**VRS Summer 2014 —** **Practice End Term**

The practice final exam is supposed to give you an idea of the actual exam.

There are six questions in this exam (numbered 0–5), and each question may have subparts.

Each answer should be relatively short. If you find you are writing more than several paragraphs, please think again whether what you are doing is correct. I would recommend you start with Problems 0 and 1. You should not spend more than 30 minutes on Problem 1.

The maximum score for this exam is 50 points.

**Problem 0.** Write your name and your student identification number.

**Problem 1.** (10 points.) There are 5 parts. Each part is worth 2 points.

a You are given a (reduced ordered) BDD $b$. How can you test in constant time whether the formula represented by $b$ is satisfiable?

b Suppose you are performing predicate abstraction of a state space using $n$ predicates. We said that the number of states in the abstraction is finite. How many states can there be in this finite abstraction?

c Let us define a new temporal modality $\varphi_1 \exists\mathcal{U}^* \varphi_2$ with the following semantics: A state $s$ of a labeled transition system satisfies $\varphi_1 \exists\mathcal{U}^* \varphi_2$ if there is a trace

$$s_0 \to s_1 \to \ldots \to s_k$$

for some $k \geq 0$ such that $s_0 = s$ and $s_k$ satisfies $\varphi_1 \mathcal{U} \varphi_2$ (the "usual" until formula).

Show that you can express $\varphi_1 \exists\mathcal{U}^* \varphi_2$ as an STL formula.

d We showed in class that two states are bisimilar iff they agree on all STL formulas. Extend that proof (you need only to write the new parts) to show that two states are bisimilar iff they agree on all CTL formulas.

e Suppose you have a Boolean formula $\varphi$ and you are interested in finding two distinct satisfying assignments to this formula. Show how you can get two distinct satisfying assignments by making at most two queries to a SAT solver.

**Problem 2.** (10 points total.)

1. (6 points) Consider an invariant verification problem with a formula $\mathit{init}(x)$ defining the initial states, a formula $\mathit{bad}(x)$ defining the bad states and a transition relation $T(x, x')$. Suppose there is a formula $\mathcal{I}(x)$ with the following properties:

   (a) $\mathit{init}(x) \Rightarrow \mathcal{I}(x)$,

   (b) $\mathcal{I}(x) \wedge \mathit{bad}(x)$ is unsatisfiable, and

   (c) $\mathsf{Post}(\mathcal{I}(x)) \Rightarrow \mathcal{I}(x)$.

   Prove that there is no trajectory that starts from the initial states in $\mathit{init}(x)$ and ends up in a bad state in $\mathit{bad}(x)$.

2. (4 points) Let $\mathcal{K} = (S, \rightarrow)$ be a transition system and let $s_0 \in S$ be an initial state. A transition $s \rightarrow t$ is called reachable if $s$ is reachable from $s_0$. A set of transitions is called a *transition invariant* if it contains every reachable transition. Give an enumerative model checking algorithm to check that a given set of transitions is a transition invariant.

**Problem 3.** (10 points total.)

1. (3 points) Show that $(\mathbb{N}^k, \leq)$ is a well quasi order. Here, $\mathbb{N}^k$ is the set of $k$-tuples of natural numbers and $u \leq v$ if for each $i = 1, \ldots, k$, we have $u_i \leq v_i$. [Hint: You can use the observation from class that the Cartesian product of two wqos is a wqo. Use induction on $k$.]

2. (4 points) Let $(S, \leq)$ be a wqo and let $U_0$, $U_1$, ... be a sequence of upward closed sets such that

$$U_0 \subseteq U_1 \subseteq \ldots$$

   Prove that there is some $i$ such that $U_i = U_{i+1}$.

3. (3 points) Let $\mathcal{K} = (S, \rightarrow, \leq)$ be a well-structured transition system. Let $U$ be an upward closed set of states. Prove or disprove: $\mathsf{Post}(U)$ is upward closed.

**Problem 4.** (10 points total.) For any set $X$, a binary relation $R \subseteq X \times X$ is *well-founded* if there does not exist an infinite sequence $s_0, s_1, \ldots$ of elements from $X$ such that for each $i \geq 0$, $(s_i, s_{i+1}) \in R$.

a (3 points) Is the relation $>$ on natural numbers well-founded? What about $>$ on integers? (Give a short justification or a counterexample in each case.)

Let $S = (X, \rightarrow)$ be a system with set of states $X$ and transition relation $\rightarrow$. Let $x_0 \in X$ be a state of $S$. Let *Reach* be the set of states reachable from $x_0$. We say $S$ *terminates* from initial state $x_0 \in X$ if there is no infinite sequence of states

$$x_0 \rightarrow x_1 \rightarrow \dots$$

b (4 points) Show that $S$ terminates from $x_0$ if the relation $\rightarrow \cap \mathit{Reach} \times \mathit{Reach}$ is well-founded.

A *ranking function* is a map $r : X \rightarrow \mathbb{N}$ such that whenever $s \rightarrow t$, we have $r(s) > r(t)$.

c (3 points) Show that if we can define a ranking function for $S$, then $S$ terminates from every initial state.

**Problem 5.** (10 points total.) Automatic test pattern generation (ATPG, for short) is a technique in electronic design to generate a test input that, when applied to a digital circuit, enables the designer to distinguish between the correct behavior of the circuit and a faulty behavior caused by defects. Such defects can appear in the circuit in the manufacturing process.

Let us first consider combinational circuits. These are circuits that take some inputs $x_1, \dots, x_n$, and (for simplicity) produce a single output $y$, and internally, have AND gates, OR gates, and NOT gates. We will consider "stuck-at" faults, where the input to a gate in the circuit is stuck at a particular logic value (0 or 1) instead of its proper value. If a circuit has $k$ wires, there are $2k$ stuck-at faults.

For example, take a circuit that has two inputs $x_1$ and $x_2$, and an output $y$ defined as the AND of $x_1$ and $x_2$. There are six stuck-at faults: the first input to the AND gate may be stuck at 0 or 1, the second input may be stuck at 0 or 1, and the output may be stuck at 0 or 1. In these cases, the circuit may ouput a value different from the correct value $(x_1 \wedge x_2)$.

Your job is to generate test cases that identify stuck-at faults. That is, for each wire of the circuit, you have to produce two tests, if possible. The first test will be an input such that the correct circuit (without the fault) will have a different output than the circuit where the wire is stuck at 0. The second one will similarly distinguish the correct circuit from the one in which the wire is stuck at 1.

1. (8 points) Give a procedure to find such tests. Your procedure should run in time polynomial in the size of the input circuit, but may make calls to a SAT solver. [A high level sketch of the steps is sufficient.]

2. (2 points) How would your answer change if the circuit has registers? (In a circuit with registers, the registers hold "state". In each cycle, the new value of registers is obtained as a combinational function of the old values of the registers and the current inputs.) Again, a brief answer is sufficient.