AUTOMATED REASONING, 2011/2012 1B: EXAM (OPEN BOOK), JAN 27, 2012

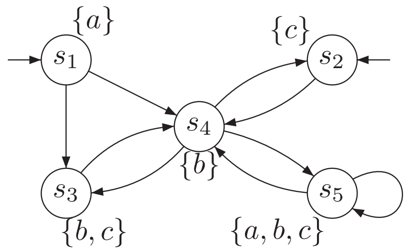
DOINA BUCUR, RUG

[**(P1) Types of specifications**] For each of the (types of) properties below, state whether they express **safety** or **liveness**, and explain why this is the case:

(1) a progress property;
(2) any invariant;
(3) the formula $p\mathbf{U}q$ (with p and q state formulas);
(4) a mutual exclusion property;
(5) a lack of starvation;
(6) a property describing *fair* execution paths.

[15%]

[**(P2) LTL checking on transition systems**] Consider the following transition system M over the set of atomic propositions $\{a, b, c\}$:



For each LTL formula f below, decide whether $\mathbf{A}f$ ("for all computation paths, f") **holds** for M. When it does not, provide a path π in M on which $\pi \not\models f$.

(1) $\mathbf{G}a$
(2) $\mathbf{FG}c$
(3) $\mathbf{GF}c$
(4) $(\mathbf{X}\neg c) \rightarrow \mathbf{XX}c$
(5) $a\mathbf{UG}(b \vee c)$

[15%]

[**(P3) Complexity issues**] Take the automata-based model checking algorithm based on a depth-first search. Say that this algorithm is run to check whether a system modelled as a Kripke structure M violates a 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).

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 size of [..], exponential in the size of [..]). Explain any statement you make.

[15%]

[(P4) New temporal operators] Take two LTL formulae f and g, and informal descriptions for three **new temporal operators**:

> **"At next":** $f\mathbf{N}g$. At the next time where g holds, f also holds.
> **"While":** $f\mathbf{W}g$. f holds at least as long as g holds.
> **"Before":** $f\mathbf{B}g$. If g holds sometime, f does so at all times before that.

Formalize each operator by providing (i) an LTL formula (using classical LTL operators), **or** (ii) an induction rule defining when each formula holds on a path π.

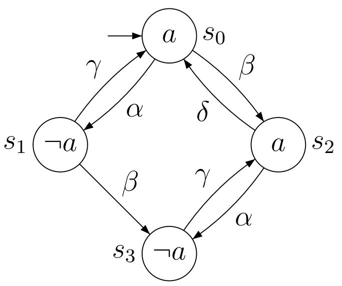
[15%]

[(P5) Equivalences of LTL formulas] Which of the following equivalences is 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.

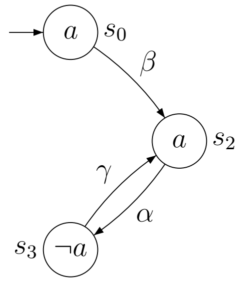
(1) $(\mathbf{FG}f_1) \wedge (\mathbf{FG}f_2) \;\Leftrightarrow\; \mathbf{F}(\mathbf{G}f_1 \wedge \mathbf{G}f_2)$
(2) $(f\mathbf{U}g)\mathbf{U}g \;\Leftrightarrow\; f\mathbf{U}g$

[15%]

[(P6) Partial-order reduction] Take the transition system M below, left, where the set of atomic propositions is simply $AP = \{a\}$, and the transitions are labelled.



(M)



(M_{reduced})

(1) Determine all pairs of independent transitions.
(2) Determine all invisible transitions.
(3) Consider the reduced system M_{reduced} above, right. Show that M and M_{reduced} are not stuttering equivalent. Which condition is violated if the ample sets are chosen as in this reduced system?

[15%]

[(P7) 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.

[10%]
