

Exercises Algorithms for Model Checking

1 CTL*

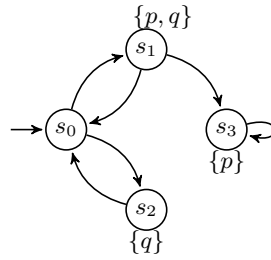


Figure 1:

1. For each of the CTL* formulae below, indicate whether it is (syntactically) a formula in LTL and/or CTL. Determine for each formula in which states of the Kripke Structure of Fig. 1 it holds.
 - (a) p ,
 - (b) $E [q R p]$,
 - (c) $E F G p$,
 - (d) $A G F p$,
 - (e) $A G E F p$,
 - (f) $A G F (p \wedge X q)$,
 - (g) $A G (\neg q \vee F p)$,
 - (h) $A ((G p) \vee (F q))$
2. For each pair of CTL* formulae below, if possible, give a Kripke Structure in which both are valid, a Kripke Structure in which both are not valid, and a Kripke Structure in which only one of them is valid.
 - (a) p and $A F p$
 - (b) $A F A G p$ and $A G A F p$
 - (c) $A F A X p$ and $A F X p$
 - (d) $A X E X p$ and $A X X p$
 - (e) $A X A X p$ and $A X X p$
 - (f) $A [p U q]$ and $A [\neg q R \neg p]$
3. Consider LTL, CTL and CTL*. State for each of the claims below whether they hold or not. Motivate your answer by providing counterexamples or a formal justification.

- (a) Every CTL* formula is equivalent to either an LTL formula or a CTL formula.
 - (b) The language LTL is more expressive than CTL.
 - (c) The language CTL is more expressive than LTL.
 - (d) On deterministic Kripke Structures (i.e., Kripke Structures with a single initial state in which each state has exactly one successor), LTL and CTL are equally expressive; that is, every LTL formula has an equivalent CTL formula and vice versa.
4. Express that along all paths, proposition p holds infinitely often and $\neg p$ holds infinitely often.
 5. Express that along all paths, proposition p holds infinitely often and $\neg p$ only holds finitely often.
 6. Prove using the semantics of CTL*, or disprove using a Kripke Structure, the following equivalences:
 - (a) $A [\phi \text{ U } \psi] \equiv \neg(E [\neg\psi \text{ U } \neg(\phi \vee \psi)] \vee E G \neg\psi)$
 - (b) $A G A F p \equiv A G F p$

2 Model Checking CTL and Fair CTL

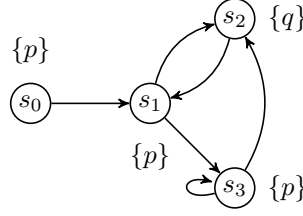


Figure 2:

1. For each of the CTL formulae below, draw a Kripke Structure in which the formula holds, a Kripke Structure in which it does not hold, but in which it does hold fairly with an appropriate fairness constraint. Also provide this fairness constraint.
 - (a) $\mathbf{A\,G\,A\,F\,(\neg p \vee q)}$
 - (b) $q \wedge \mathbf{A\,F\,q} \wedge \neg(\mathbf{E\, [\neg q\,R\,\neg p]})$
 - (c) $\neg \mathbf{A\,F\,p} \vee \mathbf{E\,G\,(\neg p \vee q)}$
 - (d) $(p \vee \mathbf{A\,F\,p}) \wedge \neg \mathbf{E\,G\,p}$
2. Determine for each of the following CTL formulae in which states of the Kripke Structure of Fig. 1 it holds using the labelling algorithm. Repeat the exercise using the symbolic model checking algorithm for CTL, using explicit set notation to represent sets of states, rather than BDDs.
 - (a) p ,
 - (b) $\mathbf{E\, [q\,R\,p]}$,
 - (c) $\mathbf{A\,G\,E\,F\,p}$,
 - (d) $\mathbf{A\,G\,p} \vee \mathbf{A\,F\,q}$
 - (e) $\mathbf{A\,F\,q}$
 - (f) $\mathbf{A\, [q\,R\,p]}$
3. Extend the Kripke Structure of Fig. 1 with the Fairness constraints $F = \{ \{s_1\}, \{s_2\} \}$. In which states do the formulae of exercise 2 *fairly* hold? Repeat the exercise using fairness constraint $F = \{ \{s_3\} \}$.
4. Answer Exercises 2 and 3 for the Kripke Structure in Fig. 2 instead of the Kripke Structure of Fig. 1.
5. Prove that $\mathbf{A\,F\,f} = \mu Z. f \cup \mathbf{A\,X\,Z}$.

3 Counterexamples and Witnesses

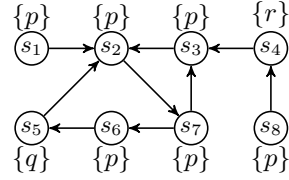


Figure 3:

1. Consider the Kripke Structure in Fig. 3.
 - (a) Fairness constraint: $\neg r$ and q . Check that $s_1 \models_F \mathbf{E} \mathbf{G} (p \vee q)$.
 - (b) Construct a witness for $s_1 \models_F \mathbf{E} \mathbf{G} (p \vee q)$, using the techniques for symbolic model checking.

4 Equivalences and Pre-Orders

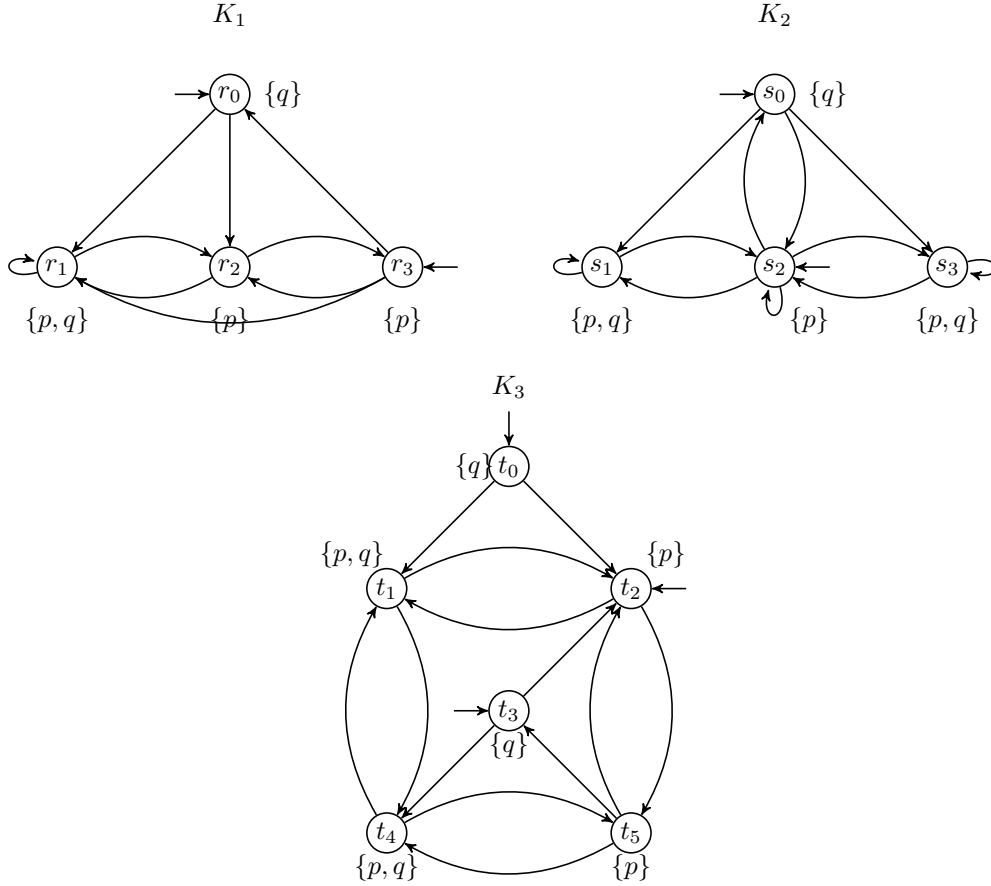


Figure 4:

1. Let K_1 and K_2 be arbitrary Kripke Structures. Let f be an arbitrary ACTL^* formula such that $K_1 \models f$ and $K_2 \not\models f$. Prove that there must be a formula g in positive form such that $K_1 \not\models g$ and $K_2 \models g$, and all path quantifiers in g are existential path quantifiers.
2. For each pair of Kripke Structures K_i, K_j in Fig. 4, prove or disprove $K_i \sqsubseteq K_j$, either by providing a simulation relation, or by providing a distinguishing ACTL -formula f (i.e., $K_i \models f$ and $K_j \not\models f$).
3. For each pair of Kripke Structures K_i, K_j in Fig. 4, prove or disprove $K_i \equiv K_j$, either by computing a bisimulation relation, or by providing a distinguishing CTL -formula f (i.e., $K_i \models f \Leftrightarrow K_j \models f$).

5 Model Checking the Modal μ -Calculus

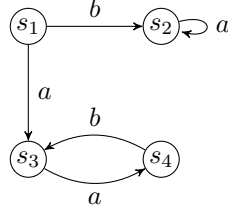


Figure 5:

1. Prove, for arbitrary environment θ , arbitrary labelled transition system \mathcal{L} with action set $Act \supseteq \{a\}$ that $\llbracket [a]\nu X.[a]X \rrbracket \theta = \llbracket \text{true} \rrbracket \theta$.
2. Prove, for arbitrary environment θ and arbitrary labelled transition system \mathcal{L} that $\llbracket \neg\mu X.\phi \rrbracket \theta = \llbracket \nu.\neg\phi[X := \neg X] \rrbracket \theta$ for all formulae ϕ . Hint: Expand $\llbracket \cdot \rrbracket$ as much as possible and perform induction over the number of fixpoint-iterations.
3. Consider the following μ -calculus formula ϕ and the labelled transition system \mathcal{L} in Fig. 5.

$$\phi := \nu X. \left([a]X \wedge \nu Y. \mu Z. (\langle b \rangle Y \vee \langle a \rangle Z) \right)$$

- (a) Explain in natural language the meaning of formula ϕ .
 - (b) Compute the set of states of \mathcal{L} where ϕ holds with the naive algorithm (give all intermediate approximations).
 - (c) Compute the set of states of \mathcal{L} where ϕ holds with the Emerson-Lei's algorithm (give all intermediate approximations).
4. Consider the following μ -calculus formula and the labelled transition system \mathcal{L} in Fig. 6.

$$\nu X. \nu Y. \left((\langle b \rangle X) \wedge (\langle a \rangle (Y \wedge \langle a \rangle X)) \right)$$

- (a) Explain in natural language the meaning of formula ϕ .
- (b) Compute the set of states of \mathcal{L} where ϕ holds with the naive algorithm (give all intermediate approximations).
- (c) Compute the set of states of \mathcal{L} where ϕ holds with the Emerson-Lei's algorithm (give all intermediate approximations).

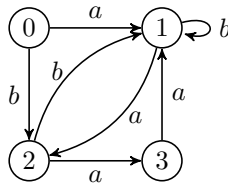


Figure 6: