Property preservation in Quotient Structures

A. Miller, A. Donaldson
Department of Computing Science
University of Glasgow
Glasgow, Scotland.

April 29, 2008

Abstract

We define a variety of models and their (reduced) quotient structures under symmetry groups. In each case we prove that certain logical properties are preserved by the reduction.

1 Introduction

Model checking [9, 19, 20] is a widely used automatic technique for verifying properties of models of systems. When no notion of probability is required, systems are modeled using finite state machines. Usually these are represented as Kripke structures. When systems have associated probabilistic behaviour (for example when a random backoff is used to avoid collisions in communications protocols) variants of Markov chains are used to model a system. In either case, as the number of components in a system increases, the size of the model representing the system can increase exponentially. This is a phenomenon known as state-space explosion. Various techniques have been developed to try to overcome this problem. One of these methods is symmetry reduction. The most common approach to symmetry reduction is to avoid full state-space exploration by replacing the model with a smaller one in which sets of equivalent states in the original model are replaced by single equivalence class representatives [3, 7, 14]. The resulting smaller structure, known as a quotient structure, can be used to check properties of the system in place of the original model. In this paper we provide proofs
of property preservation for Kripke structures and two probabilistic models, namely Discrete Time Markov Chains and Markov Decision Processes [22]. Our contribution is to provide greater detail for the proof in the case of Kripke structures than has previously appeared in the literature, and to provide full proofs for the Markov chain models for the first time.

In Section 2 we provide some basic definitions that will be used in the rest of the paper. In Section 3 we consider Kripke structures and give definitions, theoretical results and a full proof of property preservation based on similar proofs contained in the literature. In sections 4 and 5 we consider Discrete Time Markov Chains and Markov Decision Processes respectively, providing the associated definitions and theoretical results from the literature. In these cases proof of property preservation has not previously been published.

2 Preliminaries

2.1 State representation

The models we describe in this paper are all based on transition systems [8]. Each model consists of a finite set of states $S$ and transitions between the elements of $S$. The states represent the possible valuations of the set of variables $V$ in the system. More formally, if $V = \{v_1, v_2, \ldots, v_k\}$ is a finite set of system variables, where each $v_i$ ranges over a finite non-empty set $D_i$ of possible values, then $D = D_1 \times D_2 \times \cdots \times D_k$ is the set of all possible system states. We can interpret $S$ simply as $D$ or we can view $S$ as a set of nodes, each with an associated label determining the value of each element of $V$ at that state. (More precisely, determining which of a finite set of atomic propositions are true in that state). In [14] the former interpretation is adopted, and in [7] the latter. In order to simplify our proofs, we have chosen to adopt the former interpretation.

2.2 Group Theory

The symmetries of Kripke structures and Markov chains form a group. Thus our description of symmetry reduction techniques require some definitions from group theory. For more details, see e.g. [21].

Definition 1. A group is a non-empty set $G$ together with a binary operation $\circ : G \times G \to G$ which satisfies:

\begin{itemize}
\item \textbf{ Closure:} $a \circ b \in G$ for all $a, b \in G$.
\item \textbf{ Associativity:} $(a \circ b) \circ c = a \circ (b \circ c)$ for all $a, b, c \in G$.
\item \textbf{ Identity:} There is an element $e \in G$ such that $a \circ e = e \circ a = a$ for all $a \in G$.
\item \textbf{ Inverses:} For each $a \in G$, there exists an element $a^{-1} \in G$ such that $a \circ a^{-1} = a^{-1} \circ a = e$.
\end{itemize}
• For all $\alpha, \beta, \gamma \in G$, $\alpha \circ (\beta \circ \gamma) = (\alpha \circ \beta) \circ \gamma$

• There is an element $id \in G$ such that, for all $\alpha \in G$, $\alpha = id \circ \alpha = \alpha \circ id$.
  The element $id$ is called the identity of $G$.

• For all $\alpha \in G$ there is an element $\beta \in G$ such that $\alpha \circ \beta = \beta \circ \alpha = id$.
  The element $\beta$ is called the inverse of $\alpha$, denoted $\alpha^{-1}$.

In practice, the binary operation $\circ$ is usually composition of mappings, so we omit it, writing $\alpha \beta$ for $\alpha \circ \beta$.

Let $G$ be a group and let $H \subseteq G$. If $\alpha \beta \in H$ for all $\alpha, \beta \in H$ (i.e. $H$ is closed under the binary operation) then $H$ is also a group, and we say that $H$ is a subgroup of $G$, denoted $H \leq G$. If $H \subset G$ then $H$ is a proper subgroup of $G$, denoted $H < G$.

A mapping between two groups which preserves products of elements is called a homomorphism:

**Definition 2.** Let $(G_1, \circ)$, $(G_2, \ast)$ be groups. A homomorphism from $G_1$ to $G_2$ is a mapping $\theta : G_1 \rightarrow G_2$ which satisfies, for all $\alpha, \beta \in G_1$,

$$\theta(\alpha \circ \beta) = \theta(\alpha) \ast \theta(\beta).$$

If $\theta$ is injective then $\theta$ is a monomorphism from $G_1$ to $G_2$. If $\theta$ is bijective then $\theta$ is an isomorphism from $G_1$ to $G_2$, and $G_1$ and $G_2$ are said to be isomorphic, denoted $G_1 \cong G_2$.

Let $X$ be a non-empty set. A permutation of $X$ is a bijection $\alpha : X \rightarrow X$. The set of all permutations of $X$ forms a group under composition on mappings, denoted $Sym(X)$. If $X$ is finite then it can be shown that $|Sym(X)| = X!$.

**Definition 3.** Let $G \leq Sym(X)$ where $X$ is a non-empty set. The group $G$ induces an equivalence relation $\equiv_G$ on $X$ thus: $x \equiv_G y \iff x = \alpha(y)$ for some $\alpha \in G$. The equivalence class under $\equiv_G$ of an element $x \in X$, denoted $[x]_G$, is called the orbit of $x$ under $G$.

### 2.2.1 Group actions on sets

Fundamental to most applications of symmetry reduction in model checking is the idea that a group of permutations of a given set induces a group of permutations on another (usually larger) set. For example, a group of process
identifier permutations naturally induces a group of permutations of the set of states associated with a specification. We describe this idea formally using group actions. The following definition and theorem are adapted from [21].

**Definition 4.** We say that a group $G$ acts on the non-empty set $X$ if to each $x \in G$ and $x \in X$ there corresponds a unique element $\alpha(x) \in X$ and that, for all $x \in X$ and $\alpha, \beta \in G$,

- $(\alpha\beta)(x) = \alpha(\beta(x))$
- $id(x) = x$.

## 3 Kripke Structures

Model checking involves determining whether or not a finite state model describing the behaviour of a concurrent system satisfies a temporal logic formula specifying a desired safety or liveness property of the system. A **Kripke structure** is the common formalism for representing a finite state non-probabilistic model, and temporal logic formulas are usually expressed in (a sub-logic of) $CTL^*$, or the $\mu$-calculus. In this section we only prove results for $CTL^*$, although they can be shown to hold equally for the $\mu$ calculus [14].

Let $V$ and $D$ denote the set of system variables and states, as defined in Section 2.1. A Kripke structure is defined in terms of $D$ as follows:

**Definition 5.** A Kripke structure $\mathcal{M}$ over $D$ is a tuple $\mathcal{M} = (S, S_0, R)$ where:

1. $S = D$ is a non-empty, finite set of states
2. $S_0 \subseteq S$ is a set of initial states
3. $R \subseteq S \times S$ is a transition relation

A path in $\mathcal{M}$ from a state $s \in S$ is an infinite sequence of states $\pi = s_0, s_1, s_2, \ldots$ where $s_0 = s$, such that for all $i > 0$, $(s_{i-1}, s_i) \in R$. For states $s$ and $t$, it is common to denote the transition $(s, t)$ by $s \rightarrow t$. A state $s \in S$ is **reachable** if there is a path $s_0, s_1, \ldots, s, \ldots$ in $\mathcal{M}$ where $s_0 \in S_0$. A transition $(s, t) \in R$ is **reachable** if $s$ is a reachable state.

In this paper we consider only Kripke structures which have a single initial state $s_0 \in S$, and write $\mathcal{M} = (S, s_0, R)$. 

4
3.1 \textit{CTL}\(^*\)

To express properties of Kripke structures we introduce the branching time temporal logic \textit{CTL}\(^*\) [6]. The set of \textit{CTL}\(^*\) state and path formulas are defined inductively over a finite set of propositions over system variables. The quantifiers \textbf{A} and \textbf{E} are used to denote \textit{for all paths}, and for \textit{some path} respectively (where \textbf{E}\(\phi = \neg\textbf{A}\neg\phi\)). In addition, \textbf{X} and \textbf{U} represent the standard \textit{next-time} and \textit{strong until} (see e.g. [15]) operators. Two further operators \textbf{F} and \textbf{G} (eventually and always) are often used as shorthand where \textbf{F}\(\phi = \text{true}\cup\phi\), and \textbf{G}\(\phi = \neg\text{F}\neg\phi\) respectively. Note that we use \(p \Rightarrow q\) to denote \(\neg p \lor q\) in the standard way.

Let \(V\) and \(D_i, (1 \leq i \leq k)\) be as above. Then:

- true, false, \((v_i = d_i)\) and \((v_i \neq d_i)\) (for all \(v_i \in V, d_i \in D_i\)) are state formulas
- if \(\phi\) and \(\psi\) are state formulas, then so are \(\neg\phi, \phi \land \psi\) and \(\phi \lor \psi\)
- if \(\phi\) is a path formula, then \textbf{A}\(\phi\) and \textbf{E}\(\phi\) are state formulas
- any state formula \(\phi\) is also a path formula
- if \(\phi\) and \(\psi\) are path formulas, then so are \(\neg\phi, \phi \land \psi\) and \(\phi \lor \psi, \textbf{X}\phi\) and \(\phi \cup \psi\).

Given (path or state) formulas \(\phi\) and \(\psi, \psi\) is a sub-formula of \(\phi\), written \(\psi \subseteq \phi\), if either \(\psi = \phi\), \(\psi\) is an operand to one of the operators appearing in \(\phi\), or \(\psi\) is bound to a quantifier appearing in \(\psi\). The sub-formula \(\psi\) is propositional if it is a state formula which does not include \textbf{A}, \textbf{E}, \textbf{bF}, \textbf{U}. A maximal propositional sub-formula of \(\phi\) is a propositional sub-formula \(\psi\) such that if \(\psi \subseteq \psi' \subseteq \phi\), where \(\psi'\) is also a propositional sub-formula, then \(\psi = \psi'\).

The logic \textit{CTL}\(^*\) is the set of all state formulas. For a Kripke structure \(\mathcal{M}\), if the \textit{CTL}\(^*\) formula \(\phi\) holds at a state \(s \in S\) then we write \(\mathcal{M}, s \models \phi\) (or simply \(s \models \phi\) when the identity of the model is clear from the context). Otherwise we write \(\mathcal{M}, s \not\models \phi\). The relation \(\models\) is defined inductively below. Note that for a path \(\pi = s_0, s_1, \ldots\) we define \textit{first}(\(\pi\)) = \(s_0\) and, for all \(i \geq 0\), \(\pi_i\) is the suffix of \(\pi\) starting from state \(s_i\).

- \(s \models \text{true}\), and \(s \not\models \text{false}\)
\begin{itemize}
  \item $s \models (v_i = d_i)$ if and only if $s = (e_1, e_2, \ldots, e_k)$ and $e_i = d_i$
  \item $s \models (v_i \neq d_i)$ if and only if $s = (e_1, e_2, \ldots, e_k)$ and $e_i \neq d_i$
  \item $s \models \neg \phi$ if and only if $s \not\models \phi$
  \item $s \models \phi \land \psi$ if and only if $s \models \phi$ and $s \models \psi$
  \item $s \models \phi \lor \psi$ if and only if $s \models \phi$ or $s \models \psi$
  \item $s \models \text{A} \phi$ if and only if $\pi \models \phi$ for every path $\pi$ starting at $s$
  \item $s \models \text{E} \phi$ if and only if $\pi \models \phi$ for some path $\pi$ starting at $s$
  \item $\pi \models \phi$, for any state formula $\phi$, if and only if $\text{first}(\pi) \models \phi$
  \item $\pi \models \neg \phi$ if and only if $\pi \not\models \phi$
  \item $\pi \models \phi \land \psi$ if and only if $\pi \models \phi$ and $\phi \models \psi$
  \item $\pi \models \phi \lor \psi$ if and only if $\pi \models \phi$ or $\pi \models \psi$
  \item $\pi \models \phi \text{U} \psi$ if and only if, for some $i \geq 0$, $\pi_i \models \psi$ and $\pi_j \models \phi$ for all $0 \leq j < i$
  \item $\pi \models \text{X} \phi$ if and only if $\pi_1 \models \phi$
  \item $\pi \models \text{F} \phi$ if and only if $\pi_i \models \phi$, for some $i \geq 0$
  \item $\pi \models \text{G} \phi$ if and only if $\pi_i \models \phi$, for all $i \geq 0$
\end{itemize}

Given $\mathcal{M} = (S, s_0, R)$, if $\pi_s$ is a path starting from any state $s \in S$, then we say that $\mathcal{M}, \pi_s \models \phi$ if and only if $\mathcal{M}_s, \pi_s \models \phi$, where $\mathcal{M}_s = (S, s, R)$.

### 3.2 Quotient Kripke Structures

**Definition 6.** Let $\mathcal{M} = (S, s_0, R)$ be a Kripke structure. An automorphism of $\mathcal{M}$ is a permutation $\alpha : S \to S$ which preserves the transition relation and initial state. That is $\alpha$ satisfies the following conditions:

1. For all $s, t \in S$, $(s, t) \in R \Rightarrow (\alpha(s), \alpha(t)) \in R$
2. $\alpha(s_0) = s_0$. 
The set of all automorphisms of a Kripke structure $\mathcal{M}$ forms a group under composition of mappings, denoted $Aut(\mathcal{M})$.

Given a subgroup $G$ of $Aut(\mathcal{M})$, the orbits of $S$ under $G$ (see Definition 3) can be used to construct a quotient Kripke structure $\mathcal{M}_G$ as follows:

**Definition 7.** Let $\mathcal{M} = (S, s_0, R)$ be a Kripke structure and $G$ an automorphism group of $\mathcal{M}$. The quotient structure $\mathcal{M}_G$ of $\mathcal{M}$ with respect to $G$ is a tuple $\mathcal{M}_G = (S_G, s_G^0, R_G)$ where:

- $S_G = \{ rep_G(s) : s \in S \}$, where $rep_G(s)$ is a unique representative of $|s|_G$,
- $s_G^0 = rep_G(s_0) = s_0$,
- $R_G = \{(rep_G(s), rep_G(t)) : (s, t) \in R\}$.

Note that we are not concerned here with how $rep_G(s)$ is chosen. That is the subject of other papers [3, 5, 10, 11]. We also insist on a single representative being selected for each orbit, and do not allow for the use of *multiple representatives*, unlike other approaches (e.g. [7]).

If $G$ is non-trivial then the quotient structure $\mathcal{M}_G$ is smaller than $\mathcal{M}$. For any $s \in S$, the size of $|s|_G$ is bounded by $|G|$, and so the theoretical minimum size of $S_G$ is $|S|/|G|$. Since for highly symmetric systems we may have $|G| = n!$, where $n$ is the number of components, symmetry reduction potentially offers a considerable reduction in memory requirements.

The following lemma (adapted from [14]) shows that, for a model $\mathcal{M}$ and automorphism group $G$ there is a correspondence between the paths of $\mathcal{M}$ and $\mathcal{M}_G$. Similar results appear in [7] and [4].

**Lemma 1.** *(Correspondence lemma)* There is a bidirectional correspondence between paths of $\mathcal{M}$ and of the quotient structure $\mathcal{M}_G$ for any group of automorphisms $G$ of $\mathcal{M}$:

(i) If $\pi = s_0, s_1, \ldots$ is a path in $\mathcal{M}$ then $\bar{\pi} = rep_G(s_0), rep_G(s_1), \ldots$ is a path in $\mathcal{M}_G$.

(ii) If $\bar{\pi} = \bar{s}_0, \bar{s}_1, \ldots$ is a path in $\mathcal{M}_G$ then there exists a corresponding path $\pi' = s_0', s_1', \ldots$ in $\mathcal{M}$, where $s_0' = s_0$ and, for $i \geq 1$, $s_i' \in [\bar{s}_i]_G$. 

7
Proof. (i) Follows from the definition of $R_G$.
(ii) Let $s_0, s_1, \ldots, s_n$ be the path prefix of $\pi$ of length $n$. If we can show that for any $n \geq 0$ there is a path prefix of length $n$ in $M$ corresponding to the path prefix of length $n$ of $\pi$ then we are done. We proceed by induction on $n$. First note that Definition 7 implies that, if $\bar{s}_i \rightarrow \bar{s}_j$ in $M_G$ then, for all $\alpha \in G$, $\alpha(\bar{s}_i) \rightarrow \alpha(\bar{s}_j)$ in $M$.

The case $n = 0$ is trivial so we first consider $n = 1$. Now, since $s_0 = s_0$, $s_0, \bar{s}_1$ is the path prefix of length 1 of $\pi$. It follows that $\bar{s}_1 = rep_G(s'_1)$ for some $s'_1 \in S$ where $s_0 \rightarrow s'_1$ in $M$. So $s_0, s'_1$ is a corresponding path prefix of length 1 in $M$.

Suppose that we have shown that, for $k \geq 1$, there is a path prefix $s'_0, s'_1, \ldots, s'_k$ in $M$ corresponding to the path prefix $\bar{s}_0, \bar{s}_1, \ldots, \bar{s}_k$ of $\pi$. Then $s'_k \in [\bar{s}_k]_G$ and so, for some $\beta \in G$, $\bar{s}_k = \beta(s'_k)$. Let $\alpha = \beta^{-1}$. Then, since $\bar{s}_k \rightarrow \bar{s}_{k+1}$ in $M_G$ it follows that $\alpha(\bar{s}_k) \rightarrow \alpha(\bar{s}_{k+1})$ in $M$. If we let $s'_{k+1} = \alpha(\bar{s}_{k+1})$ then, since $s'_k = \alpha(\bar{s}_k)$, we have shown that there is a transition $s'_k \rightarrow s'_{k+1}$ where $s'_k \in [\bar{s}_k]_G$ and $s'_{k+1} \in [\bar{s}_{k+1}]_G$. Thus there is a path prefix $s'_0, s'_1, \ldots, s'_{k+1}$ in $M$ corresponding to the path prefix $\bar{s}_0, \bar{s}_1, \ldots, \bar{s}_{k+1}$ of $\pi$. It follows by induction that, for any $n \geq 1$, there is a path prefix of length $n$ in $M$ corresponding to the path prefix of length $n$ of $\pi$. $\square$

An equivalent result holds for paths $\pi_s$ starting from any state $s$.

Corollary 1.

(i) If $\pi_s = s, s_1, \ldots$ is a path in $M$ then $\bar{\pi} = rep_G(s), rep_G(s_1), \ldots$ is a path in $M_G$.

(ii) If $\bar{\pi} = \bar{s}, \bar{s}_1, \ldots$ is a path in $M_G$ then there exists a corresponding path $\pi' = s', s'_1, \ldots$ in $M$, where $s' \in [\bar{s}]_G$ and, for $i \geq 1$, $s'_i \in [\bar{s}_i]_G$.

It can be shown [7, 14] (see Theorem 1 below) that a model and its quotient model satisfy the same symmetric $CTL^*$ formulas. A $CTL^*$ formula $\phi$ is symmetric, or invariant, with respect to $G$ if for every maximal propositional sub-formula $f$ appearing in $\phi$ (see Section 3.1), and for every $\alpha \in G$, $M, s \models f \iff M, \alpha(s) \models f$.

Theorem 1. If $M$ and $M_G$ denote a model and its quotient model with respect to a group $G$ respectively, then $M, s \models \phi \iff M_G, rep_G(s) \models \phi$, for every symmetric $CTL^*$ formula $\phi$. 

8
We follow the proofs of Theorem 1 from [7, 14]. Note that we use an automorphism group $G$ of $\mathcal{M}$ that is an invariance group for the maximal propositional subformulas of $\phi$. In [7] $G$ is more restricted: it must be an invariance group for the atomic propositions appearing in $\phi$. In [14] $G$ is chosen to be slightly more general than the group we use. (In fact, our group is exactly that of [13], a precursor to [13].)

Theorem 1 follows directly from the following lemma, the proof of which is similar to the proof of a more general result from [4]. Note that Lemma 2 extends Theorem 1 to path formulas, which allows one to use induction over the length of the formula.

**Lemma 2.** Let $\mathcal{M} = (S, s_0, R)$ be a Kripke structure, $G$ an automorphism group of $\mathcal{M}$ and $\phi$ a symmetric $CTL^*$ formula. Let $\pi = s, s_1, \ldots$ be a path in $\mathcal{M}$ and $\bar{\pi} = rep_G(s), rep_G(s_1), \ldots$ a corresponding path in $\mathcal{M}_G$. Then

- $\mathcal{M}, s \models \phi \iff \mathcal{M}_G, rep_G(s) \models \phi$ if $\phi$ is a state formula, and
- $\mathcal{M}, \pi \models \phi \iff \mathcal{M}_G, \bar{\pi} \models \phi$, if $\phi$ is a path formula.

In order to simplify the proof of Lemma 2 we introduce the following intermediate lemma:

**Lemma 3.** If $\mathcal{M}, \mathcal{M}_G$ and $\phi$ are as for Lemma 2 and $\phi$ is a state formula, then if the first part of Lemma 2 holds, so does the second.

**Proof.** If $\mathcal{M}, \pi \models \phi$ then, since $\phi$ is a state formula, $\mathcal{M}, s \models \phi$. As $\phi$ is symmetric and the first part of Lemma 2 holds, $\mathcal{M}_G, rep_G(s) \models \phi$. Thus $\mathcal{M}_G, \bar{\pi} \models \phi$. \qed

**Proof.** (of Lemma 2) Let $\text{count}(\phi)$ denote the number of occurrences in $\phi$ of symbols from $\{U, X, A, E\}$. We proceed by induction on the value of $\text{count}(\phi)$. In all cases we prove the result in one direction only, as due to the bidirectionality of the Correspondence Lemma (Lemma 1), the proof of the converse similar.

If $\text{count}(\phi) = 0$ then $\phi$ is a propositional formula. Since $\phi$ is symmetric, it follows that, for any $s$, $\mathcal{M}, s \models \phi \iff \mathcal{M}_G, rep_G(s) \models \phi$. From Lemma 3 $\mathcal{M}, \pi \models \phi \iff \mathcal{M}_G, \bar{\pi} \models \phi$.

Suppose that $\text{count}(\phi) = N$, where $N > 0$ and that the result holds for all formulas $h$ for which $\text{count}(h) < N$. If $\phi$ is a state formula then $\phi = E \psi$ or $A \psi$ for some path formula $\psi$ and, again by Lemma 3 we need only prove that, for any $s$, $\mathcal{M}, s \models \phi \iff \mathcal{M}_G, rep_G(s) \models \phi$.

9
If $\phi = \mathbf{E}\psi$ then, since $\phi$ is symmetric, $\psi$ is. If $\mathcal{M}, s \models \phi$, for some path $\pi_s$ in $\mathcal{M}$ starting at $s$, $\psi$ holds. By Corollary 1 there is an equivalent path $\tilde{\pi}$ starting at $\text{rep}_G(s)$. By the induction hypothesis $\psi$ holds for $\tilde{\pi}$ and so $\mathcal{M}_G \models \phi$.

If $\phi = \mathbf{A}\psi$ then again $\psi$ is symmetric. If $\mathcal{M}, s \models \phi$ then all paths in $\mathcal{M}$ starting at $s$ satisfy $\psi$. Suppose that there exists a path in $\mathcal{M}_G$ starting at $\text{rep}_G(s)$ that does not satisfy $\psi$. Then from the induction hypothesis there is a path from $s$ in $\mathcal{M}$ that does not satisfy $\psi$, which is impossible.

Suppose that $\phi$ is a path formula and not a state formula. Then one of the following is true:

1. $\phi = \psi_1 \mathbf{U} \psi_2$ for symmetric formulas $\psi_1$ and $\psi_2$.

2. $\phi = \mathbf{X} \psi_1$ for symmetric formula $\psi_1$.

3. $\phi$ is a boolean combination of symmetric formulas $\psi_i$, for $2 \leq i \leq n$.

If $\phi = \psi_1 \mathbf{U} \psi_2$ and $\mathcal{M}, \pi \models \phi$ then either $\mathcal{M}, s \models \psi_2$ or, for some $r \geq 1$ $\mathcal{M}, s \models \psi_1$, $\mathcal{M}, s_i \models \psi_1$ for $1 \leq i < r$ and $\mathcal{M}, s_r \models \psi_2$. Since $\text{count}(\psi_1) < N$ and $\text{count}(\psi_2) < N$ it follows from the induction hypothesis that correspondingly $\mathcal{M}, \text{rep}_G(s) \models \psi_2$ or, for some $r \geq 1$ $\mathcal{M}, \text{rep}_G(s) \models \psi_1$, $\mathcal{M}, \text{rep}_G(s_i) \models \psi_1$ for $1 \leq i < r$ and $\mathcal{M}, \text{rep}_G(s_r) \models \psi_2$. In each case this means that $\mathcal{M}_G, \tilde{\pi} \models \psi_1 \mathbf{U} \psi_2$, i.e. $\mathcal{M}_G, \tilde{\pi} \models \phi$.

If $\phi = \mathbf{X} \psi_1$ and $\mathcal{M}, \pi \models \phi$ then $\mathcal{M}, s_1 \models \psi_1$. From the induction hypothesis it follows that $\mathcal{M}_G, \text{rep}_G(s_1) \models \psi_1$, and so $\mathcal{M}_G, \tilde{\pi} \models \phi$.

If $\phi$ is a boolean combination of symmetric formulas $\psi_i$, for $2 \leq i \leq n$ then $\phi$ is a boolean combination of $P$, a (maximal) boolean combination of propositional formulas, and formulas $f_1, f_2, \ldots, f_r$, say, which are not propositional. That is, $\phi = b(P, f_1, \ldots, f_r)$. Since $\text{count}(\phi) = N$, either (i) $\text{count}(f_i) < N$ for $1 \leq i \leq r$ or (ii) $r = 1$ and $\text{count}(f_1) = N$. In the first case,

$$\mathcal{M}, \pi \models \phi \iff \mathcal{M}, \pi \models P, \mathcal{M}, \pi \models f_1, \ldots, \mathcal{M}, \pi \models f_r.$$

In the second case, $f_1$ has one of the forms discussed above, and so we have
already shown that $\mathcal{M}, \pi \models f_1 \iff \mathcal{M}_G, \pi \models f_1$. Hence,
\[
\begin{align*}
\mathcal{M}, \pi \models \phi & \iff b(\mathcal{M}, \pi \models P, \mathcal{M}, \pi \models f_1) \\
& \iff b(\mathcal{M}_G, \pi \models P, \mathcal{M}_G, \pi \models f_1) \\
& \iff \mathcal{M}_G, \pi \models \phi
\end{align*}
\]

Since, by Condition 2 of Definition 6, the initial states of $\mathcal{M}$ are preserved by $G$, we have the following corollary:

**Corollary 2.** With the same conditions as Theorem 1, $\mathcal{M} \models \phi \iff \mathcal{M}_G \models \phi$.

## 4 Discrete Time Markov Chains

Probabilistic model checking requires a system to be modelled using a probabilistic model. The probabilistic models we discuss in this paper are variants of Markov chains, namely Discrete Time Markov Chains (DTMCs) and Markov Decision Processes (MDPs). In this section we state and prove results concerning quotients of DTMCs. We prove similar results for MDPs in Section 5.

A DTMC [22] can be viewed as a state transition system in which transitions correspond to discrete time steps and have associated probabilities. A DTMC satisfies the *Markovian* property: the choice of a transition to a new state is only determined by the current state.

As for Definition 5, we let $V = \{v_1, v_2, \ldots, v_k\}$ be the finite set of system variables, where each $v_i$ ranges over a finite non-empty set $D_i$ of possible values. Then $D = D_1 \times D_2 \times \cdots \times D_k$ is the set of all possible system states. A DTMC $\mathcal{D}$ is defined in terms of $D$ as follows:

**Definition 8.** A Discrete Time Markov Chain $\mathcal{D}$ is a tuple $\mathcal{D} = (S, S_0, P)$, where:

1. $S = D$ is a non-empty, finite set of states
2. $S_0 \subseteq S$ is a set of initial states
3. $P : S \times S \rightarrow [0, 1]$ is a transition probability matrix such that, for all states $s \in S$, $\sum_{s' \in S} P(s, s') = 1$. 

Note that, for states \( s \) and \( s' \), \( P(s, s') \) is the probability of making a transition from state \( s \) to state \( s' \).

As before, we only consider the case where there is a single initial state, and write \( \mathcal{D} = (S, s_0, P) \). A path \( \omega \) in DTMC \( \mathcal{D} \) from a state \( s \in S \) is an infinite sequence of states \( \omega = s_0, s_1, s_2, \ldots \) where \( s_0 = s \), such that for all \( i > 0 \), \( P(s_{i-1}, s_i) > 0 \). We denote the transition \((s, t) \) by \( s \rightarrow t \) and say that state \( s \in S \) is reachable if there is a path \( s_0, s_1, \ldots, s, \ldots \) in \( \mathcal{D} \). The \( i \)th state of path \( \omega \) is denoted \( \omega(i) \).

### 4.1 PCTL

For a state \( s \), \( \text{Path}^*_{s} \) and \( \text{Path}_s \) denote the sets of all finite and infinite paths starting from \( s \). In order to quantify the probability that a DTMC satisfies a given property, we define, for each state \( s \in S \), a probability measure \( \text{Prob}_s \) over \( \text{Path}_s \) (following [22]). First we give some definitions for finite paths.

**Definition 9.** For any finite path \( \omega_{\text{fin}} \in \text{Path}^*_s \),

1. the probability \( P_s(\omega_{\text{fin}}) \) is given by
   \[
P_s(\omega_{\text{fin}}) = \begin{cases} 
   1 & \text{if } n = 0 \\
   P(\omega(0), \omega(1)) \times \ldots \times P(\omega(n-1), \omega(n)) & \text{otherwise}
   \end{cases}
\]
   where \( n = |\omega_{\text{fin}}| \).

2. The cylinder set \( C(\omega_{\text{fin}}) \) of \( \omega_{\text{fin}} \) is the set of infinite paths \( \omega \) with prefix \( \omega_{\text{fin}} \).

The probability measure \( \text{Prob}_s \) is defined to be the unique measure (see [16] for details) such that \( \text{Prob}_s(C(\omega_{\text{fin}})) = P_s(\omega_{\text{fin}}) \) for all \( \omega_{\text{fin}} \in \text{Path}^*_s \).

To express properties of DTMCs we introduce the probabilistic branching time logic PCTL [22] which is a sublogic of PCTL* [1]. The set of PCTL state and path formulas are defined inductively over a finite set of propositions over system variables. Note that, for \( \infty \in \{\leq, <, \geq, >\} \), a state \( s \) satisfies \( P_{s\in\infty}[\psi] \) if the probability of taking a path from \( s \) satisfying \( \psi \) is in the interval specified by \( \infty \) (see Definition 9). In addition to the standard next-time and strong until operators \( X \) and \( U \), we also allow the bounded until operator \( U^{\leq k} \). We say that \( \phi_1 U^{\leq k} \phi_2 \) is true if \( \phi_1 \phi_2 \) and \( \phi_2 \) is satisfied within \( k \) time steps. Then:
true, false, \(v_i = d_i\) and \(v_i \neq d_i\) (for all \(v_i \in V, d_i \in D_i\)) are state formulas

- if \(\phi\) and \(\psi\) are state formulas, then so are \(\neg \phi, \phi \land \psi\) and \(\phi \lor \psi\)

- if \(\phi\) is a path formula, then \(P_{\text{exp}}[\phi]\) is a state formula for any \(\propto \in \{\leq, <, \geq, >\}\)

- any state formula \(\phi\) is also a path formula

- if \(\phi\) and \(\psi\) are state formulas, then \(X\phi, \phi U \psi\) and \(\phi U^{\leq k} \psi\) are path formulas.

A maximal propositional sub-formula of (path or state) \(PCTL\) formula is defined analogously to that for \(CTL^*\).

The logic \(PCTL\) is the set of all state formulas. For a DTMC \(D\), if the \(PCTL\) formula \(\phi\) holds at a state \(s \in S\) then we write \(D, s \models \phi\) (or simply \(s \models \phi\) when the identity of the model is clear from the context). Otherwise we write \(D, s \not\models \phi\). The relation \(\models\) is defined inductively below. Note that, for a path formula \(\psi\) and state \(s, p_s(\psi)\) is defined as \(\text{Prob}_s(\{\omega \in \text{Path}_s : \omega \models \psi\})\) where \(\text{Prob}_s\) is the probability measure on \(\Sigma_s\) defined in Definition 9.

- \(s \models \text{true}\), and \(s \not\models \text{false}\)

- \(s \models (v_i = d_i)\) if and only if \(s = (e_1, e_2, \ldots, e_k)\) and \(e_i = d_i\)

- \(s \models (v_i \neq d_i)\) if and only if \(s = (e_1, e_2, \ldots, e_k)\) and \(e_i \neq d_i\)

- \(s \models \neg \phi\) if and only if \(s \not\models \phi\)

- \(s \models \phi \land \psi\) if and only if \(s \models \phi\) and \(s \models \psi\)

- \(s \models \phi \lor \psi\) if and only if \(s \models \phi\) or \(s \models \psi\)

- \(s \models P_{\text{exp}}[\psi]\) if and only if \(p_s(\psi) \propto p\)

- \(\omega \models X\phi\) if and only if \(\omega(1) \models \phi\)

- \(\omega \models \phi U^{\leq k} \psi\) if and only if for some \(i \leq k, \omega(i) \models \psi\) and \(\omega_j \models \phi\) for all \(0 \leq j < i\)

- \(\omega \models \phi U \psi\) if and only if for some \(k \geq 0, \omega \models \phi U^{\leq k} \psi\).

Given \(D = (S, s_0, P)\), if \(\omega_s\) is a path starting from any state \(s \in S\), then we say that \(D, \omega_s \models \phi\) if and only if \(D_s, \omega_s \models \phi\), where \(D_s = (S, s, P)\).
4.2 Quotient DTMCs

**Definition 10.** Let $\mathcal{D} = (S, s_0, P)$ be a DTMC. An automorphism of $\mathcal{D}$ is a permutation $\alpha : S \rightarrow S$ which preserves the initial state and is such for all $s, t \in S$, $P(s, t) = P'(\alpha(s), \alpha(t))$.

The set of all automorphisms forms a group under composition, denoted $Aut(\mathcal{D})$ and a subgroup of this group induces orbits on the state space as before. A quotient DTMC [17] can be defined analogously to the non-probabilistic case:

**Definition 11.** Let $\mathcal{D} = (S, s_0, P)$ be a DTMC and $G$ an automorphism group of $\mathcal{D}$. The quotient DTMC of $\mathcal{D}$ with respect to $G$ is a tuple $\mathcal{D}_G = (S_G, s^0_G, P_G)$ where

- $S_G = \{ \text{rep}_G(s) : s \in S \}$, where $\text{rep}_G(s)$ is a unique representative of $\bar{s}_G$
- $s^0_G = \text{rep}_G(s_0)$
- $P_G(\text{rep}_G(s), \text{rep}_G(t)) = \sum_{x \in [\bar{t}]} P(\text{rep}_G(s), x)$.

We adapt the proofs of results on probabilistic bisimulation [18, 1] to show that, as in the non-probabilistic case, the quotient models preserve the truth of temporal properties which are invariant under symmetry. First we prove an analogous result to the Correspondence Lemma (Lemma 1):

**Lemma 4.** (Probabilistic Correspondence Lemma) There is a bidirectional correspondence between paths of $\mathcal{D}$ and of the quotient structure $\mathcal{D}_G$ for any group of automorphisms $G$ of $\mathcal{D}$:

(i) If $\omega = s_0, s_1, \ldots$ is a path in $\mathcal{D}$ then $\bar{\omega} = \text{rep}_G(s_0), \text{rep}_G(s_1), \ldots$ is a path in $\mathcal{D}_G$.

(ii) If $\bar{\omega} = \bar{s}_0, \bar{s}_1, \ldots$ is a path in $\mathcal{D}_G$ then there exists a corresponding path $\omega' = s'_0, s'_1, \ldots$ in $\mathcal{D}$, where $s'_0 = s_0$ and, for $i \geq 1$, $s'_i \in [\bar{s}_i]|_G$.

**Proof.** (i) For $i > 0$ there is some $\alpha \in G$ such that $\text{rep}_G(s_{i-1}) = \alpha(s_{i-1})$. Since $\alpha \in G$ and $P(s_{i-1}, s_i) > 0$, $P(\alpha(s_{i-1}), \alpha(s_i)) > 0$. In $\mathcal{D}_G$

$$
P_G(\text{rep}_G(s_{i-1}), \text{rep}_G(s_i)) = P_G(\alpha(s_{i-1}), \text{rep}_G(s_i)) \\
\geq P(\alpha(s_{i-1}), \alpha(s_i)) \\
> 0
$$
Since $P_G(\text{rep}_G(s_{i-1}), \text{rep}_G(s_i)) > 0$ for all $i > 0$, $\bar{\omega} = \text{rep}_G(s_0), \text{rep}_G(s_1), \ldots$ is a path in $D_G$.

(ii) Let $\bar{s}_0, \bar{s}_1, \ldots, \bar{s}_n$ be the path prefix of $\bar{\omega}$ of length $n$. If we can show that for any $n \geq 0$ there is a path prefix of length $n$ in $D$ corresponding to the path prefix of length $n$ of $\bar{\omega}$ then we are done. We proceed by induction on $n$. First note that if $P_G(\bar{s}, t) > 0$ in $D_G$ then, for some $\beta \in G$ $P(\bar{s}, \beta(t)) > 0$ in $D$.

The case $n = 0$ is trivial so we first consider $n = 1$. Now, since $\bar{s}_0 = s_0$, $s_0, \bar{s}_1$ is the path prefix of length 1 of $\bar{\omega}$ so $P_G(s_0, \bar{s}_1) > 0$ and for some $\beta \in G$, $P(s_0, \beta(\bar{s}_1)) > 0$ in $D$. If we let $s'_1 = \beta(\bar{s}_1)$, then $s_0, s'_1$ is a path prefix in $D$, where $s'_1 \in [\bar{s}_1]_G$.

Suppose that we have shown that, for $k \geq 1$, there is a path prefix $s'_0, s'_1, \ldots, s'_k$ in $D$ corresponding to the path prefix $\bar{s}_0, \bar{s}_1, \ldots, \bar{s}_k$ of $\bar{\omega}$. Then $s'_k \in [\bar{s}_k]_G$ and so, for some $\alpha \in G$, $\bar{s}_k = \alpha(s'_k)$. Since $P(\bar{s}_k, \bar{s}_{k+1}) > 0$ in $D_G$ it follows that $P(s_k, \beta(\bar{s}_{k+1})) > 0$ in $D$ for some $\beta \in G$. Therefore $P(\alpha^{-1}(\bar{s}_k), \alpha^{-1}(\beta(\bar{s}_{k+1}))) > 0$ in $D$. If we let $s'_{k+1} = \alpha^{-1}(\beta(\bar{s}_{k+1})$ then $s'_0, s'_1, \ldots, s'_{k+1}$ is a path prefix of $D$ of length $k + 1$ where $s'_{k+1} \in [\bar{s}_{k+1}]_G$. \hfill \Box

As for the non-probabilistic case, an equivalent result holds for paths $\omega_s$ starting from any state $s$.

**Corollary 3.**

(i) If $\omega = s, s_1, \ldots$ is a path in $D$ then $\bar{\omega} = \text{rep}_G(s), \text{rep}_G(s_1), \ldots$ is a path in $D_G$.

(ii) If $\bar{\omega} = \bar{s}, \bar{s}_1, \ldots$ is a path in $D_G$ then there exists a corresponding path $\omega' = s', s'_1, \ldots$ in $D$, where $s' \in [\bar{s}]_G$ and, for $i \geq 1$, $s'_i \in [\bar{s}_i]_G$.

It has been stated [17, 12] that a DTMC and its quotient satisfy the same symmetric PCTL formulas. We define symmetric PCTL formulas analogously to symmetric CTL* formulas. That is, a PCTL formula $\phi$ is symmetric, or invariant, with respect to $G$ if for every maximal propositional sub-formula $f$ appearing in $\phi$, and for every $\alpha \in G$, $D, s \models f \iff D, \alpha(s) \models f$.

**Theorem 2.** If $D$ and $D_G$ denote a DTMC and its quotient model with respect to group $G$ respectively, then $D, s \models \phi \iff D_G, \text{rep}_G(s) \models \phi$, for every symmetric PCTL formula $\phi$. 

15
To our knowledge, the proof of this result has not been presented before. Here we prove Theorem 2 by following the proof of Theorem 1 (the corresponding non-probabilistic theorem) as far as possible. We also draw on the techniques used for proving PCTL equivalence of bisimilar DTMCs [1].

Proof of Theorem 2 follows directly from the following lemma, which is directly analogous to Lemma 2.

**Lemma 5.** Let \( D \) be a DTMC, \( G \) an automorphism group of \( D \) and \( \phi \) a symmetric PCTL formula. Let \( \omega = s, s_1, \ldots \) be a path in \( D \) and \( \bar{\omega} = rep_G(s), rep(s_1), \ldots \) a corresponding path in \( D_G \). Then

(i) \( D, s \models \phi \iff D_G, rep_G(s) \models \phi \), if \( \phi \) is a state formula, and

(ii) \( D, \omega \models \phi \iff D_G, \bar{\omega} \models \phi \), if \( \phi \) is a path formula.

(iii) If \( \phi \) is a path formula, \( Prob_s\{\omega \in D : \omega(0) = s \land \omega \models \phi\} = Prob_{rep_G(s)}\{\bar{\omega} \in D_G : \bar{\omega}(0) = rep_G(s) \land \bar{\omega} \models \phi\} \)

In order to simplify the proof of Lemma 5 we introduce the following intermediate lemma:

**Lemma 6.** If \( D, D_G \) and \( \phi \) are as for Lemma 5 and \( \phi \) is a state formula, then if (i) of Lemma 5 holds, so does (ii).

**Proof.** If \( D, \omega \models \phi \) then, since \( \phi \) is a state formula, \( D, s \models \phi \). Since \( \phi \) is symmetric and (i) of Lemma 5 holds, \( D_G, rep_G(s) \models \phi \). Thus \( D_G, \bar{\omega} \models \phi \). \[ \square \]

**Proof.** (of Lemma 5) Let \( count(\phi) \) denote the number of occurrences of \( \phi \) of symbols from \( \{P_{\text{rep}}, U^{\leq k}, U, X\} \). We proceed by induction on the value of \( count(\phi) \). In all cases we prove the result in one direction only, as due to the bidirectionality of the probabilistic Correspondence Lemma (Lemma 4), the proof of the converse is similar.

If \( count(\phi) = 0 \) then \( \phi \) is a propositional formula. Since \( \phi \) is symmetric, it follows that, for any \( s, D, s \models \phi \iff D_G, rep_G(s) \models \phi \). From Lemma 6 \( D, \omega \models \phi \iff D_G, \bar{\omega} \models \phi \). Part (iii) holds trivially as the corresponding sets of paths are the complete set of paths from \( s \) and \( rep_G(s) \) respectively so have measure 1.

Suppose that \( count(\phi) = N \), where \( N > 0 \) and that the result holds for all formulas \( h \) for which \( count(h) < N \). If \( \phi \) is a state formula then \( \phi = P_{\text{rep}}[\psi] \) for path formula \( \psi \). If \( s, D \models \phi \) then \( Prob_s\{\omega \in D : \omega(0) = s \land \omega \models \phi\} \propto p \).
Since \( \text{length}(\psi) < N \), from the induction hypothesis part (iii), it follows that
\[
\text{Prob}_{\text{rep}_G(s)}\{\bar{\omega} \in \mathcal{D}_G : \bar{\omega}(0) = \text{rep}_G(s) \land \bar{\omega} \models \phi \} = \text{Prob}_s\{\omega \in \mathcal{D} : \omega(0) = s \land \omega \models \phi \} \gg p.
\]
Thus \( \mathcal{D}_G, \text{rep}_G(s) \models \phi \).

Suppose that \( \phi \) is a path formula and not a state formula. Then one of the following is true:

1. \( \phi = \psi_1 \mathbf{U}^k \psi_2 \) for symmetric formulas \( \psi_1 \) and \( \psi_2 \)
2. \( \phi = \psi_1 \mathbf{U} \psi_2 \) for symmetric formulas \( \psi_1 \) and \( \psi_2 \)
3. \( \phi = \mathbf{X} \psi_1 \) for symmetric formula \( \psi_1 \).

If \( \phi = \mathbf{X} \psi_1 \) and \( \mathcal{D}, \omega \models \phi \) then \( \mathcal{D}, s_1 \models \psi_1 \). From the induction hypothesis it follows that \( \mathcal{D}_G, \text{rep}_G(s_1) \models \psi_1 \), and so \( \mathcal{D}_G, \bar{\omega} \models \phi \).

Now
\[
\text{Prob}_s\{\omega \in \mathcal{D} : \omega(0) = s \land \omega \models \mathbf{X} \psi \} = \\
\Sigma_{x \in S} P(s, x) \cdot \text{Prob}_x\{\omega' \in \mathcal{D} : \omega'(0) = x \land \omega' \models \psi_1 \}
\]

Summing over the equivalence classes of \( S \) with respect to \( G \).
\[
\Sigma_{x \in S} P(s, x) \cdot \text{Prob}_x\{\omega' \in \mathcal{D} : \omega'(0) = x \land \omega' \models \psi_1 \} = \\
\Sigma_{\text{rep}_G(x) \in S} \Sigma_{y \in \text{rep}_G(x)} P(s, y) \cdot \text{Prob}_y\{\omega' \in \mathcal{D} : \omega'(0) = y \land \omega' \models \psi_1 \}
\]

For \( y \in \text{rep}_G(x) \), by the induction hypothesis,
\[
\text{Prob}_y\{\omega' \in \mathcal{D} : \omega'(0) = y \land \omega' \models \psi_1 \} = \\
\text{Prob}_{\text{rep}_G(x)}\{\bar{\omega}' \in \mathcal{D}_G : \bar{\omega}'(0) = \text{rep}_G(x) \land \bar{\omega}' \models \psi_1 \}
\]

So we have
\[
\text{Prob}_s\{\omega \in \mathcal{D} : \omega(0) = s \land \omega \models \mathbf{X} \psi \} = \\
\Sigma_{\text{rep}_G(x) \in S} \text{Prob}_{\text{rep}_G(x)}\{\bar{\omega}' \in \mathcal{D}_G : \bar{\omega}'(0) = \text{rep}_G(x) \land \bar{\omega}' \models \psi_1 \} \Sigma_{y \in \text{rep}_G(x)} P(s, y)
\]

Since \( \Sigma_{y \in \text{rep}_G(x)} P(s, y) = P(\text{rep}_G(s), \text{rep}_G(x)) \) by Definition 11, we have
\[
\text{Prob}_s\{\omega \in \mathcal{D} : \omega(0) = s \land \omega \models \mathbf{X} \psi \} = \\
\Sigma_{\text{rep}_G(x) \in S} P(\text{rep}_G(s), \text{rep}_G(x)) \cdot \text{Prob}_{\text{rep}_G(x)}\{\bar{\omega}' \in \mathcal{D}_G : \bar{\omega}'(0) = \text{rep}_G(x) \land \bar{\omega}' \models \psi_1 \} = \\
\text{Prob}_{\text{rep}_G(s)}\{\bar{\omega} \in \mathcal{D}_G : \bar{\omega}(0) = \text{rep}_G(s) \land \bar{\omega} \models \mathbf{X} \psi_1 \}
\]

17
as required.

If \( \phi = \psi_1 U^{\leq k} \psi_2 \) and \( D, \omega \models \phi \) then for some \( i \leq k \), \( \omega(i) \models \psi_2 \) and \( \omega(j) \models \psi_1 \) for all \( 0 \leq j < i \). Since \( \text{count}(\psi_1) < N \) and \( \text{count}(\psi_2) < N \) it follows from the induction hypothesis that correspondingly \( D_G, \bar{\omega}(i) \models \psi_2 \) and \( \bar{\omega}(j) \models \psi_1 \) for all \( 0 \leq j < i \). Hence \( D_G, \bar{\omega} \models \psi_1 U^{\leq k} \psi_2 \), i.e. \( D_G, \bar{\omega} \models \phi \).

To prove part (iii) we need to use a second induction. Hence we refer to the induction hypothesis of (iii) as \( \Pi \), and will define our second hypothesis, \( \Pi_2 \) shortly.

Recursively define path formulae \( \theta_0, \theta_1, \ldots, \theta_k \) thus:

\[
\begin{align*}
\theta_0 &= \psi_2 \\
\theta_{i+1} &= \psi_1 \land X \theta_i \quad \text{for } 1 \leq i \leq k - 1
\end{align*}
\]

Define the set of paths \( A_0^s = \{ \omega \in D : \omega(0) = s \land \omega \models \theta_n \} \) and the sets of paths \( B_i^s \), for \( 0 \leq i \leq k \) thus:

\[
\begin{align*}
B_0^s &= A_0^s \\
B_i^s &= A_i^s \setminus \left( \bigcup_{j<i} (B_j^s \cap A_{i+1}^s) \right)
\end{align*}
\]

Since the \( B_i^s \) are disjoint, it follows from elementary analysis that

\[
\text{Prob}_s(\{ \omega \in D : \omega(0) = s \land \omega \models \phi \}) = \sum_{i=0}^k \text{Prob}_s(B_i^s) \tag{1}
\]

Now let \( \bar{A}_i^{\text{rep}_G(s)} = \{ \bar{\omega} \in D_G : \bar{\omega}(0) = \text{rep}_G(s) \land \bar{\omega} \models \theta_1 \} \) and define sets of paths \( \bar{B}_i^{\text{rep}_G(s)} \), for \( 0 \leq i \leq k \) thus:

\[
\begin{align*}
\bar{B}_0^{\text{rep}_G(s)} &= \bar{A}_0^{\text{rep}_G(s)} \\
\bar{B}_{i+1}^{\text{rep}_G(s)} &= \bar{A}_{i+1}^{\text{rep}_G(s)} \setminus \left( \bigcup_{j<i} (\bar{B}_j^{\text{rep}_G(s)} \cap \bar{A}_{i+1}^{\text{rep}_G(s)}) \right)
\end{align*}
\]

We are going to show, via a second induction argument, that \( \text{Prob}_s(B_i^s) = \text{Prob}_s(\bar{B}_i^{\text{rep}_G(s)}) \) for \( 0 \leq i \leq k \). Let \( \Pi_2 \) denote this hypothesis.

Now \( \text{Prob}_s(B_0^s) = \text{Prob}_s(\{ \omega \in D : \omega(0) = s \land \omega \models \psi_2 \} \). By induction hypothesis \( \Pi \), \( \text{Prob}_s(\{ \omega \in D : \omega(0) = s \land \omega \models \psi_2 \}) = \text{Prob}_s(\{ \bar{\omega} \in D_G : \bar{\omega}(0) = \text{rep}_G(s) \land \bar{\omega} \models \psi_2 \} \) which is \( \text{Prob}_s(\bar{B}_0^{\text{rep}_G(s)}) \).

Suppose that \( \Pi_2 \) holds for all \( 0 \leq i < n - 1 \), and \( n - 1 < k \). We show that \( \Pi_2 \) holds for \( n \).

\[
\text{Prob}_s(B_n^s) = \text{Prob}_s(\{ \omega \in D : \omega(0) = s \land \omega \models (\psi_1 \land \neg \psi_2) \land \omega_1 \in B_{n-1}^{\omega(1)} \})
\]
where \( \omega_1 = \omega(1), \omega(2), \ldots \). So

\[
\text{Prob}_s(B_n^s) = \text{Prob}_s(\{\omega \in D : \omega(0) = s \land \omega \models (\psi_1 \land \neg \psi_2)\}) \times \Sigma_{x \in S} P(s, x) \text{Prob}_x(B_{n-1}^x)
\]

Now \( \text{Prob}_s(\{\omega \in D : \omega(0) = s \land \omega \models (\psi_1 \land \neg \psi_2)\}) = \text{Prob}_{\text{rep}_G(s)}(\{\tilde{\omega} \in D_G : \tilde{\omega}(0) = \text{rep}_G(s) \land \tilde{\omega} \models (\psi_1 \land \neg \psi_2)\}) \) by I1. Also, summing over all equivalence classes with respect to \( G \),

\[
\Sigma_{x \in S} P(s, x) \text{Prob}_x(B_{n-1}^x) = \Sigma_{\text{rep}_G(x) \in S} \Sigma_{y \in [\text{rep}_G(x)]} P(s, y) \text{Prob}_y(B_{n-1}^y)
\]

For \( y \in [\text{rep}_G(x)] \), by I2,

\[
\text{Prob}_y(B_{n-1}^y) = \text{Prob}_{\text{rep}_G(x)}(\tilde{B}_{n-1}^{\text{rep}_G(x)})
\]

So we have

\[
\text{Prob}_s(B_n^s) = \text{Prob}_{\text{rep}_G(s)}(\{\tilde{\omega} \in D_G : \tilde{\omega}(0) = \text{rep}_G(s) \land \tilde{\omega} \models (\psi_1 \land \neg \psi_2)\}) \times \Sigma_{\text{rep}_G(x) \in S} \text{Prob}_{\text{rep}_G(x)}(\tilde{B}_{n-1}^{\text{rep}_G(s)}) \Sigma_{y \in [\text{rep}_G(x)]} P(s, y)
\]

Since \( \Sigma_{y \in [\text{rep}_G(x)]} P(s, y) = \tilde{P}(\text{rep}_G(s), \text{rep}_G(x)) \) by Definition 11, we have

\[
\text{Prob}_s(B_n^s) = \text{Prob}_{\text{rep}_G(s)}(\{\tilde{\omega} \in D_G : \tilde{\omega}(0) = \text{rep}_G(s) \land \tilde{\omega} \models (\psi_1 \land \neg \psi_2)\}) \times \Sigma_{\text{rep}_G(x) \in S} \tilde{P}(\text{rep}_G(s), \text{rep}_G(x)) \text{Prob}_{\text{rep}_G(x)}(\tilde{B}_{n-1}^{\text{rep}_G(x)})
\]

Hence we have proved induction hypothesis I2.

Returning to our proof of (iii) for \( \phi = \psi_1 U^{\leq k} \psi_2 \), from Equation 1 we have

\[
\text{Prob}_s(\{\omega \in D : \omega(0) = s \land \omega \models \phi\}) = \Sigma_{i=0}^k \text{Prob}_s(B_i^s)
\]

Since we have shown that, for all \( i \leq k \), \( \text{Prob}_s(B_i^s) = \text{Prob}_{\text{rep}_G(s)}(\tilde{B}_i^{\text{rep}_G(s)}) \) it follows that

\[
\text{Prob}_s(\{\omega \in D : \omega(0) = s \land \omega \models \phi\}) = \Sigma_{i=0}^k \text{Prob}_s(B_i^s) = \Sigma_{i=0}^k \text{Prob}_{\text{rep}_G(s)}(\tilde{B}_i^{\text{rep}_G(s)}).
\]
and we are done.

If \( \phi = \psi_1 U \psi_2 \) then, for some \( k \geq 0 \), \( D \models \psi_1 U^{<k} \psi_2 \). From the previous case it follows that \( \omega, D_G \models \psi_1 U^{<k} \psi_2 \). It follows that \( \omega, D_G \models \psi_1 U \psi_2 \).

The proof of (iii) proceeds exactly as for the case \( \phi = \psi_1 U^{<k} \psi_2 \) except for the following:

1. (a) Path formulae \( \theta_i \) are defined recursively for all \( 0 \leq i \).
2. (b) Sets \( A_i^r, B_i^r, A_i^{rep_G(s)} \) and \( B_i^{rep_G(s)} \) are defined for all \( 0 \leq i \).
3. (c) In the induction step (for I2) we assume that I2 holds for all \( 0 \leq i \leq n - 1 \), but do not insist that \( n - 1 < k \).

Clearly, our definitions of a DTMC and a quotient DTMC extend to the case where the set of states \( S \) has infinite cardinality. As such, Theorem 2 extends in a similar way:

**Theorem 3.** If \( D \) and \( D_G \) denote an infinite state DTMC and its quotient model with respect to group \( G \) respectively, then \( D, s \models \phi \iff D_G, s_G \models \phi \), for every symmetric PCTL formula \( \phi \).

We now outline proofs of results similar to Theorem 2 and Lemma 5 for the simpler case in which we have an isomorphism between DTMCs with different (but related) sets of propositional formulas.

**Definition 12.** Let \( D = (S, s_0, P) \) and \( D' = (S', s'_0, P') \) be DTMCs and \( \delta : S \to S' \) a bijection. If \( \delta(s_0) = s'_0 \) and, for all \( s, t \in S \), \( P(s, t) = P'(\delta(s), \delta(t)) \), then \( \delta \) is an isomorphism from \( D \) to \( D' \) and \( D \) and \( D' \) are said to be isomorphic.

**Theorem 4.** Let \( D \) and \( D' \) denote DTMCs and \( F \) and \( F' \) sets of propositional formulas defined over \( D \) and \( D' \) respectively, for which there is a bijection \( \gamma : F \to F' \). If \( \delta \) is an isomorphism from \( D \) to \( D' \) such that, for every \( s \in S \) and \( f \in F \), \( s \models f \iff s_G \models \gamma(f) \), then for any PCTL formula \( \phi \) defined over \( F' \), and \( s \in S \),

\[
D, s \models \phi \iff D', s_G \models \gamma(\phi),
\]

where \( \gamma(\phi) \) is the PCTL formula over \( F' \) obtained by replacing every propositional formula \( f \in F \) occurring in \( \phi \) with \( \gamma(f) \).
Proof of Theorem 4 follows directly from the following lemma, which is analogous to Lemma 5.

**Lemma 7.** Let \( D, D', F, F', \delta \) and \( \gamma \) be as for Theorem 4. Let \( \omega = s, s_1, \ldots \) be a path in \( D \) and \( \bar{\omega} = \delta(\omega) = \delta(s), \delta(s_1), \ldots \) in \( D' \). Then

(i) \( D, s \models \phi \iff D', \delta(s) \models \gamma(\phi) \), if \( \phi \) is a state formula, and  
(ii) \( D, \omega \models \phi \iff D', \bar{\omega} \models \gamma(\phi) \), if \( \phi \) is a path formula.

(iii) If \( \phi \) is a path formula, 
\[
\Pr_s(\{ \omega \in D : \omega(0) = s \land \omega \models \phi \} = \Pr_{\delta(s)}(\bar{\omega} \in D' : \bar{\omega}(0) = \delta(s) \land \bar{\omega} \models \gamma(\phi))
\]

*Proof.* By an argument identical to that for Lemma 6, if \( \phi \) is a state formula then if (i) holds, so does (ii).

Let \( \text{count}(\phi) \) denote the number of occurrences in \( \phi \) of symbols from \( \{P_{\text{exp}}, U^{\leq k}, U, X\} \). As before we proceed by induction on the value of \( \text{count}(\phi) \). In all cases we prove the result in one direction only, as since there is a one-to-one correspondence between the paths of \( D \) and of \( D' \), the proof of the converse is similar.

If \( \text{count}(\phi) = 0 \) or \( \text{count}(\phi) = N \) and \( \phi \) is a state formula, then the proof follows exactly as for the proof of Lemma 5. Suppose then that \( \text{count}(\phi) = N \) and that \( \phi \) is a path formula and not a state formula. Then one of the following situations similar to those identified in the proof of Lemma 5 holds:

1. \( \phi = \psi_1 U^{\leq k} \psi_2 \) for formulas \( \psi_1, \psi_2 \) over \( F \)
2. \( \phi = \psi_1 U \psi_2 \) for formulas \( \psi_1, \psi_2 \) over \( F \)
3. \( \phi = X \psi_1 \) for formula \( \psi_1 \) over \( F \).

The proof for case \( \phi = X \psi_1 \) is similar to that for the corresponding case in Lemma 5.

If \( \phi = \psi_1 U^{\leq k} \psi_2 \) and \( D, \omega \models \phi \) then for some \( i \leq k \), \( \omega(i) \models \psi_2 \) and \( \omega(j) \models \psi_1 \) for all \( 0 \leq j < i \). Then clearly \( \bar{\omega}(i) \models \gamma(\psi_2) \) and \( \bar{\omega}(j) \models \gamma(\psi_1) \) for all \( 0 \leq j < i \) and so \( D', \bar{\omega} \models \gamma(\psi_1) U^{\leq k} \gamma(\psi_2) \). That is, \( D', \bar{\omega} \models \gamma(\phi) \).

To prove (iii) we let \( I_1 \) denote the hypothesis of (iii) and use a second induction \( I_2 \) as before. We define path formulas \( \theta_0, \theta_1, \ldots, \theta_k \), and sets of paths \( A_i \) and \( B_i \), for \( 0 \leq i \leq k \) as for the proof of Lemma 5. Then, as before,

\[
\Pr_s(\{ \omega \in D : \omega(0) = s \land \omega \models \phi \}) = \sum_{i=0}^{k} \Pr_s(B_i)
\]
Now let \( \bar{A}_i^{\delta(s)} = \{ \bar{\omega} \in \mathcal{D} : \bar{\omega}(0) = \delta(s) \wedge \bar{\omega} \models \theta_i \} \) and define sets of paths \( \bar{B}_i^{\delta(s)} \) for \( 0 \leq i \leq k \) thus:

\[
\bar{B}_i^{\delta(s)} = \bar{A}_i^{\delta(s)}, \\
\bar{B}_i^{\delta(s)} = \bar{A}_i^{\delta(s)} \setminus \bigcup_{j<i} (\bar{B}_j^{\delta(s)} \cap \bar{A}_{i+1}^{\delta(s)}),
\]

We show, via a second induction argument, that \( \text{Prob}_s(B_i^{a}) = \text{Prob}_{\delta(s)}(\bar{B}_i^{\delta(s)}) \) for \( 0 \leq i \leq k \). Let I2 denote this hypothesis.

Now \( \text{Prob}_s(B_0^{a}) = \text{Prob}_s(\{ \omega \in \mathcal{D} : \omega(0) = s \wedge \omega \models \psi_2 \}) \). By induction hypothesis I1, \( \text{Prob}_s(\{ \omega \in \mathcal{D} : \omega(0) = s \wedge \omega \models \psi_2 \}) = \text{Prob}_{\delta(s)}(\{ \bar{\omega} \in \mathcal{D} : \bar{\omega}(0) = \delta(s) \wedge \bar{\omega} \models \gamma(\psi_2) \}) \) which is \( \text{Prob}_{\delta(s)}(\bar{B}_0^{\delta(s)}) \).

Suppose that I2 holds for all \( 0 \leq i < n - 1 \), and \( n - 1 < k \). We show that I2 holds for \( n \).

\( \text{Prob}_s(B_n^{a}) = \text{Prob}_s(\{ \omega \in \mathcal{D} : \omega(0) = s \wedge \omega \models (\psi_1 \wedge \neg \psi_2) \wedge \omega \in B_{n-1}^{\omega(1)} \}) \)

where \( \omega = \omega(1), \omega(2), \ldots \). So

\[
\text{Prob}_s(B_n^{a}) = \text{Prob}_s(\{ \omega \in \mathcal{D} : \omega(0) = s \wedge \omega \models (\psi_1 \wedge \neg \psi_2) \}) \\
\times \sum_{x \in S} P(s, x) \text{Prob}_x(B_{n-1}^{a})
\]

Now \( \text{Prob}_s(\{ \omega \in \mathcal{D} : \omega(0) = s \wedge \omega \models (\psi_1 \wedge \neg \psi_2) \}) = \text{Prob}_{\delta(s)}(\{ \bar{\omega} \in \mathcal{D} : \bar{\omega}(0) = \delta(s) \wedge \bar{\omega} \models \gamma(\psi_1 \wedge \neg \psi_2) \}) \) by I1. Also

\[
\sum_{x \in S} P(s, x) \text{Prob}_x(B_{n-1}^{a}) = \sum_{x \in S} P(s, x) \text{Prob}_{\delta(x)}(\bar{B}_{n-1}^{\delta(x)}) \quad \text{(by I2)}
\]

\[
= \sum_{x \in S} P'(\delta(s), \delta(x)) \text{Prob}_{\delta(x)}(\bar{B}_{n-1}^{\delta(x)})
\]

\[
= \sum_{y \in S'} P'(\delta(s), y) \text{Prob}_y(\bar{B}_{n-1}^{a})
\]

Hence

\[
\text{Prob}_s(B_n^{a}) = \text{Prob}_{\delta(s)}(\{ \bar{\omega} \in \mathcal{D} : \bar{\omega}(0) = \delta(s) \wedge \bar{\omega} \models \gamma(\psi_1 \wedge \neg \psi_2) \}) \\
\times \sum_{x \in S} P'(\delta(s), y) \text{Prob}_y(B_{n-1}^{a})
\]

\[
= \text{Prob}_{\delta(s)}(\bar{B}_n^{\delta(s)})
\]

thus proving induction hypothesis I2.
Returning to our proof of (iii) for $\phi = \psi_1 U^k \psi_2$, from Equation 2 we have

\[
\text{Prob}_s(\{\omega \in D : \omega(0) = s \land \omega \models \phi\})
= \sum_{i=0}^{k} \text{Prob}_s(B^s_i)
= \sum_{i=0}^{k} \text{Prob}_{s(s)}(B^s_i(\delta(s))) \quad \text{(from I2)}
= \text{Prob}_{s(s)}(\{\tilde{\omega} \in D' : \tilde{\omega}(0) = \delta(s) \land \tilde{\omega} \models \gamma(\phi)\})
\]

The rest of the proof is as for Lemma 5. \hfill \Box

Theorem 4 extends to infinite state DTMCs thus:

**Theorem 5.** Let $D$ and $D'$ denote infinite state DTMCs and $F$ and $F'$ sets of propositional formulas defined over $D$ and $D$ respectively, for which there is a bijection $\gamma : F \to F'$. If $\delta$ is an isomorphism from $D$ to $D'$ such that, for every $s \in S$ and $f \in F$, $s \models f \iff \delta(s) \models \gamma(f)$, then for any PCTL formula $\phi$ defined over $F'$, and $s \in S$,

\[ D, s \models \phi \iff D', \delta(s) \models \gamma(\phi), \]

where $\gamma(\phi)$ is the PCTL formula over $F'$ obtained by replacing every proposition $f$ occurring in $\phi$ with $\gamma(f)$.

## 5 Markov Decision Processes

A Markov decision process is a generalisation of a DTMC in which choice can be both probabilistic and non-deterministic. Again, we define an MDP over the set of states $D$ defined as the set of all tuples of possible variable values. For a finite set $S$, let $\text{Dist}(S)$ denote the set of all probability distributions over $S$, i.e. the set of functions $\mu : S \to [0, 1]$ such that $\sum_{s \in S} \mu(s) = 1$.

**Definition 13.** A Markov Decision Process $\mathcal{M}$ is a tuple $\mathcal{M} = (S, S_0, \text{Steps})$, where:

1. $S = D$ is a non-empty, finite set of states
2. $S_0 \subseteq S$ is a set of initial states
3. $\text{Steps} : S \to 2^{\text{Dist}(S)}$ is the probabilistic transition function such that $\forall s \in S, \text{Steps}(s) \neq 0$. 

23
As usual, we assume that there is a single initial state, $s_0$ and let $\mathcal{M} = (S, s_0, \text{Steps})$ uniquely identify MDP $\mathcal{M}$.

At a given state $s$ a distribution $\mu$ is chosen non-deterministically from the set of distributions $\text{Steps}(s)$. For every state $s' \in S$ the probability of the next state being $s'$ is $\mu(s')$. A path in an MDP is a non-empty sequence of the form

$$s_0 \xrightarrow{\mu_1} s_1 \xrightarrow{\mu_2} s_2 \ldots$$

where $s_i \in S$, $\mu_{i+1} \in \text{Steps}(s_i)$ and $\mu_{i+1}(s_{i+1}) > 0$ for all $i \geq 0$. Like DTMCs, $\omega(i)$ denotes the $i$th state of path $\omega$ and the sets of finite and infinite paths starting at state $s$ are denoted $\text{Path}_s^{\text{fin}}$ and $\text{Path}_s$ respectively.

A path through an MDP is obtained by resolving both probabilistic and non-deterministic choices. To do this one assumes that non-deterministic choices are resolved by an Adversary which selects a choice based on the history of choices made so far. The following definition is from [22]:

**Definition 14.** An adversary $\mathcal{A}$ of an MDP is a function mapping every finite path $\omega_{\text{fin}}$ of $\mathcal{M}$ onto an element $\mathcal{A}(\omega_{\text{fin}})$ of the set $\text{Steps}(\text{last}(\omega_{\text{fin}}))$.

Note that $\text{last}(\omega_{\text{fin}})$ denotes the final state of finite path $\omega_{\text{fin}}$. We denote the set of adversaries for MDP $\mathcal{M}$ as $\text{Adv}_\mathcal{M}$ and, for any adversary $\mathcal{A}$ of $\mathcal{M}$ we denote the subset of $\text{Path}_s$ corresponding to $\mathcal{A}$ as $\text{Path}_s^\mathcal{A}$.

### 5.1 PCTL for MDPs

The behaviour of an MDP for a given adversary $\mathcal{A}$ is purely probabilistic and can be described as an infinite state DTMC, $D^\mathcal{A}$ (see for example [22, 23]). There is a one-to-one correspondence between the paths of $D^\mathcal{A}$ and the set of paths $\text{Path}_s^\mathcal{A}$. Hence the probability measure for DTMCs (given in Section 4.1), which extends naturally to infinite state DTMCs, can be adapted to define a probability measure $\text{Prob}_s^\mathcal{A}$ over $\text{Path}_s^\mathcal{A}$.

It is not possible to define a probability measure over all paths of an MDP [2], and reasoning over the paths for a single adversary is of limited use. However, for a set of sequences we can define a maximal probability and a minimal probability. For a set of sequences $\Delta \in \text{Path}_s$ define $\text{Prob}_s^+ (\Delta)$ and $\text{Prob}_s^- (\Delta)$ to be the maximal and minimal probability of $\Delta$ respectively. Intuitively $\text{Prob}_s^+ (\Delta)$ and $\text{Prob}_s^- (\Delta)$ represent the probability that the system follows a sequence in $\Delta$ provided that the non-deterministic choices are as favourable/unfavourable as possible.
Properties of MDPs are expressed using $PCTL$, which is defined as for DTMCs (see Section 4.1) except for the case of the $P_{\infty p} [\psi]$ operator. Here, if a state $s$ satisfies $P_{\infty p} [\psi]$ then the probability of a path from $s$ satisfying $\psi$ is in the range $\propto p$ for all adversaries. I.e.

$$s \models P_{\infty p} [\psi] \iff p_s^A \propto p$$

for all $A \in Adv_M$.

where $p_s^A \overset{def}{=} \text{Prob}_s(\{\omega \in \text{Path}_s^A : \omega \models \psi\})$.

Given $M = (S, s_0, \text{Steps})$, if $\omega_s$ is a path starting from any state $s \in S$, then we say that $M, \omega_s \models \phi$ if and only if $M_s, \omega_s \models \phi$, where $M_s = (S, s, \text{Steps})$.

**Definition 15.** If $M$ is an MDP and $s \in S$, for a path formula $\phi$ and adversary $A$ we say that

1. $A$ is most favourable for $\phi$ at $s$ if, for all adversaries $A' \in Adv_M$, $\text{Prob}_s[\omega \in D^A : \omega(0) = s \land \omega \models \phi] \geq \text{Prob}_s[\omega \in D^{A'} : \omega(0) = s \land \omega \models \phi]$.

2. $A$ is most unfavourable for $\phi$ at $s$ if, for all adversaries $A' \in Adv_M$, $\text{Prob}_s[\omega \in D^A : \omega(0) = s \land \omega \models \phi] \leq \text{Prob}_s[\omega \in D^{A'} : \omega(0) = s \land \omega \models \phi]$.

Lemma 8 is adapted from [2]:

**Lemma 8.** If $M$ is an MDP and $\phi$ a path formula, then there are adversaries $A$ and $A'$ that are at least favourable and least favourable respectively for $\phi$ at every $s \in S$.

### 5.2 Quotient MDPs

**Definition 16.** Let $M = (S, s_0, \text{Steps})$ be an MDP. An automorphism of $M$ is a permutation $\alpha : S \rightarrow S$ which preserves the initial state of $M$ and is such that, for all $s, t \in S$ for which there exists $\mu \in \text{Steps}(s)$ and $\mu(t) > 0$, there exists $\mu' \in \text{Steps}(\alpha(s))$ such that $\mu'(\alpha(t)) = \mu(t)$.

The set of all automorphisms forms a group under composition, denoted $Aut(M)$. A quotient MDP can be defined analogously to the Kripke structure/DTMC cases [17].
Definition 17. Let $\mathcal{M} = (S, s_0, \text{Steps})$ be an MDP and $G$ an automorphism group of $\mathcal{M}$. The quotient MDP of $\mathcal{M}$ with respect to $G$ is a tuple $\mathcal{M}_G = (S_G, s_0^G, \text{Steps}_G)$ where

- $S_G = \{ \text{rep}_G(s) : s \in S \}$ where $\text{rep}_G(s)$ is a unique representative of $[s]_G$
- $s_0^G = \text{rep}_G(s_0)$
- for each $\text{rep}_G(s) \in S_G$ and $\mu \in \text{Steps}(\text{rep}_G(s))$, $\text{Steps}_G(\text{rep}_G(s))$ contains a distribution $\bar{\mu} \in \text{Dist}(S_G)$ where, for $\text{rep}_G(t) \in S_G$, $\bar{\mu}(\text{rep}_G(t)) = \Sigma_{x \in [t]} \mu(x)$.

We show that, as in the DTMC case, the quotient models preserve the truth of PCTL properties which are invariant under symmetry. First we prove an analagous result to the probabilistic Correspondence Lemma (Lemma 4):

Lemma 9. (Correspondence Lemma for MDPs) There is a bidirectional correspondence between paths of MDP $\mathcal{M}$ and of the quotient structure $\mathcal{M}_G$ for any group of automorphisms $G$ of $\mathcal{M}$:

(i) If $\omega = s_0 \xrightarrow{\mu_1} s_1 \xrightarrow{\mu_2} \ldots$, where $\mu_{i+1} \in \text{Steps}(s_i)$, is a path in $\mathcal{M}$ then $\bar{\omega} = \text{rep}_G(s_0) \xrightarrow{\bar{\mu}_1} \text{rep}_G(s_1) \xrightarrow{\bar{\mu}_2} \ldots$, where $\bar{\mu}_{i+1} \in \text{Steps}_G(\text{rep}_G(s_i))$, is a path in $\mathcal{M}_G$.

(ii) If $\bar{\omega} = \bar{s}_0 \xrightarrow{\bar{\mu}_1} \bar{s}_1 \xrightarrow{\bar{\mu}_2}$, where $\bar{\mu}_{i+1} \in \text{Steps}_G(\bar{s}_i)$, is a path in $\mathcal{M}_G$ then there exists a corresponding path $\omega' = s'_0 \xrightarrow{\mu'_1} s'_1 \xrightarrow{\mu'_2} \ldots$ in $\mathcal{M}$, where $s'_0 = s_0$, $s'_i \in [s_i]_G$ and $\mu'_{i+1} \in \text{Steps}(s'_i)$.

Proof. (i) For $i > 0$ there is some $\alpha \in G$ such that $\text{rep}_G(s_{i-1}) = \alpha(s_{i-1})$. Since $\alpha$ is an automorphism, for some $\mu'_i \in \text{Steps}(\alpha(s_{i-1}))$, $\mu'_i(\alpha(s_i)) = \mu_i(s_i)$. In $\mathcal{M}_G$, $\text{Steps}_G(\text{rep}_G(s_{i-1})) = \text{Steps}_G(\alpha(s_{i-1}))$ contains a distribution $\bar{\mu}_i$ where

\[
\bar{\mu}_i(\text{rep}_G(\alpha(s_i))) = \Sigma_{x \in [\alpha(s_i)]} \mu'_i(x), \\
\geq \mu'_i(\alpha(s_i)), \\
= \mu_i(s_i), \\
> 0
\]
Hence \( \text{rep}_G(s_{i-1}) \xrightarrow{\mu_i} \text{rep}_G(\alpha(s_i)) \) in \( \mathcal{M}_G \). Since \( s_i \in [\alpha(s_i)]_G \), \( \text{rep}_G(s_i) = \text{rep}_G(\alpha(s_i)) \) and so \( \text{rep}_G(s_{i-1}) \xrightarrow{\mu_i} \text{rep}_G(s_i) \). Since this is true for all \( i > 0 \) the result follows.

(ii) Let \( s_0 \xrightarrow{\mu_1} s_1 \xrightarrow{\mu_2} \ldots \xrightarrow{\mu_n} s_n \) be the path prefix of \( \bar{\omega} \) of length \( n \). If we can show that for any \( n \geq 0 \) there is a path prefix of length \( n \) in \( \mathcal{M} \) corresponding to the path prefix of length \( n \) of \( \bar{\omega} \) then we are done. We proceed by induction on \( n \).

First note that if \( \bar{\mu}_i(t) > 0 \) in \( \mathcal{M}_G \) then, for some \( \mu_i \in \text{Steps}(s_{i-1}) \) and some \( \beta \in G, \mu_i(\beta(t)) > 0 \) in \( \mathcal{M} \).

The case \( n = 0 \) is trivial so we first consider \( n = 1 \). Now \( s_0 \xrightarrow{\mu_1} s_1 = s_0 \xrightarrow{\mu_1} s_1 \) is the path prefix of length 1 of \( \bar{\omega} \) so \( \bar{\mu}_1(s_1) > 0 \) and, for some \( \mu'_i \in \text{Steps}(s_0) \) and some \( \beta \in G, \mu'_i(\beta(s_1)) > 0 \) in \( \mathcal{M} \).

If we let \( s'_1 = \beta(s_1) \), then \( \mu'_i(s'_1) > 0 \) and \( s_0 \xrightarrow{\mu'_i} s'_1 \) is a path prefix in \( \mathcal{M} \), where \( s'_1 \in [s_1]_G \).

Suppose that we have shown that, for \( k \geq 1 \), there is a path prefix \( s'_0 \xrightarrow{\mu'_1} s'_1 \xrightarrow{\mu'_2} \ldots \xrightarrow{\mu'_k} s'_k \) in \( \mathcal{M} \) corresponding to the path prefix \( s'_0 \xrightarrow{\mu} s'_1 \xrightarrow{\mu} \ldots \xrightarrow{\mu} s'_k \) of \( \bar{\omega} \). Then \( s'_k \in [s_k]_G \) and so, for some \( \alpha \in G, s_k = \alpha(s'_k) \).

Since \( \bar{\mu}_{k+1}(s_{k+1}) > 0 \) in \( \mathcal{M}_G \) for \( \bar{\mu}_{k+1} \in \text{Steps}_G(s_k) \), \( \mu_{k+1}(\beta(s_{k+1})) > 0 \) for some \( \mu_{k+1} \in \text{Steps}(s_k) \) and \( \beta \in G \). So \( \mu'_{k+1}(\alpha^{-1}(\beta(s_{k+1}))) > 0 \) for \( \mu'_{k+1} \) in \( \text{Steps}(\alpha^{-1} s_k) = \text{Steps}(s'_k) \). If we let \( s'_{k+1} = \alpha^{-1} \beta(s_{k+1}) \) then \( s'_0 \xrightarrow{\mu'_i} s'_1 \xrightarrow{\mu'_2} \ldots \xrightarrow{\mu'_{k+1}} s'_{k+1} \) is a path prefix of \( \mathcal{M} \) of length \( k + 1 \) where \( s'_{k+1} \in [s_{k+1}]_G \). \( \Box \)

As for the non-probabilistic and DTMC cases, an equivalent result holds for paths \( \omega \), starting from any state \( s \).

**Corollary 4.**

(i) If \( \omega = s \xrightarrow{\mu_1} s_1 \xrightarrow{\mu_2} \ldots \), where \( \mu_1 \in \text{Steps}(s) \) and \( \mu_{i+1} \in \text{Steps}(s_i) \) for \( i > 0 \), is a path in \( \mathcal{M} \) then \( \bar{\omega} = \text{rep}_G(s) \xrightarrow{\bar{\mu}_1} \text{rep}_G(s_1) \xrightarrow{\bar{\mu}_2} \ldots \), where \( \bar{\mu}_1 \in \text{Steps}_G(\text{rep}_G(s)) \) and \( \bar{\mu}_{i+1} \in \text{Steps}_G(\text{rep}_G(s_i)) \) for \( i > 0 \), is a path in \( \mathcal{M}_G \).

(ii) If \( \omega = s \xrightarrow{\mu_1} \bar{s}_1 \xrightarrow{\mu_2} \ldots \) in \( \mathcal{M} \), where \( \bar{s}_1 \in [\bar{s}]_G \), \( \mu'_i \in \text{Steps}(s') \), and, for \( i > 0 \), \( s'_i \in [s'_i]_G \) and \( \mu'_{i+1} \in \text{Steps}(s'_i) \). 27
It has been stated [17, 12] that an MDP and its quotient satisfy the same symmetric PCTL formulas. We define symmetric PCTL formulas analogously to symmetric CTL$^*$ formulas. That is, a PCTL formula $\phi$ is symmetric, or invariant, with respect to $G$ if for every maximal propositional subformula $f$ appearing in $\phi$, and for every $\alpha \in G$, $\mathcal{M}, s \models f \Leftrightarrow \mathcal{M}_G, \alpha(s) \models f$.

**Theorem 6.** If $\mathcal{M}$ and $\mathcal{M}_G$ denote an MDP and its quotient model with respect to group $G$ respectively, then $\mathcal{M}, s \models \phi \Leftrightarrow \mathcal{M}_G, rep_G(s) \models \phi$, for every symmetric PCTL formula $\phi$.

Like the corresponding result for DTMCs, the proof of this theorem has not appeared before. Here we prove Theorem 6 by considering infinite state DTMCs associated with adversaries, and applying our results for DTMCs. First we prove some intermediate results.

**Theorem 7.** There is a bidirectional correspondence between the sets of adversaries $Adv$ and $Adv_G$ of $\mathcal{M}$ and $\mathcal{M}_G$ respectively. For every $A \in Adv$, if $\mathcal{D}^A$ and $\mathcal{D}^{AG}$ denote the (infinite state) DTMCs corresponding to $A$ and a corresponding adversary $A^G$ of $\mathcal{M}_G$, then $\mathcal{D}^{AG}$ is the quotient DTMC of $\mathcal{D}^A$ with respect to $G$.

**Proof.** By Definition 14, $A$ is a function mapping every finite path $\omega = s_0 \xrightarrow{\mu_1} s_1 \xrightarrow{\mu_2} \ldots s_{n-1}$ onto an element $A(\omega)$ of the set $Steps(s_{n-1})$. Define adversary $A^G$ of $\mathcal{M}_G$ corresponding to $A$ thus: If, for finite path $\omega = s_0 \xrightarrow{\mu_1} s_1 \xrightarrow{\mu_2} \ldots s_{n-1}$, $A(\omega) = \mu_{n-1}$ then, for any corresponding finite path of $\mathcal{M}_G$ (see the proof of Lemma 4), $\omega = rep_G(s_0) \xrightarrow{\mu_1} rep_G(s_1) \xrightarrow{\mu_2} \ldots rep_G(s_{n-1})$, let $A^G(\omega) = \mu_{n-1} \in Steps(rep_G(s_{n-1}))$ where $\mu_{n-1}(rep_G(s)) = \sum_{x \in rep_G(s)} \mu_{n-1}(x)$ for all $rep_G(s) \in S_G$. Similarly, for any adversary $A^G$ of $\mathcal{M}_G$, define corresponding adversary $A$ of $\mathcal{M}$ thus: If, for finite path $\omega = rep_G(s_0) \xrightarrow{\mu_1} rep_G(s_1) \xrightarrow{\mu_2} \ldots rep_G(s_{n-1}) A^G$ maps to $\mu_{n-1} \in Steps(rep_G(s_{n-1}))$ then, for any corresponding finite path of $\mathcal{M}, \omega = s_0 \xrightarrow{\mu_1} s_1 \xrightarrow{\mu_2} \ldots s_{n-1}$, let $A(\omega) = \mu_{n-1} \in Steps(s_{n-1})$ where $\sum_{x \in rep_G(s)} \mu_{n-1}(x) = \mu_{n-1}(rep_G(s))$ for each $rep_G(s) \in S_G$.

The states of $\mathcal{D}^A$ and $\mathcal{D}^{AG}$ consist of sequences of states from $S$ and $S_G$ respectively. Every state $< s_0, s_1, \ldots, s_{n-1} >$ of $\mathcal{D}^A$ associates with a finite path of $\mathcal{M}$, for which there is a corresponding path of $\mathcal{M}_G$ and accordingly state $< rep_G(s_0), rep_G(s_1), \ldots, rep_G(s_{n-1}) >$ of $\mathcal{D}^{AG}$.

For any pair of states $(\omega, \omega')$ of $\mathcal{D}^A$, $P(\omega, \omega') = 0$ unless $\omega' = < \omega, s_j >$ (the concatenation of $\omega$ and $< s_j >$) for some $s_j \in S$. If $\omega' = < \omega, s_j >$ then $P(\omega, \omega') = A(\omega)(s_j)$.
Similarly, if \((\bar{\omega}, \bar{\omega}')\) is a pair states of \(\mathcal{D}^{\mathcal{A}^{G}}\) corresponding to states \(\omega\) and \(\omega'\) of \(\mathcal{D}^{\mathcal{A}}\) respectively, then \(P(\bar{\omega}, \bar{\omega}') = 0\) unless \(\bar{\omega}' = < \bar{\omega}, rep_G(s_i) >\) for some \(rep(s_i) \in S_G\). If \(\bar{\omega}' = < \bar{\omega}, rep_G(s_i) >\) then \(P(\bar{\omega}, \bar{\omega}') = A^{G}(\bar{\omega})(rep_G(s_i)) = \sum_{x \in [rep_G(s_i)]} A(\omega)(x)\).

Let us define the action of \(G\) on the states of \(\mathcal{D}^{\mathcal{A}}\) thus:

\[ g < s_0, s_1, \ldots, s_{n-1} >= < g(s_0), g(s_1), \ldots, g(s_{n-1}) >, \text{ for all } g \in G \]

If we let \(< rep_G(s_0), rep_G(s_1), \ldots, rep_G(s_{n-1}) >\) be the orbit representative of state \(< s_0, s_1, \ldots, s_{n-1} >\) then, by (the infinite state extension to) Definition 11, \(\mathcal{D}^{\mathcal{A}^{G}}\) is the quotient of \(\mathcal{D}^{\mathcal{A}}\) with respect to \(G\).

An equivalent result holds for adversaries starting from any state \(s\).

**Corollary 5.** For any \(s \in S\) there is a bidirectional correspondence between the sets of adversaries of \(\mathcal{M}\) and \(\mathcal{M}_G\) starting at states \(s\) and \(rep_G(s)\) respectively. For every \(A_s \in Adv_s\), if \(D_s^{A}\) and \(D_{rep_G(s)}^{A}\) denote the (infinite state) DTMCs corresponding to \(A_s\) and a corresponding adversary \(A_{rep_G(s)}^{G}\) of \(\mathcal{M}_G\) starting at \(< s >\) and \(< rep_G(s) >\) respectively then, \(D_{rep_G(s)}^{A}\) is the quotient DTMC of \(D_s^{A}\) with respect to \(G\).

The following definition is adapted from [23]:

**Definition 18.** Let \(\mathcal{M}\) and \(\mathcal{D}^{\mathcal{A}}\) denote an MDP and the DTMC associated with adversary \(A \in Adv\) respectively. For \(\alpha \in Path(\mathcal{M})\), \(\alpha \uparrow_A\) returns the path of \(\mathcal{D}^{\mathcal{A}}\) corresponding to \(\alpha\). Similarly if \(\alpha' \in Path(\mathcal{D}^{\mathcal{A}})\), \(\alpha' \downarrow_A\) returns the path of \(\mathcal{M}\) corresponding to \(\alpha'\).

Lemma 10 below allows us to prove Theorem 6. Note that in the proof of Lemma 10 we use \(\pi\) and \(\bar{\pi}\) to denote paths of DTMCs rather than the usual \(\omega\) and \(\bar{\omega}\). This is to distinguish between paths of the DTMCs and the corresponding MDPs.

**Lemma 10.** If \(\mathcal{M}\) and \(\mathcal{M}_G\) denote an MDP and its quotient model with respect to group \(G\) respectively, then \(\mathcal{M}, s \models P_{\geq p}[\psi] \iff \mathcal{M}_G, rep_G(s) \models P_{\geq p}[\psi],\) for every symmetric PCTL path formula \(\psi\).

**Proof.** Let us assume that \(\geq\) is \(\leq\). The proofs for \(<,\geq\) and \(>\) are similar.

\(\mathcal{M}, s \models P_{\leq p}[\psi] \iff \text{Prob}_s(\{\omega \in Path_s^{A} : \omega \models \psi\}) \leq p\) for all \(A \in Adv\). Suppose that \(\mathcal{M}_G, rep_G(s) \not\models P_{< p}[\psi]\). Then for some \(A^G \in Adv_G\),
\[
\text{Prob}_{\text{rep}_G(s)}(\{ \tilde{\omega} \in \text{Path}_{\text{rep}_G(s)}^{A_G} : \tilde{\omega} \models \psi \}) > p. \quad \text{Let } D^{A_G} \text{ and } D^A \text{ be the DTMCs associated with } A^G \text{ and a corresponding adversary } A \text{ of } M. \text{ Then, in } D^{A_G},
\]
\[
\text{Prob}_{\text{rep}_G(s)}(\{ \tilde{\pi} \in \text{Path}(D^{A_G}) : \tilde{\pi} \downarrow_{A^G} \in \text{Path}_{\text{rep}_G(s)} \text{ and } \tilde{\pi} \downarrow_{A^G} \models \psi \}) > p.
\]

Hence \( D^{A_G}_{\text{rep}_G(s)} \notin P_\leq_p(\psi) \) and, by Corollary 5, \( D^A \notin P_\leq_p(\psi) \). But then \( \text{Prob}_{\text{rep}_G(s)}(\{ \omega \in \text{Path}_A^A : \omega \models \psi \}) > p \) and so \( M \notin P_{<p}(\psi) \), which is a contradiction. (The converse is similar.) \( \Box \)

We can now prove Theorem 6.

**Proof.** (of Theorem 6) As \( \phi \) is a state formula, either \( \phi \) is propositional, or \( \phi = P_{\infty,p}[\psi] \) for path formula \( \psi \). If \( \phi \) is propositional then it must be symmetric, and so \( M, s \models \phi \Leftrightarrow M_G, \alpha(s) \models \phi, \forall \alpha \in G \) and the result holds.

If \( \phi = P_{\infty,p}[\psi] \) then the result holds by Lemma 10. \( \Box \)

We now outline proofs of results similar Corollary 5 and to Theorem 6 for the simpler case in which we have an isomorphism between MDPs with different (but related) sets of propositional formulas.

**Definition 19.** Let \( M = (S, s_0, \text{Steps}) \) and \( M' = (S', s'_0, \text{Steps}') \) be MDPs and \( \delta : S \rightarrow S' \) a bijection. If \( \delta(s_0) = s'_0 \) and, for all \( s \in S \) and \( \mu \in \text{Steps}(s) \) there exists \( \mu' \in \text{Steps}'(\delta(s)) \) such that \( \mu(t) = \mu'(\delta(t)) \), then \( \delta \) is an isomorphism from \( M \) to \( M' \) and \( M \) and \( M' \) are said to be isomorphic.

**Lemma 11.** Let \( M \) and \( M' \) denote MDPs and \( F \) and \( F' \) sets of propositional formulas defined over \( M \) and \( M' \) respectively, for which there is a bijection \( \gamma : F \rightarrow F' \). If \( \delta \) is an isomorphism from \( M \) to \( M' \) such that, for every \( s \in S \) and \( f \in F \), \( s \models f \Leftrightarrow \delta(s) \models \gamma(f) \), then there is a bijective correspondence between the sets of adversaries of \( M \) and \( M' \) starting at states \( s \) and \( \delta(s) \) respectively. For every \( A_s \in \text{Adv}_s \), if \( D^A_s \) and \( D^{A_s}_{\delta(s)} \) denote the (finite state) DTMCs corresponding to \( A_s \) and a corresponding adversary \( A'_{\delta(s)} \) of \( M' \) starting at \( s \) and \( \delta(s) \) respectively then \( D \) and \( D' \) are isomorphic.

**Proof.** There is a bijective correspondence between the sets of adversaries \( \text{Adv}_s \) and \( \text{Adv}_{\delta(s)} \) of \( M_s \) and \( M'_{\delta(s)} \). For any \( A_s \in \text{Adv}_s \), if \( A_s \) maps finite path \( \omega_s = s \xrightarrow{\mu_1} s_1 \xrightarrow{\mu_2} \ldots s_{n-1} \), to \( \mu_{n-1} \) then corresponding adversary
$A'_{\delta(s)}$ maps corresponding finite path $\tilde{\omega}_{\delta s} = \delta(s) \xrightarrow{t_1} \delta(s_1) \xrightarrow{t_2} \ldots \delta(s_{n-1})$, to $\tilde{\mu}_{n-1} \in \text{Steps}(\delta(s_{n-1}))$ where for all $t \in S$, $\mu_{n-1}(t) = \tilde{\mu}_{n-1}(\delta(t))$. (The correspondence in the other direction is similar).

For every $A_s \in Adv_s$, let $D^A_s$ and $D^A'_{\delta(s)}$ denote the (finite state) DTMCs corresponding to $A_s$ and a corresponding adversary $A'_{\delta(s)}$ of $M'$ starting at $< s >$ and $< \delta(s) >$ respectively. Then, if $S(D^A_s)$ and $S(D^A'_{\delta(s)})$ denote the sets of states of $D^A_s$ and $D^A'_{\delta(s)}$ respectively, the map $\hat{\delta} : S(D^A_s) \rightarrow S(D^A'_{\delta(s)})$, where $\hat{\delta}(s, s_1, s_2, \ldots, s_{n-1}) = (\delta(s), \delta(s_1), \ldots, \delta(s_{n-1}))$ is an isomorphism from $D^A_s$ to $D^A'_{\delta(s)}$. $\Box$

**Theorem 8.** If $M, M', \delta$ and $\gamma$ are as defined in Lemma 11 then for any PCTL formula $\phi$ defined over $F'$, and $s \in S$,

$$M, s \models \phi \iff M', \delta(s) \models \gamma(\phi'),$$

where $\gamma(\phi)$ is the PCTL formula over $F'$ obtained by replacing every propositional formula $f$ occurring in $\phi$ with $\gamma(f)$.

**Proof.** As $\phi$ is a state formula, either $\phi \in F$ or $\phi = P_{\psi}[\psi]$ for path formula $\psi$. If $\phi \in F$ then by definition $M, s \models \phi \iff M', \delta(s) \models \gamma(\phi)$.

If $\phi = P_{\psi}[\psi]$ and $M, s \models \phi$ then $M', \delta(s) \models \gamma(\phi')$ by an argument identical to the proof of Lemma 10 (but replacing $M_G$ with $M'$, $rep_G(s)$ with $\delta(s)$ etc.) $\Box$

**References**


