

Prozessalgebra

Aufgabe 5-1

Iterationsoperatoren

Wir schreiben \mathcal{P}_i für die Menge aller Prozesse, die aus den atomaren Aktionen, den Operatoren $+$, \cdot und den (neuen) Iterationsoperatoren $*$ und ω konstruiert werden können. Es sei $\Delta_{i0} = \{(p, p) \mid p \in \mathcal{P}_{i0}\}$.

a) Transitionssystem für a^*

$$a \circlearrowleft a^* \xrightarrow{a} \checkmark$$

Transitionssystem für a^ω

$$a \circlearrowleft a^\omega$$

b) Es gilt $p^* \Leftrightarrow p + p \cdot p^*$. Wir zeigen dazu, dass die Relation $\beta = \{(p^*, p + p \cdot p^*) \mid p \in \mathcal{P}_{i0}\} \cup \Delta_{i0}$ eine Bisimulation ist.

(BS1) Sind $(p, q) \in \beta$, so gilt entweder $p \equiv q$, und es ist nichts zu zeigen, oder $p = r^*$ und $q = r + rr^*$. Gelte $p \xrightarrow{a} p'$ mit $p' \neq \checkmark$. Wir unterscheiden die folgenden Fälle gemäß den Konklusionen der Transitionsregeln; in jedem der Fälle geben wir q' an mit $q \xrightarrow{a} q'$ und $(p', q') \in \beta$.

Fall 1. $p' = r'r^*$ und $r \xrightarrow{a} r'$. Dann gilt für $q' \equiv r'r^*$ dass $q \equiv r + rr^* \xrightarrow{a} r'r^*$ und da $(q', q') \in \beta$ ist (BS1) erfüllt.

Fall 2. $p' \equiv r'$ und $p \xrightarrow{a} p'$. Setze $q' \equiv p' \equiv r'$.

Fall 3. $p' \equiv r^*$ und $r \xrightarrow{a} \checkmark$. Setze für $q' \equiv r^*$.

(BS2) Umgekehrt analog.

(BS3) Es gilt $r^* \xrightarrow{a} \checkmark$ gdw. $r \xrightarrow{a} \checkmark$ gdw. $r + rr^* \xrightarrow{a} \checkmark$.

c) Es gilt nicht, dass $(p^*)^* \Leftrightarrow p^*$. Annahme, doch. Dann gibt es für $p \equiv a$ eine Bisimulation β mit $((a^*)^*, a^*) \in \beta$. Da $(a^*)^* \xrightarrow{a} a^* \cdot (a^*)^*$ nach den Transitionsregeln(!), muss es also ein q geben mit $a^* \xrightarrow{a} q$ und $(a^* \cdot (a^*)^*, q) \in \beta$. Da $a^* \xrightarrow{a} q$, muss $q \equiv a^*$ gelten. Somit also $(a^* \cdot (a^*)^*, a^*) \in \beta$. Dieses Paar verletzt aber (BS3), da $a^* \xrightarrow{a} \checkmark$ aber $a^* \cdot (a^*)^* \xrightarrow{a} \checkmark$ nicht möglich ist.

d) Wir zeigen, dass $(p^\omega)^\omega \Leftrightarrow p^\omega$ durch Angabe einer Bisimulation. Betrachte die Relation β gegeben durch $(s, t) \in \beta$, falls

1. $s \equiv t$, oder
2. $s \equiv (p^\omega)^\omega$ und $t \equiv p^\omega$, oder
3. $s \equiv p'p^\omega r$ und $t \equiv p'p^\omega$, oder
4. $s \equiv p^\omega r$ und $t \equiv p^\omega$.

Wir zeigen, dass β eine Bisimulation ist.

(BS1) Sei $(s, t) \in \beta$. Wir unterscheiden die verschiedenen Fälle für (s, t) , wobei im ersten Fall $(s \equiv t)$ nichts zu zeigen ist.

Betrachte nun $s \equiv (p^\omega)^\omega$ und $t \equiv p^\omega$ und gelte $s \xrightarrow{a} s'$. Wir unterscheiden die folgenden Fälle, wobei wir jeweils t' angeben mit $t \xrightarrow{a} t'$ und $(s', t') \in \beta$.

Fall 1: Es gilt $s' \equiv p'(p^\omega)^\omega$ mit $p^\omega \xrightarrow{a} p'$, also $p' \equiv p^\omega$ oder $p' \equiv p''p^\omega$ wobei $p \xrightarrow{a} p'$.

Fall 1.1 $s' \equiv p^\omega(p^\omega)^\omega$. Setze $t' \equiv p^\omega$.

Fall 1.2 $s' \equiv p''p^\omega(p^\omega)^\omega$. Wäle $t' \equiv p''p^\omega$.

Fall 2. Es gilt $s' \equiv (p^\omega)^\omega$ und $P^\omega \xrightarrow{a} p'$. Setze $t' \equiv p^\omega$.

Wir betrachten nun den Fall $s \equiv p'p^\omega r$ und $t \equiv p'p^\omega$. Gelte $s \xrightarrow{a} s'$. Dann gilt $p' \xrightarrow{a} p''$ und $s' \equiv p''p^\omega r$ oder $p' \xrightarrow{a} \checkmark$ und $s' \equiv p^\omega r$. Wie oben geben wir t' an mit $t \xrightarrow{a} t'$ und $(s', t') \in \beta$.

Fall 1. $p' \xrightarrow{a} p''$ mit $p'' \neq \checkmark$ und $s' \equiv p''p^\omega r$. Setze $t' \equiv p''p^\omega$.

Fall 2. $p' \xrightarrow{a} \checkmark$ und $s' \equiv p^\omega r$. Setze $t' \equiv p^\omega$.

Sei nun $s \equiv p^\omega r$ und $t \equiv p^\omega$. Gelte $s \xrightarrow{a} s'$ mit $s' \neq \checkmark$. Dann gilt $s' \equiv p'p^\omega r$ mit $p \xrightarrow{a} p'$ oder $s' \equiv p^\omega r$ mit $p \xrightarrow{a} p'$.

Fall 1. $s' \equiv p'p^\omega r$ und $p \xrightarrow{a} p'$. Setze $t' \equiv p'p^\omega$.

Fall 2. $s' \equiv p^\omega r$. Setze $t' \equiv p^\omega$. Damit wäre (BS1) gezeigt.

(BS2) Analog, aber umgekehrt.

(BS3) kann nicht passieren.

e) Die Prozesse $p \cdot (q \cdot p)^\omega$ und $(p \cdot q)^\omega$ sind bisimilar; wir zeigen dies durch Angabe einer Bisimulation. Betrachte $\beta \subseteq \mathcal{P}_{i0} \times \mathcal{P}_{i0}$ gegeben durch $(s, t) \in \beta$, falls einer der folgenden Fälle vorliegt.

1. $s \equiv p(qp)^\omega, t \equiv (pq)^\omega$
2. $s \equiv r(qp)^\omega, t \equiv rq(pq)^\omega$
3. $s \equiv (qp)^\omega, t \equiv q(pq)^\omega$
4. $s \equiv rp(qp)^\omega, t \equiv r(pq)^\omega$.

Wir zeigen nun, dass es sich bei β um eine Bisimulation handelt.

(BS1) Wir betrachten $(s, t) \in \beta$ mit $s \xrightarrow{a} s'$ und unterscheiden die verschiedenen Möglichkeiten für s und t . In allen Fällen geben wir t' an mit $t \xrightarrow{a} t'$ und $(s', t') \in \beta$.

Gelte $s \equiv p(qp)^\omega$ und $t \equiv (pq)^\omega$. Da $s \xrightarrow{a} s'$ haben wir zwei Möglichkeiten: $p \xrightarrow{a} p' \neq \checkmark$ und $s' \equiv p'(qp)^\omega$ und $p \xrightarrow{a} \checkmark$ und $s' \equiv (qp)^\omega$.

Fall 1. $p \xrightarrow{a} p' \neq \checkmark$ und $s' \equiv p'(qp)^\omega$. Setze $t' \equiv p'q(pq)^\omega$.

Fall 2. $p \xrightarrow{a} \checkmark$ und $s' \equiv (qp)^\omega$. Setze $t' \equiv q(pq)^\omega$.

Sei nun $s \equiv r(qp)^\omega$ und $t \equiv rq(pq)^\omega$. Da $s \xrightarrow{a} s'$ haben wir wieder zwei Möglichkeiten: $r \xrightarrow{a} r' \neq \checkmark$ und $s' \equiv r'(qp)^\omega$ oder $r \xrightarrow{a} \checkmark$ und $s' \equiv (qp)^\omega$.

Fall 1. $r \xrightarrow{a} r' \neq \checkmark$ und $s' \equiv r'(qp)^\omega$. Setze $t' \equiv r'q(pq)^\omega$.

Fall 2. $r \xrightarrow{a} \checkmark$ und $s' \equiv (qp)^\omega$. Setze $t' \equiv q(pq)^\omega$.

Die Anderen Möglichkeiten $(s \equiv (qp)^\omega$ und $t \equiv q(pq)^\omega$ sowie $s \equiv rp(qp)^\omega$ und $t \equiv r(pq)^\omega$) ergeben sich durch vertauschen von p und q .

(BS2) Analog, andersherum.

(BS3) offensichtlich erfüllt, da keine Seite terminieren kann.

Aufgabe 5-2**Mehrfachausführung atomarer Aktionen**

(keine Abgabe)

Wir zeigen die Behauptung durch Induktion nach i . Für $i = 1$ erhalten wir $a \parallel a \stackrel{(P6)}{=} a \parallel a + a \parallel$
 $_ a \stackrel{(P3)}{=} a \parallel a \stackrel{(P7)}{=} a = a^2$.

Für $i \rightarrow i + 1$ berechnen wir

$$a \parallel a^{i+1} = a \parallel a^{i+1} + a^{i+1} \parallel a \quad (P6)$$

$$= a \cdot a^{i+1} + a^{i+1} \parallel a \quad (P7)$$

$$= a^{i+2} + a(a^i \parallel a) \quad (P8)$$

$$= a^{i+2} + a(a^i \parallel a + a \parallel a^i) \quad (P6)$$

$$= a^{i+2} + a(a \parallel a^i + a^i \parallel a) \quad (P1)$$

$$= a^{i+2} + a(a \parallel a^i) \quad (P6)$$

$$= a^{i+2} + aa^{i+1} \quad (IV)$$

$$= a^{i+2} + a^{i+2}$$

$$= a^{i+2} \quad (P3)$$

und die Behauptung ist bewiesen.

Aufgabe 5-3**Gleichheiten in \mathcal{P}_1**

(8 Punkte)

a) Sei $p \equiv (a + b) \parallel c$. Dann gilt mit $q \equiv ac + bc + c(a + b)$ dass $q \in \mathcal{P}_{\text{prä}}$, denn $p \stackrel{(P6)}{=} (a + b) \parallel$
 $_ c + c \parallel (a + b) \stackrel{(P9)}{=} a \parallel c + b \parallel c + c \parallel (a + b) \stackrel{(P7)}{=} ac + bc + c(a + b)$.

b) Sei $p \equiv aa \parallel bb$. Mit $q \equiv a(abb + b(ba + ab)) + b(baa + a(ab + ba))$ gilt $q \in \mathcal{P}_{\text{prä}}$ und $p = q$,
 denn

$$aa \parallel bb = aa \parallel bb + bb \parallel aa \quad (P6)$$

$$= a(a \parallel bb) + b(b \parallel aa) \quad (P8)$$

$$= a(a \parallel bb + bb \parallel a) + b(b \parallel aa + aa \parallel b) \quad (P6)$$

$$= a(abb + b(b \parallel a)) + b(baa + a(a \parallel b)) \quad (P7, P8)$$

$$= a(abb + b(b \parallel a + a \parallel b)) + b(baa + a(a \parallel b + b \parallel a)) \quad (P6)$$

$$= a(abb + b(ba + ab)) + b(baa + a(ab + ba)) \quad (P7)$$

c) Sei $p \equiv (a + b) \parallel (a + b)$. Wir setzen $q \equiv a(a + b) + b(a + b)$. Dann gilt $p = q$, denn

$$(a + b) \parallel (a + b) = (a + b) \parallel (a + b) + (a + b) \parallel (a + b) \quad (P6)$$

$$= (a + b) \parallel (a + b) \quad (P3)$$

$$= a \parallel (a + b) + (a + b) \parallel a \quad (P8)$$

$$= a(a + b) + b(a + b). \quad (P7)$$

d) Sei $p \equiv abc \parallel (d + e)$. Setze $q \equiv a(b(c(d + e) + dc + ec) + dbc + ebc) + dabc + eabc$. Dann gilt

$p = q$, denn

$$\begin{aligned}
 abc \parallel (d + e) &= abc \parallel (d + e) + (d + e) \parallel abc && (P8) \\
 &= a(bc \parallel (d + e)) + d \parallel abc + e \parallel abc && (P8, P9) \\
 &= a(bc \parallel (d + e) + (d + e) \parallel bc) + dabc + eabc && (P6, P7) \\
 &= a(b(c \parallel (d + e)) + d \parallel bc + e \parallel bc) + dabc + eabc && (P8, P9) \\
 &= a(b(c \parallel (d + e) + (d + e) \parallel c) + dbc + ebc) + dabc + eabc && (P6, P7) \\
 &= a(b(c(d + e) + d \parallel c + e \parallel c) + dbc + ebc) + dabc + eabc && (P7, P9) \\
 &= a(b(c(d + e) + dc + ec) + dbc + ebc) + dabc + eabc. && (P7)
 \end{aligned}$$

Aufgabe 5-4 **Fahrkartenautomat mit Wechselgeld** (4 Punkte)

Wir betrachten die Menge \mathcal{A} von atomaren Aktionen mit der folgenden Bedeutung:

- K : Kurzstreckenfahrkarte
- L : Langstreckenkarte
- \bar{K} : Ausgabe Kurzstreckenkarte
- \bar{L} : Ausgabe Langstreckenkarte
- 1€ : Einwurf 1 €
- 2€ : Einwurf 2 €
- 5€ : Einwurf 5 €
- $\overline{3\text{€}}$: Ausgabe 3 €
- $\overline{2\text{€}}$: Ausgabe 2 €
- $\overline{1\text{€}}$: Ausgabe 1 €
- a : Auffüllung Wechselgeld.

Weiterhin vereinbaren wir die folgenden Abkürzungen.

- $k_1 \equiv 1\text{€}\bar{K}$
- $k_2 \equiv 2\text{€}\overline{K1\text{€}}$
- $k_3 \equiv 5\text{€}\overline{K2\text{€}}$
- $l_1 \equiv 1\text{€} \cdot 1\text{€} \cdot \bar{L}$
- $l_2 \equiv 2\text{€}\bar{L}$
- $l_3 \equiv 5\text{€}\overline{L3\text{€}}$

Die Aktionsfolgen k_i modellieren die verschiedenen Möglichkeiten, eine Kurzstreckenkarte zu kaufen; mit den l_i werden die Langstreckenkarten verkauft ($i = 1, 2, 3$).

Verfügt der Automat über *nicht* genügend Wechselgeld, so kann eine Fahrkarte nur dann gekauft werden, wenn das Geld passend eingeworfen wird. Es sind also folgende Aktionen möglich:

$$R \equiv (Kk_1 + L(l_1 + l_2))^*$$

Ist genügend Wechselgeld vorhanden, so können folgende Aktionen durchgeführt werden:

$$G \equiv K(k_1 + k_2 + k_3) + L(l_1 + l_2 + l_3)^*$$

Die Definition von R und G mittels “*” trägt der Tatsache Rechnung, dass der Wechselgeldspeicher irgendwann aufgefüllt werden muss (im Falle von R – dh. R wird endlich oft ausgeführt und terminiert irgendwann) bzw. dass das Wechselgeld ausgeht (im Falle von G). Wir nehmen an, dass der Automat anfangs über genug Wechselgeld verfügt, dh. zunächst ist G möglich, dann geht das Wechselgeld aus, dann ist noch R möglich, und schliesslich wird das Wechselgeld aufgefüllt. Dieser Prozess wird unendlich oft wiederholt. Wir erhalten also insgesamt

$$A \equiv (GRa)^\omega$$

für den Automaten.