The Causal Graph Revisited for Directed Model Checking: Extended Abstract

Martin Wehrle and Malte Helmert

University of Freiburg, Germany

Directed model checking is a well-established technique to tackle the state explosion problem when the aim is to find error states in large systems. In this approach, the state space traversal is guided through a function that estimates the distance to nearest error states. States with lower estimates are preferably expanded during the search. Overall, directed model checking has proved to be a successful approach. However, its success crucially depends on the applied distance function to guide the search. The challenge is to develop distance functions that are efficiently computable on the one hand and as informative as possible on the other hand.

In this work, we introduce the *causal graph* structure to the context of directed model checking [4]. We model systems in terms of parallel processes with global synchronization. The processes are given as directed labeled graphs, consisting of local states and local transitions. In this model, the causal graph is a dependency structure that represents how the processes depend on each other. A process p depends on a process p' if there might be a need to change a local state in p' in order to change a local state in p such that p and p' can synchronize on a common synchronization label.

Based on causal graph analysis, we first propose a distance estimation function for directed model checking. This distance function is an adaptation of the causal graph heuristic that has first been proposed by Helmert in the context of AI planning [1, 2]. The causal graph heuristic estimates distances to global error states in the parallel system by computing cost estimates for each process p from the current local state to a nearest local error state. In comparison to earlier approaches, we take into account the synchronization behaviour of p with processes on which p depends (i.e., p's predecessors in the causal graph). This yields a more accurate distance estimate than, e.g., the plain graph distance, as the change of *one* local state in p may depend on complex synchronization behaviour with p's causal predecessors.

Furthermore, we investigate an abstraction technique called *safe abstraction* that is guaranteed to preserve error states. The basic idea is to identify processes of the system that do not depend on any other process on the one hand, and do not have dead ends on the other hand. Such processes are *safe* in the following sense. Abstract error traces π in systems where safe processes are abstracted away can be extended to concrete error traces in polynomial time, as spurious transitions in π can only be caused by safe processes. According to the definition of a safe process, the local states needed to resolve the spurious transition are always reachable.

We have implemented our approaches into the MCTA model checker [3]. The experimental evaluation shows the practical potential of these techniques on large and complex industrial case studies. The causal graph heuristic shows to be competitive with previously proposed distance functions in the context of directed model checking.

Moreover, the model reduction obtained by safe abstraction leads to strong performance gains when applicable, and needs only little computation time.

References

1. Malte Helmert. A planning heuristic based on causal graph analysis. In Shlomo Zilberstein, Jana Koehler, and Sven Koenig, editors, *Proceedings of the 14th International Conference on Automated Planning and Scheduling (ICAPS 2004)*, pages 161–170. AAAI Press, 2004.
2. Malte Helmert. The Fast Downward planning system. *Journal of Artificial Intelligence Research*, 26:191–246, 2006.
3. Sebastian Kupferschmid, Martin Wehrle, Bernhard Nebel, and Andreas Podelski. Faster than UPPAAL? In Aarti Gupta and Sharad Malik, editors, *Proceedings of the 20th International Conference on Computer Aided Verification (CAV 2008)*, volume 5123 of *LNCS*, pages 552–555. Springer-Verlag, 2008.
4. Martin Wehrle and Malte Helmert. The causal graph revisited for directed model checking. In Jens Palsberg and Zhendong Su, editors, *Proceedings of the 16th International Symposium on Static Analysis (SAS 2009)*, volume 5673 of *LNCS*, pages 86–101. Springer-Verlag, 2009.