Faculty of Computer Science
Free University of Bozen-Bolzano
Alessandro Artale

Formal Methods Exam – 22.June.2010

STUDENT NAME:

STUDENT NUMBER:

STUDENT SIGNATURE:

This exam will constitute the 80% of the overall course assessment.

1 Proving Properties in LTL and CTL [8 Points]

Formally prove the following properties for LTL and CTL formulas.

- **LTL equivalence.**
  Suppose we change the semantic of the 'Until' operator in the following way:
  $$\begin{aligned}\langle \mathcal{M}, i\rangle \models \varphi \mathcal{U} \psi \textbf{ iff } & \text{ there exists } j.\ (j > i) \wedge \langle \mathcal{M}, j\rangle \models \psi \wedge \\ & \text{for all } k.\ (i < k < j) \rightarrow \langle \mathcal{M}, k\rangle \models \varphi\end{aligned}$$
  Prove the following equivalence: $\bigcirc \varphi \equiv \bot \mathcal{U} \varphi$

- **CTL satisfiability.**
  Prove that the following CTL formula is not satisfiable: $\boxed{\scriptstyle P} \bigcirc \neg\varphi \wedge \Diamond_{P} \Box\varphi$.

Prove the following entailments:

- **LTL.** $\Box\varphi \vee \Box\psi \models \Box(\varphi \vee \psi)$.

- **CTL.** $\Diamond_{P} \Box(\varphi \wedge \psi) \models \Diamond_{P} \Box\varphi \wedge \Diamond_{P} \Box\psi$.

2 Expressing Properties in LTL [4 Points]

Express the following properties in LTL assumed to be true at all points in time:

1. If the event `Start` is true, then `Waiting` till `Receive` is true infinitely often.

2. If the event `Receive` is true, then `Processing` till `Sending` is true starting from the next step.

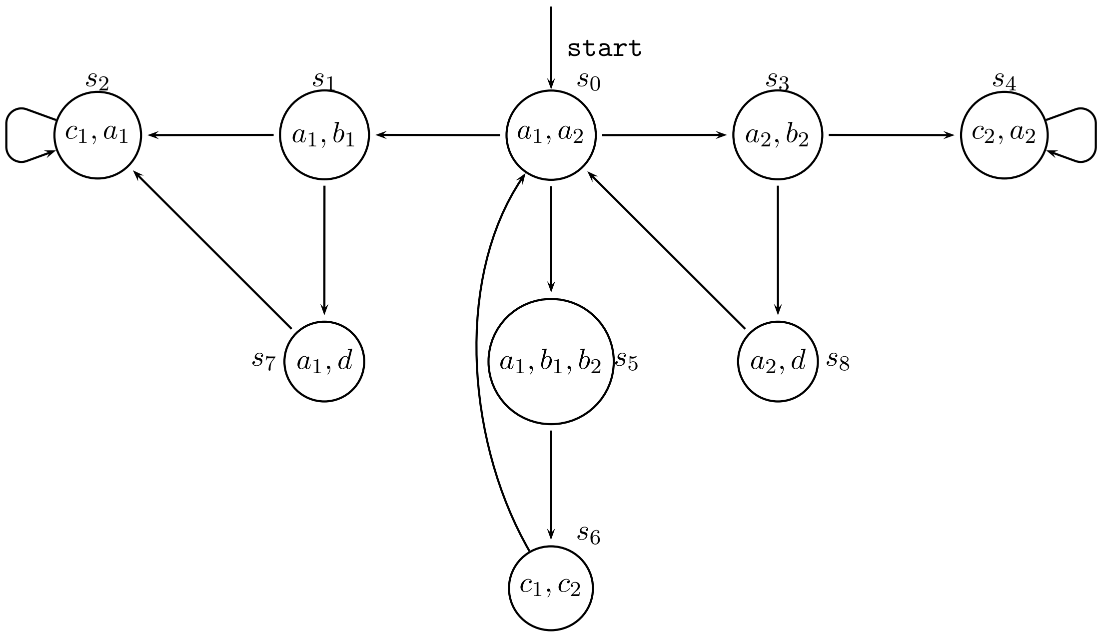
3. It is never the case that the event `Receive` happens at the same time when the event `Sending` is happening.

Finally, answer the following question:

- Discuss on the expressive power of LTL Vs. CTL.

3 Model Checking in LTL [6 Points]

You are given the following Kripke model $\mathcal{M}$:



- Extract from the above graphical representation of $\mathcal{M}$ its formal definition (limit the transitions and labelling to states s_0, s_5, s_6).

Furthermore, for each of the following **LTL** formulas φ:

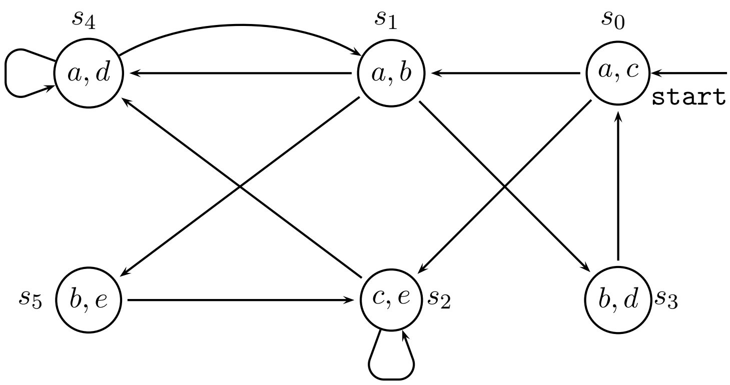
1. $\big((b_1 \wedge \neg b_2) \vee (a_1 \wedge a_2)\big) \rightarrow \bigcirc(a_1 \vee a_2) \wedge \bigcirc\bigcirc(d \vee c_1)$
2. $\Box\big(\bigcirc d \rightarrow \Box(a_1 \vee \neg b_2)\big)$
3. $\Box\Diamond c_1 \rightarrow \Box\Diamond(b_1 \wedge c_1)$
4. $(a_1 \vee a_2)\,\mathcal{U}\,(c_1 \vee c_2) \vee \Box(a_1 \vee a_2)$
5. $\Diamond((b_1 \wedge \bigcirc c_1) \rightarrow \Box\Diamond a_1)$

reply to the following question:

- Check whether $\mathcal{M} \models \varphi$, and in case the answer is negative exhibit a path that does not satisfy the formula.

4 Model Checking in CTL [8 Points]

You are given the following Kripke model $\mathcal{M}$:



For each of the following **CTL** formulas φ, rewrite them using only the CTL operators $\langle\mathrm{P}\rangle \bigcirc$, $\langle\mathrm{P}\rangle \Box$, $\langle\mathrm{P}\rangle \mathcal{U}$, and check whether $\mathcal{M} \models \varphi$ holds by using the labeling algorithm.

1. $\langle\mathrm{P}\rangle \Box(\neg d \vee \langle\mathrm{P}\rangle \bigcirc b)$
2. $[\mathrm{P}] \Box b \vee \langle\mathrm{P}\rangle (c \mathcal{U} e)$
3. $[\mathrm{P}] \bigcirc (c \wedge e)$
4. $\langle\mathrm{P}\rangle \Diamond(\neg c \wedge [\mathrm{P}] \Diamond a)$

5 Symbolic Model Checking [6 Points]

Given the Kripke model of the Exercise 4 do the following:

1. Write the characteristic function of the initial state, $\xi(s_0)$.
2. Construct the OBDD in canonical form for $\xi(s_0)$ by showing all the partial OBDD's needed to reach the final OBDD.
3. Explain how we can check that $\mathcal{M} \models \varphi$ holds with the symbolic model checking technique.