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 $\mathcal{S}$
- ✔ property specification ϕ

Model Checking: $\mathcal{S} \overset{?}{\models} \phi$

Algorithmic Solutions:

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

☞ for L, XL, ∞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 μK 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
- ☞ Ξ-run = run starting in a state satisfying Ξ

Logic: CTL* (Syntax)

assertions p

boolean operators:

- conjunction ($\phi_1 \wedge \phi_2$)
- disjunction ($\phi_1 \vee \phi_2$)

temporal operators:

- Next ($\mathsf{X}\,\psi$)
- Eventually ($\mathsf{F}\,\psi$)
- Always ($\mathsf{G}\,\psi$)

path quantifiers:

- Some Run ($\mathsf{E}\,\psi$)
- All Runs ($\mathsf{A}\,\psi$)

Logic: CTL* (Semantics I)

Interpretation over runs σ of a system $\mathcal{S}$

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

---

boolean operators: as expected

$\sigma \models \mathsf{X}\,\phi$ iff $\sigma^1 \models \phi$

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

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

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

$\sigma \models \mathsf{A}\,\psi$ iff $\eta \models \psi$ for all η with $\eta(0) = \sigma(0)$

Logic: CTL* (Semantics II)

Interpretation over set of states Ξ:

$$\mathcal{S}, \Xi \models \phi \quad \text{iff} \quad \text{all } \Xi\text{-runs of } \mathcal{S} \text{ satisfy } \phi$$

Fixed point characterisations:

$$\mathsf{F}\,\psi \quad \equiv \quad \psi \vee \mathsf{X}\,\mathsf{F}\,\psi$$

$$\mathsf{G}\,\psi \quad \equiv \quad \psi \wedge \mathsf{X}\,\mathsf{G}\,\psi$$

RHS called unfolding, denoted by $\mathsf{unf}(\mathsf{H}\,\psi)$

Deductive CTL* Model Checking

Proof Structures

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

Success Criterion

- ✓ identifies legal proofs

Success Rules

- ✓ global proof rules for success

LTL and ELL Proof Structures

Sequents

$$p \vdash_{\mathsf{A}} \Phi \qquad\qquad p \vdash_{\mathsf{E}} \Phi$$

Proof Structure for $\mathcal{S}$ and $\Xi \vdash_{\mathsf{Q}} \phi$ = dgraph with

- ✔ nodes: finite set of sequents Γ
- ✔ root: sequent $\Xi \vdash_{\mathsf{Q}} \phi$
- ✔ edges: created by application of some rule R

$$R \ \frac{\gamma}{\gamma_1 \quad \cdots \quad \gamma_n} \ C_R$$

Some LTL Rules

$$\mathsf{A}(ax) \qquad \frac{p \vdash_{\mathsf{A}} \Phi, p}{\cdot}$$

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

$$\mathsf{A}(\mathsf{H}) \qquad \frac{p \vdash_{\mathsf{A}} \Phi, \mathsf{H}\,\psi}{p \vdash_{\mathsf{A}} \Phi, \mathsf{unf}(\mathsf{H}\,\psi)}$$

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

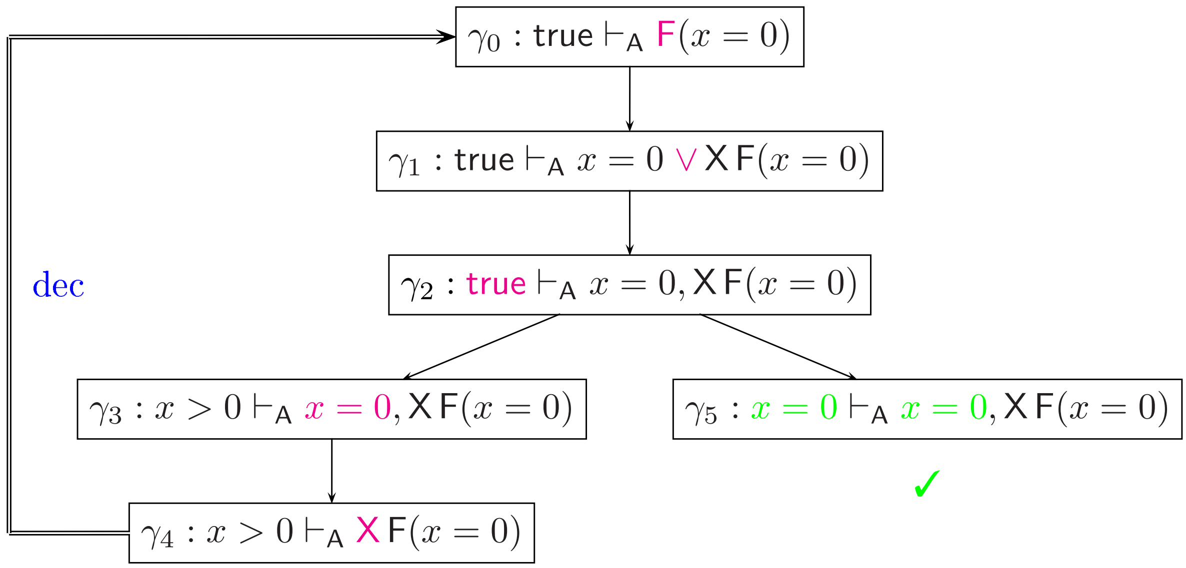
$$\mathsf{A}(sp) \qquad \frac{p \vdash_{\mathsf{A}} \Phi}{q_1 \vdash_{\mathsf{A}} \Phi \quad \cdots \quad q_n \vdash_{\mathsf{A}} \Phi} \qquad \models p \rightarrow \bigvee_{i=1}^{n} q_i$$

Example

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

$$\cdots \longrightarrow 4 \xrightarrow{dec} 3 \xrightarrow{dec} 2 \xrightarrow{dec} 1 \xrightarrow{dec} 0 \circlearrowleft_{zero}$$

Proof Structure for $\mathcal{S}$ and true $\vdash_{\mathsf{A}} \mathsf{F}(x = 0)$:



CTL* Proof Structures

Path quantified formulas

can be treated very much like assertions [EL85]

Rule example

$$\mathsf{E}(bsf) \quad \frac{p \vdash_{\mathsf{E}} \Phi, \mathsf{Q}\,\psi}{p \vdash_{\mathsf{E}} \Phi} \quad p \vdash_{\mathsf{Q}} \psi$$

CTL* proof structure

=

DAG of LTL/ELL proof structures

Successful Paths

Purpose: make sure that eventualities $\mathsf{F}\,\psi$ fulfill their promises ψ

$\mathsf{H}\,\psi$-sequents: $(p \vdash_{\mathsf{Q}} \Phi) \in \Gamma_{\mathsf{H}\,\psi}$

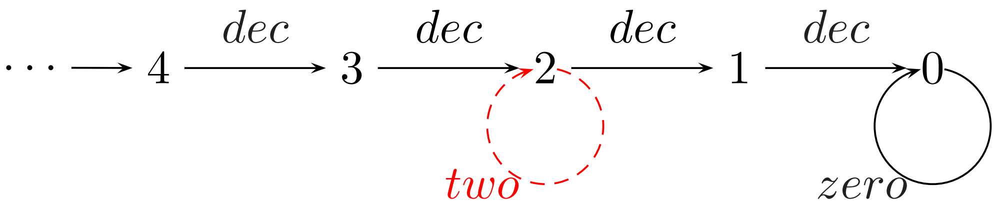
1. $\psi \notin \Phi$, and
2. $\Phi \cap \{\mathsf{H}\,\psi, \mathsf{X}\,\mathsf{H}\,\psi, \mathsf{unf}(\mathsf{H}\,\psi)\} \neq \varnothing$
   (some "unfolding form" of $\mathsf{H}\,\psi$ appears in Φ)

Successful path π:

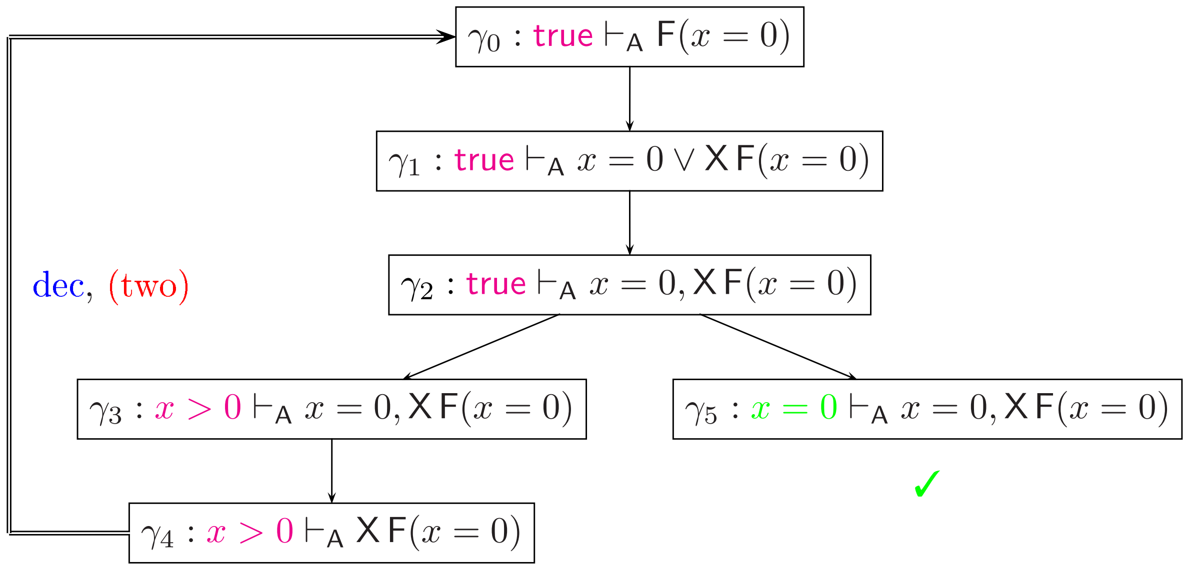
π	LTL	ELL
finite	ends in axiom	ends in axiom
infinite	for some $\mathsf{G}\,\psi$: almost all γ on π in $\Gamma_{\mathsf{G}\,\psi}$	for all $\mathsf{F}\,\psi$: infinitely many γ on π not in $\Gamma_{\mathsf{F}\,\psi}$

Example (cont.)

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



Proof Structure for $\mathcal{S}$ and true $\vdash_{\mathsf{A}}$ F$(x = 0)$:



Trails

Idea: a trail matches a run of $\mathcal{S}$ with a path of Π

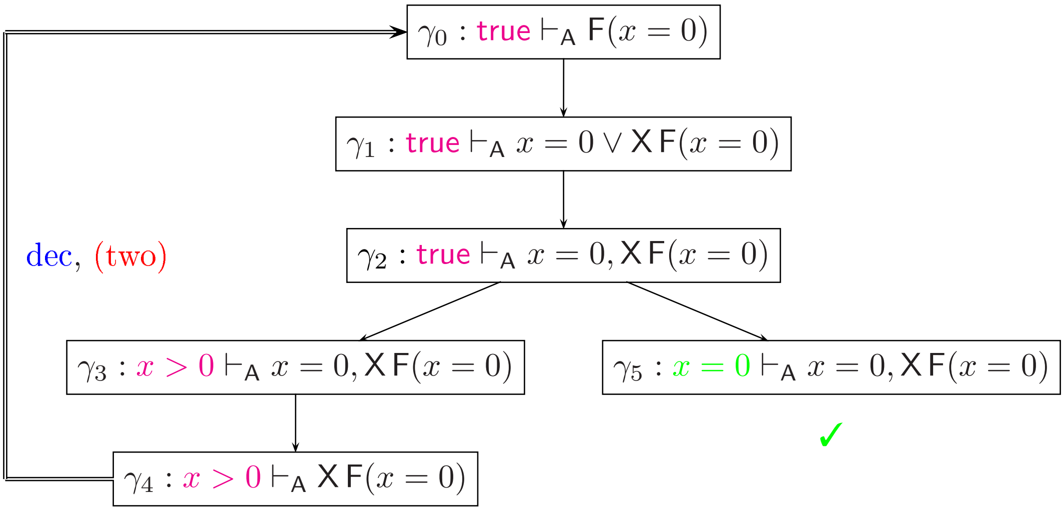
Matching pair: (s, γ) with $s \models p \;\; (\gamma = p \vdash_{\mathsf{Q}} \Phi)$

Trail of Π: maximal sequence of matching pairs

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

- ☞ γ_0 is the root sequent of Π,
- ☞ (γ_i, γ_{i+1}) is an edge in Π,
- ☞ $s_i \xrightarrow{\lambda} s_{i+1}$ if Next rule applied at γ_i
- ☞ $s_i \;=\; s_{i+1}$ otherwise

Example: Trails



Modified system:

$$\begin{array}{lcl} \vartheta & = & (3, \gamma_0) \cdots (3, \gamma_4)\, [(2, \gamma_0) \cdots (2, \gamma_4)]^{\omega} \\ \sigma_\vartheta & = & \quad\quad\quad\quad 3 \quad\quad\, [\quad\quad\quad\quad 2 \quad\quad]^{\omega} \\ \pi_\vartheta & = & \quad \gamma_0 \;\; \cdots \;\; \gamma_4 \; [\;\; \gamma_0 \;\; \cdots \;\; \gamma_4 \;]^{\omega} \end{array}$$

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

Original system: no run following infinite path π !

Success Criteria

	LTL	ELL
successful trail ϑ	π_ϑ successful path	π_ϑ successful path
successful proof structure Π	all trails successful	there is a successful trail from any matching pair (s, γ_0)
ϑ unsuccessful trail	$\sigma_\vartheta \not\models \phi$ (counterex.)	-
ϑ successful trail	-	$\sigma_\vartheta \models \phi$ (witness)

Success Rules

Success, syntactically: ($K_{\mathsf{H}\,\psi}$ denoting set $\Gamma_{\mathsf{H}\,\psi}$)

- LTL p.s. Π for $\mathcal{S}$ and $\Xi \vdash_{\mathsf{A}} \phi$ successful iff

$$\mathcal{S}^{\Pi} \models \mathsf{A}(\bigvee_{\psi \in \mathsf{G}(\phi)} \mathsf{F}\,\mathsf{G}\,K_{\psi})$$

- ELL p.s. Π for $\mathcal{S}$ and $\Xi \vdash_{\mathsf{E}} \phi$ successful iff

$$\mathcal{S}^{\Pi} \models \mathsf{E}(\bigwedge_{\psi \in \mathsf{F}(\phi)} \mathsf{G}\,\mathsf{F}\,\neg K_{\psi})$$

Technique: both success rules use

☞ auxiliary assertions α_{ψ} (one for each K_{ψ}), and

☞ ranking functions to measure progress

Soundness and Completeness via Games

LTL/ELL:

$$\begin{array}{c} \mathcal{S}, \Xi \models \mathsf{Q}\,\phi \\ \Updownarrow \\ \text{Player } \exists \text{ wins } \mathcal{G}_{\mathcal{S}}(\Xi, \mathsf{Q}\,\phi) \\ \Updownarrow \\ \mathcal{S}, \Xi \vdash_{\mathsf{Q}} \phi \end{array}$$

CTL*:

☞ result easily lifts from LTL and ELL base cases

S&C via Games: The Rough Picture

CTL* Game $\mathcal{G}_{\mathcal{S}}(\Xi, \phi)$: infinite two-player game, where

- ☞ Player $\exists$ (Player $\forall$) tries to show (refute) $\mathcal{S}, \Xi \models \phi$
- ☞ configurations (σ, ψ), Player $\forall$ chooses initial config

Proposition. *$\mathcal{S}, \Xi \models \phi$ iff Player $\exists$ wins $\mathcal{G}_{\mathcal{S}}(\Xi, \phi)$*

Trails and Strategies (LTL case):

- trail $\vartheta \mapsto$ deterministic $\forall$-strategy τ_ϑ for $\mathcal{G}_{\mathcal{S}}(\sigma_\vartheta, \phi)$
- τ_ϑ winning iff ϑ unsuccessful (roughly)
- if Player $\forall$ wins $\mathcal{G}_{\mathcal{S}}(\sigma, \phi)$, then there is a τ_ϑ winning that game (winning $\forall$-strategies represented in Π)

Proposition. *LTL proof structure Π for $\mathcal{S}$ and $\Xi \vdash_{\mathsf{A}} \phi$. Then Player $\exists$ wins $\mathcal{G}_{\mathcal{S}}(\Xi, \mathsf{A}\,\phi)$ iff Π 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 developement, we need
  - simpler success rules (no auxiliary assertions)
  - automation techniques
- real-time: fairness replaced by Non-Zenoness