Asymmetry and 3-Valued Symmetry Reduction

Ou Wei, Yong Yuan

Department of Computer Science,

University of Toronto

January 30, 2004

Abstract

Symmetry reduction is an efficient abstraction technique for symmetric systems. The reduced model produced by this method is often smaller than the original model, and is bisimilar to that model. However, it is very often that systems are not "perfectly" symmetric, while exhibiting symmetry in part of their behaviors. In [8], Emerson et al. proposed a near symmetry reduction on asymmetric systems based on near automorphism permutations. In this paper, we extend this work by defining a more general permutation, *component symmetry*, such that automorphism and near automorphism become special cases of component symmetry. We show that the component symmetry reduced model is also bisimulation equivalent to the original model.

Multi-valued models exhibit special symmetric properties because of the states and transitions labeled with multi-valued logic values. In this paper, we also investigate how to apply symmetry reduction to multi-valued models. We define automorphism and component symmetry over 3-valued logic, and show that the original 3-valued model and its symmetry reduced model refine each other. We then analyze the relationship between symmetry reduction of a 3-valued model and classical models induced by it.

1 Introduction

Model checking [5] is an automatic technique for verifying finite state concurrent systems. The verification procedure normally conducts an exhaustive search of the system's state space to determine if a property is true or false. Model checking has been used successfully in practice to verify complex circuit design and communication protocols. However, model checking suffers state explosion problem: the number of states in the system grows exponentially with the number of system variables and processes. Symmetry reduction [1, 4, 6] is an efficient abstraction method which can reduce the state space substantially for systems consisting of several identical processes. Based on the observation that the system's behaviors of interest are not changed when the roles of such processes are exchanged, an automorphism group of the system that preserves both the state labeling and the transitions can be introduced to partition the set of states into equivalence classes. A representative is chosen from each equivalence class. The quotient structure built on the set of representatives is bisimulation equivalent to the original model. Therefore, any temporal property can be safely verified on the reduced structure.

However, in practice, many systems are not "perfectly" symmetric. This often happens when the processes of a system components have similar behaviors in some part of their specification, but individually show different features in other parts. For example [8], in the reader-writer protocol, the writer has higher priority to access the book, so the overall behaviors of the reader-writer system is not symmetric although the reader and the writer have a high degree of symmetric behaviors (that is, both have the following transitons: non-critical-section $\rightarrow$ trying $\rightarrow$ critical-section $\rightarrow$ non-critical-section). To deal with this problem, Emerson et al [8] . introduced *near automorphism* which has less restrictions than automorphism. They applied near symmetry reduction to the asymmetric read-write model based on near automorphism permutations, and showed that the reduced model is bisimilar to the original model. But, near symmetry reduction can not be applied to systems where more complex asymmetric behaviors are involved. In this paper, by studying symmetry reduction and the abstraction theory of model-checking, we define a more general permutation, *component symmetry*, which can be applied to a wider class of asymmetric systems. We show that the component symmetry reduced quotient structure still preserves the bisimulation relationship with the original model.

We are also interested in symmetry reduction on multi-valued models [2, 3, 11]. Multi-valued models show special symmetric properties with states and transitions labeled with multi-valued logic values. To obtain the benefits of symmetry reduction, we need to define new notions over multi-valued logic. In this paper, we develop symmetry reduction on

3-valued models based on automorphism and component symmetry respectively. We then analyze the relationship between a 3-valued model and its symmetry reduced model, and show that they refine each other. Thus, we can get the same 3-valued model checking results on them. Because each 3-valued model can induce two classical models, we also investigate symmetry reduction on the two classical models. We show that applying symmetry reduction on a 3-valued model directly is equivalent to applying the same reduction on the two classical models separately, and then merging the results.

The rest of the paper is organized as follows: in Section 2, we give the necessary background; in Section 3, we define component symmetry, and show the bisimulation relation between a model and its component symmetry reduced quotient structure; in Section 4, we analyze the symmetry reduction on 3-valued models; related work is discussed in Section 5, and a conclusion is given in Section 6.

2 Background

2.1 Model Checking and Bisimulation

We use Kripke structure [5] to model a system. A Kripke structure is defined on a set of atomic propositions AP, $M = (S, s_0, R, L)$ where S is a finite set of states, s_0 is the initial state, $R \subseteq S \times S$ is a total transition relation, $L : S \to 2^{AP}$ is a labeling function which labels each state with the set of atomic propositions true in that state. We use *Computation Tree Logic* (CTL) as the specification language. We write $M, s \models \varphi$ to denote that a CTL formula φ is true in M. A detailed and formal description of CTL model checking can be found in [5].

Definition 2.1 [9] *Let $M = (S, s_0, R, L)$ and $M' = (S', s'_0, L', R')$ be two Kripke structures with the same atomic propositions AP. A relation $B \subseteq S \times S'$ is a* bisimulation relation *between M and M' if and only if for all $s \in S$ and $s' \in S'$, if $(s, s') \in B$ then the following conditions hold:*
(1) $L(s) = L'(s')$
(2) $(\forall t \in S)((s, t) \in R \Rightarrow (\exists t' \in S')((s', t') \in R' \wedge (t, t') \in B))$
(3) $(\forall t' \in S')((s', t') \in R' \Rightarrow (\exists t \in S)((s, t) \in R \wedge (t, t') \in B))$

We write $s \equiv s'$ for $(s, s') \in B$. We say M and $M^{'}$ are *bisimilar* (denoted by $M \equiv M'$) if there exists a bisimulation relation B over M and M'.

Definition 2.2 [9] *Let $M = (S, s_0, R, L)$ and $M' = (S', s'_0, L', R')$ be two Kripke structures with the same atomic propositions AP. A relation $H \subseteq S \times S'$ is a* simulation relation *between M and M' if and only if for all $s \in S$ and $s' \in S'$, if $(s, s') \in H$ then the following conditions hold:*
(1) $L(s) = L'(s')$
(2) $(\forall t \in S)((s, t) \in R \Rightarrow (\exists t' \in S')((s', t') \in R' \wedge (t, t') \in H))$

We write $s \preceq_{sim} s'$ for $(s, s') \in H$. We say *M' simulates M* (denoted by $M \preceq_{sim} M'$) if there exists a simulation relation H over M and M'.

The bisimulation relation over Kripke structures describes the equivalence between two Kripke structures which have the same behaviors. Simulation, on the other hand, characterizes the abstraction relation between two structures.

Theorem 2.1 [9] *Let $M = (S, s_0, R, L)$ and $M' = (S', s'_0, L', R')$ be two Kripke structures, and $M \equiv M'$, then for any CTL formula φ, $(\forall s \in S)(\forall s' \in S')(s \equiv s' \Rightarrow (M, s \models \varphi \Leftrightarrow M', s' \models \varphi))$*

2.2 Symmetry Reduction

A *permutation* σ on a set A is a bijection $\sigma : A \rightarrow A$. A set of permutations form a *permutation group* G under the composition operation if the identity permutation e is in G and G is closed under the inverse and the composition operations [1, 4]. The order of a permutation σ of G (denoted by $|\sigma|$) is the smallest positive integer k such that $\sigma^k = e$. In this paper, we apply permutation over the set of states of a Kripke structure.

Definition 2.3 *$\sigma_1, \sigma_2, \ldots, \sigma_k$ are* generators *of a permutation group G (denoted by $G = \langle \sigma_1, \sigma_2, \ldots, \sigma_k \rangle$) if G is the closure of the set $\sigma_1, \sigma_2, \ldots, \sigma_k$ under composition operation.*

A permutation that maps $t_1 \longmapsto t_2, t_2 \longmapsto t_3, \ldots, t_{k-1} \longmapsto t_k, t_k \longmapsto t_1$ is called a *cycle*, which can be denoted as $(t_1, t_2, \ldots, t_{k-1}, t_k)$. Any permutation σ can be written as a composition of disjoint cycles [13].

Definition 2.4 *A permutation σ of a Kripke structure $M = (S, s_0, R, L)$ is called an* automorphism *of M if and only if it preserves the transition relation R, that is,*
$(\forall s_1 \in S)(\forall s_2 \in S)((s_1, s_2) \in R \Rightarrow (\sigma(s_1), \sigma(s_2)) \in R)$

A permutation group G is an automorphism group of a Kripke structure M if and only if every permutation $\sigma \in G$ is an automorphism of M.

Definition 2.5 *A permutation σ of a Kripke structure $M = (S, s_0, R, L)$ is an* invariance permutation *for an atomic proposition p if and only if the following condition holds,*
$(\forall s \in S)(p \in L(s) \Leftrightarrow p \in L(\sigma(s)))$

A permutation group G of a Kripke structure $M = (S, s_0, R, L)$ is an invariance group for a formula φ if every permutation $\sigma \in G$ is an invariance permutation for every atomic proposition occuring in φ.

Let G be a permutation group on a set S, then S can be partitioned into equivalence classes induced by G [4]. The equivalence class of an element s is called the *orbit* of s, which is the set $\theta(s) = \{s' | \exists \sigma \in G, \sigma(s) = s'\}$. Because G is a group, any two states are in the same orbit if and only if both can be mapped from each other by permutations in G. Formally, for any $s_1, s_2 \in S$, $\theta(s_1) = \theta(s_2) \Leftrightarrow (\exists \sigma \in G)(s_1 = \sigma(s_2))$. A representative state is chosen from each orbit $\theta(s)$, which is called $rep(\theta(s))$.

Given a Kripke structure $M = (S, s_0, R, L)$ and let G be an automorphism group on S. The *quotient structure* $M_G = (S_G, s_G^0, R_G, L_G)$ is defined as follows:

- $S_G = \{\theta(s) | s \in S\}$
- $s_G^0 = \theta(s_0)$
- $R_G \subseteq S_G \times S_G$ and

  $\forall s \in S, \forall t \in S$,$(\theta(s), \theta(t)) \in R_G$ if and only if

$$(\exists s' \in \theta(s))(\exists t' \in \theta(t))(s', t') \in R \tag{2.1}$$

- $L_G(\theta(s)) = L(rep(\theta(s)))$

In [4], it is shown that if an automorphism group G is also an invariance group for a temporal formula φ, then M and M_G are bisimulation equivalent with respect to φ, thus φ can be safely checked in the reduced structure M_G.

Theorem 2.2 [4] *Let $M = (S, s_0, R, L)$ be a Kripke structure, G be an automorphism group of M, and φ be a CTL formula. If G is an invariance group for φ, then $(\forall s \in S)(M, s \models \varphi \Leftrightarrow M_G, \theta(s) \models \varphi)$*

2.3 Multi-valued Models and Refinement

Multi-valued model checking [2, 3, 11] is an extension of classical model checking to reasoning about systems with uncertain information, which receives a multi-valued transition system and a temporal logic formula φ defined over multi-valued logic, and returns a degree to which φ holds on the system using a multl-valued logic value. We write $||\varphi||^M(s)$ to represent the value of φ in the state s of a multi-valued model M. In this paper, we restrict multi-valued model checking to CTL model checking over 3-valued Kleene logic.

3-valued Kleene logic [12] has three elements $\top$, M, and $\bot$ interpreted as **true**, **maybe**, and **false** respectively. The *truth ordering* $\sqsupseteq$ is defined on these values to form a lattice such that $\top \sqsupseteq M \sqsupseteq \bot$ and $x \sqsupseteq x$ for all $x \in \{\top, M, \bot\}$. A preorder, called *information ordering* $\preceq$, can also be defined on the values of Kleene logic to reflect the degree of information completeness, where $M \preceq \top$, $M \preceq \bot$, $x \preceq x$ for all $x \in \{\top, M, \bot\}$, and $x \npreceq x$ otherwise.

Correspondingly, a system is modeled using 3-valued Kripke structure. A 3-valued Kripke structure is defined over a set of atomic propositions AP, $M = (S, s_0, L, R)$. The difference between 3-valued Kripke structures and the Kripke structures defined in Section 2.1 is that R and L in 3-valued Kripke structures are defined over 3-valued logic, that is, $R : S \times S \rightarrow \{\top, M, \bot\}$, and $L : S \times AP \rightarrow \{\top, M, \bot\}$. The Kripke structures defined in Section 2.1 are called *classical* Kripke structure which can be seen as a 3-valued Kripke structures that do not use the value M.

The simulation relation between classical Kripke structures can be extended to *refinement* relationship between 3-valued Kripke structures.

Definition 2.6 [11] *Let $M_c = (S_c, s_0^c, L_c, R_c)$ and $M_\alpha = (S_\alpha, s_0^\alpha, L_\alpha, R_\alpha)$ be 3-valued Kripke structures with AP as the set of atomic propositions. A relation $\rho \subseteq S_c \times S_\alpha$ is a* refinement *between M_c and M_α if and only if for all $s \in S_c$ and $a \in S_\alpha$, if $(s,\ a) \in \rho$ then*
(1) $(\forall p \in AP) L_\alpha(a,p) \preceq L_c(s,p)$
(2) $(\forall a' \in S_\alpha)(R_{\overline{\alpha}}^{\exists\top}(a,a') \Rightarrow (\exists s' \in S_c)(R_{\overline{c}}^{\exists\top}(s,s') \wedge (s',a') \in \rho))$
(3) $(\forall s' \in S_c)(R_{\overline{c}}^{\exists M}(s,s') \Rightarrow (\exists a' \in S_\alpha)(R_{\overline{\alpha}}^{\exists M}(a,a') \wedge (s',a') \in \rho))$

If there exists a refinement relation between M_c and M_α, we say M_c refines M_α, denoted by $M_\alpha \preceq_{ref} M_c$.

Definition 2.7 [14] *Let $M_a = (S_a, s_0^a, L_a, R_a)$ and $M_b = (S_b, s_0^b, L_b, R_b)$ be 3-valued Kripke structures with AP as the set of atomic propositions. Let $\rho \subseteq S_a \times S_b$ be a relation on them. ρ* preserves *CTL if and only if for any CTL formula φ, $(\forall s \in S_a)(\forall s' \in S_b)((s,s') \in \rho \Rightarrow \|\varphi\|^{M_b}(s') \preceq \|\varphi\|^{M_a}(s))$.*

Theorem 2.3 [11] *Refinement preserves CTL properties over 3-valued logic.*

3 Component Symmetry

The symmetry reduction described in Section 2.2 is based on an automorphism group on the set of states S. However, it is often the case that the systems are not symmetric with respect to automorphism relationship. In this case, to obtain the benefits of bisimulation relations between the reduced structure and the original model, we need to define permutations which have weaker constraints than automorphism. Emerson et al. [8] defined G to be a *near automorphism* permutation group if for any $\sigma \in G$ and any transition (s_1, s_2) in M, either $(\sigma(s_1), \sigma(s_2))$ is in M, or s is a fully symmetric state of G (s is a fully symmetric state of G if and only if $(\forall \sigma' \in G)$ $(\sigma'(s) = s)$). A permutation in G is called a *near automorphism* of M with respect to G. The quotient structure induced by a near automorphism group is bisimilar to M.

For example, consider the Kripke structure M shown in Figure 1(a), and a permutation group $G = \langle (s_1, s_2)(s_3, s_4) \rangle$. Note that G contains only two permutations, $(s_1, s_2)(s_3, s_4)$, and the identity permutation e. Then, for any $\sigma \in G$, if a transition (s, s') is in M then $(\sigma(s), \sigma(s'))$ is in M except for the fully symmetric state s_0. So G is a near automorphism

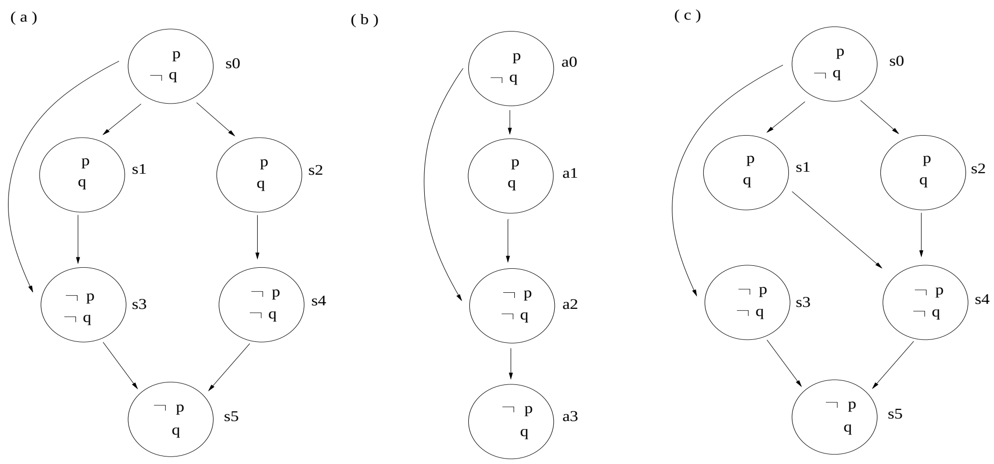

Figure 1: (a) A Kripke structure M (b) The quotient structure of M (c) A Kripke structure M'

group of M. The quotient structure of M induced by G is shown in Figure 1(b), which is bisimilar to M.

Now consider the Kripke structure M' in Figure 1(c) and the same permutation group G. G is not a near automorphism for M', because for the transitions (s_1, s_4) and (s_2, s_4), if we apply permutation $\sigma = (s_1, s_2)(s_3, s_4)$, the resulted state pairs (s_2, s_3) and (s_1, s_3) are not the transitions in M'. So the quotient structure induced by G on M' may not be bisimilar to M'.

However, by analyzing the relation between a Kripke structure M and its quotient structure M_G induced by a permutation group G, we notice that we are able to further weakening the restriction on permutations while assuring the bisimulation relationship between M and M_G. Let $M_r^{\exists\exists}$ and $M_r^{\forall\exists}$ be the abstracted models generated by applying *existential abstraction* and *universal abstraction* [9] on the set of orbits induced by G respectively. Then M_G is bisimulation equivalent to M if $M_G \equiv M_r^{\forall\exists} \equiv M_r^{\exists\exists}$. Inspired by this idea, we define *componet symmetry*, which can be applied to a wider class of asymmetric systems while obtaining a reduced structure bisimilar to the original.

3.1 Component Symmetry Group and Bisimulation

Definition 3.1 *A permutation σ of a Kripke structure $M = (S, s_0, R, L)$ is called a* component symmetry *of M if and only if the following condition holds,*
$(\forall s_1 \in S)(\forall s_2 \in S)((s_1, s_2) \in R \Rightarrow (\exists i \geq 1)(\sigma(s_1), \sigma^i(s_2)) \in R)$.

Note that any permutation σ can be written as a composition of a set of disjoint cycles, e.g. $\sigma = \sigma_1\sigma_2 \ldots \sigma_l$. Thus, if such i exists in the above definition, suppose σ_j acts on s_2, then $1 \leq i \leq |\sigma_j|$. If σ is an automorphism, then we can set i equal to 1; if σ is a near automorphism, we can chose $|\sigma_j|$ as the value for i if s_1 is a fully symmetric state, otherwise we can set i equal to 1. Therefore, automorphism and near automorphism permutations are the special cases of component symmetry.

A permutation group G is a component symmetry group of a Kripke structure M if and only if every permutation $\sigma \in G$ is a component symmetry permutation of M.

The name of this kind of permutation is given based on the following observation. Let σ be a component symmetry on M, and $\sigma = \sigma_1\sigma_2 \ldots \sigma_l$ be its decomposition into disjoint cycles. Then, it is easy to show that $\forall\sigma_m(1 \leq m \leq l), \forall\sigma_n(1 \leq n \leq l), ((\exists s_m \in \sigma_m)(\exists s_n \in \sigma_n)(s_m, s_n) \in R \Rightarrow (\forall s'_m \in \sigma_m)(\exists s'_n \in \sigma_n)(s'_m, s'_n) \in R)$. That is, the elements in the same cycle are symmetric relative to each cycle (component) of the permutation.

Given a Kripke structure $M = (S, s_0, R, L)$ and let G be a component symmetry group on S. The quotient structure $M_{G,ComSym}$ induced by G is constructed as described in Section 2.2. Next, we show that the result of Theorem 2.2 extends to component symmetry.

Lemma 3.1 *Let $M = (S, s_0, R, L)$ be a Kripke structure with AP as the set of atomic propositions. Let G be a component symmetry group of M, and $M_{G,ComSym} = (S_{G,ComSym}$, $s^0_{G,ComSym}$, $R_{G,ComSym}$, $L_{G,ComSym})$ be the quotient structure induced by G. The relation $B \subseteq S \times S_{G,ComSym}$ is defined as $\forall s \in S, (s, \theta(s)) \in B$. Then if G is an invariance group for all propositions in AP, B is a bisimulation relation between M and $M_{G,ComSym}$.*

Proof for any $(s, \theta(s)) \in B$, we show that
(1) $L(s) = L_{G,ComSym}(\theta(s))$
(2) $(\forall t \in S)((s, t) \in R \Rightarrow \exists\theta(t')(t' \in S)((\theta(s), \theta(t')) \in R_{G,ComSym} \wedge (t, \theta(t')) \in B))$

(3) $\forall\theta(t')(t' \in S)((\theta(s), \theta(t')) \in R_{G,ComSym} \Rightarrow (\exists t \in S)((s,t) \in R \wedge (t, \theta(t')) \in B)$

We first show that (1) is true. By the definition of $M_{G,ComSym}$, $L(\theta(s)) = L(rep(\theta(s))$, and by the definition of $\theta(s)$, $\exists\sigma \in G, rep(\theta(s)) = \sigma(s)$. Furthermore, because G is an invariance group for all $p \in AP$, then $(\forall p \in AP)(p \in L(s) \Rightarrow p \in L(rep(\theta(s))))$. Thus, $L_{G,ComSym}(\theta(s)) = L(rep(\theta(s))) = L(s)$.

To show (2) is true, consider any $t \in S$ such that $(s,t) \in R$. Then by the definition of $R_{G,ComSym}$, we have $(\theta(s), \theta(t)) \in R_{G,ComSym}$. Moreover, by the definition of B, we have $(t, \theta(t)) \in B$. Let $t' = t$, then (2) is true.

To show (3) is true, consider any $\theta(t') \in S_{G,ComSym}$ such that $(\theta(s), \theta(t')) \in R_{G,ComSym}$. By the definition of $R_{G,ComSym}$, we have $(\exists s_1 \in S)(\exists t_1 \in S)((s_1, t_1) \in R \wedge s_1 \in \theta(s) \wedge t_1 \in \theta(t'))$. By the definition of orbit and the property of permutation group, we have that $\exists\sigma_1 \in G, s = \sigma_1(s_1)$ and $\exists\sigma_2 \in G, t_1 = \sigma_2(t')$.

Because G is a component symmetry group, then $(\exists i \geq 1)(\sigma_1(s_1), \sigma_1^i(t_1)) \in R)$. Let $t = \sigma_1^i(t_1)$, then $(s,t) \in R$.

Let $\sigma_3 = \sigma_1^i\sigma_2$. Because G is a permutation group, $\sigma_3 \in G$. Then $t = \sigma_3(t'), t \in \theta(t')$, and $\theta(t) = \theta(t')$.

Moreover, by the definition of B, we have $(t, \theta(t)) \in B$. Then $(t, \theta(t')) \in B$.

Therefore, (3) is true. $\Box$

According to the Theorem 2.1, we then have the following corollary immediately.

Corollary 3.1 *Let $M = (S, s_0, R, L)$ be a Kripke structure with AP as the set of atomic propositions. Let G be a component symmetry group of M, and $M_{G,ComSym} = (S_{G,ComSym}$, $s^0_{G,ComSym}$, $R_{G,ComSym}$, $L_{G,ComSym})$ is the quotient structure induced by G. Let φ be any CTL formula. If G is an invariance group for all propositions in AP, then $(\forall s \in S)(M, s \models \varphi \Leftrightarrow M_{G,ComSym}, \theta(s) \models \varphi)$.*

We now give the following theorem which states that if a component symmetry group G is also an invariance group for a CTL formula φ, then the model checking result of φ on M is preserved in $M_{G,ComSym}$. By Corollary 3.1, the theorem can proved very similarly to the proof of Theorem 2.2 in [4].

Theorem 3.1 *Let $M = (S, s_0, R, L)$ be a Kripke structure. Let G be a component symmetry group of M, and $M_{G,ComSym} = (S_{G,ComSym}, s^0_{G,ComSym}, R_{G,ComSym}, L_{G,ComSym})$ is the quotient structure induced by G. Let φ be any CTL formula. If G is an invariance group for φ, then $(\forall s \in S)(M, s \models \varphi \Leftrightarrow M_{G,ComSym}, \theta(s) \models \varphi)$.*

Now consider the Kripke structure M' shown in Figure 1(c), and the permutation group $G = \langle (s_1, s_2)(s_3, s_4) \rangle$ again. It is easy to verify that G is a component symmetry group of M', and is also an invariance group for atomic propositions p and q. For example, if we apply the permutation $\sigma = (s_1, s_2)(s_3, s_4)$ to the transitions (s_1, s_4) and (s_2, s_4), then we have $(\sigma(s_1), \sigma^2(s_4))$ and $(\sigma(s_2), \sigma^2(s_4))$ belonging to G. Four orbits are induced by G: $\{s_0\}, \{s_1, s_2\}$, $\{s_3, s_4\}$, and $\{s_5\}$. The quotient structure $M'_{G,ComSym}$ is bisimulation equivalent to $M^{'}$, which is as same as the quotient structure shown in Figure 1(b).

3.2 Component Symmetry Generated Group and Bisimulation

Next, we analyze symmetry reduction using a group generated by a set of component symmetry permutations.

Definition 3.2 *A permutation group G is a* component symmetry generated group *of a Kripke structure $M = (S, s_0, R, L)$ if and only if $G = \langle g_1, g_2, \ldots, g_k \rangle$ and every generator $g_i (1 \leq i \leq k)$ is a component symmetry permutaion of M.*

Given a Kripke structure $M = (S, s_0, R, L)$, let G be a component symmetry generated group on S. We can define the quotient structure $M_{G,ComSymGen}$ induced by G similarly to $M_{G,ComSym}$. However, a component symmetry generated group may not be a component symmetry group. That is, if both σ_1 and σ_2 are component symmetry permutations, the composition of them $\sigma = \sigma_1 \sigma_2$ may not be a component symmetry permutation. Thus, the Theorem 3.1 does not apply to a component symmetry generated group. Fortunately, by the properties of permutation group and component symmetry, the reduced structure $M_{G,ComSymGen}$ also has the nice bisimulation relations with M.

Lemma 3.2 *Let $M = (S, s_0, R, L)$ be a Kripke structure with AP as the set of atomic propositions. Let $G = \langle g_1, g_2, \ldots, g_k \rangle$ be a component symmetry generated group of M, and $M_{G,ComSymGen} = (S_{G,ComSymGen}, s^0_{G,ComSymGen}, R_{G,ComSymGen}, L_{G,ComSymGen})$ is the quotient structure induced by G. Then if every generator $g_i (1 \leq i \leq k)$ is an invariance permutation* *for all propositions in AP, the relation* $B \subseteq S \times S_{G,ComSymGen}$ *defined by* $\forall s \in S, (s, \theta(s)) \in B$ *is a bisimulation relation between* M *and* $M_{G,ComSymGen}$.

Proof We show the three conditions in the proof of Lemma 4.1 are true.
Note that if every generator g_i is an invariance permutation for an atomic proposition p, then the group generated by the set $\{g_1, g_2, \ldots, g_k\}$ is an invariance group for p. So it is easy to show that (1) and (2) are true.

To show (3) is true, consider any $\theta(t') \in S_{G,ComSymGen}(t' \in S)$ such that $(\theta(s), \theta(t')) \in R_{G,ComSymGen}$. By the definition of $R_{G,ComSymGen}$, we have $(\exists s_1 \in S)(\exists t_1 \in S)((s_1, t_1) \in R \wedge s_1 \in \theta(s) \wedge t_1 \in \theta(t'))$. By the definition of orbit and the property of permutation group, we have that $\exists \sigma_1 \in G, s = \sigma_1(s_1)$ and $\exists \sigma_2 \in G, t_1 = \sigma_2(t')$.

Because G is a component symmetry generated group, then $(\exists n \geq 1)(\sigma_1 = g_{i_1} g_{i_2} \ldots g_{i_n})$ where $g_{i_m}(1 \leq m \leq n) \in \{g_1, g_2, \ldots g_k\}$.

Because every $g_l(1 \leq l \leq k)$ is a component symmetry permutation on M, then by the induction on the length of $g_{i_1} g_{i_2} \ldots g_{i_n}$, for $\sigma_1 = g_{i1} g_{i2} \ldots g_{in}$, and $(s_1, t_1) \in R$, we have that $(\exists j_1 \geq 1)(\exists j_2 \geq 1) \ldots (\exists j_n \geq 1)(g_{i_1} g_{i_2} \ldots g_{i_n}(s_1), g_{i_1}^{j_1} g_{i_2}^{j_2} \ldots g_{i_n}^{j_n}(t_1)) \in R$. Let $t = g_{i_1}^{j_1} g_{i_2}^{j_2} \ldots g_{i_n}^{j_n}(t_1)$, then $(s, t) \in R$.

Let $\sigma_3 = g_{i_1}^{j_1} g_{i_2}^{j_2} \ldots g_{i_n}^{j_n} \sigma_2$. Because G is a permutation group, $\sigma_3 \in G$. Then $t = \sigma_3(t'), t \in \theta(t')$, and $\theta(t) = \theta(t')$.

Moreover, by the definition of B, we have $(t, \theta(t)) \in B$. Then $(t, \theta(t')) \in B$.

Therefore, (3) is true. $\square$

Similarly, by Lemma 3.2, we have the following corollary and theorem.

Corollary 3.2 *Let* $M = (S, s_0, R, L)$ *be a Kripke structure with AP as the set of atomic propositions. Let* $G = \langle g_1, g_2, \ldots, g_k \rangle$ *be a component symmetry generated group of* M*, and* $M_{G,ComSymGen} = (S_{G,ComSymGen}, s^0_{G,ComSymGen}, R_{G,ComSymGen}, L_{G,ComSymGen})$ *is the quotient structure induced by G. Let* φ *be any CTL formula. Then if every generator* $g_i(1 \leq i \leq k)$ *is an invariance permutation for all propositions in AP, then* $(\forall s \in S)(M, s \models \varphi \Leftrightarrow M_{G,ComSymGen}, \theta(s) \models \varphi)$.

Theorem 3.2 *Let* $M = (S, s_0, R, L)$ *be a Kripke structure. Let* $G = \langle g_1, g_2, \ldots, g_k \rangle$ *be a component symmetry generated group of* M*, and* $M_{G,ComSymGen} = (S_{G,ComSymGen}, s^0_{G,ComSymGen},$

$R_{G,ComSymGen}$, $L_{G,ComSymGen}$) *is the quotient structure induced by* G. *Let* φ *be any CTL formula. If Then if every generator* $g_i(1 \leq i \leq k)$ *is an invariance permutation for all propositions in AP, for* φ, *then* $(\forall s \in S)(M, s \models \varphi \Leftrightarrow M_{G,ComSymGen}, \theta(s) \models \varphi)$.

4 Symmetry Reduction on 3-valued Models

In this section, we study symmetry reduction on 3-valued Kripke structures. We start by defining two kinds of permutation on 3-valued Kripke structures that correspond to automorphism and component symmetry, respectively. Then we analyze the refinement relation between a 3-valued Kripke structure and its quotient structure. We show that 3-valued model checking can be safely done on the quotient structures. Since each 3-valued Kripke structure induces two classical Kripke structures, we also analyze the relationship between symmetry reductions on 3-valued Kripke structure and the two classical Kirpke structures induced by it.

4.1 3-valued Symmetry Reduction and Refinement

We first define invariance permutation and automorphism for 3-valued models (note that equality, instead of equivalence, is used to define the relation between 3-valued logic values here).

Definition 4.1 *A permutation* σ *of a 3-valued Kripke structure* $M = (S, s_0, R, L)$ *is an invariance permutation for an atomic proposition* p *if and only if the following condition holds,*
$(\forall s \in S)(L(s, p) = L(\sigma(s), p))$

A permutation group G of a 3-valued Kripke structure $M = (S, s_0, R, L)$ is an invariance group for a formula φ if every permutation $\sigma \in G$ is an invariance permutation for every atomic proposition p occuring in φ.

Definition 4.2 *A permutation* σ *of a 3-valued Kripke structure* $M = (S, s_0, R, L)$ *is called an automorphism of* M *if and only if it does not change the value of transition relation* R, *that is,*
$(\forall s_1 \in S)(\forall s_2 \in S)(R(s_1, s_2) = R(\sigma(s_1), \sigma(s_2)))$

A permutation group G is an automorphism group of a 3-valued Kripke structure M if and only if every permutation $\sigma \in G$ is an automorphism of M.

Given a 3-valued Kripke structure $M = (S, s_0, R, L)$ with AP as the set of atomic propositions, and let G be an automorphism group on S. The quotient structure $M_G = (S_G, S_G^0, R_G, L_G)$ is defined as follows:

- $S_G = \{\theta(s) | s \in S\}$
- $s_G^0 = \theta(s_0)$
- $R_G : S_G \times S_G \to \{\top, M, \bot\}$ and $\forall s \in S, \forall t \in S$,

  $R_G(\theta(s), \theta(t)) \triangleq \top$ if and only if

  $$(\exists s' \in \theta(s))(\exists t' \in \theta(t))R(s', t') = \top \tag{4.1}$$

  $\mathrm{R}_G(\theta(s), \theta(t)) \triangleq M$ if and only if (4.1) is false and

  $$(\exists s' \in \theta(s))(\exists t' \in \theta(t))R(s', t') = M \tag{4.2}$$

  $\mathrm{R}_G(\theta(s), \theta(t)) \triangleq \bot$ if and only if both (4.1) and (4.2) are false.
- $L_G : S_G \times AP \to \{\top, M, \bot\}$ defined as follows:

  $(\forall s \in S)(\forall p \in AP)L_G(\theta(s), p) \triangleq L(rep(\theta(s), p)$

Next we show that when the automorphism group G is also an invariance group for a CTL formula φ, M and M_G refine each other with respect to φ. Thus, $(\forall s \in S)(\|\varphi\|^M(s) = \|\varphi\|^{M_G}(\theta(s)))$.

Lemma 4.1 *Let $M = (S, s_0, R, L)$ be a 3-valued Kripke structure with AP as the set of atomic propositions. Let G be a automorphism group of M, and $M_G = (S_G,\ s_G^0,\ R_G,\ L_G)$ is the quotient structure induced by G. Then, if G is an invariance group for all propositions in AP, M and M_G refines each other. That is, $M \preceq_{ref} M_G$ and $M_G \preceq_{ref} M$.*

Proof To show $M \preceq_{ref} M_G$, define $\rho_1 \subseteq S_G \times S$ as $(\forall s \in S)(\theta(s), s) \in \rho_1$. Then, for any $(\theta(s), s) \in \rho_1$. The following statements must hold:
(1)$(\forall p \in AP)L(\theta(s), p) \preceq L_G(s, p)$

$(2)(\forall s' \in S)(R^{\sqsupseteq\top}(s,s') \Rightarrow \exists\theta(t')(t' \in S)(R_G^{\sqsupseteq\top}(\theta(s),\theta(t')) \wedge (\theta(t'),s') \in \rho_1))$
$(3)\forall\theta(t')(t' \in S)(R_G^{\sqsupseteq M}(\theta(s),\theta(t')) \Rightarrow (\exists s' \in S)(R^{\sqsupseteq M}(s,s') \wedge (\theta(t'),s') \in \rho_1))$

Since G is an invariance group for all atomic propositions in AP, (1) follows trivially.

To show (2) is true, consider any $s' \in S$ such that $R(s,s') = \top \sqsupseteq \top$. Then by the definition of R_G, $R_G(\theta(s),\theta(s')) = \top \sqsupseteq \top$. Moreover, by the definition of ρ_1, $(\theta(s'),s') \in \rho_1$. Let $t' = s'$, then (2) is true.

To show (3) is true, consider any $\theta(t')(t' \in S)$ such that $R_G(\theta(s),\theta(t')) \sqsupseteq M$.

If $R_G(\theta(s),\theta(t')) = \top$, then by the definition of R_G, $(\exists s_1 \in S)(\exists t_1 \in S)(R(s_1,t_1) = \top \wedge s_1 \in \theta(s) \wedge t_1 \in \theta(t'))$. By the definition of an orbit, we have that $(\exists\sigma \in G)(s = \sigma(s_1))$.

Because G is an automorphism group of M, then $R(\sigma(s_1),\sigma(t_1)) = \top$. Let $s' = \sigma(t_1)$, then $R(s,s') = \top \sqsupseteq M$.

Because $t_1 \in \theta(t')$, then, by the definition of an orbit, $s' \in \theta(t')$ and $\theta(s') = \theta(t')$. Moreover, by the definition of ρ_1, $(\theta(s'),s') \in \rho_1$. Then $(\theta(t'),s') \in \rho_1$.

Thus, (3) is true when $R_G(\theta(s),\theta(t')) = \top$. Similarly, (3) is also true when $R_G(\theta(s),\theta(t')) = M$.

Therefore, $M \preceq_{ref} M_G$.

$M_G \preceq_{ref} M$ can be proved similarly. □

By Theorem 2.3, we have the following corollary, and then the theorem immediately.

Corollary 4.1 *Let $M = (S, s_0, R, L)$ be a 3-valued Kripke structure with AP as the set of atomic propositions. Let G be a automorphism group of M, and $M_G = (S_G,\ s_G^0,\ R_G,\ L_G)$ is the quotient structure induced by G. Let φ be any CTL formula. Then if G is an invariance group for all propositions in AP, $(\forall s \in S)(\|\varphi\|^M(s) = \|\varphi\|^{M_G}(\theta(s)))$.*

Theorem 4.1 *Let $M = (S, s_0, R, L)$ be a 3-valued Kripke structure with AP as the set of atomic propositions. Let G be a automorphism group of M, and $M_G = (S_G,\ s_G^0,\ R_G,\ L_G)$ is the quotient structure induced by G. Let φ be any CTL formula. If G is an invariance group for φ, then $(\forall s \in S)(\|\varphi\|^M(s) = \|\varphi\|^{M_G}(\theta(s)))$.*

As is the case on classical Kripke structures, the condition of automorphism is too strong to be used for a wider class of multi-valued models. In Section 3, we have shown that the component symmetry can be applied to more asymmetric structures while producing a reduced structure bisimilar to the original model. Similarly, we define component symmetry on 3-valued Kripke structure. We show that a 3-valued Kripke structure and its quotient structure induced by a component symmetry group (or component symmetry generated group) also refine each other. Thus, we get the same 3-valued CTL model checking on them.

Definition 4.3 *A permutation σ of a 3-valued Kripke structure $M = (S, s_0, R, L)$ is called a component symmetry of M if and only if the following condition holds,*
$(\forall s_1 \in S)(\forall s_2 \in S)((R(s_1, s_2) = \top \Rightarrow (\exists i \geq 1)R(\sigma(s_1), \sigma^i(s_2)) = \top) \wedge (R(s_1, s_2) = M \Rightarrow (\exists i \geq 1)R(\sigma(s_1), \sigma^i(s_2)) \sqsupseteq M))$

Intuitively, if σ is a component symmetry of a 3-valued Kripke structure M, and $\sigma = \sigma_1\sigma_2 \ldots \sigma_l$ is its decomposition into disjoint cycles, then for any two elements s_1 and s_2 in the same cycle σ_i, if s_1 has a **true** transition to an element in another cycle σ_j, then s_2 also has a **true** transition to σ_j; if s_1 has a **maybe** transition to an element in σ_j, then s_2 has either a **true** transition or a **maybe** transition to σ_j.

A permutation group G is a component symmetry group of a 3-valued Kripke structure M if and only if every permutation $\sigma \in G$ is a component symmetry of M. A permutation group G is a component symmetry generated group of a 3-valued Kripke structure $M = (S, s_0, R, L)$ if and only if $G = \langle g_1, g_2, \ldots, g_k \rangle$ and every generator $g_i (1 \leq i \leq k)$ is a component symmetry of M.

Given a 3-valued Kripke structure M, and a component symmetry group (or a component symmetry generated group) G of M, similarly as that for automorphism group, we can define the quotient structure $M_{G,ComSym}$ (or $M_{G,ComSymGen}$) and prove the following theorems.

Theorem 4.2 *Let $M = (S, s_0, R, L)$ be a 3-valued Kripke structure with AP as the set of atomic propositions. Let G be a component symmetry group of M, and $M_{G,ComSym} = (S_{G,ComSym}, s^0_{G,ComSym}, R_{G,ComSym}, L_{G,ComSym})$ be the quotient structure induced by G. Let φ be any CTL formula. If G is an invariance group for φ, then $(\forall s \in S)(\|\varphi\|^M(s) = \|\varphi\|^{M_{G,ComSym}}(\theta(s)))$.*

Theorem 4.3 *Let $M = (S, s_0, R, L)$ be a 3-valued Kripke structure. Let $G = \langle g_1, g_2, \ldots, g_k\rangle$ be a component symmetry generated group of M, and $M_{G,ComSymGen} = (S_{G,ComSymGen}$, $s^0_{G,ComSymGen}$, $R_{G,ComSymGen}$, $L_{G,ComSymGen})$ be the quotient structure induced by G. Let φ be any CTL formula. If every generator $g_i (1 \leq i \leq k)$ is an invariance permutation for φ, then $(\forall s \in S)(\|\varphi\|^M(s) = \|\varphi\|^{M_{G,ComSymGen}}(\theta(s)))$.*

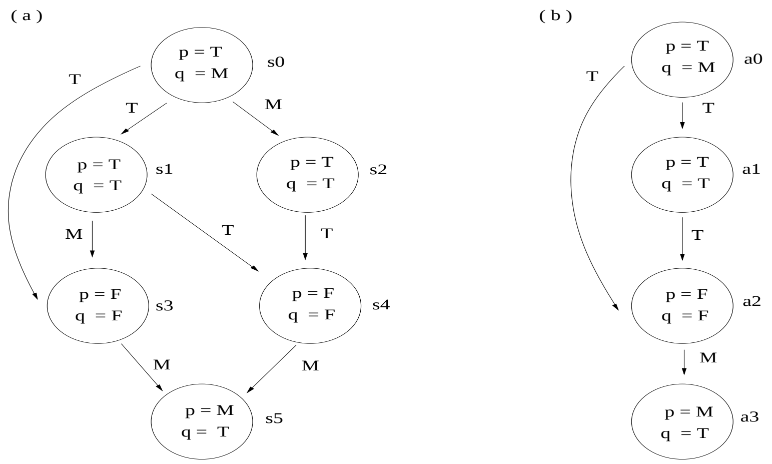

Figure 2: (a) A 3-valued Kripke structure M; (b) The quotient structure for M

For example, consider the 3-valued Kripke structure M in Figure 2(a). The permutation group $G = \langle(s_1, s_2)(s_3, s_4)\rangle$ is a component symmetry group of M, which is also an invariance group for atomic propositions p and q. Four orbits are induced by G: $\{s_0\}$, $\{s_1, s_2\}$, $\{s_3, s_4\}$, and $\{s_5\}$. The final quotient structure $M_{G,ComSym}$ is shown in Figure 2(b). Because M and $M_{G,ComSym}$ refine each other, the model checking result for any CTL formula is same on them.

4.2 Symmetry and 3-valued Model Reduction

In this section, we analyze the relationship between the quotient structure induced by a symmetry group G on a 3-valued Kripke structure M and the quotient structures induced by the same group on the two classical Kripke structures induced from M. G could be an automorphism group, component symmetry group or component symmetry generated group. Since the quotient structures induced by them have the same refinement relationship with

M by Theorem 4.1, Theorem 4.2 and Theorem 4.3, we do not distinguish between them explicitly if not necessary.

Two classical Kripke structures $M^{\sqsupseteq\top}$ and $M^{\sqsupseteq M}$ are induced by a 3-valued Kripke structure $M = (S, s_0, L, R)$, which capture all definite and all possible behaviors of M [10, 11]. $M^{\sqsupseteq\top}$ and $M^{\sqsupseteq M}$ are defined as $M^{\sqsupseteq\top} = (S,\ s_0,\ L^{\sqsupseteq\top},\ R^{\sqsupseteq\top})$ and $M^{\sqsupseteq M} = (S,\ s_0,\ L^{\sqsupseteq M},\ R^{\sqsupseteq M})$, where $L^{\sqsupseteq v}(s_1, p) \triangleq L(s_1, p) \sqsupseteq v$ and $R^{\sqsupseteq v}(s_1, s_2) \triangleq R(s_1, s_2) \sqsupseteq v$ for any $s_1, s_2 \in S$ and any atomic proposition p. The induced classical Kripke structures $M^{\sqsupseteq\top}$ and $M^{\sqsupseteq M}$ of the 3-valued Kripke structure M in Figure 2(a) are shown in Figure 3(a) and Figure 3(b) respectively.

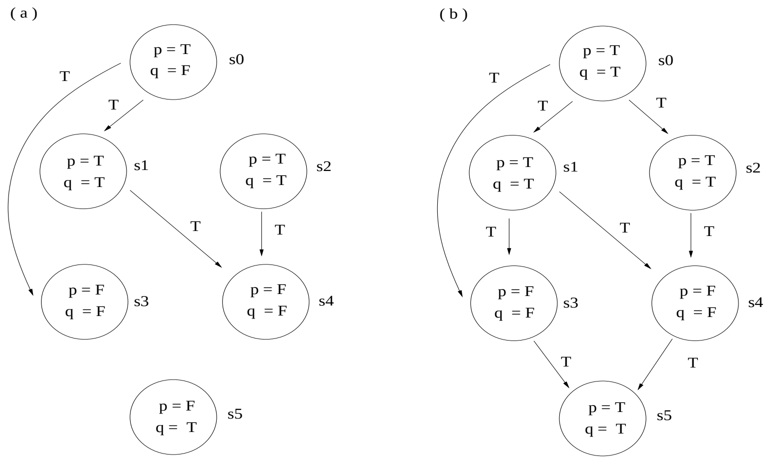

Figure 3: (a) $M^{\sqsupseteq\top}$ for M in Figure 2(a); (b) $M^{\sqsupseteq M}$ for M in Figure 2(a)

Consider the component symmetry group $G = \langle(s_1, s_2)(s_3, s_4)\rangle$ for M in Figure 2(a). Note that G is also a component symmetry group for $M^{\sqsupseteq\top}$ (Figure 3(a)) and $M^{\sqsupseteq M}$ (Figure 3(b)) over 2-valued logic, and is also an invariance group for them. Applying symmetry reduction, we get the quotient structures $M^{\sqsupseteq\top}_{\overline{G},ComSym}$ (Figure 4(a)) and $M^{\sqsupseteq M}_{\overline{G},ComSym}$ (Figure 4(b)) for $M^{\sqsupseteq\top}$ and $M^{\sqsupseteq M}$ respectively.

Note that $M^{\sqsupseteq\top}_{\overline{G},ComSym}$ and $M^{\sqsupseteq M}_{\overline{G},ComSym}$ have the same orbit sets induced by G. Thus, we can combine the two quotient structures easily. For any two orbit θ_1 and θ_2, in the combination structure, the transitions from θ_1 to θ_2 is assigned the value **true** if there are **true**

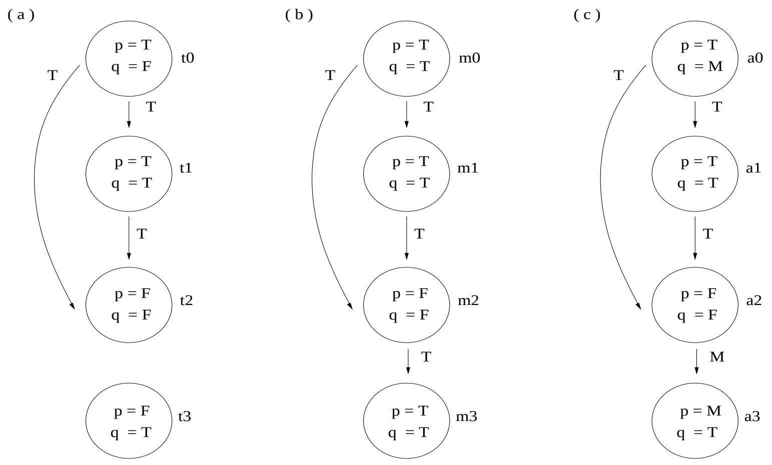

Figure 4: (a) The quotient structure $M^{\sqsupseteq\top}_{\bar{G},ComSym}$; (b) The quotient structure $M^{\sqsupseteq M}_{\bar{G},ComSym}$; (c) the combination of $M^{\sqsupseteq\top}_{\bar{G},ComSym}$ and $M^{\sqsupseteq M}_{\bar{G},ComSym}$

in both $M^{\sqsupseteq\top}_{\bar{G},ComSym}$ and $M^{\sqsupseteq M}_{\bar{G},ComSym}$; **maybe** if there is only one **true** transitions from θ_1 to θ_2 in $M^{\sqsupseteq\top}_{\bar{G},ComSym}$ and $M^{\sqsupseteq M}_{\bar{G},ComSym}$; and **false** otherwise. The labeling of atomic propositions can be done similarly. The combination structure is given in Figure 4(c).

It is not surprising to see that the combination model is as same as $M_{G,ComSym}$ in Figure 2(b). Actually, this also a way to show the correctness of the refinement relationship between a 3-valued Kripke structure M and its quotient structure M_G induced by a symmetry group G. We summarize the results formally in the following theorem:

Theorem 4.4 *Let $M = (S, s_0, R, L)$ be a 3-valued Kripke structure with AP as the set of atomic propositions. Let G be a symmetry group of M, and $M_G = (S_G,\ s^0_G,\ R_G,\ L_G)$ be the quotient structure induced by G. If G is an invariance group for all atomic propositions in AP, then M_G is the combination of the quotient structures induced by G on $M^{\sqsupseteq\top}$ and $M^{\sqsupseteq M}$.*

Proof Let $M^{\sqsupseteq\top}_{\bar{G'}} = (S^{\sqsupseteq\top}_{\bar{G'}},\ s^{0,\sqsupseteq\top}_{\bar{G'}},\ R^{\sqsupseteq\top}_{\bar{G'}},\ L^{\sqsupseteq\top}_{\bar{G'}})$ and $M^{\sqsupseteq M}_{\bar{G'}} = (S^{\sqsupseteq M}_{\bar{G'}},\ s^{0,\sqsupseteq M}_{\bar{G'}},\ R^{\sqsupseteq M}_{\bar{G'}},\ L^{\sqsupseteq M}_{\bar{G'}})$ be the quotient structures of $M^{\sqsupseteq\top}$ and $M^{\sqsupseteq M}$ induced by G respectively, and $M_{G'} = (S_{G'},\ s^0_{G'},\ R_{G'},\ L_{G'})$ be the combination of $M^{\sqsupseteq\top}_{\bar{G'}}$ and $M^{\sqsupseteq M}_{\bar{G'}}$.

By the definition of $M^{\sqsupseteq\top}$ and $M^{\sqsupseteq M}$, it is easy to show that G, under 2-valued logic, is a symmetry group of $M^{\sqsupseteq\top}$ and $M^{\sqsupseteq M}$, and also an invariance group for all atomic propositions in AP. Therefore, M_G, $M_{\overline{G'}}^{\exists\top}$ and $M_{\overline{G'}}^{\exists M}$ have the same orbit sets. Thus, $S_G = S_{G'}$ and $s_G^0 = s_{G'}^0$.

Next we show $L_G = L_{G'}$. For any $\theta_G \in S_G$, let $\theta_{G'}$, $\theta_{\overline{G'}}^{\exists\top}$ and $\theta_{\overline{G'}}^{\exists M}$ be the corresponding orbits in $S_{G'}$, $S_{\overline{G'}}^{\exists\top}$, and $S_{\overline{G'}}^{\exists M}$ respectively.

For any $p \in AP$, if $L_G(\theta_G, p) = \top$, because G is an invariance group for all atomic propositions in AP, $L(s, p) = \top$ for any $s \in \theta_G$. Then, by the definition of $L^{\exists\top}$ and $L^{\exists M}$, $L_{\overline{G'}}^{\exists\top}(\theta_{\overline{G'}}^{\exists\top}, p) = \top$ and $L_{\overline{G'}}^{\exists M}(\theta_{\overline{G'}}^{\exists M}, p) = \top$. Therefore, $L_{G'}(\theta_{G'}, p) = \top$.

Similarly, if $L_G(\theta_G, p) = M(\bot)$, then $L_{\overline{G'}}^{\exists\top}(\theta_{\overline{G'}}^{\exists\top}, p) = \bot(\bot)$ and $L_{\overline{G'}}^{\exists M}(\theta_{\overline{G'}}^{\exists M}, p) = \top(\bot)$. And then, $L_{G'}(\theta_{G'}, p) = M(\bot)$.

Thus, $L_G = L_{G'}$.

To show $R_G = R_{G'}$, consider any pair (θ_G^1, θ_G^2) in R_G, and let $(\theta_{G'}^1, \theta_{G'}^2)$, $(\theta_{\overline{G'}}^{1,\exists\top}, \theta_{\overline{G'}}^{2,\exists\top})$, $(\theta_{\overline{G'}}^{1,\exists M}, \theta_{\overline{G'}}^{2,\exists M})$ be the corresponding pairs in $R_{G'}$, $R_{\overline{G'}}^{\exists\top}$, and $R_{\overline{G'}}^{\exists M}$ respectively.

If $R_G(\theta_G^1, \theta_G^2) = \top$, then from (4.1), we have that $(\exists s' \in \theta_G^1)(\exists t' \in \theta_G^2)R(s', t') = \top$. Then, by the definition of $R^{\exists\top}$ and $R^{\exists M}$, and (2.1), $R_{\overline{G'}}^{\exists\top}(\theta_{\overline{G'}}^{1,\exists\top}, \theta_{\overline{G'}}^{2,\exists\top}) = \top$ and $R_{\overline{G'}}^{\exists M}(\theta_{\overline{G'}}^{1,\exists M}, \theta_{\overline{G'}}^{2,\exists M}) = \top$. Therefore, $R_{G'}(\theta_{G'}^1, \theta_{G'}^2) = \top$.

Similarly, if $R_G(\theta_G^1, \theta_G^2) = M(\bot)$, then $R_{\overline{G'}}^{\exists\top}(\theta_{\overline{G'}}^{1,\exists\top}, \theta_{\overline{G'}}^{2,\exists\top}) = \bot(\bot)$ and $R_{\overline{G'}}^{\exists M}(\theta_{\overline{G'}}^{1,\exists M}, \theta_{\overline{G'}}^{2,\exists M}) = \top\ (\bot)$. And then, $R_{G'}(\theta_{G'}^1, \theta_{G'}^2) = M\ (\bot)$.

Thus, $R_G = R_{G'}$. □

5 Related Work

Emerson et al. [7] proposed a *virtual symmetry* relation between a structure M and a group G, that generalizes their previous works in [8]. The idea of virtual symmetry is based on the analysis of the *symmetrization* structure (denoted by M^G) of M by G. M^G, obtained by adding all the missing arcs, is the smallest superstructure of M such that G is an automorphism group of it. Then, if every transition in M^G has a corresponding transition in M by a permutation in G, M is *virtually symmetric* with respect to G. The formal definitions are as follows:

Definition 5.1 [7] *Let $M = (S, R)$ be a structure, and G be a group that acts on S. Define $M^G = (S^G, R^G)$ is the* symmetrization *of M by G where $S^G = S$, and $R^G = \{(\sigma(s), \sigma(t)) | \sigma \in$*

G and $(s,t) \in R\}$.

Definition 5.2 [7] *Let $M = (S, R)$ be a structure, and G be a group that acts on S. $M^G = (S^G, R^G)$ is the symmetrization of M by G, then M is* virtually symmetric *with respect to G if the following condition holds: $(\forall (s,t) \in R^G)(\exists \sigma \in G)(s, \sigma(t)) \in R$.*

Emerson et al. claim that virtual symmetry is the most general condition under which the system is naturally bisimilar to its quotient structure. Actually, we find the condition can be expressed equivalently and simply as: M is virtually symmetric with respect to G if $(\forall (s,t) \in R)(\forall \sigma \in G)(\exists \sigma' \in G)(\sigma(s), \sigma'(t)) \in R$ $(*)$. It can be shown that if G is a component symmetry (generated) group for M, then M is virtually symmetric with respect to G.

Virtual symmetry is defined based on *all* the permutations in a group G. That is, virtual symmetry is a kind of property exhibited by a *group* , not a property of each *individual permutation* in the group. On the other hand, in practice, symmetry reduction is always conducted based on a set of permutations provided by users, that are used as generators of a group [1, 4]. Each generator is associated with certain symmetric property based on a high level understanding of the system. Different from virtual symmetry, component symmetry defined in this paper captures a more general condition for symmetry reduction based on the property of individual generator. The weaker constraint provided by component symmetry allows users to discover more permutations in asymmetric systems that can be used as generators for symmetry reduction.

We can extend virtual symmetry for 3-valued models based on the definition in $(*)$. A 3-valued Kripke structure $M = (S, s_0, R, L)$ is virtually symmetric with respect to a group G if $(\forall s_1 \in S)(\forall s_2 \in S)(\forall \sigma \in G)((R(s_1, s_2) = \top \Rightarrow (\exists \sigma' \in G)R(\sigma(s_1), \sigma'(s_2)) = \top) \wedge (R(s_1, s_2) = M \Rightarrow (\exists \sigma' \in G)R(\sigma(s_1), \sigma'(s_2)) \sqsupseteq M))$.

6 Conclusion

In this paper, we have extended symmetry reduction, and shown that the component symmetry reduced model is bisimilar to the original model. This allows symmetry reduction to be applied to a wider class of asymmetric systems. We also investigate the symmetry reduction induced by the group generated by a set of component symmetry permutations.

We show that even if such group is not a component symmetry group, the reduced model is still bisimilar to the original model. Our idea of component symmetry is based on the analysis of the quotient structure induced by a group and the abstracted models generated from existential abstraction and universal abstraction. Instead of focusing on the symmetric property of each state, we exploit the symmetry between the state components induced by a permutation group. We are able to develop more general symmetry reduction while preserving the bisimulation relationship between the reduced model and the original model.

We have also developed symmetry reduction on 3-valued models. For 3-valued models, we have defined automorphism and component symmetry over 3-valued logic. Using the refinement relationship between 3-valued models, we show that 3-valued CTL model checking can be safely conducted on the symmetry reduced model. We analyzed the symmetry reduction on the two classical models induced from a 3-valued model. We have shown that applying symmetry reduction on a 3-valued model directly is as same as applying symmetry reduction on the two classical models separately and then combining them together.

Acknowledgment. We thank Arie Gurfinkel for helpful discussion on the reduction and refinement relationship of multi-valued models.

References

[1] S. Barner and O. Grumberg. "Combining Symmetry Reduction and Under Approximation for Symbolic Model Checking", In *Proceedings of the 14th International Conference on Computer Aided Verification (CAV'02)*. LNCS 2404, pages 93 -106, July 2002.

[2] G. Burns and P. Godefroid. "Model Checking Partial State Spaces With 3-Valued Temporal Logics". In *Proceedings of the 11th International Conference on Computer-Aided Verification (CAV'99)*, LNCS 1633, July 1999.

[3] M. Chechik, B. Devereux, S. Esterbrook, and A. Gurfinkel. "Multi-Valued Symbolic Model-Checking". *ACM Transactions on Software Engineering and Methodology*, 2003. (Accepted for publication.).

[4] E. Clarke, T. Filkorn, and S. Jha. " Exploiting symmetry in temporal logic model checking". In *Proceedings of the 5th International Conference on Computer-Aided Verification (CAV'93)*. LNCS 697, pages 450-461, July 1993.

[5] E. Clarke, O. Grumberg, and D. Peled. *Model Checking*. MIT Press, 1999.

[6] E. A. Emerson and A. P. Sistla. "Symmetry and Model Checking", In *Proceedings of the 5th International Conference on Computer-Aided Verification (CAV'93)*, LNCS 697, June 1993.

[7] E. Allen Emerson, J. Havlicek, and Richard J. Trefler. "Virtual Symmetry Reduction". In *15th Annual IEEE Symposium on Logic in Computer Science (LICS'00)*, LICS 2000, pages 121-131, June 2000.

[8] E. A. Emerson and R. J. Trefler. "From Asymmetry to Full Symmetry: New Techniques for Symmetry Reduction in Model Checking". In *Conference on Correct Hardware Design and Verification Methods (CHARME'99)*, pages 142-157, January 1999.

[9] O. Grumberg. "Abstractions and Reductions in Model Checking", In *NATO Science Series* Vol. 62, Marktoberdorf summer school. 2001.

[10] A. Gurfinkel and M. Chechik. "Multi-Valued Model Checking via Classical Model Checking". In *Proceedings of International Conference on Concurrency Theory (CONCUR'03)*, LNCS 2761, September 2003.

[11] M. Huth, R. Jagadeesan, and D. A. Schmidt. "Modal Transition Systems: A Foundation for Three-Valued Program Analysis". In *Proceedings of the 9th International Conference on Computer-Aided Verification (CAV'97)*, LNCS 1254, pages 155-169, June 1997.

[12] S. C. Kleene. *Introduction to Matamathematics*. New York: Van Nostrand, 1952.

[13] S. MacLane and G. Birkhoff. *Algebra*. MacMillan, 1968.

[14] S. Nejati, A. Gurfinkel, and M. Chechik. "Weaker Relations, Better Abstractions", submitted for publication, October 2003.