Model Checking

LTL Model Checking By Automata

[Baier & Katoen, Chapter 5.2]

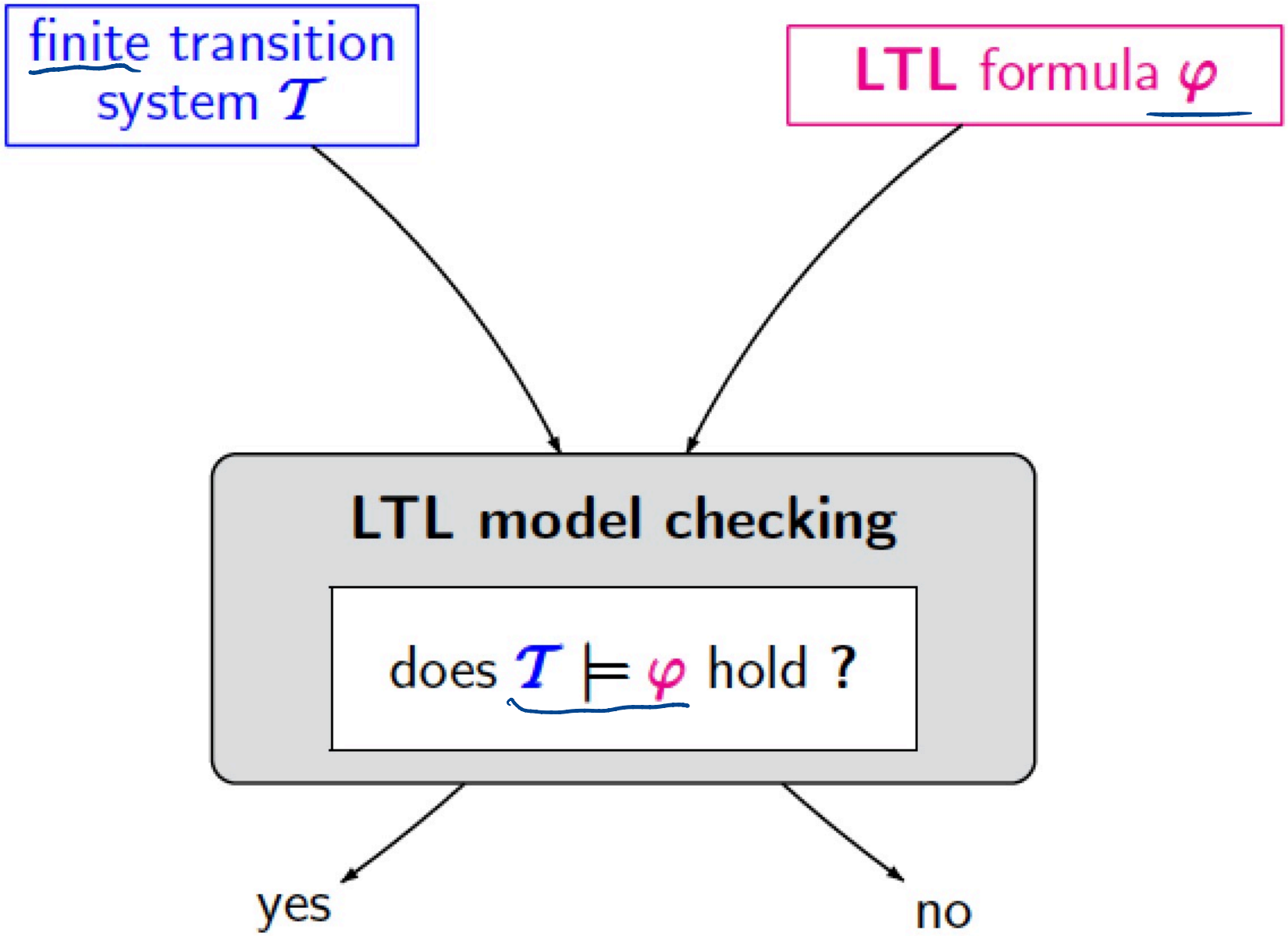
Joost-Pieter Katoen and Tim Quatmann

Software Modeling and Verification Group

RWTH Aachen, SoSe 2022

Overview

Topic


finite transition system $\mathcal{T}$
LTL formula φ
LTL model checking
does $\mathcal{T} \models \varphi$ hold ?
yes
no

Overview

LTL Syntax

Definition: LTL syntax

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

$$\varphi ::= \text{true} \mid a \mid \varphi_1 \wedge \varphi_2 \mid \neg\varphi \mid \bigcirc\varphi \mid \varphi_1 \,\mathsf{U}\, \varphi_2$$

next until

- 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

eventually

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

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

always

Semantics Over Words

Definition: LTL semantics over infinite words

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

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

$\sigma = A_0 A_1 A_2 \cdots$

$$\begin{array}{lcll}
\sigma & \vDash & \text{true} & \\
\sigma & \vDash & a & \text{iff } a \in A_0 \quad (\text{i.e., } A_0 \vDash a) \\
\sigma & \vDash & \varphi_1 \wedge \varphi_2 & \text{iff } \sigma \vDash \varphi_1 \text{ and } \sigma \vDash \varphi_2 \\
\sigma & \vDash & \neg \varphi & \text{iff } \sigma \nvDash \varphi \\
\sigma & \vDash & \bigcirc \varphi & \text{iff } \sigma[1..] = A_1 A_2 A_3 \ldots \vDash \varphi \\
\sigma & \vDash & \varphi_1 \, \mathsf{U} \, \varphi_2 & \text{iff } \exists j \geq 0.\ \sigma[j..] \vDash \varphi_2 \text{ and } \sigma[i..] \vDash \varphi_1,\ 0 \leq i < j
\end{array}$$

for $\sigma = A_0 A_1 A_2 \ldots$, let $\sigma[i..] = A_i A_{i+1} A_{i+2} \ldots$ be the suffix of σ from index i on.

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

$$\sigma \models \Diamond\varphi \quad \text{iff} \quad \exists j \geq 0.\ \sigma[j..] \models \varphi$$

$$\sigma \models \Box\varphi \quad \text{iff} \quad \forall j \geq 0.\ \sigma[j..] \models \varphi$$

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

$$\sigma \models \Diamond\varphi \quad \text{iff} \quad \exists j \geq 0.\ \sigma[j..] \models \varphi$$

$$\sigma \models \Box\varphi \quad \text{iff} \quad \forall j \geq 0.\ \sigma[j..] \models \varphi$$

$$\sigma \models \Box\Diamond\varphi \quad \text{iff} \quad \underbrace{\forall j \geq 0.\ \exists i \geq j.\ \sigma[i\ldots] \models \varphi}_{\text{infinitely often } \varphi}$$

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

$$\sigma \models \Diamond\varphi \quad \text{iff} \quad \exists j \geq 0.\ \sigma[j..] \models \varphi$$

$$\sigma \models \Box\varphi \quad \text{iff} \quad \forall j \geq 0.\ \sigma[j..] \models \varphi$$

$$\sigma \models \Box\Diamond\varphi \quad \text{iff} \quad \underbrace{\forall j \geq 0.\ \exists i \geq j.\ \sigma[i\ldots] \models \varphi}_{\text{infinitely often } \varphi}$$

$$\sigma \models \Diamond\Box\varphi \quad \text{iff} \quad \underbrace{\exists j \geq 0.\forall i \geq j.\ \sigma[i\ldots] \models \varphi}_{\text{persistence of } \varphi}$$

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 $s \in S$:

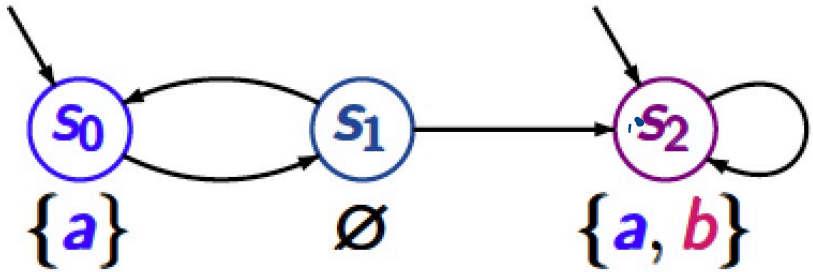
$$s \models \varphi \quad \text{iff} \quad \forall \pi \in Paths(s).\ \pi \models \varphi$$

- For transition system TS:

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

iff $\forall \sigma \in Traces(TS) : \sigma \models \varphi$

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 $s_2 \models b$, $s_0 \models \bigcirc\neg a$

refer to same pos.

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.

LTL Model Checking By Automata

In this lecture we show:

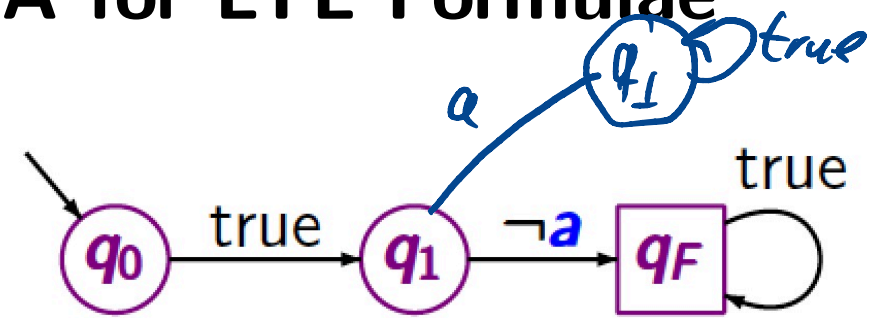
For any LTL-formula φ (over AP) there exists an NBA $\mathfrak{A}_\varphi$ over 2^{AP} with

$$\mathit{Words}(\varphi) = \mathfrak{L}_\omega(\mathfrak{A}_\varphi).$$

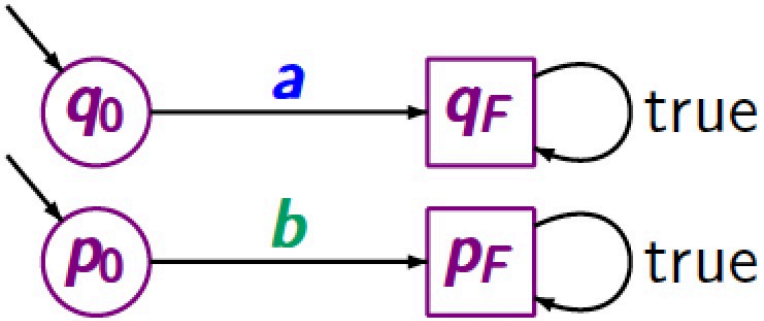
- $\mathit{Words}(\varphi)$ is ω-regular
- Given $\mathfrak{A}_\varphi$, we already know how to check $\underbrace{TS \models \mathfrak{L}_\omega(\mathfrak{A}_\varphi)}_{\text{iff } TS \models \varphi}$

Lecture #6

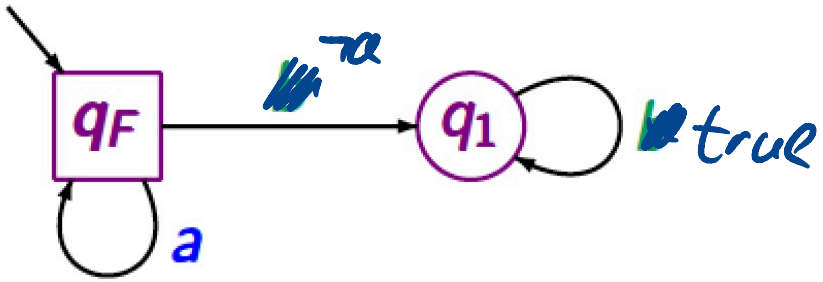
NBA for LTL Formulae



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



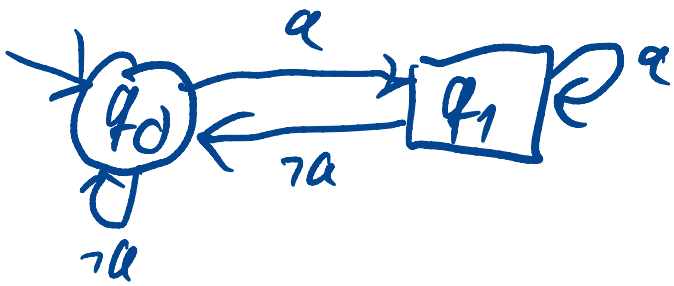
$$\mathcal{L}_\omega(\mathcal{A}) = \mathit{Words}(a \vee b)$$



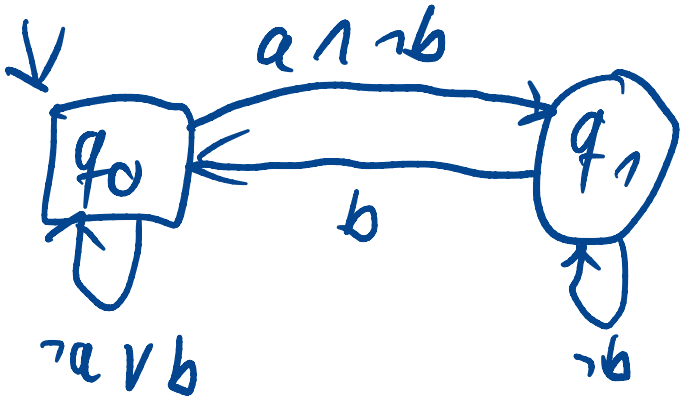
$$\mathcal{L}_\omega(\mathcal{A}) = \mathit{Words}(\Box a)$$

NBA for LTL Formulae

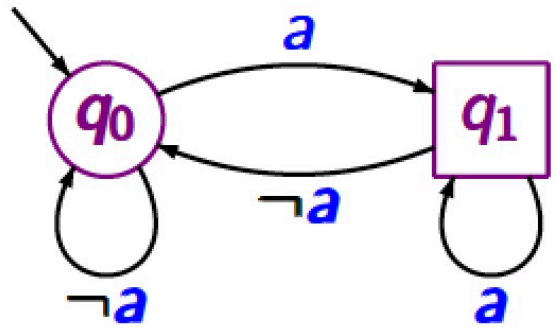
words(□◇ a)



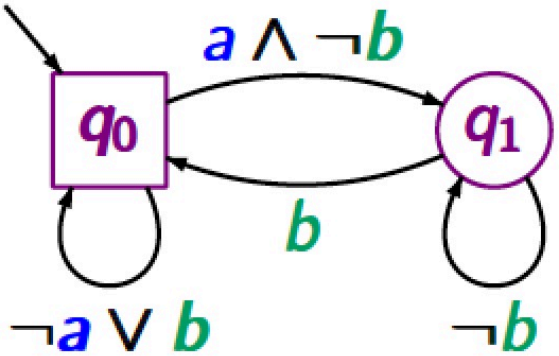
words(□ (a → ◇b))



NBA for LTL Formulae



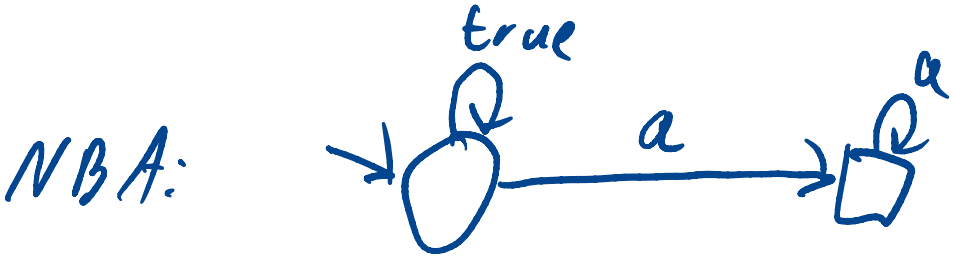
$$\mathcal{L}_\omega(\mathcal{A}) = \mathit{Words}(\Box\Diamond a)$$



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

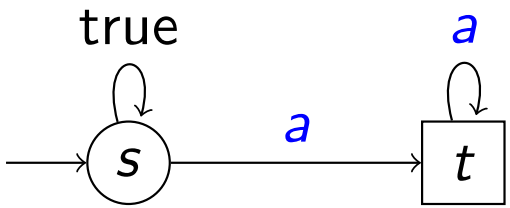
e.g., $\varnothing\,\varnothing\,\varnothing\,\varnothing\ldots = \varnothing^\omega$
$(\{a\}\,\{b\})^\omega$
} are accepted by $\mathcal{A}$

Büchi Automaton for LTL Formula $\Diamond\Box a$



Büchi Automaton for LTL Formula $\Diamond\Box a$

NBA:



Recall from Lecture #5:

No **D**BA for *Words*($\Diamond\Box a$) exists

- There is a need to use **N**BA

A Naive Attempt

$$TS \models \varphi \quad \text{if and only if} \quad Traces(TS) \subseteq Words(\varphi)$$

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

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

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

(complement Aut.)

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

$TS \models \varphi$

as on prev. slide

$$
\begin{aligned}
&\text{if and only if} && Traces(TS) \subseteq Words(\varphi) \\
&\text{if and only if} && Traces(TS) \subseteq \mathfrak{L}_\omega(\mathfrak{A}_\varphi) \\
&\text{if and only if} && Traces(TS) \cap \overline{\mathfrak{L}_\omega(\mathfrak{A}_\varphi)} = \varnothing \\
&\text{if and only if} && Traces(TS) \cap \mathfrak{L}_\omega(\overline{\mathfrak{A}_\varphi}) = \varnothing \\
&\text{if and only if} && Traces(TS) \cap \mathfrak{L}_\omega(\mathfrak{A}_{\neg\varphi}) = \varnothing \\
&\text{if and only if} && TS \otimes \mathfrak{A}_{\neg\varphi} \models \Diamond\Box\, \neg F
\end{aligned}
$$

persistence check (Nested DFS)

$\otimes$ Product

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

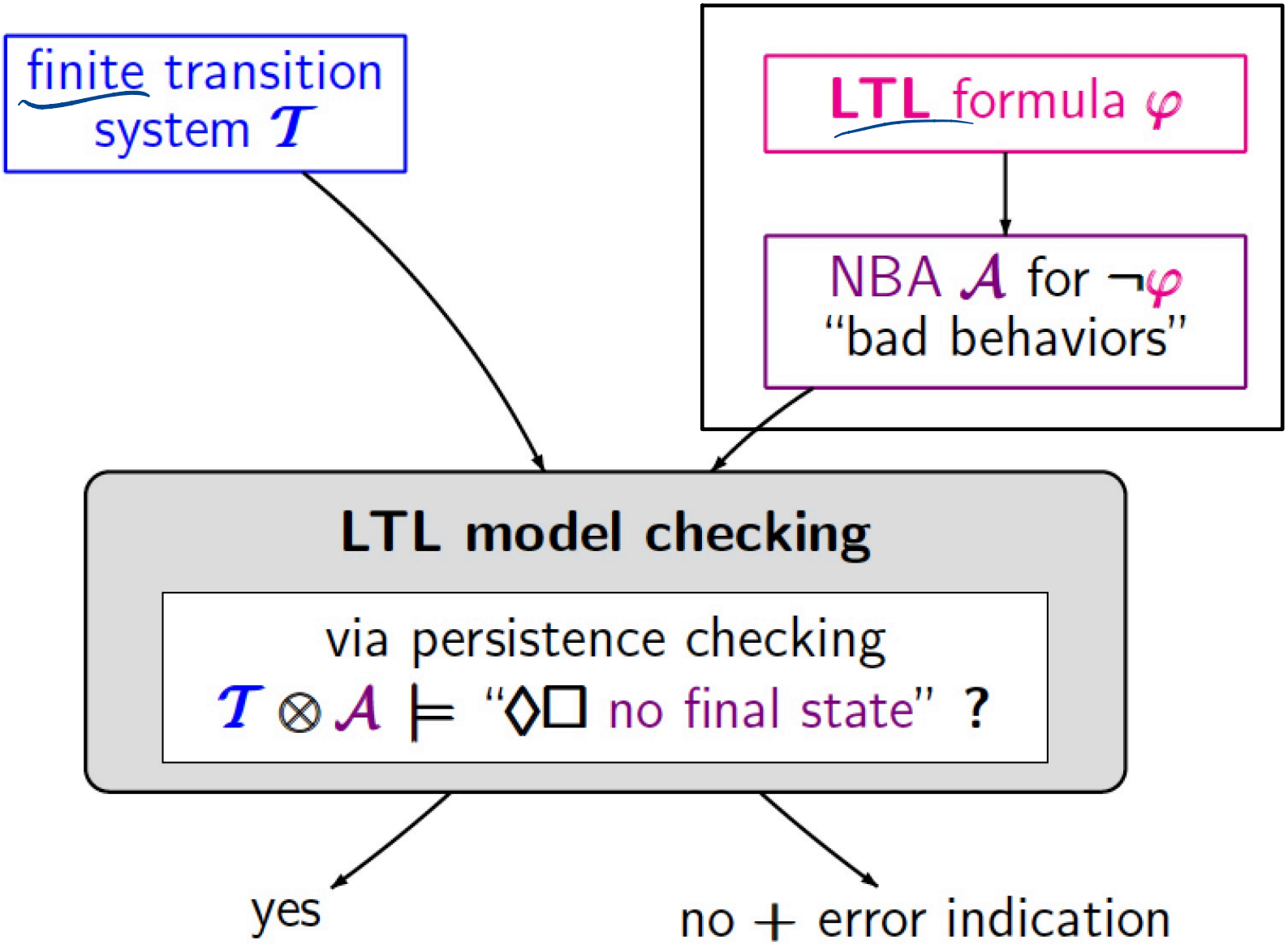
Approach

$$
\begin{aligned}
TS \models \varphi \quad & \text{if and only if} \quad Traces(TS) \subseteq Words(\varphi) \\
& \text{if and only if} \quad Traces(TS) \subseteq \mathfrak{L}_\omega(\mathfrak{A}_\varphi) \\
& \text{if and only if} \quad Traces(TS) \cap \overline{\mathfrak{L}_\omega(\mathfrak{A}_\varphi)} = \varnothing \\
& \text{if and only if} \quad Traces(TS) \cap \mathfrak{L}_\omega(\overline{\mathfrak{A}_\varphi}) = \varnothing \\
& \text{if and only if} \quad Traces(TS) \cap \mathfrak{L}_\omega(\mathfrak{A}_{\neg\varphi}) = \varnothing \\
& \text{if and only if} \quad TS \otimes \mathfrak{A}_{\neg\varphi} \models \Diamond\Box\, \neg F
\end{aligned}
$$

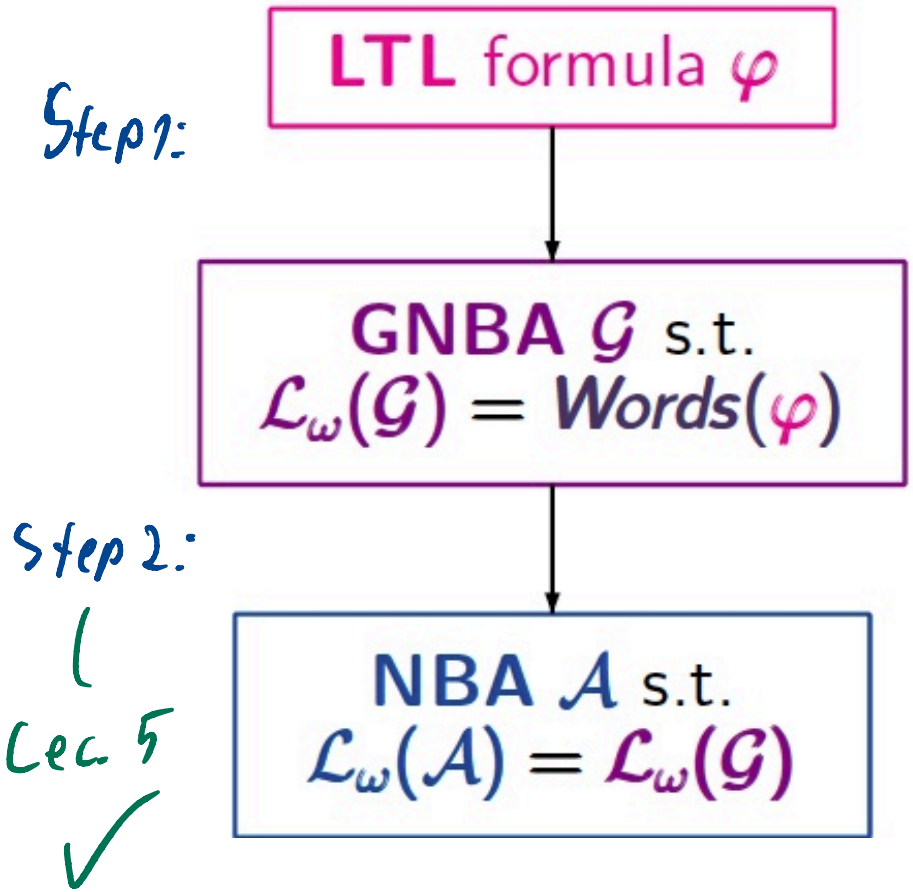
where F is the set of accept states of NBA $\mathfrak{A}_{\neg\varphi}$.

LTL model checking is thus reduced to persistence checking

Automata-Based LTL Model Checking



From LTL to NBA



generalized NBA
k acceptance sets

↓ k copies of $\mathcal{G}$

nondeterministic
Büchi automaton
1 acceptance set

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

Lec. 5

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?

Given: an LTL-formula φ over AP

- 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

Task: construct a GNBA $\mathfrak{G}_\varphi$ over 2^{AP} with $\mathfrak{L}_\omega(\mathfrak{G}_\varphi) = \mathit{Words}(\varphi)$

GNBA $\mathfrak{G}_\varphi$—Intuition (1)

- States of $\mathfrak{G}_\varphi$ encode a "guess":

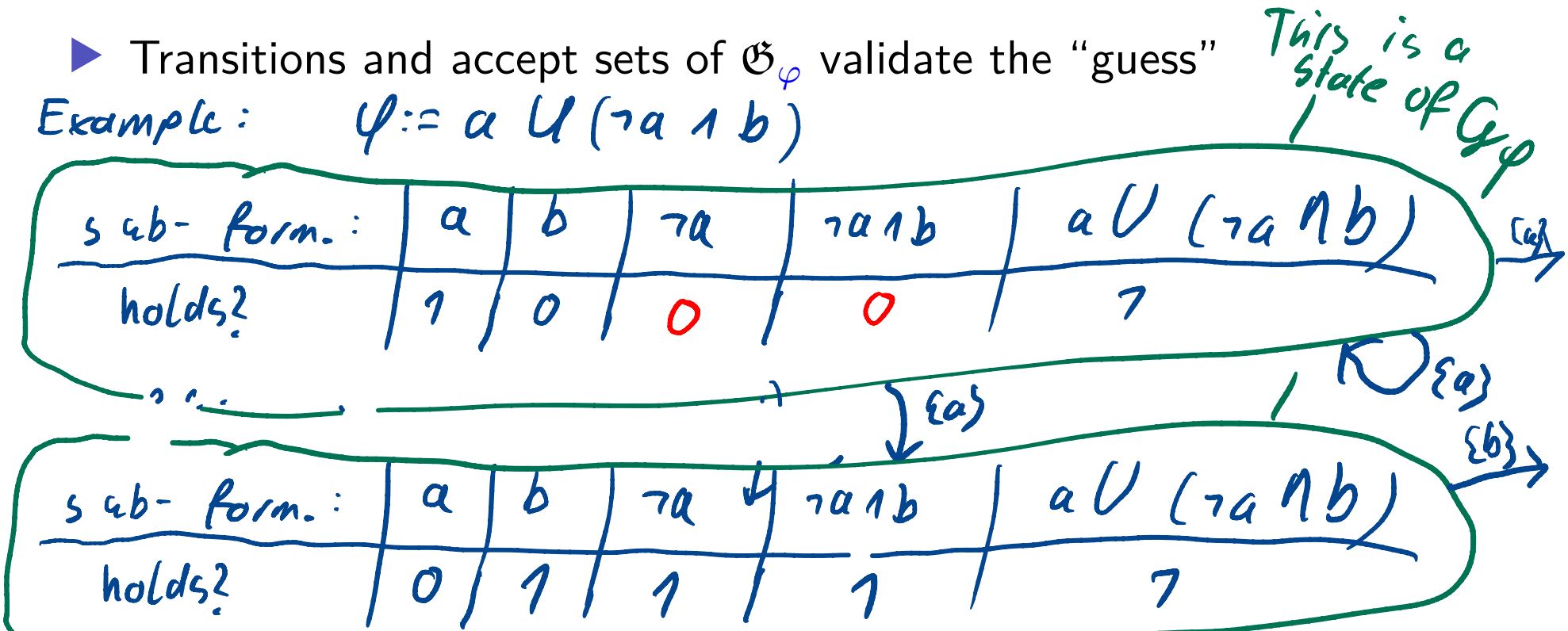
  Which sub-formulas of φ hold at the current position?

- The guess has to be consistent

  Example: if we guess that a holds, then $\neg a \wedge b$ cannot hold as well

  ✓ ✗

- Transitions and accept sets of $\mathfrak{G}_\varphi$ validate the "guess"



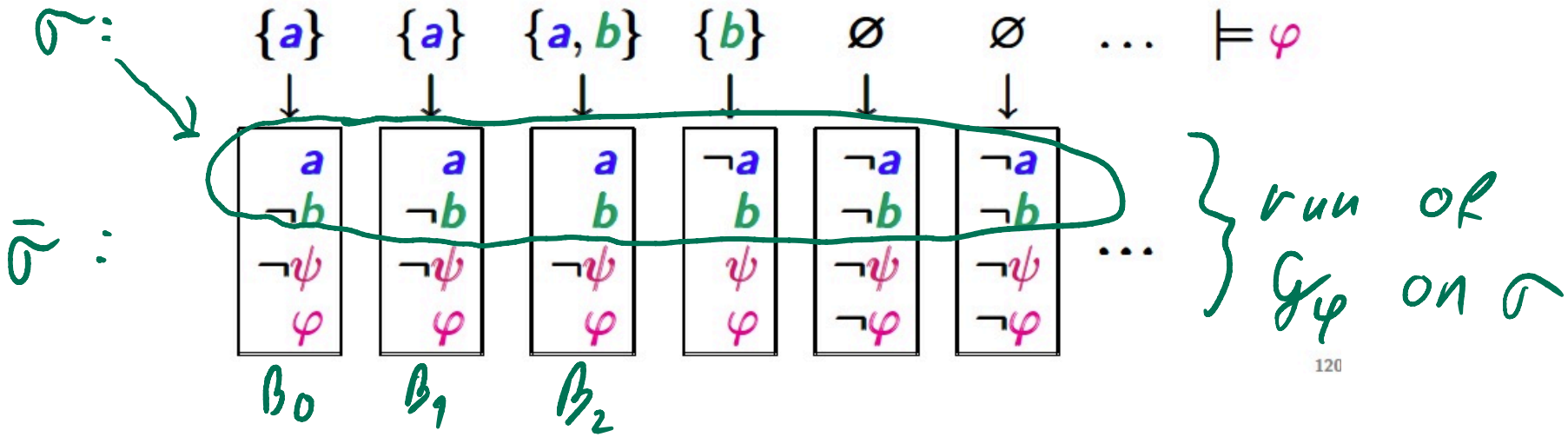
GNBA $\mathfrak{G}_\varphi$—Intuition (2)

- States of $\mathfrak{G}_\varphi$ are elementary sets B_i of sub-formulas in φ
  - for $\sigma = A_0 A_1 \ldots \in \mathit{Words}(\varphi)$, 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

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

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

Example: $\varphi = a\,\mathbf{U}(\neg a \wedge b)$ $\quad \psi = \neg a \wedge b$



GNBA $\mathfrak{G}_\varphi$—Intuition (2)

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

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

  - $\bar{\sigma}$ 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 $\sigma \vDash \varphi$

- Elementary set B_i is an initial state iff $\varphi \in B_i$

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:

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 $\varphi_2 \in B$
   - $\psi \notin B \Leftrightarrow \neg\psi \in B$
   - $\text{true} \in cl(\varphi) \Rightarrow \text{true} \in B$

propositional logic

for each subform. γ either γ or $\neg\gamma$ is in B

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 $\varphi_2 \in B$
   - $\psi \notin B \Leftrightarrow \neg\psi \in B$
   - $\text{true} \in cl(\varphi) \Rightarrow \text{true} \in B$
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 $\varphi_2 \notin B \Rightarrow \varphi_1 \in B$

– antic

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

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
  $Q_0 = \{ B \in Q \mid \varphi \in B \}$

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
  $$Q_0 = \{ B \in Q \mid \varphi \in B \}$$

Transitions:

- If $A \neq B \cap AP$, then $\delta(B, A) = \varnothing$.
- For $B' \in Q$: $B' \in \delta(B, B \cap AP)$ iff
  - (i) For every $\bigcirc \psi \in cl(\varphi)$: $\bigcirc \psi \in B \Leftrightarrow \psi \in B'$, and
  - (ii) For every $\varphi_1 \,\mathsf{U}\, \varphi_2 \in cl(\varphi)$:

$$\varphi_1 \,\mathsf{U}\, \varphi_2 \in B \Leftrightarrow \big(\varphi_2 \in B \vee (\varphi_1 \in B \wedge \varphi_1 \,\mathsf{U}\, \varphi_2 \in B')\big)$$

expansion law:

$\varphi_1 \,\mathsf{U}\, \varphi_2 \equiv \varphi_2 \vee (\varphi_1 \wedge \bigcirc\, \varphi_1 \,\mathsf{U}\, \varphi_2)$

Automaton Construction

Definition: The GNBA for and LTL Formula

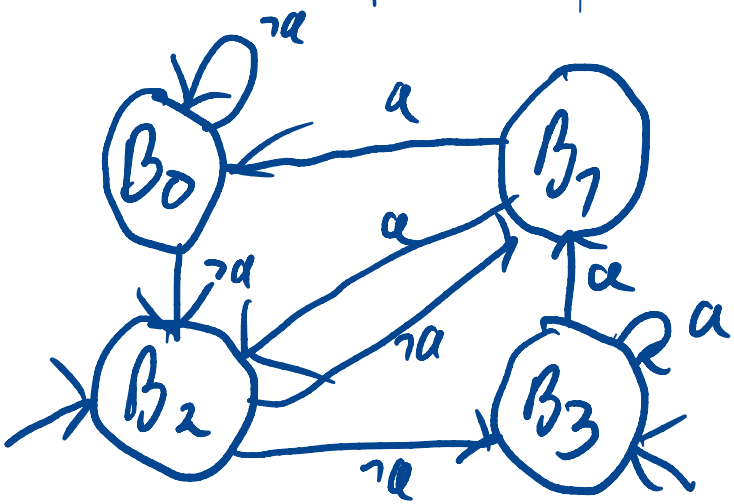
For LTL-formula φ, let $\mathfrak{G}_\varphi = (Q, 2^{AP}, \delta, Q_0, \mathfrak{F})$ where

- 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 $\delta(B, A) = \varnothing$.
- For $B' \in Q$: $B' \in \delta(B, B \cap AP)$ iff
  - (i) For every $\bigcirc \psi \in cl(\varphi)$: $\bigcirc \psi \in B \iff \psi \in B'$, and
  - (ii) For every $\varphi_1 \,\mathsf{U}\, \varphi_2 \in cl(\varphi)$:
    $$\varphi_1 \,\mathsf{U}\, \varphi_2 \in B \iff \big(\varphi_2 \in B \vee (\varphi_1 \in B \wedge \varphi_1 \,\mathsf{U}\, \varphi_2 \in B')\big)$$
- $\mathfrak{F} = \{ F_{\varphi_1 \,\mathsf{U}\, \varphi_2} \mid \varphi_1 \,\mathsf{U}\, \varphi_2 \in cl(\varphi) \}$ where
  $$F_{\varphi_1 \,\mathsf{U}\, \varphi_2} = \{ B \in Q \mid \varphi_1 \,\mathsf{U}\, \varphi_2 \notin B \text{ or } \varphi_2 \in B \}$$

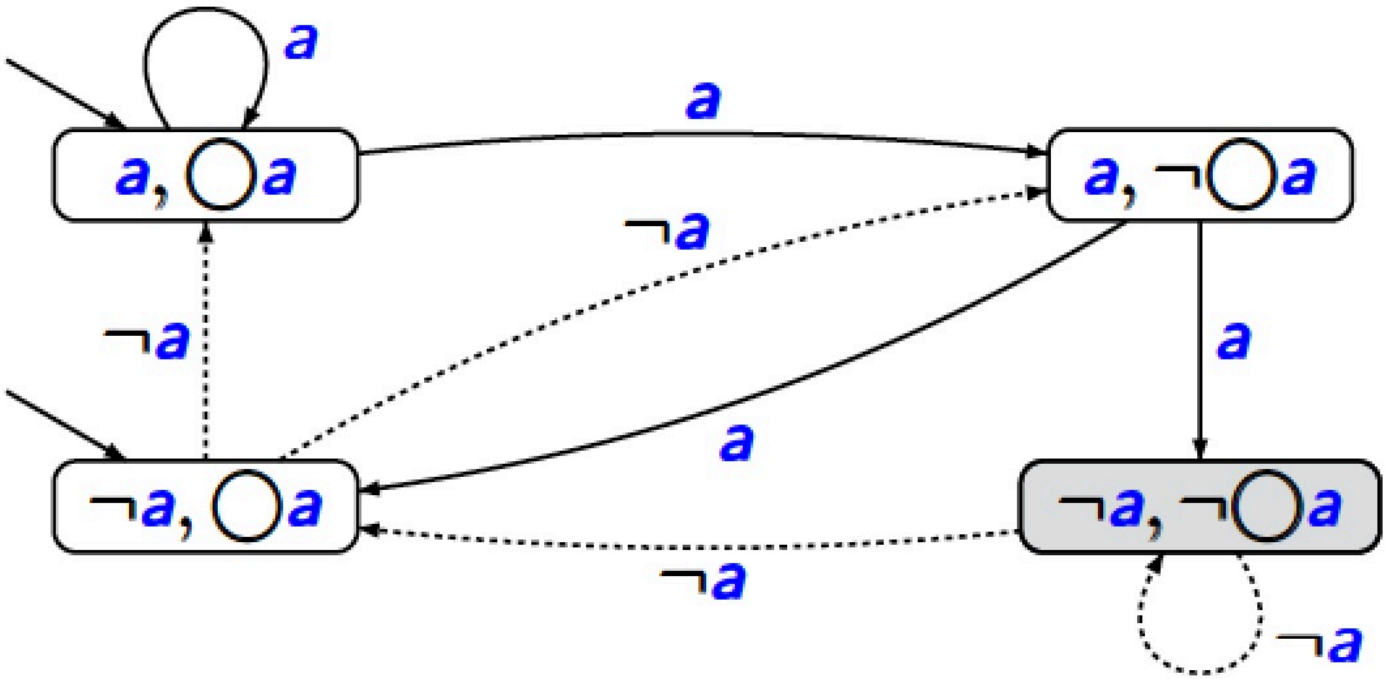
Example: $\varphi := \bigcirc a$

$cl(\varphi)$	a	$\neg a$	$\bigcirc a$	$\neg \bigcirc a$
B_0	0	1	0	1
B_1	1	0	0	1
B_2	0	1	1	0
B_3	1	0	1	0

elem. sets } init states



Example: $\varphi := \bigcirc a$



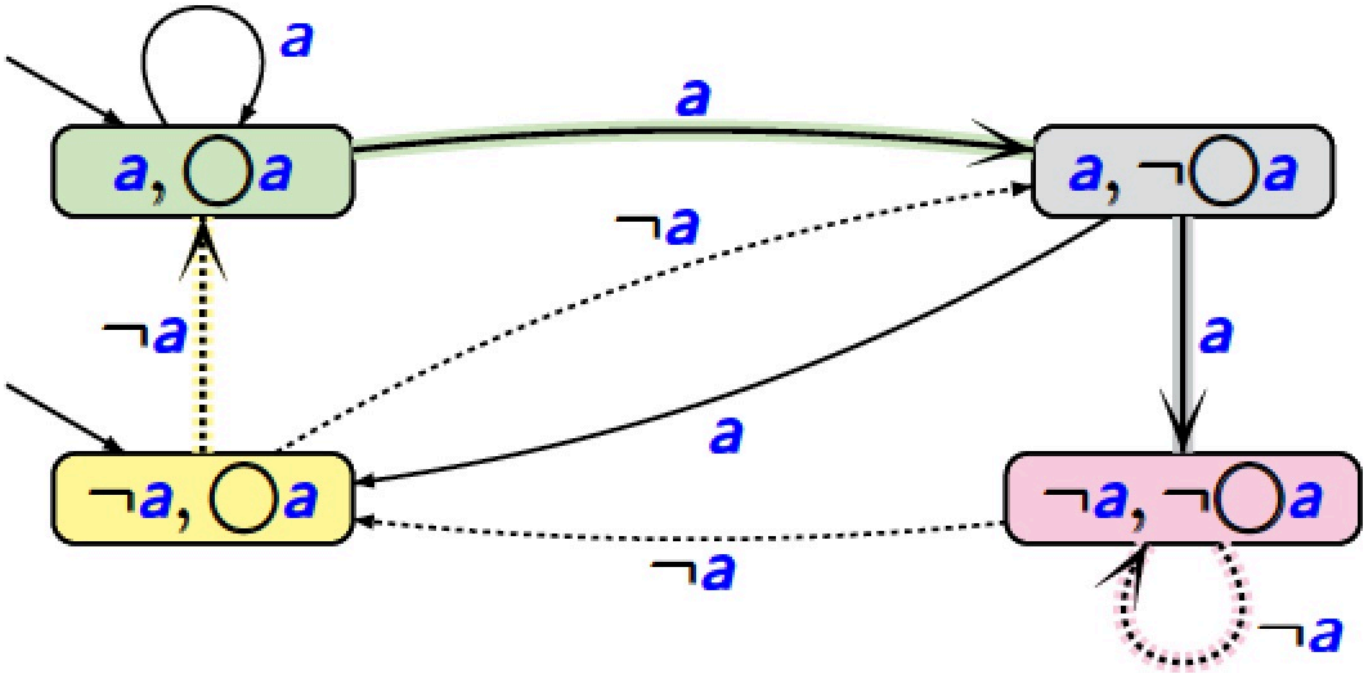
initial states: formula-sets B with $\bigcirc a \in B$

transition relation:

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

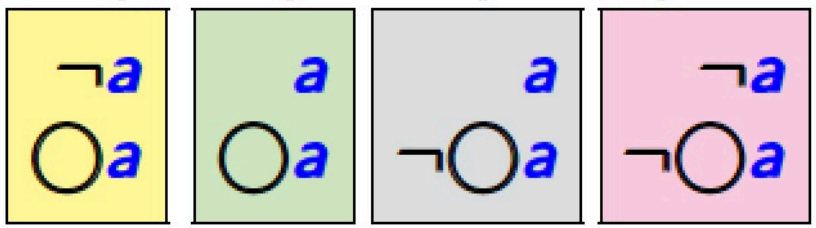
if $\bigcirc a \notin B$ then $\delta(B, B \cap \{a\}) = \{B' : a \notin B'\}$

Example: $\varphi := \bigcirc a$



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

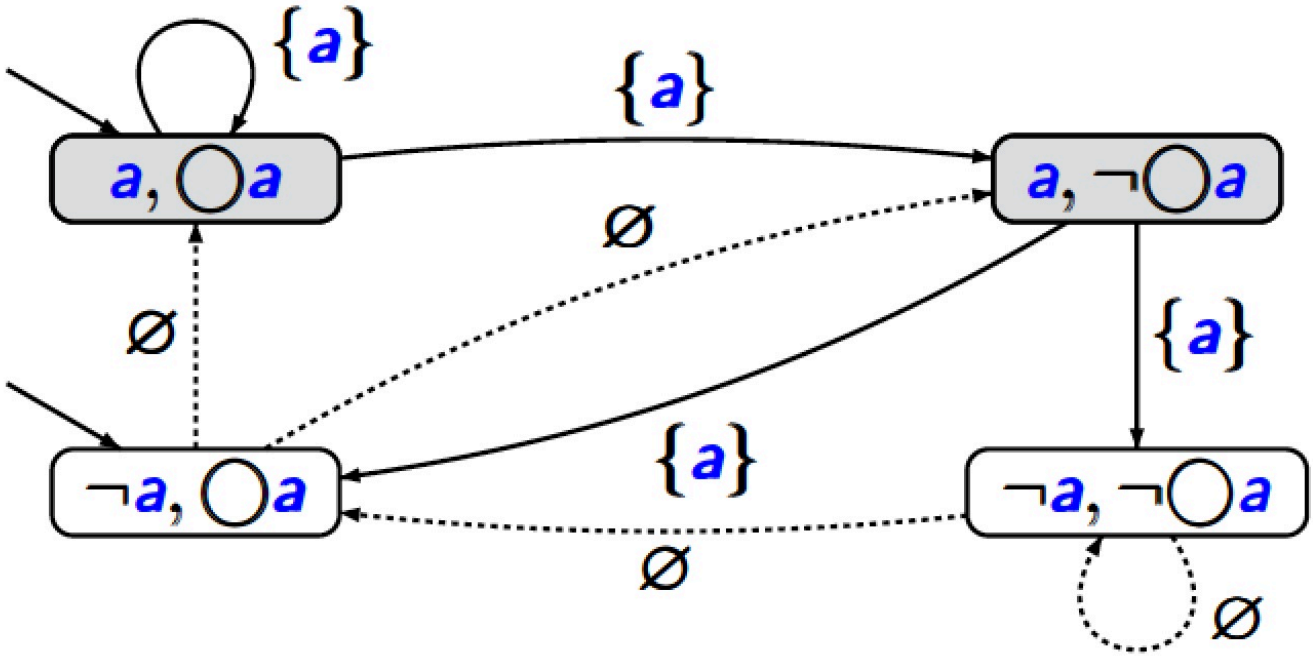
$\varnothing \quad \{a\} \quad \{a\} \quad \varnothing \quad \varnothing \quad \ldots \quad \models \bigcirc a$



$\ldots$

accepting run

Example: $\varphi := \bigcirc a$



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

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 $\{a\}$

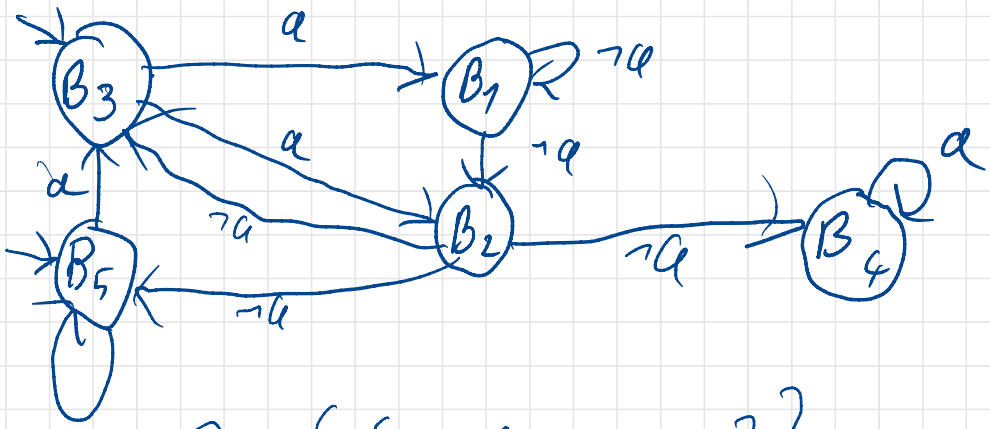
$\Longrightarrow$ $\{a\} = B_1 \cap AP = A_1$

$$\varphi = (a \wedge \bigcirc a) \mathbin{U} (a \wedge \neg \bigcirc a)$$

elementary sets: $= \varphi_1$ $= \varphi_2$

	a	$\bigcirc a$	$a \wedge \bigcirc a$	$a \wedge \neg \bigcirc a$	φ
B_1	0	0	0	0	0
B_2	0	1	0	0	0
B_3	1	0	0	1	1
B_4	1	1	1	0	0
B_5	1	1	1	0	1

Initial states



$\mathcal{F} = \{ \{B_1, B_2, B_3, B_4\} \}$

(see next side for more details)

- For $B' \in Q$: $B' \in \delta(B, B \cap AP)$ iff
  - (i) For every $\bigcirc\psi \in cl(\varphi)$: $\bigcirc\psi \in B \iff \psi \in B'$, and
  - (ii) For every $\varphi_1 \,U\, \varphi_2 \in cl(\varphi)$:

$$\varphi_1 \,U\, \varphi_2 \in B \iff (\varphi_2 \in B \vee (\varphi_1 \in B \wedge \varphi_1 \,U\, \varphi_2 \in B'))$$

equivalent: $\varphi_1 U \varphi_2 \notin B \iff (\varphi_2 \notin B \wedge (\varphi_1 \notin B \vee \varphi_1 U \varphi_2 \notin B'))$

Transitions at B_1:

$\delta(B_1, \underbrace{\emptyset}_{B_1 \cap AP}) = B'$, where (i) $a \notin B'$ (since $\bigcirc a \notin B_1$)

(ii) $\underbrace{\varphi_2 \notin B_1}_{\text{true}} \wedge (\underbrace{\varphi_1 \notin B_1}_{\text{true}} \vee \dots)$ (since $\varphi \notin B_1$)

$\rightsquigarrow B' \in \{B_1, B_2\}$

Transitions at B_2:

$\delta(B_2, \emptyset) = B'$, where (i) $a \in B'$ (since $\bigcirc a \in B_2$)

(ii) $\underbrace{\varphi_2 \notin B_2}_{\text{true}} \wedge (\underbrace{\varphi_2 \notin B_2}_{\text{true}} \vee \dots)$ (since $\varphi \notin B_2$)

$\rightsquigarrow B' \in \{B_3, B_4, B_5\}$

Transitions at B_3:

$\delta(B_3, \{a\}) = B'$, where (i) $a \notin B'$ (since $\bigcirc a \notin B_3$)

(ii) $\underbrace{\varphi_2 \in B_3}_{\text{true}} \vee \dots$ (since $\varphi \in B_3$)

$\rightsquigarrow B' \in \{B_1, B_2\}$

- For $B' \in Q$: $B' \in \delta(B, B \cap AP)$ iff
  - (i) For every $\bigcirc\psi \in cl(\varphi)$: $\bigcirc\psi \in B \iff \psi \in B'$, and
  - (ii) For every $\varphi_1 \,U\, \varphi_2 \in cl(\varphi)$:

$$\varphi_1 \,U\, \varphi_2 \in B \iff (\varphi_2 \in B \vee (\varphi_1 \in B \wedge \varphi_1 \,U\, \varphi_2 \in B'))$$

equivalent: $\varphi_1 U \varphi_2 \notin B \iff (\varphi_2 \notin B \wedge (\varphi_1 \notin B \vee \varphi_1 U \varphi_2 \notin B'))$

Transitions at B_4:

$\delta(B_4, \{a\}) = B'$, where (i) $a \in B'$ (since $\bigcirc a \in B_4$)

(ii) $\varphi_2 \notin B_4 \wedge (\varphi_1 \notin B_4 \vee \varphi_1 U \varphi_2 \notin B')$ (since $\varphi \notin B_4$)

($\varphi_2 \notin B_4$: true; $\varphi_1 \notin B_4$: false)

$\rightsquigarrow \varphi \notin B'$

$\rightsquigarrow B' \in \{B_4\}$

Transitions at B_5:

$\delta(B_5, \{a\}) = B'$, where (i) $a \in B'$ (since $\bigcirc a \in B_5$)

(ii) $\varphi_2 \in B_5 \vee (\varphi_1 \in B_5 \wedge \varphi_1 U \varphi_2 \in B')$

($\varphi_2 \in B_5$: false; $\varphi_1 \in B_5$: true)

$\rightsquigarrow \varphi \in B'$ (since $\varphi \in B_5$)

$\rightsquigarrow B' \in \{B_3, B_5\}$

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

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

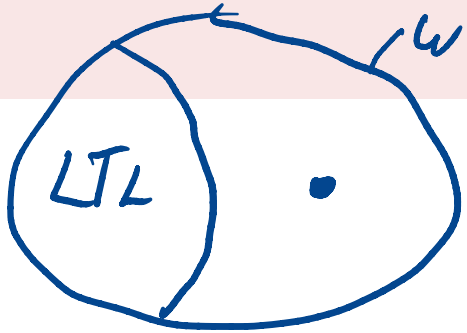
(c) #accepting sets of $\mathfrak{G}_\varphi$ is bounded above by $O(|\varphi|)$.

elementary sets i.e. sets of subf.

└ # until op. in φ

Corollary

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



For any LTL formula φ and GNBA G_φ

$$L_\omega(G_\varphi) = \text{Words}(\varphi)$$

Proof:

"$\supseteq$" let $\sigma \in \text{Words}(\varphi)$ assume $\sigma = A_0 A_1 \ldots$ where $A_i \subseteq cl(\varphi)$

that is,

$\sigma = (B_0 \cap AP)(B_1 \cap AP) \ldots$ where $A_i \cap cl(\varphi) = B_i \cap AP$

we have:

$$B_i = \{\psi \in cl(\varphi) \mid A_i A_{i+1} \ldots \models \psi\} \qquad (*)$$

① To show: $B_0 B_1 B_2 \ldots$ is a run of G_φ

② $B_0 B_1 B_2 \ldots$ is an accepting run of G_φ

$\varphi \in B_0$, $B_{i+1} \in \delta(B_i, A_i)$

ad ② let $\mathcal{F} = \{F_1, \ldots, F_k\}$. To prove $B_i \in F_j$ for inf. many i (for each j). let F_j correspond to $\varphi_{1,j} \cup \varphi_{2,j} \in cl(\varphi)$. By contraposition.

Assume $B_i \in F_j$ for finitely many i (▲)

It holds by definition

$$F_{\varphi_1 \cup \varphi_2} = \{ B \mid \varphi_1 \cup \varphi_2 \notin B \text{ or } \varphi_2 \in B \}$$

$B_i \notin F_j$ implies $\varphi_{1,j} \cup \varphi_{2,j} \in B_i$ and $\varphi_{2,j} \notin B_i$

It follows (by (*))

$B_i \notin F_j$ implies $A_i A_{i+1} \ldots \models \varphi_{1,j} \cup \varphi_{2,j}$ (1)

and $A_i A_{i+1} \ldots \not\models \varphi_{2,j}$ (2)

From (1), it follows $A_k A_{k+1} \ldots \models \varphi_{2,j}$ for some $k \geq i$

By (2), we have $k > i$. Then $\varphi_{2,j} \in B_k$ and by definition of F_j, $\boxed{B_k \in F_j}$.

Applying the reasoning for $B_i \in F_j$ now to B_k, yields that there are infinitely many indices l s.t. $B_l \in F_j$. Contradiction to ▲.

Together, this yields

$B_0 B_1 \ldots$ is an accepting run for φ.

Thus: $\sigma = A_0 A_1 A_2 \ldots \in L_\omega(\mathcal{G}_\varphi)$

"$\subseteq$"

let $\sigma = A_0 A_1 \ldots \in L_\omega(G_\varphi)$.

To prove: $\underbrace{\sigma \in \text{Words}(\varphi)}$

$\sigma \models \varphi$.

G_φ has an accepting run $B_0 B_1 \ldots$ for σ.

Since $\delta(B_i, A_i) = \emptyset$ if $A_i \neq B_i \cap AP$, it follows $A_i = B_i \cap AP$. (for $i \geq 0$) Thus:

$$\sigma = (B_0 \cap AP)(B_1 \cap AP) \ldots\ldots$$

Lemma: $\forall \psi \in cl(\varphi)$ and

$B_0 B_1 B_2 \ldots \in Q^\omega$ and

$A_0 A_1 A_2 \ldots \in (2^{AP})^\omega$, it holds!

If (i) $B_{i+1} \in \delta(B_i, A_i)$, and

(ii) $\overset{\infty}{\exists} i \,.\, B_i \in F_j$ for all $F_j \in \mathcal{F}$

Then

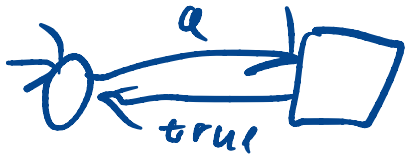
$\underbrace{\psi \in B_0}$ iff $A_0 A_1 A_2 \ldots \models \psi$

state in G_φ

How to prove this?

induction on ψ.

NBA More Expressive Than LTL



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

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

a a

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

Proof.

Omitted. □

$\varphi = a \wedge \Box(a \Rightarrow \bigcirc\bigcirc a)$ is too restrictive

e.g. $\sigma = a\,a\,a\,\emptyset\,a^\omega \not\models \varphi$ but $\sigma \in E$

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. □

$words(\varphi_n) = \{ \sigma\sigma \mid \sigma \in (2^{AP})^n \} \cdot (2^{AP})^\omega$

Proof (sketch)

L_n = Words (φ_n) where φ_n is as follows:

$$\varphi_n = \bigwedge_{a \in AP} \bigwedge_{0 \le i < n} \left(O^i a \iff O^{n+i} a \right)$$

$O^j a$ = j-fold application of the next operator to a

$$O^1 \varphi = O\varphi \qquad O^{n+1} \varphi = O\, O^n \varphi$$

Words accepted by the NBA for φ_n have the form

$$\underbrace{A_1 A_2 \dots A_n}\ \underbrace{A_1 \dots A_n}\ \emptyset\emptyset\emptyset\emptyset\dots$$

NBA A_φ needs exponentially many states, as all combination $a \in A_j$ and $a \notin A_j$ for $j < i$ have to be taken into account for A_i. ⊠

Complexity

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

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

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 $TS \otimes \mathfrak{A}_\varphi \vDash \Diamond\Box\neg F$ 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

Thursday May 12, 12:30