Prof. Dr. Andreas Podelski
Elisabeth Henkel
Dominik Klumpp

Hand in until February 7th, 2024
15:59 via ILIAS
Discussion: -

Tutorial for Cyber-Physical Systems - Discrete Models

Exercise Sheet 14

(Bonus Points Only)

Exercise 1*: Transition Systems, Program Graphs, Interleaving 8 Bonus Points

As discussed in the lecture, the transition systems $\mathcal{T}_{\mathcal{P}_1} \,|||\, \mathcal{T}_{\mathcal{P}_2}$ and $\mathcal{T}_{\mathcal{P}_1 ||| \mathcal{P}_2}$ for program graphs $\mathcal{P}_1$ and $\mathcal{P}_2$ may in general be different (and they often are). However, there exist program graphs $\mathcal{P}_1$ and $\mathcal{P}_2$ where the two transition systems are equal.

(*a*) Give an example of two such program graphs $\mathcal{P}_1$ and $\mathcal{P}_2$.

(*b*) Give the interleaving $\mathcal{P}_1 ||| \mathcal{P}_2$.

(*c*) Give the transition systems $\mathcal{T}_{\mathcal{P}_1}$ and $\mathcal{T}_{\mathcal{P}_2}$.

(*d*) Give the transition system $\mathcal{T}_{\mathcal{P}_1} \,|||\, \mathcal{T}_{\mathcal{P}_2}$ respectively $\mathcal{T}_{\mathcal{P}_1 ||| \mathcal{P}_2}$.

Exercise 2*: From LTL to NBA and Back 8 Bonus Points

The goal of this exercise is to improve your intuition regarding the connection of LTL and NBA.

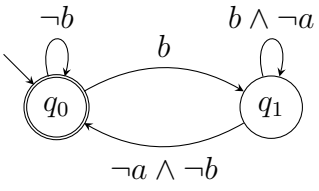
For each of the following LTL formulas provide an NBA that accepts exactly the traces that satisfy the formula.

(a) $\square(\neg a \vee \Diamond\, b)$

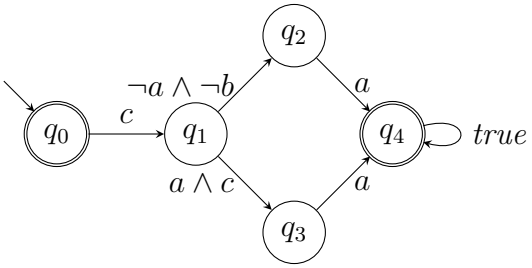
(b) $\square(a \rightarrow \Diamond\, \neg a) \vee \Diamond\, b$

For each of the following NBAs provide an LTL formula that satisfies exactly the traces accepted by the NBA.

(c)



(d)



Exercise 3*: LT Properties for a Program 7 Bonus Points

The goal of this task is to learn how to recognize safety properties in the context of a program (for atomic propositions that are defined for a given program).

Let the set AP of atomic propositions be given by $AP = \{x = 0, x > 1\}$.
Consider a nonterminating sequential program P that manipulates the variable x.
Formalize the following properties as LT properties, using set notation.

(a) false

(b) initially x is equal to 0

(c) initially x differs from 0

(d) intially x is equal to 0, but at some point x exceeds 1

(e) x exceeds 1 only finitely many times

(f) x exceeds 1 infinitely often

(g) true

Determine which of the properties are safety properties. Justify your answers.

Exercise 4*: Fair Equivalence 6 Bonus Points

The goal of this exercise is to practice simple proofs about LTL semantics, and to understand a key property that makes logical equivalence (modulo fairness) such a useful relation.

We call a relation $\sim$ between LTL formulas a *logical congruence*, if $\sim$ is an equivalence relation (it is reflexive, symmetric and transitive), and it holds for all LTL formulas $\varphi_1, \varphi_2, \psi_1, \psi_2$ that

(C1) If $\varphi_1 \sim \varphi_2$, then also $(\neg\varphi_1) \sim (\neg\varphi_2)$.

(C2) If $\varphi_1 \sim \varphi_2$ and $\psi_1 \sim \psi_2$, then also $(\varphi_1 \vee \psi_1) \sim (\varphi_2 \vee \psi_2)$.

(C3) If $\varphi_1 \sim \varphi_2$, then also $(\bigcirc \varphi_1) \sim (\bigcirc \varphi_2)$.

(C4) If $\varphi_1 \sim \varphi_2$ and $\psi_1 \sim \psi_2$, then also $(\varphi_1 \mathsf{U} \psi_1) \sim (\varphi_2 \mathsf{U} \psi_2)$.

Example: Logical equivalence ($\equiv$) between formulas is a logical congruence. This allows us to "swap out" any sub-formula ψ of a given formula φ with an equivalent sub-formula ψ', and be sure that the result is still equivalent to φ. E.g., if we know that $\bigcirc\Box a \equiv \Box\bigcirc a$, we can directly conclude that $\Diamond(b \mathsf{U} \bigcirc\Box a) \equiv \Diamond(b \mathsf{U} \Box\bigcirc a)$.

Let *fair* be any LTL fairness condition. In the lecture, we defined equivalence modulo the fairness condition *fair*, denoted $\equiv_{\mathit{fair}}$, and we discussed a proof showing that (C1) holds for $\equiv_{\mathit{fair}}$. In this exercise, we complete the proof that $\equiv_{\mathit{fair}}$ is a logical congruence. Prove the following statements:

(a) If $\varphi_1 \equiv_{\mathit{fair}} \varphi_2$ and $\psi_1 \equiv_{\mathit{fair}} \psi_2$, then also $(\varphi_1 \vee \psi_1) \equiv_{\mathit{fair}} (\varphi_2 \vee \psi_2)$.

(b) If $\varphi_1 \equiv_{\mathit{fair}} \varphi_2$, then also $(\bigcirc \varphi_1) \equiv_{\mathit{fair}} (\bigcirc \varphi_2)$.

(c) If $\varphi_1 \equiv_{\mathit{fair}} \varphi_2$ and $\psi_1 \equiv_{\mathit{fair}} \psi_2$, then also $(\varphi_1 \mathsf{U} \psi_1) \equiv_{\mathit{fair}} (\varphi_2 \mathsf{U} \psi_2)$.

Hint: You may use the fact that any suffix $A_i A_{i+1} \ldots$ of a fair trace $A_0 A_1 \ldots$ is also fair.