Exam System Validation, 2IW26
Friday, April 11, 2014, 14:00-17:00

It is neither allowed to use the study material nor a computer. The axioms formulated in the book are given as an appendix to this exam. The answers to the questions can be formulated in English or Dutch. This exam consists of **6** questions. Good luck!

1. (a) Specify a data type T consisting of a tree structure where the leaves contain a natural number. A typical instance of a tree is $\mathit{node}(\mathit{leaf}(11), \mathit{node}(\mathit{leaf}(4), \mathit{leaf}(2014)))$. The data type must have a recogniser *is_leaf* that yields true iff it is applied to a tree consisting of a single leaf.

   (b) Prove (precisely) that the tree consisting of a single leaf is not equal to a tree containing subtrees.

   (c) Define a function $\mathit{total\_sum} : T \rightarrow \mathbb{N}$ that gives the total sum of all numbers in the tree.

   (d) Describe a '*tree-splitter*'-process that reads a tree via an action *in* and forwards both subtrees via two occurrences of an action *out*. The tree consisting of only a leaf is forwarded as a whole. Extend this splitter with an option to request the cumulative sum of all numbers in all trees that the splitter has seen since startup, or since the last *reset*. For this purpose it is necessary to add a reset facility to the the splitter.

2. Consider the data type E defined as **struct** $e_1 \mid e_2 \mid e_3$. Prove exactly using the process axioms and the rules and equations for the data type E that

$$\sum_{e:E} X(e) = X(e_1) + X(e_2) + X(e_3).$$

3. Express the following properties using the modal μ-calculus.

   (a) There is a deadlock.

   (b) It is possible to do an a action infinitely often, directly from the initial state.

   (c) Whenever an action a happens, an action b must always be possible as long as the action b has not happened.

   (d) The Stella is a solar car built by a group of students at this university, which was considered the best car in the cruiser class during a cross country race through Australia that took place in the fall of 2013. The software in the Stella has been designed using mCRL2. One of the properties that the software has is that whenever a component (battery, engine, solar-panel) reports a problem, using a *report* action, this problem will always be forwarded to the support vehicle that followed the Stella using a *forward* action. Give a modal formula for this property.

   (e) You are requested to check whether the control software of an automatic pizza baking machine works well. For this purpose you want to check that the control software will never attempt to output more pizza's than that enter the machine. The action to enter a pizza in the machine is *enter* and the action to output a pizza is *out*. Write the modal formula that expresses this.

4. Consider the following pairs of modal formulas Give a labelled transition system only containing actions a and b for which the first formula is true and the second is not. Reversely, provide a labelled transition system for which the first formula is false and the second is true. If no such transitions systems exist, clearly indicate why, using the laws for modal logical formulas included in this exam.

   (a) $[b^\star]\langle a \wedge b\rangle \mathit{true}$ and $\mu X.([b]X \wedge \langle a \vee b\rangle \mathit{true})$.

   (b) $[b^\star](\mu X.[\overline{\mathit{true}}]X \wedge \langle a\rangle \mathit{true})$ and $\nu Y.\langle a\rangle \mathit{true} \wedge [b]Y$.

5. Consider a process $X = a{\cdot}a{\cdot}X$ and $Y = a{\cdot}Y{\cdot}b$. Prove using RSP that $X = Y$.

6. Consider the process equations $X = a{\cdot}(b{\cdot}X + Y)$ and $Y = a{\cdot}(X + Y)$.

   (a) Give a linear process of which the behaviour is strongly bisimilar to that of X.

   (b) Is $\tau_{\{a\}}(X)$ τ-confluent? Is $\tau_{\{a\}}(X)$ τ-convergent? Draw a state space of $\tau_{\{a\}}(X)$ after applying τ-priorisation to its maximal extent. Does this reduction preserve branching bisimulation? Explain all your answers; a simple yes or no does not suffice.

7. **END**

Score: $(10 + n)/10$ where n is the cumulative judgement given by the following table:

question	(a)	(b)	(c)	(d)	(e)
1	6	4	4	8	
2	10				
3	4	4	4	4	4
4	7	7			
5	10				
6	7	7			

MA1	$\alpha\|\beta = \beta\|\alpha$
MA2	$(\alpha\|\beta)\|\gamma = \alpha\|(\beta\|\gamma)$
MA3	$\alpha\|\tau = \alpha$
MD1	$\tau \setminus \alpha = \tau$
MD2	$\alpha \setminus \tau = \alpha$
MD3	$\alpha \setminus (\beta\|\gamma) = (\alpha \setminus \beta) \setminus \gamma$
MD4	$(a(d)\|\alpha) \setminus a(d) = \alpha$
MD5	$(a(d)\|\alpha) \setminus b(e) = a(d)\|(\alpha \setminus b(e)) \quad \text{if } a \not\equiv b \text{ or } d \not\approx e$
MS1	$\tau \sqsubseteq \alpha = \mathit{true}$
MS2	$a(d) \sqsubseteq \tau = \mathit{false}$
MS3	$a(d)\|\alpha \sqsubseteq a(d)\|\beta = \alpha \sqsubseteq \beta$
MS4	$a(d)\|\alpha \sqsubseteq b(e)\|\beta = a(d)\|(\alpha \setminus b(e)) \sqsubseteq \beta \quad \text{if } a \not\equiv b \text{ or } d \not\approx e$
MAN1	$\underline{\tau} = \tau$
MAN2	$\underline{a(d)} = a$
MAN3	$\underline{\alpha\|\beta} = \underline{\alpha}\|\underline{\beta}$

Table 1: Axioms for multi-actions

A1	$x + y = y + x$
A2	$x + (y + z) = (x + y) + z$
A3	$x + x = x$
A4	$(x + y){\cdot}z = x{\cdot}z + y{\cdot}z$
A5	$(x{\cdot}y){\cdot}z = x{\cdot}(y{\cdot}z)$
A6✠	$x + \delta = x$
A7	$\delta{\cdot}x = \delta$
Cond1	$\mathit{true}{\to}x \diamond y = x$
Cond2	$\mathit{false}{\to}x \diamond y = y$
THEN✠	$c{\to}x = c{\to}x{\diamond}\delta$
SUM1	$\sum_{d:D} x = x$
SUM3	$\sum_{d:D} X(d) = X(e) + \sum_{d:D} X(d)$
SUM4	$\sum_{d:D}(X(d) + Y(d)) = \sum_{d:D} X(d) + \sum_{d:D} Y(d)$
SUM5	$(\sum_{d:D} X(d)){\cdot}y = \sum_{d:D} X(d){\cdot}y$

Table 2: Axioms for the basic operators

M	$x \parallel y = x \llfloor y + y \llfloor x + x\|y$
LM1✠	$\alpha \llfloor x = \alpha{\cdot}x$
LM2✠	$\delta \llfloor x = \delta$
LM3✠	$\alpha{\cdot}x \llfloor y = \alpha{\cdot}(x \parallel y)$
LM4	$(x+y) \llfloor z = x \llfloor z + y \llfloor z$
LM5	$(\sum_{d:D} X(d)) \llfloor y = \sum_{d:D} X(d) \llfloor y$
S1	$x\|y = y\|x$
S2	$(x\|y)\|z = x\|(y\|z)$
S3	$x\|\tau = x$
S4	$\alpha\|\delta = \delta$
S5	$(\alpha{\cdot}x)\|\beta = \alpha\|\beta{\cdot}x$
S6	$(\alpha{\cdot}x)\|(\beta{\cdot}y) = \alpha\|\beta{\cdot}(x \parallel y)$
S7	$(x+y)\|z = x\|z + y\|z$
S8	$(\sum_{d:D} X(d))\|y = \sum_{d:D} X(d)\|y$
TC1	$(x \llfloor y) \llfloor z = x \llfloor (y \parallel z)$
TC2	$x \llfloor \delta = x{\cdot}\delta$
TC3	$(x\|y) \llfloor z = x\|(y \llfloor z)$

Table 3: Axioms for the parallel composition operators

C1	$\Gamma_C(\alpha) = \gamma_C(\alpha)$	C4	$\Gamma_C(x{\cdot}y) = \Gamma_C(x){\cdot}\Gamma_C(y)$
C2	$\Gamma_C(\delta) = \delta$	C5	$\Gamma_C(\sum_{d:D} X(d)) = \sum_{d:D} \Gamma_C(X(d))$
C3	$\Gamma_C(x+y) = \Gamma_C(x) + \Gamma_C(y)$		

Table 4: Axioms for the communication operator

V1	$\nabla_V(\alpha) = \alpha$ if $\underline{\alpha} {\in} V {\cup} \{\tau\}$	V4	$\nabla_V(x+y) = \nabla_V(x) + \nabla_V(y)$
V2	$\nabla_V(\alpha) = \delta$ if $\underline{\alpha} {\notin} V {\cup} \{\tau\}$	V5	$\nabla_V(x{\cdot}y) = \nabla_V(x){\cdot}\nabla_V(y)$
V3	$\nabla_V(\delta) = \delta$	V6	$\nabla_V(\sum_{d:D} X(d)) = \sum_{d:D} \nabla_V(X(d))$
TV1	$\nabla_V(\nabla_W(x)) = \nabla_{V\cap W}(x)$		

Table 5: Axioms for the allow operator

E1	$\partial_B(\tau) = \tau$		E6	$\partial_B(x + y) = \partial_B(x) + \partial_B(y)$
E2	$\partial_B(a(d)) = a(d)$	if $a \notin B$	E7	$\partial_B(x{\cdot}y) = \partial_B(x){\cdot}\partial_B(y)$
E3	$\partial_B(a(d)) = \delta$	if $a \in B$	E8	$\partial_B(\sum_{d:D} X(d)) = \sum_{d:D} \partial_B(X(d))$
E4	$\partial_B(\alpha\vert\beta) = \partial_B(\alpha)\vert\partial_B(\beta)$		E5	$\partial_B(\delta) = \delta$
E10	$\partial_H(\partial_{H'}(x)) = \partial_{H\cup H'}(x)$			

Table 6: Axioms for the blocking operator

R1	$\rho_R(\tau) = \tau$	
R2	$\rho_R(a(d)) = b(d)$	if $a{\to}b \in R$ for some b
R3	$\rho_R(a(d)) = a(d)$	if $a{\to}b \notin R$ for all b
R4	$\rho_R(\alpha\vert\beta) = \rho_R(\alpha)\vert\rho_R(\beta)$	
R5	$\rho_R(\delta) = \delta$	
R6	$\rho_R(x + y) = \rho_R(x) + \rho_R(y)$	
R7	$\rho_R(x{\cdot}y) = \rho_R(x){\cdot}\rho_R(y)$	
R8	$\rho_R(\sum_{d:D} X(d)) = \sum_{d:D} \rho_R(X(d))$	

Table 7: Axioms for the renaming operator

H1	$\tau_I(\tau) = \tau$		H6	$\tau_I(x{+}y) = \tau_I(x) + \tau_I(y)$
H2	$\tau_I(a(d)) = \tau$	if $a \in I$	H7	$\tau_I(x{\cdot}y) = \tau_I(x){\cdot}\tau_I(y)$
H3	$\tau_I(a(d)) = a(d)$	if $a \notin I$	H8	$\tau_I(\sum_{d:D} X(d)) = \sum_{d:D} \tau_I(X(d))$
H4	$\tau_I(\alpha\vert\beta) = \tau_I(\alpha)\vert\tau_I(\beta)$		H5	$\tau_I(\delta) = \delta$
H10	$\tau_I(\tau_{I'}(x)) = \tau_{I\cup I'}(x)$			

Table 8: Axioms for the hiding operator

W✠	$x{\cdot}\tau = x$
BRANCH✠	$x{\cdot}(\tau{\cdot}(y + z) + y) = x{\cdot}(y + z)$

Table 9: Axioms for τ, valid in rooted branching bisimulation for untimed processes

Failures equivalence	F1✠	$a\cdot(b\cdot x+u) + a\cdot(b\cdot y+v) = a\cdot(b\cdot x+b\cdot y+u) + a\cdot(b\cdot x+b\cdot y+v)$
	F2✠	$a\cdot x + a\cdot(y+z) = a\cdot x + a\cdot(x+y) + a\cdot(y+z)$
Trace equivalence	RDIS	$x\cdot(y+z) = x\cdot y + x\cdot z$
Language equivalence	Lang1	$x\cdot\delta = \delta$
	RDIS	$x\cdot(y+z) = x\cdot y + x\cdot z$
Weak trace equivalence	RDIS	$x\cdot(y+z) = x\cdot y + x\cdot z$
	WT	$\tau\cdot x = x$
	W	$x\cdot\tau = x$

Table 10: Axioms for some other equivalences for untimed processes

Proposition logic	
$\phi \wedge \psi = \psi \wedge \phi$	$\phi \vee \psi = \psi \vee \phi$
$(\phi \wedge \psi) \wedge \chi = \phi \wedge (\psi \wedge \chi)$	$(\phi \vee \psi) \vee \chi = \phi \vee (\psi \vee \chi)$
$\phi \wedge \phi = \phi$	$\phi \vee \phi = \phi$
$\neg \mathit{true} = \mathit{false}$	$\neg \mathit{false} = \mathit{true}$
$\phi \wedge \mathit{true} = \phi$	$\phi \vee \mathit{true} = \mathit{true}$
$\phi \wedge \mathit{false} = \mathit{false}$	$\phi \vee \mathit{false} = \phi$
$\phi \wedge (\psi \vee \chi) = (\phi \wedge \psi) \vee (\phi \wedge \chi)$	$\phi \vee (\psi \wedge \chi) = (\phi \vee \psi) \wedge (\phi \vee \chi)$
$\neg(\phi \wedge \psi) = \neg\phi \vee \neg\psi$	$\neg(\phi \vee \psi) = \neg\phi \wedge \neg\psi$
$\neg\neg\phi = \phi$	$\phi \rightarrow \psi = \neg\phi \vee \psi$
$\phi \Rightarrow \psi = \neg\phi \vee \psi$	$\phi \Leftrightarrow \psi = \phi \Rightarrow \psi \wedge \psi \Rightarrow \phi$
Predicate logic	
$\forall d{:}D.\phi = \phi$	$\exists d{:}D.\phi = \phi$
$\neg\forall d{:}D.\Phi(d) = \exists d{:}D.\neg\Phi(d)$	$\neg\exists d{:}D.\Phi(d) = \forall d{:}D.\neg\Phi(d)$
$\forall d{:}D.(\Phi(d){\wedge}\Psi(d)) = \forall d{:}D.\Phi(d){\wedge}\forall d{:}D.\Psi(d)$	$\exists d{:}D.(\Phi(d){\vee}\Psi(d)) = \exists d{:}D.\Phi(d){\vee}\exists d{:}D.\Psi(d)$
$\forall d{:}D.(\Phi(d){\vee}\psi) = \forall d{:}D.\Phi(d) \vee \psi$	$\exists d{:}D.(\Phi(d){\wedge}\psi) = \exists d{:}D.\Phi(d) \wedge \psi$
$\forall d{:}D.\Phi(d) \Rightarrow \Phi(e)$	$\Phi(e) \Rightarrow \exists d{:}D.\Phi(d)$
Action formulas	
$\overline{\mathit{true}} = \mathit{false}$	$\overline{\mathit{false}} = \mathit{true}$
$\overline{\alpha_1 \cup \alpha_2} = \overline{\alpha_1} \cap \overline{\alpha_2}$	$\overline{\alpha_1 \cap \alpha_2} = \overline{\alpha_1} \cup \overline{\alpha_2}$
$\overline{\exists d{:}D.A(d)} = \forall d{:}D.\overline{A(d)}$	$\overline{\forall d{:}D.A(d)} = \exists d{:}D.\overline{A(d)}$
Hennessy-Milner logic	
$\neg\langle a\rangle\phi = [a]\neg\phi$	$\neg[a]\phi = \langle a\rangle\neg\phi$
$\langle a\rangle \mathit{false} = \mathit{false}$	$[a]\mathit{true} = \mathit{true}$
$\langle a\rangle(\phi \vee \psi) = \langle a\rangle\phi \vee \langle a\rangle\psi$	$[a](\phi \wedge \psi) = [a]\phi \wedge [a]\psi$
$\langle a\rangle\phi \wedge [a]\psi \Rightarrow \langle a\rangle(\phi \wedge \psi)$	$[a](\phi \vee \psi) \Rightarrow \langle a\rangle\phi \vee [a]\psi$

Table 11: Equivalences between modal formulas (part I)

Fixed point equations	
$\mu X.\phi(X) \Rightarrow \nu X.\phi(X)$	
$\mu X.\phi = \phi$	$\nu X.\phi = \phi$
$\mu X.X = \mathit{false}$	$\nu X.X = \mathit{true}$
$\mu X.\langle R\rangle X = \mathit{false}$	$\nu X.[R]X = \mathit{true}$
$\neg\mu X.\phi(X) = \nu X.\neg\phi(\neg X)$	$\neg\nu X.\phi(X) = \mu X.\neg\phi(\neg X)$
$\mu X.\phi(X) = \phi(\mu X.\phi(X))$	$\nu X.\phi(X) = \phi(\nu X.\phi(X))$
if $\phi(\psi) \Rightarrow \psi$ then $\mu X.\phi(X) \Rightarrow \psi$	if $\psi \Rightarrow \phi(\psi)$ then $\psi \Rightarrow \nu X.\phi(X)$
Regular formulas	
$\langle\varepsilon\rangle\phi = \phi$	$[\varepsilon]\phi = \phi$
$\langle\mathit{false}\rangle\phi = \mathit{false}$	$[\mathit{false}]\phi = \mathit{true}$
$\langle\mathit{af}_1 \cup \mathit{af}_2\rangle\phi = \langle\mathit{af}_1\rangle\phi \vee \langle\mathit{af}_2\rangle\phi$	$[\mathit{af}_1 \cup \mathit{af}_2]\phi = [\mathit{af}_1]\phi \wedge [\mathit{af}_2]\phi$
$\langle\mathit{af}_1 \cap \mathit{af}_2\rangle\phi \Rightarrow \langle\mathit{af}_1\rangle\phi \wedge \langle\mathit{af}_2\rangle\phi$	$[\mathit{af}_1 \cap \mathit{af}_2]\phi \Leftarrow [\mathit{af}_1]\phi \vee [\mathit{af}_2]\phi$
$\langle\exists d{:}D.AF(d)\rangle\phi = \exists d{:}D.\langle AF(d)\rangle\phi$	$[\exists d{:}D.AF(d)]\phi = \forall d{:}D.[AF(d)]\phi$
$\langle\forall d{:}D.AF(d)\rangle\phi \Rightarrow \forall d{:}D.\langle AF(d)\rangle\phi$	$[\forall d{:}D.AF(d)]\phi \Leftarrow \exists d{:}D.[AF(d)]\phi$
$\langle R_1 + R_2\rangle\phi = \langle R_1\rangle\phi \vee \langle R_2\rangle\phi$	$[R_1 + R_2]\phi = [R_1]\phi \wedge [R_2]\phi$
$\langle R_1{\cdot}R_2\rangle\phi = \langle R_1\rangle\langle R_2\rangle\phi$	$[R_1{\cdot}R_2]\phi = [R_1][R_2]\phi$
$\langle R^\star\rangle\phi = \mu X.(\langle R\rangle X \vee \phi)$	$[R^\star]\phi = \nu X.([R]X \wedge \phi)$
$\langle R^+\rangle\phi = \langle R\rangle\langle R^\star\rangle\phi$	$[R^+]\phi = [R][R^\star]\phi$
$\neg\langle R\rangle\phi = [R]\neg\phi$	$\neg[R]\phi = \langle R\rangle\neg\phi$
$[R]\mathit{true} = \mathit{true}$	$\langle R\rangle\mathit{false} = \mathit{false}$
$\langle R\rangle(\phi \vee \psi) = \langle R\rangle\phi \vee \langle R\rangle\psi$	$[R](\phi \wedge \psi) = [R]\phi \wedge [R]\psi$
$\langle R\rangle\phi \wedge [R]\psi \Rightarrow \langle R\rangle(\phi \wedge \psi)$	$[R](\phi \vee \psi) \Rightarrow \langle R\rangle\phi \vee [R]\psi$

Table 12: Equivalences between modal formulas (part II)