Cutoff Techniques in the Verification of Open Multi-Agent Systems

Panagiotis Kouvaros and Alessio Lomuscio

Department of Computing, Imperial College London, UK

Parameterized Verification Workshop - 6 September 2014

Multi-agent systems (MAS)

Systems comprised of multiple components, namely agents, and their environment.

- Agents act autonomously and can act socially.
- The autonomous and social behaviour of MAS has been utilised in diverse applications.
  - Search and rescue,
  - Web-services,
  - Personal negotiation assistants.
- Growing need for verification before deployment.

Verification of MAS

Model checking: a leading verification technique.

- MAS model checking follows the AI tradition of reasoning about autonomous systems by ascribing high level properties.
- MAS specifications expressed as epistemic, BDI, alternating-time logic formulas.

Specification example: If an agent knows that its current goal is no longer achievable, then it will drop it at the next tick and begin replanning.

Interpreted Systems [PR85,FHMV95]

- A MAS is composed of a set of agents $A = \{1, ..., n\}$ and an environment e.
- Each agent is described by
  - A set of *local states* L_i,
  - A set of *local actions* Act_i,
  - A *local protocol* function $P : L_i \to 2^{Act_i}$.
  - An *evolution* function $\tau_i : L_i \times Act_1 \times \ldots \times Act_n \times Act_e \to L_i$.
- Evolution by synchronous composition of τ_i.

Efficient Model Checking MAS

- Bounded Model Checking [PL03].
- BDD-based Model Checking [GvdM04,LQR05].
- Abstraction [CDLR08].
- Partial Order Reduction [LPQ10].

Implementations: MCMAS (Imperial), VerICS (Warsaw), MCK (Sydney). Widely used *but number of agents is fixed*.

Model Checking **Open** MAS

MAS are often open systems.

- Swarm robotics,
- Multi-party negotiation protocols and auctions,
- Voting protocols,
- e-institutions.

The problem: Parameterised model checking for open MAS.

Our contribution: Cutoffs in the context of open MAS.

Parameterised Interpreted Systems

- All agents encoded by a single **agent template**.
- One environment modelled by an **environment template**.
- The agent and environment template define a generic system $\mathcal{S}$, representing an arbitrary number of **concrete** systems.
- Given an $n \in \mathbb{N}$, a concrete system $\mathcal{S}(n)$ is made of n indexed instantiations of the template agent composed with a parameterised environment.

Actions and Synchronisation in PIS

PIS: Essential feature is how the agents interact between them and the environment.

- Agent template $\mathcal{T} = \langle L, \iota, Act, P, t \rangle$;
- Environment template $\mathcal{E} = \langle L_E, \iota_E, Act_E, P_E, t_E \rangle$.
- From IIS [LPQ10]: Only one local action performed in a concrete system at a given round; every agent that is potentially able to perform said action has to perform it at that round.
- Agent's actions partitioned in
  - asynchronous (each concrete action admitted by exactly one agent),
  - agent-environment (each concrete action shared by exactly one agent and the environment)
  - global-synchronous (each concrete action shared by all the agents and the environment)

Actions and Synchronisation in PIS

Template action	$a \in A$	$b \in AE$	$c \in GS$
Agent 1	$a_1 \in A_1$	$b_1 \in AE_1$	$c \in GS_1$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
Agent i	$a_i \in A_i$	$b_i \in AE_i$	$c \in GS_i$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
Agent n	$a_n \in A_n$	$b_n \in AE_n$	$c \in GS_n$
Environment		$\{b_1, \ldots, b_n\} \subseteq AE_E$	$c \in GS_E$

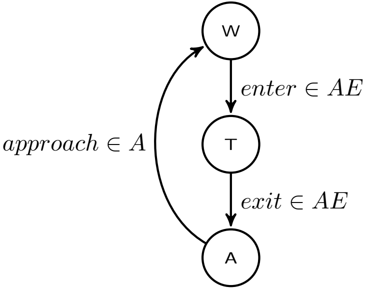
PIS: Global Transitions

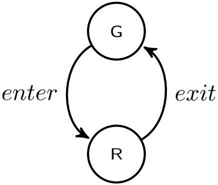
Global transitions from a concrete global state g to a successor g' can happen if:

- An asynchronous action is enabled for some agent at g.
- An agent-environment action is enabled for some agent and the environment at g.
- A global-synchronous action is enabled for all agents and the environment at g.

Modelling Example

Agent and environment templates of the untimed version of the Train-Gate-Controller.





Specs built from the logic indexed ACTL*K$\backslash X$

- Combines indexed ACTL$^* \setminus X$ with indexed epistemic modalities.
- Epistemic modalities are interpreted over epistemic accessibility relations defined on local equalities for the agents' states.
- Specifications range over m-tuples of distinct agents for $m \geq 1$.

$$\forall_{v_1} \ldots \forall_{v_m} \phi(v_1, \ldots, v_m)$$

- Example specification for the TGC.

$$\forall_i \forall_j AG(T_i \rightarrow K_i \neg T_j)$$

"whenever an agent i is in the tunnel, it knows agent j is not".

MAS Cutoffs

MAS Cutoff

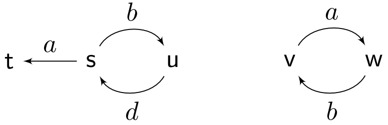
Consider the set $\Gamma(m)$ of all specifications with at most m variables and a PIS $\mathcal{S}$. $c \in \mathbb{N}$ is said to be a *MAS cutoff* for $\mathcal{S}$ if

$$\mathcal{S}(c) \models \phi \Leftrightarrow \forall n \geq c : \mathcal{S}(n) \models \phi \text{ for any } \phi \in \Gamma(m)$$

Only a Sufficient Condition

Lemma

There are PIS that admit no cutoffs for any $\Gamma(m)$



(a) Template Agent

(b) Template Environment

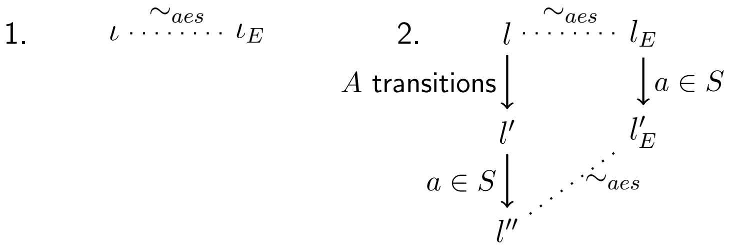
where $a, b \in AE$ (agent-environment) and $d \in A$ (asynchronous).
Specifications can count the loops on the composition above thereby counting the number of agents.

Simulations between Agent and Env Templates

Agent-environment simulations

A relation $\sim_{aes} \subseteq L \times L_E$ is an *agent-environment simulation* between $\mathcal{T}$ and $\mathcal{E}$ if

1. $\iota \sim_{aes} \iota_E$ and
2. whenever $l \sim_{aes} l_E$ then if there is $l', l'' \in L$ such that $l \rightarrow_{A*} l' \rightarrow_a l''$ for some $a \in AE \cup GS$, then $a \in P_E(l_E)$ and $l'' \sim_{aes} t_E(l_E, a)$.



Cutoff Identification

Cutoff theorem

For $\Gamma(m)$, if $\mathcal{T} \leq_{aes} \mathcal{E}$ then $c = max(2, m)$.

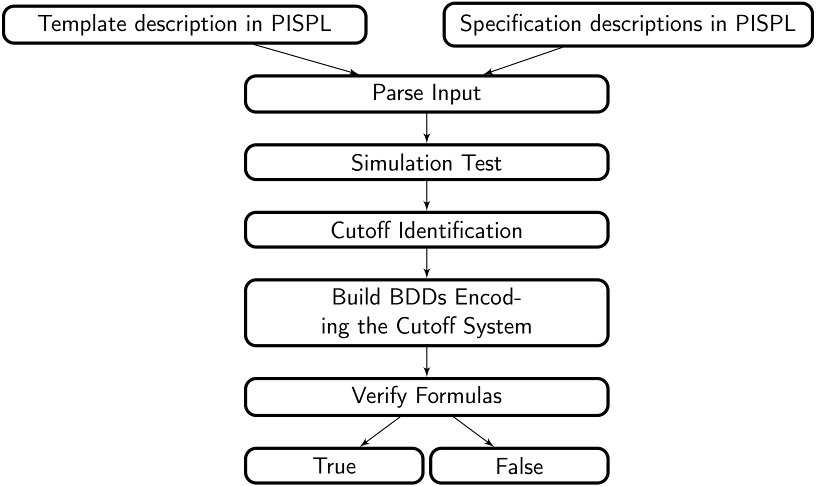
The result relies on the semantical constraint that template actions for the environment are enabled at exactly one template state.

The constraint can be relaxed in the absense of agent-environment actions.

Cutoff theorem

For $\Gamma(m)$, if $AE = \emptyset$, then $c = m$.

Implementation: MCMAS-P



Available for download from `http://vas.doc.ic.ac.uk/`.

Conclusions

- Model checking MAS now a relatively mature area of research, but many scalability issues remain.
- Current techniques to deal with state-explosion problem do not tackle unbounded number of components leading to limited applicability in many MAS applications.
- Novel parametric semantics.
- Cutoff technique for parametric temporal-epistemic specifications.
- Implementation.

Future work

- Generalised semantics.
- Multiple roles.
- Synchronous MAS and CTLK$\backslash X$.