Correctness of $\mathcal{A}_\varphi$

Proposition: $\mathcal{L}(\varphi) \subseteq \mathcal{L}(\mathcal{A}_\varphi)$

Lemma:

Let $\rho = Y_0 \xrightarrow{a_0} Y_1 \xrightarrow{a_1} Y_2 \cdots$ be an accepting run of $\mathcal{A}_\varphi$ on $u = a_0 a_1 a_2 \cdots \in \Sigma^\omega$.

Then, for all $\psi \in \mathrm{sub}(\varphi)$ and $n \geq 0$,
for all reduction path $Y_n \xrightarrow[*]{\varepsilon} Y \xrightarrow[*]{\varepsilon} Z$ with $a_n \in \Sigma_Z$ and $Y_{n+1} = \mathrm{next}(Z)$,

$$\psi \in Y \implies u, n \models \psi$$

Corollary: $\mathcal{L}(\mathcal{A}_\varphi) \subseteq \mathcal{L}(\varphi)$

$\mathcal{L}(\varphi) \subseteq \mathcal{L}(\mathcal{A}_\varphi)$

Proof:

Let $u = a_0 a_1 a_2 \cdots \in \Sigma^\omega$ be such that $u, 0 \models \varphi$. By induction, we build a run

$$\rho = Y_0 \xrightarrow{a_0} Y_1 \xrightarrow{a_1} Y_2 \cdots$$

We start with $Y_0 = \{\varphi\}$. Assume that $u, n \models \bigwedge Y_n$ for some $n \geq 0$. By Lemma [Soundness], there is $Z_n \in \mathrm{Red}(Y_n)$ such that $u, n \models \bigwedge Z_n$ and for all until subformulae $\alpha = \alpha_1 \,\mathsf{U}\, \alpha_2 \in \mathsf{U}(\varphi)$, if $u, n \models \alpha_2$ then $Z_n \in \mathrm{Red}_\alpha(Y_n)$. Then we define $Y_{n+1} = \mathrm{next}(Z_n)$. Since $u, n \models \bigwedge Z_n$, Lemma [Next Step] implies $a_n \in \Sigma_{Z_n}$ and $u, n+1 \models \bigwedge Y_{n+1}$. Therefore, ρ is a run for u in $\mathcal{A}_\varphi$.
It remains to show that ρ is successful. By definition, it starts from the initial state $\{\varphi\}$. Now let $\alpha = \alpha_1 \,\mathsf{U}\, \alpha_2 \in \mathsf{U}(\varphi)$. Assume there exists $N \geq 0$ such that $Y_n \xrightarrow{a_n} Y_{n+1} \notin T_\alpha$ for all $n \geq N$. Then $Z_n \notin \mathrm{Red}_\alpha(Y_n)$ for all $n \geq N$ and we deduce that $u, n \not\models \alpha_2$ for all $n \geq N$. But, since $Z_N \notin \mathrm{Red}_\alpha(Y_N)$, the formula α has been reduced using an ε-transition marked $!\alpha$ along the path from Y_N to Z_N. Therefore, $\mathsf{X}\,\alpha \in Z_N$ and $\alpha \in Y_{N+1}$. By construction of the run we have $u, N+1 \models \bigwedge Y_{N+1}$. Hence, $u, N+1 \models \alpha$, a contradiction with $u, n \not\models \alpha_2$ for all $n \geq N$. Consequently, the run ρ is successful and u is accepted by $\mathcal{A}_\varphi$.

$\mathcal{L}(\mathcal{A}_\varphi) \subseteq \mathcal{L}(\varphi)$

Lemma:

Let $\rho = Y_0 \xrightarrow{a_0} Y_1 \xrightarrow{a_1} Y_2 \cdots$ be an accepting run of $\mathcal{A}_\varphi$ on $u = a_0 a_1 a_2 \cdots \in \Sigma^\omega$.

Then, for all $\psi \in \mathrm{sub}(\varphi)$ and $n \geq 0$,
for all reduction path $Y_n \xrightarrow[*]{\varepsilon} Y \xrightarrow[*]{\varepsilon} Z$ with $a_n \in \Sigma_Z$ and $Y_{n+1} = \mathrm{next}(Z)$,

$$\psi \in Y \implies u, n \models \psi$$

Proof: by induction on ψ

- $\psi = \top$. The result is trivial.
- $\psi = p \in \mathrm{AP}(\varphi)$. Since p is reduced, we have $p \in Z$ and it follows $\Sigma_Z \subseteq \Sigma_p$. Therefore, $p \in a_n$ and $u, n \models p$. The proof is similar if $\psi = \neg p$ for some $p \in \mathrm{AP}(\varphi)$.
- $\psi = \mathsf{X}\,\psi_1$. Then $\psi \in Z$ and $\psi_1 \in Y_{n+1}$. By induction we obtain $u, n+1 \models \psi_1$ and we deduce $u, n \models \mathsf{X}\,\psi_1 = \psi$.
- $\psi = \psi_1 \wedge \psi_2$. Along the path $Y \xrightarrow[*]{\varepsilon} Z$ the formula ψ must be reduced so $Y \xrightarrow[*]{\varepsilon} Y' \xrightarrow[*]{\varepsilon} Z$ with $\psi_1, \psi_2 \in Y'$. By induction, we obtain $u, n \models \psi_1$ and $u, n \models \psi_2$. Hence, $u, n \models \psi$. The proof is similar for $\psi = \psi_1 \vee \psi_2$.

$\mathcal{L}(\mathcal{A}_\varphi) \subseteq \mathcal{L}(\varphi)$

Proof:

- $\psi = \psi_1 \,\mathsf{U}\, \psi_2$. Along the path $Y \xrightarrow[*]{\varepsilon} Z$ the formula ψ must be reduced so $Y \xrightarrow[*]{\varepsilon} Y' \xrightarrow{\varepsilon} Y'' \xrightarrow[*]{\varepsilon} Z$ with either $Y'' = Y' \setminus \{\psi\} \cup \{\psi_2\}$ or $Y'' = Y' \setminus \{\psi\} \cup \{\psi_1, \mathsf{X}\,\psi\}$. In the first case, we obtain by induction $u, n \models \psi_2$ and therefore $u, n \models \psi$. In the second case, we obtain by induction $u, n \models \psi_1$. Since $\mathsf{X}\,\psi$ is reduced we get $\mathsf{X}\,\psi \in Z$ and $\psi \in \mathrm{next}(Z) = Y_{n+1}$.

Let $k > n$ be minimal such that $Y_k \xrightarrow{a_k} Y_{k+1} \in T_\psi$ (such a value k exists since ρ is accepting). We first show by induction that $u, i \models \psi_1$ and $\psi \in Y_{i+1}$ for all $n \leq i < k$. Recall that $u, n \models \psi_1$ and $\psi \in Y_{n+1}$. So let $n < i < k$ be such that $\psi \in Y_i$. Let $Z' \in \mathrm{Red}(Y_i)$ be such that $a_i \in \Sigma_{Z'}$ and $Y_{i+1} = \mathrm{next}(Z')$. Since k is minimal we know that $Z' \notin \mathrm{Red}_\psi(Y_i)$. Hence, along any reduction path from Y_i to Z' we must use a step $Y' \xrightarrow[!\psi]{\varepsilon} Y' \setminus \{\psi\} \cup \{\psi_1, \mathsf{X}\,\psi\}$. By induction on the formula we obtain $u, i \models \psi_1$. Also, since $\mathsf{X}\,\psi$ is reduced, we have $\mathsf{X}\,\psi \in Z'$ and $\psi \in \mathrm{next}(Z') = Y_{i+1}$.

Second, we show that $u, k \models \psi_2$. Since $Y_k \xrightarrow{a_k} Y_{k+1} \in T_\psi$, we find some $Z' \in \mathrm{Red}_\psi(Y_k)$ such that $a_k \in \Sigma_{Z'}$ and $Y_{k+1} = \mathrm{next}(Z')$. Since $\psi \in Y_k$, along some reduction path from Y_k to Z' we use a step $Y' \xrightarrow{\varepsilon} Y' \setminus \{\psi\} \cup \{\psi_2\}$. By induction we obtain $u, k \models \psi_2$. Finally, we have shown $u, n \models \psi_1 \,\mathsf{U}\, \psi_2 = \psi$.

$\mathcal{L}(\mathcal{A}_\varphi) \subseteq \mathcal{L}(\varphi)$

Proof:

• $\psi = \psi_1 \mathsf{R}\, \psi_2$. Along the path $Y \xrightarrow[*]{\varepsilon} Z$ the formula ψ must be reduced so $Y \xrightarrow[*]{\varepsilon} Y' \xrightarrow{\varepsilon} Y'' \xrightarrow[*]{\varepsilon} Z$ with either $Y'' = Y' \setminus \{\psi\} \cup \{\psi_1, \psi_2\}$ or $Y'' = Y' \setminus \{\psi\} \cup \{\psi_2, \mathsf{X}\,\psi\}$. In the first case, we obtain by induction $u, n \models \psi_1$ and $u, n \models \psi_2$. Hence, $u, n \models \psi$ and we are done. In the second case, we obtain by induction $u, n \models \psi_2$ and we get also $\psi \in Y_{n+1}$. Continuing with the same reasoning, we deduce easily that either $u, n \models \mathsf{G}\,\psi_2$ or $u, n \models \psi_2 \,\mathsf{U}\, (\psi_1 \wedge \psi_2)$.

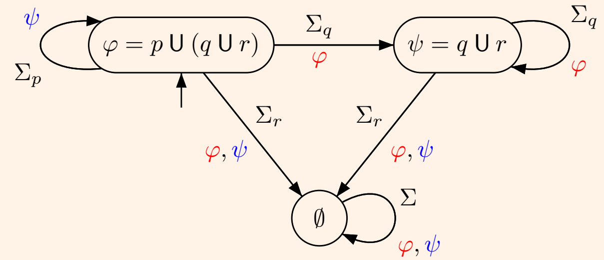
Example with two until sub-formulae

Example: Nested until: $\varphi = p \,\mathsf{U}\, \psi$ with $\psi = q \,\mathsf{U}\, r$

$\mathrm{Red}(\{\varphi\}) = \{\{p, \mathsf{X}\,\varphi\}, \{q, \mathsf{X}\,\psi\}, \{r\}\}$ $\quad$ $\mathrm{Red}(\{\psi\}) = \{\{q, \mathsf{X}\,\psi\}, \{r\}\}$

$\mathrm{Red}_\varphi(\{\varphi\}) = \{\{q, \mathsf{X}\,\psi\}, \{r\}\}$ $\quad$ $\mathrm{Red}_\varphi(\{\psi\}) = \{\{q, \mathsf{X}\,\psi\}, \{r\}\}$

$\mathrm{Red}_\psi(\{\varphi\}) = \{\{p, \mathsf{X}\,\varphi\}, \{r\}\}$ $\quad$ $\mathrm{Red}_\psi(\{\psi\}) = \{\{r\}\}$



Satisfiability and Model Checking

Corollary: PSPACE upper bound for satisfiability and model checking

- Let $\varphi \in \mathrm{LTL}$, we can check whether φ is satisfiable (or valid) in space polynomial in $|\varphi|$.
- Let $\varphi \in \mathrm{LTL}$ and $M = (S, T, I, \mathrm{AP}, \ell)$ be a Kripke structure. We can check whether $M \models_\forall \varphi$ (or $M \models_\exists \varphi$) in space polynomial in $|\varphi| + \log |M|$.

Proof:

For $M \models_\forall \varphi$ we construct a synchronized product $M \otimes \mathcal{A}_{\neg\varphi}$:

Transitions: $\dfrac{s \to s' \in M \quad \wedge \quad Y \xrightarrow{\ell(s)} Y' \in \mathcal{A}_{\neg\varphi}}{(s, Y) \xrightarrow{\ell(s)} (s', Y')}$

Initial states: $I \times \{\{\neg\varphi\}\}$.

Acceptance conditions: inherited from $\mathcal{A}_{\neg\varphi}$.

Check $M \otimes \mathcal{A}_{\neg\varphi}$ for emptiness.

On the fly simplifications $\mathcal{A}_\varphi$

Built-in: reduction of a maximal formula.

Definition: Additional reduction rules

If $\bigwedge Y \equiv \bigwedge Y'$ then we may use $Y \xrightarrow{\varepsilon} Y'$.

Remark: checking equivalence is as hard as building the automaton.
Hence we only use syntactic equivalences.

If $\psi = \psi_1 \vee \psi_2$ and $\psi_1 \in Y$ or $\psi_2 \in Y$: $\quad Y \xrightarrow{\varepsilon} Y \setminus \{\psi\}$

If $\psi = \psi_1 \,\mathsf{U}\, \psi_2$ and $\psi_2 \in Y$: $\quad Y \xrightarrow{\varepsilon} Y \setminus \{\psi\}$

If $\psi = \psi_1 \,\mathsf{R}\, \psi_2$ and $\psi_1 \in Y$: $\quad Y \xrightarrow{\varepsilon} Y \setminus \{\psi\} \cup \{\psi_2\}$

On the fly simplifications $\mathcal{A}_\varphi$

Definition: Merging equivalent states

Let A $= (Q, \Sigma, I, T, T_1, \dots, T_n)$ and $s_1, s_2 \in Q$.
We can merge s_1 and s_2 if they have the same outgoing transitions:
$\forall a \in \Sigma$, $\forall s \in Q$,

$$(s_1, a, s) \in T \iff (s_2, a, s) \in T$$
$$\text{and} \qquad (s_1, a, s) \in T_i \iff (s_2, a, s) \in T_i \qquad \text{for all } 1 \le i \le n.$$

Remark: Sufficient condition

Two states Y, Y' of $\mathcal{A}_\varphi$ have the same outgoing transition if

$$\mathrm{Red}(Y) = \mathrm{Red}(Y')$$
$$\text{and} \qquad \mathrm{Red}_\alpha(Y) = \mathrm{Red}_\alpha(Y') \qquad \text{for all } \alpha \in \mathsf{U}(\varphi).$$

Example: Let $\varphi = \mathsf{G}\,\mathsf{F}\,p \wedge \mathsf{G}\,\mathsf{F}\,q$.

Without merging states $\mathcal{A}_\varphi$ has 4 states.
These 4 states have the same outgoing transitions.
The simplified automaton has only one state.

Other constructions

- Tableau construction. See for instance [9, Wolper 85]
  + : Easy definition, easy proof of correctness
  + : Works both for future and past modalities
  − : Inefficient without optimizations
- Using Very Weak Alternating Automata [10, Gastin & Oddoux 01].
  + : Very efficient
  − : Only for future modalities
  Online tool: `http://www.lsv.ens-cachan.fr/~gastin/ltl2ba/`
- The domain is still very active.
- See other references in [6, Demri & Gastin 10].

$\mathrm{MC}^\exists(\mathsf{X},\mathsf{U}) \le_P \mathrm{SAT}(\mathsf{X},\mathsf{U})$ [11, Sistla & Clarke 85]

Let $M = (S, T, I, \mathrm{AP}, \ell)$ be a Kripke structure and $\varphi \in \mathrm{LTL}(\mathrm{AP}, \mathsf{X}, \mathsf{U})$

Introduce new atomic propositions: $\mathrm{AP}_S = \{\mathrm{at}_s \mid s \in S\}$
Define $\mathrm{AP}' = \mathrm{AP} \uplus \mathrm{AP}_S \qquad \Sigma' = 2^{\mathrm{AP}'} \qquad \pi : \Sigma'^\omega \to \Sigma^\omega$ by $\pi(a) = a \cap \mathrm{AP}$.

Let $w \in \Sigma'^\omega$. We have $w \models \varphi$ iff $\pi(w) \models \varphi$

Define $\psi_M \in \mathrm{LTL}(\mathrm{AP}', \mathsf{X}, \mathsf{F})$ of size $\mathcal{O}(|M|^2)$ by

$$\psi_M = \left(\bigvee_{s \in I} \mathrm{at}_s\right) \wedge \mathsf{G}\left(\bigvee_{s \in S}\left(\mathrm{at}_s \wedge \bigwedge_{t \ne s} \neg \mathrm{at}_t \wedge \bigwedge_{p \in \ell(s)} p \wedge \bigwedge_{p \notin \ell(s)} \neg p \wedge \bigvee_{t \in T(s)} \mathsf{X}\,\mathrm{at}_t\right)\right)$$

Let $w = a_0 a_1 a_2 \cdots \in \Sigma'^\omega$. Then, $w \models \psi_M$ iff there exists an initial infinite run σ of M such that $\pi(w) = \ell(\sigma)$ and $a_i \cap \mathrm{AP}_S = \{\mathrm{at}_{s_i}\}$ for all $i \ge 0$.

Therefore, $M \models_\exists \varphi$ iff $\psi_M \wedge \varphi$ is satisfiable
$M \models_\forall \varphi$ iff $\psi_M \wedge \neg\varphi$ is not satisfiable

Remark: we also have $\mathrm{MC}^\exists(\mathsf{X},\mathsf{F}) \le_P \mathrm{SAT}(\mathsf{X},\mathsf{F})$.

QBF Quantified Boolean Formulae

Definition: QBF

Input: A formula $\gamma = Q_1 x_1 \cdots Q_n x_n \gamma'$ with $\gamma' = \bigwedge_{1 \le i \le m} \bigvee_{1 \le j \le k_i} a_{ij}$
$Q_i \in \{\forall, \exists\}$ and $a_{ij} \in \{x_1, \neg x_1, \dots, x_n, \neg x_n\}$.

Question: Is γ valid?

Definition:

An assignment of the variables $\{x_1, \dots, x_n\}$ is a word $v = v_1 \cdots v_n \in \{0,1\}^n$.
We write $v[i]$ for the prefix of length i.
Let $V \subseteq \{0,1\}^n$ be a set of assignments.

- V is valid (for γ') if $v \models \gamma'$ for all $v \in V$,
- V is closed (for γ) if $\forall v \in V$, $\forall 1 \le i \le n$ s.t. $Q_i = \forall$,
  $\exists v' \in V$ s.t. $v[i-1] = v'[i-1]$ and $\{v_i, v'_i\} = \{0, 1\}$.

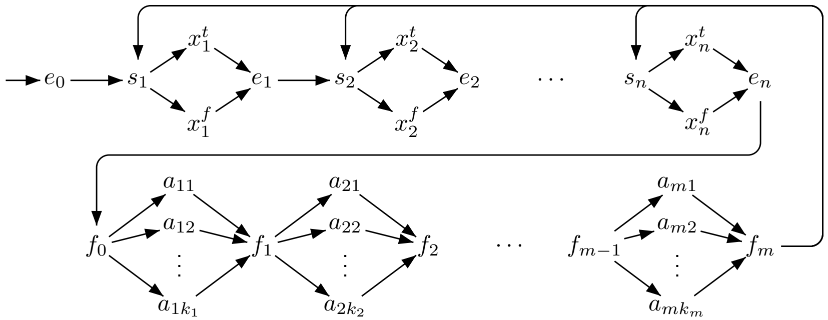
Proposition:

γ is valid iff $\exists V \subseteq \{0,1\}^n$ s.t. V is nonempty valid and closed

$\mathrm{QBF} \leq_P \mathrm{MC}^{\exists}(\mathsf{U})$ [11, Sistla & Clarke 85]

Let $\gamma = Q_1 x_1 \cdots Q_n x_n \bigwedge_{1\leq i\leq m} \bigvee_{1\leq j\leq k_i} a_{ij}$ with $Q_i \in \{\forall, \exists\}$ and a_{ij} literals.

Consider the KS M:



Let $\psi_{ij} = \begin{cases} \mathsf{G}(x_k^f \to s_k \mathrel{\mathsf{R}} \neg a_{ij}) & \text{if } a_{ij} = x_k \\ \mathsf{G}(x_k^t \to s_k \mathrel{\mathsf{R}} \neg a_{ij}) & \text{if } a_{ij} = \neg x_k \end{cases}$ and $\psi = \bigwedge_{i,j} \psi_{ij}$.

Let $\varphi_j = \mathsf{G}(e_{j-1} \to (\neg s_{j-1} \mathrel{\mathsf{U}} x_j^t) \wedge (\neg s_{j-1} \mathrel{\mathsf{U}} x_j^f))$ and $\varphi = \bigwedge_{j \mid Q_j = \forall} \varphi_j$.

Then, γ is valid iff $M \models_{\exists} \psi \wedge \varphi$.

$\mathrm{QBF} \leq_P \mathrm{MC}^{\exists}(\mathsf{U})$ [11, Sistla & Clarke 85]

Proof: If $M \models_{\exists} \psi \wedge \varphi$ then γ is valid

Each finite path $\tau = e_0 \xrightarrow{*} f_m$ in M defines a valuation v^τ by:

$$v_k^\tau = \begin{cases} 1 & \text{if } \tau, |\tau| \models \neg s_k \mathrel{\mathsf{S}} x_k^t \\ 0 & \text{if } \tau, |\tau| \models \neg s_k \mathrel{\mathsf{S}} x_k^f \end{cases}$$

Let σ be an initial infinite path of M s.t. $\sigma, 0 \models \psi \wedge \varphi$.
Let $V = \{v^\tau \mid \tau = e_0 \xrightarrow{*} f_m \text{ is a prefix of } \sigma\}$.

Claim: V is nonempty, valid and closed.

$\mathrm{QBF} \leq_P \mathrm{MC}^{\exists}(\mathsf{U})$ [11, Sistla & Clarke 85]

Proof: If γ is valid then $M \models_{\exists} \psi \wedge \varphi$

Let $V \subseteq \{0,1\}^n$ be nonempty, valid and closed.

First ingredient: extension of a run.
Assume $\tau = e_0 \xrightarrow{*} f_m$ satisfies $v^\tau \in V$ and $\tau, 0 \models \psi$.
Let $1 \leq i \leq n$ with $Q_i = \forall$.
Let $v' \in V$ s.t. $v'[i-1] = v[i-1]$ and $\{v_i, v'_i\} = \{0,1\}$.
We can extend τ in $\tau' = \tau \to s_i \xrightarrow{*} e_n \to f_0 \xrightarrow{*} f_m$ with $v^{\tau'} = v'$ and $\tau', 0 \models \psi$.
We say that τ' is an extension of τ wrt. i

Second step: the sequence of indices for the extensions.
Let $1 \leq i_\ell < \cdots < i_1 \leq n$ be the indices of universal quantifications ($Q_{i_j} = \forall$).
Define by induction $w_1 = i_1$ and if $k < \ell$, $w_{k+1} = w_k i_{k+1} w_k$. Let $w = (w_\ell 1)^\omega$.

Final step: the infinite run.
Let $v \in V \neq \emptyset$ and let $\tau = e_0 \xrightarrow{*} f_m$ with $v^\tau \in V$ and $\tau, 0 \models \psi$.
We build an infinite run σ by extending τ inductively wrt. the sequence of indices defined by w.

Claim: $\sigma, 0 \models \psi \wedge \varphi$.

Complexity of LTL

Theorem: Complexity of LTL

The following problems are PSPACE-complete:

- $\mathrm{SAT}(\mathrm{LTL}(\mathsf{X},\mathsf{U},\mathsf{Y},\mathsf{S}))$, $\mathrm{MC}^{\forall}(\mathrm{LTL}(\mathsf{X},\mathsf{U},\mathsf{Y},\mathsf{S}))$, $\mathrm{MC}^{\exists}(\mathrm{LTL}(\mathsf{X},\mathsf{U},\mathsf{Y},\mathsf{S}))$
- $\mathrm{SAT}(\mathrm{LTL}(\mathsf{X},\mathsf{F}))$, $\mathrm{MC}^{\forall}(\mathrm{LTL}(\mathsf{X},\mathsf{F}))$, $\mathrm{MC}^{\exists}(\mathrm{LTL}(\mathsf{X},\mathsf{F}))$
- $\mathrm{SAT}(\mathrm{LTL}(\mathsf{U}))$, $\mathrm{MC}^{\forall}(\mathrm{LTL}(\mathsf{U}))$, $\mathrm{MC}^{\exists}(\mathrm{LTL}(\mathsf{U}))$
- The restriction of the above problems to a unique propositional variable

The following problems are NP-complete:

- $\mathrm{SAT}(\mathrm{LTL}(\mathsf{F}))$, $\mathrm{MC}^{\exists}(\mathrm{LTL}(\mathsf{F}))$