Multi-valued Logics for MAS Verification

Francesco Belardinelli

Imperial College London, UK & Université d'Evry, France

World Logic Day 2021

joint work with A. Lomuscio (Imperial College London) & V. Malvone (Telecom Paris) & E. Yu (Johannes Kepler University)

From System to MAS Verification

The Verification Problem: given a system S and specification P, does S satisfy P?

- errors cost lives (e.g., Therac-25) and money (e.g., Pentium 5).

In safety-critical systems failure is not an option!

From System to MAS Verification

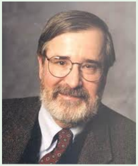
The Verification Problem: given a system S and specification P, does S satisfy P?

- errors cost lives (e.g., Therac-25) and money (e.g., Pentium 5).

In safety-critical systems failure is not an option!

Model-checking in a nutshell [Clarke, Emerson, Sifakis]

1. Model S as some transition system M_S
2. Represent specification P as a formula ϕ_P in some logic-based language
3. Check whether $M_S \models \phi_P$



From System to MAS Verification

80's-90's: single-component, stand-alone systems: temporal logics LTL, CTL [Pnu77].

From System to MAS Verification

80's-90's: single-component, stand-alone systems: temporal logics LTL, CTL [Pnu77].

Since 2000: multi-agent systems, interacting agents, game structures:

- Coalition Logic [Pau02]
- Strategy Logic [CHP07, MMPV14]
- **Alternating-time Temporal Logic (ATL)** [AHK02]

Notions of strategies, equilibria from Game Theory $\rightarrow$ Rational Synthesis

From System to MAS Verification

80's-90's: single-component, stand-alone systems: temporal logics LTL, CTL [Pnu77].

Since 2000: multi-agent systems, interacting agents, game structures:

- Coalition Logic [Pau02]
- Strategy Logic [CHP07, MMPV14]
- **Alternating-time Temporal Logic (ATL)** [AHK02]

Notions of strategies, equilibria from Game Theory $\rightarrow$ Rational Synthesis

$\Rightarrow$ Automated verification of strategic abilities of autonomous agents (Verics, **MCMAS**)

From System to MAS Verification

80's-90's: single-component, stand-alone systems: temporal logics LTL, CTL [Pnu77].

Since 2000: multi-agent systems, interacting agents, game structures:

- Coalition Logic [Pau02]
- Strategy Logic [CHP07, MMPV14]
- **Alternating-time Temporal Logic (ATL)** [AHK02]

Notions of strategies, equilibria from Game Theory → Rational Synthesis

⇒ Automated verification of strategic abilities of autonomous agents (Verics, **MCMAS**)

So far, so good ...

The Problem with MAS Verification

MAS exhibit imperfect information:

- Agents have partial observability/imperfect information about the system.
- Imperfect information makes things hard(er).
  - Model checking ATL:

	perfect inf. (PI)	**imperfect inf.** (II)
imp. recall (IR)	PTIME-complete (A. H. K., 2002)	Δ_2^P-complete (Jamroga, Dix, 2006)
perf. recall (PR)		undecidable (Dima, Tiplea, 2011)

The Problem with MAS Verification

MAS exhibit imperfect information:

- Agents have partial observability/imperfect information about the system.
- Imperfect information makes things hard(er).
  - Model checking ATL:

	perfect inf. (PI)	**imperfect inf.** (II)
imp. recall (IR)	PTIME-complete (A. H. K., 2002)	Δ_2^P-complete (Jamroga, Dix, 2006)
perf. recall (PR)		undecidable (Dima, Tiplea, 2011)

This talk:

- 3-valued logic to approximate PR with BR [BLM18].

One of several applications of multi-valued logics to formal verification [BK06, BG03, GJ03, SG04].

Alternating-time Temporal Logic and Memory

Specification Language: ATL

$$\varphi ::= \text{ atom } q \mid \neg\varphi \mid \varphi \wedge \varphi \mid \langle\langle A \rangle\rangle X\varphi \mid \langle\langle A \rangle\rangle \varphi U \varphi \mid \langle\langle A \rangle\rangle G\varphi$$

where $A \subseteq Ag$ is a *coalition* of agents.

Alternating-time Temporal Logic and Memory

Specification Language: ATL

$$\varphi ::= \text{ atom } q \mid \neg\varphi \mid \varphi \wedge \varphi \mid \langle\langle A \rangle\rangle X\varphi \mid \langle\langle A \rangle\rangle \varphi U \varphi \mid \langle\langle A \rangle\rangle G\varphi$$

where $A \subseteq Ag$ is a *coalition* of agents.

Strategy

A function F from histories (possibly of bounded length $n \in \mathbb{N}$) to actions.

Alternating-time Temporal Logic and Memory

Specification Language: ATL

$$\varphi ::= \text{ atom } q \mid \neg\varphi \mid \varphi \wedge \varphi \mid \langle\!\langle A \rangle\!\rangle X\varphi \mid \langle\!\langle A \rangle\!\rangle \varphi U \varphi \mid \langle\!\langle A \rangle\!\rangle G\varphi$$

where $A \subseteq Ag$ is a *coalition* of agents.

Strategy

A function F from histories (possibly of bounded length $n \in \mathbb{N}$) to actions.

Semantics for n-bounded recall

$(M, s) \models_n \langle\!\langle A \rangle\!\rangle \psi$ iff coalition A has n-bounded strategies F_A s.t. for all paths p consistent with F_A, $(M, p) \models_n \psi$

Alternating-time Temporal Logic and Memory

Specification Language: ATL

$$\varphi ::= \text{ atom } q \mid \neg\varphi \mid \varphi \wedge \varphi \mid \langle\!\langle A \rangle\!\rangle X\varphi \mid \langle\!\langle A \rangle\!\rangle \varphi U \varphi \mid \langle\!\langle A \rangle\!\rangle G\varphi$$

where $A \subseteq Ag$ is a *coalition* of agents.

Strategy

A function F from histories (possibly of bounded length $n \in \mathbb{N}$) to actions.

Semantics for *n*-bounded recall

$(M, s) \models_n \langle\!\langle A \rangle\!\rangle \psi$ iff coalition A has n-bounded strategies F_A s.t. for all paths p consistent with F_A, $(M, p) \models_n \psi$

For $n = \omega$, we have strategies with PR $\Rightarrow$ undecidable model checking problem.

Approximating Perfect Recall – first attempt

Naive idea: approximate PR via BR with an increasing bound.

Approximating Perfect Recall – first attempt

Naive idea: approximate PR via BR with an increasing bound.

Negative Result

Let $m, n \in \mathbb{N}^+ \cup \{\omega\}$ with $m < n$.

There exists formulas φ and $\varphi' = \neg\varphi$ in *ATL* s.t.

1. $(M, p) \not\models_m \varphi$ and $(M, p) \models_n \varphi$
2. $(M, p) \models_m \varphi'$ and $(M, p) \not\models_n \varphi'$

Approximating Perfect Recall – first attempt

Naive idea: approximate PR via BR with an increasing bound.

Negative Result

Let $m, n \in \mathbb{N}^+ \cup \{\omega\}$ with $m < n$.

There exists formulas φ and $\varphi' = \neg\varphi$ in *ATL* s.t.

1. $(M, p) \not\models_m \varphi$ and $(M, p) \models_n \varphi$
2. $(M, p) \models_m \varphi'$ and $(M, p) \not\models_n \varphi'$

Consequence

Any naive attempt to approximate PR by increasing the bound n will not succeed.

$\Rightarrow$ To solve this problem, we consider a 3-valued semantics.

3-valued Semantics for ATL

We consider Kleene's 3-valued logic:

- Besides **true** ($\top$) and **false** ($\bot$), we have a third truth value: **undefined** uu.

$((M, s) \models^3_n \langle\langle A \rangle\rangle \psi) = \top$ iff coalition A has n-bounded strategies F_A s.t. for all paths p consistent with F_A, $((M, p) \models^3_n \psi) = \top$

$((M, s) \models^3_n \langle\langle A \rangle\rangle \psi) = \bot$ iff adversary $\overline{A}$ has n-bounded strategies $F_{\bar{A}}$ s.t. for all paths p consistent with $F_{\bar{A}}$, $((M, p) \models^3_n \psi) = \bot$

In all other cases the value is undefined (uu).

For a formula $\langle\langle A \rangle\rangle \psi$ to be false $(\bot)$ is not enough the lack of a successful strategy for A. We need a fasifying strategy for $\overline{A}$!

Key Features of the 3V Semantics

Defined truth values are preserved when increasing memory.

Let $m, n \in \mathbb{N}^+ \cup \{\omega\}$ be such that $m \leq n$:

$$((M,s) \models^3_m \phi) = \top \quad \Rightarrow \quad ((M,s) \models^3_n \phi) = \top$$
$$((M,s) \models^3_m \phi) = \bot \quad \Rightarrow \quad ((M,s) \models^3_n \phi) = \bot$$

Defined truth values are preserved from 3V to 2V semantics:

$$((M,s) \models^3_n \phi) = \top \quad \Rightarrow \quad (M,s) \models^2_n \phi$$
$$((M,s) \models^3_n \phi) = \bot \quad \Rightarrow \quad (M,s) \not\models^2_n \phi$$

Approximating Perfect Recall – second attempt

1. *ATL* formulas are checked in the 3V semantics for increasingly larger bounds.
2. If $\top$ or $\bot$ is returned, this is also the value for the 2V semantics under PR.

Iterative Model Checking Procedure

Algorithm *Iterative_MC*(M, ψ, n):

$j := 0$;
$k := \mathrm{uu}$;
`while` $(j < n \wedge k = \mathrm{uu})$
  $j := j + 1$;
  $k := MC3(M, \psi, j)$;
`end while`;
`if` $k \neq \mathrm{uu}$ `then return` (j, k);
`else return` -1;

- The procedure is sound and it terminates for $n \in \mathbb{N}$.
- It might not terminate for $n = \omega$.
- This is as expected, as the problem is undecidable in general.

Conclusions

- We introduced a 3V semantics for ATL to tackle undecidability under PR and II.
- We proved preservation results for defined truth values
  - from BR to PR
  - from 3V to 2V
- We introduced an iterative procedure that, in some cases, solves the MC problem under PR by taking a bounded amount of memory.
- We implemented this approach in MCMAS_{BR}.

References

R. Alur, Th. Henzinger, and O. Kupferman.
Alternating-time temporal logic.
Journal of the ACM, 49(5):672–713, 2002.

G. Bruns and P. Godefroid.
Model checking with multi-valued logics.
Technical Report ITD-03-44535H, Bell Labs, 2003.

Thomas Ball and Orna Kupferman.
An abstraction-refinement framework for multi-agent systems.
In *Proceedings of the 21st Annual IEEE Symposium on Logic in Computer Science (LICS06)*, pages 379–388. IEEE, 2006.

F. Belardinelli, A. Lomuscio, and V. Malvone.
Approximating perfect recall when model checking strategic abilities.
In *KR2018*, 2018.

K. Chatterjee, T. Henzinger, and N. Piterman.
Strategy logic.
In *CONCUR'07*, volume 4703 of *Lecture Notes in Computer Science*, pages 59–73. Springer, 2007.

P. Godefroid and R. Jagadeesan.
On the expressiveness of 3-valued models.
In *Proceedings of the 4th International Conference on Verification, Model Checkig, and Abstract Interpretation (VMCAI03)*, volume 2575 of *LNCS*, pages 206–222. Springer-Verlag, 2003.

F. Mogavero, A. Murano, G. Perelli, and M.Y. Vardi.
Reasoning about strategies: On the model-checking problem.
ACM Transactions on Computational Logic, 15(4):34:1–34:47, 2014.

M. Pauly.
A modal logic for coalitional power in games.
Journal of Logic and Computation, 12(1):149–166, 2002.

A. Pnueli.
The temporal logic of programs.