LTL Model Checking

Lecture #16 of Model Checking

Joost-Pieter Katoen

Lehrstuhl 2: Software Modeling & Verification

E-mail: `katoen@cs.rwth-aachen.de`

December 16, 2008

Overview Lecture #16

$\Rightarrow$ Repetition: LTL and GNBA

- From LTL to GNBA

Recall: Linear Temporal Logic

modal logic over infinite sequences [Pnueli 1977]

- Propositional logic
  - $a \in AP$ — atomic proposition
  - $\neg \varphi$ and $\varphi \wedge \psi$ — negation and conjunction
- Temporal operators
  - $\bigcirc \varphi$ — neXt state fulfills φ
  - $\varphi \, \mathsf{U} \, \psi$ — φ holds Until a ψ-state is reached
- Auxiliary temporal operators
  - $\Diamond \varphi \equiv \text{true} \, \mathsf{U} \, \varphi$ — eventually φ
  - $\Box \varphi \equiv \neg \Diamond \neg \varphi$ — always φ

LTL model-checking problem

The following decision problem:

Given finite transition system TS and LTL-formula φ:

yields "yes" if $TS \models \varphi$, and "no" (plus a counterexample) if $TS \not\models \varphi$

NBA for LTL-formulae

A first attempt

$$TS \models \varphi \quad \text{if and only if} \quad \mathit{Traces}(TS) \subseteq \underbrace{\mathit{Words}(\varphi)}_{\mathcal{L}_\omega(\mathcal{A}_\varphi)}$$

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

but complementation of NBA is quadratically exponential
if $\mathcal{A}$ has n states, $\overline{\mathcal{A}}$ has c^{n^2} states in worst case

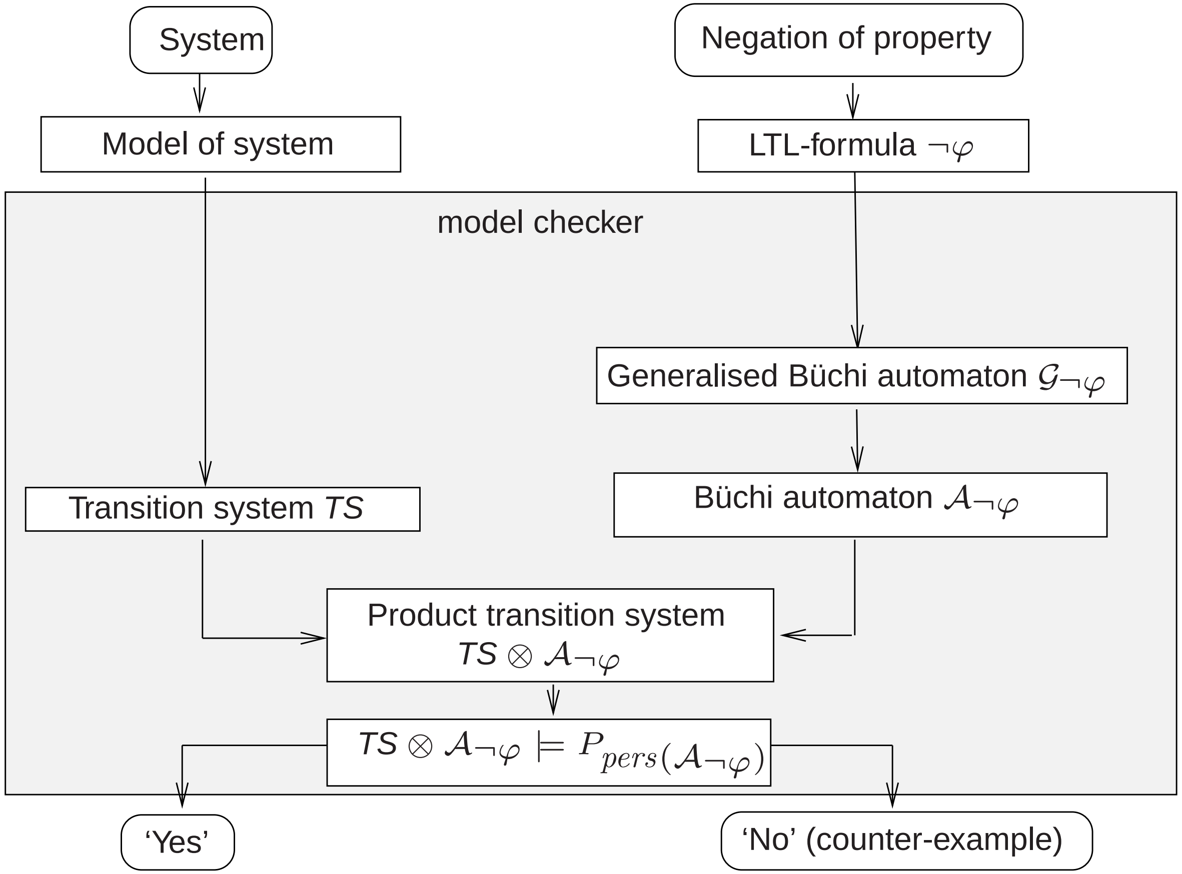
use the fact that $\mathcal{L}_\omega(\overline{\mathcal{A}_\varphi}) \; = \; \mathcal{L}_\omega(\mathcal{A}_{\neg\varphi})$!

Observation

$$
\begin{aligned}
\mathit{TS} \models \varphi \quad & \text{if and only if} \quad \mathit{Traces}(\mathit{TS}) \subseteq \mathit{Words}(\varphi) \\
& \text{if and only if} \quad \mathit{Traces}(\mathit{TS}) \cap \left((2^{AP})^\omega \setminus \mathit{Words}(\varphi) \right) = \varnothing \\
& \text{if and only if} \quad \mathit{Traces}(\mathit{TS}) \cap \underbrace{\mathit{Words}(\neg\varphi)}_{\mathcal{L}_\omega(\mathcal{A}_{\neg\varphi})} = \varnothing \\
& \text{if and only if} \quad \mathit{TS} \otimes \mathcal{A}_{\neg\varphi} \models \Diamond\Box\, \neg F
\end{aligned}
$$

LTL model checking is thus reduced to persistence checking!

Overview of LTL model checking



Recall: Generalized Büchi automata

A *generalized NBA* (GNBA) $\mathcal{G}$ is a tuple $(Q, \Sigma, \delta, Q_0, \mathcal{F})$ where:

- Q is a finite set of states with $Q_0 \subseteq Q$ a set of initial states
- Σ is an alphabet
- $\delta : Q \times \Sigma \rightarrow 2^Q$ is a transition function
- $\mathcal{F} = \{ F_1, \ldots, F_k \}$ is a (possibly empty) subset of 2^Q

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

$$|\mathcal{G}| \;=\; |Q| + \sum_{q \in Q} \sum_{A \in \Sigma} |\, \delta(q, A) \,|$$

Recall: Language of a GNBA

- GNBA $\mathcal{G} = (Q, \Sigma, \delta, Q_0, \mathcal{F})$ and word $\sigma = A_0 A_1 A_2 \ldots \in \Sigma^\omega$
- A *run* for σ in $\mathcal{G}$ is an infinite sequence $q_0\, q_1\, q_2 \ldots$ such that:
  - $q_0 \in Q_0$ and $q_i \xrightarrow{A_i} q_{i+1}$ for all $0 \leqslant i$
- Run $q_0\, q_1 \ldots$ is *accepting* if for all $F \in \mathcal{F}$: $q_i \in F$ for infinitely many i
- $\sigma \in \Sigma^\omega$ is *accepted* by $\mathcal{G}$ if there exists an accepting run for σ
- The *accepted language* of $\mathcal{G}$:

$$\mathcal{L}_\omega(\mathcal{G}) = \left\{ \sigma \in \Sigma^\omega \mid \text{ there exists an accepting run for } \sigma \text{ in } \mathcal{G} \right\}$$

Recall: From GNBA to NBA

For any GNBA $\mathcal{G}$ there exists an NBA $\mathcal{A}$ with:

$\mathcal{L}_\omega(\mathcal{G}) = \mathcal{L}_\omega(\mathcal{A})$ and $|\mathcal{A}| = \mathcal{O}(|\mathcal{G}| \cdot |\mathcal{F}|)$

where $\mathcal{F}$ denotes the set of acceptance sets in $\mathcal{G}$

- Sketch of transformation GNBA (with k accept sets) into equivalent NBA:
  - make k copies of the automaton
  - 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 Lecture #16

- Repetition: LTL and GNBA

$\Rightarrow$ From LTL to GNBA

From LTL to GNBA

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

- Assume φ only contains the operators $\wedge$, $\neg$, $\bigcirc$ and U
  - $\vee$, $\longrightarrow$, $\Diamond$, $\Box$, W , and so on, are expressed in terms of these basic operators
- States are *elementary sets* of sub-formulas in φ
  - for $\sigma = A_0 A_1 A_2 \ldots \in \mathit{Words}(\varphi)$, expand $A_i \subseteq AP$ with sub-formulas of φ
  - . . . to obtain the infinite word $\bar{\sigma} = B_0 B_1 B_2 \ldots$ such that

$$\psi \in B_i \qquad \text{if and only if} \qquad \sigma^i = A_i A_{i+1} A_{i+2} \ldots \models \psi$$

  - $\bar{\sigma}$ is intended to be a run in GNBA $\mathcal{G}_\varphi$ 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 $\sigma \models \varphi$

From LTL to GNBA: the states (example)

- Let $\varphi = a \,\mathsf{U}\, (\neg a \wedge b)$ and $\sigma = \{\, a \,\}\{\, a, b \,\}\{\, b \,\} \ldots$
  - B_i is a subset of $\{\, a, b, \neg a \wedge b, \varphi \,\} \cup \{\, \neg a, \neg b, \neg(\neg a \wedge b), \neg \varphi \,\}$
  - this set of formulas is also called the *closure* of φ
- Extend $A_0 = \{\, a \,\}$, $A_1 = \{\, a, b \,\}$, $A_2 = \{\, b \,\}$, $\ldots$ as follows:
  - extend A_0 with $\neg b$, $\neg(\neg a \wedge b)$, and φ as they hold in $\sigma^0 = \sigma$ (and no others)
  - extend A_1 with $\neg(\neg a \wedge b)$ and φ as they hold in σ^1 (and no others)
  - extend A_2 with $\neg a$, $\neg a \wedge b$ and φ as they hold in σ^2 (and no others)
  - $\ldots$ and so forth
  - this is not effective and is performed on the automaton (not on words)
- Result:
  - $\bar{\sigma} = \underbrace{\{\, a, \neg b, \neg(\neg a \wedge b), \varphi \,\}}_{B_0} \underbrace{\{\, a, b, \neg(\neg a \wedge b), \varphi \,\}}_{B_1} \underbrace{\{\, \neg a, b, \neg a \wedge b, \varphi \,\}}_{B_2} \ldots$

Closure

For LTL-formula φ, the set *closure*(φ)

consists of all sub-formulas ψ of φ and their negation $\neg\psi$

(where ψ and $\neg\neg\psi$ are identified)

for $\varphi = a \, \mathsf{U} \, (\neg a \wedge b)$, *closure*$(\varphi) = \{ \, a, b, \neg a, \neg b, \neg a \wedge b, \neg(\neg a \wedge b), \varphi, \neg\varphi \, \}$

can we take B_i as any subset of *closure*(φ)? no! they must be elementary

Elementary sets of formulae

$B \subseteq$ *closure*(φ) is *elementary* if:

1. B is *logically consistent* if for all $\varphi_1 \wedge \varphi_2, \psi \in$ *closure*(φ):
   - $\varphi_1 \wedge \varphi_2 \in B \;\Leftrightarrow\; \varphi_1 \in B$ and $\varphi_2 \in B$
   - $\psi \in B \;\Rightarrow\; \neg\psi \notin B$
   - true $\in$ *closure*$(\varphi) \;\Rightarrow\;$ true $\in B$

2. B is *locally consistent* if for all $\varphi_1 \,\mathsf{U}\, \varphi_2 \in$ *closure*(φ):
   - $\varphi_2 \in B \;\Rightarrow\; \varphi_1 \,\mathsf{U}\, \varphi_2 \in B$
   - $\varphi_1 \,\mathsf{U}\, \varphi_2 \in B$ and $\varphi_2 \notin B \;\Rightarrow\; \varphi_1 \in B$

3. B is *maximal*, i.e., for all $\psi \in$ *closure*(φ):
   - $\psi \notin B \;\Rightarrow\; \neg\psi \in B$

Examples

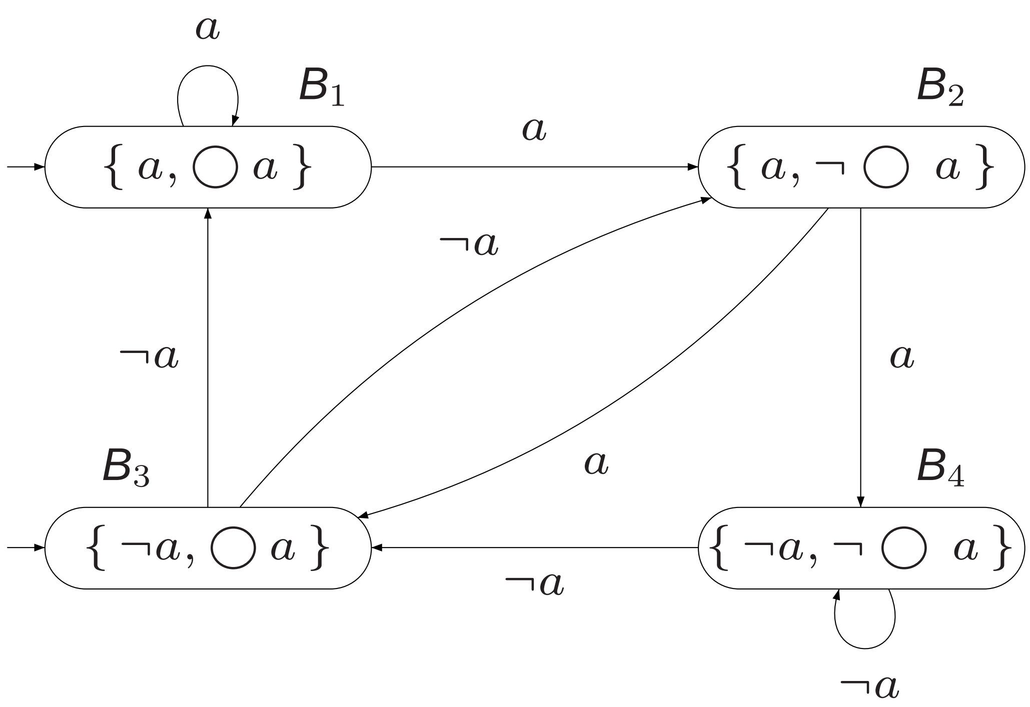
The GNBA of LTL-formula φ

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

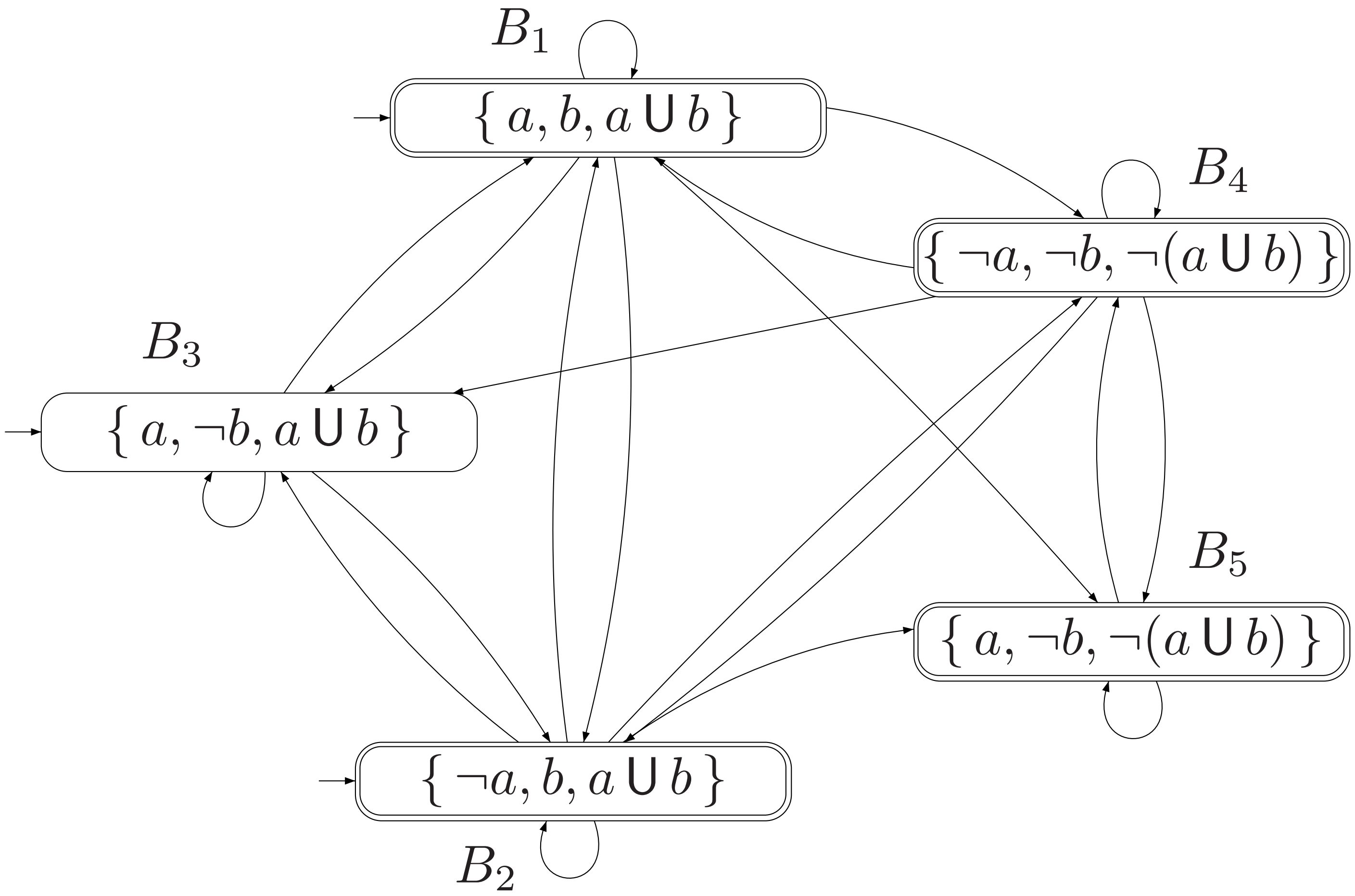
- Q is the set of all elementary sets of formulas $B \subseteq$ *closure*(φ)
  - $Q_0 \; = \; \left\{ B \in Q \mid \varphi \in B \right\}$
- $\mathcal{F} \; = \; \{ \{ B \in Q \mid \varphi_1 \,\mathsf{U}\, \varphi_2 \notin B$ or $\varphi_2 \in B \} \mid \varphi_1 \,\mathsf{U}\, \varphi_2 \in$ *closure*$(\varphi) \}$
- The transition relation $\delta : Q \times 2^{AP} \rightarrow 2^Q$ is given by:
  - $\delta(B, B \cap AP)$ is the set of all elementary sets of formulas B' satisfying:
    (i) For every $\bigcirc \psi \in$ *closure*(φ): $\bigcirc \psi \in B \;\; \Leftrightarrow \;\; \psi \in B'$, and
    (ii) For every $\varphi_1 \,\mathsf{U}\, \varphi_2 \in$ *closure*(φ):

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

GNBA for LTL-formula $\bigcirc a$



GNBA for LTL-formula $a \mathsf{U} b$



Main result

[Vardi, Wolper & Sistla 1986]

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

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

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

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

$\Rightarrow$ *every LTL-formula expresses an ω-regular property!*

Proof

NBA are more expressive than LTL

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

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

But there exists an NBA $\mathcal{A}$ with $\mathcal{L}_\omega(\mathcal{A}) = P$

$\Rightarrow$ *there are ω-regular properties that cannot be expressed in LTL!*