Symmetry Reduction for Probabilistic Systems

Alastair F. Donaldson, Alice Miller
Department of Computing Science
University of Glasgow, Scotland
{ally,alice}@dcs.gla.ac.uk

1 Introduction

Symmetry reduction techniques have been quite successful in combatting the state-space explosion problem for temporal logic model checking [2, 3]. Recently, there has been a lot of interest in using model checkers to verify properties of probabilistic systems. We describe work in progress in extending symmetry reduction techniques to apply to discrete time Markov chains and Markov decision processes, and present preliminary results implementing symmetry reduction for the PRISM model checker [6].

2 Symmetry for DTMCs and MDPs

An automorphism of a Kripke structure M is a permutation of the states of M which preserves the transition relation. We have extended this definition to apply to DTMCs and MDPs. Informally, an automorphism of a DTMC $\mathcal{D}$ is a permutation of the states of $\mathcal{D}$ which preserves the probability of making a transition between states. An automorphism of a MDP $\mathcal{M}$ is pair of permutations σ, τ, where σ permutes the states of $\mathcal{M}$, and τ permutes the actions. Any pair (σ, τ) must satisfy the following: for any states s, t, if action α may be taken from s resulting in a probability distribution μ, then action $\tau(\alpha)$ may be taken from $\sigma(s)$ resulting in probability distribution μ' such that $\mu(t) = \mu'(\sigma(t))$.

It can be shown that the set of all automorphisms of a DTMC forms a group under composition of mappings (similarly for MDPs). Any group of automorphisms acting on a DTMC $\mathcal{D}$ induces an equivalence $\sim$, say, on the states of $\mathcal{D}$ which is a probabilistic bisimulation on $\mathcal{D}$ if the labelling of states is restricted to propositions which are *invariant* under the group. Similarly, any group of automorphisms acting on an MDP $\mathcal{M}$ induces equivalences $\sim_S$ and $\sim_{Act}$, say, on the states and actions of $\mathcal{M}$ respectively. The equivalence $\sim_S$ is a probabilistic bisimulation on $\mathcal{M}$ (restricted to invariant propositions) at a level of abstraction where actions which are equivalent under $\sim_{Act}$ are regarded as the same.

In both cases, these bisimulations allow the definition of an appropriate quotient structure with respect to the group G. Given a $pCTL^*$ formula ϕ which is invariant under G, ϕ can be safely checked over the (generally smaller) quotient DTMC/MDP. For details of probabilistic bisimulations and invariance groups see [1, 4] and [2] respectively.

3 Implementing symmetry reduction for PRISM

Symbolic model checking has been shown not to be directly compatible with symmetry reduction over a quotient structure, due to the prohibitively large BDD required to compute representatives of states [2]. An alternative approach to exploiting symmetry in symbolic model checking, for fully symmetric programs, involves translation of the source program for a model into a *generic* program [3]. The state-space associated with the generic program is isomorphic to the quotient structure with respect to symmetry, but the generic program can be model checked directly, without using a BDD to compute state representatives.

# processes	time (orig)	nodes (orig)	time (generic)	nodes (generic)
10	6.2s	27,957	3.0s	17,367
12	13.3s	40,687	3.7s	22,683
14	21.0s	55,721	5.0s	28,158
16	31.6s	73,059	7.8s	39,443
18	53.1s	92,701	10.7s	46,110
20	1m34s	114,647	13.6s	52,997
22	2m22s	138,897	17.9s	60,036

Table 1: Time for construction and number of MTBDD nodes required for mutex example. Experiments performed on a PC with a 2.4GHz Intel Xenon processor.

We have extended this approach to apply to the PRISM model checker. We have implemented a tool which translates models written in a well defined subset of the PRISM language, which we call *symmetric* PRISM, to a generic form which can be model checked directly. Our approach applies to *nondeterministic* PRISM programs, for which the associated model is a MDP. Given a symmetric PRISM program and the generic program into which it is translated, the MDP associated with the generic program is isomorphic to the quotient MDP for the symmetric program with respect to its group of automorphisms. Symmetric properties for the original program can be also be translated into a generic form for model checking over the generic program.

Preliminary experiments for a randomized mutual exclusion protocol [5] are shown in Table 1. As the number of components in the model grows, the MDP for the generic program requires significantly fewer MTBDD nodes than the original, and model building is much faster.

References

[1] C. Baier, J. Katoen, H. Hermanns, and V. Wolf. Comparative Branching-Time Semantics for Markov Chains. In *CONCUR'03*, LNCS 2761, pages 482–497. Springer, 2003.

[2] E.M. Clarke, R. Enders, T. Filkhorn, and S. Jha. Exploiting Symmetry in Temporal Logic Model Checking. *Formal Methods in System Design*, 9(1–2):77–104, 1996.

[3] E. A. Emerson and T. Wahl. On Combining Symmetry Reduction and Symbolic Representation for Efficient Model Checking. In *CHARME'03*, LNCS 2860, pages 216–230. Springer, 2003.

[4] R. Givan, T. Dean, and M. Greig. Equivalence notions and model minimization in Markov decision processes. *Artificial Intelligence*, 147(1–2):163–223, 2003.

[5] A. Pnueli and L. Zuck. Verification of Multiprocess Probabilistic Protocols *Distributed Computing*, 1(1):53-72, 1986.

[6] J. Rutten, M. Kwaitowska, G. Norman, and D. Parker. *Mathematical Techniques for Analysing Concurrent and Probabilistic Systems*, volume 23 of *CRM Monograph Series*. American Mathematical Society, Centre de Recherches Mathématiques, Université de Montréal, 2004.