Partial-Order Reduction in the Weak Modal Mu-Calculus*

Y.S. Ramakrishna and Scott A. Smolka

Department of Computer Science
SUNY at Stony Brook
Stony Brook, NY 11794–4400, USA

Abstract. We present a partial-order reduction technique for local model checking of hierarchical networks of labeled transition systems in the weak modal mu-calculus. We have implemented our technique in the Concurrency Factory specification and verification environment; experimental results show that partial-order reduction can be highly effective in combating state explosion in modal mu-calculus model checking.

1 Introduction

Model checking [CE81, QS82, CES86] is a verification technique aimed at determining whether a system specification possesses a property expressed as a temporal logic formula. Model checking has enjoyed wide success in verifying, or finding design errors in, real-life systems. An interesting account of a number of these success stories can be found in [CW96].

Despite these successes, many applications lie beyond the reach of today's generation of model checkers due to the state explosion problem. State explosion occurs when a system specification gives rise to an excessively large state space. This problem is particularly compelling in the case of concurrent systems, where a system of n concurrent processes, each with a local state space of size k, can potentially generate a global state space of size \( k^n \). Somewhat mitigating the problem is the fact that, in general, the entire space need not be reachable, since interactions between individual processes may rule out certain evolutions.

Even when the size of the reachable state space is formidable, local model checking [SW91] may allow a property to be established without having to explore this state space in its entirety. Nonetheless, the worst case remains exponential in n, and this is illustrated by the simple network of 2n processes depicted in Figure 1. Now consider the formula \( \nu X. [a] X \land [\langle \rangle]tt \land [\langle-a\rangle]ff \) of the weak modal mu-calculus, which states that the visible component of every computation of the system is an infinite sequence of a actions.

A naive algorithm for model checking this formula on the network of Figure 1 would result in the exploration of each of the \( 2^n \) reachable global states and \( (n+1) \cdot 2^{(n-1)} \) global transitions of the system. Most of these states result from interleaving the system's n \( \tau \)-transitions in all possible orders, where each \( \tau \)-transition is the result of a bi-party synchronization. Alternatively, one could exploit the fact that

* Research supported in part by NSF grants CCR–9505562, and AFOSR grants F49620-96-1-0508 and F49620-96-1-0087. Email: {ysr, sas}@cs.sunysb.edu
the \( \tau \)-transitions are "independent" of one another, and thereby avoid exploring redundant interleavings. This yields a method in which no more than \( n + 1 \) of the reachable states, and \( n + 1 \) of the global transitions need be explored. This observation provides the basis for the partial-order reduction technique we present in this paper.

Partial-order techniques were first introduced for checking simple properties such as absence of deadlock [Val88, GW93]. Subsequently, they were extended to more elaborate properties, in particular, to the model checking of linear-time temporal logic (LTL), without the next-time operator [Val92, Val93, GW94, Pel96]. Recently, several of the techniques for LTL were extended to CTL* [GKPP97, WW96], representing the first application of partial-order reduction to branching-time temporal logic model checking.

Here, we continue this trend by presenting a partial-order reduction technique for the weak modal mu-calculus, a very expressive branching-time temporal logic subsuming, for example, CTL and CTL* (without the next operator) in expressive power. The weak modal mu-calculus can be seen as a variant of the (strong) modal mu-calculus [Koz83]. The essential difference is that the strong modalities \([a]\) and \(<a>\) (meaning necessarily after \(a\) and possibly after \(a\), respectively), are replaced by their weak counterparts \([a]\) and \(<a>\). A weak modal mu-calculus formula of the form \([a]\phi\) means that after performing the observable action \(a\), preceded by and followed by zero or more unobservable \(\tau\) actions, formula \(\phi\) necessarily holds; similarly for \(<a>\phi\).

The main innovations of our partial-order reduction method for the weak modal mu-calculus are the following:

- It is the first partial-order technique to be proposed expressly for a modal mu-calculus, and hence the first technique applicable to event-based models such as labeled transition systems (LTSs). In contrast, LTL, CTL, and CTL* are interpreted over state-based models such as Kripke structures.
- To bridge the gap between partial-order methods for event-based and state-based models, we consider a hybrid model called doubly labeled transition systems (DTSs), and proposed originally in [DNV95]. A DTS has action-labeled transitions, like an LTS, and proposition-labeled states, like a Kripke struc-