AUTOMATED REASONING, 2013/2014 1B: EXAM (OPEN BOOK), JAN 24, 2014

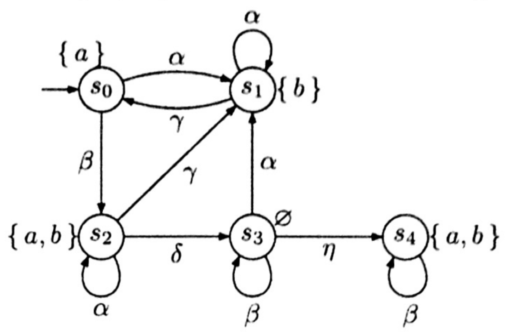
[(P1) Classify temporal properties] Consider the set AP of atomic propositions defined by $AP = \{x = 0, x > 1\}$, and a nonterminating program P that uses the variable x. Formulate the following properties in LTL:

(1) initially x is equal to zero
(2) initially x differs from zero
(3) initially x is equal to zero, but at some point x exceeds one
(4) x exceeds one only finitely many times
(5) x exceeds one infinitely often
(6) the value of x alternates between zero and non-zero

Determine which of these properties are safety properties, and justify your answers.

[18%]

[(P2) LTL checking on a Kripke structure] Consider the following system model M over the set of atomic propositions $\{a, b\}$. Note that only the positive form of the propositions is explicitly written: the state label ∅ means $\{\neg a, \neg b\}$. The transitions are also given some labels.



For each LTL formula f below, decide whether *for all computation paths*, f **holds** for M. When it does not, write the shortest counterexample π in M on which $\pi \not\models f$.

(1) $\mathbf{G}a \vee \mathbf{G}b$
(2) $\mathbf{FG}(a \vee b)$
(3) $\mathbf{GF}(a \vee b)$
(4) $a\mathbf{U}b$
(5) $\mathbf{G}(a\mathbf{U}b)$
(6) $\mathbf{F}(\neg a \wedge \neg b)$

[18%]

[(P3) Operator minimality] In temporal logics, the set of *logical operators* and *temporal operators* is not *minimal*: formulas using some operators (say, $\mathbf{G}f$) can be equivalently expressed as other formulas using other operators (say, $\neg\mathbf{F}\neg f$).

Determine the *smallest* subset of operators which is sufficient to express any temporal formula. (Ignore the Release operator **R**, but do consider the path quantifiers **A** and **E**.)

Justify that this subset is both sufficient, and minimal. Is the solution unique?

[16%]

[(P4) Complexity issues] (a) Take the automata-based **static** model checking algorithm built on a depth-first search. Say that this algorithm is run to check whether a given system modelled as a Kripke structure M violates a given temporal property f. State the (worst-case) **time complexity** of the model checking algorithm **in terms of** the size of M (e.g., the number of states in the state space) and that of f (i.e., the number of atomic propositions used in the formula).

(b) Also take the automata-based model **runtime** model checking algorithm. State the (worst-case) **runtime complexity** of the model checking algorithm, as above. Take two cases: that in which the monitor is deterministic, and that in which it is nondeterministic.

You do not need to include a detailed calculation, but should reach clear conclusions with regard to complexity classes (e.g. the algorithm is linear in the number of states in [..], exponential in the size of [..]). Justify any statement you make.

[16%]

[(P5) Equivalences of LTL formulas] All LTL specifications below describe a nonterminating system. f and g are any LTL formulas. Which of the following formula equivalences are correct? Either prove each equivalence or provide a counterexample. (If you need to use other known LTL equivalences in a proof, prove those also; otherwise, simply use the LTL induction rules.)

(1) $\mathbf{FG}f \Leftrightarrow \mathbf{GF}f$
(2) $(\mathbf{FG}f) \wedge (\mathbf{FG}g) \Leftrightarrow \mathbf{F}(\mathbf{G}f \wedge \mathbf{G}g)$
(3) $(f\mathbf{U}g)\mathbf{U}g \Leftrightarrow f\mathbf{U}g$

[18%]

[(P6) Liveness as ω-runs] The LTL induction rules tell whether an execution path π satisfies a temporal formula f, i.e. $\pi \models f$. We also linked execution paths to the concept of ω-runs; thus, you may also write $w \models f$ to state that an (in)finite word w over a set of atomic propositions AP satisfies f. We now define a liveness property more formally than before:

Definition (liveness). A temporal property f is called a *liveness* property if and only if for **any** finite word $w \in (2^{AP})^*$ there **exists** an infinite word $v \in (2^{AP})^\omega$ so that $w \cdot v \models f$, i.e., w concatenated with v satisfies f.

Intuitively, this states facts you already know about liveness properties: that it is impossible to tell whether a liveness property holds by only looking at a finite run; also, that all counterexamples to liveness properties are infinite.

Take any two temporal **liveness properties** f_1 and f_2. Using this new definition, prove or disprove that:

- $f_1 \vee f_2$ is also a liveness property;
- $f_1 \wedge f_2$ is also a liveness property.

[14%]
