ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

A. Podelski
A. Malkis
M. Wehrle

January 31, 2008
Discussion: Feb 4–Feb 8
Usual room(s)

Tutorials for Verification
Exercise sheet 12

Exercise 1: Weak Until in CTL

Prove that for any transition system,

(a) $Sat(\exists \Phi \mathsf{W} \Psi)$ is the largest set T satisfying

$$T \subseteq Sat(\Psi) \cup \{s \in Sat(\Phi) \mid Post(s) \cap T \neq \emptyset\},$$

(b) $Sat(\forall \Phi \mathsf{W} \Psi)$ is the largest set T satisfying

$$T \subseteq Sat(\Psi) \cup \{s \in Sat(\Phi) \mid Post(s) \subseteq T\}.$$

Exercise 2: Characterization of $Sat_{sfair}(\exists \Box a)$

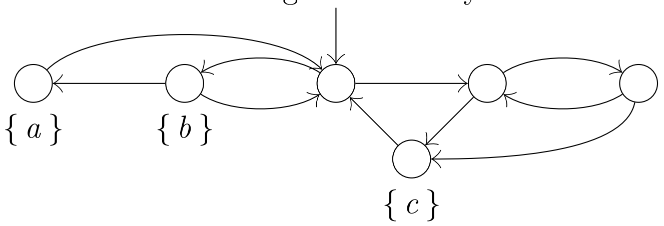
Fix a finite transition system without terminal states, an atomic proposition a, a state s and a strong fairness constraint $f = \bigwedge_{1 \leq i \leq k}(\Box \Diamond a_i \Rightarrow \Box \Diamond b_i)$. Then $s \models_f \exists \Box a$ if and only if there is a finite path fragment $t = (t_i)_{i=0}^n$ and a cycle $t' = (t'_i)_{i=0}^r$ such that

- $t_0 = s$ and $t_n = t'_0 = t'_r$ and
- $t_i \models a$ and $t'_j \models a$ (for all $0 \leq i \leq n$, $0 \leq j \leq r$) and
- $Sat(a_i) \cap \{t'_1, \ldots, t'_r\} = \emptyset$ or $Sat(b_i) \cap \{t'_1, \ldots, t'_r\} \neq \emptyset$ (for all $1 \leq i \leq k$).

Hint: the proof in the script is only a proof attempt.

Exercise 3: CTL with fairness model-checking

Consider the following transition system:



We have two strong fairness constraints for a and b and a weak fairness constraint for c.

$$fair \equiv (\Box \Diamond \exists \bigcirc a \rightarrow \Box \Diamond a) \wedge (\Box \Diamond \exists \bigcirc b \rightarrow \Box \Diamond b) \wedge (\Diamond \Box \exists \bigcirc c \rightarrow \Box \Diamond c)$$

(a) Convert the weak fairness constraint to an equivalent strong fairness constraint.

(b) Apply the algorithm of the lecture to compute $Sat_{fair}(\exists\Box\text{true})$.

(c) Apply the algorithm of the lecture to compute $Sat_{fair}(\exists\Box\neg a)$.

(d) Apply the algorithm of the lecture to compute $Sat_{fair}(\exists\Box\neg c)$.

Exercise 4: Semantics of CTL$^+$ and syntactic sugar
Give the precise semantics of formulas of CTL$^+$. Define disjunction, $\forall$ and $\Box$ in terms of other operators.

Exercise 5*: Converting CTL$^+$ formulas into CTL formulas
Prove the following equivalences of CTL$^+$ formulas (Greek letters denote state formulas and Latin letters denote path formulas):

(a) $\neg\bigcirc\Phi \equiv \bigcirc\neg\Phi$

(b) $\neg(\Phi \,\mathsf{U}\, \Psi) \equiv (\neg\Psi \,\mathsf{U}\, \neg\Phi \wedge \neg\Psi) \vee \Box\neg\Psi$

(c) $\exists(f \vee g) \equiv \exists f \vee \exists g$

(d) $\bigcirc(\Phi \wedge \Psi) \equiv \bigcirc\Phi \wedge \bigcirc\Psi$

(e) $\Box(\Phi \wedge \Psi) \equiv \Box\Phi \wedge \Box\Psi$

(f) $\exists\left(\bigwedge_{j=1}^{n}\left[(\Phi_j \,\mathsf{U}\, \Psi_j) \wedge \bigcirc\chi \wedge \Box\Xi\right]\right) \equiv$
$\bigvee_{J\subseteq\{1,\ldots,n\}}\left(\bigwedge_{j\in J}\Psi_j \wedge \Xi \wedge \exists\bigcirc\left[\chi \wedge \exists((\bigwedge_{j\notin J}(\Phi_j \,\mathsf{U}\, \Psi_j)) \wedge \Box\Xi)\right]\right)$

(g) $\exists\left(\bigwedge_{j=1}^{n}\left[(\Phi_j \,\mathsf{U}\, \Psi_j) \wedge \Box\Xi\right]\right) \equiv$

$$\bigvee_{\pi \text{ is a permutation of } \{1,\ldots,n\}}\Bigg[\bigwedge_{1\le j\le n}\Phi_j \wedge \Xi \,\mathsf{U}$$
$$(\Psi_{\pi(1)} \wedge \exists(\bigwedge_{\substack{1\le j\le n,\\ j\notin\{\pi(1)\}}}\Phi_j \wedge \Xi \,\mathsf{U}$$
$$(\Psi_{\pi(2)} \wedge \exists(\bigwedge_{\substack{1\le j\le n,\\ j\notin\{\pi(1),\pi(2)\}}}\Phi_j \wedge \Xi \,\mathsf{U}$$
$$\cdots$$
$$(\Psi_{\pi(n-1)} \wedge \exists(\bigwedge_{\substack{1\le j\le n,\\ j\notin\{\pi(1),\ldots,\pi(n-1)\}}}\Phi_j \wedge \Xi \,\mathsf{U}\, (\Psi_{\pi(n)} \wedge \exists\Box\Xi)))))))\Bigg]$$

Show how to convert CTL$^+$ formulas into CTL formulas.