The University of Auckland

Department of Electrical, Computer and Software Engineering

COMPSYS 705 Formal Methods for Safety Critical Software Test, 17 October 2023

Last name	Name	ID

Question	Mark
Q1	
Q2	
Q3	
Q4	
Q5	
Q6	
Total	

Assignment Project Exam Help
https://powcoder.com
Add WeChat powcoder

NOTE

1. Answer ALL questions. Part I (Partha's part) covers 70 marks, while Part II (Avinash's Part) covers 30 marks in this test.
2. Questions 1-4 are for Part I and the rest are Part II.
3. The maximum score on this test is 100 marks.
4. Weighting is 50%.
5. Show all code for Questions 5 and 6.
6. Write answer in the box provided.
7. Answers should be legible.

1. Answer the following questions related to the process algebra CCS (20 Marks):

   (a) Consider two processes P, Q shown in Figure 1. Are these processes *bisimilar*, *weakly bisimilar*, *similar* or there is no relationship between them? Justify your selection mathematically by either finding the corresponding relation or showing the absence of any such relation. (5 Marks)

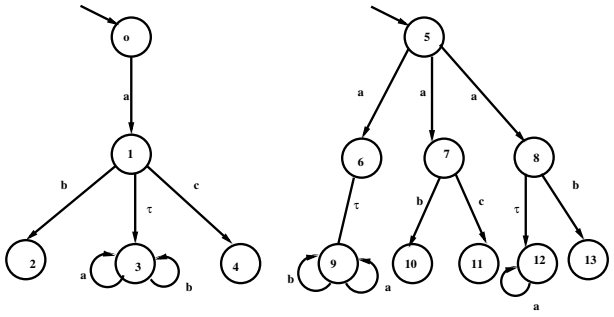


Figure 1: Two CCS Processes

   (b) Consider two processes P and Q defined using system of Equations 1 and Equations 2 respectively. Draw the label transition system (LTS) corresponding to these two processes and then draw the LTS corresponding to $P||Q$ (draw only up to the second-level successors). (10 Marks)

Assignment Project Exam Help

$$P \triangleq a.P1 + b.c.P2$$
$$P1 \triangleq \bar{a}.c + \bar{b}.P \tag{1}$$
$$P2 \triangleq b.P$$

https://powcoder.com

Add WeChat powcoder

$$Q \triangleq \bar{a}.Q1$$
$$Q1 \triangleq a.Q \tag{2}$$

   (c) Which is stronger: simulation or bisimulation and why? Justify using a suitable example. (5 Marks)

Answer box for Q1

Assignment Project Exam Help

https://powcoder.com

Add WeChat powcoder

Answer box for Q1 continued

Assignment Project Exam Help

https://powcoder.com

Add WeChat powcoder

2. Temporal logic and model checking (20 Marks)

(a) Show all the steps of model checking the formula $AF(\neg P1 \wedge \neg P2) \vee P3$ over the model shown in Figure 2. Does, the model satisfy this property? (10 Marks)

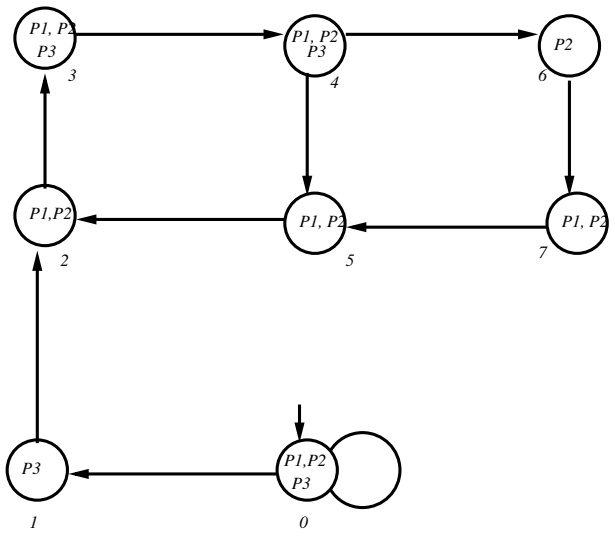


Figure 2: An example Kripke model

(b) Identify valid CTL formulae from the following with suitable justification. Convert the valid formulae you identified into their equivalent forms that are just using adequate sets. Here, $AP = \{p1, p2, p3\}$ and the converted formulae can only include temporal operators EX, EG, EU. (10 Marks)

- $(AG(p1 \Rightarrow AX(p1 \wedge p2)))$
- $AF(p1 \Rightarrow FG(p1 U p2))$
- $AF(p1 \Rightarrow AXp2)$
- $((AFp \Rightarrow EGq) \vee EFp)$

Assignment Project Exam Help
https://powcoder.com
Add WeChat powcoder

Answer box for Q2

Assignment Project Exam Help

https://powcoder.com

Add WeChat powcoder

Answer box for Q2 continued

Assignment Project Exam Help

https://powcoder.com

Add WeChat powcoder

3. Real-time systems and automata (20 Marks)

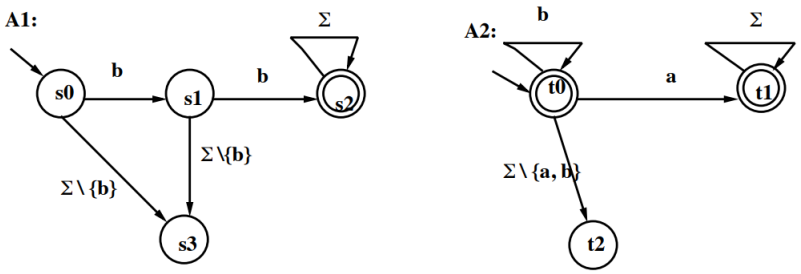


Figure 3: Two automata

(a) Let $\Sigma = \{a,b,c,d\}$ and let $A1, A2$ be two automata as shown in Figure 3. Answer the following questions: (10 Marks)

- Draw the product automaton.
- $bbabab^*$ is accepted by $A1$? Is this true or false? Justify.
- $b^*d^*a^*b^*$ is accepted by $A2$? Is this true or false? Justify.
- $bbbb^*a^*d^*c^*$ is accepted by $A1 \bigcap A2$? Is this true or false? Justify.
- $aabc^*d^*b \in \Sigma^*$. Is this true or false? Justify.

Assignment Project Exam Help

(b) In a timed automata which of the following are valid clock constraints and why? Assume that x, y, z are clocks. (5 Marks)

https://powcoder.com

i. $z >= 12 \wedge x == 20$
ii. $x + y >= \frac{25}{3}$
iii. $x - y <= z$
iv. $z == x + 5$
v. $x - z >= 1000$

Add WeChat powcoder

(c) Distinguish between run-time verification and run-time enforcement. Which one is more suitable for securing pacemakers and why? (5 Marks)

Answer box for Q3

Assignment Project Exam Help

https://powcoder.com

Add WeChat powcoder

Answer box for Q3 continued

Assignment Project Exam Help

https://powcoder.com

Add WeChat powcoder

4. Short answer questions (10 Marks)

   (a) We studied some approaches for using run-time verification for securing pacemakers. Using a suitable diagram, explain how such a monitor works, without being able to access the pacemaker directly.

   (b) Provide an example property as a timed automaton, which can be used by a run-time verification monitor, to determine if a pacemaker has been hacked by using an ECG sensor?

Assignment Project Exam Help

https://powcoder.com

Add WeChat powcoder

Answer box for Q4

Assignment Project Exam Help

https://powcoder.com

Add WeChat powcoder

Answer box for Q4 continued

Assignment Project Exam Help

https://powcoder.com

Add WeChat powcoder

5. Prove that the `swap1` and `swap2` functions below return the same swapped values for *all* the same inputs `a` and `b` of type `int`. Encode the equivalence (validation) problem as SMT constraints in Z3 Python API. Show the Python code. (15 marks)

```
def swap1(a, b):
 tmp = b
 b = a
 a = tmp
 return a, b
```

```
def swap2(a, b):
 a = a + b
 b = a - b
 a = a - b
 return a, b
```

Assignment Project Exam Help

https://powcoder.com

Add WeChat powcoder

Answer box for Q5

Assignment Project Exam Help

https://powcoder.com

Add WeChat powcoder

Answer box for Q5 continued

Assignment Project Exam Help

https://powcoder.com

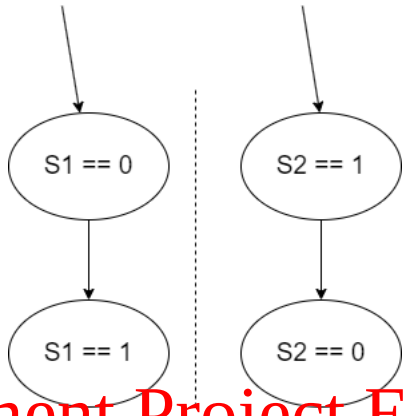
Add WeChat powcoder

6. Figure 4 gives two FSMs executing currently on a single CPU. (1) Draw/give the asynchronous product of the two FSMs as a single FSM. (2) Model *all* the traces/paths of the asynchronous product FSM from (1) using Python Z3 API (see appendix later/below for API functions and their usage). (3) Pose the LTL safety property $\square(\neg((S1 == 1) \wedge (S2 == 1)))$, where $S1$ and $S2$ are integer (`int`) state variables, to Z3 using the Python API, so that it can check this property on the modelled traces from (2). Show all Python code and figures. (15 marks)

   Note:

   (a) You should need no more than 4 variables to model the traces and property.

   (b) This problem is called symbolic bounded model-checking.



Assignment Project Exam Help

Figure 4: Two Finite State Machines (FSMs) running asynchronously on a single CPU. Integer type variables S1 and S2 capture the state value of FSMs.

https://powcoder.com

Add WeChat powcoder

Answer box for Q6

Assignment Project Exam Help

https://powcoder.com

Add WeChat powcoder

Answer box for Q6 continued

Assignment Project Exam Help

https://powcoder.com

Add WeChat powcoder

Example Z3 API function and usage

```
from z3 import IntSort, Solver, sat, DeclareSort, Consts, ForAll,
from z3 import Function, sat, Or, And, RealSort, Implies, Exists
# Defining a new sort (type)
T = DeclareSort('T')
# Defining a binary function that works with type T and returns int type
f = Function('f', T, T, IntSort())
# New object of type Solver
s = Solver()
# Defining two variables of type T
a, b = Consts('a b', T)
# Adding a forall example constraint to solver
s.add(ForAll([a, b], a >= b))
# Example of using Exists
s.add(Exists([a, b], a < b)
# Example of using Implies (a > 0 => b < 10)
s.add(Implies(a > 0, b < 10))
# Example of using implies inside another operator
s.add(ForAll([a, b], Implies(a > 10, b < 100)))
# Defining Variables of type Int
x, y = Consts('x y', IntSort())
# Adding example constraint of variables x and y
s.add(And(Or(x + y > 10, x - y < 100), x * y == 90))
# Defining Variables of type Real (float)
j, k = Consts('j k', RealSort())
# Adding example constraint of variables j and k
s.add(And(Or(j + k > 10.90, j - k < 10/80), j * k == 90.3))
# Checking if a solution exists
ret = s.check()
if ret == sat:
 print(s.model()) # Print the result of check if sat
```

Assignment Project Exam Help
https://powcoder.com
Add WeChat powcoder

Scratch Pad

Assignment Project Exam Help

https://powcoder.com

Add WeChat powcoder

Scratch Pad

Assignment Project Exam Help

https://powcoder.com

Add WeChat powcoder