CSC2108, Fall 2007: Automated Verification
Assignment 1

Due: October 3, classtime

1. Solve the following problem: Use the definition of $\models$ between states and CTL formulas to explain why $s \models AGAF\varphi$ means that φ is true infinitely often along every path starting at s.

2. Which of the following pairs of CTL formulas are equivalent? For those which are not, exhibit a model of one of the pair which is not a model of the other. Otherwise, use the definition of CTL formulas and relationships between them to show that the formulas are equivalent.

   (a) $(\mathrm{EG}\ \varphi) \vee (\mathrm{EG}\ \psi)$ and $\mathrm{EG}\ (\varphi \vee \psi)$

   (b) $(\mathrm{AF}\ \varphi) \wedge (\mathrm{AF}\ \psi)$ and $\mathrm{AF}\ (\varphi\ \wedge\ \psi)$

   (c) $\top$ and $(\mathrm{AG}\ \varphi) \rightarrow (\mathrm{EG}\ \varphi)$

   (d) $\top$ and $(\mathrm{EG}\ \varphi) \rightarrow (\mathrm{AG}\ \varphi)$

   (e) $\mathrm{A}\ [\varphi\ \mathrm{U}\ \psi]$ and $\varphi \wedge\ \mathrm{AF}(\psi)$

   (f) $\mathrm{A}\ [\varphi\ \mathrm{U}\ \psi] \vee \mathrm{A}\ [\tau\ \mathrm{U}\ \psi]$ and $\mathrm{A}[(\tau \vee \varphi)\ \mathrm{U}\ \psi]$

   (g) $\mathrm{A}[\varphi\ \mathrm{U}\ \mathrm{A}[\psi\ \mathrm{U}\ \tau]]$ and $\mathrm{A}[\mathrm{A}[\varphi\ \mathrm{U}\ \psi]\ \mathrm{U}\ \tau]$

3. Express the following properties in CTL. You may invent any boolean variables necessary to express your atomic propositions. Do not use the pattern system.

   (a) Whenever we get into that situation, we will sometimes be able to get out of it.

   (b) Both of those things may happen, but not at the same time.

   (c) If that ever happens, it won't keep happening forever.

   (d) When this situation happens, it may persist for a while, but not forever, and it is always followed immediately by that situation.

   (e) One should be able to get candy and drinks from the vending machine, but not both at the same time.

   (f) An elevator should keep its doors open until there is a request to use it.

   (g) After p, q is never true. Express it so that the constraint is meant to apply on all computation paths.

   (h) Transitions to states satisfying p occur at most twice on all computation paths.

   (i) p precedes s and t on all computation paths. (Hint: try the negation of this specification first.)

4. Which of the following pairs of LTL formulas are equivalent? For the equivalent formulas, show the equivalence. For those that are not,exhibit a model of one of the pair that is not the model of the other:

    (a) $\diamond(p \wedge q)$ and $\diamond p \ \wedge \ \diamond q$

    (b) $\Box \diamond (p \vee q)$ and $\Box \diamond p \vee \Box \diamond q$

    (c) $\circ(p\ U\ q)$ and $(p\ U\ \ \circ q) \vee q$

    (d) $\circ \diamond p$ and $\diamond \circ p$

5. Do $\circ$ and U form the adequate set for LTL? If so, prove it.

6. Find a transition system which distinguishes the following pairs of formulas (CTL and LTL). That is, show that they are *not* equivalent:

    (a) $\Box \diamond p$ and AG EF p

    (b) $\circ p \vee (\circ \circ p)$ and AX p $\vee$ AX AX p

7. Show that the following LTL formulas are *valid*, i.e., true in any state of any model

    (a) $\neg q$ U $(\neg p \ \wedge \ \neg q) \rightarrow \neg \Box p$

    (b) $\Box \neg q \ \wedge \ \diamond \neg p \rightarrow \neg q$ U $(\neg p \ \wedge \ \neg q)$

    (c) Expand $\neg((p \ \text{U} \ q) \vee \Box p)$ using de Morgan rules and the LTL equivalence $\neg(a \ \text{U} \ b) \equiv (\neg b \ \text{U} \ (\neg a \ \wedge \ \neg b)) \vee \neg \diamond b$. Using this expansion and the facts above, show that $\neg((p \ \text{U} \ q) \vee \Box p) \rightarrow \neg q \ \text{U} \ (\neg p \ \wedge \ \neg q)$

8. Using the pattern hierarchy, express the following properties in CTL and LTL:

    (a) When a client A makes a method call to a server B, it will eventually receive the results of its call if the server is OK.

    (b) It is always the case that when the `req-search-state` is not enabled, then the req-close-state shall not be closed and will remain not closed until the `req-search-state` is enabled.

    (c) After opening a network connection, an error message will pop up in response to a network error.

    (d) Every time the form is shown on screen, it must have been preceded by a corresponding `request-view` event.

    (e) Checkout is 0 until the status of the book is charged or on hold

9. Consider the property (using the property patterns): P is universal between S and T.

(a) Is the interval open/closed on the left/right? (Use the LTL and CTL mappings to answer this question).

(b) According to the mappings, when the specification is satisfied, must P occur when T first becomes true?

(c) According to the mappings, when the specification is satisfied, can S occur without T?

(d) According to the mappings, when the specification is satisfied, if there is no matching T for an S, is P required to hold after the S with no matching T?

(e) For each combination of open/closed on left/right, create the LTL universality pattern.

10. Repeat parts (a)-(d) of the previous problem for the specification P is universal after S until T.