

13. Übung zum Modul Kommunizierende und mobile Systeme

Aufgabe 1 (Starke Äquivalenz):

3 Punkte

Zeigen Sie $P_i \sim Q_i, i \in \{0, 2\}$ für die angegebenen Prozesse.

$$\begin{array}{ll} P_0 \stackrel{\text{def}}{=} !x(a) & Q_0 \stackrel{\text{def}}{=} x(a) !x(a) \\ P_1 \stackrel{\text{def}}{=} \text{new } x(x(a) | \bar{x}(b) | y(b)) & Q_1 \stackrel{\text{def}}{=} \tau.y(c) + y(a).\tau \\ P_2 \stackrel{\text{def}}{=} x(a).\bar{a}(c) & Q_2 \stackrel{\text{def}}{=} x(b).\bar{b}(c) \end{array}$$

Aufgabe 2 (Wide-mouthed-frog-protocol):

3 Punkte

Betrachten Sie für die Implementierung des *wide-mouthed-frog-protocols* folgende Prozesse:

$$\begin{array}{l} ALICE \stackrel{\text{def}}{=} \text{new } key_{AB} \overline{key_A}(key_{AB}).\overline{key_{AB}}(m) \\ BOB \stackrel{\text{def}}{=} key_B(key_{AB}).key_{AB}(m) \\ SERVER \stackrel{\text{def}}{=} key_A(key).\overline{key_B}(key) \end{array}$$

Zeigen Sie, dass die Implementierung

$$\text{new } key_A, key_B (ALICE | SERVER | BOB)$$

die folgende Spezifikation erfüllt:

Nach außen sind nur drei τ -Transitionen sichtbar, wenn die Schlüssel key_A und key_B nicht bekannt sind.

Formalisieren Sie dazu diese Spezifikation als π -Kalkül-Prozess $SPEC$ und zeigen Sie

$$\text{new } key_A, key_B (ALICE | SERVER | BOB) \sim SPEC$$

Aufgabe 3 (Rekursionstiefe):

6 Punkte

In der Vorlesung wurde für den Beweis von $!P \not\equiv !!P$ die Replikationstiefe rd eines π -Kalkül Prozesses P benutzt.

- Geben Sie eine induktive Definition der Funktion $rd : \mathcal{P}_\pi \rightarrow \mathbb{N}$ an.
- Zeigen Sie durch strukturelle Induktion die Implikation

$$P \equiv Q \Rightarrow rd(P) = rd(Q).$$

- Zeigen Sie

$$!P \not\equiv !P | P$$

Hinweis: Benutzen Sie eine Bewertungsfunktion ähnlich zu rd .