Virtual Symmetry Reduction

E. Allen Emerson and John W. Havlicek*
Department of Computer Sciences and
Computer Engineering Research Center
The University of Texas at Austin
emerson@cs.utexas.edu, havlicek@cs.utexas.edu

Richard J. Trefler
AT&T Labs–Research, USA
trefler@research.att.com

Abstract

We provide a general method for ameliorating state explosion via symmetry reduction in certain asymmetric systems, such as systems with many similar, but not identical, processes. The method applies to systems whose structures (i.e., state transition graphs) have more state symmetries than arc symmetries. We introduce a new notion of "virtual symmetry" that strictly subsumes earlier notions of "rough symmetry" and "near symmetry" [ET99]. Virtual symmetry is the most general condition under which the structure of a system is naturally bisimilar to its quotient by a group of state symmetries.

We give several example systems exhibiting virtual symmetry that are not amenable to symmetry reduction by earlier techniques: a one-lane bridge system, where the direction with priority for crossing changes dynamically; an abstract system with asymmetric communication network; and a system with asymmetric resource sharing motivated from the drinking philosophers problem. These examples show that virtual symmetry reduction applies to a significantly broader class of asymmetric systems than could be handled before.

1. Introduction

Model checking [CE81, QS82] is an algorithmic method for checking whether a finite-state system satisfies (i.e., models) a temporal logic formula. The system is represented by a finite structure (i.e., state transition graph). Standard model-checking algorithms have complexities that are efficient in their dependence on the size of the structure (linear, for example, in the case of CTL model checking). Nevertheless, in practice, it is the contribution from the structure size that dominates the computational cost (cf. [LP85]). Furthermore, the number of states of the structure may be exponentially larger than the size of the textual description of the system. This blowup is referred to as *state explosion*.

For systems comprising many identical or isomorphic components, the structure may be large but may also exhibit considerable symmetry. The symmetry can be expressed through the action of a group of graph automorphisms of the structure. For example, a system that is the parallel composition of n identical processes with complete communication network has a structure that admits an automorphism for each of the $n!$ permutations of the processes.

Symmetry of a structure often constitutes redundancy for the purpose of model checking a temporal logic formula. Symmetry reduction (cf. [JR91, ID96, ES96, CE+96, HI+95, MAV96, ES97, GS97, ET98, AHI98]) is an abstraction technique in which a symmetry-reduced quotient M/G is formed by identifying states of the structure M that are related by elements of the group G. Under the quotient relation, M and M/G are bisimilar as labelled digraphs for any labelling that is invariant under the action of G. For suitably symmetric temporal logic formulas, model checking can be performed on M/G rather than on the original

*These authors were supported in part by NSF grant CCR-980-4736, Semiconductor Research Corporation contract 99-TJ-685, and Texas Advanced Research Program project 003658-0650-1999.

0-7695-0725-5/00 $10.00 © 2000 IEEE

structure M.[1] Since M/G may be exponentially smaller than M, symmetry reduction can significantly ameliorate state explosion. In any case, maximum compression is obtained by taking G to capture as many symmetries of M as possible.

The technique of symmetry reduction is limited by the genuine symmetry of the structure M. For example, if a system of identical processes has communication network that is a ring rather than complete, then the symmetries of M may be restricted to a cyclic or dihedral group. In this case, the symmetry reduction can produce at most a saving that is linear in the number of processes. As another example, consider a system in which otherwise identical processes are partitioned into two groups, one of which takes priority in certain transitions. If there are m processes in the first group and n in the second, then M may have a genuine symmetry group of order $m!n!$ rather than $(m+n)!$. Yet another source of asymmetry is non-uniform access by processes to various shared resources.

These kinds of asymmetries are exhibited by structures whose group of state symmetries is larger than its group of arc symmetries. The asymmetry arises because arcs are missing from the structure. For many interesting temporal logic formulas, asymmetries of these kinds are irrelevant for model checking. We introduce a new condition, *virtual symmetry*, under which a structure M can be reduced by a group of state symmetries that may be larger than its genuine symmetry group. Virtual symmetry is the most general condition under which a structure with a group of state symmetries is bisimilar to its group quotient via the standard quotient relation. The group quotient is an abstract structure whose states are equivalence classes of original states related by the action of the group. The quotient relation is the "natural" one relating a state to its equivalence class. In this sense, the bisimulation is "natural." The bisimulation is also label-preserving for any labelling that is invariant under the action of the group.

We also introduce *strong virtual symmetry*, a condition that implies virtual symmetry and that is equivalent to virtual symmetry for asynchronous structures under the group of all permutations of the processes. Strong virtual symmetry strictly subsumes the earlier notions of "rough symmetry" [ET99] and symmetry with respect to a group of "near automorphisms" [ET99]. Informally, rough symmetry accommodates asymmetry arising from static priorities for the processes, while strong virtual symmetry can also accommodate dynamic priorities. Symmetry under a group of near automorphisms requires that an asymmetric arc (i.e., an arc of the structure that can be driven by a state symmetry to a missing arc) initiate only from a state that is itself highly symmetric. Strong virtual symmetry is defined by more liberal criteria than these earlier notions, and so it applies to a broader class of asymmetric systems.

We give several example systems exhibiting virtual symmetry. One is a solution of the readers-writers problem with writer priority. Because of the static writer priority, this system is also roughly symmetric. To distinguish (strong) virtual symmetry from rough symmetry and from symmetry with respect to a group of near automorphisms, we give an example of a one-lane bridge system, where the direction with priority for crossing changes dynamically. An asymmetric communication network is illustrated in a simple, abstract example in which pairs of processes begin and end communication synchronously. A further example, exhibiting asymmetric sharing of resources, is motivated from the drinking philosophers problem. A common feature of these examples is that asymmetric arcs are, in an intuitive sense, "widely enabled." The systems include reasonable limits (denoted λ) that ensure the existence of the required asymmetric arcs.

We also give a counting condition on the number of missing arcs. The condition provides a convenient criterion for determining if a system is strongly virtually symmetric. For asynchronous structures under the group of all permutations of the processes, a simplifying assumption reduces the condition to a bound at each state on the number of missing arcs initiating from the state. The simplifying assumption requires that all asymmetric arcs arise from a *single* local transition. Apart from the asymmetric communication network, which has synchronized transitions, each of the examples mentioned above satisfies the simplifying assumption, and its strong virtual symmetry can be demonstrated easily by counting missing arcs.

An appendix provides background material on group actions as well as the lemmas and proofs omitted from the main text.

2. Preliminaries

2.1. Conventions

Let X and Y be sets. The cardinality of X is denoted $|X|$. $Sym(X)$ denotes the group of all permutations (i.e., bijections) of X. Y^X denotes the set of functions with domain X and codomain Y. If $R \subseteq X \times Y$, then

$$R^{-1} = \{(y,x) \in Y \times X \,:\, (x,y) \in R\} \ .$$

Let G be a group that acts on X. If $Y \subseteq X$, then

$$Aut(Y;G) = \{g \in G \,:\, gY = Y\} \ .$$

$Aut(Y;G)$ is the largest subgroup of G whose elements leave Y set-wise invariant. For $x \in X$, we write $Aut(x;G)$

[1] Alternatively, one may form the product of an annotated quotient with an automaton for the complement of the temporal logic formula and check the resulting structure for non-emptiness [ES97, GS97].

0-7695-0725-5/00 $10.00 © 2000 IEEE

to mean $Aut(\{x\};G)$. When the group is clear from context, we may write $Aut(Y)$ in place of $Aut(Y;G)$.

2.2. Structures and simulations

A structure is a pair (S,R), where S is a set, the *state set* of the structure, and $R \subseteq S \times S$, the *arc set* or *transition relation* of the structure. We use the notation $s \to t$ interchangeably with (s,t) for an arc.

NOTATION: If M is a structure, then S_M denotes the state set of M and R_M denotes the transition relation of M. $\square$

Let M, N be structures. A function $f\colon S_M \to S_N$ is a *homomorphism from M to N*, written $f\colon M \to N$, if, for every $s \to t \in R_M$, $f(s) \to f(t) \in R_N$. A relation $\mathcal{B} \subseteq S_M \times S_N$ is a *simulation* of M by N if, for any $(s,s') \in \mathcal{B}$ and any $s \to t \in R_M$, there exists $t' \in S_N$ such that $(t,t') \in \mathcal{B}$ and $s' \to t' \in R_N$. For example, if f is a homomorphism from M to N, then f (viewed as a subset of $S_M \times S_N$) is a simulation of M by N. If $\mathcal{B}$ is a simulation of M by N and $\mathcal{B}^{-1}$ is a simulation of N by M, then $\mathcal{B}$ and $\mathcal{B}^{-1}$ are *bisimulations* between M and N.

2.3. Indexed and asynchronous structures

For virtual symmetry reduction, many structures of interest arise from parallel composition of similar processes. A state of such a structure is an assignment of local states to each of the processes.[2]

To be precise, let $\mathcal{I}$ be a finite set of indexes, to be thought of as process identifiers, and let $\mathcal{L}$ be a set of local states. A function $s \in \mathcal{L}^{\mathcal{I}}$ represents the global state in which, for each $i \in \mathcal{I}$, the local state of process i is $s(i)$. An *$\mathcal{L}^{\mathcal{I}}$-structure* is a structure whose state set is a subset of $\mathcal{L}^{\mathcal{I}}$. If $L \subseteq \mathcal{L}$, then we define $\#L$ to be the function $\mathcal{L}^{\mathcal{I}} \to [0:|\mathcal{I}|]$ that maps $s \mapsto |s^{-1}(L)|$.[3] Thus, $\#L(s)$ is the number of processes that, in global state s, are assigned a local state from the set L. For $x \in \mathcal{L}$, we write $\#x$ for $\#\{x\}$. If $\mathcal{J} \subseteq \mathcal{I}$, then we define $\#(\mathcal{J},L)$ to be the function $\mathcal{L}^{\mathcal{I}} \to [0:|\mathcal{J}|]$ that maps $s \mapsto |\mathcal{J} \cap s^{-1}(L)|$. $\#(\mathcal{J},L)(s)$ is the number of processes in $\mathcal{J}$ that, in global state s, are assigned a local state from the set L.

Notice that $Sym(\mathcal{I})$ acts on $\mathcal{L}^{\mathcal{I}}$ by

$$\pi s = s \circ \pi^{-1} \qquad (*)$$

for $\pi \in Sym(\mathcal{I})$ and $s \in \mathcal{L}^{\mathcal{I}}$. If $X \subseteq \mathcal{L}^{\mathcal{I}}$ and $G \subseteq Aut(X; Sym(\mathcal{I}))$, then G acts on X according to $(*)$. Unless stated otherwise, $(*)$ will be the action understood for subgroups of $Sym(\mathcal{I})$ acting on subsets of $\mathcal{L}^{\mathcal{I}}$.

An *asynchronous $\mathcal{L}^{\mathcal{I}}$-structure* is a pair (S,R) such that $S \subseteq \mathcal{L}^{\mathcal{I}}$, $R \subseteq S \times \mathcal{I} \times S$, and, for every $(s,i,t) \in R$ and every $j \in \mathcal{I} - \{i\}$, $s(j) = t(j)$. By *asynchronous structure* we mean an asynchronous $\mathcal{L}^{\mathcal{I}}$-structure for some $\mathcal{L}$ and $\mathcal{I}$. A triple $(s,i,t) \in R$ is thought of as an arc from s to t with label i; it will also be written $s \xrightarrow{i} t$. An asynchronous structure determines an underlying structure by omitting the labels from the arcs.[4]

To define asynchronous structures, it is convenient to use a language of guarded local transitions. For our purposes, a *guard* is a predicate γ whose interpretation $[\gamma]$ is a subset of $\mathcal{I} \times \mathcal{L}^{\mathcal{I}}$. A *guarded local transition* is a pair $\gamma : x \to y$, where γ is a guard and $x, y \in \mathcal{L}$. The transition $\gamma : x \to y$ is enabled for process i in global state s provided $(i,s) \in [\gamma]$ and $s(i) = x$. If $\gamma : x \to y$ is enabled for i in s, and if t is defined by

$$t(j) = \begin{cases} s(j) & j \neq i \\ y & j = i \,, \end{cases}$$

then we say that $s \xrightarrow{i} t$ results from *firing* $\gamma : x \xrightarrow{i} y$ in global state s.

For $\mathcal{J} \subseteq \mathcal{I}$, it is a convenient abuse to understand $\mathcal{J}$ to denote the guard whose interpretation is $\mathcal{J} \times \mathcal{L}^{\mathcal{I}}$. Thus, $(i,s) \in [\mathcal{J}]$ if and only if $i \in \mathcal{J}$.

EXAMPLE 1: *Readers-writers with writer priority*. Let $\mathcal{I}$ be partitioned into the non-empty sets $\mathcal{R}$ and $\mathcal{W}$ of "readers" and "writers." Let $\mathcal{L} = \{N,T,C\}$. The intuitive meanings of the local states N, T, and C are, respectively, "non-trying," "trying," and "critical." We define an asynchronous $\mathcal{L}^{\mathcal{I}}$-structure, M, using guarded local transitions. S_M is the set of all states in $\mathcal{L}^{\mathcal{I}}$. The guarded local transitions are the following:

1. $\mathit{true} : N \to T$.
2. $\gamma : T \to C$, where
$$\gamma \equiv (\#C = 0) \wedge \big(\mathcal{R} \Rightarrow (\#(\mathcal{W},T) = 0)\big)\ .$$
3. $\mathit{true} : C \to N$.

Recall that $\mathcal{R}$ is interpreted to constrain the indexes which may fire. Informally, "$\mathcal{R} \Rightarrow (\#(\mathcal{W},T) = 0)$" means that if the firing process is a reader, then there is no writer in local state T. This conjunct of γ ensures writer priority in the local transition $T \to C$. $\square$

3. Virtual and Strong Virtual Symmetry

Let M be a structure, and let G be a group that acts on S_M (i.e., G is a group of state symmetries of M). There is

[2] For simplicity, we ignore shared variables.

[3] $s^{-1}(L) = \{i \in \mathcal{I}\colon s(i) \in L\}$, the pre-image of L under s.

[4] The asynchronous structure may have multiple self-loops on a single node, e.g. $s \xrightarrow{i} s$ and $s \xrightarrow{j} s$, that are collapsed to a single self-loop when passing to the underlying structure.

0-7695-0725-5/00 $10.00 © 2000 IEEE

an induced action of G on $S_M \times S_M$ defined by

$$g(s,t) = (gs, gt)$$

for $g \in G$ and $(s,t) \in S_M \times S_M$. We say that M is (*genuinely*) *symmetric with respect to* G if and only if, for every $s \to t \in R_M$ and every $g \in G$, $gs \to gt \in R_M$. Thus, M is genuinely symmetric with respect to G if and only if $G = Aut(R_M; G)$.

The *quotient structure* M/G is defined by

$$S_{M/G} = \{Gs \,:\, s \in S_M\}$$

and

$$R_{M/G} = \{Gs \to Gt \,:\, (\exists\, g, h \in G : gs \to ht \in R_M)\} \ .$$

Thus, the states of M/G are the G-orbits of S_M, and there is an arc in M/G from Gs to Gt if and only if there exists an arc of M whose initial state is in Gs and whose terminal state is in Gt. For computation, $S_{M/G}$ is typically identified with a transversal for the action of G on S_M.

There are two relations of particular interest in connection with the action of G on S_M. The first is the orbit relation

$$\mathcal{O} = \{(s, s') \in S_M \times S_M : Gs = Gs'\} \ .$$

The second is the quotient relation

$$\mathcal{Q} = \{(s, Gs) \,:\, s \in S_M\} \ .$$

Notice that $\mathcal{Q}$ is a homomorphism $M \to M/G$, hence $\mathcal{Q}$ is a simulation of M by M/G. [ES96, CE+96] proved that if M is genuinely symmetric with respect to G, then $\mathcal{Q}$ is a bisimulation between M and M/G.

Remark: $\mathcal{Q}$ is a "natural" relation between S_M and $S_{M/G}$ in the following sense: if $f\colon M \to N$ is a homomorphism of structures, where N also has G as a group of state symmetries, and if $f(gs) = gf(s)$ for every $g \in G$ and $s \in S_M$, then there is a unique homomorphism $(f/G)\colon M/G \to N/G$ such that $(f/G) \circ \mathcal{Q} = \mathcal{Q} \circ f$. □

Suppose that M is not genuinely symmetric with respect to G. Then there exists an arc $s \to t \in R_M$ and an element $g \in G$ such that $gs \to gt \notin R_M$. We refer to $s \to t$ as an *asymmetric arc* of M, and we say that $gs \to gt$ is *missing* from M. In this case, $\mathcal{Q}$ may or may not be a bisimulation between M and M/G. In Proposition 1 below, we show that $\mathcal{Q}$ is a bisimulation between M and M/G if and only if $\mathcal{O}$ is a bisimulation between M and the genuinely symmetric structure obtained from M by adding the missing arcs. Proposition 1 also shows that these conditions are equivalent to a simple third condition, which we take as the definition of virtual symmetry.

Define M^G, the *symmetrization of M by G*, according to

$$S_{M^G} = S_M$$

and

$$R_{M^G} = \{gs \to gt \,:\, g \in G \text{ and } s \to t \in R_M\} \ .$$

In other words, M^G is obtained from M by adding all the missing arcs. M^G is the smallest superstructure of M that is genuinely symmetric with respect to G.

Let M be an asynchronous $\mathcal{L}^{\mathcal{I}}$-structure, and let G be a subgroup of $Aut(S_M; Sym(\mathcal{I}))$, acting according to $(*)$.[5] An asynchronous symmetrization can be arranged by letting

$$R_{M^G} = \{gs \xrightarrow{gi} gt \,:\, g \in G \text{ and } s \xrightarrow{i} t \in R_M\} \ .$$

In this case, the ordinary symmetrization of the $\mathcal{L}^{\mathcal{I}}$-structure underlying M is equal to the $\mathcal{L}^{\mathcal{I}}$-structure underlying the asynchronous symmetrization of M.

EXAMPLE 2: For the readers-writers of Example 1, the asynchronous symmetrized structure is obtained by replacing γ with $\gamma' \equiv (\#C = 0)$. □

Proposition 1: *Let M be a structure, and let G act on S_M. The following are equivalent:*

(1) *$\mathcal{Q}$ is a bisimulation between M and M/G.*

(2) *$\mathcal{O}$ is a bisimulation between M and M^G.*

(3) *For any $s \to t \in R_{M^G}$, there exists $g \in G$ such that $s \to gt \in R_M$.*

□

If M is an asynchronous structure, then Proposition 1 applies to the underlying structure. The result also applies to the original asynchronous structure by ignoring arc labels.

Definition: Let M be a structure, and let G act on S_M. M is *virtually symmetric* (*with respect to G*) if condition (3) of Proposition 1 is satisfied. M is *strongly virtually symmetric* (*with respect to G*) if, for any $s \to t \in R_{M^G}$, there exists $g \in Aut(s; G)$ such that $s \to gt \in R_M$. An asynchronous structure is (strongly) virtually symmetric if its underlying structure is (strongly) virtually symmetric. □

Remark: From Proposition 1, M is virtually symmetric with respect to G if and only if $\mathcal{Q}$ is a bisimulation between M and M/G. In this sense, virtual symmetry is the most general condition under which M is naturally bisimilar (i.e., bisimilar via $\mathcal{Q}$) to M/G. □

EXAMPLE 3: These simple examples illustrate the preceding definition. In each, $S_M = \{s, t, u\}$, and $G = \{1, \tau\}$, where 1 is the identity, $\tau^2 = 1$, and τ acts on S by fixing u and swapping s with t. In the figures, M is on the left, M^G is on the right, and the arcs of $R_{M^G} - R_M$ (i.e., the missing arcs) are dashed.

[5] This assumption ensures that, for $g \in G$ and $s \xrightarrow{i} t \in R_M$, $(gs)(j) = (gt)(j)$ for all $j \in \mathcal{I} - \{gi\}$.

0-7695-0725-5/00 $10.00 © 2000 IEEE

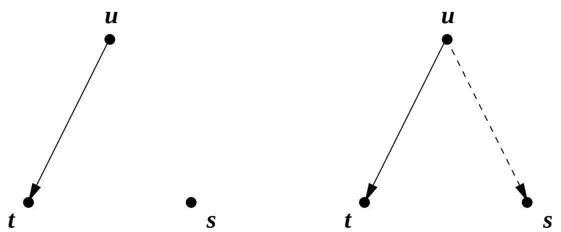

Figure 1. Illustration of Example 3(a). M **is strongly virtually symmetric with respect to** G**.**

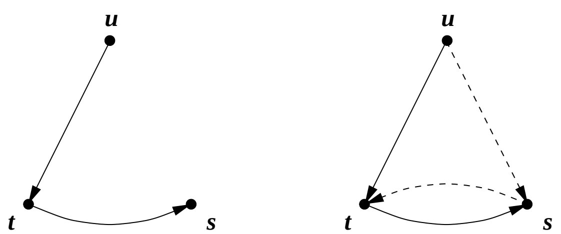

Figure 2. Illustration of Example 3(b). M **is not virtually symmetric with respect to** G**.**

(a) R_M has the single transition $u \to t$, and so R_{M^G} has the additional transition $u \to s$. See Figure 1. Since τ fixes u and drives $u \to s$ to $u \to t$, M is strongly virtually symmetric with respect to G.

(b) R_M has the transitions $u \to t$ and $t \to s$, and so R_{M^G} has the additional transitions $u \to s$ and $s \to t$. See Figure 2. There is no transition in R_M with s as initial state, so the condition of the definition of virtual symmetry fails for $s \to t$.

(c) R_M has the transitions $u \to t$, $t \to t$, $t \to s$, and $s \to s$. R_{M^G} has the additional transitions $u \to s$ and $s \to t$. See Figure 3. It is not difficult to check that M is virtually symmetric with respect to G. For example, for $s \to t \in R_{M^G}$, $s \to \tau t = s \to s \in R_M$. Since τ does not fix s, M is not strongly virtually symmetric.

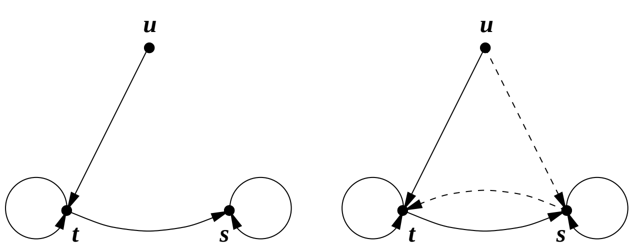

Figure 3. Illustration of Example 3(c). M **is virtually symmetric, but not strongly virtually symmetric, with respect to** G**.**

□

EXAMPLE 4: Returning to the readers-writers, it is easy to see that M is genuinely symmetric with respect to $Sym(\mathcal{R}) \times Sym(\mathcal{W})$, but, because of writer priority, M is not symmetric with respect to the action of the full group $Sym(\mathcal{I})$.

We check that M is strongly virtually symmetric with respect to $Sym(\mathcal{I})$. Recall that the asynchronous symmetrization results by replacing γ with $\gamma' \equiv (\#C = 0)$. Suppose that $s \xrightarrow{i} t \in R_{M^{Sym(\mathcal{I})}} - R_M$. The transition results from firing $\gamma' : T \xrightarrow{i} C$, and it follows that $(i, s) \in [\gamma'] - [\gamma]$ and $s(i) = T$. Therefore, $i \in \mathcal{R}$, yet $T \in s(\mathcal{W})$. Pick $j \in \mathcal{W}$ so that $s(j) = T$, and let $\pi \in Sym(\mathcal{I})$ be the permutation that swaps i with j and fixes all other indexes. Plainly $\pi \in Aut(s)$. Notice that $(j, s) \in [\gamma]$, and so $s \xrightarrow{j} \pi t$ is obtained by firing $\gamma : T \xrightarrow{j} C$ in s. Therefore, $s \xrightarrow{j} \pi t \in R_M$. □

The next proposition shows that virtual symmetry and strong virtual symmetry are equivalent for asynchronous structures under the group of all permutations of the processes.

Proposition 2: *Let M be an asynchronous $\mathcal{L}^{\mathcal{I}}$-structure, and let $Sym(\mathcal{I})$ act on S_M according to $(*)$. M is virtually symmetric with respect to $Sym(\mathcal{I})$ if and only if it is strongly virtually symmetric with respect to $Sym(\mathcal{I})$.* □

4. Relation to Prior Work

Prior work [ET99] introduced several notions of near symmetry: symmetry under a group of "near automorphisms" and "rough symmetry." Each of these notions yields a group quotient that is bisimilar via $\mathcal{Q}$ to the original structure. Thus, Proposition 1 implies that each is subsumed by virtual symmetry. In this section, we show that these notions are strictly subsumed by strong virtual symmetry.

Definition [ET99]: Let M be an $\mathcal{L}^{\mathcal{I}}$-structure, and let $Sym(\mathcal{I})$ act on $\mathcal{L}^{\mathcal{I}}$ according to $(*)$. An element $\pi \in Aut(S_M; Sym(\mathcal{I}))$ is a *near automorphism* of M if, for every $s \to t \in R_M$, either

1. $\pi s \to \pi t \in R_M$ or

2. $Aut(S_M; Sym(\mathcal{I})) \subseteq Aut(s; Sym(\mathcal{I}))$.

□

0-7695-0725-5/00 $10.00 © 2000 IEEE

Proposition 3: *Let M be an $\mathcal{L}^{\mathcal{I}}$-structure and let G be a group of near automorphisms of M. Then M is strongly virtually symmetric with respect to G.* □

Definition [ET99]: Let $\mathcal{I}$ be totally ordered, let M be an asynchronous $\mathcal{L}^{\mathcal{I}}$-structure, let $Sym(\mathcal{I})$ act on $\mathcal{L}^{\mathcal{I}}$ according to $(*)$, and let G be a subgroup of $Aut(S_M; Sym(\mathcal{I}))$. M is *roughly symmetric with respect to the order on $\mathcal{I}$ and the group G* if, for any $i \in \mathcal{I}$, for any $s \xrightarrow{i} t \in R_M$, and for any $s' \in Gs$, there exists $\pi \in G$ such that

1. $\pi s = s'$,
2. $\pi i = \max\{j' : s(i) = s'(j')\}$, and
3. $\pi s \xrightarrow{\pi i} \pi t \in R_M$.

□

EXAMPLE 5: Let M be the structure for readers-writers with writer priority. Choose a total order of $\mathcal{I}$ so that $i \in \mathcal{R}$ and $j \in \mathcal{W}$ imply $i < j$, and let $G = Sym(\mathcal{I})$. The argument of Example 4 that M is strongly virtually symmetric can be modified to show that M is roughly symmetric with respect to this order on $\mathcal{I}$ and the group G. (See [ET99].) □

Proposition 4: *Let M be an asynchronous $\mathcal{L}^{\mathcal{I}}$-structure that is roughly symmetric with respect to some ordering of $\mathcal{I}$ and the subgroup G of $Aut(S_M; Sym(\mathcal{I}))$. Then M is strongly virtually symmetric with respect to G.* □

The remainder of this section presents an example showing that strong virtual symmetry strictly subsumes rough symmetry and symmetry with respect to a group of near automorphisms. The example illustrates dynamically varying priorities for a critical shared resource. The processes are statically partitioned into two blocks, and only processes of a single block are allowed to be trying for or in the critical section at one time. The processes in the block with access have priority, but which block has access may change over time. In this sense, the example is like a one-lane bridge, where the blocks correspond to directions of travel. The symmetrized structure allows the partition into blocks to change dynamically, something like roundhouse switching of rail connections.

EXAMPLE 6: Let $\mathcal{I}$ be partitioned into the sets $\mathcal{I}_0$ and $\mathcal{I}_1$, and assume that $|\mathcal{I}_0| = |\mathcal{I}_1| = \lambda > 1$. Let $\mathcal{L} = \{N, T, C\}$, and let $S_M = \mathcal{L}^{\mathcal{I}}$. For $a \in \{0, 1\}$, let

$$P_a \equiv \left(\#\{T, C\} = \#(\mathcal{I}_a, \{T, C\})\right) ,$$

and let

$$good \equiv P_0 \vee P_1 .$$

A state satisfies *good* if and only if all processes whose local state is T or C come from the same partition of $\mathcal{I}$.

Define R_M by the following guarded local transitions:

1. $(\#\{T, C\} < \lambda) \wedge \gamma : N \to T$, where
$$\gamma \equiv \bigvee_{a=0}^{1} \left(\mathcal{I}_a \wedge (good \Rightarrow P_a)\right) .$$
2. $\#C = 0 : T \to C$.
3. $true : C \to N$.

If a state satisfies *good* and has at least one process in local state T or C, then one of the partitions of $\mathcal{I}$, say $\mathcal{I}_a$, contains all processes whose local state is T or C. In such a state, γ gives priority for the transition $N \to T$ to non-trying processes in $\mathcal{I}_a$.

The group $G = Sym(\mathcal{I})$ acts on S_M, but, because of the priority imposed by γ, M is not symmetric with respect to G. The symmetrization M^G is obtained by replacing γ with *true*.

We check that M is strongly virtually symmetric with respect to G. Let $s \xrightarrow{p} t \in R_{M^G} - R_M$, and let $p \in \mathcal{I}_a$. Then this transition is of type 1, $s \models \#\{T, C\} < \lambda$, $s \models good$, yet $s \not\models P_a$. Since $s \models good$, $s \models P_b$, where $b \neq a$. For any process $q \in \mathcal{I}_b$, $(q, s) \in [\gamma]$, so it suffices to show that some process of $\mathcal{I}_b$ has local state N. This follows because

$$\#\{T, C\}(s) < \lambda = |\mathcal{I}_b| .$$

Next, we check that M is not roughly symmetric with respect to G for any total ordering of $\mathcal{I}$. Pick $a \in \{0, 1\}$ so that $\mathcal{I}_a$ contains the largest element, p, of $\mathcal{I}$. Let b be the other element of $\{0, 1\}$. Let q, r be distinct indexes in $\mathcal{I}_b$ (here we use $\lambda > 1$). Let s be a state so that $s(q) = T$ and $s(i) = N$ for all i distinct from q. Then R_M has a transition $s \xrightarrow{r} t$ in which r changes local state from N to T. However, there is no element π of G such that $\pi s = s$, $\pi r = p$, and $s \xrightarrow{\pi r} \pi t$ is a transition of R_M. Indeed, no index in $\mathcal{I}_a$ can fire $N \to T$ in state s to produce a transition of R_M because $s(q) = T$.

Finally, notice that R_M contains a transition $s \xrightarrow{i} t$ of type 1, where $i \in \mathcal{I}_0$, $s(j) = T$ for some $j \in \mathcal{I}_0 - \{i\}$, and $s(k) = N$ for all $k \neq j$. Any element of $Aut(s)$ must fix j, so $Aut(s)$ is not equal to G. Also, if π swaps i with i', where $i' \in \mathcal{I}_1$, and fixes all other indexes, then $\pi s \to \pi t \notin R_M$. Therefore, G is not a group of near automorphisms of M. □

5. Further Examples

The following abstract example addresses asymmetry of a communication network. A process can communicate with at most one other process at a time, and communication between two processes is established and terminated synchronously.

EXAMPLE 7: Let $\mathcal{N}$ be the graph representing the communication network of a system whose set of processes is $\mathcal{I}$. Specifically, $\mathcal{N}$ has node set $\mathcal{I}$, and, for $i, j \in \mathcal{I}$, there is an edge between i and j in $\mathcal{N}$ if and only if (1) $i \neq j$ and (2) there is a channel between i and j in the network.

Let λ be a positive integer such that any matching in $\mathcal{N}$ of size less than λ can be extended to a matching of size λ. We think of λ as a *load limit* for the communication network.

A global state of M is a matching in the complete graph on $\mathcal{I}$. The presence of the edge $\{i, j\}$ in the matching signifies that processes i and j are communicating in the state. A global state is *good* if it is a matching in $\mathcal{N}$. If s, t are global states, there is a transition $s \to t$ if and only if one of the following two conditions is satisfied:

1. t is obtained from s by adding a single edge, $|t| \leq \lambda$, and if $s \models good$then $t \models good$

2. t is obtained from s by deleting a single edge.

A transition of type 1 represents synchronous establishment of communication between the processes of the edge added to s to obtain t. A transition of type 2 represents synchronous termination of communication between the processes of the edge deleted from s to obtain t.

The group $G = Sym(\mathcal{I})$ acts on S_M as follows: for $\pi \in G$,

$$\pi\{\{i_1, j_1\}, \ldots, \{i_r, j_r\}\} = \{\{\pi(i_1), \pi(j_1)\}, \ldots, \{\pi(i_r), \pi(j_r)\}\} .$$

M^G is obtained by omitting the requirement "if $s \models good$ then $t \models good$" from condition 1.

We check that M is strongly virtually symmetric with respect to G. Suppose $s \to t$ is a transition in $R_{M^G} - R_M$. Then the transition is of type 1, the size of s is less than λ, $s \models good$, but $t \not\models good$. Let $\{i, j\}$ be the edge added to s to obtain t. Then $\{i, j\}$ is not an edge of $\mathcal{N}$. Since the size of s is less than λ, s can be extended to a matching u in $\mathcal{N}$ of size λ. Pick $\{i', j'\}$ an edge in $u - s$. Let π be a permutation that interchanges $\{i, j\}$ with $\{i', j'\}$ and that fixes all other indexes. It follows that $\pi s = s$ and $s \to \pi t \in R_M$. $\square$

The next example illustrates asymmetric sharing of resources. It is motivated from the drinking philosophers problem [CM84].

EXAMPLE 8: Let $\mathcal{R}$ be a set of critical resources shared among the processes of $\mathcal{I}$. Let $can\_use \subseteq \mathcal{I} \times \mathcal{R}$ be the relation describing resource sharing: $i \ can\_use \ r$ if and only if process i shares resource r. For $r \in \mathcal{R}$, let

$$users\_of(r) = \{i \in \mathcal{I} \colon i \ can\_use \ r\} .$$

Let λ be an integer such that

$$\lambda \leq \min_{r \in \mathcal{R}} \left\lfloor \frac{|users\_of(r)|}{|\mathcal{R}|} \right\rfloor . \qquad (\dagger)$$

We assume that λ can be chosen positive. For any resource, the number of processes that can be waiting for or using the resource will be bounded by λ.

Define an asynchronous structure M as follows. The set of local states is

$$\mathcal{L} = \{N\} \cup \{T^r \colon r \in \mathcal{R}\} \cup \{C^r \colon r \in \mathcal{R}\} .$$

Let $S_M = \mathcal{L}^{\mathcal{I}}$. For any $r \in \mathcal{R}$, the guarded local transitions are the following:

1. $\gamma : N \to T^r$, where
$$\gamma \equiv users\_of(r) \wedge (\#\{T^r, C^r\} < \lambda) .$$

2. $\#C^r = 0 : T^r \to C^r$.

3. $true : C^r \to N$.

The group $G = Sym(\mathcal{I})$ acts on S_M, and M^G is obtained by replacing γ by $\#\{T^r, C^r\} < \lambda$.

We check that M is strongly virtually symmetric with respect to G. Suppose $s \xrightarrow{i} t \in R_{M^G} - R_M$. The transition must be of type 1 for some r that is not shared by i. It suffices to show that s satisfies

$$\#(users\_of(r), N) \geq 1 .$$

Notice that any process not in local state N must be in local state T^ρ or C^ρ for some $\rho \in \mathcal{R}$. Furthermore, in s,

$$\begin{aligned} \sum_{\rho \in \mathcal{R}} \#\{T^\rho, C^\rho\} &= \#\{T^r, C^r\} + \sum_{\rho \in \mathcal{R} - \{r\}} \#\{T^\rho, C^\rho\} \\ &\leq \lambda - 1 + (|\mathcal{R}| - 1)\lambda \\ &= \lambda|\mathcal{R}| - 1 \\ &< |users\_of(r)| , \end{aligned}$$

the last inequality following from $(\dagger)$. $\square$

6. Counting

Local counting of missing arcs can be used to establish that a structure is strongly virtually symmetric. We give a counting condition that is equivalent to strong virtual symmetry.

NOTATION: $R_{s;M}$ denotes the subset of R_M consisting of those arcs with s as initial state. $\square$

0-7695-0725-5/00 $10.00 © 2000 IEEE

Proposition 5: *Let M be a structure, and let G act on S_M. M is strongly virtually symmetric with respect to G if and only if, for each $s \to t \in R_{M^G} - R_M$,*

$$|Aut(s)(s \to t) - R_{s;M}| < [Aut(s) : Aut(s) \cap Aut(t)] \ .$$

$\square$

For brevity, write $\delta(s \to t) = [Aut(s) : Aut(s) \cap Aut(t)]$. For asynchronous structures under the group of all permutations of the processes, $\delta(s \to t)$ is easily computed.

Proposition 6: *Let M be an asynchronous $\mathcal{L}^{\mathcal{I}}$-structure, let $G = Sym(\mathcal{I})$ act on S_M according to $(*)$, and let $s \to t \in R_{M^G}$ result from the local transition $x \to y$. If $x = y$, then $\delta(s \to t) = 1$. Otherwise, $\delta(s \to t) = \#x(s)$.* $\square$

Under the additional simplifying assumption that all asymmetric arcs arise from a *single* local transition, the counting condition reduces to a simple bound at each state on the number of missing arcs initiating from the state.

Corollary: *Let M be an asynchronous $\mathcal{L}^{\mathcal{I}}$-structure, and let $G = Sym(\mathcal{I})$ act on S_M according to $(*)$. For simplicity, assume that every transition in $R_{M^G} - R_M$ is obtained by firing the* single *local transition $x \to y$, where $x \neq y$. M is strongly virtually symmetric with respect to G if and only if, for every $s \in S_M$,*

$$|R_{s;M^G} - R_{s;M}| < \max(1, \#x(s)) \ .$$

$\square$

The corollary can be used to demonstrate easily the strong virtual symmetry of the structures in Examples 4, 6, and 8 by counting missing arcs.

7. Conclusion

Virtual symmetry reduction is a general method for ameliorating state explosion in asymmetric systems. It subsumes previous methods of rough symmetry reduction and reduction by a group of near automorphisms. Virtual symmetry is the most general condition under which an asymmetric structure is naturally bisimilar to its quotient by a group of state symmetries. We have described example systems exhibiting virtual symmetry that are not amenable to symmetry reduction by earlier techniques. These examples show that virtual symmetry reduction applies to a significantly broader class of asymmetric systems than could be handled before.

References

[AHI98] K. Ajami, S. Haddad, and J.-M. Ilie, Exploiting symmetry in linear time temporal logic model checking: one step beyond. In *Tools and Algorithms for the Construction and Analysis of Systems, 4th International Conference, ETAPS-98*, LNCS 1384, Springer, 1998.

[CM84] K.M. Chandy and J. Misra, The drinking philosophers problem. In *ACM TOPLAS* **6**(4):632–646, 1984.

[CE81] E.M. Clarke and E.A. Emerson, Design and verification of synchronization skeletons using branching time temporal logic. In *Logics of Programs Workshop*, Springer, LNCS 131, pp. 52–71, 1981.

[CE+96] E.M. Clarke, R. Enders, T. Filkorn, S. Jha, Exploiting symmetry in temporal logic model checking. *Formal Methods in System Design*, **9**(1/2), 1996.

[ES96] E.A. Emerson and A.P. Sistla, Symmetry and model checking. *Formal Methods in System Design*, **9**(1/2), 1996.

[ES97] E.A. Emerson and A.P. Sistla, Utilizing symmetry when model checking under fairness assumptions. *ACM TOPLAS* **19**(4):617–638, 1997.

[ET98] E.A. Emerson and R.J. Trefler, Model checking real-time properties of symmetric systems. In *Mathematical Foundations of Computer Science, 23rd International Symposium*, LNCS 1450, Springer, 1998.

[ET99] E.A. Emerson and R.J. Trefler, From asymmetry to full symmetry. *CHARME99*.

[GS97] V. Gyuris and A.P. Sistla, On-the-fly model checking under fairness that exploits symmetry. In *Proceedings of the 9th International Conference on Computer Aided Verification*, 1997.

[HI+95] S. Haddad, J.-M Ilie, M. Taghelit, and B. Zouari, Symbolic reachability graph and partial symmetries. In *Application and Theory of Petri Nets 1995*, LNCS 935, Springer, 1995.

[ID96] C-W.N. Ip and D.L. Dill, Better verification through symmetry. *Formal Methods in System Design*, **9**(1/2), 1996.

[JR91] K. Jensen and G. Rozenberg (eds.), *High-Level Petri Nets: Theory and Application*, Springer, 1991.

[LP85] O. Lichtenstein and A. Pnueli, Checking that finite state concurrent programs satisfy their linear specifications. In *POPL-85*, pp. 97–107, 1985.

0-7695-0725-5/00 $10.00 © 2000 IEEE

[MAV96] F. Michel, P. Azema, and F. Vernadat, Permutable agents in process algebra. In *tools and Algorithms for the Construction and Analysis of Systems, 1996,* LNCS 1055, Springer, 1996.

[QS82] J.P. Queille and J. Sifakis, Specification and verification of concurrent programs in CESAR. In *Proc. 5th Int. Symp. Prog.*, LNCS 137, Springer, pp. 195–220, 1982.

8. Appendix

8.1. Group actions

Let G be a group, and let X be a set. An *action* of G on X is a pairing

$$G \times X \to X \ ,$$

written

$$(g, x) \mapsto gx \ ,$$

such that

$$g(g'x) = (gg')x \quad \text{and} \quad 1_G x = x$$

whenever $g, g' \in G$, $x \in X$, and 1_G is the identity element of G.

Let G act on X. For fixed $g \in G$, the function $X \to X$ by $x \mapsto gx$ is a bijection whose inverse is given by $x \mapsto g^{-1}x$. $Sym(X)$ denotes the group of all permutations (i.e., bijections) of X with group operation defined to be composition of functions. It is not difficult to check that the map $G \to Sym(X)$ that sends g to the bijection $x \mapsto gx$ is a homomorphism of groups, and any such homomorphism defines an action of G on X.

For $x \in X$, the *G-orbit* of x is the set

$$Gx = \{gx\colon g \in G\} \ .$$

Notice that $Gx = Gx'$ if and only if there exists $g \in G$ such that $x' = gx$. The G-orbits are the equivalence classes of the relation

$$\mathcal{O} = \{(x, x') \in X \times X\colon Gx = Gx'\} \ ,$$

known as the *orbit relation* on X. A subset T of X is a *transversal* for the action of G on X if T contains exactly one element from each G-orbit of X. In other words, a transversal for the action of G on X is a set of representatives of the G-orbits of X.

Let $Y \subseteq X$. If $g \in G$, then we write

$$gY = \{gy \ : \ y \in Y\} \ .$$

Also, we let

$$Aut(Y; G) = \{g \in G \ : \ gY = Y\} \ ,$$

the largest subgroup of G whose elements leave Y setwise invariant. For $x \in X$, we write $Aut(x; G)$ to mean $Aut(\{x\}; G)$. $Aut(x; G)$ is often called the *stabilizer* or *isotropy group* of x with respect to the action of G. When G is clear from context it may be dropped from the notation.

The size of a G-orbit is expressed algebraically by

$$|Gx| = [G : Aut(x; G)] \ ,$$

where, for H a subgroup of G, $[G : H]$ denotes the index of H in G. Notice that for $g, g' \in G$ and $x \in X$, $gx = g'x$ if and only if $gAut(x; G) = g'Aut(x; G)$. In other words, g and g' send x to the same element under the action if and only if g and g' are in the same right coset of $Aut(x; G)$.

8.2. Lemmas and proofs omitted from the text

Although $S_M = S_{M^G}$ and $\mathcal{O} = \mathcal{O}^{-1}$, it is convenient in the proofs below to imagine that S_M is distinguished from S_{M^G} and to regard $\mathcal{O}$ as a subset of $S_M \times S_{M^G}$ and $\mathcal{O}^{-1}$ as a subset of $S_{M^G} \times S_M$.

Lemma 1: *Let M be a structure, and let G act on S_M. Then the orbit relation $\mathcal{O}$ is a simulation of M by M^G.*

Proof: Suppose $s, s' \in S_M$, $(s, s') \in \mathcal{O}$, and $s \to t \in R_M$. Then $Gs = Gs'$, so there exists $g \in G$ such that $gs = s'$. By the definition of M^G, $s' \to gt \in R_{M^G}$, and, as $(t, gt) \in \mathcal{O}$, the simulation is demonstrated. □

Lemma 2: *Let M be a structure, and let G act on S_M. The following are equivalent:*

(1) *$\mathcal{Q}^{-1}$ is a simulation of M/G by M.*

(2) *$\mathcal{O}^{-1}$ is a simulation of M^G by M.*

(3) *For any $s \to t \in R_{M^G}$, there exists $g \in G$ such that $s \to gt \in R_M$.*

Proof: (1) $\Rightarrow$ (2). Suppose $s \in S_M$, $Gs = Gs'$, and $s' \to t' \in R_{M^G}$. By the definition of R_{M^G}, there exists $g \in G$ such that $gs' \to gt' \in R_M$. Therefore, $Gs \to Gt' \in R_{M/G}$. According to (1), there exists $t \in Gt'$ such that $s \to t \in R_M$. Since $t \in Gt'$, $Gt = Gt'$.

(2) $\Rightarrow$ (3). Suppose $s \to t \in R_{M^G}$. Since $(s, s) \in \mathcal{O}^{-1}$, (2) implies that there exists $s \to t' \in M$ such that $Gt = Gt'$. Then there exists $g \in G$ such that $gt = t'$.

(3) $\Rightarrow$ (1). Suppose $Gs \in S_{M/G}$, $s' \in Gs$, and $Gs \to Gt \in R_{M/G}$. Then there exists $g' \in G$ such that $s' = g's$, and, by the definition of $R_{M/G}$, there exist $g, h \in G$ such that $gs \to ht \in R_M$. By the definition of R_{M^G}, $s' \to$

0-7695-0725-5/00 $10.00 © 2000 IEEE

$(g'g^{-1}h)t \in R_{M^G}$. By (3), there exists $g'' \in G$ such that, with $t' = (g''g'g^{-1}h)t$, $s' \to t' \in R_M$. $\square$

Proposition 1: *Let M be a structure, and let G act on S_M. The following are equivalent:*

(1) *$\mathcal{Q}$ is a bisimulation between M and M/G.*

(2) *$\mathcal{O}$ is a bisimulation between M and M^G.*

(3) *For any $s \to t \in R_{M^G}$, there exists $g \in G$ such that $s \to gt \in R_M$.*

Proof: Apply the lemmas and the fact that $\mathcal{Q}$ is always a simulation of M by M/G. $\square$

Lemma 3: *Suppose $t \in \mathcal{L}^{\mathcal{I}}$, $g \in Sym(\mathcal{I})$, and $p, q \in \mathcal{I}$.*

(1) *If $t(i) = (gt)(i)$ for all $i \neq p$, then $t = gt$.*

(2) *If $t(i) = (gt)(i)$ for all $i \notin \{p, q\}$, then there exists $g' \in Sym(\mathcal{I})$ such that g' fixes $\mathcal{I} - \{p, q\}$ and $gt = g't$.*

Proof: (1) Let $x = t(p)$, and let $a = \#x(t)$. Then

$$a - 1 = \#(\mathcal{I} - \{p\}, x)(t) = \#(\mathcal{I} - \{p\}, x)(gt) \; .$$

Since $a = \#x(t) = \#x(gt)$, we must have $(gt)(p) = x$. Therefore, $t = gt$.

(2) If $p = q$, then by (1) we can take g' to be the identity permutation. Assume $p \neq q$. Let $x = t(p)$, $y = t(q)$, $a = \#x(t)$, $b = \#y(t)$. Consider first the case that $x = y$. Then

$$a - 2 = \#(\mathcal{I} - \{p, q\}, x)(t) = \#(\mathcal{I} - \{p, q\}, x)(gt) \; .$$

Since $a = \#x(t) = \#x(gt)$, we must have $(gt)(p) = (gt)(q) = x$. Therefore, we can take g' to be the identity permutation. Consider now the case that $x \neq y$. Then

$$a - 1 = \#(\mathcal{I} - \{p, q\}, x)(t) = \#(\mathcal{I} - \{p, q\}, x)(gt)$$

and

$$b - 1 = \#(\mathcal{I} - \{p, q\}, y)(t) = \#(\mathcal{I} - \{p, q\}, y)(gt)$$

Since $a = \#x(t) = \#x(gt)$ and $b = \#y(t) = \#y(gt)$, it follows that

$$\{(gt)(p), (gt)(q)\} = \{x, y\} \; .$$

Therefore, g' can be taken either as the identity permutation or as the permutation that swaps p with q and fixes $\mathcal{I} - \{p, q\}$. $\square$

Proposition 2: *Let M be an asynchronous $\mathcal{L}^{\mathcal{I}}$-structure, and let $Sym(\mathcal{I})$ act on S_M according to $(*)$. M is virtually symmetric with respect to $Sym(\mathcal{I})$ if and only if it is strongly virtually symmetric with respect to $Sym(\mathcal{I})$.*

Proof: From the definition, strong virtual symmetry implies virtual symmetry. Assume that M is virtually symmetric with respect to $G = Sym(\mathcal{I})$. Consider $s \xrightarrow{p} t \in R_{M^G}$. Then there exists $g \in G$ such that $s \xrightarrow{q} gt \in R_M$. According to interleaving, $s(i) = t(i)$ for $i \neq p$ and $s(i) = (gt)(i)$ for $i \neq q$. Therefore, $t(i) = (gt)(i)$ for $i \notin \{p, q\}$.

If $p = q$, then part (1) of Lemma 3 gives $t = gt$, and so $s \xrightarrow{p} t \in R_M$. Assume $p \neq q$. Part (2) of the lemma gives $g' \in G$ such that g' fixes $\mathcal{I} - \{p, q\}$ and $g't = gt$. Then $s \xrightarrow{q} g't \in R_M$. If g' is the identity permutation, then $g' \in A\ ut(s)$. Otherwise, g' interchanges p with q. Then

$$s(p) = (gt)(p) = (g't)(p) = t(q) = s(q) \; ,$$

and so $g' \in A\ ut(s)$. $\square$

Proposition 3: *Let M be an $\mathcal{L}^{\mathcal{I}}$-structure and let G be a group of near automorphisms of M. Then M is strongly virtually symmetric with respect to G.*

Proof: Let $s \to t \in R_{M^G} - R_M$. Since R_M contains a transversal for the action of G on R_{M^G}, there exist $s' \to t' \in R_M$ and $g' \in G$ such that $g'(s' \to t') = s \to t$. Since g' is a near automorphism, we must have $A\ ut(S_M) \subseteq Aut(s')$. It follows that $G \subseteq A\ ut(s')$, hence $s' = s$. Therefore, the condition of the definition of strong virtual symmetry is satisfied by letting $g = (g')^{-1}$. $\square$

Proposition 4: *Let M be an asynchronous $\mathcal{L}^{\mathcal{I}}$-structure that is roughly symmetric with respect to some ordering of $\mathcal{I}$ and the subgroup G of $Aut(S_M; Sym(\mathcal{I}))$. Then M is strongly virtually symmetric with respect to G.*

Proof: Let $s \xrightarrow{i} t \in R_{M^G}$, and suppose that $s \xrightarrow{i} t \notin R_M$. Since R_M contains a transversal for the action of G on R_{M^G}, there exists $g' \in G$ such that $g's \xrightarrow{g'i} g't \in R_M$. Since $s \in G(g's)$, rough symmetry gives $\pi \in G$ such that $\pi g's = s$ and $s \xrightarrow{\pi g' i} \pi g't \in R_M$. With $g = \pi g'$, it is easy to check that $gs = s$ and $s \xrightarrow{gi} gt \in R_M$. $\square$

Proposition 5: *Let M be a structure, and let G act on S_M. Then M is strongly virtually symmetric with respect to G if and only if, for each $s \to t \in R_{M^G} - R_M$,*

$$|A\ ut(s)(s \to t) - R_{s;M}| < [Aut(s) : Aut(s) \cap A\ ut(t)] \; .$$

Proof: We understand $A\ ut(s) = Aut(s; G)$ and $A\ ut(t) = A\ ut(t; G)$. Recall that G acts on $S_M \times S_M$ via $g(s \to t) = gs \to gt$. M is strongly virtually symmetric with respect to G if and only if, for any $s \to t \in R_{M^G} - R_M$,

$$A\ ut(s)(s \to t) \cap R_{s;M} \neq \emptyset \; .$$

Notice that

$$Aut(s \to t; Aut(s)) = Aut(s) \cap Aut(t) \; .$$

0-7695-0725-5/00 $10.00 © 2000 IEEE

Therefore,

$$|Aut(s)(s \to t)| = [Aut(s) : Aut(s) \cap Aut(t)] \; .$$

The claimed strict inequality thus holds if and only if $Aut(s)(s \to t) \cap R_{s;M} \neq \emptyset$. □

Proposition 6: *Let M be an asynchronous $\mathcal{L}^{\mathcal{I}}$-structure, let $G = Sym(\mathcal{I})$ act on S_M according to $(*)$, and let $s \to t \in R_{M^G}$ result from the local transition $x \to y$. If $x = y$, then $\delta(s \to t) = 1$. Otherwise, $\delta(s \to t) = \#x(s)$.*

Proof: If $x = y$, then $s = t$, hence $\delta(s \to t) = 1$. [This reflects the fact that M is strongly virtually symmetric only if there is no self-loop in $R_{M^G} - R_M$.] Otherwise, $x \neq y$. Let i be the process that undergoes the local state change $x \to y$. Notice that

$$Aut(s) \cong \prod_{z \in s(\mathcal{I})} Sym(s^{-1}(z)) \; ,$$

and similarly for $Aut(t)$. Since $t(j) = s(j)$ for $j \neq i$, it follows that $t^{-1}(x) = s^{-1}(x) - \{i\}$, $t^{-1}(y) = s^{-1}(y) \cup \{i\}$, and $t^{-1}(z) = s^{-1}(z)$ for $z \notin \{x, y\}$. Any element of $Aut(s) \cap Aut(t)$ must fix i, and thus

$$\frac{Aut(s)}{Aut(s) \cap Aut(t)} \cong \frac{Sym(s^{-1}(x)) \times Sym(s^{-1}(y))}{Sym(s^{-1}(x) - \{i\}) \times Sym(s^{-1}(y))} \; .$$

Therefore

$$\begin{aligned} \delta(s \to t) &= [Sym(s^{-1}(x)) : Sym(s^{-1}(x) - \{i\})] \\ &= \#x(s) \; . \end{aligned}$$

[In fact, the $\#x(s)$ elements of $Aut(s)(s \to t)$ are obtained by firing $x \xrightarrow{j} y$ in state s for each $j \in s^{-1}(x)$.] □

Corollary: *Let M be an asynchronous $\mathcal{L}^{\mathcal{I}}$-structure, and let $G = Sym(\mathcal{I})$ act on S_M according to $(*)$. For simplicity, assume that every transition in $R_{M^G} - R_M$ is obtained by firing the* single *local transition $x \to y$, where $x \neq y$. M is strongly virtually symmetric with respect to G if and only if, for every $s \in S_M$,*

$$|R_{s;M^G} - R_{s;M}| < \max(1, \#x(s)) \; .$$

Proof: ($\Rightarrow$) If $R_{s;M^G} - R_{s;M}$ is empty, then the inequality above holds trivially. Otherwise, let $s \xrightarrow{p} t$ and $s \xrightarrow{p'} t'$ be transitions in $R_{s;M^G} - R_{s;M}$. Each results from the local transition $x \to y$. Let $\pi \in G$ interchange p with p' and fix all other indexes. Then $\pi \in Aut(s)$, and

$$\pi(s \xrightarrow{p} t) = s \xrightarrow{p'} t' \; .$$

Therefore, $R_{s;M^G} - R_{s;M}$ is contained in $Aut(s)(s \to t) - R_{s;M}$, and the inequality above follows from Propositions 5 and 6.

($\Leftarrow$) Consider $s \to t \in R_{M^G} - R_M$. This transition results from the local transition $x \to y$, so $\#x(s) \geq 1$. By the inequality above, $|R_{s;M^G} - R_{s;M}| < \#x(s)$. Plainly, $Aut(s)(s \to t) - R_{s;M}$ is contained in $R_{s;M^G} - R_{s;M}$, and so, by Proposition 6, $|Aut(s)(s \to t) - R_{s;M}| < \delta(s \to t)$. According to Proposition 5, M is strongly virtually symmetric with respect to G. □

0-7695-0725-5/00 $10.00 © 2000 IEEE