From One To Many: Checking A Set Of Models

Rohit Dureja and Kristin Yvonne Rozier

Iowa State University

October 4, 2017
Complex systems’ design often requires analyzing several models of the system under development.
Motivation

Complex systems’ design often requires analyzing several models of the system under development.

- Narrowing in on the final system design,
Motivation

Complex systems’ design often requires analyzing several models of the system under development.

- Narrowing in on the final system design,
- Check capabilities of systems with varying features, and
Motivation

Complex systems’ design often requires analyzing several models of the system under development.

- Narrowing in on the final system design,
- Check capabilities of systems with varying features, and
- Regression development to make a design robust.
Motivation

Complex systems’ design often requires analyzing several models of the system under development.

- Narrowing in on the final system design,
- Check capabilities of systems with varying features, and
- Regression development to make a design robust.
Contributions

Lift traditional model checking to model-set checking.

System Model $M$

Requirement $\varphi$

Traditional Model Checker

$M \models \varphi$ -> Proof

$M \not\models \varphi$ -> Error Trace

Model Set $\mathcal{M} = \{M_1, \ldots, M_n\}$

Requirements Set $\mathcal{P} = \{\varphi_1, \ldots, \varphi_m\}$

Model-Set Checker

For every Model-Requirement pair

Report
- Proof
- Trace

From One To Many: Checking A Set Of Models
Results

![Graph showing checking times for different models](image)

- Typical IC3
- Incremental IC3
- FuseIC3
- FuseIC3+Ordering
- FuseIC3+Ranking

**Property ID**

- 0
- 500
- 1000
- 1500
- 2000
- 2500

**Checking time (minutes)**

- 0
- 5
- 10
- 15
- 20
- 25
- 30
- 34

Rohit Dureja

From One To Many: Checking A Set Of Models