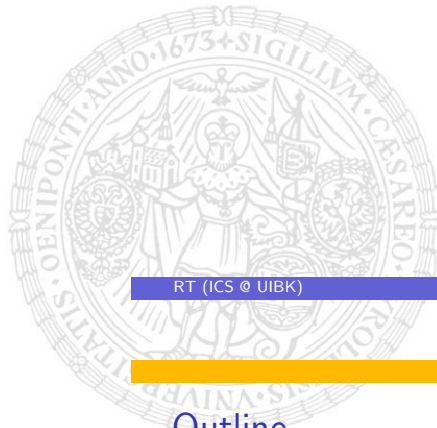


Introduction to Model Checking

René Thiemann

Institute of Computer Science
University of Innsbruck

WS 2007/2008



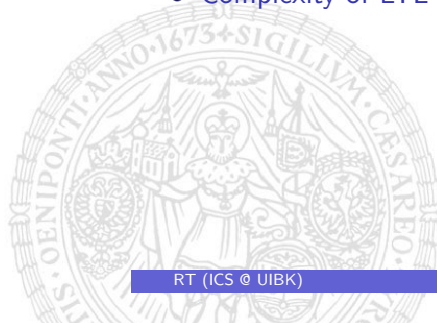
RT (ICS @ UIBK)

week 9

1/20

Outline

- Last Lecture
- Complexity of LTL Model Checking



RT (ICS @ UIBK)

week 9

2/20

φ -Expansion

a	0 1 1 0 1 0 0 1 1 1 ...
b	0 0 1 1 0 1 0 1 0 1 ...
$\neg b$	1 1 0 0 1 0 1 0 1 0 ...
Xa	1 1 0 1 0 0 1 1 1 1 ...
$XaU b$	1 1 1 1 0 1 1 1 1 1 ...
$\neg b \wedge (XaU b)$	1 1 0 0 0 0 1 0 1 0 ...

Idea of LTL to NBA-Translation

- NBA guesses the φ -expansion of w
- ... and **checks that guesses are correct**
- ... and demands that value for whole formula is 1 for whole word w

Definition (Consistency Checks)

$$\begin{aligned}
 \varphi_j = \neg \varphi_{j_1} &\Rightarrow w[i..]^j = 1 \text{ iff } w[i..]^{j_1} = 0 \\
 \varphi_j = \varphi_{j_1} \wedge \varphi_{j_2} &\Rightarrow w[i..]^j = 1 \text{ iff } w[i..]^{j_1} = 1 \text{ and } w[i..]^{j_2} = 1 \\
 \varphi_j = X \varphi_{j_1} &\Rightarrow w[i..]^j = 1 \text{ iff } w[i+1..]^{j_1} = 1 \\
 \varphi_j = \varphi_{j_1} U \varphi_{j_2} &\Rightarrow w[i..]^j = 1 \text{ iff } w[i..]^{j_2} = 1 \text{ or } \\
 &\quad (w[i..]^{j_1} = 1 \text{ and } w[i+1]^j = 1)
 \end{aligned}$$

All checks can be performed locally, i.e., column per column!

Consistency Checks and LTL-Models

Lemma

$w \models \varphi$ iff there exists an expansion $v \in (2^m)^\omega$ of w such that

1. v satisfies the consistency checks
2. $v[0..]^m = 1$
3. whenever $\varphi_j = \varphi_{j_1} \cup \varphi_{j_2}$ and $v[i..]^j = 1$ then there exists $i' \geq i$ such that $v[i'..]^{j_2} = 1$

Translating LTL to GNBA

Definition (GNBA for an LTL formula φ)

Let $cl(\varphi) = a_1, \dots, a_n, \varphi_{n+1}, \dots, \varphi_m$ where $\varphi_m = \varphi$.

Define $\mathcal{A}_\varphi = (2^m \uplus \{q_0\}, 2^n, q_0, \delta, F_1, \dots, F_k)$ where

- $(c_1, \dots, c_m)^T \in \delta((b_1, \dots, b_m)^T, (d_1, \dots, d_n)^T)$ iff
 1. $c_j = d_j$ for all $j \leq n$ (expansion)
 2. $(b_1, \dots, b_m)^T (c_1, \dots, c_m)^T$ is consistent (consistent expansion)
- $(c_1, \dots, c_m)^T \in \delta(q_0, (d_1, \dots, d_n)^T)$ iff
 1. $c_j = d_j$ for all $j \leq n$ (expansion)
 2. $(c_1, \dots, c_m)^T$ is consistent (consistent expansion)
 3. $c_m = 1$ (φ is satisfied)
- if $\varphi_j = \varphi_{j_1} \cup \varphi_{j_2}$ is i -th U-subformula in $cl(\varphi)$ then

$$F_i = \{(b_1, \dots, b_m)^T \mid b_j = 0 \text{ or } (b_j = 1 \text{ and } b_{j_2} = 1)\}$$

Soundness of Translation

Theorem (Vardi,Wolper)

For every LTL formula φ

$$\mathcal{L}(\varphi) = \mathcal{L}(\mathcal{A}_\varphi)$$

Proof of Lemma.

By induction on φ using the consistency checks. ■

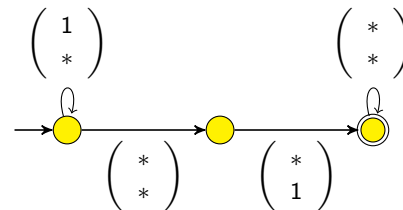
Proof of Theorem.

- Construction of \mathcal{A}_φ directly corresponds to requirements 1 and 2 in Lemma
- Remaining difficulty:
Show that visiting F_i infinitely often is the same as requirement 3 in Lemma for i -th U-subformula $\varphi_j = \varphi_{j_1} \cup \varphi_{j_2}$ ■

Last Exercises

Construct the NBA for the formula $aUXb$

- intuitively by hand



- using the construction of Vardi & Wolper

Complexity of LTL Model Checking

Model Checking: Given TS and φ construct automaton \mathcal{A} such that

$$\mathcal{L}(\mathcal{A}) = (2^n)^\omega \setminus \mathcal{L}(\varphi) \quad (*)$$

and then check

$$\mathcal{L}(TS \otimes \mathcal{A}) = \emptyset \quad (**)$$

Two alternatives for (*) available:

- $\mathcal{A} = \overline{\mathcal{A}_\varphi}$ implies $|\mathcal{A}| = \exp(|\mathcal{A}_\varphi|)$ (NBA complementation)
- $\mathcal{A} = \mathcal{A}_{\neg\varphi}$ implies $|\mathcal{A}| = 2 \cdot |\mathcal{A}_\varphi|$ (formula complementation)

Still, (**) has complexity $\mathcal{O}(|TS| \cdot |\mathcal{A}_{\neg\varphi}|) = \mathcal{O}(|TS| \cdot 2^{|\varphi|} \cdot |\varphi|)$

Lower bound

Theorem

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

Proof (1)

Let $AP = \{a\}$ and:

$$\mathcal{L}_n = \{ b_1 \dots b_n b_1 \dots b_n w \mid b_i \in \{0, 1\}, w \in \{0, 1\}^\omega \}, \quad \text{for } n \geq 0$$

It follows $\mathcal{L}_n = \mathcal{L}(\varphi_n)$ where $\varphi_n = \bigwedge_{0 \leq i < n} (X^i a \leftrightarrow X^{n+i} a)$

φ_n is an LTL formula of polynomial length: $|\varphi_n| \in \mathcal{O}(n^2)$

However, any NBA \mathcal{A} with $\mathcal{L}_\omega(\mathcal{A}) = \mathcal{L}_n$ has at least 2^n states

Proof (2)

Is Bad Complexity a Result of Automata Approach? **No!**

Theorem

The LTL model checking problem $TS \models \varphi$ is coNP-hard.



Proof.

- The **Hamiltonian path problem** (HPP) is NP-hard.

Given a directed graph $\mathcal{G} = (N, E)$, $E \subseteq N \times N$,
is there a path which traverses each node exactly once?

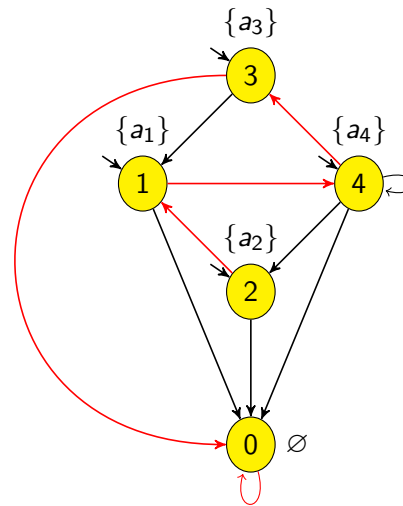
- Reduce **HPP** for graph \mathcal{G} in polynomial time to an **LTL model checking problem** $(TS_{\mathcal{G}}, \varphi_{\mathcal{G}})$ such that:

\mathcal{G} has Hamiltonian path iff $TS_{\mathcal{G}} \models \varphi_{\mathcal{G}}$

If $N = \{1, \dots, n\}$ choose $\varphi_{\mathcal{G}}$ and $TS_{\mathcal{G}} = (S, \rightarrow, I, AP, L)$ as follows



Example



Complexity is Even Worse ...

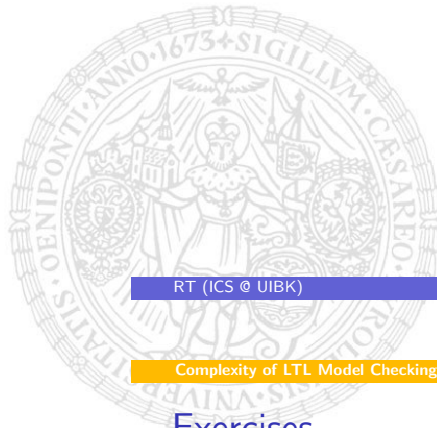
Theorem (Sistla, Clarke)

The LTL model checking problem $TS \models \varphi$ is PSPACE-hard.

... But There is a Limit

Theorem

The LTL model checking problem $TS \models \varphi$ is PSPACE-complete.



Exercises

Show that LTL model checking is coNP-hard by a reduction from SAT.

Reminder:

- The SAT problem is the question whether a propositional formula φ in conjunctive normal form (CNF) is satisfiable. It is the most famous NP-complete problem.
- A formula is in CNF iff it is a conjunction of disjunctions of literals. E.g., the following formula is in CNF:

$$(\neg q \vee \neg p) \wedge p \wedge (r \vee \neg q \vee p)$$

Only give the construction without a formal proof.

