Model-Checking Based Verification of Cyber-Physical Systems with Alternating Signal Temporal Logic

Software Engineering 2023, Student Research Competition, Sami Kharma

Motivation

Cyber-physical systems (CPS) utilize software while at the same time being able to sense or interact with the real world. We could model the system "Environment and CPS" and then verify the CPS by model checking a specification against the system.

Signal Temporal Logic

$$\varphi ::= s \sim c \mid \top \mid \neg\varphi \mid (\varphi \vee \varphi) \mid (\varphi \,\mathbf{U}_I\, \varphi)$$

Real-time • Real-valued • Linear-time

Alternating-Time Temporal Logic

$$\varphi ::= p \mid \top \mid \neg\varphi \mid (\varphi \vee \varphi) \mid \langle\!\langle A \rangle\!\rangle \bigcirc \varphi \mid \langle\!\langle A \rangle\!\rangle \Box \varphi \mid \langle\!\langle A \rangle\!\rangle (\varphi \,\mathbf{U}\, \varphi)$$

Discrete-time • Discrete-valued • Branching-time
Can express existence of strategies for players

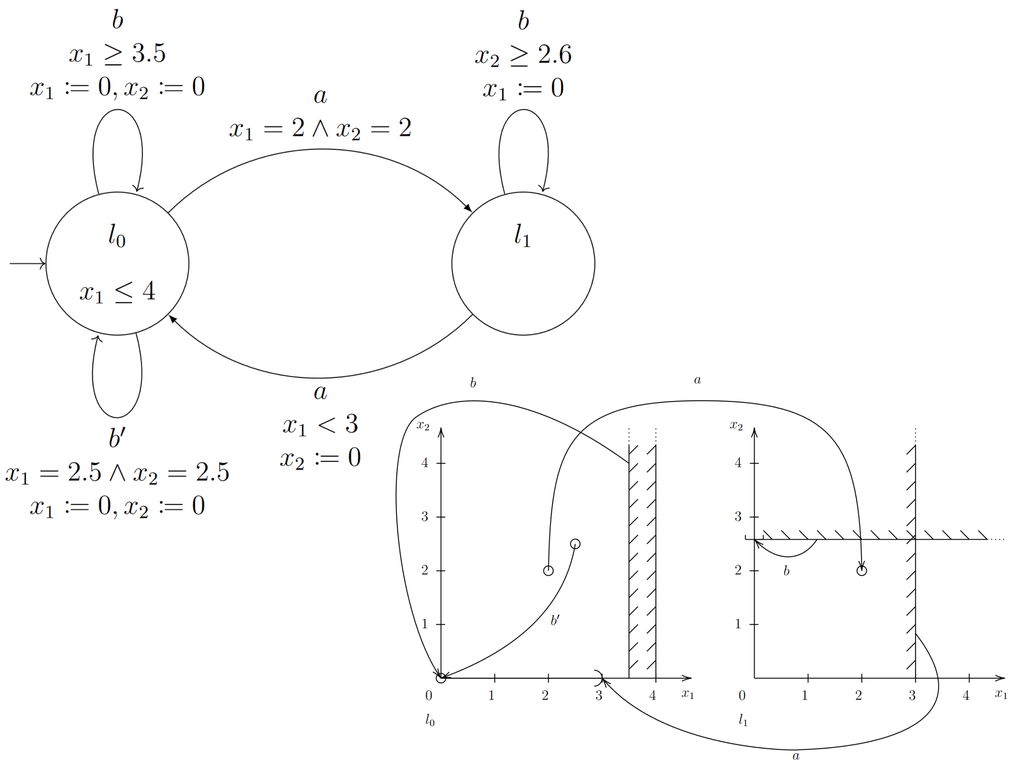
Alternating Signal Temporal Logic

$$\varphi ::= s \sim c \mid \top \mid \neg\varphi \mid (\varphi \vee \varphi) \mid (\varphi \,\mathbf{U}_I\, \varphi)$$

Real-time • Real-valued • Branching-time
Can express existence of strategies for players

Timed Games

Timed automaton extension with multiple players and actions for said players activation transitions



Bounded Model Checking

Extension of Pre-Image based algorithm for ATL

Algorithm 1 ASTL symbolic model-checking

Input: timed game $\mathcal{T}$, ASTL formula φ
Output: boolean *true* or *false*

for φ' **in** $\mathrm{Sub}(\varphi)$ **do**
  case $\varphi' = \top$
    $[\varphi'] \leftarrow Q_I$
  case $\varphi' = x \sim c$
    $[\varphi'] \leftarrow \mathrm{Reg}_{\mathcal{T}}(x \sim c)$
  case $\varphi' = \neg\theta$
    $[\varphi'] \leftarrow Q_I \setminus [\theta]$
  case $\varphi' = (\theta_1 \vee \theta_2)$
    $[\varphi'] \leftarrow [\theta_1] \cup [\theta_2]$
  case $\varphi' = \langle\!\langle A \rangle\!\rangle (\theta_1 \,\mathbf{U}_I\, \theta_2)$
    $[\varphi'] \leftarrow \mathrm{Pre}^*_{\mathcal{T},I}(A, [\theta_2], [\theta_1])$
end for
return $q_0 \in [\varphi]$

Rules
1. System "timed game" as game-structure extension of timed automata
2. Only non-zeno structures
3. No infinite intervals in specification

Proof Ideas

Correctness: Induction over ASTL semantics
Computability:

1. Split pre-image computation into series of discrete (action) and continuous (time) steps
2. Show that each step is computable, and a pre-image computation involves finitely many steps
3. Show that any pre-image can be symbolically represented as regions in state-space
4. Final inclusion check of algorithm through translation of symbolic representation to first-order logic formulas over the theory of real-closed fields, quantifier elimination computable (Tarski-Seidenberg Theorem)

Caveats and Further Work

- Infeasible runtime (quantifier-elimination in the theory of real-closed fields) – really necessary?
- ASTL* in relation to ASTL (analogously to ATL*)
- Robust semantics for ASTL

Literature

[AHK02] Rajeev Alur, Thomas A. Henzinger, and Orna Kupferman. "Alternating-time temporal logic". In: (2002).

[AL87] E. Allen Emerson and Chin-Laung Lei. "Modalities for model checking: branching time logic strikes back". In: (1987).

[Alf+03] Luca Alfaro et al. "The Element of Surprise in Timed Games". In: 2003.

[Alu99] Rajeev Alur. "Timed Automata". In: 1999.

[BL19] Kyungmin Bae and Jia Lee. "Bounded model checking of signal temporal logic properties using syntactic separation". In: (2019).

[BM88] Edward Bierstone and Pierre D. Milman. "Semianalytic and subanalytic sets". In: (1988).

[Bri+07] Thomas Brihaye et al. "Timed Concurrent Game Structures". In: 2007.

[Bur+92] J.R. Burch et al. "Symbolic model checking: 1020 States and beyond". In: (1992).

[Cas+05] Franck Cassez et al. "Efficient On-the-Fly Algorithms for the Analysis of Timed Games". In: 2005.

[CDL09] Thomas Chatain, Alexandre David, and Kim Larsen. "Playing Games with Timed Games". In: (2009).

[CHP07] Krishnendu Chatterjee, Thomas A. Henzinger, and Nir Piterman. "Strategy Logic". In: 2007.

[Déh06] David Déharbe. "Techniques for Temporal Logic Model Checking". In: 2006.

[DH88] James H. Davenport and Joos Heintz. "Real quantifier elimination is doubly exponential". In: (1988).

[Don13] Alexandre Donzé. "On Signal Temporal Logic". In: 2013.

[DR15] Alexandre Donz\'e and Vasumathi Raman. "BluSTL: Controller Synthesis from Signal Temporal Logic Specifications". In: 2015.

[Hen+98] Thomas A. Henzinger et al. "What's Decidable about Hybrid Automata?" In: (1998).

[Hen96] T.A. Henzinger. "The theory of hybrid automata". In: 1996.

[HHM99] Thomas A. Henzinger, Benjamin Horowitz, and Rupak Majumdar. "Rectangular Hybrid Games". In: 1999.

[HSW11] Frédéric Herbreteau, B. Srivathsan, and Igor Walukiewicz. "Efficient Emptiness Check for Timed Büchi Automata (Extended version)". In: (2011).

[KM19] Damian Kurpiewski and Diego Marmsoler. "Strategic logics for collaborative embedded systems". In: (2019).

[MN04] Oded Maler and Dejan Nickovic. "Monitoring Temporal Properties of Continuous Signals". In: ed. by Yassine Lakhnech and Sergio Yovine. 2004.

[PBV95] A. Puri, V. Borkar, and P. Varaiya. "Epsilon-Approximation of Differential Inclusions". In: 1995.

[Roe+16] Hendrik Roehm et al. "STL Model Checking of Continuous and Hybrid Systems". In: 2016.

[Sch20] Bernd-Holger Schlingloff. "Specification, Synthesis and Validation of Strategies for Collaborative Embedded Systems". In: 2020.

[Tar98] Alfred Tarski. "A Decision Method for Elementary Algebra and Geometry". In: 1998.