EXPLOITING SYMMETRY IN TEMPORAL LOGIC MODEL CHECKING[8]

Anas Anis
Motivation

- Concurrent systems often exhibit symmetry (replicated components)
- ...states space explosion problem
- Goal: techniques for reducing model checking complexity by exploiting symmetry

This paper:
- defines what is a symmetric system
- describes tech. for reduction of explicit or symbolic system representations
- investigates complexity of critical steps: orbit relation
The past

- In the past: exploiting symmetry in explicit states representation [1]
- BDDs as symbolic representation for symbolic model checking [2].
- Reachability analysis[3,4].
Outline

- Fundamentals
  - Symmetry groups
  - CTL*
- Quotient Models
  - Orbit of a state
  - Invariance group
- Model Checking with Symmetry
- Complexity of orbit calculations
Kripke Structure over AP is $M=(S,R,S_0,L)$:

- $S$: finite set of states
- $R$: transition relation
- $S_0 \subseteq S$: subset of $S$, initial states
- $L$: labeling function $S \rightarrow 2^{\text{AP}}$
2 processes with a mutual exclusion technique
**Fundamentals, permutations**

- **Permutation** over a finite set $S$: a bijective function from $S$ to $S$.

- A permutation $\sigma$, is a **symmetry** of $M$ iff it preserves $R$:
  
  $$(\forall s_1 \in S)(\forall s_2 \in S)((s_1, s_2) \in R \iff (\sigma s_1, \sigma s_2) \in R)$$

- Example: $\sigma = (S_1, S_2)$ on the concurrent processes.
Fundamentals, permutations

Symmetry Permutation

Non Symmetry Permutation
Fundamentals

- $G$: a group of permutations acting on $S$. Each group contains the identity permutation.
- $G$ is a symmetry group of $M$ iff every $\sigma \in G$ is a symmetry permutation of $M$.
- $G = \langle g_1, \ldots, g_k \rangle$: the group $G$ is generated by the set of permutations $\{g_1, \ldots, g_k\}$. 
Fundamentals

- Temporal logic CTL* over AP:
  - Formalization of requirements in temporal logic.
  - Combination of LTL & CTL: state or path formulae
  - Examples: $p, q, G\varphi, F\psi, A[\chi U \varphi], ...$
Quotient Models, orbit of a state

- $G$, a group of permutations acting on $S$
- $\theta(s)$: orbit of a state $s \in S$
  - $\theta(s) = \{t \mid (\exists \sigma \in G)(\sigma s = t)\}$

- e.g. $\theta(S_0) = \{S_0\}$, $\theta(S_1) = \theta(S_2) = \{S_1, S_2\}$
Quotient Models

- **Quotient model:** \( M_G = \{S_G, R_G, S_{0G}, L_G\} \)
  - \( S_G = \{\theta(s) \mid s \in S\} \)
  - \( R_G = \{(\theta(s_1), \theta(s_2)) \mid (s_1, s_2) \in R\} \)
  - \( S_{0G} = \{\theta(s_0) \mid s_0 \in S_0\} \)
  - \( L_G(\theta(s)) = L(\text{rep}(\theta(s))) \) | \( \text{rep}(\theta(s)) \) is the unique representative of \( \theta(s) \)
A CTL* formula $h$ is symmetric under a group $G$ iff

- for every maximal propositional subformula $f$ in $h$,
  
  $\forall \sigma \in G \ (\forall s \in S): M, s \models f \iff M, \sigma s \models f$ [7].

- We call $G$ in this case an invariance group for $f$. 
Example $h = G(\neg(c_1 \land c_2))$, KS of two processes with the group $G$.

- $h$ is symmetric under $G=\{1, \sigma(S_1, S_2)\}$: $f = \neg(c_1 \land c_2)$
Quotient Models

- **Theorem[7]:** $h$ a CTL* formula, $G$ is an invariance group for each maximal propositional subformula $f$ in $h$, then
  - $M, s \models h \iff M_G, \theta(s) \models h \mid h$ is a state formula
  - $M, \pi \models h \iff M_G, \pi_G \models h \mid h$ is a path formula

- Result: MC performed on **massively reduced** model
Model checking with symmetry, reachability algorithm

- Need to find reachable states in KS, to check whether an error state could be reached.

- **Reachability algorithm** uses the unique representative function $\xi(s)$
  - ... starts with $\xi(s_0): s_0 \in S_0$
  - ... adds them to: Reached, Unexplored
  - ... removes a state from Unexplored
  - ... adds its next ‘states’ to Reached & Unexplored
  - ... circulates until Unexplored is empty.

- Could be extended to a full CTL MC algorithm[9].
Model checking with symmetry, representative function

- Construction of $\xi(s)$ requires efficient computation of $\Theta$
- Orbit relation: $\Theta(s, s') \equiv (s \in \theta(s'))$
- ... is the least fixed point of the equation\[ Y(s, s') \equiv (s = s') \lor (\exists s'')(Y(s, s'')) \land (s'' = g_1 s' \lor \cdots \lor s'' = g_k s') \]
- This fixed point is computable using BDDs for a given BDD-representation of $M[2]$. 
Function **Compatible** with a Relation, e.g.

\[ \mathcal{F}(s, s') \mid (s, s') \in \mathcal{R} \land \forall s''((s, s'') \in \mathcal{R} \implies \mathcal{N}(s'') \geq \mathcal{N}(s')) \]

**Usefulness:** unique representation of states.
Projection example
Projection example

\[ \sigma = (S_1, S_2) \]
Model checking with symmetry, representative & orbit relation

- $\xi \equiv projection(\Theta) \implies \text{presentable by BDDs}[8]$.  
- $R_G(x, y) = (\exists x_1)(\exists y_1)(R(x_1, y_1) \land$  
  $\xi(x_1) = x \land \xi(y_1) = y)$
Model checking with symmetry

- Summary:
  - KS over AP: $M=(S,R,S_0,L)$ representable by BDDs
  - Find reachable states using representative function $\xi$
  - $\Theta$ representable as BDD (fix point),
  - $\xi \equiv projection(\Theta)$ also representable as BDDs,
  - $R_G$ representable using $\xi$ as BDDs.
Complexity of orbit calculations

- Complexity: the orbit problem is as hard as graph isomorphism problem (NP-complete)[8].

- $\sigma$ acting on $\{1,\ldots,n\}$, then $\sigma$ can act on vectors in $B^n$ ($B = \{0,1\}$) in the way:
  - $\sigma(x_1,\ldots,x_n) = (x_{\sigma(1)},\ldots,x_{\sigma(n)})$

- The orbit problem:
  - $x \in B^n, y \in B^n$: is there a permutation $\sigma \in G$ where $y = \sigma x$?
Conclusion

- Concurrent systems with symmetry can be compressed to decrease MC complexity.
- Construction of Quotient Model ‘equivalent’ to original one. Depending on:
  - Orbit relation $\Theta$
  - Representative function $\xi$
Conclusion

- Complexity of orbit calculations is like graph isomorphism (NP-complete)
- In practice: massive saving in size of states’ space
Conclusion

<table>
<thead>
<tr>
<th>system config.</th>
<th>trans. relation</th>
<th>no symmetry</th>
<th></th>
<th>processors</th>
<th>symmetry cache lines</th>
<th>combination</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>BDD nodes</td>
<td>BDD nodes</td>
<td>time sec.</td>
<td>BDD nodes</td>
<td>time sec.</td>
<td>BDD nodes</td>
</tr>
<tr>
<td>2P2C</td>
<td>631</td>
<td>920</td>
<td>2</td>
<td>668</td>
<td>1</td>
<td>368</td>
</tr>
<tr>
<td>4P2C</td>
<td>8,534</td>
<td>6,048</td>
<td>11</td>
<td>2,573</td>
<td>4</td>
<td>2,855</td>
</tr>
<tr>
<td>2P4C</td>
<td>1,519</td>
<td>6,166</td>
<td>36</td>
<td>3,917</td>
<td>18</td>
<td>1,458</td>
</tr>
<tr>
<td>4P4C</td>
<td>22,154</td>
<td>42,595</td>
<td>231</td>
<td>14,626</td>
<td>62</td>
<td>6,831</td>
</tr>
<tr>
<td>2P8C</td>
<td>3,295</td>
<td>17,446</td>
<td>756</td>
<td>10,837</td>
<td>407</td>
<td>2,618</td>
</tr>
<tr>
<td>4P8C</td>
<td>49,394</td>
<td>121,475</td>
<td>5,911</td>
<td>40,466</td>
<td>1,400</td>
<td>11,551</td>
</tr>
<tr>
<td>2P12C</td>
<td>5,071</td>
<td>28,726</td>
<td>5,136</td>
<td>17,757</td>
<td>2,884</td>
<td>3,778</td>
</tr>
<tr>
<td>4P12C</td>
<td>76,686</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>16,271</td>
</tr>
</tbody>
</table>

[8]
Considered as an “Initial results on symmetry reduction for model checking”[5]. Emphasis on progress in applying tech. on realistic systems.

- Difficulties in symmetry detection: reachability of “breaking-symmetry” states is like model checking without symmetry [5].

- Language Tailored for Symmetry: Murφ, first explicit-state model checker to exploit symmetry [5].

- [6] developed alternative approach to exploit symmetries without manipulating & comparing encodings of reachable states
References


