Verification of Generic, Relational Transition Systems

Diego Calvanese\textsuperscript{1,2}, Giuseppe De Giacomo\textsuperscript{3}, Marco Montali\textsuperscript{1} and Fabio Patrizi\textsuperscript{3}

\textsuperscript{1}Free University of Bozen-Bolzano, Italy
\textsuperscript{2}Umeå University, Sweden
\textsuperscript{3}Sapienza University of Rome, Italy

Abstract
Generic, relational transition systems form an interesting class of infinite-state transition systems that naturally captures the execution semantics of a variety of formalisms expressing processes operating over (relational) data. Examples of such data-aware processes include action theories in the situation calculus in AI and data-centric business processes in BPM. In this extended abstract, we summarize the main body of results produced in a decade-long research program focused on the verification of generic, relational transition systems against properties specified using variants of first-order temporal logics.

Keywords
data-aware processes, first-order temporal logics, verification, model checking, action theories, state-boundedness

1. Introduction

Relational transition systems (RTSs) are possibly infinite-state transition systems whose states are labeled by first-order (FO) interpretations \cite{1}. Generic RTSs are RTSs with the key property that states with isomorphic interpretations induce the same transitions modulo renaming of objects \cite{2, 3}. This implies that, whenever the current state of the system has a successor state where new, (locally) fresh objects are injected, then what matters about such fresh objects is only how they relate to each other and to those already present in the current state. In this respect, genericity of an RTS is indeed reminiscent of the well-known notion of genericity in first-order logic and relational databases \cite{4}.

Generic RTSs naturally capture the execution semantics of a variety of dynamic systems operating over relational data (henceforth called data-aware dynamic systems), which have been investigated in AI, BPM, and data management. Example of such systems are:

• action theories in the Situation Calculus \cite{5, 6, 7}, possibly operating over description-logic knowledge bases \cite{8, 9, 10, 11};
• multiagent systems with data-aware, interacting agents \cite{12, 13, 14, 15};
• artifact- and data-centric business processes \cite{16, 17, 18};
• variants of colored Petri nets where tokens carry (tuples of) data that can be compared by
  (in)equality [19, 20, 21, 22].

A long series of works has investigated how to analyze these systems, focusing in particular
on verification [3, 13, 18, 23, 7] and synthesis (typically, planning) [24, 9, 11]. Notably, properties
of interest have to combine, in this setting, temporal/dynamic operators with the ability of
querying the interpretations contained in the state, in turn making it possible to predicate on
the (un)desired evolution of objects and relations as the system unfolds. Natural candidates to
express such properties are thus first-order temporal logics.

In this extended abstract, we summarize the main body of results on verification of first-order
temporal logics over generic RTSs that we have obtained in a decade-long research program.

2. Verification of Generic RTSs

Verification of generic RTSs is in general undecidable even under severe restrictions on the
dynamics that the system can exhibit, and the signature of the FO interpretations. In fact, it is
undecidable to even check reachability of a proposition in data-aware dynamic systems that
manipulate two unary relations through simple actions that can (i) test whether one of the
relations is empty, (ii) insert a new object in one of them, (iii) remove an object from one of
them provided that an object exists [25, 26].

State-boundedness. In this extremely simple setting, undecidability mainly resides in the
ability of the system to accumulate unboundedly many data in a single state. To limit this ability,
the notion of state-boundedness has been introduced in [12, 18] and further studied in [27].
Essentially, in a state-bounded RTS, every state contains a bounded number of objects. Infinitely
many distinct objects can thus be potentially observed along a run, but only boundedly many
can be accumulated in each single state.

State-boundedness is a semantic property, decidable to check for a given bound and unde-
cidable to check if the bound is not known [8, 7]. In this light, different data-aware dynamic
systems that provide compact ways of specifying generic RTSs have been studied, with the aim
of identifying classes that guarantee that the corresponding RTS is indeed state-bounded. This
has been done considering:
  • sufficient, syntactic conditions over the system specification [8, 27];
  • action theories with fading memory [7];
  • resource-constrained colored Petri nets [20];
  • controlled generation of fresh identifiers and other modeling guidelines [28, 29].

The property of state-boundedness turns out to be essential towards singling out decidable
classes for verification. Distinct results are obtained depending on whether branching- or
linear-time first-order temporal logics are considered.

Branching-time FO temporal logics. In [2, 3], it is shown that verification of the full FO
\( \mu \)-calculus is decidable over state-bounded, generic RTSs. This is proved constructively, showing
how to compute a finite-state abstract RTSs that is guaranteed to satisfy all and only the FO
\( \mu \)-calculus properties of the original one. The abstraction is built by considering the input
RTS, the bound, and the number of variables contained in the formula of interest. Notably, the abstraction can be computed also without fixing a specific value for the bound [8].

In [8, 2, 3], fragments of the full FO $\mu$-calculus are studied. Of particular interest is the one with persistent quantification, where FO quantification tracks over time only the identity of objects that remain active in consecutive states (whereas objects disappearing from a state are not tracked anymore). For this fragment, it is shown that an abstract RTS can be constructed independently from the formula to verify, that is, considering only the input RTS.

**Linear-time FO temporal logics.** In [3], it is shown that FO LTL behaves radically differently from the FO $\mu$-calculus: verification of FO LTL properties is undecidable over generic, state-bounded RTSs with a bound of 1. This is particularly interesting, as it implies that in the FO setting, the $\mu$-calculus does not subsume LTL, differently from the propositional setting. In [26], the reason for undecidability is singled out, thanks to a reduction from LTL with freeze quantifiers [30]: it resides in the ability of the logic to unrestrictedly quantify over objects that may be arbitrarily far away from each other. This, in turn, hints that decidability may hold for FO LTL with persistent quantification. As shown in [26], this is indeed the case, and further decidability results are obtained for the problem of monitoring state-bounded, evolving traces.

**References**


