LTL Model Checking using Automata

Lecture #19 + #20 of Model Checking

Joost-Pieter Katoen

Lehrstuhl 2: Software Modeling & Verification

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

January 10, 2006

Overview Lecture #19 + #20

$\Rightarrow$ LTL and GNBA revisited

- From LTL to GNBA
- Complexity results

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
  - φ U ψ — φ holds Until a ψ-state is reached
- Auxiliary temporal operators
  - $\Diamond\, \varphi \equiv$ true U φ — 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

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

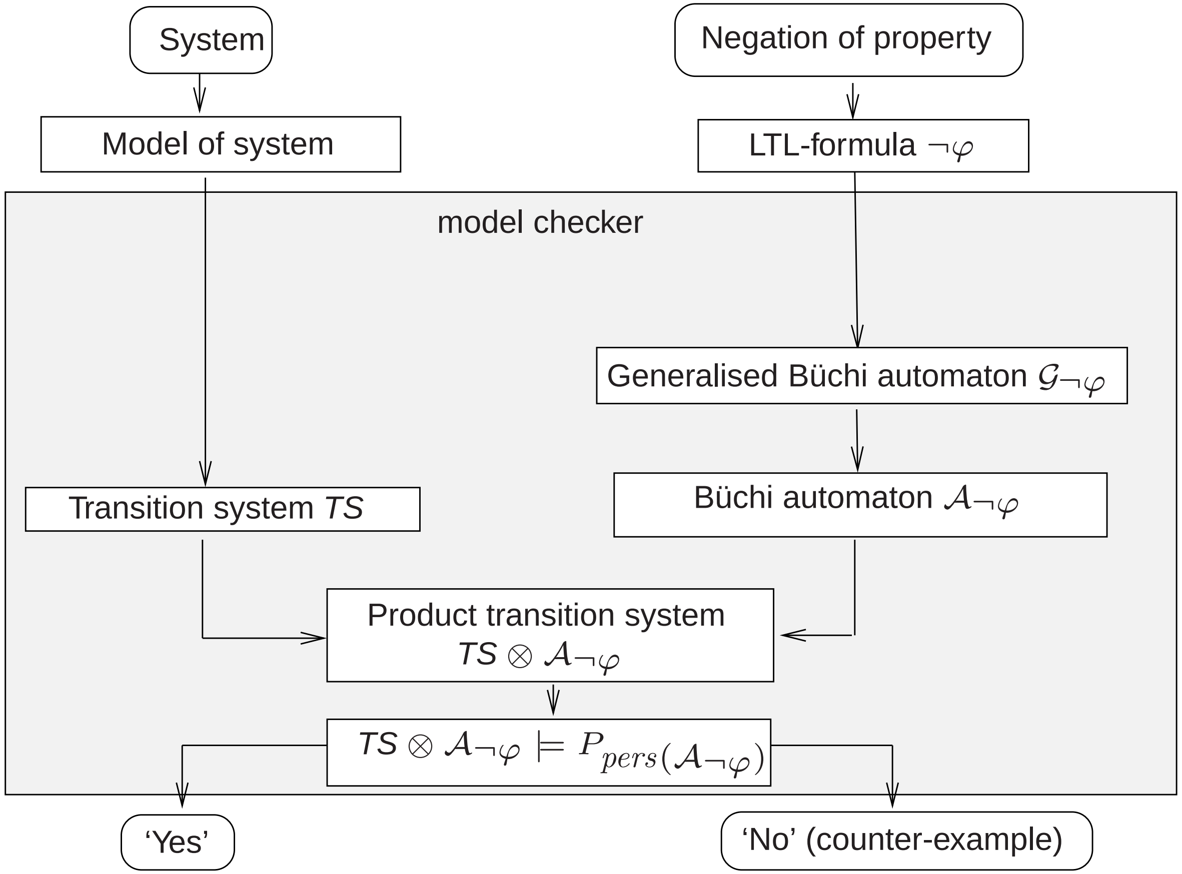
$$\text{if and only if} \quad \mathit{Traces}(\mathit{TS}) \cap \left((2^{\mathit{AP}})^{\omega} \setminus \mathit{Words}(\varphi)\right) = \varnothing$$

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

$$\text{if and only if} \quad \mathit{TS} \otimes \mathcal{A}_{\neg\varphi} \models \Diamond\Box\,\neg F$$

LTL model checking is thus reduced to persistence checking

Overview of LTL model checking



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 $\mathcal{G}$:

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

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 $q_i \xrightarrow{A_{i+1}} q_{i+1}$ 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 $\mathcal{G}$:

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

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 $\mathcal{G}$

Overview Lecture #19 + #20

- LTL and GNBA revisited

$\Rightarrow$ From LTL to GNBA

- Complexity results

From LTL to GNBA

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

- 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 subformulas of φ
  - ... to obtain the infinite word $\bar{\sigma} = B_0 B_1 B_2 \ldots$ such that

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

  - subformulas ψ of φ are considered as well as their negation $\neg\psi$

- Transitions are derived from semantics and expansion laws

- Accepting conditions for $\mathcal{G}_\varphi$ guarantee that:
  - $\bar{\sigma}$ is accepting if and only if $\sigma \models \varphi$

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)

Elementary sets of formulae

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

1. B is *logically consistent*:

    - $\varphi_1 \wedge \varphi_2 \in B \;\Leftrightarrow\; \varphi_1 \in B$ 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*:

    - $\varphi_2 \in B \;\Rightarrow\; \varphi_1 \,\mathsf{U}\, \varphi_2 \in B$
    - $\varphi_1 \,\mathsf{U}\, \varphi_2 \in B$ 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

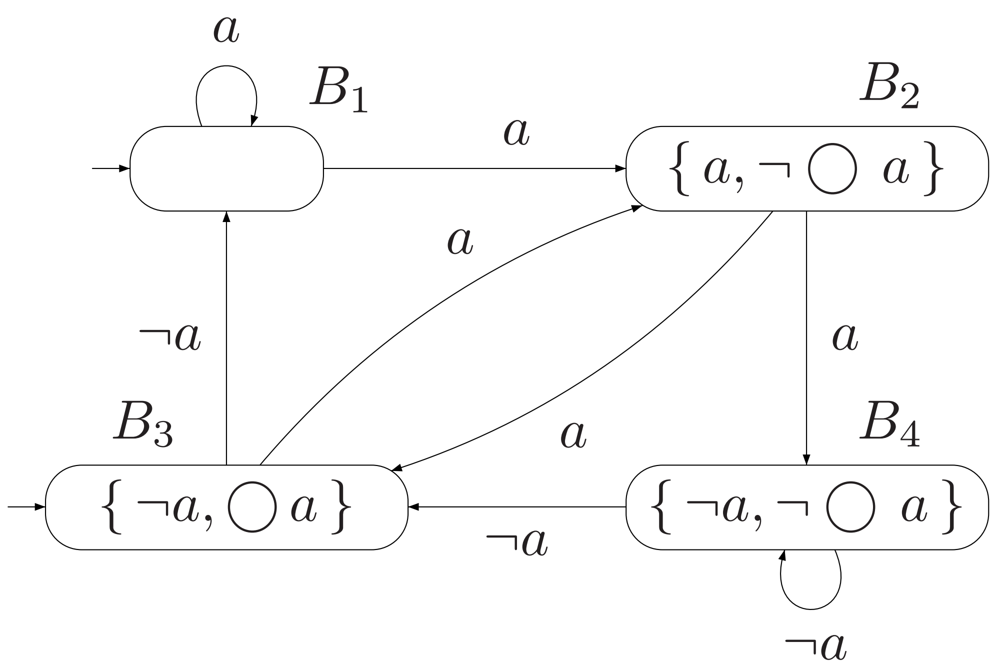
The GNBA of LTL-formula φ

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

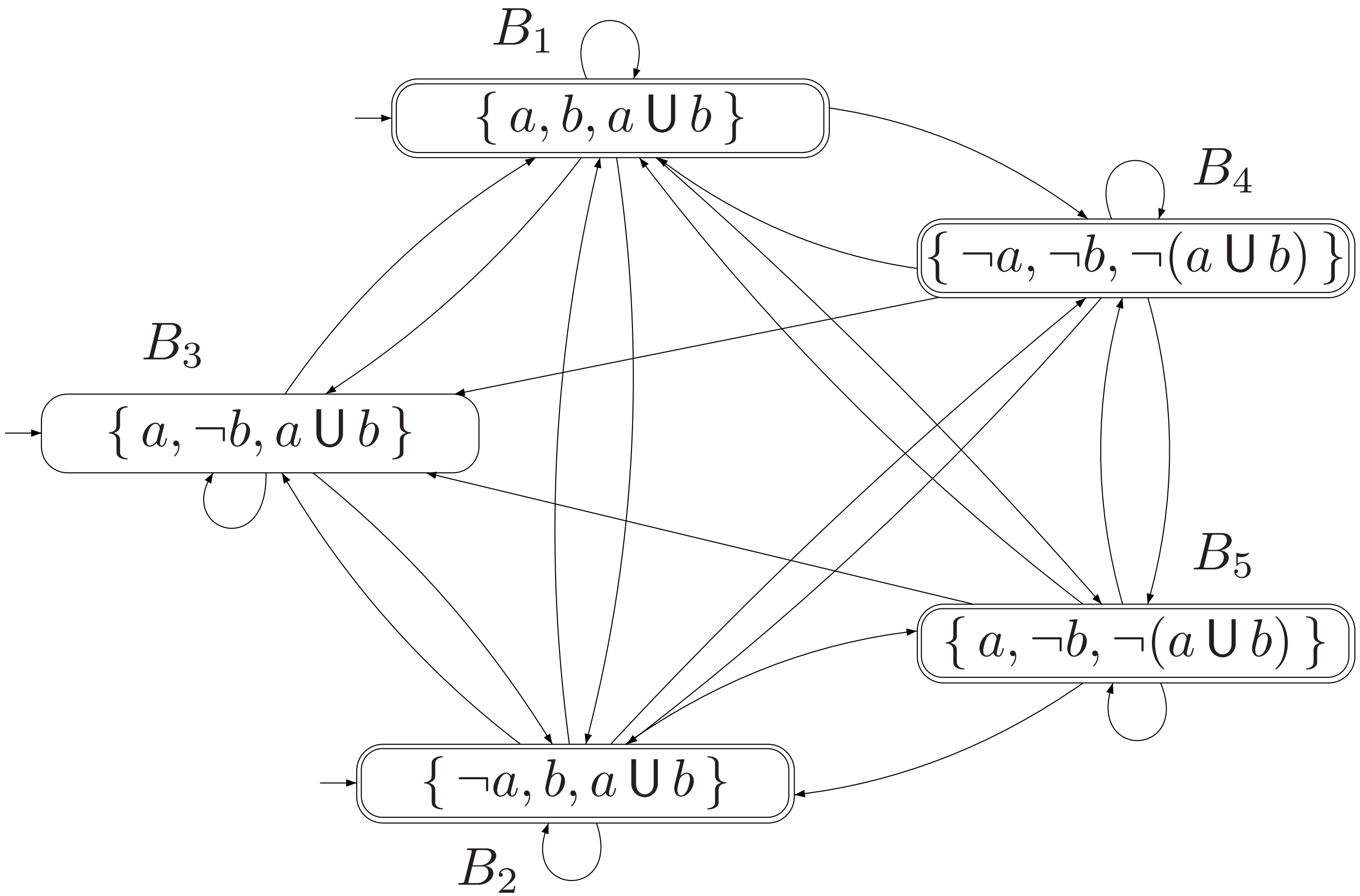
- Q is the set of all elementary sets of formulas $B \subseteq \mathit{closure}(\varphi)$
  - $Q_0 \ = \ \left\{ B \in Q \mid \varphi \in B \right\}$
- $\mathcal{F} \ = \ \{ \{ B \in Q \mid \varphi_1 \,\mathsf{U}\, \varphi_2 \notin B$ or $\varphi_2 \in B \} \mid \varphi_1 \,\mathsf{U}\, \varphi_2 \in \mathit{closure}(\varphi) \}$
- 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 $\bigcirc \psi \in \mathit{closure}(\varphi)$: $\bigcirc \psi \in B \ \Leftrightarrow \ \psi \in B'$, and
    (ii) For every $\varphi_1 \,\mathsf{U}\, \varphi_2 \in \mathit{closure}(\varphi)$:

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

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!*

Overview Lecture #19 + #20

- LTL and GNBA revisited
- From LTL to GNBA

$\Rightarrow$ Complexity results

Complexity for LTL to NBA

For any LTL-formula φ (over *AP*) there exists an NBA $\mathcal{A}_\varphi$

with *Words*$(\varphi) = \mathcal{L}_\omega(\mathcal{A}_\varphi)$ and

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

Lower bound

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

Complexity for LTL model checking

The time and space complexity of LTL model checking is in $\mathcal{O}\left(|TS| \cdot 2^{|\varphi|}\right)$

On-the-fly LTL model checking

- Idea: find a counter-example *during* the generation of $\mathit{Reach}(\mathit{TS})$ and $\mathcal{A}_{\neg\varphi}$
  - exploit the fact that $\mathit{Reach}(\mathit{TS})$ and $\mathcal{A}_{\neg\varphi}$ can be generated in parallel

$\Rightarrow$ Generate $\mathit{Reach}(\mathit{TS} \otimes \mathcal{A}_{\neg\varphi})$ "on demand"

- consider a new vertex only if no accepting cycle has been found yet
- only consider the successors of a state in $\mathcal{A}_{\neg\varphi}$ that match current state in *TS*

$\Rightarrow$ Possible to find an accepting cycle without generating $\mathcal{A}_{\neg\varphi}$ entirely

- This on-the-fly scheme is adopted in e.g. the model checker SPIN

The LTL model-checking problem is co-NP-hard

The Hamiltonian path problem is polynomially reducible to the complement of the LTL model-checking problem.

In fact, the LTL model-checking problem is PSPACE-hard [Sistla & Clarke 1985]