Master 1 Informatique **2018-2019**
Université de Rennes 1

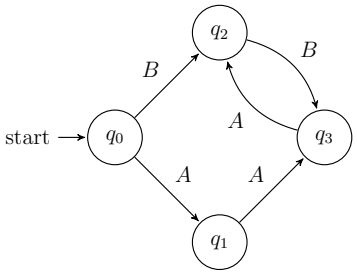
Modélisation et Vérification Formelle par Automates

Examination December 19, 2018
Subject leaders: Sophie Pinchinat and Victor Roussanaly

You may **not** *use written notes, published materials, testing aids, or any unauthorized material during the examination. By default, any of your answer should be justified. You are free to answer in French or in English. The scoring scale is indicative, and the sign (*) means a fairly difficult question.*

Exercise 1 Büchi automata

Consider the following Büchi automata $\mathcal{A}$ over alphabet $\{A, B\}$ whose accepting set F is not specified yet.



For the three following definitions of the accepting set, do we have $\mathcal{L}_\omega(\mathcal{A}) \neq \emptyset$? (Justify).

1. The accepting set is $\{q_0, q_1\}$. $\mathcal{L}_\omega(\mathcal{A}) = \emptyset$

2. The accepting set is $\{q_2, q_3\}$. $\mathcal{L}_\omega(\mathcal{A}) \neq \emptyset$

3. The accepting set is $\{q_1, q_3\}$. $\mathcal{L}_\omega(\mathcal{A}) \neq \emptyset$

Exercise 2 Logics

1. Define the syntax and the semantics of the logics LTL et CTL.

2. What can you tell about the compared expressivity of these two logics? (*give an succinct well-argued answer*).

3. When possible, give an example of a transtion system TS and a formula $\phi \in CTL$ such that $TS \not\models \phi$ and $TS \not\models \neg\phi$. Justify.

4. When possible, give an example of a transtion system TS and a formula $\psi \in LTL$ such that $TS \not\models \psi$ and $TS \not\models \neg\psi$. Justify.

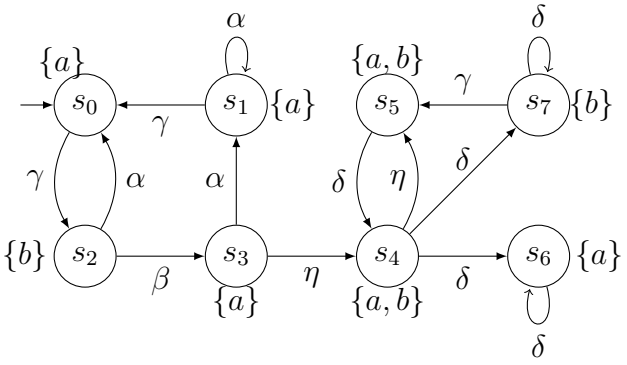
Exercise 3 Fairness

Let P the following LT property over $AP = \{a, b\}$:

$$\{A_0A_1A_2\cdots \in (2^{AP})^\omega \mid \exists n \geq 0, A_n = \{a\} \wedge \forall k > n, (A_k = \{a\} \rightarrow A_{k+1} = \{b\})\}$$

.

and TS the following transition system:



Considering the following fairness assumptions, decide whether $TS \models_{\mathcal{F}_i} P$ for each $\mathcal{F}_i$. Explain your answers.:

- $\mathcal{F}_1 = (\{\{\gamma\}\}, \{\{\beta\}, \{\alpha, \eta\}\}, \{\{\delta\}\})$.
- $\mathcal{F}_2 = (\{\{\gamma\}\}, \{\{\beta\}, \{\alpha\}, \{\eta\}\}, \{\{\delta\}\})$.
- $\mathcal{F}_3 = (\emptyset, \{\{\beta\}, \{\alpha\}, \{\eta\}, \{\gamma\}\}, \{\{\delta\}\})$.

Exercise 4 Linear-time properties

1. What is a linear time property? todo

2. Which subclass(es) of linear-time properties are remarkable? (Define them). todo

3. Among the subclasses you defined in the previous question, which ones are closed under union? interection? complementation? Justify. Safety properties are close under union and intersection, since the corresponding set of bad prefixes can be obtained by the dual operations intersection and union. Moreover, using NFA constructions, this reasoning shows that regular safety properties are also closed under union and intersection.

Safety properties are not closed under complementation since for the complement of the property "always a" is "eventually not a" and this latter is not a safety property: indeed, safety properties are those equal to their own closure, but the closure of "eventually not a" contain the infinite trace a^ω.

Liveness properties are closed under union but not under intersection: take "eventually always a" and "eventually always not a". The intersection is empty but the empty set is not a liveness property.

Also liveness properties are not closed under complementation, consider the complement of "eventually a", as above.

Exercise 5 New operators in LTL

Let ϕ and ψ be LTL formulas. We enrich LTL with new operators:

Operator S for "surround": A path satisfies the formula $\phi \mathbf{S} \psi$ if at any moment i along that path where ψ holds, there is a moment before i where ϕ holds and a moment after i where ϕ also holds.

Operator $\mathbf{J}^n$ for "jump n": (where $n \in \mathbb{N}$) A path satisfies $\mathbf{J}^n \phi$ i, starting from the current moment, ϕ holds now but also at every n-th steps; for example $\mathbf{J}^2 a$ means that proposition a holds at every even moment along the path.

1. Formalize the semantics of these operators. Let π be a path.

Operator S: we define $\pi \models \phi \mathbf{S} \psi$ by for every $i \in \mathbb{N}$, $\pi \models \psi$ implies there exist $0 \leq j \leq i \leq k$ such that $\pi[j..] \models \phi$ and $\pi[k..] \models \phi$.

Operator $\mathbf{J}^n$: we define $\pi \models \mathbf{J}^n \phi$ by for every $i \in \mathbb{N}$, $\pi[i \times n..] \models \phi$.

2. (*) Argue whether these operators can be expressed in terms of regular LTL or not.

Operator S: $\phi \mathbf{S} \psi \equiv \Box \neg \psi \vee (\neg \psi U (\phi U (\psi U \phi)))$, or something like that.

Operator $\mathbf{J}^n$: It is known that operator $\mathbf{J}^2$ is not expressible in LTL, see Wolper.

Exercise 6

Comment the following claims: are they correct or wrong, or you may need to make them more precise to answer?

1. Every invariant linear-time property is a safety property.
2. For every transition systems $\mathcal{T}$ and $\mathcal{T}'$, $Traces_{fin}(\mathcal{T}) \subseteq Traces_{fin}(\mathcal{T}')$ implies $Traces(\mathcal{T}) \subseteq Traces(\mathcal{T}')$.
3. Every invariant property is regular.
4. The property "Whenever a philosopher eats then he will think some time afterwards" is a safety property.
5. Every Generalized Büchi automaton is equivalent to a Büchi automaton.
6. Let a and b be two atomic propositions. The LTL formulas $\Diamond(a \wedge b)$ and $\Diamond a \wedge \Diamond b$ are equivalent.
7. Let a and b be two atomic propositions. The LTL formula $\Box\Diamond a \rightarrow \Box\Diamond b$ is a weak fairness property.
8. Fairness assumptions are expressible in LTL.
9. If a property is expressible both in CTL and in LTL, then one may use a CTL model checker rather than LTL model checker.
10. There exists an LTL formula whose equivalent Büchi automata all have an exponential size.

See inside the source file.