Model checking for LTL

Definition: Model checking problem

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

Question: Does $M \models \varphi$?

- Universal MC: $M \models_\forall \varphi$ if $\ell(\sigma), 0 \models \varphi$ for all initial infinite run 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 [11, Sistla, Clarke 85], [12, Lichtenstein & Pnueli 85]

The Model checking problem for LTL is PSPACE-complete

Satisfiability for LTL

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

Definition: Satisfiability problem

Input: A formula $\varphi \in \mathrm{LTL}(\mathrm{AP}, \mathsf{Y}, \mathsf{S}, \mathsf{X}, \mathsf{U})$

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 $\varphi \in \mathrm{LTL}(\mathrm{AP}, \mathsf{Y}, \mathsf{S}, \mathsf{X}, \mathsf{U})$

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

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

Theorem (Sistla, Clarke 85, Lichtenstein et. al 85)

The satisfiability problem for LTL is PSPACE-complete

Definition: (Initial) validity

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

Decision procedure for LTL

Definition: The core

From a formula $\varphi \in \mathrm{LTL}(\mathrm{AP}, \ldots)$, construct a Büchi automaton $\mathcal{A}_\varphi$ such that

$$\mathcal{L}(\mathcal{A}) = \mathcal{L}(\varphi) = \{w \in \Sigma^\omega \mid w, 0 \models \varphi\}.$$

Satisfiability (initial)

Check the Büchi automaton $\mathcal{A}_\varphi$ for emptiness.

Model checking

Construct a synchronized product $\mathcal{B} = M \otimes \mathcal{A}_{\neg\varphi}$ so that
the successful runs of $\mathcal{B}$ correspond to the initial runs of M satisfying $\neg\varphi$.

Then, check $\mathcal{B}$ for emptiness.

Theorem:

Checking Büchi automata for emptiness is NLOGSPACE-complete.

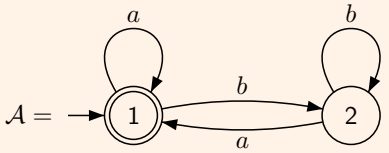
Büchi automata

Definition:

$\mathcal{A} = (Q, \Sigma, I, T, F)$ where

- Q: finite set of states
- Σ: finite set of labels
- $I \subseteq Q$: set of initial states
- $T \subseteq Q \times \Sigma \times Q$: transitions
- $F \subseteq Q$: set of accepting states (repeated, final)

Example:



$$\mathcal{L}(\mathcal{A}) = \{w \in \{a, b\}^\omega \mid |w|_a = \omega\}$$

Büchi automata for some LTL formulae

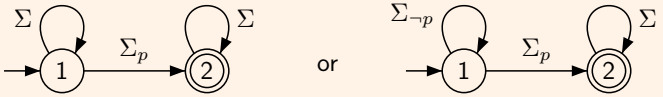
Definition:

Recall that $\Sigma = 2^{\mathrm{AP}}$. For $\psi \in \mathbb{B}(\mathrm{AP})$ we let $\Sigma_\psi = \{a \in \Sigma \mid a \models \psi\}$.
For instance, for $p, q \in \mathrm{AP}$,

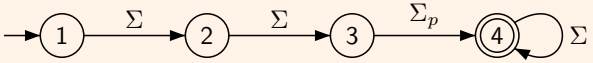
- $\Sigma_p = \{a \in \Sigma \mid p \in a\}$ and $\Sigma_{\neg p} = \Sigma \setminus \Sigma_p$
- $\Sigma_{p \wedge q} = \Sigma_p \cap \Sigma_q$ and $\Sigma_{p \vee q} = \Sigma_p \cup \Sigma_q$
- $\Sigma_{p \wedge \neg q} = \Sigma_p \setminus \Sigma_q$ ...

Examples:

F p:



X X p:

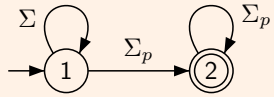


G p:

Büchi automata for some LTL formulae

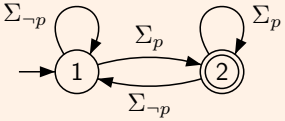
Examples:

F G p:



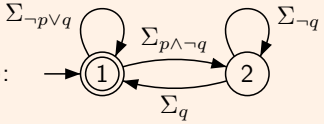
no deterministic Büchi automaton.

G F p:



deterministic Büchi automata
are not closed under complement.

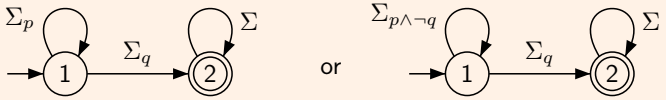
G($p \to$ F q):



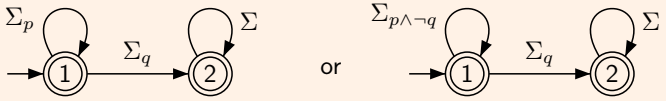
Büchi automata for some LTL formulae

Examples:

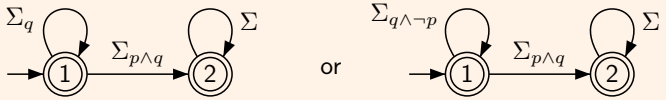
p U q:



p W q:



p R q:



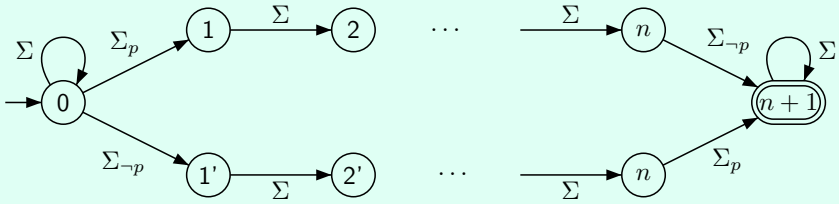
Büchi automata

Properties

Büchi automata are closed under union, intersection, complement.

- Union: trivial
- Intersection: easy (exercice)
- complement: hard

Let $\varphi = \mathrm{F}((p \wedge \mathrm{X}^n \neg p) \vee (\neg p \wedge \mathrm{X}^n p))$



Any non deterministic Büchi automaton for $\neg\varphi$ has at least 2^n states.

Büchi automata

Exercise:

Given Büchi automata for φ and ψ,

- Construct a Büchi automaton for $\mathsf{X}\,\varphi$ (trivial)
- Construct a Büchi automaton for $\varphi\,\mathsf{U}\,\psi$

This gives an inductive construction of $\mathcal{A}_\varphi$ from $\varphi \in \mathrm{LTL}(\mathrm{AP}, \mathsf{X}, \mathsf{U})$ ...

... but the size of $\mathcal{A}_\varphi$ might be non-elementary in the size of φ.

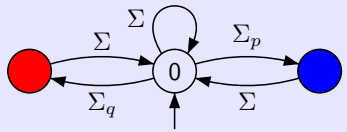
Generalized Büchi automata

Definition: acceptance on states

$\mathcal{A} = (Q, \Sigma, I, T, F_1, \ldots, F_n)$ with $F_i \subseteq Q$.

An infinite run σ is successful if it visits infinitely often each F_i.

$\mathsf{G}\,\mathsf{F}\,p \wedge \mathsf{G}\,\mathsf{F}\,q$:

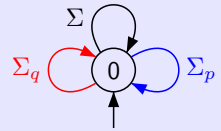


Definition: acceptance on transitions

$\mathcal{A} = (Q, \Sigma, I, T, T_1, \ldots, T_n)$ with $T_i \subseteq T$.

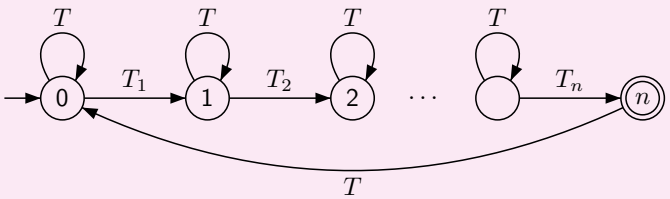
An infinite run σ is successful if it uses infinitely many transitions from each T_i.

$\mathsf{G}\,\mathsf{F}\,p \wedge \mathsf{G}\,\mathsf{F}\,q$:



GBA to BA

Proof: Synchronized product with $\mathcal{B}$



Transitions: $\dfrac{t = s_1 \xrightarrow{a} s_1' \in \mathcal{A} \wedge s_2 \xrightarrow{t} s_2' \in \mathcal{B}}{(s_1, s_2) \xrightarrow{a} (s_1', s_2')}$

Accepting states: $Q \times \{n\}$

Negative normal form

Definition: Syntax ($p \in \mathrm{AP}$)

$$\varphi ::= \top \mid \bot \mid p \mid \neg p \mid \varphi \vee \varphi \mid \varphi \wedge \varphi \mid \mathsf{X}\,\varphi \mid \varphi\,\mathsf{U}\,\varphi \mid \varphi\,\mathsf{R}\,\varphi$$

Proposition: Any formula can be transformed in NNF

$$\neg(\varphi \vee \psi) \equiv (\neg\varphi) \wedge (\neg\psi) \qquad \neg(\varphi \wedge \psi) \equiv (\neg\varphi) \vee (\neg\psi)$$
$$\neg(\varphi\,\mathsf{U}\,\psi) \equiv (\neg\varphi)\,\mathsf{R}\,(\neg\psi) \qquad \neg(\varphi\,\mathsf{R}\,\psi) \equiv (\neg\varphi)\,\mathsf{U}\,(\neg\psi)$$
$$\neg\,\mathsf{X}\,\varphi \equiv \mathsf{X}\,\neg\varphi \qquad \neg\neg\varphi \equiv \varphi$$

This does not increase the number of Temporal subformulae.

Temporal formulae

Definition: Temporal formulae

- literals
- formulae with outermost connective X, U or R.

Reducing the number of temporal subformulae

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

From LTL to BA [6, Demri & Gastin 10]

Definition:

- $Z \subseteq \mathrm{NNF}$ is consistent if $\bot \notin Z$ and $\{p, \neg p\} \not\subseteq Z$ for all $p \in \mathrm{AP}$.
- For $Z \subseteq \mathrm{NNF}$, we define $\bigwedge Z = \bigwedge_{\psi \in Z} \psi$.
  Note that $\bigwedge \emptyset = \top$ and if Z is inconsistent then $\bigwedge Z \equiv \bot$.

Intuition for the BA $\mathcal{A}_\varphi = (Q, \Sigma, I, T, (T_\alpha)_{\alpha \in \mathsf{U}(\varphi)})$

Let $\varphi \in \mathrm{NNF}$ be a formula.

- $\mathrm{sub}(\varphi)$ is the set of sub-formulae of φ.
- $\mathsf{U}(\varphi)$ the set of until sub-formulae of φ.
- We construct a BA $\mathcal{A}_\varphi$ with $Q = 2^{\mathrm{sub}(\varphi)}$ and $I = \{\varphi\}$.
- A state $Z \subseteq \mathrm{sub}(\varphi)$ is a set of obligations.
- If $Z \subseteq \mathrm{sub}(\varphi)$, we want $\mathcal{L}(\mathcal{A}_\varphi^Z) = \{u \in \Sigma^\omega \mid u, 0 \models \bigwedge Z\}$
  where $\mathcal{A}_\varphi^Z$ is $\mathcal{A}_\varphi$ using Z as unique initial state.

Reduced formulae

Definition: Reduced formulae

- A formula is reduced if it is a literal (p or $\neg p$) or a next-formula ($\mathsf{X}\,\beta$).
- $Z \subseteq \mathrm{NNF}$ is reduced if all formulae in Z are reduced,

For $Z \subseteq \mathrm{NNF}$ consistent and reduced, we define

- $\mathrm{next}(Z) = \{\alpha \mid \mathsf{X}\,\alpha \in Z\}$
- $\Sigma_Z = \bigcap_{p \in Z} \Sigma_p \quad \cap \quad \bigcap_{\neg p \in Z} \Sigma_{\neg p}$

Lemma: Next step

Let $Z \subseteq \mathrm{NNF}$ be consistent and reduced.
Let $u = a_0 a_1 a_2 \cdots \in \Sigma^\omega$ and $n \geq 0$. Then

$$u, n \models \bigwedge Z \quad \text{iff} \quad u, n+1 \models \bigwedge \mathrm{next}(Z) \text{ and } a_n \in \Sigma_Z$$

- $\mathcal{A}_\varphi$ will have transitions $Z \xrightarrow{\Sigma_Z} \mathrm{next}(Z)$.
  Note that $\emptyset \xrightarrow{\Sigma} \emptyset$.
- Problem: $\mathrm{next}(Z)$ is not reduced in general (it may even be inconsistent).

Reduction rules

Definition: Reduction of obligations to literals and next-formulae

Let $Y \subseteq \mathrm{NNF}$ and let $\psi \in Y$ maximal not reduced.

If $\psi = \psi_1 \wedge \psi_2$: $\quad Y \xrightarrow{\varepsilon} (Y \setminus \{\psi\}) \cup \{\psi_1, \psi_2\}$

If $\psi = \psi_1 \vee \psi_2$: $\quad Y \xrightarrow{\varepsilon} (Y \setminus \{\psi\}) \cup \{\psi_1\}$, $\quad Y \xrightarrow{\varepsilon} (Y \setminus \{\psi\}) \cup \{\psi_2\}$

If $\psi = \psi_1\ \mathsf{R}\ \psi_2$: $\quad Y \xrightarrow{\varepsilon} (Y \setminus \{\psi\}) \cup \{\psi_1, \psi_2\}$, $\quad Y \xrightarrow{\varepsilon} (Y \setminus \{\psi\}) \cup \{\psi_2, \mathsf{X}\,\psi\}$

If $\psi = \mathsf{G}\,\psi_2$: $\quad Y \xrightarrow{\varepsilon} (Y \setminus \{\psi\}) \cup \{\psi_2, \mathsf{X}\,\psi\}$

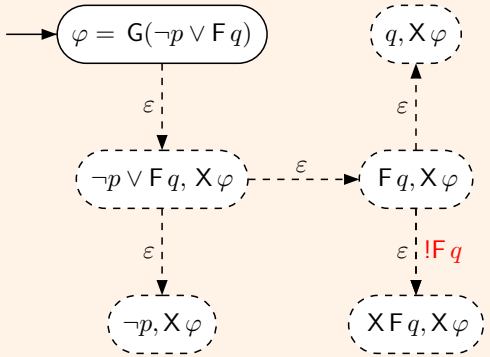
If $\psi = \psi_1\ \mathsf{U}\ \psi_2$: $\quad Y \xrightarrow{\varepsilon} (Y \setminus \{\psi\}) \cup \{\psi_2\}$, $\quad Y \xrightarrow[!\psi]{\varepsilon} (Y \setminus \{\psi\}) \cup \{\psi_1, \mathsf{X}\,\psi\}$

If $\psi = \mathsf{F}\,\psi_2$: $\quad Y \xrightarrow{\varepsilon} (Y \setminus \{\psi\}) \cup \{\psi_2\}$, $\quad Y \xrightarrow[!\psi]{\varepsilon} (Y \setminus \{\psi\}) \cup \{\mathsf{X}\,\psi\}$

Note the mark $!\psi$ on the second transitions for U and F.

Reduction rules

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



State = set of obligations.

Reduce obligations to literals and next-formulae.

Note again the mark !F q on the last edge

Reduction

Lemma: Soundness

- if there is only one rule $Y \xrightarrow{\varepsilon} Y_1$ then $\bigwedge Y \equiv \bigwedge Y_1$
- if there are two rules $Y \xrightarrow{\varepsilon} Y_1$ and $Y \xrightarrow{\varepsilon} Y_2$ then $\bigwedge Y \equiv \bigwedge Y_1 \vee \bigwedge Y_2$

Definition:

For $Y \subseteq \mathrm{NNF}$ and $\alpha \in \mathsf{U}(\varphi)$, let

$$\mathrm{Red}(Y) = \{Z \text{ consistent and reduced} \mid \text{there is a path } Y \xrightarrow{\varepsilon}_* Z\}$$
$$\mathrm{Red}_\alpha(Y) = \{Z \text{ consistent and reduced} \mid \text{there is a path } Y \xrightarrow{\varepsilon}_* Z \text{ without using an edge marked with } !\alpha\}$$

Lemma: Soundness

- Let $Y \subseteq \mathrm{NNF}$, then $\bigwedge Y \equiv \bigvee_{Z \in \mathrm{Red}(Y)} \bigwedge Z$
- Let $u = a_0 a_1 a_2 \cdots \in \Sigma^\omega$ and $n \geq 0$ with $u, n \models \bigwedge Y$.
  Then, $\exists Z \in \mathrm{Red}(Y)$ such that $u, n \models \bigwedge Z$
  and $Z \in \mathrm{Red}_\alpha(Y)$ for all $\alpha = \alpha_1 \,\mathsf{U}\, \alpha_2 \in \mathsf{U}(\varphi)$ such that $u, n \models \alpha_2$.

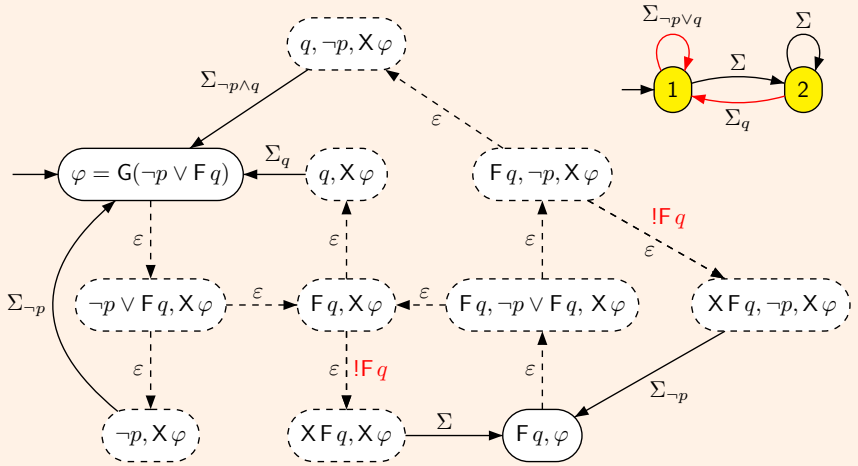
Automaton $\mathcal{A}_\varphi$

Definition: Automaton $\mathcal{A}_\varphi$

- States: $Q = 2^{\mathrm{sub}(\varphi)}$, $\quad I = \{\varphi\}$
- Transitions: $T = \{Y \xrightarrow{a} \mathrm{next}(Z) \mid Y \in Q, a \in \Sigma_Z \text{ and } Z \in \mathrm{Red}(Y)\}$
- Acceptance: $T_\alpha = \{Y \xrightarrow{a} \mathrm{next}(Z) \mid Y \in Q, a \in \Sigma_Z \text{ and } Z \in \mathrm{Red}_\alpha(Y)\}$ for each $\alpha \in \mathsf{U}(\varphi)$.

Automaton $\mathcal{A}_\varphi$

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



Transition = check literals and move forward.

Simplification