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 $a \in AP$:

$$
\varphi ::= \text{true} \mid a \mid \varphi_1 \land \varphi_2 \mid \neg \varphi \mid \Diamond \varphi \mid \varphi_1 U \varphi_2
$$

- **Propositional logic**
  - $a \in AP$
  - \(\neg \varphi\) and \(\varphi \land \psi\)

- **Temporal modalities**
  - $\Diamond \varphi$ neXt state fulfills $\varphi$
  - $\varphi U \psi$ $\varphi$ holds Until a $\psi$-state is reached

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

**Semantics Over Words**

**Definition: LTL semantics over infinite words**

The LT-property induced by LTL formula $\varphi$ over $AP$ is:

$$\text{Words}(\varphi) = \{ \sigma \in 2^{AP}^\omega \mid \sigma \models \varphi \}$$

where $\models$ is the smallest relation with:

- $\sigma \models \text{true}$
- $\sigma \models a$ iff $a \in A_0$ (i.e., $A_0 \models a$)
- $\sigma \models \varphi_1 \land \varphi_2$ iff $\sigma \models \varphi_1$ and $\sigma \models \varphi_2$
- $\sigma \models \neg \varphi$ iff $\sigma \not\models \varphi$
- $\sigma \models \Diamond \varphi$ iff $\sigma[1..] = A_1 A_2 A_3 \ldots \models \varphi$
- $\sigma \models \varphi_1 U \varphi_2$ iff $\exists j \geq 0. \sigma[j..] \models \varphi_2$ and $\sigma[i..] \models \varphi_1$, $0 \leq i < j$

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 $\sigma$ from index $i$ on.

**Derived Operators**

- $\Diamond \varphi \equiv \text{true} U \varphi$ “some time in the future”
- $\Box \varphi \equiv \neg \Diamond \neg \varphi$ “from now on forever”

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

- $\sigma \models \Diamond \varphi$ iff $\exists j \geq 0. \sigma[j..] \models \varphi$
- $\sigma \models \Box \varphi$ iff $\forall j \geq 0. \sigma[j..] \models \varphi$
- $\sigma \models \Box \Diamond \varphi$ iff $\forall j \geq 0. \exists i \geq j. \sigma[i..] \models \varphi$ infinitely often $\varphi$
- $\sigma \models \Diamond \Box \varphi$ iff $\exists j \geq 0. \forall i \geq j. \sigma[i..] \models \varphi$ persistence of $\varphi$
Semantics over Transition Systems

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

- For infinite path fragment $\pi$ of $TS$:
  $$\pi \models \varphi \iff \text{trace}(\pi) \models \varphi$$

- For state $s \in S$:
  $$s \models \varphi \iff \forall \pi \in \text{Paths}(s). \pi \models \varphi$$

- For transition system $TS$:
  $$TS \models \varphi \iff \text{Traces}(TS) \subseteq \text{Words}(\varphi) \iff \forall s \in I. s \models \varphi$$

Example

$$\begin{align*}
T &\models a &\text{as } s_0 \models a \text{ and } s_2 \models a \\
T &\not\models \Box \Diamond a &\text{as } s_0 s_1 s_0 s_1 \ldots \not\models \Box \Diamond a \\
T &\models \Diamond \Box b \lor 
\Box \Diamond (\neg a \land \neg b) &\text{as } s_2 \models b, s_1 \not\models a, b \\
T &\models \Box (a \rightarrow (\Box \neg a \lor b)) &\text{as } s_2 \models b, s_0 \models \Box \neg a
\end{align*}$$

Overview

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

The LTL Model Checking Problem

Given:

1. finite transition system $TS$, and
2. LTL-formula $\varphi$

decide whether $TS \models \varphi$, and if $TS \not\models \varphi$, provide a counterexample.
NBA for LTL Formulae

\[ \mathcal{L}_\omega(A) = \text{Words}(\varphi) \]

A Naive Attempt

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

if and only if \( \text{Traces}(TS) \subseteq \mathcal{L}_\omega(A_\varphi) \)

if and only if \( \text{Traces}(TS) \cap \mathcal{L}_\omega(A_\neg \varphi) = \emptyset \)

if and only if \( \text{Traces}(TS) \cap \mathcal{L}_\omega(A_\neg \varphi) = \emptyset \).

Naive idea: check whether \( TS \) has no behaviour accepted by NBA \( A_\varphi \)

But complementation of NBA yields a blow-up:

if \( A \) has \( n \) states, \( \overline{A} \) has \( c^n \) states in worst case

\[ \Rightarrow \text{use the fact that: } \mathcal{L}_\omega(A_\varphi) = \mathcal{L}_\omega(A_\neg \varphi) \]

Approach

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

if and only if \( \text{Traces}(TS) \subseteq \mathcal{L}_\omega(A_\varphi) \)

if and only if \( \text{Traces}(TS) \cap \mathcal{L}_\omega(A_\neg \varphi) = \emptyset \)

if and only if \( \text{Traces}(TS) \cap \mathcal{L}_\omega(A_\neg \varphi) = \emptyset \)

if and only if \( TS \otimes A_{\neg \varphi} \not\models \square \neg F \)

where \( F \) is the set of accept states of NBA \( A_{\neg \varphi} \).

LTL model checking is thus reduced to persistence checking.
Automata-Based LTL Model Checking

Overview

Recap: Generalized Büchi Automata

Definition: Generalized Büchi automata

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

\[
\mathcal{F} = \{ F_1, \ldots, F_k \}
\]

with \(F_i \subseteq Q\)

for some natural \(k \in \mathbb{N}\).

Run \(q_0 q_1 \ldots \in Q^\omega\) is accepting if \(\forall F_j \in \mathcal{F}: q_i \in F_j\) for infinitely many \(i\).

The size of \(\mathcal{G}\), denoted \(|\mathcal{G}|\), is the number of states and transitions in \(\mathcal{G}\).
GNBA and NBA are Equally Expressive

For every GNBA \( G \) there exists an NBA \( A \) with

\[
\mathcal{L}_\omega(G) = \mathcal{L}_\omega(A) \quad \text{with} \quad |A| = O(|G| \cdot |F|)
\]

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

Proof.

For \( k=0,1 \), this result follows directly. For \( k > 1 \), make \( k \) copies of \( G \):
- 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

How to Obtain a GNBA?

GNBA \( G_\varphi \) over \( 2^{AP} \) for LTL-formula \( \varphi \) with \( \mathcal{L}_\omega(G_\varphi) = \text{Words}(\varphi) \):

- Assume \( \varphi \) only contains the operators \( \land, \neg, \Box, \Diamond, W \), and so on, are derived from these base operators

- States are elementary sets of sub-formulas in \( \varphi \)
  - for \( \sigma = A_0 A_1 \ldots \in \text{Words}(\varphi) \), expand \( A_i \in AP \) with sub-formulas of \( \varphi \)
  - \( \ldots \) to obtain the infinite word \( \bar{\sigma} = B_0 B_1 \ldots \) with \( B_i \) a set of sub-formulas of \( \varphi \) such that
    \[
    \psi \in B_i \quad \text{if and only if} \quad \sigma' = A_0 A_1 \ldots \models \psi
    \]
  - \( \bar{\sigma} \) is intended to be a run of GNBA \( G_\varphi \) for \( \sigma \)

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

**Definition: Closure**

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

**Example**

For $\varphi = a U (\neg a \land b)$ we have

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

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 $\varphi_1 \land \varphi_2 \in cl(\varphi)$:
   - $\varphi_1 \land \varphi_2 \in B \iff \varphi_1 \in B$ and $\varphi_2 \in B$
   - $\psi \notin B \iff \neg \psi \in B$
   - true in $cl(\varphi) \Rightarrow$ true in $B$

2. $B$ is locally consistent, i.e., for all $\varphi_1 U \varphi_2 \in cl(\varphi)$:
   - $\varphi_2 \in B \Rightarrow \varphi_1 U \varphi_2 \in B$
   - $\varphi_1 U \varphi_2 \in B$ and $\varphi_2 \notin B \Rightarrow \varphi_1 \in B$

Automaton Construction

**Definition: The GNBA for and LTL Formula**

For LTL-formula $\varphi$, let $\varphi = (Q, 2^{AP}, \delta, Q_0, \mathcal{F})$ 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 $\delta(B, A) = \emptyset$.

- $\delta(B, B \cap AP)$ is the set $B' \subseteq Q$ satisfying:
  (i) For every $\psi \in cl(\varphi)$: $\bigcirc \psi \in B \iff \psi' \in B'$, and
  (ii) For every $\varphi_1 U \varphi_2 \in cl(\varphi)$:
    $$\varphi_1 U \varphi_2 \in B \iff (\varphi_2 \in B \vee (\varphi_1 \in B \land \varphi_1 U \varphi_2 \in B'))$$

- $\mathcal{F} = \{\nexists \varphi_1 U \varphi_2 \mid \varphi_1 U \varphi_2 \in cl(\varphi)\}$ where
  $$\mathcal{F'} = \{B \in Q \mid \varphi_1 U \varphi_2 \notin B \text{ or } \varphi_2 \in B\}$$
Main Theorem

[Vardi, Wolper & Sistla 1986]

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

(a) $\text{Words}(\varphi) = \omega_l(G)$
(b) $\mathcal{G}_\varphi$ can be constructed in time and space $O(2^{\mid \varphi \mid})$
(c) $\#$ accepting sets of $\mathcal{G}_\varphi$ is bounded above by $O(\mid \varphi \mid)$.

Corollary

For every LTL-formula $\varphi$, $\text{Words}(\varphi)$ is $\omega$-regular.
NBA More Expressive Than LTL

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

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

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

**Proof.**

Omitted.

---

Lower Bound

There exists a family of LTL formulas $\varphi_n$ with $|\varphi_n| = O(\text{poly}(n))$ such that every NBA $\mathfrak{A}_{\varphi_n}$ for $\varphi_n$ 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 $\varphi$ has size in $O(|\varphi|)$
2. the number of elementary sets is in $O(2^{|\varphi|})$
3. the number of states in the GNBA $\mathcal{G}_\varphi$ is in $O(2^{|\varphi|})$
4. the number of acceptance sets in GNBA $\mathcal{G}_\varphi$ 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 $TS \otimes \mathfrak{A}_\varphi \models \Diamond \square \neg F$ is in $O(|TS \otimes \mathfrak{A}_\varphi|)$. 
LTL model checking exploits a GNBA $\exists_{\omega\varphi}$ for the negation of $\varphi$.

States of the GNBA are subsets of certain sub-formulas of $\varphi$.

Taking these subsets gives rise to an exponential blow-up. This cannot be avoided.

For each until-sub-formula of $\varphi$, the GNBA has one acceptance set.

Each LTL-formula describes an $\omega$-regular LT property.

LTL is strictly less expressive than $\omega$-regular expressions.

LTL model checking by automata is linear in the size of the transition system and exponential in the size of $\varphi$.

Friday November 15, 14:30