Verifying Auctions as Artifact Systems: Decidability via Finite Abstraction

Francesco Belardinelli
Laboratoire IBISC, Université d’Evry

based on work with Alessio Lomuscio
Imperial College London, UK

and Fabio Patrizi
Sapienza Università di Roma, Italy

Imperial College London – 13 March 2014
Model checking: technique(s) to automatically verify that a system design $S$ satisfies a property $P$ before deployment.

More formally, given

- a model $M_S$ of system $S$
- a formula $\phi_P$ representing property $P$

we check that

$$M_S \models \phi_P$$
Turing Award 2007

(a) E. Clarke  
(CMU, USA)

(b) A. Emerson  
(U. Texas, USA)

(c) J. Sifakis  
(IMAG, F)

- Jury justification

“For their roles in developing model checking into a highly effective verification technology, widely adopted in the hardware and software industries.”
Motivation and Background:

- Artifact Systems as *data-aware* systems
- Parallel English (ascending bid) Auctions as Artifact Systems (eBay, etc.)
Motivation and Background:
- Artifact Systems as *data-aware* systems
- Parallel English (ascending bid) Auctions as Artifact Systems (eBay, etc.)

Main task: *formal verification of infinite-state AS*
- model checking is appropriate for control-intensive applications...
- ...but less suited for data-intensive applications (data typically range over infinite domains) [1]
Overview

Motivation and Background:
- Artifact Systems as *data-aware* systems
- Parallel English (ascending bid) Auctions as Artifact Systems (eBay, etc.)

Main task: *formal verification of infinite-state AS*
- model checking is appropriate for control-intensive applications...
- ...but less suited for data-intensive applications (data typically range over infinite domains) [1]

Key contribution:
- Verification of *rigid*, *bounded* and *uniform* AS is decidable
  ⇒ Verification of Parallel English Auctions is decidable
Artifact Systems

Outline

- Recent paradigm in Service-Oriented Computing [2].
- **Motto**: let’s give *data* and *processes* the same relevance!
- **Artifact**: data model + lifecycle
  - (nested) records equipped with actions
  - actions may affect several artifacts
  - evolution stemming from the interaction with other artifacts/external actors

- **Artifact System**: interacting artifacts, representing services, manipulated by agents.

- **Auctions as Artifact Systems**

- **Logical Perspective**: first-order modal (temporal epistemic) Kripke models
A single auctioneer $A$ and a finite number of bidders $B_1, \ldots, B_\ell$. 
A single auctioneer $A$ and a finite number of bidders $B_1, \ldots, B_\ell$.  

1. the auctioneer puts on sale a finite number of items, starting from a base price that is public to all bidders;
A single *auctioneer* $A$ and a finite number of *bidders* $B_1, \ldots, B_\ell$.

1. the auctioneer puts on sale a finite number of items, starting from a *base price* that is public to all bidders;

2. at each round the bidder can either choose to bid for a specific item or to skip the round;
A single auctioneer $A$ and a finite number of bidders $B_1, \ldots, B_\ell$.

1. the auctioneer puts on sale a finite number of items, starting from a base price that is public to all bidders;
2. at each round the bidder can either choose to bid for a specific item or to skip the round;
3. at the end of the bidding process, the item is assigned to the bidder with the highest offer.
A single auctioneer $A$ and a finite number of bidders $B_1, \ldots, B_\ell$.

1. the auctioneer puts on sale a finite number of items, starting from a base price that is public to all bidders;
2. at each round the bidder can either choose to bid for a specific item or to skip the round;
3. at the end of the bidding process, the item is assigned to the bidder with the highest offer.

Assumptions:
A single auctioneer $A$ and a finite number of bidders $B_1, \ldots, B_\ell$.

1. the auctioneer puts on sale a finite number of items, starting from a base price that is public to all bidders;
2. at each round the bidder can either choose to bid for a specific item or to skip the round;
3. at the end of the bidding process, the item is assigned to the bidder with the highest offer.

Assumptions:

- each bidder is rational;
Artifact Systems
Parallel English (ascending bid) Auctions

A single auctioneer $A$ and a finite number of bidders $B_1, \ldots, B_\ell$.

1. the auctioneer puts on sale a finite number of items, starting from a base price that is public to all bidders;
2. at each round the bidder can either choose to bid for a specific item or to skip the round;
3. at the end of the bidding process, the item is assigned to the bidder with the highest offer.

Assumptions:
- each bidder is rational;
- he has an intrinsic value for each item being auctioned;
A single *auctioneer* $A$ and a finite number of *bidders* $B_1, \ldots, B_\ell$.

1. the auctioneer puts on sale a finite number of items, starting from a *base price* that is public to all bidders;
2. at each round the bidder can either choose to bid for a specific item or to skip the round;
3. at the end of the bidding process, the item is assigned to the bidder with the highest offer.

**Assumptions:**
- each bidder is rational;
- he has an *intrinsic value* for each item being auctioned;
- and he keeps this information private from other bidders and the auctioneer.
Auction Data Model

**Bidding**

<table>
<thead>
<tr>
<th>item</th>
<th>base_price</th>
<th>bid₁</th>
<th>...</th>
<th>bidₗ</th>
<th>status</th>
</tr>
</thead>
</table>

- \( \text{init}_A(\text{item}, \text{base}_\text{price}) \)
- \( \text{bid}_i(\text{item}, \text{bid}) \)
- \( \text{time}_\text{out}(\text{item}) \)
- \( \text{skip}_A \)
- \( \text{skip}_i \)
- \( \text{skip}_i \)
- \( \ldots \)

**trueValue_i**

<table>
<thead>
<tr>
<th>item</th>
<th>true_value</th>
</tr>
</thead>
</table>

- \( \text{init}_i(\text{item}, \text{true}_\text{value}) \)
- \( \ldots \)
Artifact Systems
Auction Lifecycle

- Agents operate on artifacts.
  - e.g., the bidder sends a new bid to the auctioneer.

- Actions add/remove artifacts or change artifact attributes.
  - e.g., the auctioneer puts a new item on auction.

- The whole system can be seen as a \textit{data-aware} dynamic system.
  - at every step, an action yields a change in the current state.
Research questions

1. Which syntax and semantics to specify AS?
Research questions

1. Which syntax and semantics to specify AS?

2. Is verification of AS decidable?
Research questions

1. Which syntax and semantics to specify AS?
2. Is verification of AS decidable?
3. If not, can we identify relevant fragments that are reasonably well-behaved?
Challenges

Multi-agent systems, but . . .
Challenges

Multi-agent systems, but . . .
  • . . . states have a relational structure,
Challenges

Multi-agent systems, but . . .

• . . . states have a relational structure,

• data are potentially infinite,
Challenges

Multi-agent systems, but . . .

- . . . states have a relational structure,
- data are potentially infinite,
- the state space is infinite in general.
Challenges

Multi-agent systems, but . . .

- . . . states have a relational structure,
- data are potentially infinite,
- the state space is infinite in general.

⇒ The model checking problem cannot be tackled by standard techniques.
Artifact Systems

Results

Artifact-centric multi-agent systems (AC-MAS) as a formal model for AS.

Intuition: databases (?) that evolve in time and are manipulated by agents.
Artifact Systems
Results

1. *Artifact-centric multi-agent systems* (AC-MAS) as a formal model for AS.
   **Intuition:** databases (?) that evolve in time and are manipulated by agents.

2. FO-CTLK as a specification language:

   \[
   AG \forall it, \vec{bd}, s (\exists ! bp \text{ Bidding}(it, \vec{bd}, bp, s) \land \exists^{\leq 1} tv \text{ trueValue}_i(it, tv))
   \]

   for each item there is exactly one base price, while bidders associate at most one true value to each item (possibly none).
Artifact Systems
Results

1. **Artifact-centric multi-agent systems (AC-MAS)** as a formal model for AS.
   **Intuition:** databases (?) that evolve in time and are manipulated by agents.

2. FO-CTLK as a specification language:
   \[ AG \forall it, bd, s(\exists! bp Bidding(it, bd, bp, s) \land \exists_{\leq 1} tv \text{ trueValue}_i(it, tv)) \]
   for each item there is exactly one base price, while bidders associate at most one true value to each item (possibly none).

3. Model theory of FO modal logic: abstraction and bisimulation to tackle model checking.
   **Main result:** under specific conditions MC can be reduced to the finite case.
Artifact Systems

Results

1. **Artifact-centric multi-agent systems** (AC-MAS) as a formal model for AS.
   
   **Intuition**: databases (?) that evolve in time and are manipulated by agents.

2. FO-CTLK as a specification language:

   \[ AG \forall it, \vec{bd}, s(\exists!bp \ Bidding(it, \vec{bd}, bp, s) \land \exists^{\leq 1} tv \ trueValue_i(it, tv)) \]

   *for each item there is exactly one base price, while bidders associate at most one true value to each item (possibly none).*

3. Model theory of FO modal logic: abstraction and bisimulation to tackle model checking.
   
   **Main result**: under specific conditions MC can be reduced to the finite case.

4. **Case study**: modelling and verifying auctions as AC-MAS.
Semantics: Databases

The data model of AS is given as a particular kind of database.

- a **database schema** is a **finite** set \( D = \{ P_1/a_1, \ldots, P_n/a_n, Q_1/b_1, \ldots, Q_m/b_m \} \) of relation symbols \( R_i \) with arity \( c_i \in \mathbb{N} \).

- an **instance** on a domain \( U \) is a mapping \( D \) associating
  - each symbol \( P_i \) with a **finite** \( a_i \)-ary relation on \( U \)
  - each symbol \( Q_i \) with a (possibly infinite) \( b_i \)-ary relation on \( U \)

- the **active domain** \( \text{adom}(D) \) is the set of all \( u \in U \) appearing in some \( D(P_i) \).

- the **disjoint union** \( D \oplus D' \) is the \( (D \cup D') \)-interpretation s.t.
  1. \( D \oplus D'(R_i) = D(R_i) \)
  2. \( D \oplus D'(R'_i) = D'(R_i) \)

We consider untyped languages; the extension to types is not problematic.
Artifact-centric Multi-agent Systems

Agents

Agents have partial access (views) to the artifact system.

- An agent is a tuple \( A_i = \langle D_i, Act_i, Pr_i \rangle \) where
  - \( D_i \) is the local database schema
  - \( Act_i \) is the set of local actions \( \alpha(\vec{x}) \) with parameters \( \vec{x} \)
  - \( Pr_i : D_i(U) \mapsto 2^{Act_i(U)} \) is the local protocol function

- the setting is reminiscent of the interpreted systems semantics for MAS [3], ...

- ...but here the local state of each agent is relational.

Intuitively, agents manipulate artifacts and have (partial) access to the information contained in the global db schema \( \mathcal{D} = \mathcal{D}_1 \cup \cdots \cup \mathcal{D}_\ell \).
Example 1: Parallel English Auction

- Agents: \textbf{Auctioneer, Bidder}_1, \ldots, \textbf{Bidder}_\ell

- local db schema \(\mathcal{D}_A\) for the auctioneer
  - \(Bidding(item, base\_price, bid_1, \ldots, bid_\ell, status)\)
  - \(<\) on \(\mathbb{Q}\)

- local db schema \(\mathcal{D}_i\) for the bidders
  - \(Bidding(item, base\_price, bid_1, \ldots, bid_\ell, status)\)
  - \(TValue_i(item, true\_value)\)
  - \(<\) on \(\mathbb{Q}\)

- then, \(\mathcal{D} = \{Bidding, TValue_1, \ldots, TValue_\ell, <\}\)

- Actions introduce values from an infinite domain \(U = \text{Items} \cup \mathbb{Q} \cup \{\text{active, term}\}:\)
  - \(init_A(item, base\_price), time\_out(item), skip_A\) belong to \(\text{Act}_A\)
  - \(init_i(item, true\_value), bid_i(item, bid), skip_i\) belong to \(\text{Act}_i\)

- The protocol function specifies the preconditions for actions:
  - e.g., \(bid_i(item, bid) \in Pr_i(D)\) whenever
    - item appears in \(D(TValue_i)\)
    - the highest bid \(bid_j\) in \(Bidding, j \neq i\), for item is \(<\) \(true\_value\) for bidder \(B_i\)
    - \(bid_j < bid \leq true\_value\)
    - \(D(status) = active\) for item
  - the \(skip\) actions are always enabled.
Agents are modules that can be composed together to obtain AC-MAS.

- **Global states** are tuples $s = \langle D_0, \ldots, D_\ell \rangle \in \mathcal{D}(U)$.

- An **AC-MAS** is a tuple $\mathcal{P} = \langle \text{Ag}, s_0, \rightarrow \rangle$ where
  - $\text{Ag} = \{A_0, \ldots, A_\ell\}$ is a **finite set of agents**
  - $s_0 \in \mathcal{D}(U)$ is the **initial global state**
  - $s \xrightarrow{\alpha(\vec{u})} s'$ is the **transition relation**

- **Epistemic relation**: $s \sim_i s'$ iff $D_i = D'_i$

- An AC-MAS $\mathcal{P}$ is **rigid** iff for all states $s, s'$, symbols $Q$, and agents $A_i, A_j \in \text{Ag}$, $D_i(Q) = D'_j(Q)$.

- AC-MAS are **infinite-state systems in general**

AC-MAS are first-order temporal epistemic structures.

$\Rightarrow$ **FO-CTLK** can be used as a specification language.
Example 2: the Auction AC-MAS

The *Auction AC-MAS* \( \mathcal{A} = \langle \mathcal{A}g, s_0, \rightarrow \rangle \) is defined as

- \( \mathcal{A}g = \{A, B_1, \ldots, B_\ell\} \)
- \( s_0 \) is the *empty interpretation* of \( \mathcal{D} = \{Bidding, TValue_1, \ldots, TValue_\ell, <\} \) but for <

- \( \rightarrow \) is the *transition relation* s.t. \( s \xrightarrow{\alpha (\vec{u})} s' \) whenever
  - \( \alpha_i = bid_i(\text{item}, bid') \) and \( s' \) modifies \( s \) by replacing any tuple \( (\text{item}, \ldots, bid_i, \ldots, \text{status}) \) in \( D_s(Bidding) \) with \( (\text{item}, \ldots, bid'_i, \ldots, \text{status}) \)
  - \( \alpha_A = \text{timeout}(\text{item}) \) and the value of \( \text{status} \) in \( D_{s'}(Bidding) \) for \( \text{item} \) is *term*
  - ...

Notice: the auction AC-MAS \( \mathcal{A} \) is *rigid*
Syntax: FO-CTLK

• Data call for First-order Logic.
• Evolution calls for Temporal Logic.
• Agents (operating on artifacts) call for Epistemic Logic.

The specification language FO-CTLK:

\[ \varphi ::= R(t_1, \ldots, t_c) \mid t = t' \mid \neg \varphi \mid \varphi \rightarrow \varphi \mid \forall x \varphi \mid AX \varphi \mid A\varphi U \varphi \mid E\varphi U \varphi \mid K_i \varphi \]

Alternation of free variables and modal operators is enabled.
Semantics of FO-CTLK

Formal definition

An AC-MAS $\mathcal{P}$ satisfies an FO-CTLK-formula $\varphi$ in a state $s$ for an assignment $\sigma$, iff

$$
\begin{align*}
(\mathcal{P}, s, \sigma) &\models R(t) & \text{iff} & & \langle \sigma(t_1), \ldots, \sigma(t_c) \rangle \in D_s(R) \\
(\mathcal{P}, s, \sigma) &\models t = t' & \text{iff} & & \sigma(t) = \sigma(t') \\
(\mathcal{P}, s, \sigma) &\models \neg \varphi & \text{iff} & & (\mathcal{P}, s, \sigma) \not\models \varphi \\
(\mathcal{P}, s, \sigma) &\models \varphi \rightarrow \psi & \text{iff} & & (\mathcal{P}, s, \sigma) \not\models \varphi \text{ or } (\mathcal{P}, s, \sigma) \models \psi \\
(\mathcal{P}, s, \sigma) &\models \forall x \varphi & \text{iff} & & \text{for all } u \in \text{adom}(s), (\mathcal{P}, s, \sigma^u_x) \models \varphi \\
(\mathcal{P}, s, \sigma) &\models AX \varphi & \text{iff} & & \text{for all runs } r, r(0) = s \text{ implies } (\mathcal{P}, r(1), \sigma) \models \varphi \\
(\mathcal{P}, s, \sigma) &\models A\varphi U \varphi' & \text{iff} & & \text{for all runs } r, r(0) = s \text{ implies } (\mathcal{P}, r(k), \sigma) \models \varphi' \text{ for some } k \geq 0, \text{ and } (\mathcal{P}, r(k'), \sigma) \models \varphi \text{ for all } 0 \leq k' < k \\
(\mathcal{P}, s, \sigma) &\models E\varphi U \varphi' & \text{iff} & & \text{there exists } r \text{ s.t. } r(0) = s, (\mathcal{P}, r(k), \sigma) \models \varphi' \text{ for some } k \geq 0, \text{ and } (\mathcal{P}, r(k'), \sigma) \models \varphi \text{ for all } 0 \leq k' < k \\
(\mathcal{P}, s, \sigma) &\models Ki \varphi & \text{iff} & & \text{for all states } s', s \sim_i s' \text{ implies } (\mathcal{P}, s', \sigma) \models \varphi
\end{align*}
$$

- Active-domain semantics, but...
  - ...we can refer to individuals that no longer exist
  - the number of states is infinite in general

19
Semantics of FO-CTLK

Intuition

(d) $AX \varphi$

(e) $A\varphi U \psi$

(f) $E \varphi U \psi$
Verification of AC-MAS

How do we check FO-CTLK specifications on auctions?

- the true value of items for each bidder is secret to all other bidders and to the auctioneer:
  \[ AG \forall item \neg \exists \text{true_value} \bigvee_{j \neq i \land j = A} K_j \text{TValue}_i(it, \text{true_value}) \]

- for each bidder, each bid is less or equal to her true value:
  \[ AG \forall it, \vec{x}, bd_i, \vec{y}, tv(Bidding(it, \vec{x}, bd_i, \vec{y}) \land \text{TValue}_i(it, tv) \rightarrow bd_i \leq tv) \]

- each bidder can raise her bid unless she has already hit her true value:
  \[ AG \forall it, \vec{x}, bd_i, \vec{y}(Bidding(it, \vec{x}, bd_i, \vec{y}) \rightarrow \neg \exists \vec{x}', bd_i', \vec{y}'(bd_i' > bd_i \land Bidding(it, \vec{x}', bd_i', \vec{y}')))) \]

Problem: the infinite domain \( U \) may generate infinitely many states!

Investigated solution: can we simulate the concrete values in \( U \) with a finite set of abstract symbols?
Abstraction: Isomorphism and Bisimulation

- two states $s, s'$ are isomorphic, or $s \simeq s'$, if there is a bijection

$$\iota : \text{adom}(s) \cup C \mapsto \text{adom}(s') \cup C$$

such that

- $\iota$ is the identity on $C$
- for every $\bar{u}$ in adom($s$), $A_i \in A_g$, $\bar{u} \in D_i(R) \Leftrightarrow \iota(\bar{u}) \in D_i'(R)$

\[
\begin{array}{|c|c|c|} 
\hline
 & D(R) & \sim \ & D'(R) \\
\hline
A_1 & a & b & A_1 & 1 & 2 \\
A_2 & b & c & A_2 & 2 & c \\
A_3 & d & e & A_3 & 4 & 5 \\
\hline
\end{array}
\]

- $\iota : a \mapsto 1$
  $b \mapsto 2$
  $c \mapsto c$
  $d \mapsto 4$
  $e \mapsto 5$
two states $s, s'$ are *bisimilar*, or $s \approx s'$, if

1. $s \approx s'$
2. if $s \rightarrow t$ then there is $t'$ s.t. $s' \rightarrow t'$, $s \oplus t \approx s' \oplus t'$, and $t \approx t'$
Abstraction: Isomorphism and Bisimulation

- two states $s, s'$ are *bisimilar*, or $s \approx s'$, if
  1. $s \simeq s'$
  2. if $s \rightarrow t$ then there is $t'$ s.t. $s' \rightarrow t'$, $s \oplus t \simeq s' \oplus t'$, and $t \approx t'$

\[ s \rightarrow t \]
\[ s' \rightarrow t' \]

- the other direction holds as well
- similar conditions for the epistemic relation $\sim_i$
Abstraction: Isomorphism and Bisimulation

However, bisimulation is not sufficient to preserve FO-CTLK formulas:

\[ \phi = \text{AG} \ \forall x \ (P(x) \rightarrow \text{AX} \ \text{AG} \ \neg P(x)) \]
Uniformity

- Intuitively, the behaviour of uniform AC-MAS is *independent* from data not explicitly named in the system description.

Also, rigid AC-MAS must satisfy a condition akin to density of $<$ on $Q$. 
**Uniformity**

- Intuitively, the behaviour of uniform AC-MAS is *independent* from data not explicitly named in the system description.
- More formally, an AC-MAS $\mathcal{P}$ is *uniform* iff for $s, t, s', t' \in S$ and $t' \in \mathcal{D}(U)$:

  $s \rightarrow t$ and $s \oplus t \simeq s' \oplus t'$ imply $s' \rightarrow t'$

\[
\begin{array}{c|c|c|c|c}
  & a & b & c & e \\
  a &   &   &   &   \\
  b &   &   &   &   \\
  d &   &   &   &   \\
\end{array}
\quad 
\begin{array}{c|c|c}
  & a & f \\
  a &   & f \\
  f &   & c \\
\end{array}
\]

\[
\begin{array}{c|c|c}
  s' & 1 & 2 \\
  1 &   &   \\
  2 &   & c \\
  4 &   & 5 \\
\end{array}
\quad 
\begin{array}{c|c|c}
  t' & 1 & 6 \\
  1 &   & 6 \\
  6 &   & c \\
\end{array}
\]\n
Also, rigid AC-MAS must satisfy a condition akin to density of $\prec$ on $Q$. 

Uniform AC-MAS cover many interesting cases [2, 4], including the auction AC-MAS $\mathcal{A}$.
Uniformity

- Intuitively, the behaviour of uniform AC-MAS is *independent* from data not explicitly named in the system description.
- More formally, an AC-MAS $\mathcal{P}$ is uniform iff for $s, t, s', t' \in S$ and $t' \in D(U)$:

1. $s \to t$ and $s \oplus t \simeq s' \oplus t'$ imply $s' \to t'$

\[
\begin{array}{c|c|c|c|c|c|c|c}
& a & b & c & d & e & f & c \\
\hline
s & & & & & & & \\
\hline
\end{array}
\]

\[
\begin{array}{c|c|c|c|c|c|c|c}
& a & f & c & f & c & & \\
\hline
t & & & & & & & \\
\hline
\end{array}
\]

\[
\begin{array}{c|c|c|c|c|c|c|c}
1 & 2 & & & & & & \\
\hline
s' & & & & & & & \\
\hline
2 & c & & & & & & \\
\hline
4 & 5 & & & & & & \\
\hline
\end{array}
\]

\[
\begin{array}{c|c|c|c|c|c|c|c}
1 & 6 & & & & & & \\
\hline
(t') & & & & & & & \\
\hline
2 & c & & & & & & \\
\hline
4 & 5 & & & & & & \\
\hline
\end{array}
\]

2. Also, rigid AC-MAS must satisfy a condition akin to density of $<$ on $\mathbb{Q}$. 


Uniformity

- Intuitively, the behaviour of uniform AC-MAS is *independent* from data not explicitly named in the system description.
- More formally, an AC-MAS $\mathcal{P}$ is *uniform* iff for $s, t, s' \in S$ and $t' \in D(U)$:

1. $s \rightarrow t$ and $s \oplus t \simeq s' \oplus t'$ imply $s' \rightarrow t'$

![Diagram](image)

2. Also, rigid AC-MAS must satisfy a condition akin to density of $<$ on $\mathbb{Q}$.

- Uniform AC-MAS cover many interesting cases [2, 4], including the auction AC-MAS $\mathcal{A}$. 
Bisimulation and Equivalence w.r.t. FO-CTLK

Theorem

Consider

- bisimilar and uniform AC-MAS $\mathcal{P}$ and $\mathcal{P}'$
- an FO-CTLK formula $\varphi$

If

1. $|U'| \geq 2 \cdot \sup_{s \in \mathcal{P}} \{|\text{adom}(s)| + |C| + |\text{vars}(\varphi)|\}$
2. $|U| \geq 2 \cdot \sup_{s' \in \mathcal{P}'} \{|\text{adom}(s')| + |C| + |\text{vars}(\varphi)|\}$

then

$$\mathcal{P} \models \varphi \iff \mathcal{P}' \models \varphi$$

Can we apply this result to finite abstraction?
Abstraction

Abstractions are defined in an agent-based, modular way.

- Let $A = \langle D, Act, Pr \rangle$ be an agent defined on the domain $U$.
  Given a domain $U'$, the abstract agent $A' = \langle D, Act, Pr' \rangle$ on $U'$ is s.t.
  - $Pr'$ is the smallest function s.t. if $\alpha(\vec{u}) \in Pr(D)$, $D' \in D'(U')$ and $D' \simeq D$ for some witness $\iota$, then $\alpha(\iota(\vec{u})) \in Pr'(D')$.

- Let $P = \langle Ag, s_0, \rightarrow \rangle$ be an AC-MAS.
  The abstraction $P' = \langle Ag', s'_0, \rightarrow' \rangle$ of $P$ is an AC-MAS s.t.
  - $Ag'$ be the set of abstract agents on $U'$
  - $s'_0 \simeq s_0$
  - $\rightarrow'$ is the smallest function s.t. if $s \xrightarrow{\alpha(\vec{u})} t$, and $s \oplus t \simeq s' \oplus t'$ for some witness $\iota$, then $s' \xrightarrow{\alpha(\iota(\vec{u}))} t'$.

Notice: the abstraction of a rigid AC-MAS is not necessarily rigid!
Abstraction

- Let $N_{Ag} = \sum_{A_i \in Ag} \max\{\alpha(\vec{x}) \in Act_i\} |\vec{x}|$ be the sum of the maximum numbers of parameters contained in the action types of each agent.

Lemma

Consider

- a rigid and uniform AC-MAS $\mathcal{P}$
- a set $U' \supseteq C$ s.t. $|U'| \geq 2 \sup_{s \in \mathcal{P}} |adom(s)| + |C| + N_{Ag}$

Then, there exists an abstraction $\mathcal{P}'$ of $\mathcal{P}$ that is uniform and bisimilar to $\mathcal{P}$.

How can we define finite abstractions?
Bounded Models and Finite Abstractions

- An AC-MAS $\mathcal{P}$ is $b$-bounded iff for all $s \in \mathcal{P}$, $|\text{adom}(s)| \leq b$.
- Bounded systems can still be infinite!

**Theorem**

Consider

- a $b$-bounded, rigid and uniform AC-MAS $\mathcal{P}$ on an infinite domain $U$
- an FO-CTLK formula $\varphi$

Given a finite $U' \supseteq C$ s.t.

$$|U'| \geq 2b + |C| + \max\{|\text{vars}(\varphi)|, N_{\text{Ag}}\}$$

there exists a finite abstraction $\mathcal{P}'$ of $\mathcal{P}$ s.t.

- $\mathcal{P}'$ is uniform and bisimilar to $\mathcal{P}$

Moreover,

$$\mathcal{P} \models \varphi \iff \mathcal{P}' \models \varphi$$

$\Rightarrow$ Under specific circumstances, we can model check an infinite-state system by verifying its finite abstraction.
• **Notice:** the auction AC-MAS $\mathcal{A}$ is bounded by $b = |\text{Items}|(2|\text{Ag}| - 1) + 2$

• Consider a finite $U' \geq 2b + \text{vars}(\phi)$

• Abstract agents **Auctioneer** $A'$ and **Bidders** $B'_i$
  
  ▶ the local db schemas $\mathcal{D}'_A$ and $\mathcal{D}'_i$ are the same as for $A$ and $B_i$
  
  ▶ the sets of actions $\text{Act}'_A$ and $\text{Act}'_i$ are the same as for $A$ and $B_i$
  
  ▶ the protocol function $\text{Pr}'_A$ is the same as for $A$
  
  ▶ as to $\text{Pr}'_i$, $\text{bid}_i(\text{item}, \text{bid}) \in \text{Pr}'_i(\mathcal{D}')$ whenever
    
    * ... 
    
    * bid is an abstract value that does not represent any bid in $\mathcal{D}'$
The abstract auction AC-MAS $\mathcal{A}' = \langle \mathcal{A}'_g, s'_0, \tau' \rangle$ is defined as

- $\mathcal{A}'_g = \{ A', B'_1, \ldots, B'_\ell \}$
- $s'_0$ is the empty interpretation of $\mathcal{D}$
- $\rightarrow'$ mimics $\rightarrow$
  - e.g., if $\alpha_i = bid_i(\text{item}, \text{bid})$, then $s \xrightarrow{\alpha(\vec{u})} t$ whenever $t$ modifies $s$ by replacing any tuple $(\text{item}, \ldots, bid_i, \ldots, \text{status})$ in $D_s(\text{Bidding})$ with $(\text{item}, \ldots, bid'_i, \ldots, \text{status})$, where the value $bid' \in U'$ has been found as above. In particular, $bid < bid' \leq \text{true-value}$ in $t$.
- By the assumption that $U' \geq 2b + \text{vars}(\phi)$ and Theorem 3 we have that $\mathcal{A}'$ is a finite abstraction of $\mathcal{A}$.
- In particular, $\mathcal{A}'$ is uniform and bisimilar to $\mathcal{A}$ (but not rigid) and $\mathcal{A} \models \phi$ iff $\mathcal{A}' \models \phi$.
Extensions

1. Non-uniform AC-MAS: for *sentence-atomic* FO-CTL the results above still hold.

\[ AG \forall it, \vec{bd}, s(\exists! bp \text{ Bidding}(it, \vec{bd}, bp, s) \land \exists^{\leq 1} tv \text{ TValue}_i(it, tv)) \]
Extensions

1. Non-uniform AC-MAS: for sentence-atomic FO-CTL the results above still hold.
   \[ \text{AG } \forall \text{it}, \vec{bd}, s(\exists ! bp \text{ Bidding(it, bd, bp, s)} \wedge \exists^{\leq 1} tv \ TValue_i(it, tv)) \]

2. Non-uniform and unbounded AC-MAS: one-way preservation result for FO-ACTLK\(^-\).

**Theorem**

For every AC-MAS \( P \) and \( \varphi \in \text{FO-ACTLK}^- \), there exists a finite abstraction \( P' \) s.t.

\[ P' \models \varphi \Rightarrow P \models \varphi \]
Extensions

1. Non-uniform AC-MAS: for sentence-atomic FO-CTL the results above still hold.
   \[ AG \forall it, \vec{bd}, s(\exists!bp \text{ Bidding}(it, \vec{bd}, bp, s) \land \exists^{\leq 1} tv \text{ TValue}_i(it, tv)) \]


**Theorem**

*For every AC-MAS \( \mathcal{P} \) and \( \varphi \in \text{FO-ACTLK}^- \), there exists a finite abstraction \( \mathcal{P}' \) s.t.*

\[ \mathcal{P}' \models \varphi \implies \mathcal{P} \models \varphi \]

3. *Model checking bounded* AC-MAS w.r.t. FO-CTL is undecidable.
Extensions

1. Non-uniform AC-MAS: for *sentence-atomic* FO-CTL the results above still hold.

\[ AG \forall it, \vec{bd}, s(\exists ! bp \ Bidding(it, \vec{bd}, bp, s) \land \exists^{\leq 1} tv \ TValue_i(it, tv)) \]


**Theorem**

*For every AC-MAS $\mathcal{P}$ and $\varphi \in$ FO-ACTLK$^-$, there exists a finite abstraction $\mathcal{P}'$ s.t.*

\[ \mathcal{P}' \models \varphi \implies \mathcal{P} \models \varphi \]

3. *Model checking bounded* AC-MAS w.r.t. FO-CTL is undecidable.

4. Complexity result:

**Theorem**

*The model checking problem for finite AC-MAS w.r.t. FO-CTLK is EXPSPACE-complete in the size of the formula and data.*
• Bisimulation and finite abstraction for first-order Kripke models.

• We are able to model check AC-MAS w.r.t. full FO-CTLK...

• ...however, our results hold only for rigid, uniform and bounded systems.

• This class includes many interesting systems (AS programs, [2, 4],

• including parallel English auctions.
Next Steps

- Constructive techniques for finite abstraction.
- Model checking techniques for finite-state systems are effective on AC-MAS?
- How to perform the boundedness check?
- What if the system is \textit{unbounded/not uniform}?
Thank you!
References

Christel Baier and Joost-Pieter Katoen.

*Principles of Model Checking.*

D. Cohn and R. Hull.


*Reasoning About Knowledge.*

B. Bagheri Hariri, D. Calvanese, G. De Giacomo, R. De Masellis, and P. Felli.

Foundations of Relational Artifacts Verification.