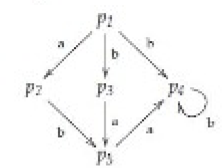
5.3 Definition („Model-Checking-Semantik“ von HML; S. 96 in [AILS07])

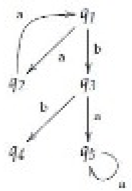
Sei $T = (\mathsf{Proc}, \mathsf{Act}, \mathsf{Tran})$, mit $\mathcal{M}$ definiert über Act.
Die Relation $\models : (\mathsf{Proc}, \mathcal{M})$ ist induktiv definiert durch:

p	$\models$	tt	für alle $p \in \mathsf{Proc}$
p	$\models$	ff	für kein $p \in \mathsf{Proc}$
p	$\models$	$F \wedge G$	falls $p \models F$ und $p \models G$
p	$\models$	$F \vee G$	falls $p \models F$ oder $p \models G$
p	$\models$	$[\alpha]F$	falls für alle $p' \in \mathrm{Der}(p, \alpha)$ gilt $p' \models F$
p	$\models$	$\langle\alpha\rangle F$	falls es $p' \in \mathrm{Der}(p, \alpha)$ gibt mit $p' \models F$

Aufgabe 2: Hennessy-Milner Logik: Semantik I

Gegeben sei folgendes LTS:





2.a) Werte die Formeln aus:

(i) $F_1 = tt$
(ii) $F_2 = \langle a\rangle tt$
(iii) $F_3 = \langle b\rangle tt$
(iv) $F_4 = [a]tt$
(v) $F_5 = \langle a\rangle ff$
(vi) $F_6 = [b]ff$
(vii) $F_7 = [b]ff \wedge [a]ff$
(viii) $F_8 = [b]([b]ff \wedge [a]ff)$
(ix) $F_9 = [a](\langle a\rangle tt \wedge \langle b\rangle tt)$
(x) $F_{10} = \langle b\rangle(\langle a\rangle[a]ff \vee \langle b\rangle tt)$
(xi) $F_{11} = [b](\langle b\rangle tt \wedge (\langle a\rangle tt \vee \langle b\rangle tt))$

$[\![tt]\!] = \mathsf{Proc}$
$[\![\langle a\rangle tt]\!] = \{p_1, p_3, p_5\}$
$[\![[a]tt]\!] = \{p_1, p_2, \dots, p_5\}$
$\mathrm{Der}(p_1, a) = \{p_2\} \subseteq \mathsf{Proc} = [\![tt]\!]$
$\mathrm{Der}(p_2, a) \subseteq \mathsf{Proc} = [\![tt]\!]$

2.b) Welche der folgenden Aussagen sind korrekt? Begründe deine Antwort.
(i) $p_2 \models F_4$ □ (ii) $p_4 \models F_5$ □ (iii) $p_3 \models F_7$ □ (iv) $p_5 \models F_8$ □

$[\![\langle a\rangle tt \wedge \langle b\rangle tt]\!] = \{p_1\}$

$[\![\langle \alpha\rangle ff]\!] = \{\cancel{p_1}, p_2, p_3, p_4, p_5\} = \emptyset$

$[\![[b]ff]\!] = \{\cancel{p_1}, \cancel{p_2}, p_3, \cancel{p_4}, p_5\}$

$[\![[b]ff \wedge [\quad]]\!] = \emptyset$

$[\![F_8]\!] = \{\cancel{p_1}, p_2, \cancel{p_3}, p_4, \cancel{p_5}\} =$

$[a]\{p_1\} = \{\cancel{p_1}, p_2, \cancel{p_3}, p_4, \cancel{p_5}\}$

5.4 Definition (Denotationelle HML-Semantik; Def. 5.2 in [AILS07])

Sei $T = (\mathsf{Proc}, \mathsf{Act}, \mathsf{Tran})$, mit $\mathcal{M}$ definiert über Act.
Die Funktion $[\![\cdot]\!] : \mathcal{M} \to 2^{\mathsf{Proc}}$ ist induktiv definiert durch:

$$
\begin{aligned}
[\![tt]\!] &\triangleq \mathsf{Proc} \\
[\![ff]\!] &\triangleq \emptyset \\
[\![F \wedge G]\!] &\triangleq [\![F]\!] \cap [\![G]\!] \\
[\![F \vee G]\!] &\triangleq [\![F]\!] \cup [\![G]\!] \\
[\![[\alpha]F]\!] &\triangleq [\cdot\alpha\cdot][\![F]\!] \\
[\![\langle\alpha\rangle F]\!] &\triangleq \langle\cdot\alpha\cdot\rangle[\![F]\!]
\end{aligned}
$$

wobei die Operatoren $[\cdot\alpha\cdot], \langle\cdot\alpha\cdot\rangle : 2^{\mathsf{Proc}} \to 2^{\mathsf{Proc}}$ gegeben sind durch:

$$
\begin{aligned}
[\cdot\alpha\cdot]S &\triangleq \{\, p \in \mathsf{Proc} \mid \forall p' \in \mathrm{Der}(p, \alpha)\ .\ p' \in S \,\} = \{p \in \mathsf{Proc} \mid \mathrm{Der}(p, \alpha) \subseteq S\} \\
\langle\cdot\alpha\cdot\rangle S &\triangleq \{\, p \in \mathsf{Proc} \mid \exists p' \in \mathrm{Der}(p, \alpha)\ .\ p' \in S \,\}
\end{aligned}
$$

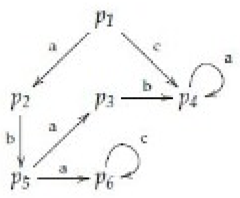
Die Semantik $[\![\cdot]\!]$ für die n-stelligen Varianten $\bigwedge$ und $\bigvee$ ergibt sich analog durch die n-stelligen Varianten $\bigcap$ und $\bigcup$.

$[\![\langle a\rangle[a]ff]\!]$ Menge aller Prozesse, die p2 oder p4 als a-Nachfolger haben

$= \{p_2, p_4\}$

$= \{p_1, \cancel{p_2}, \cancel{p_3}, \cancel{p_4}, p_5\} = \{p_1, p_5\}$

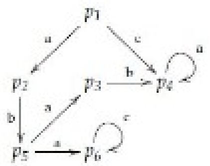
Logik: Semantik II



$[\![\langle c\rangle\langle c\rangle tt]\!] = \{p_6\}$
$[\![\langle a\rangle\langle a\rangle tt]\!] = \{p_4\}$
$F_7 = \quad [\![\langle b\rangle tt]\!] = \{p_3, p_2$

Aufgabe 3: Hennessy-Milner Logik: Semantik II

Gegeben sei folgendes LTS:



3.a) Gegeben seien die Mengen A_1, A_2, A_3 wie folgt:

(i) $A_1 = \{p_2, p_3\}$ (ii) $A_2 = \{p_1\}$ (iii) $A_3 = \{p_2, p_3, p_4, p_6\}$

$F_1 = \langle b \rangle tt$

$F_2 = \langle a \rangle tt \wedge \langle c \rangle tt$

$F_1 =$ Prozesse, die b-Nachfolger haben

$\langle b \rangle tt$

$F_2 =$ Prozesse, die sowohl a-Nachfolger als auch b-Folger haben

1/2

$[\![\langle c \rangle \langle c \rangle tt]\!] = \{p_6\}$

$[\![\langle a \rangle \langle a \rangle tt]\!] = \{p_4\}$

$F_3 = \quad [\![\langle b \rangle tt]\!] = \{p_3, p_2\}$

$\langle c \rangle \langle c \rangle tt \vee \langle a \rangle \langle a \rangle tt \vee \langle b \rangle tt$

$[a]\{p_1\} = \{\cancel{p_1}, p_2, \cancel{p_3}, p_4, \cancel{p_5}\}$

$[\![[b] ff]\!] = \{\cancel{p_1}, \cancel{p_2}, p_3, \cancel{p_4}, p_5\}$

$[\![[b] ff \wedge [\quad]]\!] = \emptyset$

$[\![ff]\!] = \{\cancel{p_1}, p_2, \cancel{p_3}, p_4, \cancel{p_5}\} =$

$[\![\langle a \rangle [a] ff]\!]^c$

$= \{p_2, p_4\}$

$= \{p_1, \cancel{p_2}, \cancel{p_3}, \cancel{p_4}, p_5\} = \{p_1, p_3, p_5\}$

Finde drei Hennessy-Milner Formeln F_1, F_2, F_3, passend zum LTS, so dass $[\![F_1]\!] = A_1$, $[\![F_2]\!] = A_2$ und $[\![F_3]\!] = A_3$.

3.b) Formalisiere die folgenden Aussagen:

(i) Eine a-Aktion ist möglich. $\langle \alpha \rangle tt$

(ii) Nach jeder b-Aktion ist eine a-Aktion möglich. $[b]\langle a \rangle tt$

(iii) Nach jeder c-Aktion ist eine b-Aktion möglich.

(iv) Nach jeder c-Aktion gilt, es ist eine b-Aktion oder eine a-Aktion möglich.

(v) Es ist keine c-Aktion möglich.

(vi) Es ist weder eine a-Aktion, noch eine b-Aktion möglich.

(vii) Es ist sowohl eine a-Aktion, als auch eine b-Aktion möglich.

In welchen Zuständen des LTS gilt jede dieser Formeln?

ii) $[b]\langle a \rangle tt$

iii) $[c]\langle b \rangle tt$

iv) $[c](\langle a \rangle tt \vee \langle b \rangle tt)$

v) $[c] ff$

vi) $[a] ff \wedge [b] ff$

vii) $\langle a \rangle tt \wedge \langle b \rangle tt$

5.7 Definition (Negation)

Sei $T = (\mathsf{Proc}, \mathsf{Act}, \mathsf{Tran})$, mit $\mathcal{M}$ definiert über Act.
Die Funktion $(\cdot)^c : \mathcal{M} \to \mathcal{M}$ ist gegeben durch:

1) $(tt)^c \triangleq ff$

2) $(ff)^c \triangleq tt$

3) $(F \wedge G)^c \triangleq (F)^c \vee (G)^c$

4) $(F \vee G)^c \triangleq (F)^c \wedge (G)^c$

5) $([\alpha]F)^c \triangleq \langle \alpha \rangle (F)^c$

6) $(\langle \alpha \rangle F)^c \triangleq [\alpha] (F)^c$

Es gilt für alle $F \in \mathcal{M}$:

1. $[\![(F)^c]\!] = \mathsf{Proc} \setminus [\![F]\!]$;
2. $((F)^c)^c = F$.

Aufgabe 1: Komplementierung

Zeige, dass die folgende Aussage gilt: $\forall F \in \mathcal{M}.\ (F^c)^c = F$

Beweis mit struktureller Induktion

IA $F = tt$:

$(F^c)^c = ((tt)^c)^c = (ff)^c = tt = F$

IA $F = ff$

IV: Seien F, G Formel mit $(F^c)^c = F$ und $(G^c)^c = G$

IS: zu zeigen: $((F \vee G)^c)^c = F \vee G$

$((F \vee G)^c)^c \overset{4)}{=} (F^c \wedge G^c)^c =$

$\overset{3)}{=} (F^c)^c \vee (G^c)^c = F \vee G$ ☒

IV

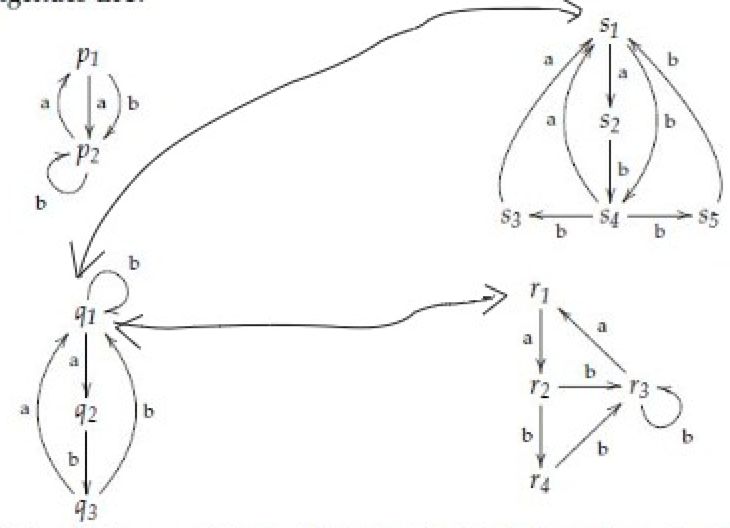
2. $((F)^c)^c = F$.

$\underline{IV}$: Sein F, G

$(G^c) = G$

Aufgabe 2: Unterscheidende Formeln

2.a) Gegeben sei folgendes LTS:



$p_1 \in [\![\langle a\rangle\langle a\rangle tt]\!]$

$q_1 \notin [\![\langle a\rangle\langle a\rangle tt]\!]$

ii) $\langle b\rangle\langle a\rangle\langle b\rangle tt$

iii) $\langle b\rangle tt$

Gelten unten stehende Aussagen? Falls nicht, gib eine HML-Formel an, die die jeweiligen Prozesse unterscheidet.

(i) $p_1 \sim q_1$
(ii) $q_1 \sim s_1$
(iii) $q_1 \sim r_1$

5.10 Theorem (Hennessy-Milner-Theorem; Theorem 5.1 in [AILS07])
Sei $T = (Proc, Act, Tran)$ Bild-endlich.
Seien $p, q \in Proc$.
Dann gilt:

$$p \sim q \quad \text{genau dann, wenn} \quad [\![p]\!] = [\![q]\!]$$

$$p \sim_i q \quad \text{genau dann, wenn} \quad [\![p]\!]^{\leqslant i} = [\![q]\!]^{\leqslant i}$$

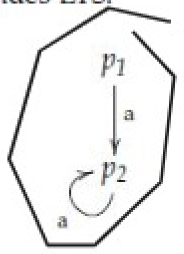
5.3 Definition („Model-Checking-Semantik" von HML; S. 96 in [AILS07])

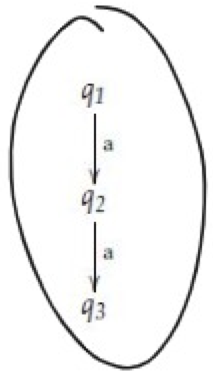
Sei $T = (Proc, Act, Tran)$, mit $\mathcal{M}$ definiert über Act.
Die Relation $\models : (Proc, \mathcal{M})$ ist induktiv definiert durch:

$p \models tt$		für alle $p \in Proc$
$p \models ff$		für kein $p \in Proc$
$p \models F \wedge G$		falls $p \models F$ und $p \models G$
$p \models F \vee G$		falls $p \models F$ oder $p \models G$
$p \models [\alpha]F$		falls für alle $p' \in Der(p, \alpha)$ gilt $p' \models F$
$p \models \langle\alpha\rangle F$		falls es $p' \in Der(p, \alpha)$ gibt mit $p' \models F$

Aufgabe 3: n-Bisimulation und das Hennessy-Milner-Theorem

Gegeben sei folgendes LTS:





3.a) Bestimme $\sim_0, \sim_1, \sim_2$ und $\sim_3$.
3.b) Gilt $(q_2, q_3) \in \sim_1$? Falls nicht, begründe deine Antwort.
3.c) Begründe: p_1 und q_1 sind 2-bisimilar.
3.d) Wie stehen $\sim_{i+1}$ und $\sim_i$ in Beziehung?
3.e) Gilt $p_1 \sim q_1$? Begründe deine Antwort.

5.10 Theorem (Hennessy-Milner-Theorem; Theorem 5.1 in [AILS07])

Sei $T = (\mathrm{Proc}, \mathrm{Act}, \mathrm{Tran})$ Bild-endlich.
Seien $p, q \in \mathrm{Proc}$.
Dann gilt:

$$p \sim q \quad \text{genau dann, wenn} \quad [\![p]\!] = [\![q]\!]$$

$$p \sim_i q \quad \text{genau dann, wenn} \quad [\![p]\!]^{\leqslant i} = [\![q]\!]^{\leqslant i}$$

3a) $\sim_0 = Proc \times Proc$

Formeln mit Modaltiefe $\leq 1 = \{\langle a\rangle tt, \langle\alpha\rangle ff, [\alpha]ff, [\alpha]tt, \dots\}$
$\langle\alpha\rangle tt \vee [\alpha]ff, \dots$

$\sim_1 = s(r(\{(p_1,q_1),(p_2,q_2)$

$= (Proc \times Proc) \setminus \{(q_3,q_1) \dots\}$

$s(\{q_3\} \times Proc) \cup \cancel{Proc \times \{q_3\}})$

$\sim_2 =$

$\langle\langle a\rangle\langle a\rangle tt\rangle\rangle$

3d) $\sim_{i+1} \subseteq \sim_i$

$\sim_{i+1} \subseteq \sim_i$

$s(r(\{(p_1,q_1),(p_1,p_2),(p_2,q_1)\}))$

$\sim_3 = s(r(\{(p_1,p_2)\}))$

Aufgabe 1: Ausdrucksstärke HML vs HML mit Rekursion

Seien $a, b, c \in Act$. Welche der folgenden Aussagen lassen sich mit HML Formeln formalisieren und welche nicht? Zur Begründung gib entweder eine Formel an, oder erkläre kurz, warum es keine Formel gibt.

1.a) Es ist *immer* möglich eine Aktion auszuführen.
1.b) Nach jeder a-Aktion ~~gilt~~, ~~X~~ ist eine b-Aktion möglich.
1.c) Es ist *irgendwann* möglich eine a-Aktion auszuführen.
1.d) Es ist möglich eine a-Aktion zu machen, so dass es danach *immer wieder* möglich ist eine b-Aktion auszuführen.
1.e) Wenn eine a-Aktion möglich ist, dann ist keine b-Aktion möglich.
1.f) Es ist *immer* möglich nach einer b-Aktion eine c-Aktion zu machen, *bis* keine a-Aktion mehr möglich ist.

1a) $X = \langle Act\rangle tt \wedge [Act]X$

1b) $X = [a]\langle b\rangle tt \wedge X$

$\cancel{X = [a]tt}$