CS 267 – Spring 2023 – Homework Assignment 3

Due Wednesday June 7th by 5:00pm. Turn in a hard copy either in class or drop in the instructor's mailbox at HFH 2108. Do not discuss the problems with anyone other than the instructor.

1. Give a Büchi automaton A_f that corresponds to the LTL property GFp.

Given the transition system $T = (S, I, R)$ where $I = \{0\}$, $S = \{0, 1, 2\}$ and $R = \{(0, 1), (1, 2), (2, 1), (1, 1)\}$, assume that the only state which satisfies the atomic proposition p is 1. Show the Büchi automaton A_T that corresponds to this transition system (based on the construction given in the lecture notes), and the product automaton $A_T \times A_f$.

If there is one, show an accepting run of the product automaton and show the path in the transition system T which corresponds to this run and satisfies the LTL formula GFp.

Does the transition system T satisfy the property $FG\neg p$? Why?

2. Construct a Büchi automaton that corresponds to the LTL property $p\ U\ (q \wedge X\ (\neg q))$ using the LTL-Büchi automata translation algorithm. Show the intermediate steps (like the example in the lecture notes).

3. Given the following piece of code:

```
x = y;
while (x < z) {
  x++;
}
assert(x == z);
```

demonstrate the verification approach used by the CBMC model checker by 1) converting it to a loop free code by unwinding the loop 2 times, 2) converting the resulting code to the static single assignment form, 3) generating the constraint for the verification of the assertion. Determine if the generated constraint is satisfiable and give a satisfying assignment if it is.

4. Consider the following two transition systems:

$M_1 = (AP, S, R, S_0, L)$ with the set of states $S = \{0, 1, 2, 3\}$, the initial set of states $S_0 = \{0\}$, the transition relation $R = \{(0, 1), (1, 2), (2, 3), (1, 0), (3, 2)\}$, the set of atomic propositions $AP = \{p, q\}$ and the labeling function $L : S \to 2^{AP}$ where $L(0) = \{p\}$, $L(1) = \{p\}$, $L(2) = \{q\}$, and $L(3) = \{q\}$.

$M_2 = (AP, S, R, S_0, L)$ with the set of states $S = \{0, 1\}$, the initial set of states $S_0 = \{0\}$, the transition relation $R = \{(0, 0), (0, 1), (1, 1), \}$, the set of atomic propositions $AP = \{p, q\}$ and the labeling function $L : S \to 2^{AP}$ where $L(0) = \{p\}$, and $L(1) = \{q\}$.

Is there a simulation relation between these two transition systems? If there is, show the simulation relation.

Determine if M_2 satisfies AGp, AGq, AFp, AFq by identifying the states of M_2 that satisfy these properties. Given these results, can you determine if M_1 satisfies these properties?

5. Assume that you are given the statement "y := x + 1" and two predicates $y > x$ and $y > 0$. Show how predicate abstraction technique would abstract this statement by 1) computing the preconditions, 2) checking the implications, and 3) generating the abstract code. (Assume that x and y are unbounded integer variables). In the second step (checking the implications) use the web interface for the Z3 theorem prover which is available at:
https://microsoft.github.io/z3guide/docs/logic/intro/
(use the Playground tab to enter a formula and run Z3)

In addition to the results of the steps 1, 2 and 3, turn in the formulas that you checked with Z3.