Title: **Reexamining Two Results in Partial Order Reduction**

Author: Stephen F. Siegel

Kind: Technical Report UD-CIS-2011/06

Verified Software Laboratory
Department of Computer and Information Sciences
University of Delaware
Newark DE 19716
USA
http://vsl.cis.udel.edu

REEXAMINING TWO RESULTS IN PARTIAL ORDER REDUCTION

STEPHEN F. SIEGEL

Abstract. This paper reexamines two results dealing with ample-set-based Partial Order Reduction (POR) for explicit-state model checking. The first is a theorem asserting that POR and "on-the-fly" model checking can be safely combined. It is shown that the proof of this theorem contains a gap, though I am not aware of a counterexample to the theorem itself. The second result asserts that a specific relation between the reduced and full state spaces is a visible simulation. This result is incorrect: the posited relation is not a simulation, and a counterexample is given.

1. Combing POR and On-the-fly Model Checking

The basic automata-theoretic model checking algorithm involves the search for reachable acceptance cycles in the product of an automaton representing the Kripke structure and a Büchi automaton corresponding to $\neg\phi$. This search can take place *on the fly*, i.e., without first constructing the Kripke structure. An algorithm combining the on-the-fly approach with (invisibility-based) ample-set POR is presented in [2]; it is similar to the algorithm implemented in Spin [1].

Theorem 4.2 of [2] asserts that partial order reduction can be safely combined with on-the-fly model checking, but the proof contains a gap in the claim "It is easy to see that $L(\mathcal{A}') = L(G') \cap L(\mathcal{B})$" (p. 58). It is easy to see that the left-hand side is contained in the right, but the reverse is not clear.

To see why it is not clear, recall that, using the notation of [2], $\mathcal{A}'$ is the subgraph of G' consisting of all nodes $\langle x, y\rangle$ for which $y < n$. Suppose $\lambda_0\lambda_1\cdots \in L(G')\cap L(\mathcal{B})$, where $\lambda_i \in 2^P$. The fact that this string is in $L(G')$ means there is some path π

$$\langle x_0, y_0\rangle \overset{\langle\alpha_0,\zeta_0\rangle}{\to} \langle x_1, y_1\rangle \overset{\langle\alpha_1,\zeta_1\rangle}{\to} \cdots$$

in G' such that $L(x_i) = \lambda_i$ $(i \geq 0)$. Here x_i is a state in the program, $0 \leq y_i \leq n$, α_i is an operation in the program, and ζ_i is either a transition in $\mathcal{B}$ or a special symbol to denote there is no transition labeled λ_i departing from state y_i in $\mathcal{B}$; in this last case $y_j = n$ for all $j > i$.

One must show there is a path in $\mathcal{A}'$ generating the same string $\lambda_0\lambda_1\cdots$. This would obviously hold if we knew π was a path in A'. However, this does not have to be the case, because $\mathcal{B}$ may be a nondeterministic Büchi automaton. That is, it is possible that $\lambda_0\lambda_1\cdots$ is in $L(\mathcal{B})$ but nevertheless there is some i such that there is no transition labeled λ_i departing from y_i, because there are two different paths in B that generate the same prefix $\lambda_0\cdots\lambda_{i-1}$ but end in two different states, one of which has an outgoing λ_i transition and one of which does not.

This material is based upon work supported by the National Science Foundation under Grant Nos. CCF-0541035, CCF-0733035, and CCF-0953210.

Note that you cannot assume $\mathcal{B}$ is deterministic since for Büchi automata there are nondeterministic automata that have no equivalent deterministic automaton.

I am not aware of any counterexample to [2, Thm. 4.2], but I also do not see how to fill the gap in the proof.

2. Forming Paths and a Visible Simulation

Theorem 5.12 of [3] asserts that the "*forming path*" [3, Def. 5.6] relation from the reduced sub-state space to the full state space is a "*visible simulation*" [3, Def. 5.5]. That result would provide a much simpler proof of the main theorem of this paper. However, [3, Thm. 5.12] is incorrect.

A counterexample with 2 processes, P_0 and P_1, can be constructed as follows. P_0 has 3 states (0, 1, and 2), and two transitions $0 \xrightarrow{\alpha} 1$ and $0 \xrightarrow{\beta} 2$. P_1 has two states (0 and 1) and one transition $0 \xrightarrow{\gamma} 1$. The dependence relation consists of only (α, β) (i.e., there are no dependencies between the two processes). Assume α and β are invisible, and γ is visible. The initial state is $s_0 = (0, 0)$. The full state space has 6 states.

At s_0, all 3 transitions are enabled. For the ample set at s_0, take the set $S = \{\alpha, \beta\}$. This satisfies all the requirements for an ample set, in particular it satisfies condition **C1** of [3, Sec. 4.1], which requires that for every path in the full state space starting from s_0, a transition that is dependent on some transition in the ample set cannot appear before a transition from the ample set. The reduced structure therefore has two transitions emanating from s_0. For all other states the ample sets are full. The reduced state space has 5 states: all states in the full space except $(0, 1)$.

The definition of a *forming path* [3, Def. 5.6] $s_0 \xrightarrow{a_0} \cdots$ requires that a_0 be invisible (note there is a typo in the text: s_i should presumably be a_i), and that the *singleton set* $\{a_0\}$ satisfies condition **C1** from s_0, i.e., that nothing dependent on a_0 can occur without a_0 occurring first. The singleton set $\{\alpha\}$ does not satisfy the condition since β is dependent on α and β can occur before α. Similarly, $\{\beta\}$ does not satisfy the condition. Neither does $\{\gamma\}$, since it is visible. So there is no forming path departing from the initial state, other than the trivial path of length 0. There is also no forming path from the state $(0, 1)$, by the same reasoning. So there are no forming paths at all, other than the trivial paths of length 0. The forming relation therefore consists of all pairs (s, s) where s is in the reduced space, i.e., all (s, s) except when $s = (0, 1)$.

In particular, [3, Lem. 5.11] is false for the state s_0: there is no forming path from s_0 to a fully-expanded state.

This also means the forming path relation from the full space to the reduced space is not a visible simulation. For example, consider the edge $s_0 \xrightarrow{\gamma} t$, where $t = (0, 1)$. If the relation is a visible simulation there must exist a path in the reduced space from some state $s' = s_0$ to $t' = t$ (given that the forming relation is the identity), but this is impossible since t is not in the reduced space. There may be a visible simulation in this case but it is not the one defined by forming paths.

References

[1] G. J. Holzmann and D. Peled. An improvement in formal verification. In D. Hogrefe and S. Leue, editors, *Proceedings of the 7th IFIP WG6.1 Intl. Conference on Formal Description*

Techniques (Forte '94), volume 6 of *IFIP Conference Proceedings*, pages 197–211. Chapman & Hall, 1995.

[2] D. Peled. Combining partial order reductions with on-the-fly model-checking. *Formal Methods in System Design*, 8(1):39–64, Jan. 1996.

[3] D. A. Peled. Partial order reduction: linear and branching temporal logics and process algebras. In D. A. Peled, V. R. Pratt, and G. J. Holzmann, editors, *Partial Order Methods in Verification: Workshop on Partial Order Methods in Verification, July 24–26, 1996, Princeton University*, volume 29 of *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, pages 233–258. American Mathematical Society, 1997.

The Verified Software Laboratory, Department of Computer and Information Sciences, University of Delaware, Newark, DE 19716, USA

E-mail address: siegel@cis.udel.edu