Name: LOKESH MEHRA

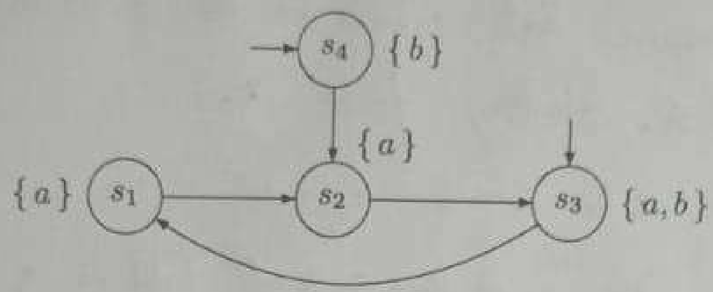
Roll No: 220591 (e.g. 170001)

Dept.: EE (e.g. CSE)

Indian Institute of Technology Kanpur
CS637 Embedded and Cyber-Physical Systems
Homework Assignment 3
Deadline: November 8, 2024

Total: **40 marks**

Problem 1. (10 points)
Consider the following state machine over the set of atomic propositions $\{a, b\}$:



Decide for each of the following LTL specifications whether the model satisfies it. For the positive outcome, provide a proof. For the negative outcome, provide a counterexample trace.
Note that the symbols $\bigcirc$, $\Box$, $\Diamond$, and $\mathtt{U}$ represent the "next", "always", "eventually", and "until" temporal operators respectively.

(a) $\bigcirc\bigcirc\bigcirc a$
(b) $\Box b$
(c) $\Box\Diamond a$
(d) $\Box(b \,\mathtt{U}\, a)$
(e) $\Diamond(a \,\mathtt{U}\, b)$

Name: LOKESH MEHRA

Roll No: 220591 Dept.: EE

Indian Institute of Technology Kanpu
CS637 Embedded and Cyber-Physical Systen
Homework Assignment
Deadline: November 8, 20

Ans 1 a) ○ ○ ○ a

This formula requires that a holds in the third state following the current state. Starting from s_1;

→ The path from s_1 is $s_1 \to s_2 \to s_3 \to s_1$.

→ Following this path, a ~~do~~ does indeed hold in s_1 (~~the~~ the third state after the starting state)

Therefore, the model satisfies ○○○a

b) □b

The specification requires that b holds in all states in every possible path.

→ In the model, state s_2 does not satisfy b (only a holds in s_2)

→ This means that there is at least one state in the model where b does not hold.

Thus, the model ~~does~~ does not ~~at~~ satisfy □b. ~~Ano~~

→ A counterexample is the path $s_1 \to s_2$, where b is not true in s_2

c) □ ~~◇~~ ◇a

This formula means that there is some point in the future where a will hold in all subsequent states.

→ However, there is a cycle $s_1 \to s_2 \to s_3 \to s_1$ that does not guarantee a holds always. (for instance, s_3 has both a and b)

Name: LOKESH MEHRA
Roll No: 220593 Dept.: EE

Indian Institute of Technology Kanpur
CS637 Embedded and Cyber-Physical Systems
Homework Assignment 3
Deadline: November 8, 2024

→ Thus, the model does not satisfy $\square\Diamond a$.

→ A counterexample is the path $s_1 \to s_2 \to s_3 \to s_1$, where b appears periodically.

d) $\square(b \cup a)$

This specification means that in all paths, b must hold until a eventually holds.

→ In the path $s_4 \to s_2$, b holds in s_4, and a holds in ~~s~~ s_2, which satisfies $b \cup a$.

→ In the ~~cy~~ cycle $s_1 \to s_2 \to s_3 \to s_1$, a is present in each state, which also satisfies $b \cup a$.

Therefore, the model satisfies $\square(b \cup a)$

e) $\Diamond(a \cup b)$

This formula specifies that there exists a path where a holds ~~unt~~ until b eventually holds.

→ In the path $s_1 \to s_3$, a holds in s_1, and b holds in s_3.

→ This satisfies the condition that a holds until b is encountered.

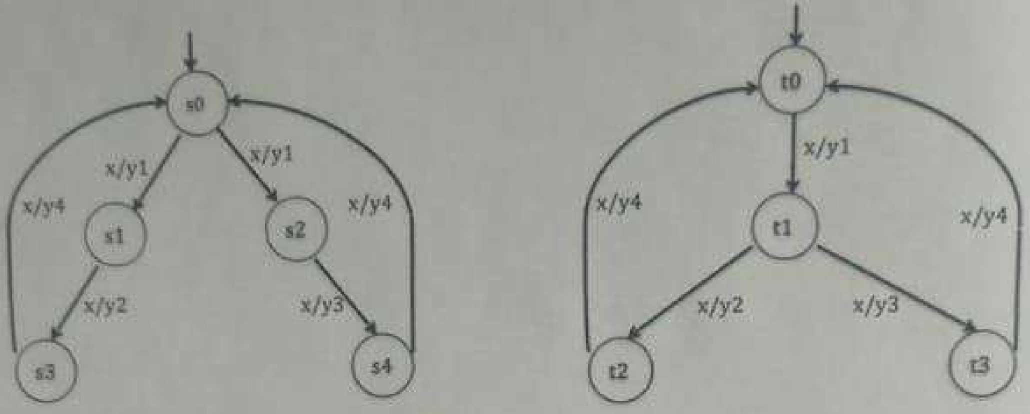
Thus, the model satisfies $\Diamond(a \cup b)$

Name: LOKESH MEHRA

Roll No: 220591
e.g. 170001

Dept.: EE
e.g. CSE

Problem 2. (10 points)
Consider the two state machines in Figure 1 and answer the following questions:



(a) M_1 (b) M_2

Figure 1

(a) Does the state machine M_1 simulate the state machine M_2? If yes, provide the simulation relation. If no, provide a transition of M_2 that M_1 cannot match.

(b) Does the state machine M_2 simulate the state machine M_1? If yes, provide the simulation relation. If no, provide a transition of M_1 that M_2 cannot match.

(c) Are the two state machines bisimilar? If yes, provide the bisimulation relation. If no, provide one reason.

Name: LOKESH MEHRA

Roll No: (e.g. 170001) 220591 Dept.: (e.g. CSE) EE

a) To verify if M_1 simulates M_2, we need to check if there ~~is~~ exists a simulation relation $R \subseteq M_1 \times M_2$ such that for every pair of states $(s, t) \in R$, every transition from t in M_2 can be matched by a corresponding transition from s in M_1.

- From t_0 in M_2, we have three transitions: $(t_0, x/y_1, t_1)$, $(t_0, x/y_4, t_2)$, and $(t_0, x/y_4, t_3)$
- From s_0 in M_1, there are also three transitions: $(s_0, x/y_1, s_1)$, $(s_0, x/y_4, s_3)$ and $(s_0, x/y_4, s_4)$.

By mapping s_1 to t_1, s_3 to t_2, and s_4 to t_3, we can ~~create~~ create a relation $R = \{(s_0, t_0), (s_1, t_1), (s_3, t_2), (s_4, t_3)\}$ such that every transition from a state in M_2 can be matched by a transition from the corresponding state in M_1.

Therefore, M_1 simulates M_2.

b) To verify if M_2 simulates M_1, we again need to check if there exists a simulation relation $R' \subseteq M_2 \times M_1$ such that every transition from a state in M_1 can be matched by a corresponding transition in M_2.

Name: LOKESH MEHRA
Roll No: 220591 Dept.: EE

Let's examine the states:

- From s_0 in M_1, there is a transition $(s_0, x/y2, s_3)$
- In M_2, t_0 does not have a corresponding $x/y2$ transition

Since M_2 cannot match the transition $(s_0, x/y2, s_3)$ from M_1, there is no simulation relation from M_2 to M_1. Therefore, M_2 does not simulate M_1.

(c) Bisimilarity requires both M_1 simulates M_2 and M_2 simulates M_1. As we know for (a & b),

M_1 simulates M_2 but M_2 does not simulate M_1,

Since mutual simulation does not hold, M_1 and M_2 are not bisimilar

Name: LOKESH MEHRA

Roll No: 220591 (e.g. 170001) Dept.: EE (e.g. CSE)

Problem 3. (10 points)
Consider the processes P_1 and P_2 with the shared variables b_1, b_2, and x. Variables b_1 and b_2 are Boolean variables, while variable x can take either the value 1 or 2. Initially, each process P_i is in the non-critical section (i.e., P_i is in location $noncrit_i$). The scheduling strategy for giving the processes access to the critical section is realized using x as follows. If both processes want to enter the critical section (i.e., P_i is in location $wait_i$), the value of variable x decides which of the two processes may enter its critical section: if $x = i$, then P_i may enter its critical section $crit_i$ (for $i = 1, 2$). On entering location $wait_1$, process P_1 performs $x := 2$, thus giving privilege to process P_2 to enter the critical section. The value of x thus indicates which process has its turn to enter the critical section. Symmetrically, P_2 sets x to 1 when starting to wait. The variables b_i provide information about the current location of P_i. More precisely, b_i is set when P_i starts to wait, and is reset when the process exits the critical section. In pseudocode, P_1 performs as follows (the code for process P_2 is similar):

P_1 **loop** forever

⋮ (*noncritical actions*)

$b_1 := true; x := 2$

wait until $(x = 1 \vee \neg b_2)$ (*request*)

do critical section **od**

$b_1 := false$ (*release*)

⋮ (*noncritical actions*)

end loop

(a) Draw the state machines for P_1 and P_2.

(b) Show the state machine that is obtained by asynchronous composition of P_1 and P_2.

(c) How many total states are there in the composed state machine? How many of them are reachable?

(d) Provide an LTL formula that captures the requirement that the process P_1 and P_2 will not enter the critical section simultaneously. Using the composed state machine, determine whether the two systems satisfy the formula (property).

Name: LOKESH MEHRA

Roll No: 220591 (e.g. 170001) Dept.: EE (e.g. CSE)

Indian Institute of Technology Kanp
CS637 Embedded and Cyber-Physical Systen
Homework Assignment
Deadline: November 8, 20

Ans The pseudocode for P_1 and P_2 indicates that each process has five main states:

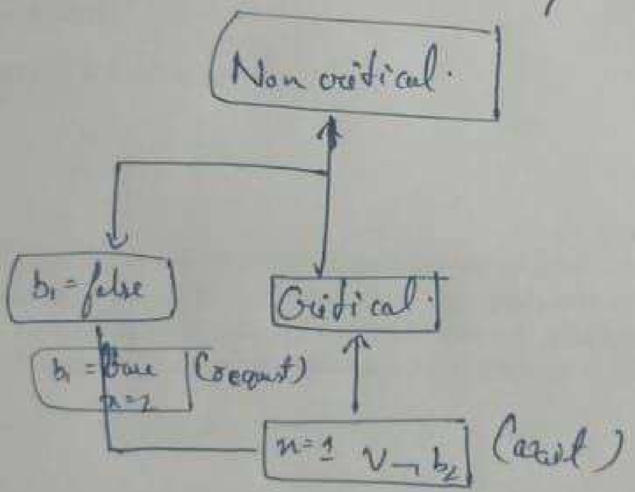
N → Noncritical Actions R → Request (setting b_i := true and $x = i$)

W → Wait (waiting for the condition to enter the critical section)

C → Critical section (executing critical section code)

L → Release (resetting b_i := false upon exiting the critical section)

The state machines for P_1 and P_2 are as follows.



b) To compose the state machines asynchronously we consider the Cartesian product of the states of P_1 and P_2. Each combined state represents a pair of states, one from P_1's state machine and one from P_2's state machine.

Name: LOKESH MEHRA
Roll No: 220591 (e.g. 170001)
Dept.: EE (e.g. CSE)

Indian Institute of Technology Kanpur
CS637 Embedded and Cyber-Physical Systems
Homework Assignment 3
Deadline: November 8, 2024

(N, N), (N, R), (N, W), (N, C), (N, L),
(R, N), (R, R), (R, W), (R, C), (R, L),
(W, N), (W, R), (W, W), (W, C), (W, L),
(C, N), (C, R), (C, W), (C, C), (C, L),
(L, N), (L, R), (L, W), (L, C), (L, L)

Thus, there are a total of $5 \times 5 = 25$ states.

(c) Total states in the Composed State machine and Reachability
We need to analyse which state pairs can be reached based on the ~~rules~~ rules set by x, b_1, b_2. For example:- (C, C) is unreachable because it violates mutual exclusion (both processes cannot be in the critical section at the same time).
- Other unreachable states might include cases where both are waiting indefinitely due to incompatible conditions in x and b_i.

d) To specify that P_1 and P_2 cannot both be in the critical section simultaneously, we use the following Linear Temporal Logic (LTL) formula:-

$$\Box \neg (C_1 \wedge C_2)$$

where :- C_1 denotes P_1 in the critical section. - C_2 denotes P_2 in the critical section.
This formula asserts that at no point in time ($\Box$, meaning "always") will both P_1 and P_2 be in critical section simultaneously

Name: LOKESH MEHRA

Roll No: 220591 (e.g. 170001) Dept.: EE (e.g. CSE)

Problem 4. (10 points)
Consider the following program:

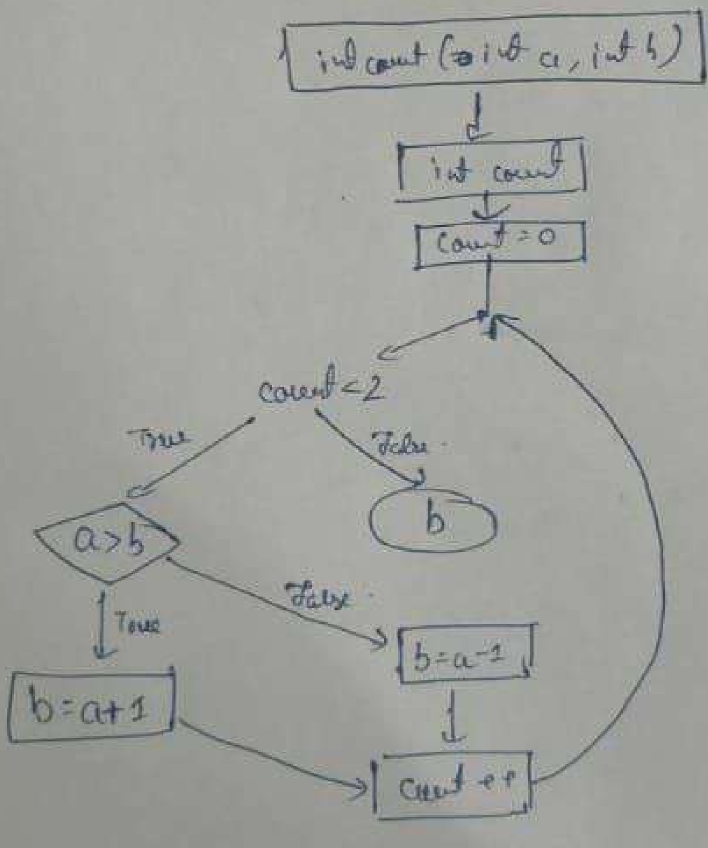
```
int count (int a, int b)
{
    int count;
    for (count = 0; count < 2; count++)
    {
        if (a > b)
            b = a + 1;
        else
            b = a - 1;
    }
    return b;
}
```

(a) Draw a control flow graph for the program.
(b) How many paths are there in the program? How many paths are feasible?
(c) Assume the following:

- An assignment statement (for example, count = 0) requires 2 unit time for execution.
- A statement involving an arithmetic operation followed by an assignment (for example, count ++ b = a + 1) requires 6 unit time for execution.
- A comparison statement (for example, count < 2) requires 4 unit time for execution.

Compute a tight bound on the worst-case execution time for the program.

Ans a)



Name: LOKESH MEHRA
Roll No: 220591 (e.g. 170001)
Dept.: EE (e.g. CSE)

b) Total no. of paths = 4

i) ~~(a>b)~~ Path 1 : (a > b) is true in both iterations.

ii) Path 2 :- (a > b) is true in the first iteration and false in the second.

iii) Path 3 :- (a > b) is false in ~~the~~ the first iteration and true in the second.

iv) Path 4 : (a > b) is false in both iterations.

→ Since b is modified in each iteration, the outcome of a > b can change between iterations.

→ All four paths are feasible depending on the initial values of a and b.

c) Worst Case Execution Time (WCET) Calculation :-

Given Execution times :-

- Initialization
  - count = 0 ; → 2 units.
- First Loop condition Check :
  - count < 2 ; → 4 units
- First iteration
  - count ++ ; → 6 units
  - a > b ; → 4 units
  - b = a ± 1 ; → 6 units
  - Total for first iteration : 6 + 4 + 6 = 16 units

Name: LOKESH MEHRA
Roll No: 220591 Dept.: EE

Indian Institute of Technology Kanpu
CS637 Embedded and Cyber-Physical System
Homework Assignment
Deadline: November 8, 202

- Second Loop Condition Check:
  - count < 2; → 4 units
- Second Iteration:
  - count ++; → 6 units
  - a > b; → 4 units
  - b = a + 1; → 6 units
  - Total for second iteration: 6 + ~~4~~ + 6 = 16 units
- Third Loop Condition Check:
  - count < 2; → 4 units (condition fails, loop ~~exit~~ exits)
- Return Statement:
  - return b; → Execution time negligible or not specified.

Total WCET Calculation:-

Total time = Initialization + First Loop Check + First Iteration + Second Loop Check + Second Iteration + Third Loop Check

= 2 + 4 + 16 + 4 + 16 + 4

= 46 units