme $\not\models \{\text{true}\}\ r\ \{\text{false}\}$) dass $\sigma_0, \sigma_1, \ldots, \sigma_k \in \mathit{State}$ existieren mit $\sigma_0 \models \text{true}$ und $\sigma_k \not\models \text{false}$, so dass

$$(r_1; \ldots; r_k, \sigma_0) \to \cdots \to (r_k, \sigma_{k-1}) \to \sigma_k$$

eine valide Ableitung in Small-Step Semantik ist.

c) Um den Beweis abzuschliessen, zeigen Sie dass $\sigma_i \models q_i$ (damit ist c echt). Bemerken Sie dass $(r_{i+1}, \sigma_i) \to \sigma_{i+1}$ gilt, da $(r_{i+1}; \ldots; r_k, \sigma_i) \to (r_{i+2}; \ldots; r_k, \sigma_{i+1})$ und r ein Ablauf ist.

Abgabe bis 24.01.2018 um 12 Uhr im Kasten neben Raum IZ 343