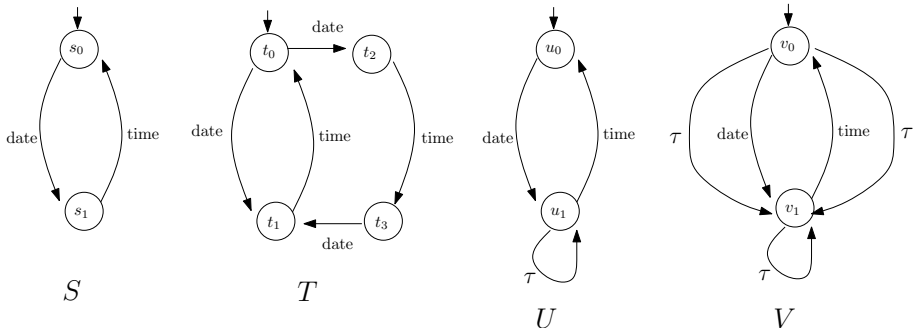
System Validation (IN4387) Final Examination
November 10, 2011, 14:00-17:00

Important Notes. It is not allowed to use study material, computers, or calculators during the examination. The examination comprises 5 question and 3 pages. Please check beforehand whether your copy is properly printed. Give complete explanation and do not confine yourself to giving the final answer. The answers may be given in Dutch or in English. **Good luck!**

Exercise 1 (20 points) Consider the following specifications of a clock.



Check which one of the following equalities hold and explain the reason.

1. S and T are strongly bisimilar,
2. S and U are branching bisimilar,
3. S and V are branching bisimilar,
4. S and V are rooted branching bisimilar.

Answer 1

1. S and T are bisimilar because there exists a bisimulation relation $R = \{(s_0, t_0), (s_1, t_1), (s_1, t_2), (s_0, t_3)\}$ such that $(s_0, t_0) \in R$.
2. S and U are branching bisimilar because there exists a branching bisimulation relation $R = \{(s_0, t_0), (s_1, t_1)\}$ such that $(s_0, t_0) \in R$.
3. S and V are not branching bisimilar. Assume that they were branching bisimilar, then there would exist a branching bisimulation relation R such that $(s_0, v_0) \in R$. Since $v_0 \xrightarrow{\tau} v_1$, the only possibly to mimic this behavior in S is to remain in s_0, which means that $(s_0, v_1) \in R$. However, $v_1 \xrightarrow{time} v_0$, but this transition cannot be mimicked by s_0.
4. S and V are not rooted branching bisimilar, because they are not branching bisimilar.

Exercise 2 (20 points) Assume that the sort *iNatural* of natural numbers is defined as follows:

```
sort  iNatural;
cons  zero: iNatural;
      succ: iNatural → iNatural;
map   eq: iNatural × iNatural → Bool;
var   i, j: iNatural;
eqn   eq(i, i)= true;                    (1)
      eq(zero, succ(i))= false;          (2)
      eq(succ(i), zero)= false;          (3)
      eq(succ(i), succ(j))= eq(i,j);     (4)
```

1. Prove that zero cannot be the same as succ(zero).
2. Define the operation multiply, which multiplies two natural numbers.

Answer 2

1. Assume towards a contradiction that zero is the same as succ(zero). Then the following derivation (leading to contradiction) follows.

true	=	(1)
eq(zero, zero)	=	(assumption)
eq(zero, succ(zero))	=	(2)
false		

2.

```
var   i,j: Nat;
map   add: iNatural × iNatural → iNatural;
      multiply: iNatural × iNatural → iNatural;
eqn   add(zero, i)= i;
      add(succ(i), j)= succ(add(i, j));
      multiply(zero, i)= zero;
      multiply(succ(i), j)= add(i, multiply(i, j));
```

Exercise 3 (20 points) Prove the following equations using the axioms provided in the appendix.

1. $c \to (c' \to x \diamond y) \diamond y = c \wedge c' \to x \diamond y$,
2. $(a + a) \cdot (a + b) + (b + \delta) \cdot (a + b) + b \cdot (a + b) = (a + b) \cdot (a + b)$,
3. $\delta \between a = a \cdot \delta$,
4. $a \between (b + c) = (b + c) \cdot a + ((b + c) \mid a) + a \cdot (b + c)$.

Note that sequential composition binds stronger than nondeterministic choice.

Answer 3 1. By induction on c.

2.
$$\begin{array}{lcl}
(a + a) \cdot (a + b) + (b + \delta) \cdot (a + b) + b \cdot (a + b) & = & \text{(A6)} \\
(a + a) \cdot (a + b) + b \cdot (a + b) + b \cdot (a + b) & = & \text{(A3)} \\
a \cdot (a + b) + b \cdot (a + b) + b \cdot (a + b) & = & \text{(A3)} \\
a \cdot (a + b) + b \cdot (a + b) & = & \text{(A4)} \\
(a + b) \cdot (a + b) & &
\end{array}$$

3. In the following derivations, $\lfloor\!\lfloor$ and $\mid$ both bind more strongly than $+$ and less strongly than $\cdot$.

$$\begin{array}{lcl}
\delta \between a & = & \text{(M)} \\
\delta \lfloor\!\lfloor a + a \lfloor\!\lfloor \delta + \delta \mid a & = & \text{(LM2)} \\
\delta + a \lfloor\!\lfloor \delta + \delta \mid a & = & \text{(A1,A6)} \\
a \lfloor\!\lfloor \delta + \delta \mid a & = & \text{(LM1)} \\
a.\delta + \delta \mid a & = & \text{(S1,S4)} \\
a.\delta + \delta & = & \text{(A6)} \\
a.\delta & &
\end{array}$$

4.
$$\begin{array}{lcl}
a \between (b + c) & = & \text{(M)} \\
a \lfloor\!\lfloor (b + c) + (b + c) \lfloor\!\lfloor a + a \mid (b + c) & = & \text{(LM1)} \\
a \cdot (b + c) + (b + c) \lfloor\!\lfloor a + a \mid (b + c) & = & \text{(LM4)} \\
a \cdot (b + c) + b \lfloor\!\lfloor a + c \lfloor\!\lfloor a + a \mid (b + c) & = & \text{(LM1)} \times 2 \\
a \cdot (b + c) + b \cdot a + c \cdot a + a \mid (b + c) & = & \text{(LM1)} \times 2 \\
a \cdot (b + c) + b \cdot a + c \cdot a + a \mid (b + c) & = & \text{(A4)} \\
a \cdot (b + c) + (b + c) \cdot a + a \mid (b + c) & = & \text{(A1,S1)} \\
a \cdot (b + c) + (b + c) \mid a + (b + c) \cdot a & &
\end{array}$$

Exercise 4 (20 points) Give an mCRL2 specification for a simple ice-cream machine which can be refilled by executing action *refill*, when empty. After each refill, it can produce 100 ice-creams by executing action *ice*. At each point of time, it can also show its capacity (the number of ice creams it can produce before refilling), by executing action $togo(n)$, where n is a natural number denoting the capacity. The ice-cream machine is assumed to be initially empty.

Answer 4

```
act   togo : Nat;
      refill, ice ;

proc  IceMachine (cap: Nat)  =
                                  togo(cap) · IceMachine(c) +
                                  (cap > 0) → ice · IceMachine(Int2Nat(cap-1))+
                                  (cap ≈ 0) → refill.IceMachine(100)
init  IceMachine (0) ;
```

Exercise 5 (20 points) Specify the following properties in the Modal μ-Calculus. Assume that the set of actions is $Act = \{\mathit{fill}, \mathit{produce}, \mathit{empty}\}$.

1. Directly after every *fill* actions, either a *produce* or an *empty* action must be taken.
2. After each *empty* action, another *empty* cannot be done.
3. Always after each *empty* action, eventually a *fill* action will be taken.
4. There is no infinite path of only *produce* actions.

Properties 1 and 2 should hold in the initial state and need not hold everywhere. Properties 3 and 4 should hold everywhere.

Answer 5

1. $[\mathit{fill}]((\langle \mathit{produce} \rangle \mathit{true} \vee \langle \mathit{empty} \rangle \mathit{true}) \wedge [\mathit{fill}]\mathit{false})$,
2. $[\mathit{empty}][\mathit{empty}]\mathit{false}$,
3. $\nu X.([Act]X \wedge [\mathit{empty}]Y)$
   $\mu Y.([\{\mathit{empty}, \mathit{produce}\}]Y \wedge \langle Act \rangle \mathit{true})$,
4. $\nu X.([Act]X \wedge [\mathit{produce}]Y)$
   $\mu Y.[\{\mathit{produce}\}]Y$,

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	$\mathit{true}\rightarrow x \diamond y = x$
Cond2	$\mathit{false}\rightarrow x \diamond y = y$
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 1: Axioms for the basic operators

Note that α and β range over (multi)actions and x, y and z ranger over processes.

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

Table 2: Axioms for the parallel composition operators