Scalable Verification of Design with Multiple Properties

Rohit Dureja
Iowa State University

fmcad.19
October 23, 2019
Model Checking

Model $M$ → Verification Engine(s) → Property $P$ → (Trace)
Model Checking

Usually multiple properties to be verified
Model Checking

Model $M$ 

Verification Engine(s) 

Multiple Properties 

All properties 

Report 
- Proof 
- Trace 
- Other
Make multi-property verification scalable
Multi-Property Verification
Multi-Property Verification

Inter-property Relationships

Find logical dependencies between properties, check minimal set

<table>
<thead>
<tr>
<th>keys</th>
<th>values</th>
<th>result</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\varphi_1$</td>
<td>$T$</td>
<td>$\varphi_1$, $\varphi_2$, $\varphi_3$, $\varphi_4$, $\varphi_5$, $\varphi_6$</td>
</tr>
<tr>
<td>$\varphi_2$</td>
<td>$F$</td>
<td>$\checkmark$</td>
</tr>
<tr>
<td>$\varphi_3$</td>
<td>$T$</td>
<td>$\checkmark$</td>
</tr>
<tr>
<td>$\varphi_4$</td>
<td>$T$</td>
<td>$\checkmark$</td>
</tr>
<tr>
<td>$\varphi_5$</td>
<td>$T$</td>
<td>$\checkmark$</td>
</tr>
<tr>
<td>$\varphi_6$</td>
<td>$T$</td>
<td>$\checkmark$</td>
</tr>
</tbody>
</table>

Property Table

Result Array
Multi-Property Verification

Inter-property Relationships
Find logical dependencies between properties, check minimal set

Information Reuse
Model checking information reused across runs, e.g., state space approximations
Multi-Property Verification

Inter-property Relationships
Find logical dependencies between properties, check minimal set

Information Reuse
Model checking information reused across runs, e.g., state space approximations

Improved Orchestration
Partially order and group properties to maximize information reuse