Developing an Open-Source, State-of-the-Art Symbolic Model-Checking Framework for the Model-Checking Research Community

Kristin Yvonne Rozier
Iowa State University

23rd Formal Methods in Computer-Aided Design
October 24, 2023

Evolution of Model-Checking Algorithms

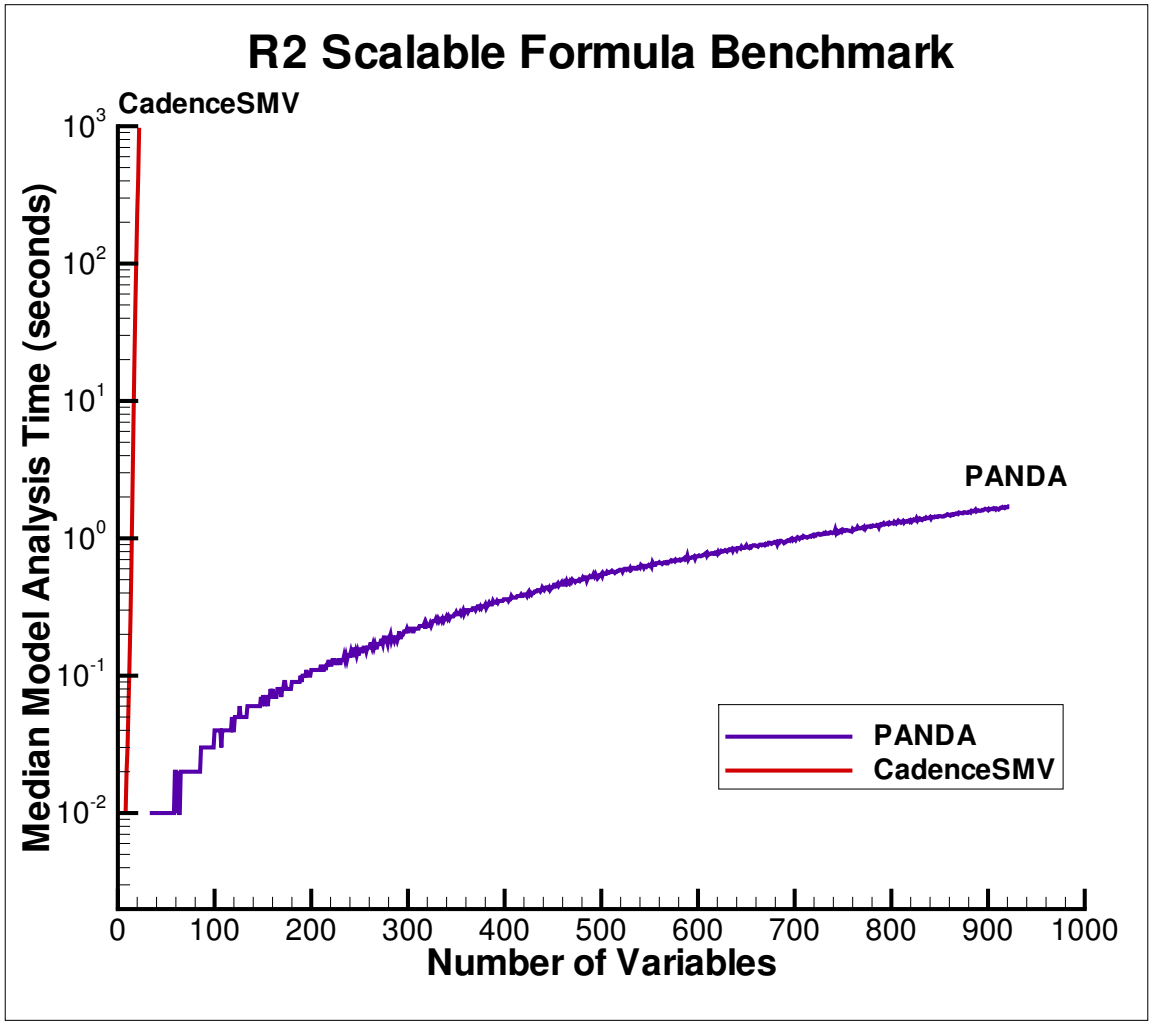
1. BDD-based
2. SAT-based / bounded model checking
3. IC3 / k-liveness

Evolution of Model-Checking Algorithms

1. BDD-based
2. SAT-based / bounded model checking
3. IC3 / k-liveness

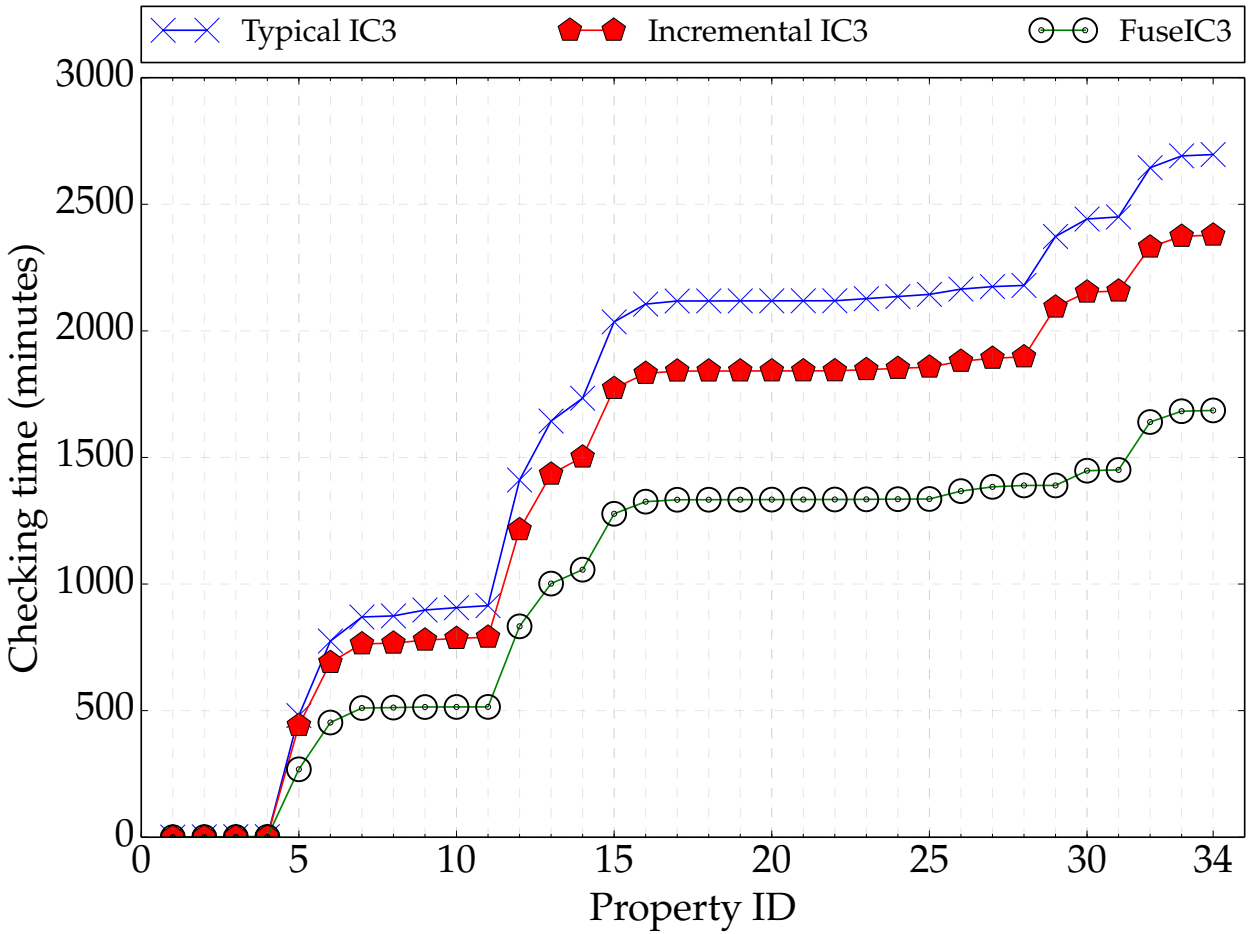
Symbolic model checking progressed from bit-level to word level

The Problem[1]



[1] K.Y.Rozier and M.Y.Vardi, "A Multi-Encoding Approach for LTL Symbolic Satisfiability Checking," FM 2011.

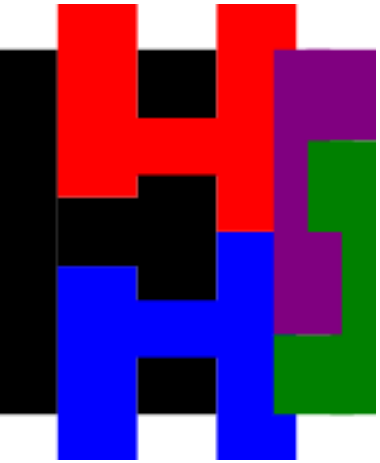
FuseIC3: An Algorithm for Checking Large Design Spaces[2]



Model checking **34 formulas** over **1,620 models** is **5.48x faster**

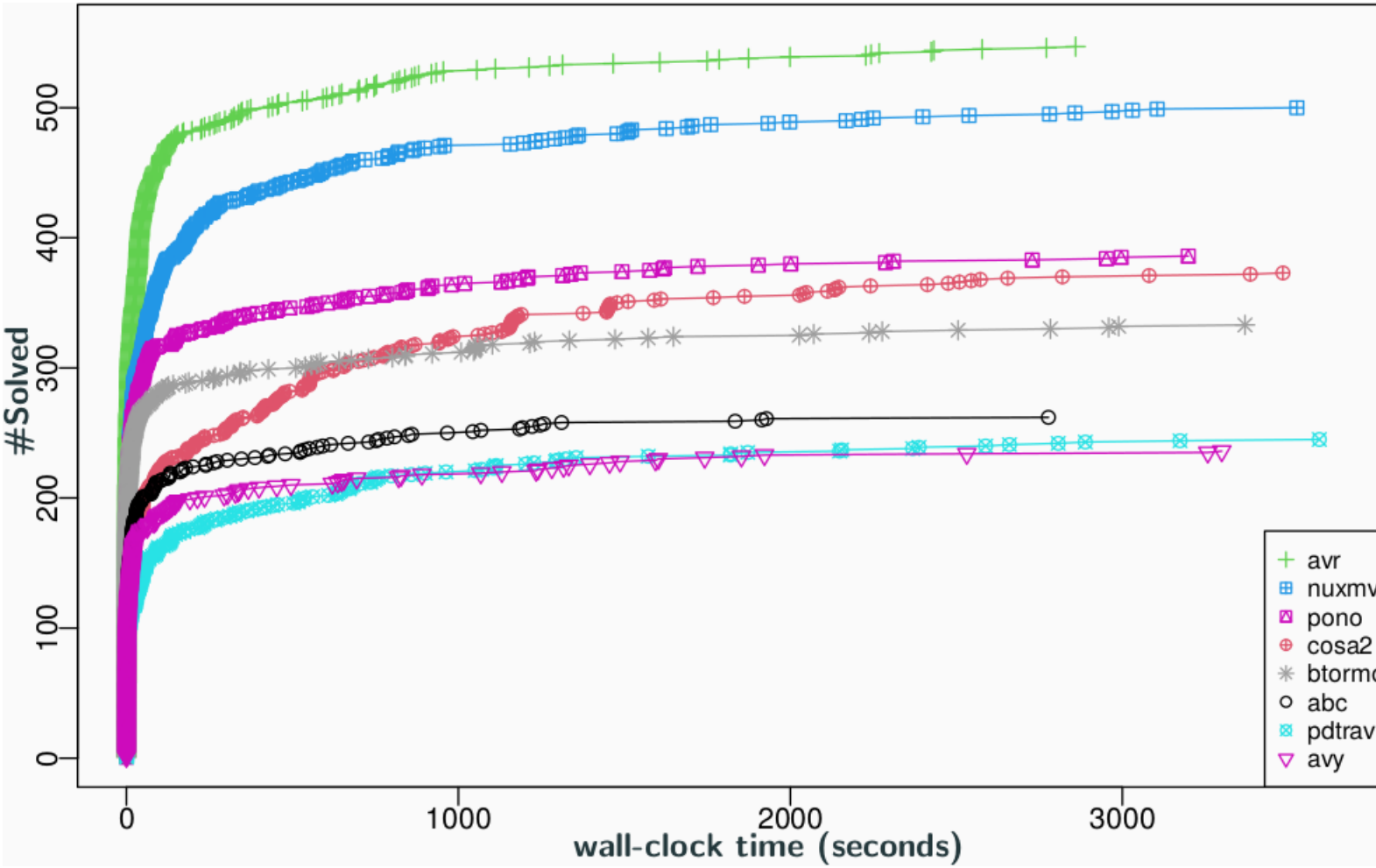
[2] Rohit Dureja and Kristin Yvonne Rozier. "FuseIC3: An Algorithm for Checking Large Design Spaces." In Formal Methods in Computer-Aided Design (FMCAD), IEEE/ACM, Vienna, Austria, October 2-6, 2017.

HWMCC: Hardware Model Checking Competition (2020)



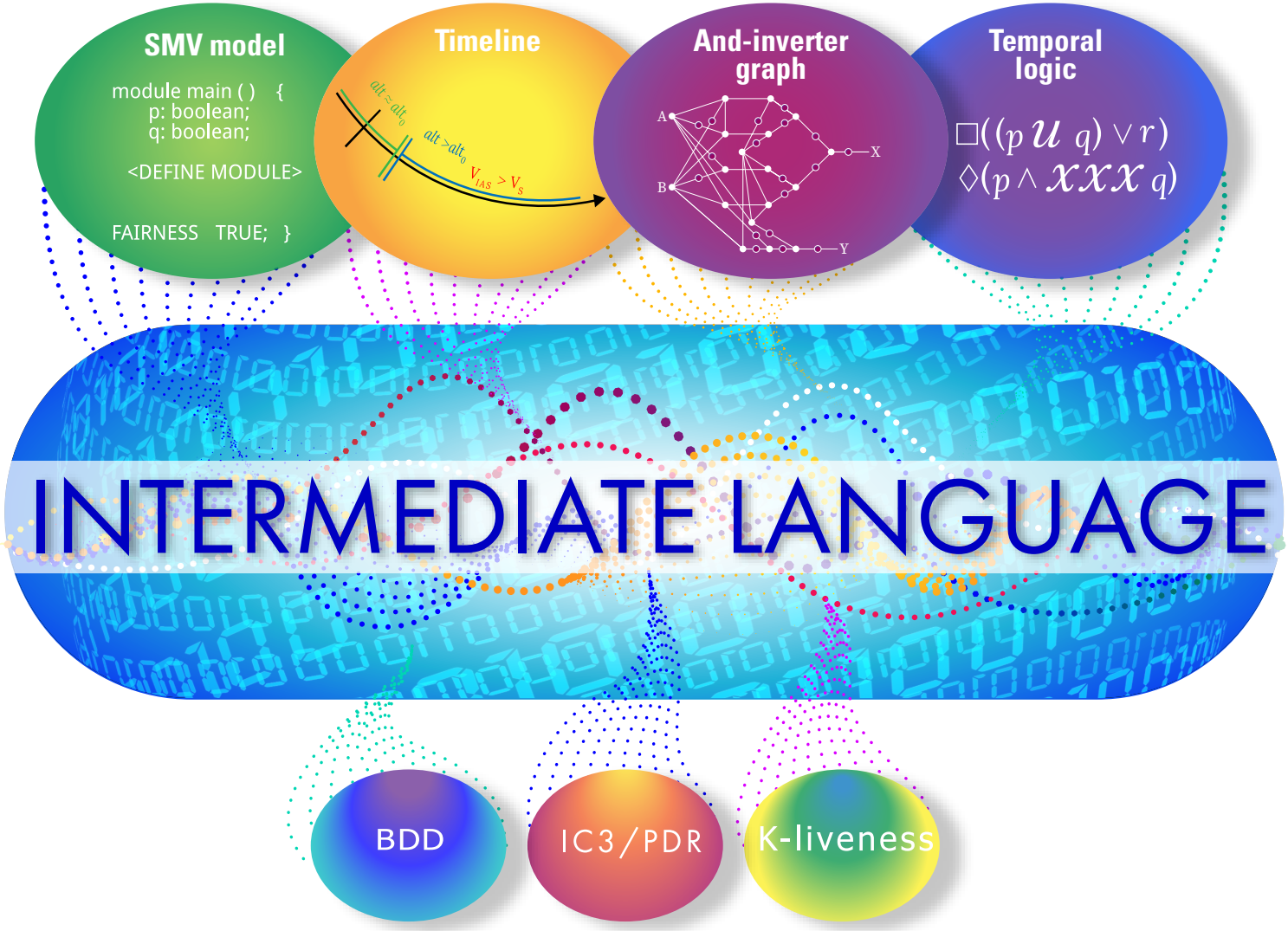
Word-level reasoning

BTOR2



The Problem Continues...

- nuXmv, CadenceSMV, others are **closed source**
- ABC, HWMCC tools are **limited to low-level modeling languages**
- No **open-source, research-enabling connection** between:
  - Rich modeling languages with real-world benchmark models
  - State-of-the-art back-end MC algorithms


SMV model
module main ( ) {
p: boolean;
q: boolean;
<DEFINE MODULE>
FAIRNESS TRUE; }
Timeline
alt ≥ alt0
alt >alt0
VIAS > Vs
And-inverter graph
A
B
X
Y
Temporal logic
□((p U q) ∨ r)
◊(p ∧ XXX q)
INTERMEDIATE LANGUAGE
BDD
IC3/PDR
K-liveness

Goals for Intermediate Language

- Allow adding a **modeling language** via **translation to/from IL**
- Allow adding an **MC algorithm** via **translation to/from IL**
- IL is efficient/accessible so as to **encourage usage in future MCs**
- IL suitable for on-going **community standard**

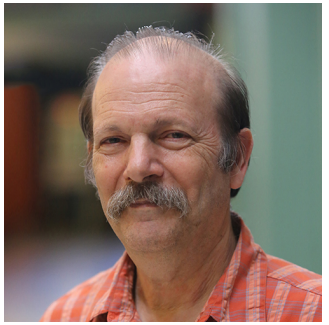
Core Design Team

Investigators:

K.Y. Rozier

Natarajan Shankar

Cesare Tinelli

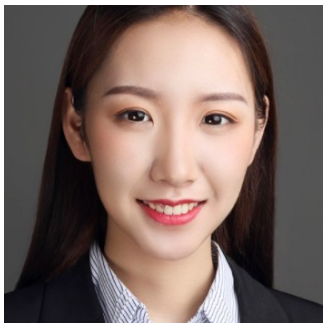


Moshe Vardi

Students:

Laura Gamboa Guzman

Chris Johannsen



Yi Lin

Technical Advisory Board (TAB)

Rajeev Alur (Univ of Pennsylvania)
Clark Barrett (Stanford)
Armin Biere (Albert-Ludwigs Univ)
Nikolaj Bjorner (Microsoft Research)
Dimitra Giannakopoulou (Amazon)
Alberto Griggio (FBK)
Orna Grumberg (Technion)
Aarti Gupta (Princeton)
Arie Gurfinkel (Univ of Waterloo)

Ahmed Irfan (SRI)
John Matthews (Intel)
Ken McMillan (UT Austin)
Alan Mishchenko (Berkeley)
Karem Sakallah (Univ of Michigan)
Bernhard Steffen (TU Dortmund)
Aaron Tomb (Amazon)
Stefano Tonetta (FBK)

Project Links

Home:

https://modelchecker.temporallogic.org

GitHub Organization:

https://modelchecker.github.io/

Intermediate Language Definition:

https://github.com/ModelChecker/IL/blob/main/description.md

Summary

The time has come for model-checking community standards

- **Participate:** name vote, email list, language design feedback, community forums
- Coming Next: **SMV** $\leftrightarrow$ **IL** $\leftrightarrow$ **BTOR2**
- **Contribute** future translators:
  - Your Modeling Language $\leftrightarrow$ Intermediate Language
  - Intermediate Language $\leftrightarrow$ Your Back-end MC Algorithm
- **Optimize! Expand! Compare! Research!**

modelchecker.temporallogic.org

SBMF Keynote: https://www.youtube.com/watch?v=XjkjVPOKVT8