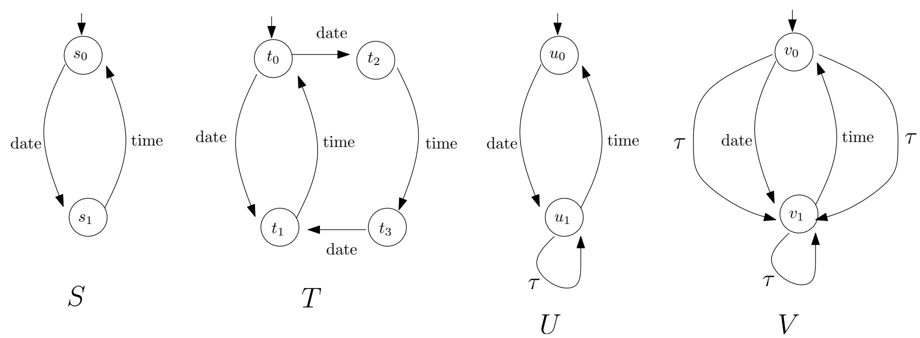
System Validation (IN4387) Final Examination
November 10, 2011, 14:00-17:00

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.

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;
       eq(zero, succ(i))= false;
       eq(succ(i), zero)= false;
       eq(succ(i), succ(j))= eq(i,j);
```

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

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. $\delta \parallel a = a \cdot \delta$,
4. $a \parallel (b+c) = (b+c) \cdot a + ((b+c) \mid a) + a \cdot (b+c)$.

Note that sequential composition binds stronger than nondeterministic choice.

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.

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

1. Directly after every *fill* actions, either a *produce* or an *empty* action must be taken.
2. Directly 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.

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

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

Table 2: Axioms for the parallel composition operators

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