CS652 Mid-Semester Examination

SAHIL DHULL

TOTAL POINTS

50 / 60

QUESTION 1

1 Question 1 8 / 10

- **- 0 pts** Correct
- **- 2 pts** Q1(a) incorrect
- ✓ **- 2 pts Q1(b) incorrect**
- **- 2 pts** Q1(c) incorrect
- **- 2 pts** Q1(d) incorrect
- **- 2 pts** Q1(e) incorrect

QUESTION 2

2 Question 2 8.5 / 10

- **- 0 pts** Correct
- **- 2 pts** Q2(a) incorrect
- **- 2 pts** Q2(b) incorrect
- **- 2 pts** Q2(c) incorrect
- ✓ **- 1 pts Q2(d)(i) incorrect**
- **- 1 pts** Q2(d)(ii) incorrect
- **- 1 pts** Q2(e)(i) incorrect
- **- 1 pts** Q2(e)(ii) incorrect

- 0.5 Point adjustment

-0.5: You have missed one state in both the execution fragment in Q2(e).

QUESTION 3

3 Question 3 10 / 12

- **- 0 pts** Correct
- **- 4 pts** Q3(a) incorrect
- **- 1 pts** Q3(b)(i) incorrect
- **- 1 pts** Q3(b)(ii) incorrect
- **- 1 pts** Q3(b)(iii) incorrect
- **- 1 pts** Q3(b)(iv) incorrect
- **- 1 pts** Q3(c)(i) incorrect
- **- 1 pts** Q3(c)(ii) incorrect
- **- 1 pts** Q3(c)(iii) incorrect
- ✓ **- 1 pts Q3(c)(iv) incorrect**

- 1 Point adjustment

-1.0: Some transitions are wrong in Q3(a)

QUESTION 4

4 Question 4 4 / 8

- **- 0 pts** Correct
- **- 3 pts** 4(a) incorrect
- ✓ **- 2 pts 4(b) incorrect**
- **- 1 pts** 4(c) incorrect
- ✓ **- 1 pts 4(d)(i) incorrect**
- ✓ **- 1 pts 4(d)(ii) incorrect**

What about the following LTL formula for P? ((A ∨ B) U ([ ] B)) ∨ [ ] A

QUESTION 5

5 Question 5 12 / 12

- ✓ **- 0 pts Correct**
- **- 1 pts** Q5(a)(i) incorrect
- **- 1 pts** Q5(a)(ii) incorrect
- **- 1 pts** Q5(a)(iii) incorrect
- **- 1 pts** Q5(a)(iv) incorrect
- **- 1 pts** Q5(a)(v) incorrect
- **- 1 pts** Q5(b)(i) incorrect
- **- 1 pts** Q5(b)(ii)-1 incorrect
- **- 1 pts** Q5(b)(ii)-2 incorrect
- **- 1 pts** Q5(b)(ii)-3 incorrect
- **- 2 pts** Q5(b)(iii)-1 incorrect
- **- 1 pts** Q5(b)(iii)-2 incorrect

QUESTION 6

6 Question 6 7.5 / 8

- **- 0 pts** Correct
- **- 3 pts** Q6(a) incorrect
- **- 5 pts** Q6(b) incorrect

- 0.5 Point adjustment

-0.5: Two self-loops are missing in the GNBA.

Name: Sahil Dhull

Roll No: 160607 (e.g. 170001) Dept.: CSE (e.g. CSE)

Indian Institute of Technology Kanpur
CS652: Computer-Aided Verification
Mid-Semester Examination
Date: September 20, 2019
Duration: 2 hours

Instructions: *Total:* **60 marks**

1. This question paper contains a total of 20 pages (20 sides of paper). Please verify.
2. Write your name, roll number, department on **every side of every sheet** of this booklet.
3. Write final answers **neatly with a pen** in the given boxes.

Problem 1. (2+2+2+2+2 = 10 points)
Determine whether the following statements are `true` or `false`. Provide a brief justification in support of your choice.

(a) If formal verification of a system is successful, the system is bug-free.

(b) Let the transition system TS' be an abstraction of the transition system TS. The number of traces in TS is greater than or equal to the number of traces in TS'.

(c) For a given transition system TS and an LT property P, $TS \models_{\mathcal{F}_{strong}} P \Rightarrow TS \models_{\mathcal{F}_{uncond}} P$, where $\mathcal{F}_{uncond}$ and $\mathcal{F}_{strong}$ denote *unconditional* and *strong* fairness conditions respectively.

(d) $\Box\psi \equiv \psi \vee \bigcirc\Box\psi$

(e) $\Box(a \vee b) \equiv \Box a \vee \Box b$.

a) False. There maybe bug in specification or the model for the system itself, in which case formal verification maybe successful, but system can have a bug.

b) True. The number of ~~states~~ traces in an abstraction is always less than ~~or~~ equal to that in the original Transition system.

c) True. Because any trace that is unconditionally fair is always strongly fair.
$\Rightarrow$ Uncond fair traces $\subseteq$ strong fair traces $\subseteq P$.

d) False
Consider a trace ψ. This is satisfied by RHS but not by LHS.

Name: Sahil Dhull

Roll No: e.g. 170001 160607

Dept.: e.g. CSE CSE

Indian Institute of Technology Kanpur
CS652: Computer-Aided Verification
Mid-Semester Examination
Date: September 20, 2019
Duration: 2 hours

e) False

$\Box(a \vee b)$ means at each step either a or b will be true.
whereas $\Box a \vee \Box b$ means either always a will be true,
or always b will be true.
Consider a trace $(ab)^\omega$.
LHS satisfies this, but RHS doesn't.

Name:

Roll No:
e.g. 170001

Dept.:
e.g. CSE

Name: Sahil Dhull

Roll No: 160607 (e.g. 170001) Dept.: CSE (e.g. CSE)

Indian Institute of Technology Kanpur
CS652: Computer-Aided Verification
Mid-Semester Examination
Date: September 20, 2019
Duration: 2 hours

Problem 2. (2+2+2+2+2 =10 points)

Consider the two simplified processes P_i, $i = 1, 2$. P_i is given as follows:

loop forever
.
. /* non-critical actions */
.
`request` for lock and wait
$y > 0 : y := y - 1$; `enter` critical section
$y := y + 1$; `release` lock
.
. /* non-critical actions */
.
end loop

(a) Draw the program graphs PG_1 and PG_2 for processes P_1 and process P_2.

(b) Draw the program graph $PG_1 \mid\mid\mid PG_2$ capturing the interleaving of the two processes.

(c) Provide the transition system $TS(PG_1 \mid\mid\mid PG_2)$.

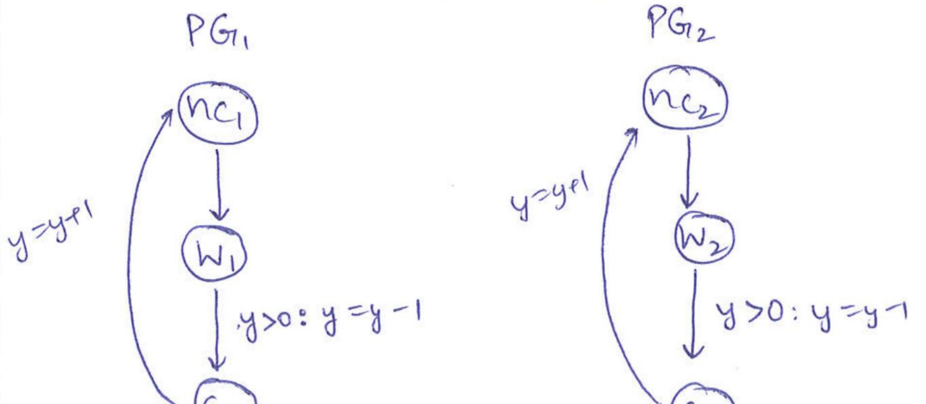
(d) Total how many states are there in the system? Assuming that both processes start from the non-critical section with the value of y to be 1 initially, how many reachable state are there for the composed system?

(e) Let the action performed by the second process while entering the critical section is $enter_2$.

(i) Provide an execution fragment in the transition system which is strongly fair with respect to the set of actions $A = \{enter_2\}$, but is not unconditionally fair with respect to the action.

(ii) Provide an execution fragment in the transition system which is weakly fair with respect to the set of actions $A = \{enter_2\}$, but is not strongly fair with respect to the action.

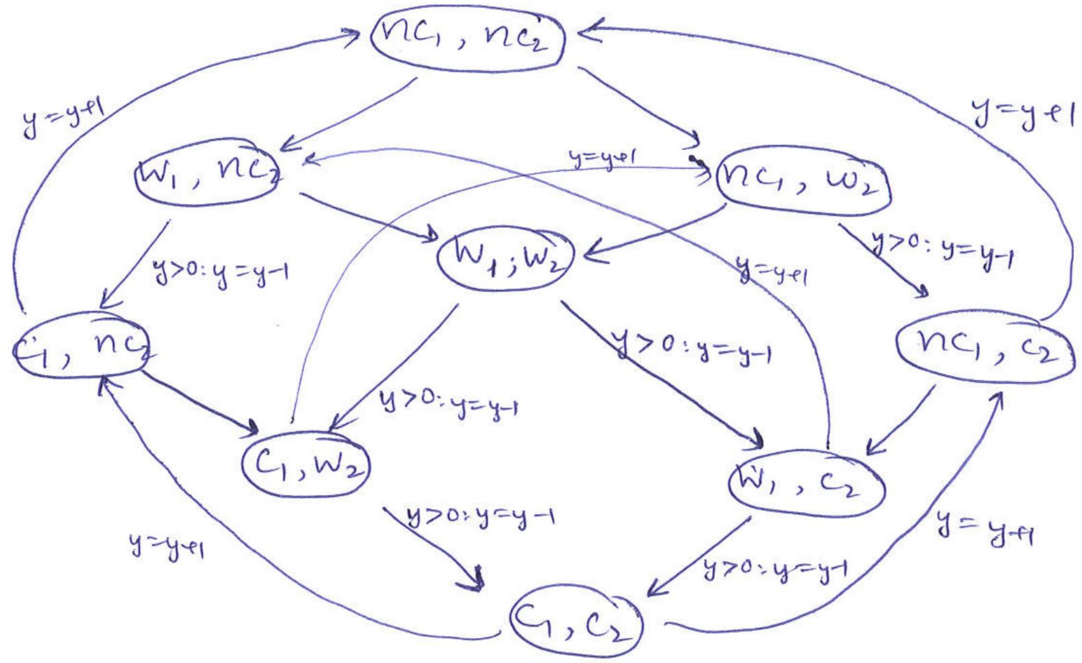
a) let non-critical sections be denoted by nc_1 & nc_2.
& critical by c_1 & c_2.



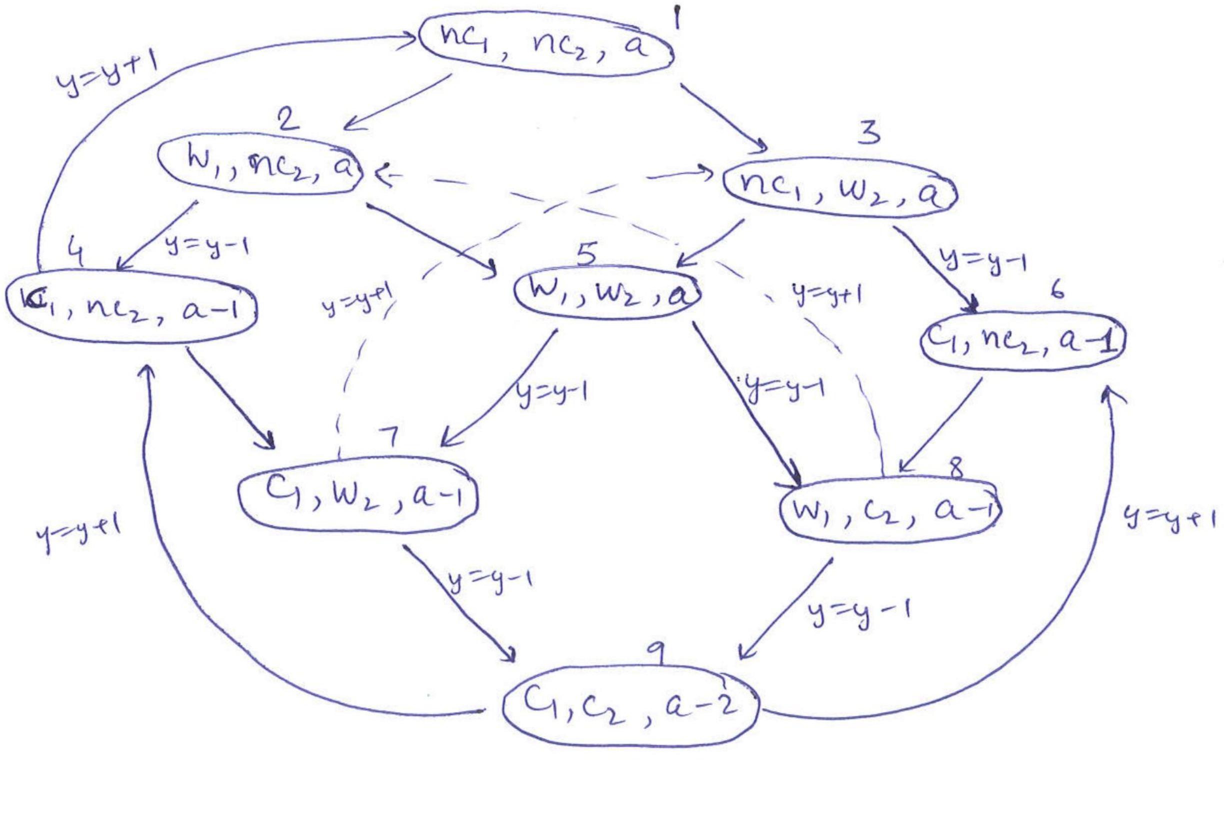
Indian Institute of Technology Kanpur
CS652: Computer-Aided Verification
Mid-Semester Examination
Date: September 20, 2019
Duration: 2 hours

Name: Sahil Dhull
Roll No: 160607 (e.g. 170001)
Dept.: CSE (e.g. CSE)

(b)



(c) Considering initial value of y to be $a \in \mathbb{Z}$



Name: Sahil Dhull

Roll No: 160607 (e.g. 170001) Dept.: CSE (e.g. CSE)

Indian Institute of Technology Kanpur
CS652: Computer-Aided Verification
Mid-Semester Examination
Date: September 20, 2019
Duration: 2 hours

d) Total Number of states = 9
If $y=1$, there 8 reachable states.
the state $\langle c_1, c_2, a-2 \rangle$ will not be reachable

e)
(i) Let α stands for all transitions which do not have any action.
The execution fragment which is strongly fair but not unconditional fair is

$(\langle nc_1, nc_2, a\rangle, (\alpha), \langle w_1, nc_2, a\rangle, (y=y-1), \langle c_1, nc_2, a-1\rangle, (y=y+1))^\omega$

i.e. the cycle in which 1st process alternates ~~and~~ between critical and non-critical states.

(ii) The execution fragment which is weakly fair but not strongly fair is

$\langle nc_1, nc_2, a\rangle, \alpha, (\langle nc_1, w_2, a\rangle, (\alpha), \langle w_1, w_2, a\rangle, \text{enter1} (y=y-1),$
$\langle c_1, w_2, a-1\rangle, (y=y+1))^\omega$

or using states marked 1-9,

$1, \alpha, (3, \alpha, 5, \text{enter} 1, 7, y=y+1)^\omega$.

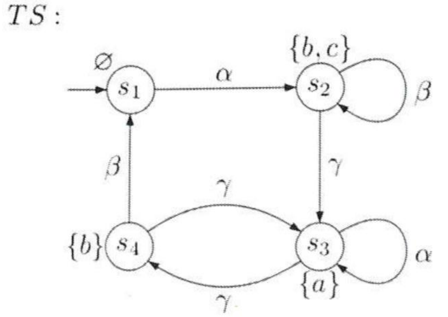
Indian Institute of Technology Kanpur
CS652: Computer-Aided Verification
Mid-Semester Examination
Date: September 20, 2019
Duration: 2 hours

Name: Sahil Dhull

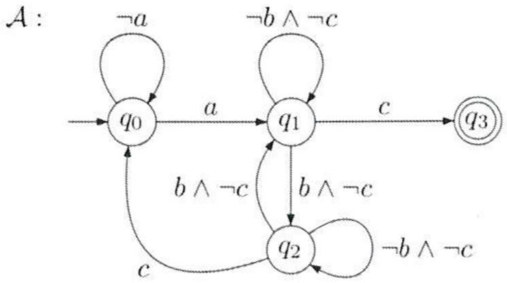
Roll No: 160607 (e.g. 170001) Dept.: CSE (e.g. CSE)

Problem 3. $(4+4+4=12$ points)

(a) Let $AP=\{a,b,c\}$. Consider the following transition system TS and the following NFA $\mathcal{A}$. Construct the product $TS \otimes \mathcal{A}$.



(a) TS



(b) $\mathcal{A}$

Figure 1: Transition System and NFA

(b) What is an LT property? Define Invariants, Safety and Liveness properties as LT properties.

(c) Provide an example of the following types of LT properties. The property has to be defined in the context of a system. The formal definition of the systems in terms of transition systems need NOT be provided.

(i) Provide an example of an invariant.
(ii) Provide an example of a safety property which is not an invariant.
(iii) Provide an example of a liveness property.
(iv) Provide an example of an LT property which is neither a safety property nor a liveness property.

(a) – on next page

(b) LT property or linear Time property is ~~set of traces of any~~ property over 2^{AP} which can be satisfied by set of traces of a transition system.

Invariant:

Defined over $\phi \subseteq 2^{AP}$,

$$P_{inv} = \{ A_1, A_2 A_3 --- \mid \forall i, A_i \models \phi \}$$

Safety property (P_{safe})

Consider a trace $\sigma \in (2^{AP})^\omega \setminus P_{safe}$

then there exists a finite prefix of σ, $\hat{\sigma}$, whose all infinite extensions are in this set.

ie $\exists \hat{\sigma} = \text{Prefix}(\sigma)$, s.t. $\hat{\sigma}.\sigma' \in (2^{AP})^\omega \setminus P_{safe}$. $\forall \sigma'$

Indian Institute of Technology Kanpur
CS652: Computer-Aided Verification
Mid-Semester Examination
Date: September 20, 2019
Duration: 2 hours

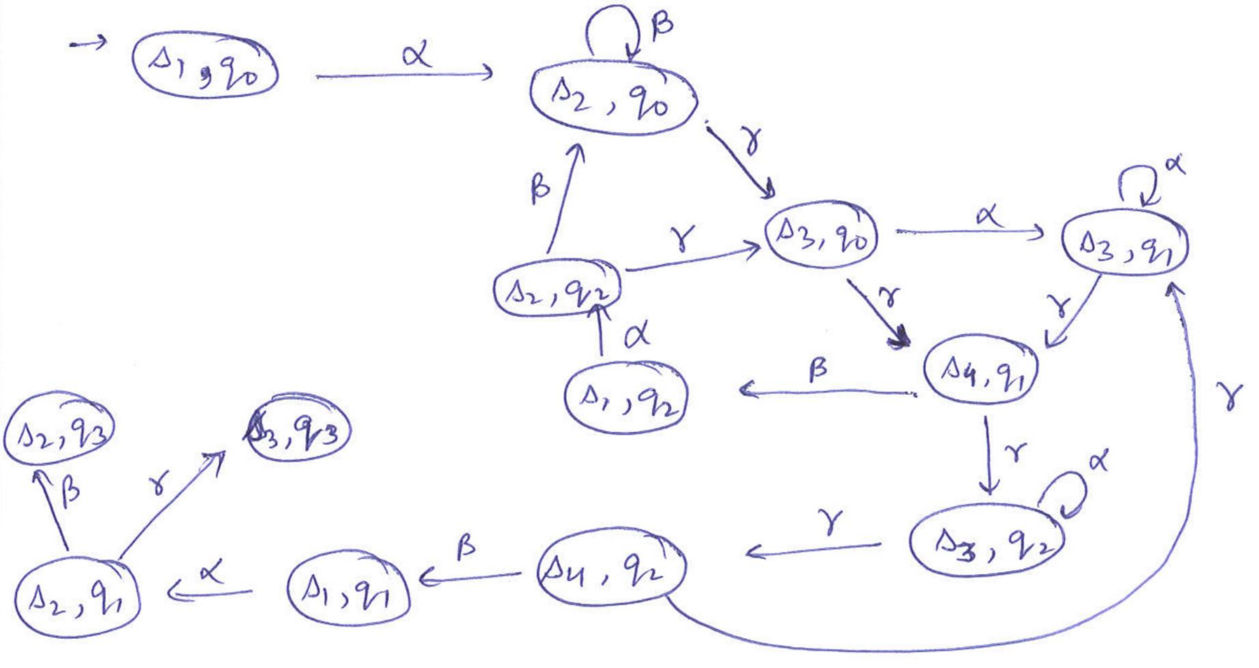
Name: Sahil Dhull

Roll No: 160607 (e.g. 170001)

Dept.: CSE (e.g. CSE)

Liveness property (P_{live})
Given any finite trace, there exists its infinite extension which lies in P_{live} ie
$\forall \hat{\sigma} \in (2^{AP})^*$, $\exists \sigma'$ s.t. $\hat{\sigma}.\sigma' \in P_{live}$.

(a) $I_0 = \{\langle s_1, q_0 \rangle\}$. , $L(\langle s_i, q_i \rangle) = \{q_i\}$
so, label are not mentioned in the Transition system.



(c) Consider the system to be traffic light where red, yellow and green denote the current color.

(i) $\square(\neg(\text{red} \wedge \text{green}))$
ie Red and green can't be on at the same time always. (at any time)

Name: Sahil Dhull

Roll No: 160607 (e.g. 170001) Dept.: CSE (e.g. CSE)

Indian Institute of Technology Kanpur
CS652: Computer-Aided Verification
Mid-Semester Examination
Date: September 20, 2019
Duration: 2 hours

(ii) "Red is always preceeded by yellow light."
This is safety property, but it is not invariant

(iii) "Always eventually green" is a liveness property

(iv) The property $P = \phi$ (empty) is neither a liveness nor a safety property.

Name: Sahil Dhull

Roll No: 160607
e.g. 170001

Dept.: CSE
e.g. CSE

Indian Institute of Technology Kanpur
CS652: Computer-Aided Verification
Mid-Semester Examination
Date: September 20, 2019
Duration: 2 hours

Problem 4. (3+ 2+ 1 + 2 = 8 points)

(a) Consider the GNBA shown in Figure 2. The acceptance sets of the GNBA are $F_1 = \{q_1\}$ and $F_2 = \{q_2\}$. Construct an equivalent NBA.

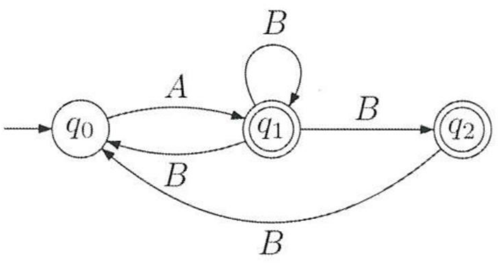


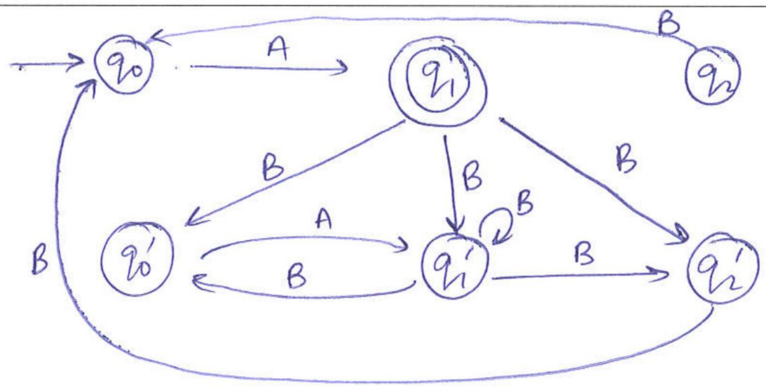
Figure 2: A transition system

(b) Provide two automata that when interpreted as NBAs accept the same languages, but when interpreted as NFA accept two different languages.

(c) Provide an LT property for which there does not exist a DBA that accepts the LT property. Provide an NBA that accepts the LT property.

(d) Provide an LT property P that cannot be represented as an LTL formula. Provide an NBA $\mathcal{A}$ such that $P = \mathcal{L}_\omega(\mathcal{A})$.

(a)



Equivalent NBA.

$F = \{q_1\}$.
$Q_0 = \{q_0\}$

(b) Consider the following automata

as NFA, both accept ~~$a a^\omega$~~ $a a^*$

But as NBA, 1st one accepts nothing whereas 2nd one accepts a^ω.

Name: Sahil Dhull

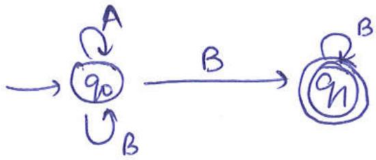
Roll No: 160607
e.g. 170001

Dept.: CSE
e.g. CSE

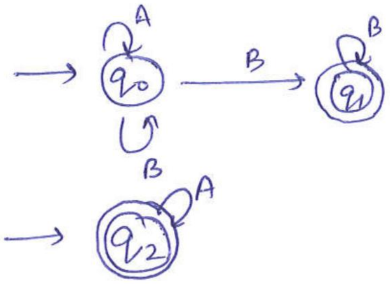
Indian Institute of Technology Kanpur
CS652: Computer-Aided Verification
Mid-Semester Examination
Date: September 20, 2019
Duration: 2 hours

(c) Property $\longrightarrow$ $(A+B)^* B^\omega$

NBA :



(d) $P = (A+B)^* B^\omega + A^\omega$



NBA A ~~for~~ with
$P = L_\omega(A)$.

Name:

Roll No:
e.g. 170001

Dept.:
e.g. CSE

Name: Sahil Dhull

Roll No: 160607
e.g. 170001

Dept.: CSE
e.g. CSE

Indian Institute of Technology Kanpur
CS652: Computer-Aided Verification
Mid-Semester Examination
Date: September 20, 2019
Duration: 2 hours

Problem 5. ((1+1+1+1+1) + (1+3+3) = 12 points)

(a) Consider the transition system in Figure 3.

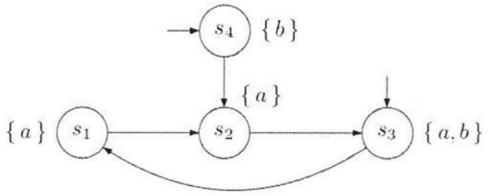


Figure 3: A transition system

Determine whether the transition system satisfies the following LTL properties: (i) $b \wedge \bigcirc \bigcirc b$, (ii) $\Diamond\Box a$, (iii) $\Box\Diamond b$, (iv) $\Box(b\, \mathcal{U}\, a)$, (v) $\Diamond(a\, \mathcal{U}\, b)$

(b) Consider a pedestrian traffic light that switches between red and green. When the traffic light is in the red mode, it may automatically switch off to save energy and may get back to the red mode again after some time.

(i) Provide a transition system model T for the traffic light.

(ii) We would like to prove that the transition system satisfies the following property φ : "infinitely often green". What is the complement of this property? Show an NBA $\mathcal{A}$ for the complement property. What is the persistent property P corresponding to the NBA $\mathcal{A}$?

(iii) Construct a product transition system from the transition system T and the NBA A. Using the persistent property P and the product transition system, show that T does not satisfy φ. Provide a counterexample.

(a)
(i) ~~Satisfies $\phi = b \wedge \bigcirc\bigcirc b$~~ Doesn't satisfy $\phi = b \wedge \bigcirc\bigcirc b$

(ii) Satisfies $\phi = \Diamond\Box a$.

(iii) satisfies $\phi = \Box\Diamond b$

(iv) Satisfies $\Box(b\, \mathcal{U}\, a)$

(v) Satisfies $\Diamond(a\, \mathcal{U}\, b)$

(b) ~~Let the start state of T~~

(i) $TS = (S, Act, \rightarrow, AP, L, I)$

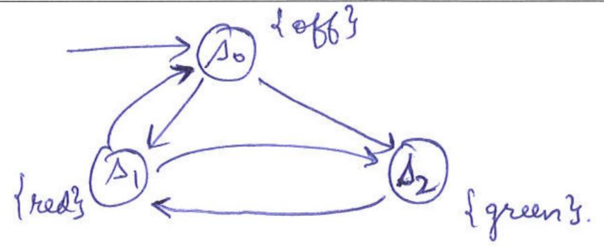
$S = \{s_0, s_1, s_2\}$, $AP = \{red, green, off\}$

$I = \{s_0\}$ let the start state be the off state ie q_0.

Name: Sahil Dhull

Roll No: 160607 (e.g. 170001) Dept.: CSE (e.g. CSE)

Indian Institute of Technology Kanpur
CS652: Computer-Aided Verification
Mid-Semester Examination
Date: September 20, 2019
Duration: 2 hours



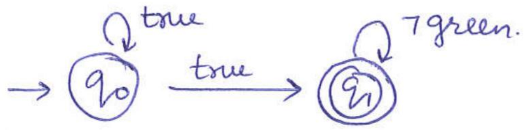
Transition system

(ii) ~~P ≡ □◇ green.~~ $\varphi = \Box\Diamond$ green.

~~$\overline{\Phi}$~~ $\overline{\varphi} = \Diamond\Box(\neg \text{green})$

$[\because\ \overline{\varphi} = \neg\Box\Diamond g = \neg(\neg\Diamond\neg\Diamond g) = \Diamond(\neg\Diamond g) = \Diamond\Box(\neg g)]$

NBA:

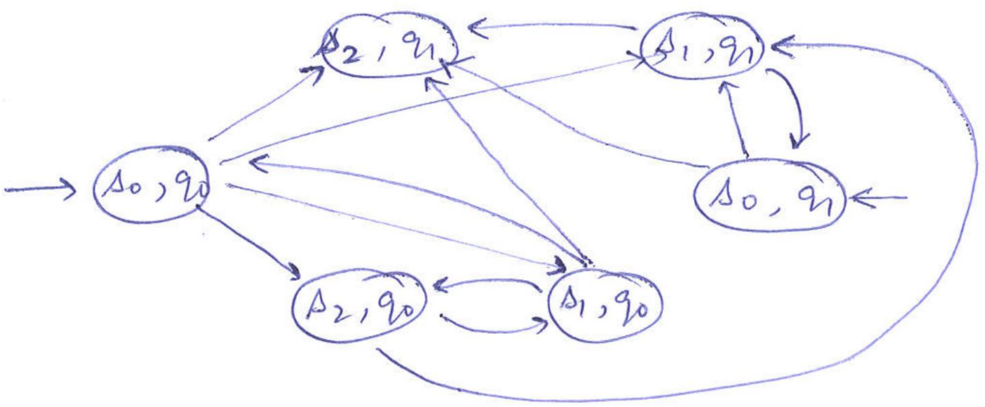


~~Persistent property $\Phi = \neg$ green.~~, $P_{pers} = \Diamond\Box(\neg \text{green})$
~~$(\because P_{pers} = \Diamond\Box\Phi.)$~~

~~(iii)~~ Persistent property here is defined in terms of final states of NBA.

so, $P_{pers} = \Diamond\Box(\neg q_1)$, $\phi = \neg q_1$

(iii) Product Automata



To check, if φ is satisfied or not, we check for any

Name: Sahil Dhull

Roll No: 160607 (e.g. 170001) Dept.: CSE (e.g. CSE)

reachable state from where a cycle containing $\neg\phi$ is formed.

In this case, the cycle $(s_0, q_1) \rightleftarrows (s_1, q_1)$ contains $\neg\phi$ states and is reachable.

Hence T does not satisfy φ.

Counter Example of a Trace :

Off Red Off Red ......

Indian Institute of Technology Kanpur
CS652: Computer-Aided Verification
Mid-Semester Examination
Date: September 20, 2019
Duration: 2 hours

Name: Sahil Dhull

Roll No: 160607 (e.g. 170001)   Dept.: CSE (e.g. CSE)

Problem 6. (3 + 5 = 8 points)

(a) Given a finite transition system T and LTL formula φ, provide an outline of the algorithm to verify whether T satisfies φ.

You do NOT need to provide the details of the graph search algorithm.

(b) Construct a GNBA for the LTL formula $\Box\neg a$, where a is an atomic proposition. Show the closure, the elementary sets, and the components of the automaton clearly.

(b) $\phi = \Box \neg a$

$= \neg \Diamond \neg(\neg a) = \neg \Diamond a = \neg(\text{true} \, \mathcal{U} \, a)$

Closure $(\phi) = \{\text{true}, \text{false}, a, \neg a, \phi, \neg\phi\}$.

$B_1 = \{\text{true}, a, \neg\phi\}$.

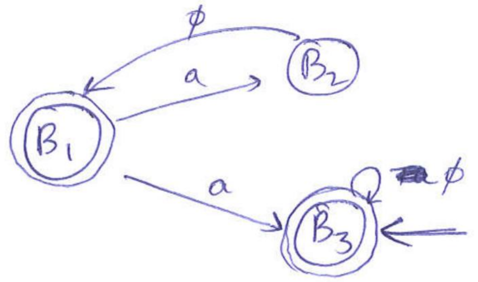
$B_2 = \{\text{true}, \neg a, \neg\phi\}$

$B_3 = \{\text{true}, \neg a, \phi\}$

$Q_0 = \{B_3\}$

$F_{\text{true} \, \mathcal{U} a} = \{B_1, B_3\}$

So, $F = \{\{B_1, B_3\}\}$.



(a) Given Transition system T, and LTL formula ϕ.

We want to know if T satisfies ϕ or not.

ie $T \overset{?}{\models} \phi$

· We consider lets say $T \not\models \phi$

then ~~$\exists\sigma$~~ Traces $(T) \not\subseteq$ Words (ϕ)

$\Rightarrow$ Traces $(T) \cap$ Words $(\overline{\phi}) \neq \phi$

We construct NBA "A" for Words $(\overline{\phi})$

such that $\mathcal{L}(A) =$ Words $(\overline{\phi})$,

Name: Sahil Dhull

Roll No: 160607 (e.g. 170001)   Dept.: CSE (e.g. CSE)

Indian Institute of Technology Kanpur
CS652: Computer-Aided Verification
Mid-Semester Examination
Date: September 20, 2019
Duration: 2 hours

Then we take the product of T and A.

ie $T' = T \otimes A$.

$T' = (S \times Q, Act, \rightarrow, AP, L)$

~~the~~ where all terms are defined as in the case of product of TS and NFA.

$L(\langle s, q \rangle) = \{q\}$.

We define Persistent property as $P_{pers} = \Diamond \Box (\neg F)$

where $\neg F = \neg f_1 \wedge \neg f_2 \wedge \cdots$

where $f_1, f_2, \cdots \in F$ (final state of NBA A).

~~Then we run algorithm~~

Let $\Phi = \neg F$.

So, $P_{pers} = \Diamond \Box \Phi$

We run 2 DFS, where in outer DFS finds the state that satisfies $\neg \Phi$ and inner DFS checks if it is contained in a cycle or not.

If a cycle contains $\neg \Phi$ state, $T \not\models \Phi$

Else $T \models \Phi$.

Name:

Roll No:
e.g. 170001

Dept.:
e.g. CSE

Name:

Roll No:
e.g. 170001

Dept.:
e.g. CSE

Indian Institute of Technology Kanpur
CS652: Computer-Aided Verification
Mid-Semester Examination
Date: September 20, 2019
Duration: 2 hours

BLANK SPACE: Any answers written here will be left ungraded.
No exceptions.
You may use this space for rough work.

BLANK SPACE: Any answers written here will be left ungraded.
No exceptions.
You may use this space for rough work.

Name:

Roll No: e.g. 170001 Dept.: e.g. CSE

Indian Institute of Technology Kanpur
CS652: Computer-Aided Verification
Mid-Semester Examination
Date: September 20, 2019
Duration: 2 hours