CS613:	**Homework 2**	Due in class Wednesday, Oct. 6, 2004

Reading: Please read all of chapter three of Huth and Ryan. Read or skim parts of the NuSMV 2.2 User Manual and NuSMV 2.2 Tutorial as needed.

Problems: (Most of these are taken from Huth and Ryan.) To do problems 3 and 4 you need to download and install NuSMV 2.2, with Chaff. See: http://nusmv.irst.itc.it/ . Also, many of the figures and tables from Huth and Ryan are on-line so you don't have to type in their specifications. See: http://www.cs.bham.ac.uk/research/lics/ancillary/index.html.

1. Which of the following pairs of CTL formulas are equivalent? For each pair, give an informal proof of equivalence or a model on which they differ.

   (a) $\mathbf{EF}\varphi \vee \mathbf{EF}\psi$; $\mathbf{EF}(\varphi \vee \psi)$

   (b) $\mathbf{AF}\varphi \vee \mathbf{AF}\psi$; $\mathbf{AF}(\varphi \vee \psi)$

   (c) $\mathbf{A}[p\mathbf{U}\mathbf{A}[q\mathbf{U}r]]$; $\mathbf{A}[\mathbf{A}[p\mathbf{U}q]\mathbf{U}r]$. [Hint: first think about a model that has only one path.]

2. Express each of the following properties in CTL and LTL if possible. If neither is possible try to express in CTL*. [Hint: sometimes it seems easier to first express the negation of the property.]

   (a) Event p precedes s and t on all computation paths, i.e., whenever s or t holds, p held at some strictly previous time.

   (b) On all computation paths, after p holds, q never holds. (I read this to mean **strictly** afterwards. The English is often somewhat ambiguous. Maybe it would be more clear to say, "On all computation paths, when p holds for the first time, then q may hold then, but at no later time.")

   (c) "Between the events q and r, event p is never true." (I took this directly from the book. It is open to several interpretations. Please assume that what is meant is that on all paths, p is false throughout each closed interval $[q, r]$ where q holds at the beginning of the interval and r holds at the end of the interval and only at the end.) Because of ambiguity, it is often a non-trivial task to go from specifications in English to appropriate formal specifications. In this case, the question was did we mean the strict or inclusive meaning of "between"? I chose the inclusive meaning. The strict meaning would be that p is false in the open interval (q, r).)

   (d) Property p is true for every second state along some path, i.e., it is true at $s_2, s_4, s_6,$ and so on. I don't care about the odd states.

3. Use NuSMV to verify the four LTL specifications, call them φ_1 through φ_4, from Figure 3.10, page 196. Note that for your convenience the specified model is drawn in Fig 3.11 on page 198. Also use NuSMV to check which, if any, of the two fairness assertions are necessary for each of φ_1 through φ_4 to hold.

4. Use NuSMV to solve the ferryman puzzle as detailed on pages 199 to 201. In particular, write a specification meaning that the ferryman safely gets the goat, wolf, and cabbage safely to the other side **and leaves them there**. Next, as explained in the text, use the bounded model checking feature of NuSMV to show that you have the shortest possible solution to this puzzle.