1. Consider a transition system with two states encoded using a single boolean variable $x$, where the initial state is $x$ and the transition relation is defined as $x \land \neg x' \lor \neg x \land x'$.

(a) Show the Boolean logic formula that corresponds to unrolling the above transition system twice starting from the initial state.

(b) Assume that we would like to check the property $\text{EX(\text{EX}(\neg x))}$. Using the result from part (a), construct a boolean logic formula $F$ that is satisfiable if the initial state satisfies the property. Give a satisfying assignment to the variables in the formula $F$ if $F$ is satisfiable.

(c) Now, assume that we would like to check the property $\text{EF}(x)$. Again, using the result from part (a), construct a boolean logic formula $F$ that is satisfiable if the initial state satisfies the formula $\text{EF}(x)$ within two steps of execution. Give a satisfying assignment to the variables in the formula $F$ if $F$ is satisfiable.

2. Given the following piece of code:

```c
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 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.

3. 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 $L : S \rightarrow 2^{AP}$ 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 $L : S \rightarrow 2^{AP}$ where $L(0) = \{p\}$, and $L(1) = \{q\}$.

Is there a simulation relation between $M_2$ and $M_1$? If there is, show the relation.

Determine if $M_2$ satisfies $\text{AG}_p$, $\text{AG}_q$, $\text{AF}_p$, $\text{AF}_q$ by identifying the states of $M_2$ that satisfy these properties. Given these results, can you determine if $M_1$ satisfies these properties?

4. 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: http://rise4fun.com/z3

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

5. Consider the following two papers that you read as part of your reading assignments:


Briefly explain the verification techniques used in these papers. Compare and contrast the verification techniques used in these papers and discuss their advantages and disadvantages.