PAPER Special Section on Formal Approach

Probabilistic Symmetry Reduction for a System with Ring Buffer

Toshifusa SEKIZAWA[†,††a)], *Member*, Takashi TOYOSHIMA[†††], Koichi TAKAHASHI[††], *Nonmembers*, *and* Kazuko TAKAHASHI[†††], *Member*

SUMMARY Probabilistic model checking is an emerging technology for analyzing systems which exhibit stochastic behaviors. The verification of a larger system using probabilistic model checking faces the same state explosion problem as ordinary model checking. Probabilistic symmetry reduction is a technique to tackle this problem. In this paper, we study probabilistic symmetry reduction for a system with a ring buffer which can describe various applications. A key of probabilistic symmetry reduction is identifying symmetry of states with respect to the structure of the target system. We introduce two functions; $Shift_\delta$ and *Reverse* to clarify such symmetry. Using these functions, we also present pseudo code to construct a quotient model. Then, we show two practical case studies; the one-dimensional Ising model and the Automatic Identification System (AIS). Behaviors of them were verified, but suffered from the state explosion problem. Through the case studies, we show that probabilistic symmetry reduction takes advantage of reducing the size of state space.

key words: *probabilistic symmetry reduction, ring buffer, model checking, the Ising model, AIS*

1. Introduction

Given a model representing a system, model checking [1] verifies whether or not the model satisfies a given specification by exhaustively searching the state space of the model. The technique has successfully been applied to verify many systems. Probabilistic model checking [2] is an extension of model checking to probabilistic systems. In both probabilistic and normal model checking, the size of state space usually increases exponentially as the number of variables increases. This general problem is called the *state explosion problem*.

This state explosion problem brings computational difficulties which affect the verifiable size and the performance of verification. To tackle the problem, various techniques have been proposed. *Symmetry reduction* is such a technique, it aggregates states by exploiting presence of symmetry and reduces the size of state space. This technique has been used in various applications, for example; cache coherence protocols in [3] and [4], and concurrent C programs in [5].

In this study, we employ symmetry reduction for probabilistic system called *probabilistic symmetry reduction*, and deal with systems containing ring buffers. Such systems behave according to the interactions between neighboring elements of the ring buffer.

The ring buffer is an important data structure that consists of a finite number of elements and has boundary conditions. The structure is used in many applications where resource bounds require the overwriting of old data. For example, in communication processing, ring buffer is used for temporary storage. The use of this concept of a data structure and boundary conditions extends beyond the field of computer science. For example, in a physical simulation, boundary conditions are assumed to simulate macroscopic behaviors caused by the results of microscopic behaviors.

The main contributions of this study are; i) to clarify how probabilistic symmetry reduction works, and ii) to show its application to systems with ring buffers.

When studying probabilistic symmetry reduction, it is important to determine equivalent classes of symmetries. We introduce two functions $Shift_\delta$ and *Reverse* which determine symmetry conditions and identify equivalent classes. Using these functions, we also show pseudo code for construction of a quotient model for automatic calculation. Using this pseudo code, we implemented programs which identify quotient states and calculate transition probabilities.

We specify details of probabilistic symmetry reduction through addressing two practical cases, a one-dimensional Ising model and an Automatic Identification System (AIS), in which a ring buffer plays an important role. The authors have already verified their behavior using probabilistic model checking [6], [7]. However, the state explosion problem restricted the verifiable size. The efficiency of our proposed procedures are evaluated by comparing the results of applying probabilistic symmetry reduction to these case studies.

There have been many approaches for theoretical calculation and case studies. For example, Kwiatkowska et al. presented a symbolic implementation of probabilistic symmetry reduction using multi-terminal binary decision diagrams (MTBDDs) and case studies [8]. This implementation is built into probabilistic model checker PRISM. Other case studies include GRIP, a tool which converts a PRISM model into a reduced model [9]. However, many of case studies only present results and do not indicate how symmetry is defined. Even if determination of symmetry is intu-

Manuscript received July 19, 2010.
Manuscript revised November 14, 2010.

[†]The author is with Faculty of Informatics, Osaka Gakuin University, Suita-shi, 564–8511 Japan.
[††]The authors are with National Institute of Advanced Industrial Science and Technology (AIST), Tsukuba-shi, 305–8568 Japan.
[†††]The authors are with School of Science and Technology, Kwansei Gakuin University, Sanda-shi, 669–1337 Japan.
a) E-mail: sekizawa@ogu.ac.jp

DOI: 10.1587/transinf.E94.D.967

itively easy, it is hard to reproduce.

The outline of this paper is as follows. In Sect. 2, we define probabilistic symmetry reduction, Discrete Time Markov Chains, and a ring buffer. Procedures for construction of a quotient model are described in Sect. 3. Section 4 and 5 are case studies. Finally, Sect. 6 concludes this study.

2. Preliminaries

In this section, definitions of probabilistic symmetry reduction, Discrete Time Markov Chains and ring buffer are given.

2.1 Probabilistic Symmetry Reduction

Symmetry reduction is known as an effective technique for reducing the size of state space by exploiting presence of symmetry in a model [1], [10].

Given a transition system $M = (S, R)$, where S is a finite set of states and $R : S \times S$ is a set of transition relations. When a map $\pi : S \rightarrow S$ is a bijection, we say π is a *permutation*. If $(s, s') \in R$ and $(\pi(s), \pi(s')) \in R$, we say π *preserves* R. Such a π is called an *automorphism*. For given a group G of such automorphism under composition of function, there exists an equivalence relation θ on S where $(s, s') \in \theta$. Given a set of states $\overline{S}$ which contains a representative state for each equivalent class then for each $s \in S$, we define a function *rep* $: S \rightarrow \overline{S}$ mapping a state to the corresponding representative. Using this function, we can define a new transition relation $\overline{R} = \{(rep(s), rep(s')) | (s, s') \in R\}$. A transition system $\overline{M} = (\overline{S}, \overline{R})$ obtained in this manner is called a *quotient model*. The quotient model $\overline{M}$ is bisimilar to the original transition system M, because all permutations in G preserve the transition relation R.

The discussion above relates to deterministic systems. Formal verification has extended its subjects to probabilistic systems. Recent studies [8], [9] have extended symmetry reduction to probabilistic systems. This technique is called *probabilistic symmetry reduction*. When applying probabilistic symmetry reduction, there are difficulties caused by certain characteristics of probabilities. Unlike deterministic systems, probabilistic systems contain probabilities assigned to transitions, and their behavior is determined by such probabilities. The consideration of these probabilities is a matter of concern when identifying transition relations of a quotient model.

2.2 Discrete Time Markov Chain

For verification of a probabilistic system, various models are proposed such as Discrete Time Markov Chains (DTMCs), Continuous Time Markov Chains (CTMCs), and Markov Decision Processes (MDPs). Some probabilistic model checkers, for example PRISM [11], adopts these models as inputs for its model.

In this paper, we consider systems represented as DTMCs. A DTMC is defined as follows. Let $\mathtt{AP}$ be a set of atomic propositions. A DTMC is a quadruple $\mathcal{M} = (S, s_0, \mathcal{T}, \mathcal{L})$ where S is a finite set of states, $s_0 \in S$ is the initial state, $\mathcal{T} : S \times S \rightarrow [0, 1]$ is a transition probability function such that $\forall s \in S, \sum_{s' \in S} \mathcal{T}(s, s') = 1$, and $\mathcal{L} : S \rightarrow 2^{\mathtt{AP}}$ is a labeling function. The current state $s \in S$ at computational time t has a transition to state $s' \in S$ at $t+1$ with probability $\mathcal{T}(s, s')$. A *path* is a sequence of states. The probability of a path $s_0, s_1, \cdots$ is $\prod_{i \geq 0} \mathcal{T}(s_i, s_{i+1})$. A DTMC satisfies the *Markov property*. That is, if we choose a state s at a computational time t, then the next state at $t+1$ depends only on the current state and is independent of the preceding states.

2.3 Ring Buffer

A *ring buffer* is a data structure that contains a number of finite elements and has periodic boundary conditions. In the following, we assume that a ring buffer b consists of n elements and denote the i-th element by $b[i]$. Then, the periodic boundary condition is $b[n] = b[0]$.

Transitions of a ring buffer are defined individually. If a transition in a ring buffer satisfies the Markov property, a ring buffer can be converted into a DTMC. In this conversion, an alignment sequence of elements in a ring buffer corresponds to a state of DTMC, and a probabilistic transition of a ring buffer guides a transition of DTMC.

3. Construction of a Quotient Model

In this section, we consider procedures of probabilistic symmetry reduction for a system that contains a ring buffer. The general procedure for constructing a quotient transition system $\overline{M} = (\overline{S}, \overline{R})$ is as follows.

Step 1: Identify quotient states $\overline{S}$.
Step 2: Identify a set of probabilistic transitions $\overline{R}$.

We also describe pseudo code of these procedures for automated calculation of probabilistic symmetry reduction.

3.1 Step 1: Identify Quotient States

For this procedure we divide a concrete state space $S = \{s_0, s_1, \ldots, s_n\}$ into disjoint subsets of states called a *partition* $A = \{A_0, A_1, \ldots, A_{n'}\}$ $(n' \leq n)$ (ideally, $n' \ll n$) on the state space according to some symmetry conditions which are described below. Then, a set of quotient states $\overline{S} = \{\overline{s}_0, \overline{s}_1, \ldots, \overline{s}_{n'}\}$ is formed by representatives of each A_i. In the process of identifying a set of quotient states, it is important to choose appropriate symmetry without any effect of the concrete behaviors to be verified.

Let *Buf* be a set of ring buffers for a fixed number of elements m, and a state $b' = \{b'[0], \ldots, b'[m-1]\}$ after applying an operation to a state $b = \{b[0], \ldots, b[m-1]\}$. We define a partition over *Buf* by taking *Buf* as S. To judge whether two ring buffers b and b' are equivalent, we introduce two functions; *Shift*$_\delta$ and *Reverse*. These two functions determine symmetry in different manners.

First, for an integer δ ($0 \leq \delta \leq m-1$), the function $\mathit{Shift}_\delta : \mathit{Buf} \rightarrow \mathit{Buf}$ is defined as follows.

$$b'[i] = b[(i-\delta+m) \bmod m]$$

This function shifts all elements of state b to b'. By applying the function Shift_δ on Buf, theoretical minimum of $|A|$ is $\frac{|\mathit{Buf}|}{m}$.

Next, for $b, b' \in \mathit{Buf}$, the function $\mathit{Reverse} : \mathit{Buf} \rightarrow \mathit{Buf}$ is defined as follows.

$$b'[i] = b[m-1-i]$$

Intuitively, this function maps every element *Buf* to its corresponding mirrored element. In the case of *Reverse*, theoretical minimum of $|A|$ is $\frac{|\mathit{Buf}|}{2}$.

Let R be a transition relation between buffers. Both Shift_δ and *Reverse* are permutations on *Buf* and preserve R. We define the equivalence relation $\sim$ over *Buf* such that $b \sim b'$ if b' is obtained from b by finitely applying Shift_δ and *Reverse*. We adopt $\mathit{Buf}/\sim$, the quotient set of *Buf* by $\sim$, as a partition.

Lastly, for $b, b' \in \mathit{Buf}$, we define a predicate $\mathit{Equiv}(b, b')$ which evaluates true if all elements of b and b' are the same, otherwise false. Then $\mathit{Equiv}(b, (\mathit{Shift}_\delta \circ \mathit{Reverse}?)(b))$ holds, where $\circ$ is composition of functions and '?' is a regular expression which indicates *Reverse* is applied either zero or one times.

In Fig. 1, we show pseudo code to identify quotient states from a set of concrete ring buffers for a fixed number of elements m. The procedure begins with empty sets A and $\overline{S}$ which store partition and quotient states, respectively. It identifies quotient states one-by-one by tracing all concrete ring buffers. For each concrete ring buffer, it is judged whether or not it is equivalent to an identified quotient state, i.e., the representative of the set $a \in A$, according to the result of composite function of Shift_δ and *Reverse*. Then predicate $\mathit{Equiv}(b, (\mathit{Shift}_\delta \circ \mathit{Reverse}?)(b))$ is calculated for all δ ($0 \leq \delta < n$). Note that δ is searched exhaustively within the range of 0 to $n-1$. If there exists at least one δ that satisfies *Equiv*, it results that $\mathit{rep}(b) = \overline{b}'$ and b is an element of the set a. When there is no δ that satisfies *Equiv*, then create a new element of partition which consists of an element b. Last, choose appropriate representatives for every element in the partition, and let them be a set of quotient states. Note that, an arbitrary element of a can be a representative. An example to decide such a representative is to choose the first state in lexicographic order.

```
procedure IdentifyQuotientStates
$A = \emptyset$    /* A is a partition*/
$\overline{S} = \emptyset$    /* $\overline{S}$ contains quotient states */
LOOP:
for all ring buffer $b$ in $Buf$ do
  for all the set $a$ in $A$ do
    $\overline{b}'$ = representative of $a$
    if there exists at least one $\delta$ satisfying
      $Equiv(b, (Shift_\delta \circ Reverse?)(b))$
    then
      add $b$ to $a$
      continue LOOP
    fi
  od
  create a new element of partition $a' = \{b\}$
  add $a'$ to $A$
od
$\overline{S}$ be a set of representatives of $A$
```

Fig. 1 Pseudo code to identify quotient states from a set of concrete states using composite function of Shift_δ and *Reverse*.

3.2 Step 2: Identify Transitions

This section describes how to form a transition probability matrix for the quotient model which simulates the concrete model. To do this, it is necessary to identify every transition probability between quotient states.

In the following, we restrict our consideration to the case where the quotient model can be considered to be a DTMC. Historically, transition probabilities of quotient models were studied by Kemeny and Snell [12] and following their study, we introduce calculation of transition probabilities.

First, let us call $\Pr(s, s')$ the transition probability between concrete states $s, s' \in S$. Then, the transition probability from a concrete state s to an element of partition $a \in A$ is given as follows.

$$\Pr(s, a) = \sum_{\{s_i \in S \,|\, \mathit{rep}(s_i) = a\}} \Pr(s, s_i)$$

Here, it should be noted that the Markov property is not necessarily preserved by the construction of a quotient model. It is stated that a condition known as *lumpability* is a necessary and sufficient condition for a quotient model to satisfy the Markov property with respect to the partition [12], [13]. That is, a DTMC is lumpable with respect to the partition A if and only if, for any $a_i, a_j \in A$, and for any states $s_k, s_l \in a_i$;

$$\Pr(s_k, a_j) = \Pr(s_l, a_j)$$

Schweitzer reported a survey of exact calculation of the transition probability between quotient states [14]. Let probability vector at the state s_j be ς_j which is a vector with elements representing outgoing probabilities from the state s_j to all the states. The transition probability between sets of partition $a, a' \in A$ is formed as follows.

$$\Pr(a, a') = \frac{\sum_{s_j \in a} \sum_{s_i \in a'} \varsigma_j \Pr(s_j, s_i)}{\sum_{s_k \in a} \varsigma_k}$$

where functional $\sum \varsigma$ stands for the sum of all elements of vector ς, i.e., for $\varsigma = (\varsigma_0, \varsigma_1, \cdots, \varsigma_{m-1})$, $\sum \varsigma \equiv \varsigma_0 + \varsigma_1 + \cdots + \varsigma_{m-1}$.

Assume that quotient model is lumpable with respect to the partition A, Fig. 2 shows a pseudo code to identify the transition probability matrix of a quotient model.

In the following sections we present case studies using programs based on the pseudo code presented here. At the end of the process of each program, the number of quotient states and transitions are summed. Every program outputs PRISM model. This means that these programs work as a preprocessing stage in probabilistic model checking.

3.3 Discussion

As described above, lumpability is assumed to identify the transition probabilities. In general, there is no way of telling whether or not lumpability holds with respect to a partition without proof. Therefore, even if existence of symmetry seems to be obvious, mathematically strict proof of lumpability is necessary to assure existence of symmetry to apply probabilistic symmetry reduction. Our proposed procedures are based on lumpability. Therefore, we start from checking lumpability for every case study described in Sect. 4 and Sect. 5.

We consider complexity of the procedures to construct a quotient model. However, exact complexity of the procedures is hard to estimate, because the procedures depend on the size of the partition A. Here we consider the worst case in which the size of the partition is the same as the number of concrete states $|S|$, i.e., no reduction was achieved. Let m be the number of elements in a ring buffer, and r be the range of an element of a ring buffer. For step 1, frequency of calling predicate *Equiv* is $|Buf| \cdot |A| \cdot m$. In the worst case we have $|Buf| = r^m$ and $|A| = r^m$, respectively. Then the calling frequency is mr^{2m}. In step 2, the dominant factor in time complexity is the calculation of transition probabilities. The frequency of calling Pr is $|A|^2 = r^{2m}$. Therefore complexity of the procedures is $O\left(mr^{2m}\right)$.

Note that such worst cases will not occur frequently because the size of the partition is usually smaller than that of concrete states. Additionally, we point out that performance may possibly be improved by considering characteristics of the target system.

In probabilistic symmetry reduction, it is important to determine which states are regarded as equivalent. In related work, [8] adopts *component symmetry* which considers occurrence frequency of elements. Here, we quote an example from [8] to make the point clear.

> In component symmetry, two states (A, B, A, A) and (A, A, B, A) are equivalent. They would both be mapped to (A, A, A, B) and $(A = 3, B = 1)$, respectively. [8]

```
/* assume $\overline{S}$ is lumpable w.r.t. the partition $A$ */
procedure IdentifyTransitionProbabilities
$P = (0)$   /* $P$ is transition probability matrix */
for all element $a$ in $A$ do
  for all element $a'$ in $A$ do
    $\Pr(a, a') = \dfrac{\sum_{s_j \in a} \sum_{s_i \in a'} \varsigma_j \Pr(s_j, s_i)}{\sum_{s_k \in a} \varsigma_k}$
    store $\Pr(a, a')$ on $P$ as an corresponding element
  od
od
```

Fig. 2 Pseudo code to identify transition probability between elements of the partition.

Though it is intuitive, component symmetry does not work well for a system with a ring buffer in which alignment sequence of elements is important. For such systems, component symmetry sometimes causes over-classification, i.e., the quotient states constructed by component symmetry do not preserve relations between elements, because component symmetry ignores alignment sequence of elements.

On the other hand, our proposed approach preserves the sequence of elements. As a corollary, reduction rate is lower than the component symmetry. Meanwhile it may prevent over-classification. In the following sections, we show two systems in which sequence of elements of a ring buffer plays an important role.

4. Case Study 1: The 1D Ising Model

Our first case study for probabilistic symmetry reduction is the Ising model [15], [16] which is a simplified model for magnets named after Ernst Ising, the physicist who proposed the model. The Ising model is defined on a collection of elementary objects called *spins* and its energy. Each spin is located on a site of lattice, and can only take one of two values; +1 (*up-spin*) or −1 (*down-spin*). A collection of states of all spins is said to be a *configuration*. The energy of the Ising model is determined by interactions among spins. In the standard form of the Ising model, interactions among spins are restricted to nearby spins and the energy E is defined as a function as follows.

$$E = -J \sum_{\langle i,j \rangle} \sigma_i \sigma_j - H \sum_k \sigma_k,$$

where σ_i is the value of the spin at the i-th site in the lattice, J is an interaction coefficient, H is the external magnetic field, and $\langle i, j \rangle$ denotes the interaction of two spins σ_i and σ_j located on nearby sites.

The one-dimensional (1D) Ising model is the one-dimensionally-confined Ising model in which spins are located on sites of a line. We assume that a model consists of finite n spins $\sigma_0, \sigma_1, \ldots \sigma_{n-1}$, periodic boundary condition such that $\sigma_n = \sigma_0$, and no external magnetic field. Figure 3 shows a 1D Ising model with a periodic boundary condition for n spins.

Transitions of the Ising model obey probabilistic distributions. The Metropolis method is a widely-used method to define such behaviors. When the Metropolis method is applied to the Ising model, it is called *random spin flipping* and uses the following algorithm:

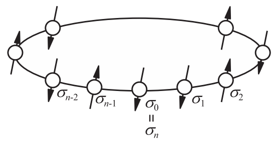


Fig. 3 One-dimensional Ising model with periodic boundary condition.

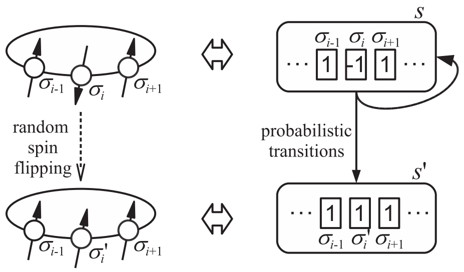


Fig. 4 Correspondence between 1D Ising model and DTMC.

1. Choose a spin σ_i at random for an individual flip.
2. Evaluate the energy difference $\Delta E = E' - E$ caused by spin flipping from σ_i to $\sigma'_i = -\sigma_i$, where $E = E(\sigma_0, \ldots, \sigma_i, \ldots, \sigma_{n-1})$ and $E' = E(\sigma_0, \ldots, \sigma'_i, \ldots, \sigma_{n-1})$.
3. If $\Delta E \leq 0$, the spin flip is accepted. Otherwise, the spin flip is accepted with probability $e^{-\Delta E/T}$, where T is a fixed temperature.
4. Repeat steps 1 to 3 for a sufficient number of times to simulate physical behavior depends on the passage of time.

Note that if the Ising model obeys random spin flipping, the next condition only depends on the current condition, i.e., it is independent of the past condition. This *memoryless property* satisfies the Markov property.

4.1 Symmetry Reduction for the 1D Ising Model

Intuitively, a configuration can be converted into a ring buffer by considering every spin to an element of ring buffer, and one random spin flipping guides a transition. Figure 4 shows an example of correspondence between two configurations and concrete states of a DMTC. For the probabilistic symmetry reduction, we follow the procedures described in Sect. 3.

4.1.1 States

In considering interactions among spins, we use the *Shift*$_\delta$ function for identifying quotient states. This is because physical behaviors of the Ising model is based on alignment sequence of spins. The *Shift*$_\delta$ function preserves such an alignment and can aggregate configurations which have the same intrinsic behavior.

According to the definition of the 1D Ising model, *Shift*$_\delta$ can be applied in a straightforward manner by considering a configuration as a ring buffer. Then quotient states are identified by the pseudo code of Fig. 1. Some characteristics can be enumerated with respect to the partition A identified by *Shift*$_\delta$. First, all states in a set in the partition have the same energy, i.e., $\forall a \in A, \forall s_i, s_j \in a, E(s_i) = E(s_j)$. This is obvious because both s_i and s_j have relatively the same alignment sequence of spins, and the energy of a state is decided by such alignment. Second, for every pair of states in a set in the partition, there is no one-step transition in a concrete model if these states are different, $\forall a \in A, \forall s_i \in a, \forall s_i \neq s_j \in a, \Pr(s_i, s_i) \neq 0$. This is because if two states s_i and s_j are different then at least two spins have different values, and one random spin flipping only changes the value of one spin. Otherwise, if two states s_i and s_j are the same then there exists a transition with probability greater than 0. In this case spin flipping is not accepted.

In addition, we apply the functions *Shift*$_\delta$ and *Reverse* to observe efficiency when both of the functions are applied. This is because quotient states identified by *Shift*$_\delta$ and *Reverse* overlap. For example, in the case of 6 spins, two configurations $(+1, +1, +1, -1, -1, -1)$ and $(-1, -1, -1, +1, +1, +1)$ are identified as equivalent by either *Shift*$_\delta$ or *Reverse*. But two configurations $(+1, -1, -1, +1, +1, -1)$ and $(-1, +1, +1, -1, -1, +1)$ are only identified as equivalent by applying both *Shift*$_\delta$ and *Reverse*.

4.1.2 Probability Transitions

For step 2, we identify transitions between quotient states on the assumption of the random spin flipping algorithm.

As described in Sect. 4.1.1, all configurations in an equivalent class have the same energy. Therefore, for two fixed sets in the partition, the energy difference is the same. These facts derive lumpability with respect to the partition A, such that $\forall a_i, a_j \in A, \forall s_k, s_l \in a_i, \Pr(s_k, a_j) = \Pr(s_l, a_j)$.

Recall that the transition probability between sets of partition $a, a' \in A$ is formed as;

$$\Pr(a, a') = \frac{\sum_{s_j \in a} \sum_{s_i \in a'} \varsigma_j \Pr(s_j, s_i)}{\sum_{s_k \in a} \varsigma_k}$$

For fixed s_j and s_i, the transition probability between these states is constant. Here, let $p \equiv \Pr(s_j, s_i)$ and $c(a, a')$ be the total number of transitions between states s_j and s_i, i.e., $c(a, a') \equiv |\{(s_j, s_i) \mid s_j \in a, s_i \in a'\}|$ for convenience. Then, for an arbitrary pair $a, a' \in A$, we have

$$\Pr(a, a') = \frac{c(a, a')}{|a|} p$$

We can then identify the transition matrix by calculating all transition probabilities according to the pseudo code 2.

4.2 Experimental Results

We implemented a program to construct a quotient model of the 1D Ising model. Table 1 shows the results of applying probabilistic symmetry reduction compared with concrete states and transitions. In Table 1, the second column shows the result of applying both *Shift*$_\delta$ and *Reverse*, the third column shows the result of only applying *Shift*$_\delta$ and the last column shows the result without any reduction.

In our implementation we adopt some heuristics to improve the performance of calculations. For example, we use the fact that all configurations in an element of a partition

Table 1 Results of probabilistic symmetry reduction for the 1D Ising model, comparing after/before reduction.

	Shift$_\delta$+*Reverse*		*Shift*$_\delta$		concrete	
spins	states	trans	states	trans	states	trans
6	13	48	14	61	64	428
8	30	166	36	252	256	2258
10	78	608	108	1061	1024	11142
12	224	2302	352	4329	4096	52924
14	687	8958	1182	17370	16384	244918
16	2250	35167	4116	69317	65536	1111906

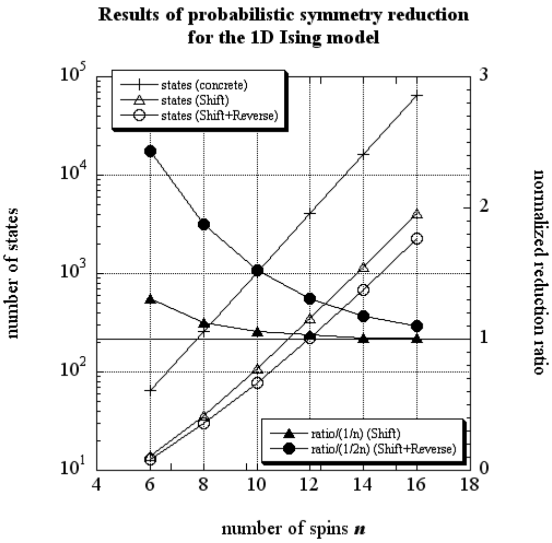


Fig. 5 Number of states (the Y-axis), and the value for the reduction ratio of quotient states per $1/n$ for *Shift*$_\delta$ and per $1/(2n)$ for *Shift*$_\delta$ + *Reverse* (the secondary Y-axis).

have the same energy. This fact induces that if the energies of two configurations are different, these two configurations are not in the same element of partition. Then, we can decrease frequency of calling the *Shift*$_\delta$ function.

4.3 Evaluation

We illustrate the effect of probabilistic symmetry reduction in Fig. 5. The X-axis is the number of spins n, and the Y-axis reflects three results of the number of states; concrete states, quotient states applied *Shift*$_\delta$ and quotient states applied *Shift*$_\delta$ + *Reverse*. The secondary Y-axis reflects the value for the normalized reduction ratio of quotient states. These values are divided by the theoretical minimum values; i.e., $1/n$ for *Shift*$_\delta$ and $1/(2n)$ for *Shift*$_\delta$ + *Reverse*.

As we can see, the normalized reduction ratio converges to 1. This indicates that composition of *Shift*$_\delta$ and *Reverse* effectively acts close to its theoretical limitation. Therefore, we can conclude that the *Shift*$_\delta \circ$*Reverse* function has power to reduce the size of state space of the 1D Ising model. Note that the normalized reduction ratio is greater than 1 for all n. This is because, there are elements of the partition for which the number of equivalent classes is less than $2n$. For example, a configuration consisting only of up-spins forms a singleton set in the partition.

5. Case Study 2: AIS

The second case study is the Automatic Identification System (AIS) which is specified by the International Maritime Organization (IMO) and is required to be mounted on every ship to ensure safety at sea [17]. The AIS, ship-to-ship communication system, uses the Self Organized Time Division Multiple Access (SOTDMA) method which defines each minute as one frame and each frame is divided into 2250 slots. Individual ships are assigned a slot in every frame and broadcast navigation data such as identification code, position, and course on this slot. If more than one ship transmits a message in the same slot, data collision occurs and the messages are lost. To avoid such collisions, each ship reserves its own slot in the next frame. Every ship has its own table in which reservations for the current frame and the next frame are written. When its turn comes in the current frame, a ship sends a message to reserve a slot in the next frame with its navigation data. When a ship receives a message from another ship, it writes the information in its own table and selects a next slot. Because communications in AIS are not interactive, simultaneous reservations of messages may occur and causes “double-booking”. As a result, data collision occurs, and much worse, ships do not know this fact. This problem has not been seriously considered because probability of the occurrence of such an event is low and the problem can be eliminated over the long run. The authors have proposed several new strategies for selecting a slot and constructed models on these strategies. These were used to analyze the probability and allowable rate of the occurrence of bad events using probabilistic model checking and verified that these models can ensure safety [7].

5.1 Symmetry Reduction for the AIS

In this section, we address probabilistic symmetry reduction of the `det` model that is based on a deterministic 1-neighbor strategy for the AIS. In this model, the reservation table is determined as follows. Each ship compares the occupants of adjacent slots on either side of its own slot in the current frame (called *a current slot*). If more ships exist in the left slot than the right one, the left slot is selected as a next frame. If more ships exist in the right slot than the left one, the right slot is selected as a next frame. If these numbers are the same, either of left/right slot or the current slot is selected at probability 1/3, respectively [7]. Figure 6 shows an example of `det` model which presents transition rules.

Here, we formalize the `det` model. *A reservation table* represents the state of reservations of all ships. It is defined as $s = \{v_0, \ldots, v_{m-1}\}$ where m is the number of slots in a frame and each v_i is the number of ships reserving the i-slot. We do not distinguish ships and consider only the number of ships that reserve a slot. The reservation table can be regarded as a ring buffer whose element may have multiple values, while only -1 or 1 is allowed in the Ising model.

This model has the Markov property, since the next

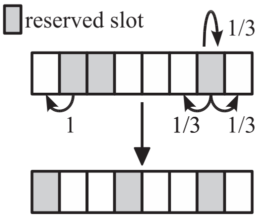


Fig. 6 Example of `det` model and its transitions.

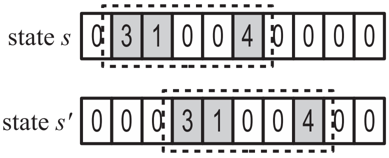


Fig. 7 Example of equivalent states. States s and s' are judged as equivalent by $Shift_2$.

state is defined depending only on the current state. Thus we can convert it to a DTMC.

Assume that there exist n ships ($n < m$). If a ship $ship_j$ ($0 \leq j \leq n-1$) selects the next slot on some reservation table with a probability p_j, then the transition probability to the next reservation table is $\prod_{j=0}^{n-1} p_j$.

5.1.1 States

First, quotient states are identified by the pseudo code of Fig. 1. According to the result of the Ising model, the composition of $Shift_\delta$ and *Reverse* reduces the number of quotient states. Therefore we apply both $Shift_\delta$ and *Reverse* to the AIS. Figure 7 shows an example of equivalent states judged as equivalent by $Shift_2$.

5.1.2 Probability Transitions

Next, we construct a quotient model with consideration of transition probabilities.

After identifying quotient states, partition A is obtained. In the `det` model, the next state of each slot is determined depending only on the current slot and its nearest neighbors, the sequence of elements in the reservation table is preserved in applying $Shift_\delta$ or *Reverse*. Therefore, for any pair $a_i, a_j \in A$ ($a_i \neq a_j$), and for any state $s \in a_i$, if there exists a transition from s to $s' \in a_j$, there exists no $s'' \in a_j$ such that $s' \neq s''$. Moreover, for any pair $s, t \in a_i$ ($s \neq t$), if there exist transitions from s to $s' \in a_j$, and from t to $t' \in a_j$, $\Pr(s, s') = \Pr(t, t')$ holds. Therefore, for any $a_i, a_j \in A$, and for any states $s_k, s_l \in a_i$, $\Pr(s_k, a_j) = \Pr(s_l, a_j)$ holds, that is, lumpability is satisfied.

Then, for any pair of quotient states $\overline{s}, \overline{s}'$, transition probability between $\overline{s}$ and $\overline{s}'$ is calculated according to the pseudo code of Fig. 2.

5.2 Experimental Results

Table 2 shows the results of applying probabilistic symmetry reduction comparing to concrete states and transitions. The experiment was repeated for several problem sizes with ratio of ships and slots kept almost stable. If we increased the number of ships more than seven, we could not obtain the results for the following two reasons: (i) We could not obtain the result of a concrete model since PRISM could not produce an output. (ii) We could not obtain the result of a quotient model since PRISM could not load the entire program code of the quotient model.

Table 2 Results of probabilistic symmetry reduction for the AIS, comparing after/before reduction.

	$Shift_\delta$ + *Reverse*		concrete	
ships/slots	states	transitions	states	transitions
3/10	14	87	220	3740
4/13	92	1578	1820	75816
5/16	632	28997	15504	1.6×10^6
6/20	5296	650531	1.8×10^5	4.6×10^7

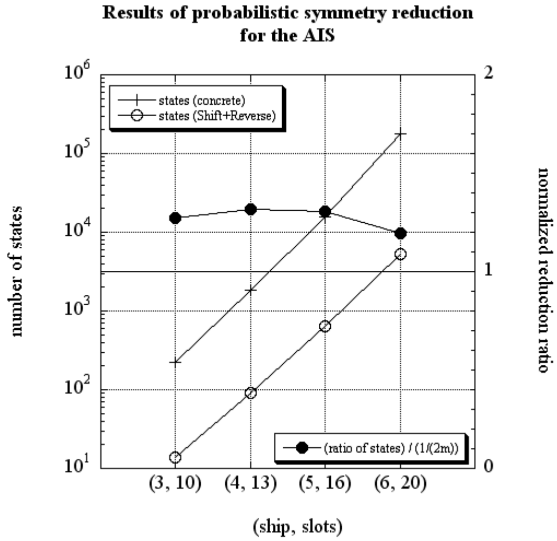


Fig. 8 Reduction ratio of states/transition, and the value for the reduction ratio of states per $1/(2m)$.

5.3 Evaluation

Figure 8 shows the results in Table 2. The X-axis is the numbers of ships/slots and the Y-axis is the number of states. The second Y-axis is the value for the reduction ratio of quotient states per $1/(2m)$ where m is the number of the slots. The normalized reduction ratio is close to 1, which matches the result of the theoretical analysis. The number of ships and the slots increases, the ratio is estimated to converge. Note that the normalized reduction ratio is about 1.2 when m is 3, whereas it is about 2.4 when the number of spins is 6 in the Ising model. This indicates that the $Shift_\delta \circ Reverse$ function acts much more effectively in the AIS.

6. Conclusion

We studied probabilistic symmetry reduction for a system with ring buffer, and described two case studies.

The procedure to construct a quotient model using probabilistic symmetry reduction consists of two steps; i) identifying quotient states and ii) identifying transition probabilities. To identify quotient states, we introduced two functions $Shift_\delta$ and *Reverse* to define symmetries in consideration of structure of a ring buffer. We presented pseudo code to construct a quotient model using these functions and procedures to identify transition probabilities.

Based on the pseudo code, we presented two case studies, the one-dimensional Ising model and the Automatic Identification System (AIS), in which a ring buffer plays an important role. Through these case studies, we showed how the process of probabilistic symmetry reduction works, and evaluated the efficiency of the $Shift_\delta$ and *Reverse* functions. Many systems, not limited to fields of information science, have interactions based on a ring buffer. Therefore, the proposed procedures may easily be applied to them.

Probabilistic symmetry reduction is considered as a preprocessing step in probabilistic model checking. To that end, construction of a quotient model is time-consuming. However, once a quotient model is constructed, it is reusable for verification of existing specifications. The reduced model achieves better performance and enables verification of larger systems.

We hope to extend this study to the analysis of more complicated systems. For example, the two-dimensional Ising model which shows more interesting physical behaviors, such as phase transition. Another example is more practical verification of the AIS in which realistic number of ships are modeled. Further reduction should be required for that purpose. We plan to study combination of our proposed procedures and other abstraction techniques such as predicate abstraction [18], [19].

Acknowledgements

We would like to express our thanks to Hideaki Nishihara in Collaborative Facilities for Verification and Specification, National Institute of Advanced Industrial Science and Technology, for his advice for calculation of probabilistic symmetry reduction.

References

[1] E.M. Clarke, O. Grumberg, and D.A. Peled, Model Checking, The MIT Press, Cambridge, Massachusetts, 1999.

[2] C. Baier and J.P. Katoen, Principles of Model Checking, The MIT Press, 2008.

[3] C.N. Ip and D.L. Dill, "Better verification through symmetry," Formal Methods in System Design, vol.9, no.1/2, pp.41–75, 1996.

[4] E.M. Clarke, S. Jha, R. Enders, and T. Filkorn, "Exploiting symmetry in temporal logic model checking," Formal Methods in System Design, vol.9, no.1/2, pp.77–104, 1996.

[5] P. Godefroid, "Exploiting symmetry when model-checking software," FORTE, IFIP Conference Proceedings, vol.156, pp.257–275, Kluwer, 1999.

[6] T. Sekizawa, T. Tsuchiya, K. Takahashi, and T. Kikuno, "Probabilistic model checking of the one-dimensional Ising model," IEICE Trans. Inf. & Syst., vol.E92-D, no.5, pp.1003–1011, May 2009.

[7] T. Toyoshima and K. Takahashi, "Probabilistic model checking of an automatic identification system," Proc. 13th IASTED International Conference on Software Engineering and Applications, pp.45–52, ACTA Press, Cambridge, Massachusetts, USA, Nov. 2009.

[8] M. Kwiatkowska, G. Norman, and D. Parker, "Symmetry reduction for probabilistic model checking," Proc. 18th International Conference on Computer Aided Verification (CAV'06), Lecture Notes in Computer Science, vol.4114, pp.234–248, Springer-Verlag, Seattle, WA, USA, 2006.

[9] A.F. Donaldson and A. Miller, "Symmetry reduction for probabilistic model checking using generic representatives," ATVA, Lect. Notes Comput. Sci., vol.4218, pp.9–23, Springer, 2006.

[10] E.M. Clarke, E.A. Emerson, S. Jha, and A.P. Sistla, "Symmetry reductions in model checking," Lect. Notes Comput. Sci., vol.1427, pp.147–158, 1998.

[11] A. Hinton, M. Kwiatkowska, G. Norman, and D. Parker, "PRISM: A tool for automatic verification of probabilistic systems," TACAS, LNCS, vol.3920, pp.441–444, Springer, Vienna, Austria, 2006.

[12] J.G. Kemeny and J.L. Snell, Finite Markov Chains, Van Nostrand, Princeton, New Jersey, 1960.

[13] J. Hillston, A Compositional Approach to Performance Modelling, Cambridge University Press, 1996.

[14] P.J. Schweitzer, "A survey of aggregation-disaggregation in large Markov chains," 1st Int. Conf. on the Numerical Solution of Markov Chains, pp.53–80, Jan. 1990.

[15] E. Ising, "Beitrag zur theorie des ferromagnetismus," Zeitschrift für Physik, vol.31, pp.254–258, 1925.

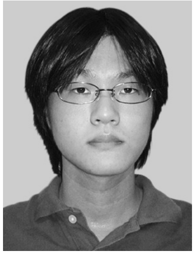
[16] R. Kindermann and L.J. Snell, Markov Random Fields and Their Applications, Amer Mathematical Society, 1980.

[17] Japan Coast Guard, AIS: Universal Ship-Borne Automatic Identification System, 1999.

[18] S. Graf and H. Saïdi, "Construction of abstract state graphs with PVS," 9th International Conference on Computer Aided Verification (CAV), LNCS, vol.1254, pp.72–83, Springer, Haifa, Israel, 1997.

[19] M. Kattenbelt, M. Kwiatkowska, G. Norman, and D. Parker, "Game-based probabilistic predicate abstraction in PRISM," Proc. 6th Workshop on Quantitative Aspects of Programming Languages (QAPL'08), 2008.

Toshifusa Sekizawa received his M.S. degree in physics from Gakushuin University in 1998, and Ph.D. in information science and technology from Osaka University in 2009. He previously worked at Nihon Unisys Ltd., Japan Science and Technology Agency, and National Institute of Advanced Industrial Science and Technology. He is currently working in Osaka Gakuin University. His research interests include model checking and its applications.



Takashi Toyoshima received his B.E. degree from Kwansei Gakuin University in 2008. Currently, he belongs to the graduate School of Science and Technology, Kwansei Gakuin University. He is interested in formal methods and system verification.

Koichi Takahashi received his B.S. and M.S. degrees in mathematics from Nagoya University in 1986 and 1988, and Ph.D. degree in information science from the University of Tokyo in 2002. Since 1988 he has worked at the Electrotechnical Laboratory (currently the National Institute of Advanced Industrial Science and Technology). His research interests include theoretical verifications.

Kazuko Takahashi received the degrees of B.S. and Dr. of Engineering from Kyoto University in 1982 and 1994, respectively. She was a researcher at the Central Research Laboratory and Advanced Technology R&D Center of Mitsubishi Electric Corporation from 1982 to 2000. In 2000, she joined the School of Science, Kwansei Gakuin University as an associate professor. Since 2006, she has been a professor at School of Science & Technology, Kwansei Gakuin University. She is interested in knowledge representation and formal treatment of systems.