Software Modeling and Verification
Lehrstuhl für Informatik 2
RWTH Aachen University

Prof. Dr. Ir. J.-P. Katoen
Priv.-Doz. Dr. T. Noll
T. Han, M. Neuhäußer

Modeling Concurrent and Probabilistic Systems

Winter Term 07/08

– Solution 7 –

Exercise 1 (3 + 3 + 1 + 1 points)

We modify the CCS specification of the ABP to model lossy channels. If a message or an acknowledgement is lost, a timeout leads to a retransmission.

a) The following process definition introduces timeouts in the alternating bit protocol to model lossy channels:

$$
\begin{aligned}
\mathit{Sender} &= \mathsf{new}\ \{\mathit{timeout}, \mathit{start}, \mathit{stop}\}\big(\mathit{Sender}_0 \mid\mid \mathit{Timer}\big)\\
\mathit{Sender}_b &= \sum_{d\in D} \mathit{accept}_d.\mathit{Send}_{db}\\
\mathit{Send}_{db} &= \overline{\mathit{send}}_{db}.\overline{\mathit{start}}.\mathit{Wait}_{db}\\
\mathit{Wait}_{db} &= \mathit{ack}_b.(\overline{\mathit{stop}}.\mathit{Sender}_{1-b} + \mathit{timeout}.\mathit{Sender}_{1-b})\\
&\quad + \mathit{ack}_{1-b}.(\overline{\mathit{stop}}.\mathit{Send}_{db} + \mathit{timeout}.\mathit{Send}_{db})\\
&\quad + \mathit{timeout}.\mathit{Send}_{db}
\end{aligned}
$$

$$
\begin{aligned}
\mathit{Receiver} &= \mathsf{new}\ \{\mathit{timeout}, \mathit{start}, \mathit{stop}\}\big(\mathit{Receiver}'_0 \mid\mid \mathit{Timer}\big)\\
\mathit{Receiver}'_0 &= \sum_{d\in D} \mathit{trans}_{d0}.\mathit{Reply}_{d0}\\
&\quad + \sum_{d\in D} \mathit{trans}_{d1}.\overline{\mathit{reply}}_1.\overline{\mathit{start}}.\mathit{Receiver}_0\\
\mathit{Receiver}_b &= \sum_{d\in D} \mathit{trans}_{db}.(\mathit{timeout}.\mathit{Reply}_{db} + \overline{\mathit{stop}}.\mathit{Reply}_{db})\\
&\quad + \sum_{d\in D} \mathit{trans}_{d(1-b)}.(\mathit{timeout}.\overline{\mathit{reply}}_{1-b}.\overline{\mathit{start}}.\mathit{Receiver}_b + \overline{\mathit{stop}}.\overline{\mathit{reply}}_{1-b}.\overline{\mathit{start}}.\mathit{Receiver}_b)\\
&\quad + \mathit{timeout}.\overline{\mathit{reply}}_{1-b}.\overline{\mathit{start}}.\mathit{Receiver}_b\\
\mathit{Reply}_{db} &= \overline{\mathit{deliver}}_d.\overline{\mathit{reply}}_b.\overline{\mathit{start}}.\mathit{Receiver}_{1-b}
\end{aligned}
$$

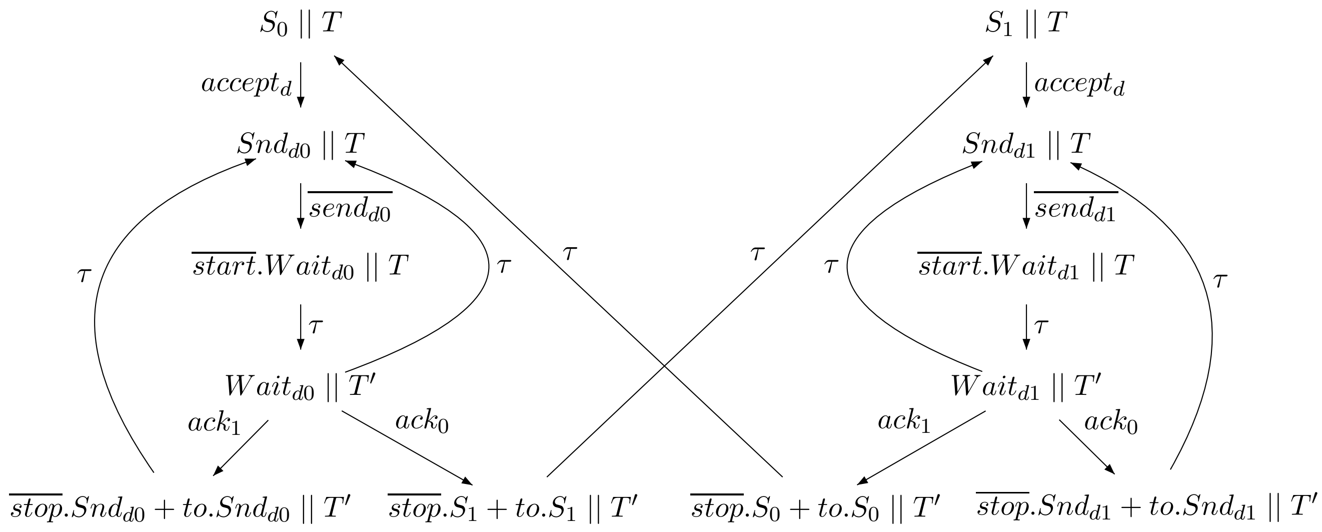
$$
\begin{aligned}
\mathit{Trans} &= \sum_{\substack{d\in D\\ b\in\{0,1\}}} \mathit{send}_{db}.\big(\underbrace{\overline{\mathit{trans}}_{db}.\mathit{Trans}}_{\text{msg success}} + \underbrace{\mathit{Trans}}_{\text{msg loss}}\big)\\
\mathit{Ack} &= \sum_{b\in\{0,1\}} \mathit{reply}_b.\big(\underbrace{\overline{\mathit{ack}}_b.\mathit{Ack}}_{\text{ack success}} + \underbrace{\mathit{Ack}}_{\text{ack loss}}\big)
\end{aligned}
$$

$$
\mathit{Timer} = \mathit{start}.(\overline{\mathit{timeout}}.\mathit{Timer} + \mathit{stop}.\mathit{Timer})
$$

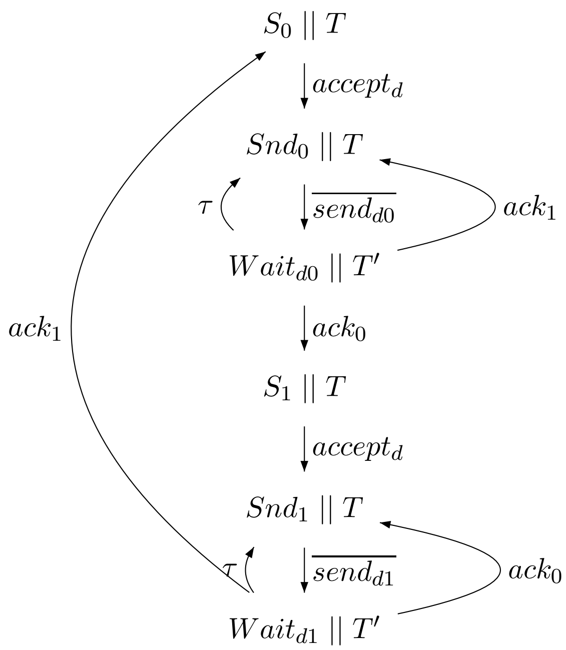
$$
\mathit{ABP}(\mathit{accept}, \mathit{deliver}) = \mathsf{new}\, L\ \big(\mathit{Sender} \mid\mid \mathit{Trans} \mid\mid \mathit{Ack} \mid\mid \mathit{Receiver}\big)
$$

where $L = \{\mathit{send}_{db}, \mathit{trans}_{db}, \mathit{reply}_b, \mathit{ack}_b \mid d \in D, b \in \{0,1\}\}$.

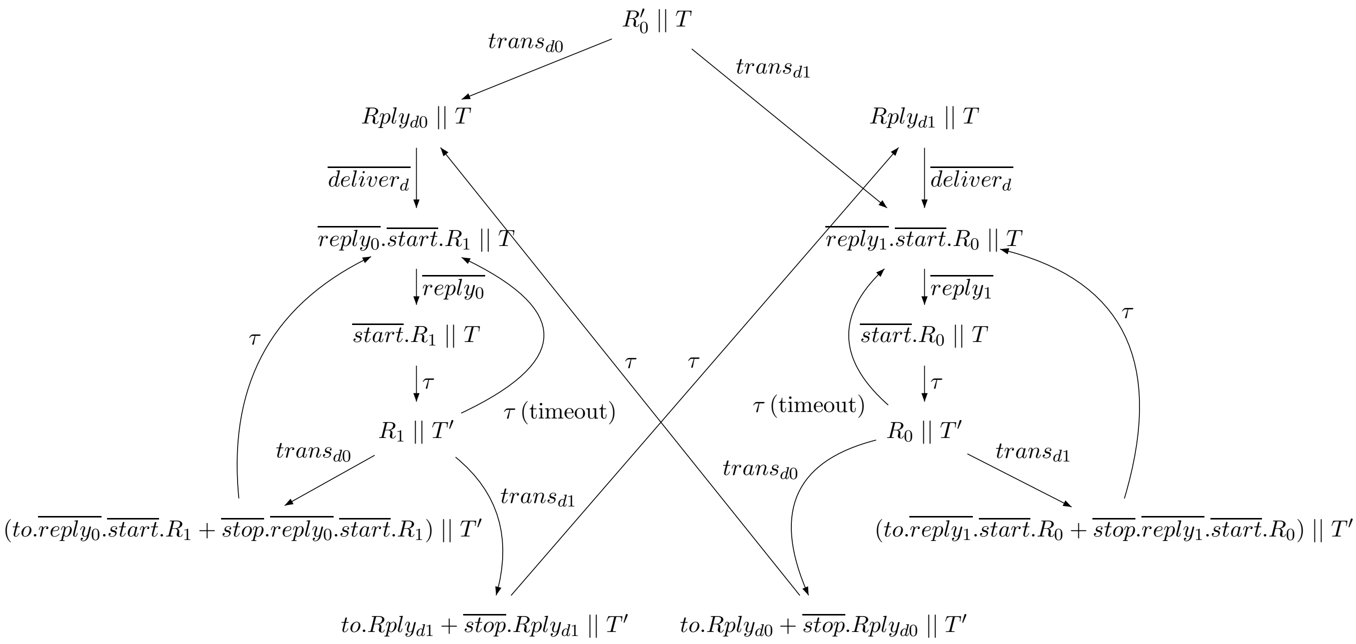
b) LTS of *Sender* || *Timer*:



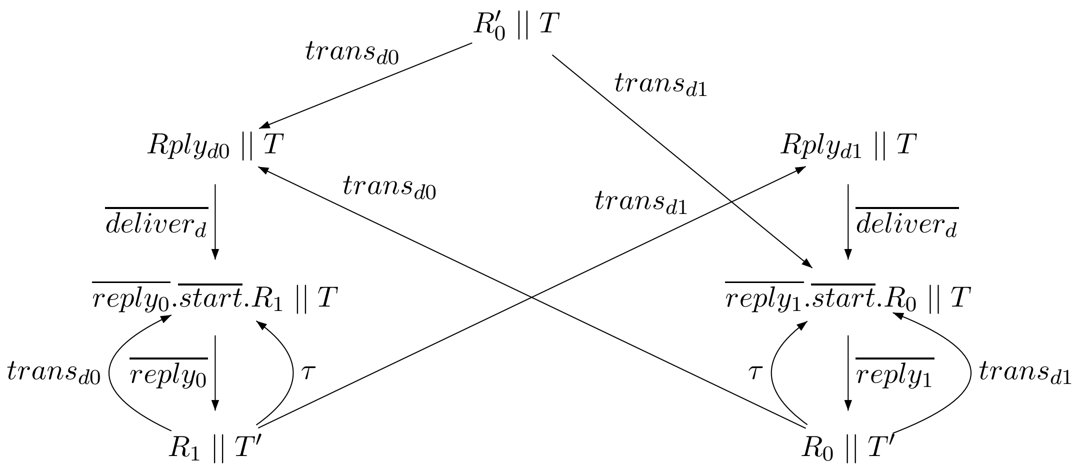
Steps of partitioning algorithm: see last page!
Reduced LTS (w.r.t. weak bisimilarity):



c) LTS of *Receiver* || *Timer*:



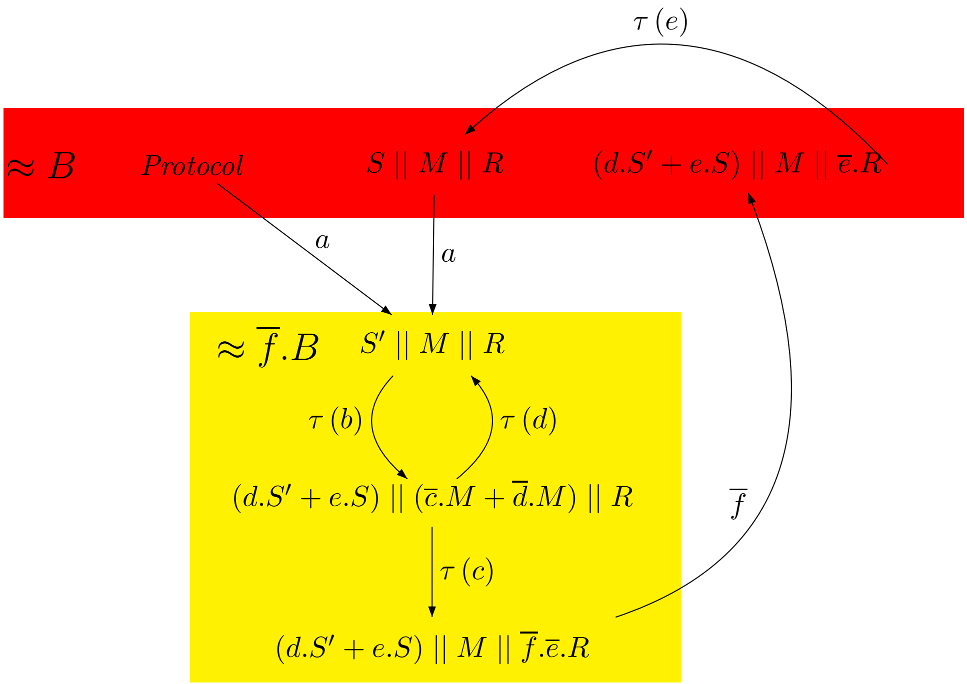
Reduced LTS (w.r.t. weak bisimilarity):



d) Weak bisimilarity is not a congruence. In general, if $P_1 \approx P_2$ and $Q_1 \approx Q_2$, $P_1 + Q_1 \not\approx P_2 + Q_2$. However, weak bisimilarity is preserved under parallel composition and restriction. As these are the only operators we use to compose the *ABP* process, this is a valid approach.

Exercise 2 (6 points)

Unrealistic: direct, error-free connection between Receiver and Sender (action e).
Transition system (S = Sender, R = Receiver, M = Medium; without `new` ...):



One-place buffer: $B \underset{\overline{f}}{\overset{a}{\rightleftarrows}} \overline{f}.B$

$\Rightarrow$ $Protocol \approx B$

Moreover $Protocol$ and B can only execute a

$\Rightarrow$ $Protocol \simeq B$ (because neither $Protocol$ nor B can execute a τ-action)

Partitioning algorithm, first iteration:

P	$S_0 \parallel T$	$Snd_{d0} \parallel T$	$\overline{start}.W_{d0} \parallel T$	$W_{d0} \parallel T'$	$(\overline{stop}.S_1 + to.S_1) \parallel T'$	$(\overline{stop}.Snd_{d0} + to.Snd_{d0}) \parallel T'$	$S_1 \parallel T$	$Snd_{d1} \parallel T$	$start.W_{d1} \parallel T$	$W_{d1} \parallel T'$	$(\overline{stop}.S_0 + to.S_0) \parallel T'$	$(\overline{stop}.Snd_{d1} + to.Snd_{d1}) \parallel T'$
$accept^*$	$\{S\}$	$\emptyset$	$\emptyset$	$\emptyset$	$\{S\}$	$\emptyset$	$\{S\}$	$\emptyset$	$\emptyset$	$\emptyset$	$\{S\}$	$\emptyset$
$\overline{send^*_{d0}}$	$\emptyset$	$\{S\}$	$\{S\}$	$\{S\}$	$\emptyset$	$\{S\}$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\overline{send^*_{d1}}$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\{S\}$	$\{S\}$	$\{S\}$	$\emptyset$	$\{S\}$
ack^*_0	$\emptyset$	$\emptyset$	$\{S\}$	$\{S\}$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\{S\}$	$\{S\}$	$\emptyset$	$\emptyset$
ack^*_1	$\emptyset$	$\emptyset$	$\{S\}$	$\{S\}$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\{S\}$	$\{S\}$	$\emptyset$	$\emptyset$
τ^*	$\{S\}$	$\{S\}$	$\{S\}$	$\{S\}$	$\{S\}$	$\{S\}$	$\{S\}$	$\{S\}$	$\{S\}$	$\{S\}$	$\{S\}$	$\{S\}$
Block	B_1	B_2	B_3	B_3	B_1	B_2	B_1	B_4	B_5	B_5	B_1	B_4

Second iteration:

P	$S_0 \parallel T$	$\overline{stop}.S_0 + to.S_0 \parallel (\overline{to}.T + stop.T)$	$S_1 \parallel T$	$\overline{stop}.S_1 + to.S_1 \parallel (\overline{to}.T + stop.T)$	$Snd_{d0} \parallel T$	$\overline{stop}.Snd_{d0} + to.Snd_{d0} \parallel \overline{to}.T + stop.T$	$\overline{start}.wait_{d0} \parallel T$	$W_{d0} \parallel (\overline{to}.T + stop.T)$
$accept^*$	$\{B_2\}$	$\{B_2\}$	$\{B_4\}$	$\{B_4\}$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\overline{send^*_{d0}}$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\{B_3, B_2\}$	$\{B_3, B_2\}$	$\{B_2, B_3\}$	$\{B_2, B_3\}$
$\overline{send^*_{d1}}$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
ack^*_0	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\{B_1\} \rightsquigarrow \{B_{1,2}\}$	$\{B_1\} \rightsquigarrow \{B_{1,2}\}$
ack^*_1	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\{B_2\}$	$\{B_2\}$
τ^*	$\{B_1\} \rightsquigarrow \{B_{1,1}\}$	$\{B_1\} \rightsquigarrow \{B_{1,1}\}$	$\{B_1\} \rightsquigarrow \{B_{1,2}\}$	$\{B_1\} \rightsquigarrow \{B_{1,2}\}$	$\{B_2\}$	$\{B_2\}$	$\{B_3, B_2\}$	$\{B_3, B_2\}$

P	$Snd_{d1} \parallel T$	$\overline{stop}.Snd_{d1} + to.Snd_{d1} \parallel (\overline{to}.T + stop.T)$	$\overline{start}.wait_{d1} \parallel T$	$W_{d1} \parallel (\overline{to}.T + stop.T)$
$accept^*$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\overline{send^*_{d0}}$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\overline{send^*_{d1}}$	$\{B_5, B_4\}$	$\{B_5, B_4\}$	$\{B_5, B_4\}$	$\{B_5, B_4\}$
ack^*_0	$\emptyset$	$\emptyset$	$\{B_4\}$	$\{B_4\}$
ack^*_1	$\emptyset$	$\emptyset$	$\{B_1\} \rightsquigarrow \{B_{1,1}\}$	$\{B_1\} \rightsquigarrow \{B_{1,1}\}$
τ^*	$\{B_4\}$	$\{B_4\}$	$\{B_5, B_4\}$	$\{B_5, B_4\}$

$\Rightarrow$ split B_1 into $B_{1,1}$ and $B_{1,2}$, all other blocks remain unchanged.
Result: Weak bisimulation quotient with six states.