Master of Science in Grenoble Mosig – 1st year – December 2021

Software Engineering exam – Part II: Formal methods (5 points)

Write your answers directly on this sheet and hand it in with the rest of your copy. Don't write your name. Bad answers will count negatively, to avoid random answers.

Algebraic specifications

We consider natural numbers nat defined by constructors $0 : \rightarrow \text{nat}$ and $s : \text{nat} \rightarrow \text{nat}$, as well as lists of natural numbers nat_list with constructors $\text{nil} : \rightarrow \text{nat\_list}$ and $\text{cons} : \text{nat}, \text{nat\_list} \rightarrow \text{nat\_list}$. We define three functions f_1, f_2, and cat as follows (the identifier between parentheses after each equation is the equation name):

$f_1 : \text{nat\_list}, \text{nat} \rightarrow \text{nat\_list}$		$f_2 : \text{nat\_list}, \text{nat} \rightarrow \text{nat\_list}$	
$f_1(l, 0) = \text{nil}$	(f_1_1)	$f_2(l, 0) = l$	(f_2_1)
$f_1(\text{nil}, \text{s}(n)) = \text{nil}$	(f_1_2)	$f_2(\text{nil}, \text{s}(n)) = \text{nil}$	(f_2_2)
$f_1(\text{cons}(m, l), \text{s}(n)) = \text{cons}(m, f_1(l, n))$	(f_1_3)	$f_2(\text{cons}(m, l), \text{s}(n)) = f_2(l, n)$	(f_2_3)
$\text{cat} : \text{nat\_list}, \text{nat\_list} \rightarrow \text{nat\_list}$			
$\text{cat}(\text{nil}, l) = l$	(cat_1)		
$\text{cat}(\text{cons}(m, l_1), l_2) = \text{cons}(m, \text{cat}(l_1, l_2))$	(cat_2)		

1) What does the function $f_1(l, n)$ compute?

- ☑ the list of the n first elements of l
- ☐ the list of the n last elements of l
- ☐ the list of all but the n first elements of l
- ☐ the list of all but the n last elements of l

2) We want to show that $(\forall l \in \text{nat\_list}, n \in \text{nat})\ \text{cat}(f_1(l, n), f_2(l, n)) = l$. We first consider an arbitrary l and $n = 0$. Complete this part of the proof by applying the specified equations:

$$\begin{aligned} \text{cat}(f_1(l, 0), f_2(l, 0)) &= \underline{\text{cat}(\text{nil}, f_2(l, 0))} && (\text{f\_1\_1}) \\ &= \underline{f_2(l, 0)} && (\text{cat\_1}) \\ &= \underline{l} && (\text{f\_2\_1}) \end{aligned}$$

3) We now assume that there exists n such that $(\forall l)\ \text{cat}(f_1(l, n), f_2(l, n)) = l$ and we call this equation (ih_1). We want to show that $\text{cat}(f_1(l, \text{s}(n)), f_2(l, \text{s}(n))) = l$. To this aim, we first consider the case $l = \text{nil}$. Complete this part of the proof (provide the name of each equation applied):

$$\begin{aligned} \text{cat}(f_1(\text{nil}, \text{s}(n)), f_2(\text{nil}, \text{s}(n))) &= \underline{\text{cat}(\text{nil}, f_2(\text{nil}, \text{s}(n)))} && (\underline{\text{f\_1\_2}}) \\ &= \underline{f_2(\text{nil}, \text{s}(n))} && (\underline{\text{cat\_1}}) \\ &= \underline{\text{nil}} && (\underline{\text{f\_2\_2}}) \end{aligned}$$

4) Finally, we prove that $\text{cat}(f_1(\text{cons}(m, l), \text{s}(n)), f_2(\text{cons}(m, l), \text{s}(n))) = \text{cons}(m, l)$ using (ih_1) as follows. Complete the proof by providing the equation that was used at each line:

$$\begin{aligned} \text{cat}(f_1(\text{cons}(m, l), \text{s}(n)), f_2(\text{cons}(m, l), \text{s}(n))) &= \text{cat}(\text{cons}(m, f_1(l, n)), f_2(\text{cons}(m, l), \text{s}(n))) && (\underline{\text{f\_1\_3}}) \\ &= \text{cat}(\text{cons}(m, f_1(l, n)), f_2(l, n)) && (\underline{\text{f\_2\_3}}) \\ &= \text{cons}(m, \text{cat}(f_1(l, n), f_2(l, n))) && (\underline{\text{cat\_2}}) \\ &= \text{cons}(m, l) && (\underline{\text{ih\_1}}) \end{aligned}$$

5) We now have proven that $(\forall l, n)\ \mathrm{cat}(f_1(l,n), f_2(l,n)) = l$. How do you call the type of reasoning that we have used?

This is called a proof by (structural) induction.

B method

6) What can you guarantee when you have proven the proof obligations of a B state machine?

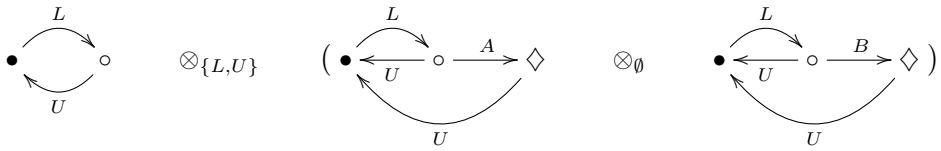
☐ That the implemented system will have no bug
☑ That the invariant of the state machine is satisfied
☐ That the state machine is a concrete program

7) What is the result of [**IF** $X < 0$ **THEN** $Y := Y - 1$ **ELSE** $Y := Y + 1$ **END IF**] $Y = 10$?

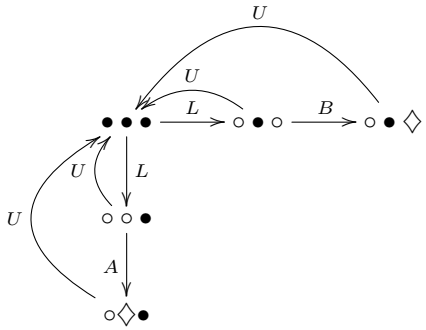
☑ $(X < 0 \wedge Y = 11) \vee (X \geq 0 \wedge Y = 9)$
☑ $(X < 0 \Rightarrow Y = 11) \wedge (X \geq 0 \Rightarrow Y = 9)$
☐ $9 \leq Y \wedge Y \leq 11$
Both checked answers are equivalent. Giving only one of them was considered correct.

Automata-based verification

We consider the following product of automata, where $\bullet, \circ$, and $\diamondsuit$ represent states and where $\bullet$ is initial state:



8) The reachable states are depicted below. Draw the transitions of the product.



9) What is the meaning of the temporal logic formula $\langle a^*.b \rangle\ \varphi$?

☐ There exists a sequence of transitions consisting of zero or one a followed by one b, leading to a state where the formula φ holds
☑ There exists a sequence of transitions consisting of (zero or more) a's followed by one b, leading to a state where the formula φ holds
☐ All sequences of transitions consisting of zero or one a followed by one b lead to states where φ holds
☐ All sequences of transitions consisting of (zero or more) a's followed by one b lead to states where φ holds

10) $\langle \beta \rangle\ \varphi = \neg[\beta]\ \neg\varphi$

☑ This equality is true for all regular action formula β and state formula φ
☐ This equality is false: there exist action formulas β and state formulas φ such that $\langle \beta \rangle\ \varphi \neq \neg[\beta]\ \neg\varphi$)