No calculator allowed in this examination

UNIVERSITY OF BIRMINGHAM

School of Computer Science

LH Computer-Aided Verification

Main Examinations January 2023

Time allowed: 2 hours

[Answer all questions]

Note

Answer ALL questions. Each question will be marked out of 20. The paper will be marked out of 60, which will be rescaled to a mark out of 100.

Question 1 Reactive Modelling

Consider the following two reactive modules. Module *Machine* describes a coffee machine with two operating states R and M, which respectively stand for "ready" and "making", while module *Controller* keeps track of external user requests.

module *Machine*
  external $n : \mathbb{N}$
  interface $state : \{R, M\}$
  atom *A1* **controls** *state* **awaits** n
  init
    $[\!]\ true \to state' := R$
  update
    $[\!]\ state = R \wedge n' > 0 \to state' := M$
    $[\!]\ state = M \to state' := R$
    $[\!]\ n' = 0 \to state' := R$

module *Controller*
  external $request : \mathbb{E}; state : \{R, M\}$
  interface $n : \mathbb{N}$
  atom *A2* **controls** n **awaits** *request*
    reads n, *request*
  init
    $[\!]\ true \to n' := 0$
  update
    $[\!]\ ?request \wedge state = R \to n' := n + 1$
    $[\!]\ ?request \wedge state = M \to n' := n$
    $[\!]\ \neg ?request \wedge state = M \to n' := n - 1$
    $[\!]\ \neg ?request \wedge state = R \to n' := n$

Note: Recall that uncontrolled variables are inherently non-deterministic, and variables type $\mathbb{E}$ are Boolean variables that represent events. An event x occurs when its value changes, that is, proposition "$?x$" denotes proposition "$x' \neq x$".

(a) Give a trajectory of the parallel composition *Machine* $\|$ *Controller* that produces the sequence of values shown below. **[5 marks]**

Round	0	1	2	3	4	5	6	7	8
	s_0	s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8
state									
n	0	0	1	1	2	1	1	0	0
request									

(b) Express each of the properties below as an LTL or a CTL model checking problem; if neither LTL or CTL are appropriate, then use CTL*. For each property, state the logic you are using and provide an appropriate formula in that logic. Specify whether your formula represents the given property positively (Pos) or whether it represents its negation (Neg). Write the formulae in positive normal form, i.e., without using negation $\neg$ except on atomic propositions.

Note: This question uses the variables of the model above (and the respective type) and atomic propositions should be propositions over these variables. For instance, "$n > 0$" or "$request = 0$" are valid atomic propositions. Note that it is not needed to understand the model to specify these model checking problems.

(i) There exists an initialised trajectory $s_0 s_1 s_2 \ldots$ such that

  i. $s_i(n) = 50$ for some $i \geq 0$, and

  ii. $s_i(n) > 0$ for all $i \geq 1$.

(ii) Every reachable state admits a transition to $state = R$. Formally, for every initialised trajectory $s_0 s_1 s_2 \ldots$, every state s_i for $i \geq 0$ admits at least one transition $s_i \to t$ to a state t such that $t(state) = R$.

(iii) Event "request" occurs infinitely often on every trajectory. Formally, for every initialised trajectory $s_0 s_1 s_2 \ldots$, there exist infinitely many states s_i with $i \geq 0$ such that $s_i(request) \neq s_{i+1}(request)$.

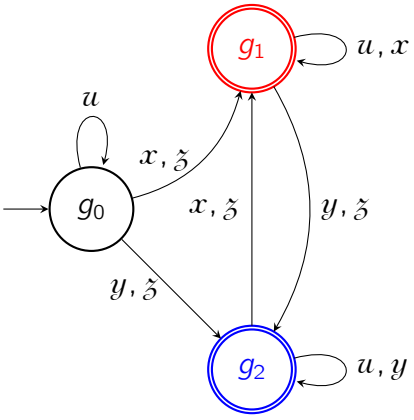
	Logic	Formula	Pos/Neg
(i)			
(ii)			
(iii)			

[9 marks]

(c) Is the model *Machine* $\|$ *Controller* amenable to bounded model checking using SAT, when a finite bound k is given? Briefly elaborate on your answer. If the answer is yes, give a sufficiently large number of propositional variables to encode the entire unrolling of the transition relation. If the answer is no, argue on the impossibility of obtaining such encoding. **[6 marks]**

Question 2 Linear Temporal Logic

Let $\mathsf{Ap} = \{a, b\}$ to be the set of atomic propositions in this question. We wil use the shorthands $u = \varnothing$, $x = \{a\}$, $y = \{b\}$ and $z = \{a, b\}$ for the letters of $\Sigma = 2^{\mathsf{Ap}}$. Consider the generalized non-deterministic Büchi automaton $\mathcal{G} = (G, G_0, \Sigma, \delta, \mathcal{F})$ with set of states $G = \{g_0, g_1, g_2\}$, set of initial states $G_0 = \{g_0\}$, alphabet $\Sigma = \{u, x, y, z\}$, set of acceptance sets $\mathcal{F} = \{F_1, F_2\}$ with $F_1 = \{g_1\}$ and $F_2 = \{g_2\}$, and the transition function δ given by the following diagram



(a) Are the following words accepted by $\mathcal{G}$? Justify your answer. **[6 marks]**

(i) $w_1 = x^\omega = xxxxx\ldots$

(ii) $w_2 = (xy)^\omega = xyxyx\ldots$

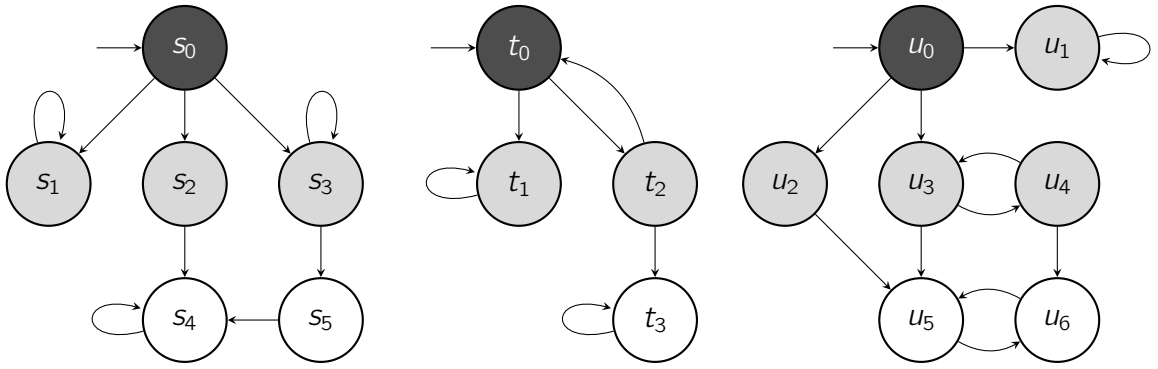
(iii) $w_3 = (uyz)^\omega = uyzuy\ldots$

(b) Follow the *degeneralization procedure* to give an equivalent non-deterministic Büchi automaton $\mathcal{A}$ with only one acceptance set. **[8 marks]**

(c) What is $\mathcal{L}_\omega(\mathcal{G})$ the language of infinite words reconized by $\mathcal{G}$? Give a LTL formula ψ over Ap such that $\mathcal{L}_\psi = \mathcal{L}_\omega(\mathcal{G})$. **[6 marks]**

Question 3 Computational Tree Logic

Consider the three Kripke models $\mathcal{M}_1$, $\mathcal{M}_2$ and $\mathcal{M}_3$ below. They are defined over the set of atomic propositions $\mathsf{Ap} = \{a, b, c\}$ such that the labelling of black states, e.g. s_0, is $L(\mathit{black}) = \{a\}$, the labelling of grey states, e.g. s_1, is $L(\mathit{grey}) = \{b\}$, and the labelling of white states, e.g. s_4, is $L(\mathit{white}) = \{c\}$ accross all three models.



(a) Consider the CTL formula $\Phi = \forall\bigcirc(\exists(b\,\mathsf{U}\,c) \vee \forall\Diamond b)$. We will use the fixpoint model checking algorithm to determine whether $\mathcal{M}_1 \models \Phi$. **[8 marks]**

(i) Compute Ψ the *Existential Normal Form* of Φ.

(ii) For each *state subformula* of Ψ, give the set of states in $\mathcal{M}_1$ that satisfy it.

(iii) In conclusion, does $\mathcal{M}_1 \models \Phi$? Explain your answer.

(b) We suppose that each state in $\mathcal{M}_2$ is encoded as the binary representation of its index using 2 Boolean variables x_0 and x_1 as follows: **[6 marks]**

	x_0	x_1
t_0	0	0
t_1	0	1
t_2	1	0
t_3	1	1

(i) Build a BDD representing the set of initial states of $\mathcal{M}_2$.

(ii) Build a BDD representing the set of states accepting b in $\mathcal{M}_2$.

(iii) Explain how you would check algorithmically whether $\mathcal{M}_2 \models b$ based on the BDDs constructed in (i) and (ii).

(c) For each pair of models, say whether they are bisimilar and justify your answer.

Hint: If the two models are bisimilar, give a bisimulation for them; if they are not, give a CTL formula that is satisfied in one and not in the other. **[6 marks]**

End of Paper

Do not complete the attendance slip, fill in the front of the answer book or turn over the question paper until you are told to do so

Important Reminders

- Coats/outwear should be placed in the designated area.
- Unauthorised materials (e.g. notes or Tippex) must be placed in the designated area.
- Check that you do not have any unauthorised materials with you (e.g. in your pockets, pencil case).
- Mobile phones and smart watches **must** be switched off and placed in the designated area or under your desk. They must not be left on your person or in your pockets.
- You are not permitted to use a mobile phone as a clock. If you have difficulty seeing a clock, please alert an Invigilator.
- You are not permitted to have writing on your hand, arm or other body part.
- Check that you do not have writing on your hand, arm or other body part – if you do, you must inform an Invigilator immediately
- Alert an Invigilator immediately if you find any unauthorised item upon you during the examination.

Any students found with non-permitted items upon their person during the examination, or who fail to comply with Examination rules may be subject to Student Conduct procedures.