Verification of temporal logics on infinite-state systems

Exercises on Day 2

Stéphane Demri and Valentin Goranko

ESSLLI 2007, Dublin, July 2007

If you are not familiar with the concepts referred in a particular exercise, just ignore it.

1 Reachability

1. Show that rational graphs with length-preserving transition relations have decidable existential reachability from a rational set to a rational set.

2. Express in terms of suitable reachabilities the following properties: safety, eventuality, partial correctness, total correctness, weak and strong fairness.

3. Write set-theoretic conditions for universal reachability in a finite transition system:
   (a) From state to state.
   (b) from state to set.
   (c) From set to set.

4. Likewise for existential recurrent and universal recurrent reachability.

5. Find algorithms, as efficient as you can, for solving the various reachability problems on finite transition systems.

   Estimate their complexity and try to argue their optimality.

   Then consult the literature.

1.1 Pushdown systems

1. Fill in the details of the inductive proof in the construction of $A_{\text{pre}^*}$ that $A_n$ accepts precisely the configurations in $\text{pre}^n(C)$.

2. Consider the pushdown system of the example presented in the lecture:

   $\mathcal{P} = (P, \Gamma, \Delta)$, where: $P = \{p_0, p_1, p_2\}; \Gamma = \{\gamma_0, \gamma_1, \gamma_2\}$;

   $\Delta = \{(p_0, \gamma_0) \rightarrow (p_1, \gamma_1), (p_1, \gamma_1) \rightarrow (p_2, \gamma_2\gamma_0),$
   $(p_2, \gamma_2) \rightarrow (p_0, \gamma_1), (p_0, \gamma_1) \rightarrow (p_0, \varepsilon)\}$.

   (a) Construct $\mathcal{P}$-automata recognizing the set of configurations $X_1 = \{p_0, \gamma_0^n \mid n \in N\}$ and $X_2 = \{p_2, \gamma_2\gamma_0^n \mid n \in N\}$.

   (b) Construct finite automata computing the sets $\text{pre}^*(X_1)$ and $\text{pre}^*(X_2)$. 
1.2 Temporal logics

Exercises on LTL:

1. Check the validity of the following LTL-formulae:
   (a) $G \infty \varphi \rightarrow F \infty \varphi$;
   (b) $G \varphi \land F \psi \rightarrow \varphi U \psi$;
   (c) $G \varphi \leftrightarrow \varphi \land X G \varphi$;
   (d) $\varphi \land G (\varphi \rightarrow X \varphi) \rightarrow G \varphi$;
   (e) $\varphi \land G (\varphi \rightarrow F \varphi) \rightarrow GF \varphi$;
   (f) $(\varphi \rightarrow \chi) U \psi \land \varphi U \psi \rightarrow \chi U \psi$;
   (g) $\varphi U \psi \leftrightarrow (\psi \lor (\varphi \land X (\varphi U \psi)))$;
   (h) $\psi U (\varphi \lor \chi) \leftrightarrow (\psi U \varphi \lor \psi U \chi)$;
   (i) $G (\psi \lor (\varphi \land X \theta)) \rightarrow (\theta \rightarrow \varphi U \psi)$.

2. Show that the following LTL-formulae are not valid, by constructing appropriate counter-models:
   (a) $F \infty \varphi \rightarrow G \infty \varphi$;
   (b) $F \infty (\varphi \land \psi) \equiv F \infty \varphi \land F \infty \psi$;
      (But one of the implications holds. Which one?)
   (c) $G \infty (\varphi \lor \psi) \equiv G \infty \varphi \lor G \infty \psi$;
      (Likewise.)
   (d) $\psi U (\varphi \rightarrow \chi) \land \psi U \varphi \rightarrow \psi U \chi$;
   (e) $G (\theta \rightarrow (\psi \lor (\varphi \land X \theta))) \rightarrow (\theta \rightarrow \varphi U \psi)$.

3. Check the following equivalences in LTL:
   (a) $G \infty \neg \varphi \equiv \neg F \infty \varphi$;
   (b) $G \infty G \infty \varphi \equiv G \infty \varphi$;
   (c) $F \infty F \infty \varphi \equiv F \infty \varphi$;
   (d) $F \infty (\varphi \lor \psi) \equiv F \infty \varphi \lor F \infty \psi$;
   (e) $G \infty (\varphi \land \psi) \equiv G \infty \varphi \land G \infty \psi$;

4. Formalize the following specifications in LTL:
   (a) “The event $\varphi$ will not occur before the event $\psi$ which may or may not occur at all.”
   (b) “The event $\varphi$ will not occur before the event $\psi$ which will occur.”
   (c) “Every occurrence of the event $\psi$ is preceded by an occurrence of the event $\varphi$, after the previous occurrence of $\psi$, if any.”
      Question: can this specification be simplified to:
      “Between every two successive occurrences of the event $\psi$ there is an occurrence of the event $\varphi$.”?
   (d) “Every time when a message is sent, it will not be marked as ‘sent’ before an acknowledgment of receipt is returned.”
Exercises on CTL and CTL\(^*\):

1. Check the validity of the following CTL\(^*\)-formulae:
   
   (a) \(\forall \varphi\) for every LTL-valid formula \(\varphi\).
   (b) \(\forall \varphi \rightarrow \varphi\); (NB: \(\varphi\) can be a path or a state formula.)
   (c) \(\forall X \varphi \rightarrow X \forall \varphi\);
   (d) \(\forall G \varphi \rightarrow G \forall \varphi\);
   (e) \(\forall G \exists F \varphi \rightarrow \exists GF \varphi\); (Burgess’s formula)
   (f) \(\forall (\varphi \rightarrow \psi) \rightarrow (\forall \varphi \rightarrow \forall \psi)\);
   (g) \(\forall G (\varphi \rightarrow \exists X \varphi) \rightarrow (\varphi \rightarrow \exists G \varphi)\);
   (h) \(\forall G (\forall \varphi \rightarrow \exists X F \forall \varphi) \rightarrow (\forall \varphi \rightarrow \exists GF \forall \varphi)\);
   (i) (Difficult.) \(\forall G (\exists \varphi \rightarrow \exists X ((\exists \psi U \exists \theta))) \rightarrow (\exists \varphi \rightarrow \exists G ((\exists \psi U \exists \theta)))\) (Reynold’s limit closure formula).

2. Show that the following formulae are not CTL\(^*\)-valid by constructing appropriate counter-models.
   
   (a) \(G \forall \varphi \rightarrow \forall G \varphi\);
   (b) \(\forall FG \varphi \rightarrow \forall F \forall G \varphi\);
   (c) \(\forall G \exists F \varphi \rightarrow \forall GF \varphi\);
   (d) \(\forall G (\varphi \rightarrow \exists XF \varphi) \rightarrow (\varphi \rightarrow \exists G \varphi)\).

3. Show that the following pairs of CTL\(^*\)-formulae are equivalent, i.e. true on the same pairs \((M, \sigma)\).
   
   (a) \(\forall G \varphi \) and \(\neg \exists F \neg \varphi\);
   (b) \(\exists G \varphi \) and \(\neg \forall F \neg \varphi\);
   (c) \(\forall GF \varphi \) and \(\forall G \forall F \varphi\);
   (d) \(\exists FG \varphi \) and \(\exists F \exists G \varphi\).

4. Show that the following pairs of CTL\(^*\)-formulae are not equivalent, by constructing appropriate counter-models. Determine which implications are valid.
   
   (a) \(\exists GF \varphi \) and \(\exists G \forall F \varphi\);
   (b) \(\exists GF \varphi \) and \(\exists G \exists F \varphi\);
   (c) \(\forall FG \varphi \) and \(\forall F \exists G \varphi\);
   (d) \(\exists FG \varphi \) and \(\exists F \forall G \varphi\).

5. Formalize the following specifications in CTL or CTL\(^*\). (Only one of them needs CTL\(^*\).)
   
   (a) “For every future state \(s\) where \(\varphi\) is true, every successor state satisfies \(\psi\) and there is a computation starting from \(s\) on which \(\psi\) is true until \(\varphi\) becomes false.”
   (b) “From every state of every computation on which \(q\) is eventually true, a computation starts on which \(p\) will be eventually always true.”
   (c) “There is no computation on which some state where \(q\) is true starts a computation on which \(p\) is never true.
   (d) “If \(\varphi\) is eventually true on every computation starting from the current state, then there is a future state, on every computation starting from which \(\psi\) will remain false until \(\varphi\) becomes true.”