Information and Computation ••• (••••) •••–•••

Contents lists available at ScienceDirect

Information and Computation

www.elsevier.com/locate/yinco

Well-structured graph transformation systems ☆

Barbara König *, Jan Stückrath

Abteilung für Informatik und Angewandte Kognitionswissenschaft, Universität Duisburg-Essen, Lotharstraße 65, 47057 Duisburg, Germany

ARTICLE INFO

Article history:
Received 11 December 2014
Available online xxxx

ABSTRACT

Graph transformation systems (GTSs) can be seen as well-structured transition systems (WSTSs) and via well-structuredness it is possible to obtain decidability results for certain classes of GTSs. We present a generic framework, parameterized over the well-quasi-order (wqo), in which several types of GTSs can be seen as (restricted) WSTSs. We instantiate this framework with three orders: the minor ordering, the subgraph ordering and the induced subgraph ordering. Furthermore we consider two case studies where we apply the theory to analyze a leader election protocol and a simple access rights management system with our tool UNCOVER.

1. Introduction

Well-structured transition systems [3,4] are one of the main sources for decidability results for infinite-state systems. They equip a state space with a quasi-order, which must be a well-quasi-order (wqo) and a simulation relation for the transition relation. The latter condition is also known as compatibility condition or monotonicity requirement. If a system can be seen as a WSTS and some additional conditions are satisfied, one can decide the coverability problem, i.e., the problem of verifying whether, from a given initial state, one can reach a state that covers a final state, i.e., is larger than the final state with respect to the chosen order. Often, these given final states, and all larger states, are considered to be error states and one can hence check whether an error state is reachable. Large classes of infinite-state systems are well-structured, for instance (unbounded) Petri nets and certain lossy systems. For these classes of systems the theory of [3,4] provides a generic backwards reachability algorithm.

A natural specification language for concurrent, distributed systems are graph transformation systems [5] and they usually generate infinite state spaces (even if one factors the state space through graph isomorphism). In those systems states are represented by (hyper-)graphs and state changes by (local) transformation rules, consisting of a left-hand and a right-hand side graph. Graph transformation systems are especially suitable for modeling systems with a variable topology and dynamic creation and deletion of objects.

When working with graphs, we have several orders at our disposal: for instance, the minor ordering, the subgraph ordering and the induced subgraph ordering, leading to different notions of coverability.

The minor ordering is a well-quasi-order for all graphs [6,7], however in order to obtain well-structuredness, we can only allow certain rule sets, for instance one can consider lossy graph transformation systems, where we require an edge contraction rule for each edge label.

☆ This paper is based on our CONCUR '14 paper [1] and also integrates some results which were first published in CAV '08 [2]. The research is partially supported by the DFG project GaReV (KO 2185/6).

* Corresponding author.
E-mail addresses: barbara_koenig@uni-due.de (B. König), jan.stueckrath@uni-due.de (J. Stückrath).

http://dx.doi.org/10.1016/j.ic.2016.03.005
0890-5401/

Please cite this article in press as: B. König, J. Stückrath, Well-structured graph transformation systems, Inf. Comput. (2016), http://dx.doi.org/10.1016/j.ic.2016.03.005

Concerning the subgraph and the induced subgraph ordering, the compatibility condition of WSTSs holds for all rules and it is unnecessary to restrict to lossy systems. On the other hand, the subgraph and the induced subgraph ordering are well-quasi-orders not on the set of all graphs, but only on those graphs where the length of undirected paths is bounded [8]. (For the induced subgraph ordering we additionally have to bound edge multiplicity.) So, in order to obtain a decision procedure, we have to consider a system where only graphs satisfying this restriction are reachable. Even if this condition is not satisfied, the procedure can yield useful partial coverability results. Also, it often terminates even if not all reachable graphs satisfy the restriction (as in our running example), still producing exact results. We make these considerations precise by introducing Q-*restricted* WSTSs, where the order need only be a wqo on Q, a subset of the state space. In general, one wants Q to be as large as possible to obtain stronger statements.

It is clear that there is no order that is superior over all the others, instead there is a trade-off: while the stricter order allows us to consider all graph transformation rules, we have to restrict the state space to a subset Q. Instead, a coarser order requires certain conditions on rule sets, but allows larger state spaces, possibly the set of all graphs. In order to avoid redoing the proofs for every case, we introduce here a flexible general framework which works for orders that can be represented by a class of graph morphisms. This is the case for the three orders mentioned above. Especially, we state the conditions required to perform the backwards search.

In the paper we present two case studies: the verification of a leader election protocol (via the minor ordering) and the verification of a simple access rights management system (via the subgraph ordering). The algorithms for the case of the subgraph and the minor ordering have been implemented in the tool Uncover.[1] We discuss the tool and give runtime results for our running examples as well as for other case studies.

2. Preliminaries

2.1. Well-structured transition systems

We define an extension to the notion of WSTSs as introduced in [3,4], a general framework for decidability results for infinite-state systems, based on well-quasi-orders. Our terminology concerning WSTSs is mainly based on [4].

Definition 1 *(Well-quasi-order and upward closure).* Let X be some set. A quasi-order $\leq$ over X is a *well-quasi-order (wqo)* if for any infinite sequence $x_0, x_1, x_2, \ldots$ of elements of X, there exist indices $i < j$ with $x_i \leq x_j$.

An *upward-closed set* is any set $I \subseteq X$ such that $x \leq y$ and $x \in I$ implies $y \in I$. For a subset $Y \subseteq X$, we define its upward closure $\uparrow Y = \{x \in X \mid \exists y \in Y : y \leq x\}$. Then, a *basis* of an upward-closed set I is a set I_B such that $I = \uparrow I_B$. A *downward-closed set*, downward closure and a basis of a downward-closed set can be defined analogously.

The definition of wqos gives rise to properties which are important for the correctness and termination of the backwards search algorithm presented later.

Lemma 1. *(See [9].) Let $\leq$ be a wqo, then the following two statements hold:*

1. *Any upward-closed set I has a finite basis.*
2. *For any infinite, increasing sequence of upward-closed sets $I_0 \subseteq I_1 \subseteq I_2 \subseteq \ldots$ there exists an index $k \in \mathbb{N}$ such that $I_i = I_{i+1}$ for all $i \geq k$.*

The first property must hold, since an infinite minimal basis implies that the elements of this basis would contain an infinite sequence of elements violating the wqo property. If the second property would not hold, we could form such an infinite sequence by taking elements of $I_{i+1} \setminus I_i$ for each i.

A Q-restricted well-structured transition system (WSTS) is a transition system, equipped with a quasi-order, such that the quasi-order is a (weak) simulation relation on all states and a wqo on a restricted set of states Q.

Definition 2 *(Q-restricted WSTSs).* Let S be a set of states and let Q be a downward closed subset of S, where membership is decidable, i.e. for every $s \in S$ we can decide whether $s \in Q$ or not. A *Q-restricted well-structured transition system (Q-restricted WSTS)* is a transition system $\mathcal{T} = (S, \Rightarrow, \leq)$, where the following conditions hold:

Ordering: $\leq$ is a quasi-order on S and a wqo on Q.
Compatibility: For all $s_1 \leq t_1$ and transitions $s_1 \Rightarrow s_2$, there exists a sequence $t_1 \Rightarrow^* t_2$ of transitions such that $s_2 \leq t_2$.

$$\begin{array}{ccc} t_1 & \overset{*}{\Longrightarrow} & t_2 \\ \vee & & \vee \\ s_1 & \Longrightarrow & s_2 \end{array}$$

[1] The tool is available via www.ti.inf.uni-due.de/research/tools/uncover/.

Please cite this article in press as: B. König, J. Stückrath, Well-structured graph transformation systems, Inf. Comput. (2016), http://dx.doi.org/10.1016/j.ic.2016.03.005