“Model checking”

Prof. Dr. Marcel Kyas

Assignment 3, October 28, 2009

Exercise 6 (4 Points) The following incorrect mutual exclusion algorithm has been published in the January 1966 issue of the „Communication of the ACM“. The algorithm is for two processes; let $i \in \{0, 1\}$ be their identities. It uses three shared variables turn, flag[0] and flag[1]. Initially, flag[0]=0 and flag[1]=0. The initial value of turn is either 0 or 1.

```
process P[i = 0,1] {
  for (;;) {
    // Remainder
    flag[i] = 1;
    while (turn == 1 − i) {
      await flag[1−i] == 0;
      turn = i;
    }
    // Critical section
    flag[i] = 0;
  }
}
```

1. Formalise this algorithm in Promela
2. Formalise the mutual exclusion property by a never claim.
3. Use SPIN to find the error in this algorithm.
4. Carefully explain the counter example trace that SPIN generates.

Exercise 7 (6 Points) The following program is a mutual exclusion protocol for two processes due to Amir Pnueli. There is a single shared variable s that is either 0 or 1 and initially 1. Besides, each process has a local Boolean variable y that initially equals 0. The program text for process P_i ($i \in \{0, 1\}$ is as follows:

```
for(;;) {
  // Non−critical section
  ($y_i$,s) = (1,i);
  await (($y_{1-i}$==0) || (s != i));
  // critical section
  $y_i$ = 0;
}
```

Here, the statement (y_i,s)=(1,i) is a multiple assignment in which y_i=1 and s=i are executed as one single atomic step.

1. Formalise this algorithm in Promela.
2. Formulate a never claim that demonstrates whether the algorithm is correct.
3. Formulate a never claim that demonstrates whether the algorithm is free of deadlock.
4. Formulate a never claim that demonstrates whether the algorithm is free of starvation.

The last three questions may be answered by using SPIN.

Exercise 8 (4 Points) Consider the set AP of atomic propositions defined by $\{x = 0, x > 1\}$ and consider a non-terminating sequential computer program P manipulates the variable x. Formulate the following informally stated properties as LTL properties.

1. false.
2. initially x is equal to zero.
3. initially x differs from zero.
4. initially x is equal to zero, but at some point x exceeds one.
5. x exceeds one only finitely many times.
6. x exceeds infinitely often.
7. the value of x alternates between zero and some value larger than one.
8. true.

Determine which of the provided LTL properties are safety properties. Justify your answers.

Exercise 9 (5 Points) The following list of temporal congruences and equivalences contains valid and invalid formulae. Break each congruence into two entailments and each equivalence into two implications. For each entailment or implication claimed to be valid, give an informal (semantic) justification. For an entailment or implication φ claimed to be invalid, describe a sequence σ such that $\sigma \not\models \varphi$.

(1) $$\Diamond p \land \Box q \iff \Diamond(p \land \Box q)$$

(2) $$\Diamond p \land \Box q \iff \Box(\Diamond p \land q)$$

(3) $$\Diamond\Box p \land \Diamond\Box q \iff \Diamond(\Box p \land \Box q)$$

(4) $$(p\mathcal{U}q)\mathcal{U}q \iff p\mathcal{U}q$$

(5) $$p\mathcal{U}q \iff ((\neg p)\mathcal{U}q \to p\mathcal{U}q)$$

(6) $$p\mathcal{U}q \land q\mathcal{U}r \iff p\mathcal{U}r$$

(7) $$\Box p \lor \Diamond q \iff (\Diamond q)\mathcal{R}p$$

(8) $$\Diamond\Box(p \to \Box q) \leftrightarrow (\Diamond\Box q \lor \Diamond\Box\neg p)$$

(9) $$\neg(p\mathcal{U}q) \leftrightarrow (\neg q)\mathcal{W}(\neg p \land \neg q)$$

(10) $$\neg(p\mathcal{U}q) \iff (\neg q)\mathcal{W}(\neg p \land \neg q)$$

Exercise 10 (6 Points) Consider the following classic problem:

> A farmer has a goat, a wolf and a cabbage. He must cross a river in a boat that will only carry himself and one item at a time. If he leaves the goat and the cabbage and takes the wolf, the goat will eat the cabbage. If he leaves the wolf and the goat and takes the cabbage, the wolf will eat the goat. The same applies once they are on the other side.

Model this problem in Promela and write a specification in SPIN that solves this problem. Your claim should provide an error trail that represents a correct solution to this problem.

Exercise 11 (6 Points) The article "Experience with Literate Programming in the Modelling and Validation of Systems" by Theo C. Ruys and Ed Brinksma (1998) (doi:10.1007/BFb0054159) describes the following problem:

> Four soldiers who are heavily injured, try to flee to their home land. The enemy is chasing them and in the middle of the night they arrive at a bridge that spans a river which is the border between the two countries at war. The bridge has been damaged and can only carry two soldiers at a time. Furthermore, several landmines have been placed on the bridge and a torch is needed to sidestep all the mines. The enemy is on their tail, so the soldiers know that they have only 60 minutes to cross the bridge. The soldiers only have a single torch and they are not equally injured. The following table lists the crossing times (one-way!) for each of the soldiers:
>
> | | |
> |---|---|
> | soldier S_0 | 5 minutes |
> | soldier S_1 | 10 minutes |
> | soldier S_2 | 20 minutes |
> | soldier S_3 | 25 minutes |
>
> Does a schedule exist which gets all four soldiers to the safe side within 60 minutes?

Model this problem in PROMELA. Express a property that allows you to fing a schedule that answers this question.

Handing in this Assignment Please submit your hand-written solutions to exercise 8 and 9 on paper no later than November 11, 2009, 18:00 (before the tutorial session).

The models shall be placed in a directory that carries the last name of one of the group members. Add a readme file, or better, a `Makefile`, that explains or automates the modelling and checking procedures. Explain, how to interprete the results of model checking in an accompanying PDF file.

Put all this into a tape archive that shares the name with the directory and send it by e-mail to marcel.kyas@fu-berlin.de. Use "Model checking 09 Series 3 *your last names*" as the subject line.