

2IW05 Final Examination – Software Specification

Faculteit Wiskunde en Informatica
Technische Universiteit Eindhoven (TU/e)

January 16, 2009, 14.00 – 17.00

Exercise 1 (15 points) Consider the following algebraic specification of the natural numbers (\mathbb{N}) and lists of natural numbers (\mathbb{L}):

Constructor function symbols

0	:		\rightarrow	\mathbb{N}
S	:	\mathbb{N}	\rightarrow	\mathbb{N}
$[]$:		\rightarrow	\mathbb{L}
$_{<}$:	$\mathbb{L} \times \mathbb{N}$	\rightarrow	\mathbb{L}

Additional function symbols

$+$:	$\mathbb{N} \times \mathbb{N}$	\rightarrow	\mathbb{N}
$length$:	\mathbb{L}	\rightarrow	\mathbb{N}

Equations

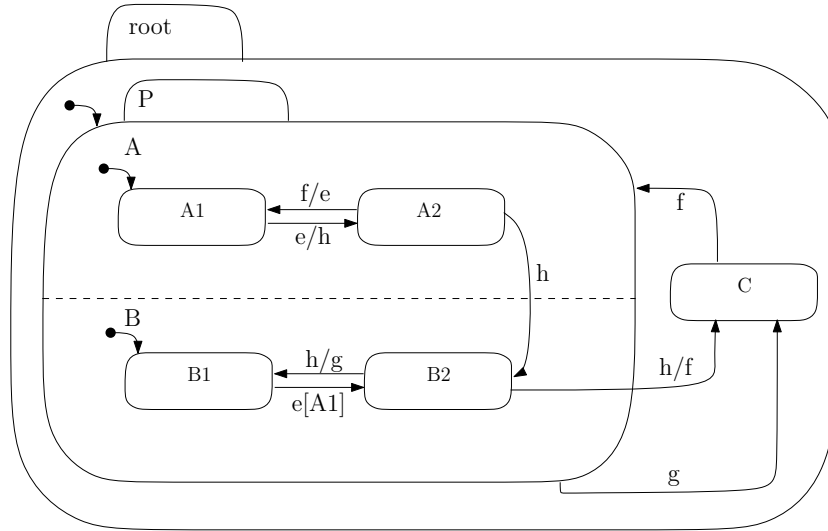
$n + 0$	=	n
$n + S(m)$	=	$S(n + m)$
$length([])$	=	0
$length(l < n)$	=	$S(length(l))$

1. Extend the algebraic specification with additional function symbol $_{\bowtie}$: $\mathbb{L} \times \mathbb{L} \rightarrow \mathbb{L}$ that concatenates two lists. **(5 points)**
2. Prove that $length(l \bowtie l') = length(l) + length(l')$. **(10 points)**

Exercise 2 (20 points) Consider the following informal specification. An insurance company has a number of clients, who are insured for one or more incidents, each for a maximum amount. After an incident happens, a client reports the incident and the amount of incurred loss due to the incident. If the client is insured for that incident, then the amount of loss (up to the maximum insured amount) is paid. Otherwise, it is reported that the client is not insured for the reported incident.

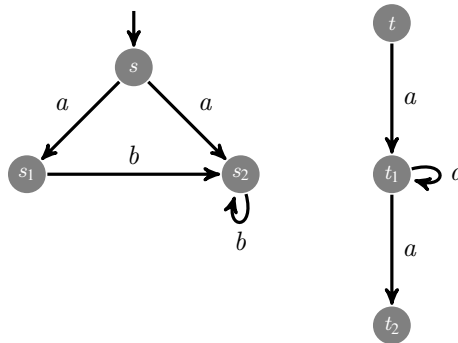
1. Specify a state schema specifying the state of the insurance company. **(10 points)**
2. Specify operation schema $handleIncident$, as described above. **(10 points)**

Exercise 3 (30 points) Consider the following statechart.



1. Assume that the current situation is $(\{\text{root}, P, A, A2, B, B2\}, \{h\})$. Calculate the exit and enter sets of the transitions labeled h , h/g and h/f . **(15 points)**
2. Starting from the initial configuration $\{\text{root}, P, A, A1, B, B1\}$, draw the LTS of the statechart up to depth three (i.e., three transitions from the environment interleaved with three transitions from the statechart), assuming that the transitions of the environment are labeled $\{e, \emptyset\}$ and \emptyset , respectively. **(15 points)**

Exercise 4 (10 points) Consider the following labeled transition system.



1. Determine $\llbracket X \rrbracket$ with $X \stackrel{\text{max}}{=} \langle b \rangle \text{true} \wedge [b]X$. **(5 points)**
2. Determine $\llbracket X \rrbracket$ with $X \stackrel{\text{min}}{=} \langle b \rangle \text{true} \vee \langle \{a, b\} \rangle X$. **(5 points)**

Exercise 5 (15 points) Let $Act = \{a, b\}$. Give a formula in the regular alternation-free modal μ -calculus for the following property: between any two consecutive a -actions at least one b action occurs.

Exercise 6 (10 points) Give a labeled transition system that illustrates the difference between the formulas

$$\llbracket \text{true}^* \cdot a \rrbracket \llbracket \text{true}^* \cdot b \rrbracket \text{true} \quad \text{and} \quad \llbracket \text{true}^* \cdot a \cdot \bar{b}^* \rrbracket \llbracket \bar{b}^* \cdot b \rrbracket \text{true}$$

Answer 1

1. The equations for $_ \bowtie _ : \mathbb{L} \times \mathbb{L} \rightarrow \mathbb{L}$ are

$$\begin{aligned} l \bowtie [] &= l \\ l \bowtie (l' \triangleleft n) &= (l \bowtie l') \triangleleft n \end{aligned}$$

2. An inductive proof is straightforward

Basis $length(l \bowtie []) = length(l) = length(l) + 0 = length(l) + length([])$

Step IH: $length(l \bowtie l') = length(l) + length(l')$

$$length(l \bowtie (l' \triangleleft n)) = length((l \bowtie l') \triangleleft n) = S(length(l \bowtie l')) = length(l) + S(length(l')) = length(l) + length(l' \triangleleft n)$$

Answer 2

[*Clients, Incidents*]
Report ::= done | notInsured
Amount == Z

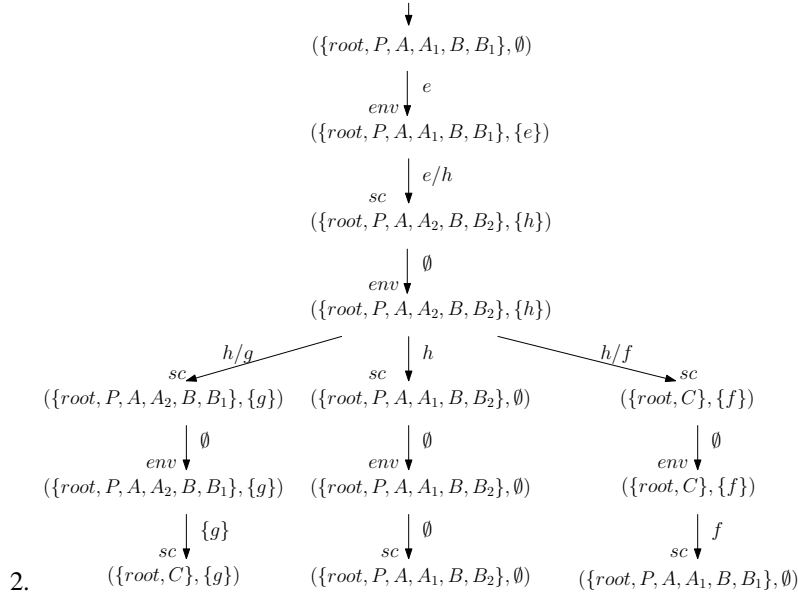
<p><i>InsuranceCompany</i></p> <p><i>insured : Clients</i> \leftrightarrow (<i>Incidents</i> \leftrightarrow <i>Amount</i>)</p> <p>$\forall c : Clients \mid c \in \text{dom } insured \bullet insured(c) \neq \emptyset$</p>
--

<p><i>HandleIncident</i></p> <p>$\exists InsuranceCompany$</p> <p><i>c? : Client</i></p> <p><i>in? : Incident</i></p> <p><i>loss? : Amount</i></p> <p><i>payment! : Amount</i></p> <p><i>report! : Report</i></p> <p>$((c? \notin \text{dom } insured \vee (c? \in \text{dom } insured \wedge in? \notin \text{dom } insured(c?))) \wedge$ $report! = notInsured \wedge payment! = 0) \vee$ $(c? \in \text{dom } insured \wedge in? \in \text{dom } insured(c?) \wedge report! = done \wedge$ $((loss? \geq insured(c?) \wedge payment! = insured(c?)) \vee$ $(loss? < insured(c?) \wedge payment! = loss?))$</p>
--

A logically equivalent formulation of *HandleIncident* is also possible by using a conjunction of two implications.

Answer 3

1. $Ext(h) = \{P, A, A2, B, B2\}$, $Ent(h) = \{P, A, A1, B, B2\}$
 $Ext(h/g) = \{B2\}$, $Ent(h/g) = \{B1\}$
 $Ext(h/f) = \{P, A, A2, B, B2\}$, $Ent(h/f) = \{C\}$



Answer 4

1. $O_{F_X}(S) = \{s_1, s_2\} \cap [\cdot b \cdot]S$
 - $S = Proc$: $O_{F_X}(Proc) = \{s_1, s_2\} \cap [\cdot b \cdot]Proc = \{s_1, s_2\} \cap Proc = \{s_1, s_2\}$
 - $S = Proc$: $O_{F_X}(\{s_1, s_2\}) = \{s_1, s_2\} \cap [\cdot b \cdot]\{s_1, s_2\} = \{s_1, s_2\} \cap \{s_1, s_2\} = \{s_1, s_2\}$
2. $O_{F_X}(S) = \{s_1, s_2\} \cup (\langle \cdot a \cdot \rangle S \cup \langle \cdot b \cdot \rangle S)$
 - $S = \emptyset$: $O_{F_X}(\emptyset) = \{s_1, s_2\} \cup (\langle \cdot a \cdot \rangle \emptyset \cup \langle \cdot b \cdot \rangle \emptyset) = \{s_1, s_2\} \cup (\emptyset \cup \emptyset) = \{s_1, s_2\} \cup \emptyset = \{s_1, s_2\}$
 - $S = \{s_1, s_2\}$: $O_{F_X}(\{s_1, s_2\}) = \{s_1, s_2\} \cup (\langle \cdot a \cdot \rangle \{s_1, s_2\} \cup \langle \cdot b \cdot \rangle \{s_1, s_2\}) = \{s_1, s_2\} \cup (\{s\} \cup \{s_2, s_2\}) = \{s, s_1, s_2\}$
 - $S = \{s, s_1, s_2\}$: $O_{F_X}(\{s, s_1, s_2\}) = \{s_1, s_2\} \cup (\langle \cdot a \cdot \rangle \{s, s_1, s_2\} \cup \langle \cdot b \cdot \rangle \{s, s_1, s_2\}) = \{s_1, s_2\} \cup (\{s\} \cup \{s_2, s_2\}) = \{s, s_1, s_2\}$

Answer 5

$$[true^* \cdot a \cdot \bar{b}^* \cdot a] \text{ false}$$

Answer 6 The first formula expresses that any reachable state that is reached by an a -action allows a path in which a b -action occurs. The second formula expresses that for any reachable state that is reached by an a -action, in any future in which b has not occurred (yet), b can occur on some path.

A simple labelled transition system for which the first formula holds and the second doesn't is the following transition system

