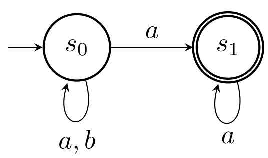
Midterm Exam – Introduction to Verification

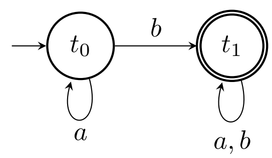
November 10, 2023

Time: 2h. Answers can be given in either French or English. Justify all your answers. All course materials are allowed. *Note: The text of the exercises contains a few corrections given during the exam.*

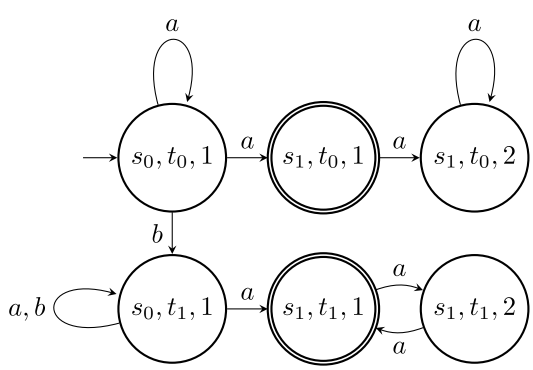
1 LTL and Büchi Automata

(a) Consider the two Büchi automata shown below. Construct a third Büchi automaton accepting the intersection of their languages, using the general Büchi cross product shown in the course.



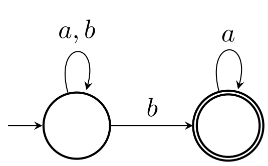


Solution : Applying the systematic construction from the course, one obtains the following automaton (two unreachable states excluded):



(b) Find an automaton equivalent to the result of (a), with as few states as possible.

Solution : A smaller automaton (with an ad-hoc construction) is shown below. Effectively, the second automaton requires at least one b in the word to accept, while the first requires a finite number of b.

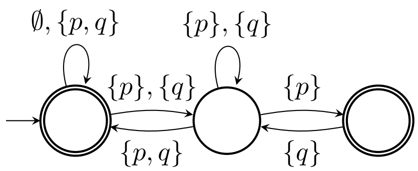


(c) Let $AP = \{p, q\}$ and $\Sigma = 2^{AP}$. Design a Büchi automaton accepting $[\![\phi]\!]$, for the LTL formula $\phi := \mathsf{G}((p \rightarrow (p \,\mathsf{U}\, q)) \wedge (q \rightarrow (q \,\mathsf{U}\, p)))$.

Solution : Notice that the implications $p \rightarrow (p \,\mathsf{U}\, q)$ and $q \rightarrow (q \,\mathsf{U}\, p)$ must be fulfilled in every (infinite) suffix of an accepted sequence.

- Any suffix of the form $\emptyset\Sigma^\omega$ fulfils both implications.
- Any other suffix either contains $\{p, q\}$ or not. If it does, then it must have a prefix of the form $(\{p\} + \{q\})^*\{p, q\}$.
- Moreover, any infinite sequence of the form $(\{p\}+\{q\})^\omega$ fulfils ϕ iff both p and q appear infinitely often iff the factor $\{p\}\{q\}$ appears infinitely often.

With this in mind, one can construct the following automaton:



2 Subclasses of LTL

Eventuality formulae are a subclass of LTL formulae of the following syntax, where ϕ stands for any LTL formula:

$$\alpha ::= \mathsf{F}\,\phi \mid \alpha \vee \alpha \mid \alpha \wedge \alpha \mid \mathsf{X}\,\alpha \mid \phi \,\mathsf{U}\, \alpha \mid \alpha \,\mathsf{R}\, \alpha$$

Alternating formulae are another subclass defined as follows:

$$\beta ::= \mathsf{G}\,\alpha \mid \neg\beta \mid \beta \vee \beta \mid \mathsf{X}\,\beta \mid \phi \,\mathsf{U}\, \beta$$

Let $\Sigma := 2^{AP}$, for some set of atomic propositions AP.

(a) Let α be an eventuality formula, $w \in \Sigma^\omega$, and $0 \leq i \leq j$. Show that $w, j \models \alpha$ implies $w, i \models \alpha$.

Solution : Let α an eventuality formula and $w, j \models \alpha$. We proceed by structural induction:

- If $\alpha = \mathsf{F}\,\phi$, then there exists $k \geq j \geq i$ such that $w, k \models \phi$, hence $w, i \models \mathsf{F}\,\phi$.
- If $\alpha = \mathsf{X}\,\alpha_1$, then $w, j+1 \models \alpha_1$, so by induction $w, i+1 \models \alpha_1$ (since $i+1 \leq j+1$), so $w, i \models \mathsf{X}\,\alpha_1$.
- If $\alpha = \phi \,\mathsf{U}\, \alpha_1$, then in particular there exists $k \geq j \geq i$ such that $w, k \models \alpha_1$, hence $w, i \models \alpha_1$ and trivially $w, i \models \phi \,\mathsf{U}\, \alpha_1$, too.
- For $\alpha = \alpha_1 \,\mathsf{R}\, \alpha_2$, recall that this is equivalent to $(\mathsf{G}\,\alpha_2) \vee (\alpha_2 \,\mathsf{U}\, (\alpha_1 \wedge \alpha_2))$. Either $w, j \models \mathsf{G}\,\alpha_2$, so $w, \ell \models \alpha_2$ for all $\ell \geq j$, thus by induction $w, \ell \models \alpha_2$ for all $i \leq \ell < j$, too; hence $w, i \models \mathsf{G}\,\alpha_2$. Or $w, j \models \alpha_2 \,\mathsf{U}\, (\alpha_1 \wedge \alpha_2)$, then the statement follows directly from the induction hypothesis.
- The cases $\alpha_1 \vee \alpha_2$ and $\alpha_1 \wedge \alpha_2$ are trivial.

(b) Let β be an alternating formula, $w \in \Sigma^\omega$, and $0 \leq i \leq j$. Show that $w, i \models \beta$ iff $w, j \models \beta$.

Solution : Let β be an eventuality formula, we again proceed by structural induction:

- Suppose $\beta = \mathsf{G}\,\alpha$. If $w, i \models \mathsf{G}\,\alpha$, then $w, j \models \mathsf{G}\,\alpha$ is immediate. If $w, j \models \mathsf{G}\,\alpha$, then we get $w, i \models \mathsf{G}\,\alpha$ from (a) on α.
- Suppose $\beta = \phi \mathsf{U} \beta_1$. If $w, i \models \beta$, then there exists $k \geq i$ with $w, k \models \beta_1$, so by induction $w, j \models \beta_1$ (which implies $w, j \models \phi \,\mathsf{U}\, \beta_1$). The case $w, j \models \beta$ is analogous.
- The cases $\neg\beta_1$ or $\beta_1 \vee \beta_2$ are trivial, and for $\mathsf{X}\,\beta_1$ we get it by using the induction hypothesis on β_1, $i+1$, $j+1$.

(c) Let β be an alternating formula and ϕ any LTL formula. Show that β, $\mathsf{X}\,\beta$, $\phi \,\mathsf{U}\, \beta$, and $\phi \,\mathsf{R}\, \beta$ are all equivalent.

Solution : Let γ be any of the four formulae. If $w \models \gamma$, then in all four cases, there exists at least one k such that $w, k \models \beta$ so by (b) $w, i \models \beta$ for all $i \geq 0$. Then $w \models \mathsf{G}\,\beta$, which by definition implies $\phi \,\mathsf{R}\, \beta$. Also, from $w, 0 \models \beta$ we get $w \models \beta \wedge (\phi \,\mathsf{U}\, \beta)$, and from $w, 1 \models \beta$ we get $w \models \mathsf{X}\,\beta$.

3 CTL and CTL*

For any $n \geq 1$, we define a CTL* formula $\phi_n := \mathsf{A}((\mathsf{X}^n\, p) \vee (\mathsf{F}\, q))$.

(a) Find a CTL formula ψ_1 equivalent to ϕ_1.

Solution : $\psi_1 = q \vee \mathsf{AX}(p \vee \mathsf{AF}\, q)$.

(b) Generally for $n > 1$, find a CTL formula ψ_n equivalent to ϕ_n.

Solution : Every path must either contain a p-state after n steps or a q-state anywhere. In branches that contain a q-state before n steps, we no longer need to check for p. With that in mind, and with ψ_1 from (a), we set $\psi_n = q \vee \mathsf{AX}\,\psi_{n-1}$.

(c) Prove or refute that the CTL* formula $\phi := \mathsf{A}((\mathsf{X}\, p) \vee (p \,\mathsf{U}\, q))$ can be expressed in CTL.

All paths must either satisfy $\mathsf{X}\, p$ or $p \,\mathsf{U}\, q$. We make a case distinction:

(i) Either we start with a q-state, in which case $p \,\mathsf{U}\, q$ holds.

(ii) Or we start with a p-state. Then for $p \,\mathsf{U}\, q$, the following state must in particular satisfy p or q. If p holds, the path also satisfies $\mathsf{X}\, p$, if q holds, it satisfies $p \,\mathsf{U}\, q$; in either case we are done.

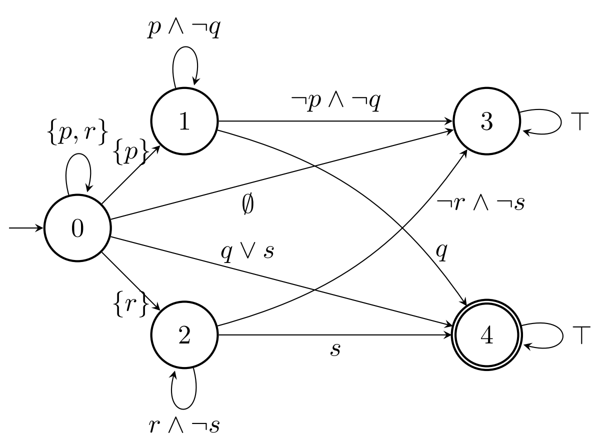
(iii) If we start in a non-p and non-q-state, then no path can satisfy $p \,\mathsf{U}\, q$, and all successors must be p-states.

Each of these three cases translates into a CTL formula, we take their disjunction:

$$q \vee (p \wedge \mathsf{AX}(p \vee q)) \vee \mathsf{AX}\, p$$

(d) Prove or refute that the CTL* formula $\phi' := \mathsf{A}((p \,\mathsf{U}\, q) \vee (r \,\mathsf{U}\, s))$ can be expressed in CTL.

Solution : The formula inside the A-quantifier is a pure LTL formula, call it ψ. For the following, it helps to imagine the following Büchi automaton (BA) for ψ:



(Note: Some edges use set notation where it is more compact, e. g., $\{p, r\}$ means $p \wedge \neg q \wedge r \wedge \neg s$. We shall use the same abbreviations in the formulae below.)

Since this BA is deterministic and complete and its only accepting state is a sink, we can exceptionally obtain its complement by swapping accepting and non-accepting states. We then wish to state that there exists no path that terminally stays in states 0, 1, 2, or 3. A CTL formula equivalent to ϕ' is then $\neg(\chi_0 \vee \chi_1 \vee \chi_2 \vee \chi_{0,3} \vee \chi_{1,3} \vee \chi_{2,3})$, where:

- $\chi_0 := \mathsf{EG}\{p,r\}$;
- $\chi_1 := \{p,r\}\ \mathsf{EU}\ (\{p\} \wedge \mathsf{EX}\,\mathsf{EG}(p \wedge \neg q))$;
- $\chi_2 := \{p,r\}\ \mathsf{EU}\ (\{r\} \wedge \mathsf{EX}\,\mathsf{EG}(r \wedge \neg s))$;
- $\chi_{0,3} := \{p,r\}\ \mathsf{EU}\ \emptyset$;
- $\chi_{1,3} := \{p,r\}\ \mathsf{EU}\ (\{p\} \wedge \mathsf{EX}(\neg q\ \mathsf{EU}\ (\neg p \wedge \neg q))$;
- $\chi_{2,3} := \{p,r\}\ \mathsf{EU}\ (\{r\} \wedge \mathsf{EX}(\neg s\ \mathsf{EU}\ (\neg r \wedge \neg s))$.

Note that by using the "weak until" modality EW, we can summarize $\chi_0 \vee \chi_1 \vee \chi_{1,3}$ by τ_1 and likewise $\chi_0 \vee \chi_2 \vee \chi_{2,3}$ by τ_2 as follows:

- $\tau_1 := \{p,r\}\ \mathsf{EW}\ (\{p\} \wedge \mathsf{EX}(\neg q\ \mathsf{EW}\ (\neg p \wedge \neg q)))$;
- $\tau_2 := \{p,r\}\ \mathsf{EW}\ (\{r\} \wedge \mathsf{EX}(\neg s\ \mathsf{EW}\ (\neg r \wedge \neg s)))$.

An alternative CTL formula equivalent to ϕ' would therefore be

$$\neg(\{p,r\}\ \mathsf{EW}\ (\emptyset \vee (\{p\} \wedge \mathsf{EX}(\neg q\ \mathsf{EW}\ (\neg p \wedge \neg q))) \vee (\{r\} \wedge \mathsf{EX}(\neg s\ \mathsf{EW}\ (\neg r \wedge \neg s))).$$

And if one also allows the release operator ER, one can shorten the above to:

$$\neg(\{p,r\}\ \mathsf{EW}\ (\emptyset \vee (\{p\} \wedge \mathsf{EX}(\neg p\ \mathsf{ER}\ \neg q)) \vee (\{r\} \wedge \mathsf{EX}(\neg r\ \mathsf{ER}\ \neg s))).$$

4 ω-automata

An ω-*automaton* is a tuple $\langle \Sigma, S, s_0, \Delta, \mathcal{F} \rangle$, where Σ is a finite alphabet, S is a finite set of states, s_0 the initial state, and $\Delta \subseteq S \times \Sigma \times S$ the transitions, with the usual notions. $\mathcal{F}$ is an *acceptance condition*, to be clarified below. For a run $\rho \in S^\omega$, we note $\mathit{Inf}(\rho) = \{\, s \mid \forall i \exists j \geq i : \rho(i) = s \,\}$ the set of states occurring infinitely often in ρ.

The following types of ω-automata were shown to be equivalent in the course and exercises:

- Büchi automata (BA) with $\mathcal{F} \subseteq S$, where a run ρ is accepted if $\mathit{Inf}(\rho) \cap \mathcal{F} \neq \emptyset$;
- generalized BA (GBA) with $\mathcal{F} \subseteq 2^S$, where ρ is accepted if $\forall F \in \mathcal{F} : \mathit{Inf}(\rho) \cap F \neq \emptyset$;

We consider the following additional types of ω-automaton:

- Parity automata (PA), where $\mathcal{F} = \langle F_0, F_1, \ldots, F_k \rangle$ (for some $k \geq 1$), where $F_0, \ldots, F_k$ are a partition of S; a run ρ is accepted if the maximal n such that $\mathit{Inf}(\rho)$ intersects F_n is even.
- Muller automata (MA) with $\mathcal{F} \subseteq 2^S$, where ρ is accepted if $\mathit{Inf}(\rho) \in \mathcal{F}$.

(a) Show that PA are equivalent to BA, i.e. for every PA one can construct a BA accepting the same language, and vice versa.

Solution : Given a BA $\langle \Sigma, S, s_0, \Delta, F \rangle$, an equivalent PA is $\langle \Sigma, S, s_0, \Delta, \langle \emptyset, S \setminus F, F \rangle \rangle$.

Let $\mathcal{P} := \langle \Sigma, S, s_0, \Delta, \mathcal{F} \rangle$ be a PA, with $\mathcal{F} = \langle F_0, \ldots, F_{2k+1} \rangle$ for some $k \geq 0$. (If the highest index in $\mathcal{F}$ was even, we could always add an additional empty set to reach an odd number.) Suppose that in a run ρ, n is the highest index such that $\mathit{Inf}(\rho)$ intersects F_n. Then all sets with higher indices will stop occurring after some time. So we will build an equivalent BA $\mathcal{B}$ that has all the states from $\mathcal{P}$ and $k+1$ additional copies of $\mathcal{P}$. At any point, the automaton can transition to the j-th copy (for any $0 \leq j \leq k$), however movement in the j-th copy is restricted to states up to index $2j$ (with states from F_{2j} being accepting. Formally, $\mathcal{B} = \langle \Sigma, Q, s_0, \Delta', F \rangle$, where:

- $Q = S \cup (S \times \{0, \ldots, k\})$;
- $F = \bigcup_{j=0}^{k} (F_{2j} \times \{j\})$;
- $\Delta' := \Delta \cup \Delta_t \cup \bigcup_{j=0}^{k} \Delta_j$, where

– $\Delta_t = \{ \langle s, a, \langle s', j \rangle \rangle \mid \langle s, a, s' \rangle \in \Delta,\ 0 \leq j \leq k \}$;
– $\Delta_j = \{ \langle \langle s, j \rangle, a, \langle s', j \rangle \rangle \mid \langle s, a, s' \rangle \in \Delta,\ s, s' \in F_0 \cup \cdots \cup F_{2j} \}$

(Note: In each copy of $\mathcal{P}$ there will be some useless states (whose index is too high), in which the computation will get stuck; it was simply easier to write it up like this.)

(b) Same question for MA. *Hint:* In an MA, it may be useful to say that $\mathcal{F} = \{F_1, \ldots, F_n\}$ for some n, and that every $F_i = \{q_{i,1}, \ldots, q_{i,k_i}\}$, for every $1 \leq i \leq n$ and some $k_i \geq 1$.

Solution : Given a BA $\langle \Sigma, S, s_0, \Delta, F \rangle$, an equivalent MA is $\langle \Sigma, S, s_0, \Delta, \mathcal{F}' \rangle$, where $\mathcal{F}'$ contains every subset of S that intersects F.

If $\mathcal{M}$ is an MA (with the form above), it is easiest to construct a GBA $\mathcal{B}_i$ for each $1 \leq i \leq n$, which accepts the runs ρ such that $\mathit{Inf}(\rho) = F_i$ in $\mathcal{M}$. Then one exploits that GBA=BA and that BA are closed under union.

$\mathcal{B}_i$ consists of two copies of $\mathcal{M}$, where we can go to the second copy when no more states from $S \setminus F_i$ will occur. The acceptance condition then assures that all states of F_i will occur in the second copy. Formally, $\mathcal{B}_i = \langle \Sigma, S \times \{0, 1\}, \langle s_0, 0 \rangle, \Delta', \mathcal{F}' \rangle$, where:

- $\Delta' = \{ \langle \langle s, b \rangle, a, \langle s', b' \rangle \rangle \mid \langle s, a, s' \rangle \in \Delta \wedge (b = 0 \vee b' = 1) \wedge (b = 1 \Rightarrow s \in F_i) \}$;
- $\mathcal{F}' = \langle \{ \langle q_{i,1}, 1 \rangle \}, \ldots, \{ \langle q_{i,k_i}, 1 \rangle \} \rangle$

Note: Again, for simplicity, there are some superfluous states in the second copy from which no movement is possible.