ECE/CS 584: Embedded System Verification	Fall 2008
Homework 1 on Modelling— Due on October 2^{nd}, 2012	*Your name*

Problem 1 (10 points). Consider a idealized billiard table of length a and width b. This table has no pockets, its surface has no friction, and it's boundary bounces the balls perfectly. Write a hybrid automaton model of the position of a ball on this table which is shot from the initial position (x_0, y_0) with the initial velocity (v_x, v_y). Before starting, read Problem 2.

Problem 2 (10 + 20 = 30 points). Consider two satellites orbiting the earth on circular orbits with (constant) angular speeds ω_1 and ω_2.

Part (a) Write a hybrid automaton model of the position of the satellite-pair in the $[0, 2\pi]^2$ space.

Part (b) For appropriate choice of ω_1, ω_2, and the initial position of the satellites, show that this hybrid automaton is bisimilar to the hybrid automaton in Problem 1.

Problem 3. (15 + 5 + 20 = 40 points) In this problem, you will model an n-process distributed token ring system as a single hybrid automaton and prove an invariant. In a future homework we will use a theorem prover to prove the same property.

System description. Consider n processes $0, \ldots, n-1$ connected in a directed ring. We say process $i + 1 \mod n$ is the successor of process i. Each process i, has a value v_i which can be an element of the set $\{0, \ldots, k\}$ for some $k > n$. Each process behaves as follows: Process i, $i \neq 0$, is said to have a token iff $v_i \neq v_{i-1}$. Process 0 has a token iff $v_0 = v_{n-1}$. Each process has a real-valued period parameter $\Delta_i > 0$. Exactly every Δ_i time, process i performs the following action if it has the token: if $i = 0$ then $v_i := (v_i + 1) \mod n$, otherwise $v_i := v_{i-1}$.

Part (a) Write a complete hybrid automaton specification for this system. In your hybrid automaton model, you'll need array type variables. For example, with an array $v : [n] \rightarrow [k]$, each $v[i]$ could model the cooresponding v_i's. You may need additional variablies, for example, for the timers.

Part (b) Show two executions of the system: one that starts from an initial state with a single token and a second with multiple tokens.

Part (c) Suppose that in any initial state of the system, only one process has a token. Prove the following invariant inductively: In any reachable state of the system, only one process has a token. Use the inductive-invariant proof rule

Problem 4 (bonus problem). Let $\mathcal{A}_1$ and $\mathcal{A}_2$ be compatible hybrid automata and let $\mathcal{A} = \mathcal{A}_1 \| \mathcal{A}_2$. Prove the following.

(a) If $\alpha \in \mathsf{Execs}_{\mathcal{A}}$, then $\alpha \lceil A_i \in \mathsf{Execs}_{\mathcal{A}_i}$, for $i \in \{1, 2\}$.

(b) Suppose β be an alternating sequence of actions in $E_{\mathcal{A}}$ and trajectories for the empty set of variables. If $\beta \lceil \mathcal{A}_i \in \mathsf{Traces}_{\mathcal{A}_i}$ then $\beta \in \mathsf{Traces}_{\mathcal{A}}$.

Notation. For an execution (or a trace) α of $\mathcal{A}$, $\alpha \lceil \mathcal{A}_i$, for $i \in \{1, 2\}$, is the restricted sequence which captures the actions of $\mathcal{A}_i$ and the evolution of the variables of $\mathcal{A}_i$. See Chapter 2 of [1] for a formal definition.

References

[1] Dilsun K. Kaynar, Nancy Lynch, Roberto Segala, and Frits Vaandrager. *The Theory of Timed I/O Automata*. Synthesis Lectures on Computer Science. Morgan Claypool, November 2005. Also available as Technical Report MIT-LCS-TR-917.