VRS — Summer 2014	**Problem Set #4**
Computer-Aided Verification	**Due See below, 2014**

The due date for problems 1-4 is July 16. The due date for problem 5 is July 9.

Problem 1.1. Let $(S, \to, A, \langle\!\langle\cdot\rangle\!\rangle)$ be a labeled transition system (S is a set of states, $\to$ is a binary relation on S, A is a set of labels, and $\langle\!\langle\cdot\rangle\!\rangle : S \to A$ is a function mapping states to labels).

A binary relation R on S is a *simulation* if (1) $R(s,t)$ implies $\langle\!\langle s\rangle\!\rangle = \langle\!\langle t\rangle\!\rangle$, and (2) $R(s,t)$ and $s \to s'$ imply the existence of $t' \in S$ such that $t \to t'$ and $R(s', t')$. If there is a simulation R such that $R(s,t)$, we say that s *simulates* t and write $s \preceq t$.

A binary relation R on S is a *bisimulation* if (1) $R(s,t)$ implies $\langle\!\langle s\rangle\!\rangle = \langle\!\langle t\rangle\!\rangle$, (2) $R(s,t)$ and $s \to s'$ imply the existence of $t' \in S$ such that $t \to t'$ and $R(s', t')$, and (3) $R(s,t)$ and $t \to t''$ imply the existence of $s'' \in S$ such that $s \to s''$ and $R(s'', t'')$. If there is a bisimulation R such that $R(s,t)$, we say that s and t are *bisimilar* and write $s \cong t$.

1. Show that if $s \cong t$ and s can reach a state labeled p, then t can also reach a state labeled p.
2. Show by an example that $s \preceq t$ and $t \preceq s$ does not imply $s \cong t$.

Problem 1.2. Define the *implicational interpolant* of two formulas A and B as follows. If $A \Rightarrow B$, an implicational interpolant is a formula C such that $A \Rightarrow C$ and $C \Rightarrow B$ and C is over the common variables between A and B. Given the interpolation procedure discussed in the class, how can you get a procedure to compute implicational interpolants?

Problem 1.3. A pair $(A, \leq)$ of a set A and a binary relation $\leq$ on A is called a *well-quasi-ordering (wqo)* if $\leq$ is reflexive and transitive, and if for every sequence of elements $a_0, a_1, \ldots$, there are $i < j$ such that $a_i \leq a_j$. Given $(A, \leq)$ (not necessarily a wqo), set $U \subseteq A$ is said to be *upward-closed* if for every $x \in U$ and every $y \in A$, $x \leq y$ implies $y \in U$.

1. Show that if $(A_1, \leq_1)$ and $(A_2, \leq_2)$ are wqos, then $(A_1 \times A_2, \leq)$ is a wqo, where $(a,b) \leq (c,d)$ iff $a \leq_1 c$ and $b \leq_2 d$. Argue why this implies $(\mathbb{N}^k, \leq)$ is a wqo, where $\leq$ is pointwise comparison. Is $(\mathbb{Z}, \leq)$ a wqo?
2. Let $(A, \leq)$ be a wqo and let $U_0 \subseteq U_1 \subseteq \ldots$ be a sequence of upward-closed subsets of A. Show that there is an i such that $U_i = U_{i+1}$.

Problem 1.4. Show that on termination, McMillan's interpolation-based model checking algorithm either produces a counterexample trace (i.e., a path to a bad state) or an inductive invariant showing that no bad states can be reached.

Problem 1.5. Write a one-page summary of your project. Write a paragraph (or more) about each of these points: the goal of the project, the current status (e.g., papers you have read, what progress you have made), what you aim to achieve, and the timeline for the next three weeks. Write this together with your project group. Each group should submit a single report.