Büchi automata with output

Definition: SBT: Synchronous (letter to letter) Büchi transducer

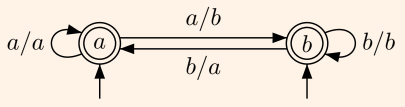
Let A and B be two alphabets.
A synchronous Büchi transducer from A to B is a tuple $\mathcal{A} = (Q, A, I, T, F, \mu)$ where (Q, A, I, T, F) is a Büchi automaton (input) and $\mu : T \to B$ is the output function.
It computes the relation

$$[\![\mathcal{A}]\!] = \{(u, v) \in A^\omega \times B^\omega \mid \exists\, \rho = q_0, a_0, q_1, a_1, q_2, a_2, q_3, \ldots \text{ accepting run with } u = a_0 a_1 a_2 \cdots \text{ and } v = \mu(\rho), \text{ i.e., } v = b_0 b_1 b_2 \cdots \text{ with } b_i = \mu(q_i, a_i, q_{i+1}) \text{ for } i \geq 0\}$$

If (Q, A, I, T, F) is unambiguous then $[\![\mathcal{A}]\!] : A^\omega \to B^\omega$ is a (partial) function, in which case we also write $[\![\mathcal{A}]\!](u) = v$ for $(u, v) \in [\![\mathcal{A}]\!]$.

We will also use SGBT: synchronous transducers with generalized Büchi acceptance.

Example: Left shift with $A = B = \{a, b\}$



Composition of Büchi transducers

Definition: Composition

Let A, B, C be alphabets.
Let $\mathcal{A} = (Q, A, I, T, (F_i)_i, \mu)$ be an SGBT from A to B.
Let $\mathcal{A}' = (Q', B, I', T', (F'_j)_j, \mu')$ be an SGBT from B to C.
Then $\mathcal{A} \cdot \mathcal{A}' = (Q \times Q', A, I \times I', T'', (F_i \times Q')_i, (Q \times F'_j)_j, \mu'')$ defined by:

$$\tau'' = (p, p') \xrightarrow{a} (q, q') \in T'' \text{ and } \mu''(\tau'') = c$$

iff

$$\tau = p \xrightarrow{a} q \in T \text{ and } \tau' = p' \xrightarrow{\mu(\tau)} q' \in T' \text{ and } c = \mu'(\tau')$$

is an SGBT from A to C.
When the transducers define functions, we also denote the composition by $\mathcal{A}' \circ \mathcal{A}$.

Proposition: Composition

1. We have $[\![\mathcal{A} \cdot \mathcal{A}']\!] = [\![\mathcal{A}]\!] \cdot [\![\mathcal{A}']\!]$.
2. If $(Q, A, I, T, (F_i)_i)$ and $(Q', B, I', T', (F'_j)_j)$ are unambiguous (resp. prophetic) then $(Q \times Q', A, I \times I', T'', (F_i \times Q')_i, (Q \times F'_j)_j)$ is also unambiguous (resp. prophetic), and
$\forall u \in A^\omega$ we have $[\![\mathcal{A}' \circ \mathcal{A}]\!](u) = [\![\mathcal{A}']\!]([\![\mathcal{A}]\!](u))$.

Product of Büchi transducers

Definition: Product

Let A, B, C be alphabets.
Let $\mathcal{A} = (Q, A, I, T, (F_i)_i, \mu)$ be an SGBT from A to B.
Let $\mathcal{A}' = (Q', A, I', T', (F'_j)_j, \mu')$ be an SGBT from A to C.
Then $\mathcal{A} \times \mathcal{A}' = (Q \times Q', A, I \times I', T'', (F_i \times Q')_i, (Q \times F'_j)_j, \mu'')$ defined by:

$$\tau'' = (p, p') \xrightarrow{a} (q, q') \in T'' \text{ and } \mu''(\tau'') = (b, c)$$

iff

$$\tau = p \xrightarrow{a} q \in T \text{ and } b = \mu(\tau) \text{ and } \tau' = p' \xrightarrow{a} q' \in T' \text{ and } c = \mu'(\tau')$$

is an SGBT from A to $B \times C$.

Proposition: Product

We identify $(B \times C)^\omega$ with $B^\omega \times C^\omega$.

1. We have $[\![\mathcal{A} \times \mathcal{A}']\!] = \{(u, v, v') \mid (u, v) \in [\![\mathcal{A}]\!] \text{ and } (u, v') \in [\![\mathcal{A}']\!]\}$.
2. If $(Q, A, I, T, (F_i)_i)$ and $(Q', A, I', T', (F'_j)_j)$ are unambiguous (resp. prophetic) then $(Q \times Q', A, I \times I', T'', (F_i \times Q')_i, (Q \times F'_j)_j)$ is also unambiguous (resp. prophetic), and
$\forall u \in A^\omega$ we have $[\![\mathcal{A} \times \mathcal{A}']\!](u) = ([\![\mathcal{A}]\!](u), [\![\mathcal{A}']\!](u))$.

Subalphabets of $\Sigma = 2^{\mathrm{AP}}$

Definition:

For a propositional formula ξ over AP, we let $\Sigma_\xi = \{a \in \Sigma \mid a \models \xi\}$.
For instance, for $p, q \in \mathrm{AP}$,

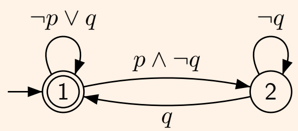
- $\Sigma_p = \{a \in \Sigma \mid p \in a\}$ and $\Sigma_{\neg p} = \Sigma \setminus \Sigma_p$
- $\Sigma_{p \wedge q} = \Sigma_p \cap \Sigma_q$ and $\Sigma_{p \vee q} = \Sigma_p \cup \Sigma_q$
- $\Sigma_{p \wedge \neg q} = \Sigma_p \setminus \Sigma_q$ ...

Notation:

In automata, $s \xrightarrow{\Sigma_\xi} s'$ stands for the set of transitions $\{s\} \times \Sigma_\xi \times \{s'\}$.

To simplify the pictures, we use $s \xrightarrow{\xi} s'$ instead of $s \xrightarrow{\Sigma_\xi} s'$.

Example: $\mathsf{G}(p \to \mathsf{F}\, q)$



Semantics of LTL with sequential functions

Definition: Semantics of $\varphi \in \mathrm{LTL}(\mathrm{AP}, \mathsf{SU}, \mathsf{SS})$

Let $\Sigma = 2^{\mathrm{AP}}$ and $\mathbb{B} = \{0, 1\}$.

Define $[\![\varphi]\!] : \Sigma^\omega \to \mathbb{B}^\omega$ by $[\![\varphi]\!](u) = b_0 b_1 b_2 \cdots$ with $b_i = \begin{cases} 1 & \text{if } u, i \models \varphi \\ 0 & \text{otherwise.} \end{cases}$

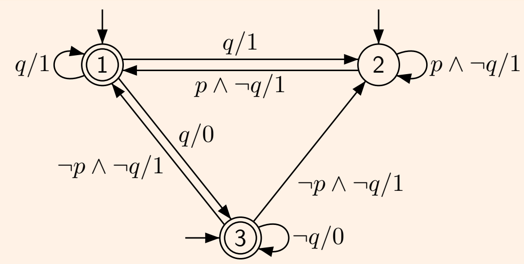
Example:

$$[\![p \,\mathsf{SU}\, q]\!](\emptyset\{q\}\{p\}\emptyset\{p\}\{p\}\{q\}\emptyset\{p\}\{p,q\}\emptyset^\omega) = 1001110110^\omega$$
$$[\![\mathsf{X}\, p]\!](\emptyset\{q\}\{p\}\emptyset\{p\}\{p\}\{q\}\emptyset\{p\}\{p,q\}\emptyset^\omega) = 0101100110^\omega$$
$$[\![\mathsf{F}\, p]\!](\emptyset\{q\}\{p\}\emptyset\{p\}\{p\}\{q\}\emptyset\{p\}\{p,q\}\emptyset^\omega) = 1111111110^\omega$$

The aim is to compute $[\![\varphi]\!]$ with synchronous Büchi transducers (actually, SGBT).

Synchronous Büchi transducer for $p \,\mathsf{SU}\, q$

Example: An SBT for $[\![p \,\mathsf{SU}\, q]\!]$



Lemma: The input BA is prophetic

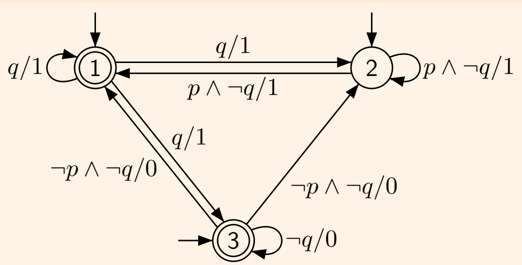
For all $u = a_0 a_1 a_2 \cdots \in \Sigma^\omega$,
there is a unique final run $\rho = s_0, a_0, s_1, a_1, s_2, a_2, s_3, \ldots$ of $\mathcal{A}$ on u.

The run ρ satisfies for all $i \geq 0$, $s_i = \begin{cases} 1 & \text{if } u, i \models q \\ 2 & \text{if } u, i \models \neg q \wedge (p \,\mathsf{U}\, q) \\ 3 & \text{if } u, i \models \neg(p \,\mathsf{U}\, q) \end{cases}$

Hence, the SBT computes $[\![p \,\mathsf{SU}\, q]\!]$.

Synchronous Büchi transducer for $p \,\mathsf{U}\, q$

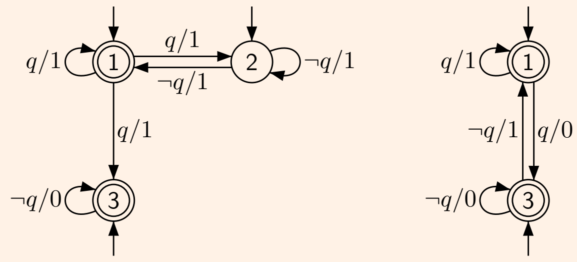
Example: An SBT for $[\![p \,\mathsf{U}\, q]\!]$



The automaton is prophetic (same input BA as for $p \,\mathsf{SU}\, q$).
This SBT computes $[\![p \,\mathsf{U}\, q]\!]$.

Special cases of Until: Future and Next

Example: $\mathsf{F}\, q = \top \,\mathsf{U}\, q$ and $\mathsf{X}\, q = \perp \mathsf{SU}\, q$



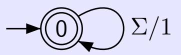
Exercise: Give SBT's for the following formulae:

$\mathsf{SF}\, q$, $\mathsf{SG}\, q$, $p \,\mathsf{SR}\, q$, $p \,\mathsf{SS}\, q$, $\mathsf{Y}\, q$, $\mathsf{G}\, q$, $p \,\mathsf{R}\, q$, $p \,\mathsf{S}\, q$, $\mathsf{G}(p \to \mathsf{F}\, q)$.

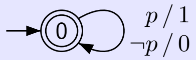
From LTL to Büchi automata

Definition: SBT for LTL modalities

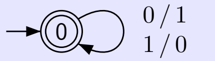
- $\mathcal{A}_\top$ from Σ to $\mathbb{B} = \{0,1\}$:



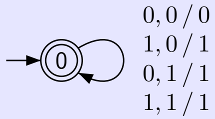
- $\mathcal{A}_p$ from Σ to $\mathbb{B} = \{0,1\}$:



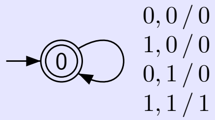
- $\mathcal{A}_\neg$ from $\mathbb{B}$ to $\mathbb{B}$:



- $\mathcal{A}_\vee$ from $\mathbb{B}^2$ to $\mathbb{B}$:



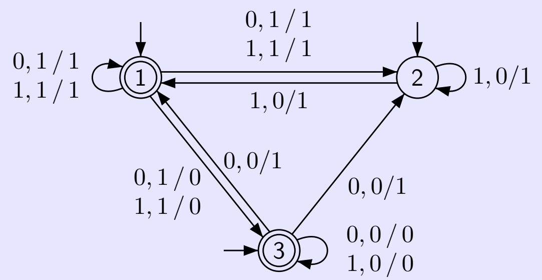
- $\mathcal{A}_\wedge$ from $\mathbb{B}^2$ to $\mathbb{B}$:



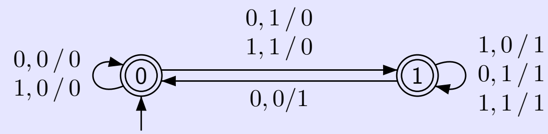
From LTL to Büchi automata

Definition: SBT for LTL modalities (cont.)

- $\mathcal{A}_{\mathsf{SU}}$ from $\mathbb{B}^2$ to $\mathbb{B}$:
  Prophetic



- $\mathcal{A}_{\mathsf{SS}}$ from $\mathbb{B}^2$ to $\mathbb{B}$:
  Deterministic
  Not prophetic



From LTL to Büchi automata

Definition: Translation from LTL to SGBT

For each $\xi \in \mathrm{LTL}(\mathrm{AP}, \mathsf{SU}, \mathsf{SS})$ we define inductively an SGBT $\mathcal{A}_\xi$ as follows:

- $\mathcal{A}_\top$ and $\mathcal{A}_p$ for $p \in \mathrm{AP}$ are already defined
- $\mathcal{A}_{\neg\varphi} = \mathcal{A}_\neg \circ \mathcal{A}_\varphi$
- $\mathcal{A}_{\varphi\vee\psi} = \mathcal{A}_\vee \circ (\mathcal{A}_\varphi \times \mathcal{A}_\psi)$
- $\mathcal{A}_{\varphi \mathsf{SS} \psi} = \mathcal{A}_{\mathsf{SS}} \circ (\mathcal{A}_\varphi \times \mathcal{A}_\psi)$
- $\mathcal{A}_{\varphi \mathsf{SU} \psi} = \mathcal{A}_{\mathsf{SU}} \circ (\mathcal{A}_\varphi \times \mathcal{A}_\psi)$

Theorem: Correctness of the translation

For each $\xi \in \mathrm{LTL}(\mathrm{AP}, \mathsf{SU}, \mathsf{SS})$, we have $[\![\mathcal{A}_\xi]\!] = [\![\xi]\!]$ and $\mathcal{A}_\xi$ is unambiguous.
Moreover, the number of states of $\mathcal{A}_\xi$ is at most $2^{|\xi|_{\mathsf{SS}}} \cdot 3^{|\xi|_{\mathsf{SU}}}$
the number of acceptance conditions is $|\xi|_{\mathsf{SU}}$
where $|\xi|_{\mathsf{SS}}$ (resp. $|\xi|_{\mathsf{SU}}$) is the number of SS (resp. SU) occurring in ξ.

Remark:

- If a subformula φ occurs serveral time in ξ, we only need one copy of $\mathcal{A}_\varphi$.
- We may also use automata for other modalities: $\mathcal{A}_{\mathsf{X}}$ (2 states), $\mathcal{A}_{\mathsf{U}}$, …

Useful simplifications

Reducing the number of temporal subformulae

$$(\mathsf{X}\,\varphi) \wedge (\mathsf{X}\,\psi) \equiv \mathsf{X}(\varphi \wedge \psi) \qquad (\mathsf{X}\,\varphi)\ \mathsf{SU}\ (\mathsf{X}\,\psi) \equiv \mathsf{X}(\varphi\ \mathsf{SU}\ \psi)$$
$$(\mathsf{G}\,\varphi) \wedge (\mathsf{G}\,\psi) \equiv \mathsf{G}(\varphi \wedge \psi) \qquad \mathsf{G}\,\mathsf{F}\,\varphi \vee \mathsf{G}\,\mathsf{F}\,\psi \equiv \mathsf{G}\,\mathsf{F}(\varphi \vee \psi)$$
$$(\varphi_1\ \mathsf{SU}\ \psi) \wedge (\varphi_2\ \mathsf{SU}\ \psi) \equiv (\varphi_1 \wedge \varphi_2)\ \mathsf{SU}\ \psi \qquad (\varphi\ \mathsf{SU}\ \psi_1) \vee (\varphi\ \mathsf{SU}\ \psi_2) \equiv \varphi\ \mathsf{SU}\ (\psi_1 \vee \psi_2)$$

Merging equivalent states

Let $\mathcal{A} = (Q, \Sigma, I, T, (F_i)_i, \mu)$ be an SGBT and $s_1, s_2 \in Q$.
We can merge s_1 and s_2 if they satisfy the same final conditions:

$$s_1 \in F_i \iff s_2 \in F_i \qquad \text{for all } i$$

and they have the same outgoing transitions: $\forall a \in \Sigma$, $\forall s \in Q$,

$$\tau_1 = (s_1, a, s) \in T \iff \tau_2 = (s_2, a, s) \in T \qquad \text{and} \qquad \mu(\tau_1) = \mu(\tau_2)$$

Other constructions

- Tableau construction. See for instance [15, Wolper 85]
  + : Easy definition, easy proof of correctness
  + : Works both for future and past modalities
  − : Inefficient without strong optimizations
- Using Very Weak Alternating Automata [16, Gastin & Oddoux 01].
  + : Very efficient
  − : Only for future modalities

  Online tool: http://www.lsv.ens-cachan.fr/~gastin/ltl2ba/
- Using reduction rules [6, Demri & Gastin 10].
  + : Efficient and produces small automata
  + : Can be used by hand on real examples
  − : Only for future modalities
- The domain is still very active.

Some References

[9] O. Lichtenstein and A. Pnueli.
Checking that finite state concurrent programs satisfy their linear specification.
In *ACM Symposium PoPL'85*, 97–107.

[15] P. Wolper.
The tableau method for temporal logic: An overview,
Logique et Analyse. **110–111**, 119–136, (1985).

[10] A. Sistla and E. Clarke.
The complexity of propositional linear temporal logic.
Journal of the Association for Computing Machinery. **32** (3), 733–749, (1985).

[16] P. Gastin and D. Oddoux.
Fast LTL to Büchi automata translation.
In *CAV'01*, vol. 2102, *Lecture Notes in Computer Science*, pp. 53–65.
Springer, (2001).
http://www.lsv.ens-cachan.fr/~gastin/mes-publis.php

[6] S. Demri and P. Gastin.
Specification and Verification using Temporal Logics.
In Modern applications of automata theory, IISc Research Monographs 2.
World Scientific, 2012.
http://www.lsv.ens-cachan.fr/~gastin/mes-publis.php

Satisfiability for LTL over $(\mathbb{N}, <)$

Let AP be the set of atomic propositions and $\Sigma = 2^{\mathrm{AP}}$.

Definition: Satisfiability problem

Input: A formula $\varphi \in \mathrm{LTL}(\mathrm{AP}, \mathsf{SU}, \mathsf{SS})$

Question: Existence of $w \in \Sigma^\omega$ and $i \in \mathbb{N}$ such that $w, i \models \varphi$.

Definition: Initial Satisfiability problem

Input: A formula $\varphi \in \mathrm{LTL}(\mathrm{AP}, \mathsf{SU}, \mathsf{SS})$

Question: Existence of $w \in \Sigma^\omega$ such that $w, 0 \models \varphi$.

Remark: φ is satisfiable iff $\mathsf{F}\,\varphi$ is *initially* satisfiable.

Definition: (Initial) validity

φ is valid iff $\neg\varphi$ is not satisfiable.

Theorem [10, Sistla, Clarke 85], [9, Lichtenstein & Pnueli 85]

The satisfiability problem for LTL is PSPACE-complete.

Model checking for LTL

Definition: Model checking problem

Input: A Kripke structure $M = (S, T, I, \mathrm{AP}, \ell)$
A formula $\varphi \in \mathrm{LTL}(\mathrm{AP}, \mathsf{SU}, \mathsf{SS})$

Question: Does $M \models \varphi$?

- Universal MC: $M \models_\forall \varphi$ if $\ell(\sigma), 0 \models \varphi$ for all initial infinite runs of M.
- Existential MC: $M \models_\exists \varphi$ if $\ell(\sigma), 0 \models \varphi$ for some initial infinite run of M.

$$M \models_\forall \varphi \quad \text{iff} \quad M \not\models_\exists \neg\varphi$$

Theorem [10, Sistla, Clarke 85], [9, Lichtenstein & Pnueli 85]

The Model checking problem for LTL is PSPACE-complete

$\mathrm{MC}^\exists(\mathsf{SU}) \leq_P \mathrm{SAT}(\mathsf{SU})$ [10, Sistla & Clarke 85]

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

Introduce new atomic propositions: $\mathrm{AP}_S = \{\mathrm{at}_s \mid s \in S\}$
Define $\mathrm{AP}' = \mathrm{AP} \uplus \mathrm{AP}_S$ $\quad \Sigma' = 2^{\mathrm{AP}'}$ $\quad \pi : \Sigma'^\omega \to \Sigma^\omega$ 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

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

Let $w = a_0 a_1 a_2 \cdots \in \Sigma'^\omega$. Then, $w \models \psi_M$ iff there exists an initial infinite run $\sigma = s_0, s_1, s_2, \ldots$ of M such that $\pi(w) = \ell(\sigma)$ and $a_i \cap \mathrm{AP}_S = \{\mathrm{at}_{s_i}\}$ for all $i \geq 0$.

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

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

QBF Quantified Boolean Formulae

Definition: QBF

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

Question: Is γ valid?

Definition:

An assignment of the variables $\{x_1, \ldots, x_n\}$ 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 $\forall v \in V$, $\forall 1 \leq i \leq n$ s.t. $Q_i = \forall$,
  $\exists v' \in V$ s.t. $v[i-1] = v'[i-1]$ and $v'_i = 1 - v_i$.

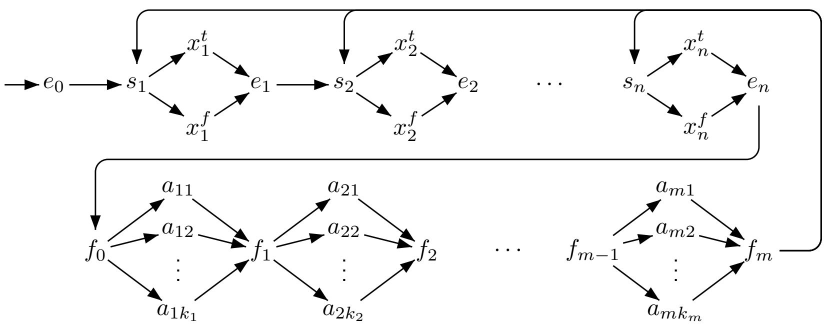
Proposition:

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

$\mathrm{QBF} \leq_P \mathrm{MC}^\exists(\mathsf{U})$ [10, 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 $\psi_{ij} = \begin{cases} \mathsf{G}(x_k^f \to s_k \,\mathsf{R}\, \neg a_{ij}) & \text{if } a_{ij} = x_k \\ \mathsf{G}(x_k^t \to s_k \,\mathsf{R}\, \neg a_{ij}) & \text{if } a_{ij} = \neg x_k \end{cases}$ and $\psi = \bigwedge_{i,j} \psi_{ij}$.

Let $\varphi_i = \mathsf{G}(e_{i-1} \to (\neg s_{i-1} \,\mathsf{U}\, x_i^t) \wedge (\neg s_{i-1} \,\mathsf{U}\, x_i^f))$ and $\varphi = \bigwedge_{i \mid Q_i = \forall} \varphi_i$.

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

Complexity of LTL

Theorem: Complexity of LTL

The following problems are PSPACE-complete:

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

The following problems are NP-complete:

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

Complexity of CTL^*

Definition: Syntax of the Computation Tree Logic CTL^*

$$\varphi ::= \bot \mid p\ (p \in \mathrm{AP}) \mid \neg\varphi \mid \varphi \vee \varphi \mid \mathsf{X}\,\varphi \mid \varphi\,\mathsf{U}\,\varphi \mid \mathsf{E}\,\varphi \mid \mathsf{A}\,\varphi$$

Theorem

The model checking problem for CTL^* is PSPACE-complete

Proof:

PSPACE-hardness: follows from $\mathrm{LTL} \subseteq \mathrm{CTL}^*$.

PSPACE-easiness: reduction to LTL-model checking by inductive eliminations of path quantifications.

Satisfiability for CTL^*

Definition: $\mathrm{SAT}(\mathrm{CTL}^*)$

Input: A formula $\varphi \in \mathrm{CTL}^*$

Question: Existence of a model M and a run σ such that $M, \sigma, 0 \models \varphi$?

Theorem

The satisfiability problem for CTL^* is 2-EXPTIME-complete