Model Checking

Lecture #8: LTL Model Checking By Automata

[Baier & Katoen, Chapter 5.2]

Joost-Pieter Katoen

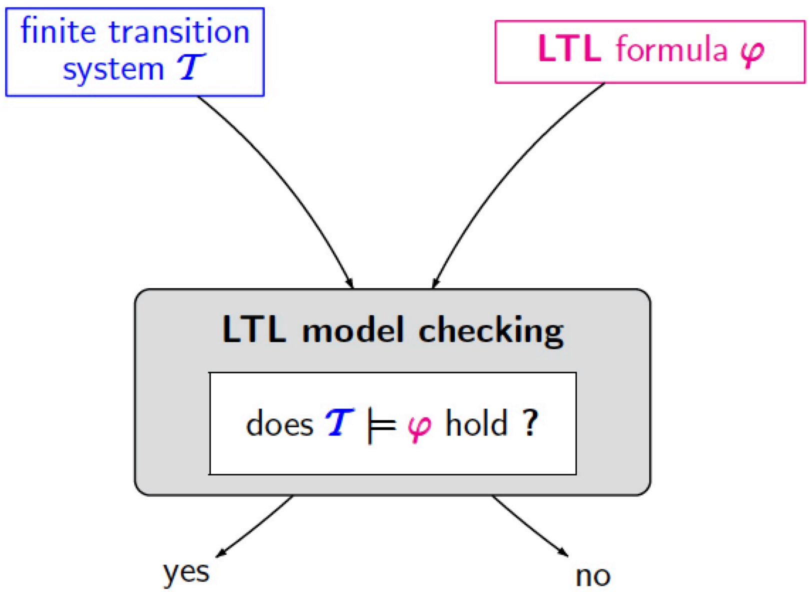
Software Modeling and Verification Group

Model Checking Course, RWTH Aachen, WiSe 2019/2020

Overview

1. Linear Temporal Logic
2. LTL Model Checking
3. From LTL to GNBA
4. Complexity
5. Summary

Topic



Overview

1. Linear Temporal Logic
2. LTL Model Checking
3. From LTL to GNBA
4. Complexity
5. Summary

LTL Syntax

Definition: LTL syntax

BNF grammar for LTL formulas with proposition $a \in AP$:

$$\varphi \ ::= \ \mathrm{true} \ \big| \ a \ \big| \ \varphi_1 \wedge \varphi_2 \ \big| \ \neg\varphi \ \big| \ \bigcirc\varphi \ \big| \ \varphi_1 \,\mathsf{U}\, \varphi_2$$

- Propositional logic
  - $a \in AP$ — atomic proposition
  - $\neg\varphi$ and $\varphi \wedge \psi$ — negation and conjunction
- Temporal modalities
  - $\bigcirc\varphi$ — neXt state fulfills φ
  - $\varphi \,\mathsf{U}\, \psi$ — φ holds Until a ψ-state is reached

Linear Temporal Logic (LTL) is a logic to describe LT properties

Derived Operators

$\Diamond\varphi \equiv \mathrm{true}\,\mathsf{U}\,\varphi$ "some time in the future"

$\Box\varphi \equiv \neg\Diamond\neg\varphi$ "from now on forever"

Semantics Over Words

Definition: LTL semantics over infinite words

The LT-property induced by LTL formula φ over AP is:

$$Words(\varphi) = \left\{ \sigma \in \left(2^{AP}\right)^{\omega} \mid \sigma \vDash \varphi \right\}, \text{where } \vDash \text{ is the smallest relation with:}$$

$$\begin{array}{lllll}
\sigma & \vDash & \mathrm{true} & & \\
\sigma & \vDash & a & \text{iff} & a \in A_0 \quad (\text{i.e., } A_0 \vDash a) \\
\sigma & \vDash & \varphi_1 \wedge \varphi_2 & \text{iff} & \sigma \vDash \varphi_1 \text{ and } \sigma \vDash \varphi_2 \\
\sigma & \vDash & \neg\varphi & \text{iff} & \sigma \nvDash \varphi \\
\sigma & \vDash & \bigcirc\varphi & \text{iff} & \sigma[1..] = A_1A_2A_3\ldots \vDash \varphi \\
\sigma & \vDash & \varphi_1 \,\mathsf{U}\, \varphi_2 & \text{iff} & \exists j \geq 0.\ \sigma[j..] \vDash \varphi_2 \text{ and } \sigma[i..] \vDash \varphi_1,\ 0 \leq i < j
\end{array}$$

for $\sigma = A_0A_1A_2\ldots$, let $\sigma[i..] = A_iA_{i+1}A_{i+2}\ldots$ be the suffix of σ from index i on.

Semantics of $\Box$, $\Diamond$, $\Box\Diamond$ and $\Diamond\Box$

$$\begin{array}{lllll}
\sigma & \vDash & \Diamond\varphi & \text{iff} & \exists j \geq 0.\ \sigma[j..] \vDash \varphi \\
\sigma & \vDash & \Box\varphi & \text{iff} & \forall j \geq 0.\ \sigma[j..] \vDash \varphi \\
\sigma & \vDash & \Box\Diamond\varphi & \text{iff} & \underbrace{\forall j \geq 0.\ \exists i \geq j.\ \sigma[i\ldots] \vDash \varphi}_{\text{infinitely often } \varphi} \\
\sigma & \vDash & \Diamond\Box\varphi & \text{iff} & \underbrace{\exists j \geq 0. \forall i \geq j.\ \sigma[i\ldots] \vDash \varphi}_{\text{persistence of } \varphi}
\end{array}$$

Semantics over Transition Systems

Let $TS = (S, Act, \rightarrow, I, AP, L)$ be a transition system and φ be an LTL-formula over AP.

- For infinite path fragment π of TS:

$$\pi \models \varphi \quad \text{iff} \quad trace(\pi) \models \varphi$$

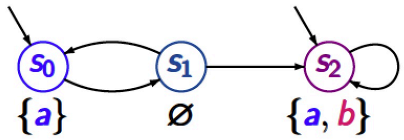
- For state $s \in S$:

$$s \models \varphi \quad \text{iff} \quad \forall \pi \in Paths(s).\ \pi \models \varphi$$

- For transition system TS:

$$TS \models \varphi \quad \text{iff} \quad Traces(TS) \subseteq Words(\varphi) \quad \text{iff} \quad \forall s \in I.\ s \models \varphi$$

Example



$AP = \{a, b\}$

$\mathcal{T} \models a$ as $s_0 \models a$ and $s_2 \models a$

$\mathcal{T} \not\models \Diamond\Box a$ as $s_0\, s_1\, s_0\, s_1 \ldots \not\models \Diamond\Box a$

$\mathcal{T} \models \Diamond\Box b \vee \Box\Diamond(\neg a \wedge \neg b)$ as $s_2 \models b$, $s_1 \not\models a, b$

$\mathcal{T} \models \Box(a \rightarrow (\bigcirc\neg a \vee b))$ as $s_2 \models b$, $s_0 \models \bigcirc\neg a$

Overview

The LTL Model Checking Problem

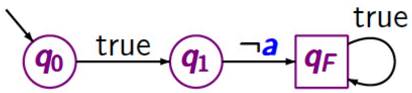
Given:

1. finite transition system TS, and
2. LTL-formula φ

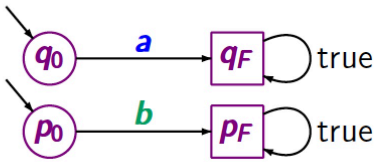
:

decide whether $TS \models \varphi$, and if $TS \not\models \varphi$, provide a counterexample.

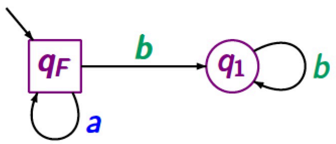
NBA for LTL Formulae



$\mathcal{L}_\omega(\mathcal{A}) = Words(\bigcirc \neg a)$

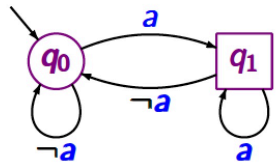


$\mathcal{L}_\omega(\mathcal{A}) = Words(a \vee b)$

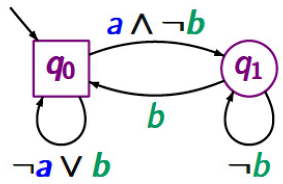


$\mathcal{L}_\omega(\mathcal{A}) = Words(\Box a)$

NBA for LTL Formulae



$\mathcal{L}_\omega(\mathcal{A}) = Words(\Box\Diamond a)$



$\mathcal{L}_\omega(\mathcal{A}) = Words(\Box(a \rightarrow \Diamond b))$

e.g., $\left.\begin{array}{l} \varnothing\,\varnothing\,\varnothing\,\varnothing \ldots = \varnothing^\omega \\ (\{a\}\,\{b\})^\omega \end{array}\right\}$ are accepted by $\mathcal{A}$

A Naive Attempt

$TS \models \varphi$ if and only if $Traces(TS) \subseteq Words(\varphi)$

if and only if $Traces(TS) \subseteq \mathfrak{L}_\omega(\mathfrak{A}_\varphi)$

if and only if $Traces(TS) \cap \overline{\mathfrak{L}_\omega(\mathfrak{A}_\varphi)} = \varnothing$

if and only if $Traces(TS) \cap \mathfrak{L}_\omega(\overline{\mathfrak{A}_\varphi}) = \varnothing$.

Naive idea: check whether TS has no behaviour accepted by NBA $\overline{\mathfrak{A}_\varphi}$

But complementation of NBA yields a blow-up:
if $\mathfrak{A}$ has n states, $\overline{\mathfrak{A}}$ has c^{n^2} states in worst case

$\Rightarrow$ use the fact that: $\mathfrak{L}_\omega(\overline{\mathfrak{A}_\varphi}) = \mathfrak{L}_\omega(\mathfrak{A}_{\neg\varphi})$

Approach

$TS \models \varphi$ if and only if $Traces(TS) \subseteq Words(\varphi)$

if and only if $Traces(TS) \subseteq \mathfrak{L}_\omega(\mathfrak{A}_\varphi)$

if and only if $Traces(TS) \cap \overline{\mathfrak{L}_\omega(\mathfrak{A}_\varphi)} = \varnothing$

if and only if $Traces(TS) \cap \mathfrak{L}_\omega(\overline{\mathfrak{A}_\varphi}) = \varnothing$

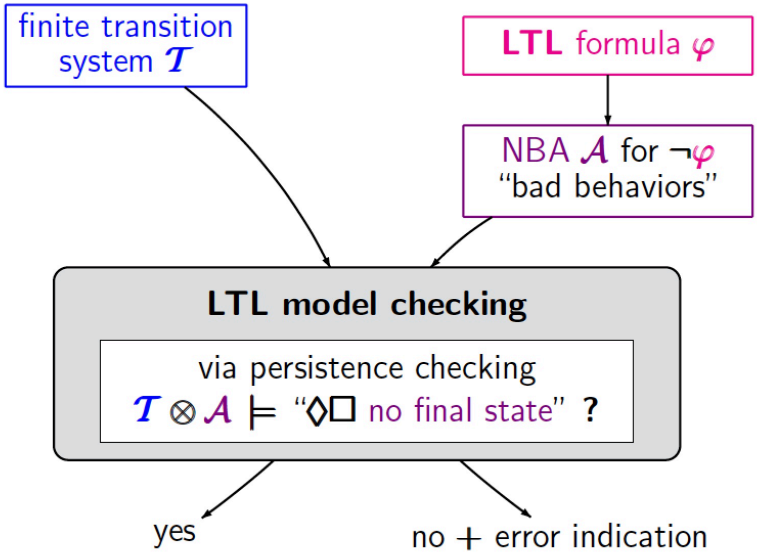
if and only if $Traces(TS) \cap \mathfrak{L}_\omega(\mathfrak{A}_{\neg\varphi}) = \varnothing$

if and only if $TS \otimes \mathfrak{A}_{\neg\varphi} \models \Diamond\Box\,\neg F$

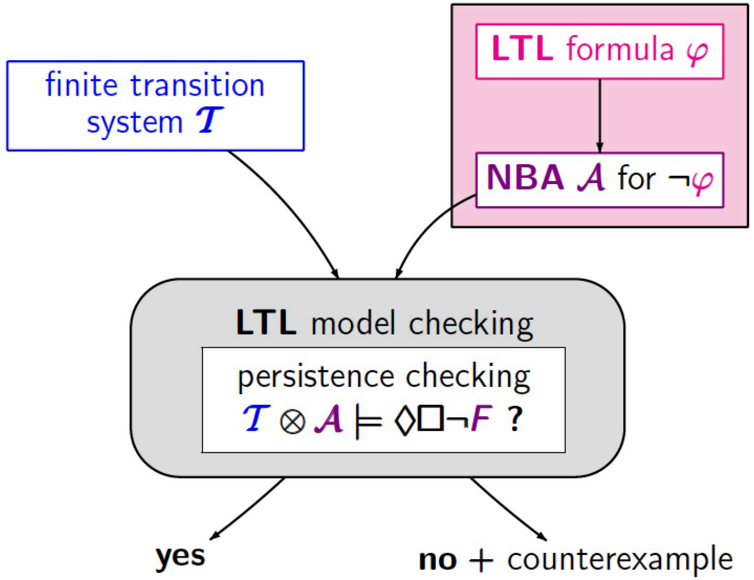
where F is the set of accept states of NBA $\mathfrak{A}_{\neg\varphi}$.

LTL model checking is thus reduced to persistence checking

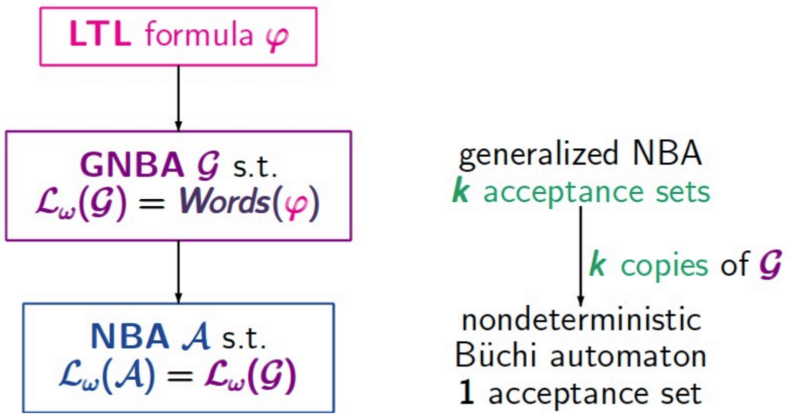
Automata-Based LTL Model Checking



Overview



Overview



Recap: Generalized Büchi Automata

Definition: Generalized Büchi automata

A generalized NBA (GNBA) $\mathfrak{G}$ is a tuple $(Q, \Sigma, \delta, Q_0, \mathfrak{F})$ where Q, Σ, δ, Q_0 are as before and

$$\mathfrak{F} = \{ F_1, \ldots, F_k \} \quad \text{with} \quad F_i \subseteq Q$$

for some natural $k \in \mathbb{N}$.

Run $q_0 \, q_1 \ldots \in Q^\omega$ is accepting if $\forall F_j \in \mathfrak{F}$: $q_i \in F_j$ for infinitely many i

The size of $\mathfrak{G}$, denoted $|\mathfrak{G}|$, is the number of states and transitions in $\mathfrak{G}$

GNBA and NBA are Equally Expressive

For every GNBA $\mathfrak{G}$ there exists an NBA $\mathfrak{A}$ with

$$\mathfrak{L}_\omega(\mathfrak{G}) \;=\; \mathfrak{L}_\omega(\mathfrak{A}) \quad \text{with} \quad |\mathfrak{A}| = O(|\mathfrak{G}| \cdot |\mathfrak{F}|)$$

where $\mathfrak{F} = \{ F_1, \ldots, F_k \}$ denotes the set of acceptance sets in $\mathfrak{G}$.

Proof.

For k=0, 1, this result follows directly. For $k > 1$, make k copies of $\mathfrak{G}$:

- initial states of NBA := the initial states in the first copy
- final states of NBA := accept set F_1 in the first copy
- on visiting in i-th copy a state in F_i, then move to the $(i+1)$-st copy

□

Overview

How to Obtain a GNBA?

GNBA $\mathfrak{G}_\varphi$ over 2^{AP} for LTL-formula φ with $\mathfrak{L}_\omega(\mathfrak{G}_\varphi) = Words(\varphi)$:

- Assume φ only contains the operators $\wedge$, $\neg$, $\bigcirc$ and U

  $\vee$, $\rightarrow$, $\Diamond$, $\Box$, W, and so on, are derived from these base operators

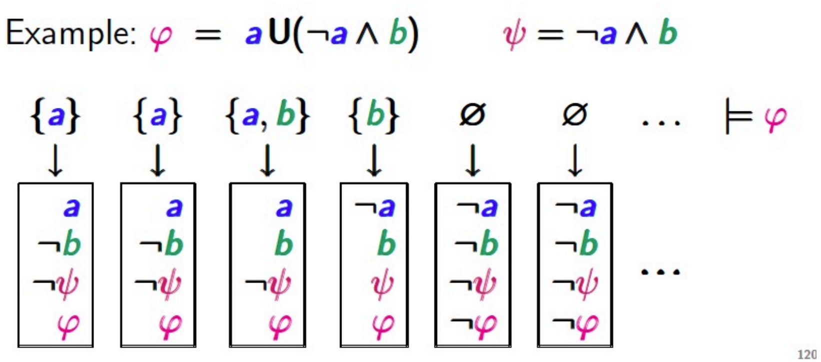
- States are elementary sets of sub-formulas in φ
  - for $\sigma = A_0 A_1 \ldots \in Words(\varphi)$, expand $A_i \subseteq AP$ with sub-formulas of φ
  - ... to obtain the infinite word $\bar{\sigma} \;=\; B_0 B_1 \ldots$ with B_i a set of sub-formulas of φ such that

    $$\psi \in B_i \qquad \text{if and only if} \qquad \sigma^i = A_i A_{i+1} \ldots \models \psi$$

  - $\bar{\sigma}$ is intended to be a run of GNBA $\mathfrak{G}_\varphi$ for σ

- Transitions are derived from semantics $\bigcirc$ and expansion law for U
- Accept sets guarantee that: $\bar{\sigma}$ is an accepting run for σ iff $\sigma \models \varphi$

States by Example



Closure

Definition: Closure

The closure of LTL-formula φ is the set $cl(\varphi)$ consisting of all sub-formulas ψ of φ and their negation $\neg\psi$ where ψ and $\neg\neg\psi$ are identified.

Example

For $\varphi = a \,\mathsf{U}\, (\neg a \wedge b)$ we have

$$cl(\varphi) \;=\; \{\, a, b, \neg a, \neg b, \neg a \wedge b, \neg(\neg a \wedge b), \varphi, \neg\varphi \,\}.$$

We cannot take B_i as arbitrary subset of $cl(\varphi)$.
They must be elementary.

Elementary Sets

Definition: Elementary sets

$B \subseteq cl(\varphi)$ is elementary if all following conditions hold:

1. B is maximally consistent, i.e., for all $\varphi_1 \wedge \varphi_2, \psi \in cl(\varphi)$:
   - $\varphi_1 \wedge \varphi_2 \in B \;\Leftrightarrow\; \varphi_1 \in B$ and $\varphi_2 \in B$
   - $\psi \notin B \;\Leftrightarrow\; \neg\psi \in B$
   - $\mathrm{true} \in cl(\varphi) \;\Rightarrow\; \mathrm{true} \in B$
2. B is locally consistent, i.e., for all $\varphi_1 \,\mathsf{U}\, \varphi_2 \in cl(\varphi)$:
   - $\varphi_2 \in B \;\Rightarrow\; \varphi_1 \,\mathsf{U}\, \varphi_2 \in B$
   - $\varphi_1 \,\mathsf{U}\, \varphi_2 \in B$ and $\varphi_2 \notin B \;\Rightarrow\; \varphi_1 \in B$

Examples

Elementary or not? LTLMC3.2-49

Let $\varphi = a\,\mathsf{U}(\neg a \wedge b)$.

$B_1 = \{a, b, \neg a \wedge b, \varphi\}$	not elementary propositional inconsistent
$B_2 = \{\neg a, b, \varphi\}$	not elementary, not maximal as $\neg a \wedge b \notin B_2$ $\neg(\neg a \wedge b) \notin B_2$
$B_3 = \{\neg a, b, \neg a \wedge b, \neg\varphi\}$	not elementary not locally consistent for U
$B_4 = \{\neg a, \neg b, \neg(\neg a \wedge b), \neg\varphi\}$	elementary

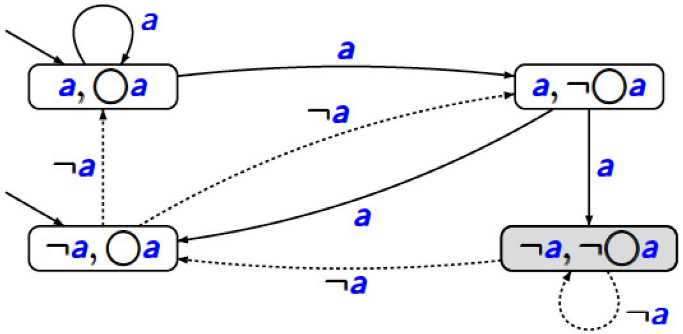
Automaton Construction

Definition: The GNBA for and LTL Formula

For LTL-formula φ, let $\mathfrak{G}_\varphi = (Q, 2^{AP}, \delta, Q_0, \mathfrak{F})$ where

- Q is the set of all elementary sets of formulas $B \subseteq cl(\varphi)$ with
  $Q_0 \;=\; \{\, B \in Q \mid \varphi \in B \,\}$
- If $A \neq B \cap AP$, then $\delta(B, A) \;=\; \varnothing$.
- $\delta(B, B \cap AP)$ is the set $B' \subseteq Q$ satisfying:
  (i) For every $\bigcirc\psi \in cl(\varphi)$: $\bigcirc\psi \in B \;\Leftrightarrow\; \psi \in B'$, and
  (ii) For every $\varphi_1 \,\mathsf{U}\, \varphi_2 \in cl(\varphi)$:
  $$\varphi_1 \,\mathsf{U}\, \varphi_2 \in B \;\Leftrightarrow\; (\varphi_2 \in B \vee (\varphi_1 \in B \wedge \varphi_1 \,\mathsf{U}\, \varphi_2 \in B'))$$
- $\mathfrak{F} \;=\; \{\, \mathfrak{F}_{\varphi_1 \mathsf{U} \varphi_2} \mid \varphi_1 \,\mathsf{U}\, \varphi_2 \in cl(\varphi) \,\}$ where
  $\mathfrak{F}_{\varphi_1 \mathsf{U} \varphi_2} \;=\; \{\, B \in Q \mid \varphi_1 \,\mathsf{U}\, \varphi_2 \notin B \text{ or } \varphi_2 \in B \,\}$

Example (1)



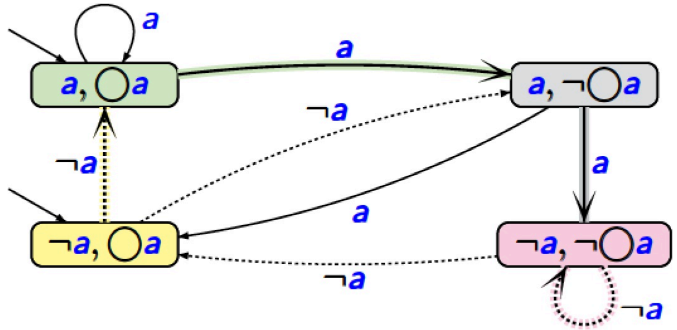
initial states: formula-sets B with $\bigcirc a \in B$

transition relation:

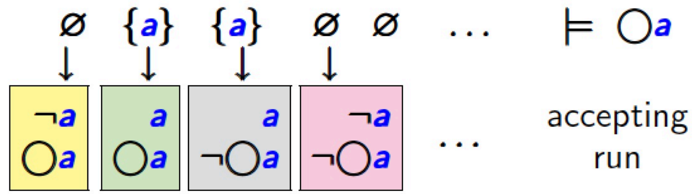
if $\bigcirc a \in B$ then $\delta(B, B \cap \{a\}) = \{B' : a \in B'\}$

if $\bigcirc a \notin B$ then $\delta(B, B \cap \{a\}) = \{B' : a \notin B'\}$

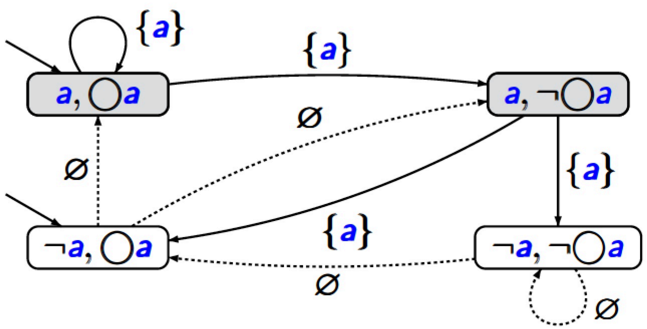
Example (2)



set of acceptance sets: $\mathcal{F} = \varnothing$



Example (3)



for all words $\sigma = A_0\, A_1\, A_2\, A_3 \ldots \in \mathcal{L}_\omega(\mathcal{G})$: $\quad A_1 = \{a\}$

proof: Let $B_0\, B_1\, B_2 \ldots$ be an accepting run for σ.

$\Longrightarrow$ $\bigcirc a \in B_0$ and therefore $a \in B_1$

$\Longrightarrow$ the outgoing edges of B_1 have label $\{a\}$

$\Longrightarrow$ $\{a\} = B_1 \cap AP = A_1$

Main Theorem

[Vardi, Wolper & Sistla 1986]

For any LTL-formula φ (over AP) there exists a GNBA $\mathfrak{G}_\varphi$ over 2^{AP} with:

(a) $Words(\varphi) = \mathcal{L}_\omega(\mathfrak{G}_\varphi)$

(b) $\mathfrak{G}_\varphi$ can be constructed in time and space $O\left(2^{|\varphi|}\right)$

(c) #accepting sets of $\mathfrak{G}_\varphi$ is bounded above by $O(|\varphi|)$.

Corollary

For every LTL-formula φ, $Words(\varphi)$ is ω-regular.

NBA More Expressive Than LTL

There is no LTL formula φ with $Words(\varphi) = E$ for the LT-property:

$$E = \left\{ A_0 A_1 A_2 \ldots \in \left(2^{\{a\}}\right)^{\omega} \mid a \in A_{2i} \text{ for } i \geq 0 \right\}$$

But there exists an NBA $\mathfrak{A}$ with $\mathfrak{L}_{\omega}(\mathfrak{A}) = E$.

Proof.

Omitted. □

Overview

Lower Bound

There exists a family of LTL formulas φ_n with $|\varphi_n| = O(poly(n))$ such that every NBA $\mathfrak{A}_{\varphi_n}$ for φ_n has at least 2^n states.

Proof.

On the black board. □

Complexity

The time and space complexity of automata-based LTL model checking is

$$O(\,|TS| \cdot 2^{|\varphi|}\,)$$

Proof.

1. the closure of LTL formula φ has size in $O(|\varphi|)$
2. the number of elementary sets is in $O(2^{|\varphi|})$
3. the number of states in the GNBA $\mathfrak{G}_{\varphi}$ is in $O(2^{|\varphi|})$
4. the number of acceptance sets in GNBA $\mathfrak{G}_{\varphi}$ is in $O(|\varphi|)$
5. the size of the NBA $\mathfrak{A}_{\varphi}$ is in $O(|\varphi| \cdot 2^{|\varphi|})$
6. the size of $TS \otimes \mathfrak{A}_{\varphi}$ is in $O(\,|TS| \cdot 2^{|\varphi|}\,)$
7. determining $TS \otimes \mathfrak{A}_{\varphi} \models \Diamond \Box \neg F$ is in $O(|TS \otimes \mathfrak{A}_{\varphi}|)$. □

Overview

Summary

- LTL model checking exploits a GNBA $\mathfrak{A}_{\neg\varphi}$ for the negation of φ
- States of the GNBA are subsets of certain sub-formulas of φ
- Taking these subsets give rises to an exponential blow-up. This cannot be avoided
- For each until-sub-formula of φ, the GNBA has one acceptance set
- Each LTL-formula describes an ω-regular LT property
- LTL is strictly less expressive than ω-regular expressions
- LTL model checking by automata is linear in the size of the transition system and exponential in the size of φ

Next Lecture

Friday November 15, 14:30