Prof. Bernd Finkbeiner, Ph.D.
Martin Zimmermann, Ph.D.
Leander Tentrup, B.Sc.

Summer term 2013
Problem Set 19
October 4, 2013

Verification

Problem 1: Theories / Nelson-Oppen [4 Points]

For the formula

$$1 \leq x \land x \leq 2 \land \mathsf{cons}(1, y) \neq \mathsf{cons}(x, y) \land \mathsf{cons}(2, y) \neq \mathsf{cons}(x, y),$$

identify the combination of theories in which it lies. To avoid ambiguity, prefer $T_{\mathbb{Z}}$ to $T_{\mathbb{Q}}$. Then apply the Nelson-Oppen method and then use the appropriate decision procedures for the resulting formulas.

Problem 2: Theories / Nelson-Oppen [2 Points]

For the formula

$$a[i] \geq 1 \land a[i] + x \leq 2 \land x > 0 \land x = i \land a\langle x \triangleleft 2\rangle[i] \neq 1,$$

identify the combination of theories in which it lies. To avoid ambiguity, prefer $T_{\mathbb{Z}}$ to $T_{\mathbb{Q}}$. Then apply the Nelson-Oppen method and argue informally whether the resulting formulas are satisfiable.

The following exercises belong to the afternoon session.

Problem 3: True or False [0 Points]

1. $\mathsf{AX}\,\mathsf{AG}\,p \equiv \mathsf{AG}\,\mathsf{AX}\,p$
2. $\mathsf{EX}\,\mathsf{EG}\,p \equiv \mathsf{EG}\,\mathsf{EX}\,p$
3. $\mathsf{AF}\,\mathsf{AG}\,p$ can be expressed in LTL.
4. If Φ is a CTL formula and ψ is an LTL formula such that $\Phi \equiv \psi$, then $\neg\Phi \equiv \neg\psi$.
5. $s \models \mathsf{EF}\,\mathsf{EG}\,p$ iff there is a path π from s with $\pi \models \mathsf{F}\,\mathsf{G}\,p$.
6. $s \models \mathsf{EG}\,\mathsf{EF}\,p$ iff there is a path π from s with $\pi \models \mathsf{G}\,\mathsf{F}\,p$.
7. Let TS be a transition system and Φ a CTL formula. If TS does *not* satisfy $\neg\Phi$, then TS satisfies Φ.

8. Let s_1, s_2 be states of a transition system and let

$$\Phi = \mathsf{E}\,(a\,\mathsf{U}\,(\mathsf{EX}\,b \wedge \mathsf{EX}\,c)).$$

   If $s_1 \models \Phi$ and *not* $s_2 \models \Phi$ then $\mathit{Traces}(s_1) \neq \mathit{Traces}(s_2)$.

9. CTL* equivalence is strictly finer than CTL equivalence.

10. LTL equivalence is strictly finer than CTL equivalence.

11. CTL equivalence is strictly finer than LTL equivalence.

12. If $s \models \mathsf{AF}\,p$ then $s \models_{fair} \mathsf{AF}\,p$.

13. If $s \models \mathsf{EF}\,p$ then $s \models_{fair} \mathsf{EF}\,p$.

14. $s \models_{fair} \mathsf{E}\,(a\,\mathsf{U}\,b)$ iff $s \models \mathsf{E}\,(a\,\mathsf{U}\,(b \wedge \mathsf{EG}\,\mathit{true}))$

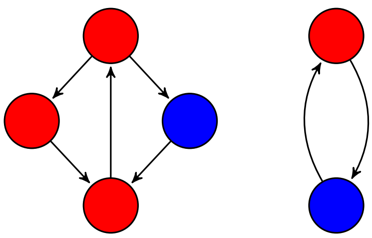
15. $s \models_{fair} \mathsf{E}\,(a\,\mathsf{U}\,b)$ iff $s \models \mathsf{E}\,(a\,\mathsf{U}\,(b \wedge a_{fair}))$ where a_{fair} is an atomic proposition with $s \models a_{fair}$ iff $s \models_{fair} \mathsf{EG}\,\mathit{true}$.

16. For each Büchi automaton A there is an LTL formula φ such that Words(φ) is the language of A.

17. If two states s_1 an s_2 in a finite transition system satisfy the same $CTL_{\setminus \mathsf{U}}$ formulas, then s_1 and s_2 are bisimilar.

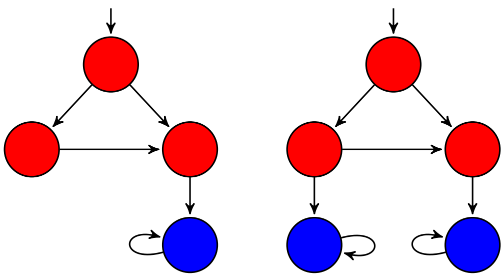
18. Bisimilar transition systems are simulation equivalent.

19. The following two transition systems are stutter-trace equivalent.



20. Let TS_1 and TS_2 be two stutter-bisimilar transition systems and let φ be an LTL formula without Next then either both TS_1 and TS_2 satisfy φ or neither satisfies φ.

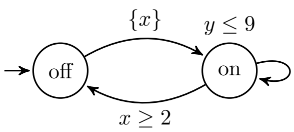
21. The following two transition systems are divergence-sensitive stutter-bisimilar.



22. For every boolean function there is a variable ordering such that the size of the ROBDD is polynomial.

23. For every boolean function there is a variable ordering such that the size of the ROBDD is exponential.

24. The following timed automaton satisfies $\mathsf{EF}\, on$:



25. Each nonzeno timed automaton is timelock-free.

26. The state graph and the region graph of a timed automaton are bisimilar over AP'.

27. Clock equivalence is a bisimulation.

28. If there is a P-inductive program annotation, then P is partially correct.

29. It holds that

$$wp(F, \texttt{assume } c) = F \wedge c$$

30.

$$f(a) = f(b) \rightarrow a = b$$

is T_E-satisfiable.

31. T_E is decidable.

32.

$$a[i] = e \;\rightarrow\; a\langle i \triangleleft e\rangle = a$$

is T_{A}-valid.

33. The quantifier-free fragment of the theory of arrays with extensionality is decidable.

34. The limitations of the Nelson-Oppen method are as follows:
Given formula F in theory $T_1 \cup T_2$.
   a) F must be quantifier-free.
   b) Signatures Σ_i of the combined theory only share $=$, i.e.,

$$\Sigma_1 \cap \Sigma_2 = \{=\}$$

   and both must contain the axioms of the theory of equality.
   c) Theories must be stably infinite.
   d) Theories T_1, T_2 must be convex.