DD2452 Formal Methods

TAKE-HOME EXAMINATION PROBLEMS
25 October 2018

Dilian Gurov, KTH EECS
08-790 81 98

Give cleanly written solutions in English or Swedish, each problem beginning on a new page. Write your name on all sheets. The maximal number of points is given for each problem. Up to two bonus points from the homework assignments will be taken into account for each level (E, C, and A). Upload your solutions on CANVAS, as a PDF file, no later than 10:00 on Monday, 29 October 2018. The exam is strictly individual. KTH's rules for cheating and plagiarism apply.

---

1 Level E

For passing level E you need 8 (out of 10) points from this section.

1. Consider **Dilian's Verification Condition Generator**, presented in class (slides 16-17 of Lecture 2). Explain briefly the idea behind the vc-function. How does it relate to the wlp-function, presented on slide 11? Why does it introduce an accumulator? How is this accumulator used? [2p]
2. Consider the wp-function over the **Intermediate Language**, presented on slide 23, and the treatment of annotated while-loops presented on slide 26. Explain briefly the idea behind this treatment. Why does it work? How does it relate to the $\mathsf{Partial-while}$ rule of Hoare logic? [2p]
3. Consider the **adequate set** of CTL connectives: [3p]

   $$\phi ::= \mathsf{false} \mid p \mid \neg\phi \mid \phi \wedge \phi \mid \mathsf{EX}\,\phi \mid \mathsf{AF}\,\phi \mid \mathsf{E}\,(\phi\,\mathsf{U}\,\phi)$$

   which we used in the Labelling Algorithm, and the re-write rules for the remaining connectives, presented on slide 8 of Lecture 6. Complete the rules with a rule for $\mathsf{A}\,(\phi\,\mathsf{U}\,\psi)$. Justify formally your new rule. (*Hint*: See book.)
4. Apply the **CDCL algorithm** from the Lecture 4 slides to determine the (un)satisfiability of the following Boolean formula. Whenever the algorithm does not clearly specify what clause or literal to consider next, hence allowing for more than one choice, you are free to make your own choice (assumption). Each step of the algorithm should be properly explained in the final solution. [3p]

   $(x_1 \vee x_2 \vee x_3) \wedge (\neg x_1 \vee x_2 \vee x_3) \wedge (x_1 \vee \neg x_2 \vee x_3) \wedge (\neg x_1 \vee \neg x_2 \vee x_3) \wedge (x_1 \vee x_2 \vee \neg x_3)$
   $\wedge (\neg x_1 \vee \neg x_2 \vee \neg x_3) \wedge (x_1 \vee \neg x_2 \vee \neg x_3) \wedge (\neg x_1 \vee x_2 \vee \neg x_3)$

---

2 Level C

For grade D you need to have passed level E and obtained 5 (out of 10) points from this section.
For passing level C you need 8 points from this section.

1. Consider again the wp-function presented on slide 23 of Lecture 2. In particular, notice that (unlike the vc-function) the wp-function works *without* using an accumulator parameter. Use the same underlying idea to present a modified version of the vc-function (that is, also defined on the source language!) that is still defined by structural induction on C, but does *not* use an accumulator. Explain and justify your new definition. (*Hint*: Combine the translation to Intermediate Language with the wp-function to derive a defining clause for $\mathsf{vc}(\{\eta\}\ \texttt{while}\ B\ \{C\}, \psi)$. Show your derivation as justification.) Explain also how, even though without using an accumulator, your version achieves the same result as the original vc-function. [5p]
2. In the course, we gave a "local" **Semantics of CTL** (slide 24 of Lecture 5), in the sense that it was given as a satisfaction relation $\mathcal{M}, s \models \phi$ over individual states s. This presentation makes it less suitable for a formal justification of the **Labelling Algorithm** (slides 9-10 of Lecture 6).
   (a) [3p] Define an alternative, *global semantics* of CTL, by means of a *denotation* $\|\phi\|^{\mathcal{M}}$ consisting of all states $s \in S$ that satisfy ϕ. That is, define $\| \phi \|^{\mathcal{M}}$ by *structural induction*, where it suffices (for brevity) to consider just the adequate set from Problem E3 above. You are encouraged to introduce suitable state transformers in order to make the formal definition more elegant.
   (b) [2p] Use your global semantics of CTL to formally justify the Labelling Algorithm.

---

3 Level A

For grade B you need to have passed level C and obtained 5 (out of 10) points from this section. For grade A you need 8 points from this section.

1. [4p] Consider again your global **Semantics of CTL** from Problem C2a. Show that your semantics is consistent with the local one given in class (slide 24 of Lecture 5). That is, prove by *structural induction* that $s \in \| \phi \|^{\mathcal{M}}$ if and only if $\mathcal{M}, s \models \phi$. State explicitly the induction hypotheses in each inductive case, and indicate where you use them. Show the proofs of (at least) the three cases p, $\phi_1 \wedge \phi_2$ and $\mathsf{EX}\,\phi$.
2. Consider the following program snippet and show via **Predicate Abstraction** that location `BOOM` is not reachable.

```
x = num;
y = num + 1;
if (x == y) {
   //BOOM
}
```

   (a) [3p] Create an abstract *Boolean program* using the set of predicates $P = \{x == num\}$, and explain why location `BOOM` is reachable in the abstract program. Explain why this is not a real counterexample for the original program.
   (b) [3p] Extend the set of predicates P with additional predicates that allow to prove that location `BOOM` is not reachable.

Good luck!