Formal Model and Verification

Exercise 9: Symbolic on-the-fly safety analysis and liveness analysis

1. We have the following GCM program rules with integer variables x, y, z.

when (x==1) may x = 0; y = *1*; z = y;
when (x==0 && z > 0) may z = z-1;
when (x==0 && y > 0 && z == 0) may y = y-1; z = y;
when (x==0 && y == 0 && z == 0) may y = y+2;

The range of the three variables are all [0,10]. The initial condition of the program is x==1 && y == 0 && z == 0. Please use the on-the-fly least fixpoint algorithm for forward analysis to construct a formula for the forward reachable states from the initial states.

2. Continued from question 1, assume now we have a risk condition y==1&&z==1. Please use the on-the-fly least fixpoint algorithm for backward analysis to check whether the system is safe or not.

3. Continued from question 1, please use the on-the-fly symbolic greatest fixpoint algorithm to construct a propositional formula that characterizes states satisfying ∃□(*y*<2). According to the formula you constructed, please tell me whether the initial state satisfies ∀◇(y>=2) ?