Deductive Model Checking of CTL* Properties

Christoph Sprenger

Swiss Federal Institute of Technology
Lausanne, Switzerland

Talk at

Swedish Institute of Computer Science
Kista, Sweden

October 9, 2000
What is it all about?

Given:

✓ system model $S$
✓ property specification $\phi$

Model Checking: $S \models \phi$

Algorithmic Solutions:

✗ limited to finite-state systems
✗ suffers from state space explosion problem

☞ for L, XL, $\omega$L problems: generally have to resort to proof system for deductive model checking
Motivation

• Yet another proof system??
  ✔ first one for CTL* and infinite-state systems

• Why CTL*?
  ✔ good trade-off expressiveness vs. readability

• Fine, but proof systems for more expressive $\mu$K exist. Why not use one of these?
  ❌ translation complex and often obscures meaning
Model: Transition Systems

Transition System: labeled directed graph, where

- nodes: set of states $S$
- edges: labeled set of transition relations

Runs

- run = infinite path through a transition system
- $\Xi$-run = run starting in a state satisfying $\Xi$
Logic: CTL* (Syntax)

assertions $p$

boolean operators:

- conjunction $(\phi_1 \land \phi_2)$
- disjunction $(\phi_1 \lor \phi_2)$

temporal operators:

- Next ($X\psi$)
- Eventually ($F\psi$)
- Always ($G\psi$)

path quantifiers:

- Some Run ($E\psi$)
- All Runs ($A\psi$)
Logic: CTL* (Semantics I)

Interpretation over runs $\sigma$ of a system $S$

$$\sigma \models p \iff \sigma(0) \models p$$

---

Boolean operators: as expected

$$\sigma \models X \phi \iff \sigma^1 \models \phi$$

$$\sigma \models F \phi \iff \sigma^i \models \phi \text{ for some } i \in \mathbb{N}$$

$$\sigma \models G \phi \iff \sigma^i \models \phi \text{ for all } i \in \mathbb{N}$$

---

$$\sigma \models E \psi \iff \eta \models \psi \text{ for some } \eta \text{ with } \eta(0) = \sigma(0)$$

$$\sigma \models A \psi \iff \eta \models \psi \text{ for all } \eta \text{ with } \eta(0) = \sigma(0)$$
Logic: CTL* (Semantics II)

Interpretation over set of states $\Xi$:

$S, \Xi \models \phi$  iff  all $\Xi$-runs of $S$ satisfy $\phi$

Fixed point characterisations:

$F\psi \equiv \psi \lor X F \psi$

$G\psi \equiv \psi \land X G \psi$

RHS called unfolding, denoted by $\text{unf}(H\psi)$
Deductive CTL* Model Checking

Proof Structures

✓ dgraphs constructed using a set of local proof rules
✓ two basic brands: LTL (A $\varphi$) and ELL (E $\varphi$)

Success Criterion

✓ identifies legal proofs

Success Rules

✓ global proof rules for success
LTL and ELL Proof Structures

Sequents

\[ p \vdash_A \Phi \quad p \vdash_E \Phi \]

Proof Structure for \( S \) and \( \Xi \vdash_Q \phi = \text{dgraph with} \)

✔ nodes: finite set of sequents \( \Gamma \)

✔ root: sequent \( \Xi \vdash_Q \phi \)

✔ edges: created by application of some rule \( R \)

\[ R \quad \gamma \quad \gamma_1 \cdots \gamma_n \quad C_R \]
Some LTL Rules

A(ax) \quad \frac{p \vdash_{A} \Phi, p}{.}

A(bsf) \quad \frac{p \vdash_{A} \Phi, q}{p \vdash_{A} \Phi} \quad \models p \rightarrow \neg q

A(H) \quad \frac{p \vdash_{A} \Phi, H \psi}{p \vdash_{A} \Phi, \text{unf}(H \psi)}

A(X) \quad \frac{p \vdash_{A} X \phi_1, \ldots, X \phi_n}{q \vdash_{A} \phi_1, \ldots, \phi_n} \quad \models \{p\} \Lambda \{q\}

A(sp) \quad \frac{p \vdash_{A} \Phi}{q_1 \vdash_{A} \Phi \quad \cdots \quad q_n \vdash_{A} \Phi} \quad \models p \rightarrow \bigvee_{i=1}^{n} q_i
Example

System $S$: (single variable $x$: nat)

Proof Structure for $S$ and $\text{true} \vdash_A F(x = 0)$:
**CTL* Proof Structures**

Path quantified formulas

can be treated very much like assertions [EL85]

**Rule example**

\[
E(bsf) \quad \frac{p \vdash_E \Phi, \psi}{p \vdash_E \Phi} \quad \frac{p \vdash_E \Phi}{p \vdash_Q \psi}
\]

CTL* proof structure

= 

DAG of LTL/ELL proof structures
Successful Paths

Purpose: make sure that eventualities Fψ fulfill their promises ψ

Hψ-sequents: (p ⊢ψ Φ) ∈ ΓHψ

1. ψ /∈ Φ, and

2. Φ ∩ {Hψ, XHψ, unf(Hψ)} ≠ ∅
   (some “unfolding form” of Hψ appears in Φ)

Successful path π:

<table>
<thead>
<tr>
<th>π</th>
<th>LTL</th>
<th>ELL</th>
</tr>
</thead>
<tbody>
<tr>
<td>finite</td>
<td>ends in axiom</td>
<td>ends in axiom</td>
</tr>
<tr>
<td>infinite</td>
<td>for some Gψ:</td>
<td>for all Fψ:</td>
</tr>
<tr>
<td></td>
<td>almost all</td>
<td>infinitely many</td>
</tr>
<tr>
<td></td>
<td>γ on π in ΓGψ</td>
<td>γ on π not in ΓFψ</td>
</tr>
</tbody>
</table>
Example (cont.)

System $S$: (single variable $x : \text{nat}$)

\[ \cdots \rightarrow 4 \xrightarrow{\text{dec}} 3 \xrightarrow{\text{dec}} 2 \xrightarrow{\text{two}} 1 \xrightarrow{\text{dec}} 0 \]

Proof Structure for $S$ and $\text{true} \vdash A F(x = 0)$:

\[
\begin{align*}
\gamma_0 : & \text{true} \vdash A F(x = 0) \\
\gamma_1 : & \text{true} \vdash A x = 0 \lor XF(x = 0) \\
\gamma_2 : & \text{true} \vdash A x = 0, XF(x = 0) \\
\gamma_3 : & x > 0 \vdash A x = 0, XF(x = 0) \\
\gamma_4 : & x > 0 \vdash A XF(x = 0) \\
\gamma_5 : & x = 0 \vdash A x = 0, XF(x = 0)
\end{align*}
\]
Trails

**Idea:** a trail matches a run of $S$ with a path of $\Pi$

**Matching pair:** $(s, \gamma)$ with $s \models p$ ($\gamma = p \vdash_{Q} \Phi$)

**Trail of $\Pi$:** maximal sequence of matching pairs

$$\vartheta: (s_0, \gamma_0) \cdots (s_j, \gamma_j) \cdots$$

- $\gamma_0$ is the root sequent of $\Pi$,
- $(\gamma_i, \gamma_{i+1})$ is an edge in $\Pi$,
- $s_i \xrightarrow{\lambda} s_{i+1}$ if Next rule applied at $\gamma_i$
- $s_i = s_{i+1}$ otherwise
Example: Trails

\[ \gamma_0 : \text{true} \vdash \mathcal{F}(x = 0) \]
\[ \gamma_1 : \text{true} \vdash x = 0 \lor \mathcal{X}\mathcal{F}(x = 0) \]
\[ \gamma_2 : \text{true} \vdash x = 0, \mathcal{X}\mathcal{F}(x = 0) \]
\[ \gamma_3 : x > 0 \vdash x = 0, \mathcal{X}\mathcal{F}(x = 0) \]
\[ \gamma_5 : x = 0 \vdash x = 0, \mathcal{X}\mathcal{F}(x = 0) \]
\[ \gamma_4 : x > 0 \vdash \mathcal{X}\mathcal{F}(x = 0) \]

Modified system:

\[ \vartheta = (3, \gamma_0) \cdots (3, \gamma_4) [(2, \gamma_0) \cdots (2, \gamma_4)]^{\omega} \]
\[ \sigma_{\vartheta} = \begin{bmatrix} 3 \\ 2 \end{bmatrix}^{\omega} \]
\[ \pi_{\vartheta} = \begin{bmatrix} \gamma_0 & \cdots & \gamma_4 \\ \gamma_0 & \cdots & \gamma_4 \end{bmatrix}^{\omega} \]

run $\sigma_{\vartheta} = 3 \cdot 2^{\omega}$ is a counterexample: $\sigma_{\vartheta} \not\models \mathcal{F}(x = 0)$

Original system: no run following infinite path $\pi$!
# Success Criteria

<table>
<thead>
<tr>
<th></th>
<th>LTL</th>
<th>ELL</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>successful trail $\vartheta$</strong></td>
<td>$\pi_{\vartheta}$ successful path</td>
<td>$\pi_{\vartheta}$ successful path</td>
</tr>
<tr>
<td><strong>successful proof structure II</strong></td>
<td>all trails successful</td>
<td>there is a successful trail from any matching pair $(s, \gamma_0)$</td>
</tr>
<tr>
<td>$\vartheta$ <strong>unsuccessful trail</strong></td>
<td>$\sigma_{\vartheta} \not\models \phi$ (counterex.)</td>
<td>-</td>
</tr>
<tr>
<td>$\vartheta$ <strong>successful trail</strong></td>
<td>-</td>
<td>$\sigma_{\vartheta} \models \phi$ (witness)</td>
</tr>
</tbody>
</table>
Success Rules

Success, syntactically: \((K_H \psi \text{ denoting set } \Gamma_H \psi)\)

- LTL p.s. \(\Pi\) for \(S\) and \(\Xi \vdash_A \phi\) successful iff

\[
S^\Pi \models A\left( \bigvee_{\psi \in G(\phi)} F G K_\psi \right)
\]

- ELL p.s. \(\Pi\) for \(S\) and \(\Xi \vdash_E \phi\) successful iff

\[
S^\Pi \models E\left( \bigwedge_{\psi \in F(\phi)} GF \neg K_\psi \right)
\]

Technique: both success rules use

- auxiliary assertions \(\alpha_\psi\) (one for each \(K_\psi\), and
- ranking functions to measure progress
Soundness and Completeness via Games

LTL/ELL:

\[ S, \Xi \models Q \phi \]
\[ \iff \]
Player \( \exists \) wins \( G_S(\Xi, Q \phi) \)
\[ \iff \]
\[ S, \Xi \vdash Q \phi \]

CTL*:

\( \checkmark \) result easily lifts from LTL and ELL base cases
S&C via Games: The Rough Picture

CTL* Game $G_S(\Xi, \phi)$: infinite two-player game, where
- Player $\exists$ (Player $\forall$) tries to show (refute) $S, \Xi \models \phi$
- configurations $(\sigma, \psi)$, Player $\forall$ chooses initial config

Proposition. $S, \Xi \models \phi$ iff Player $\exists$ wins $G_S(\Xi, \phi)$

 Trails and Strategies (LTL case):
- trail $\vartheta \mapsto$ deterministic $\forall$-strategy $\tau_\vartheta$ for $G_S(\sigma_\vartheta, \phi)$
- $\tau_\vartheta$ winning iff $\vartheta$ unsuccessful (roughly)
- if Player $\forall$ wins $G_S(\sigma, \phi)$, then there is a $\tau_\vartheta$ winning that game (winning $\forall$-strategies represented in $\Pi$)

Proposition. LTL proof structure $\Pi$ for $S$ and $\Xi \vdash_{A} \phi$. Then Player $\exists$ wins $G_S(\Xi, A\phi)$ iff $\Pi$ is successful.
Conclusions

extension of CTL* model checking under fairness constraints to infinite-state systems

Properties

✔ arbitrary CTL* formulas (no need for canonical form)
✔ all temporal reasoning reduced to assertional reasoning
✔ sound and complete relative to assertional validity
Open Problems/Future Work

• connection with abstraction
  – GVDs, abstract interpretation (Dam et al.) etc.
  – abstract games (P. Stevens)

• for tool development, we need
  – simpler success rules (no auxiliary assertions)
  – automation techniques

• real-time: fairness replaced by Non-Zenoness