ISCAS 中国科学院软件研究所学术年会 暨重点实验室科技活动周 2025 第十届
学术论文

rIC3硬件模型检测求解器

The rIC3 Hardware Model Checker

37th International Conference on Computer Aided Verification

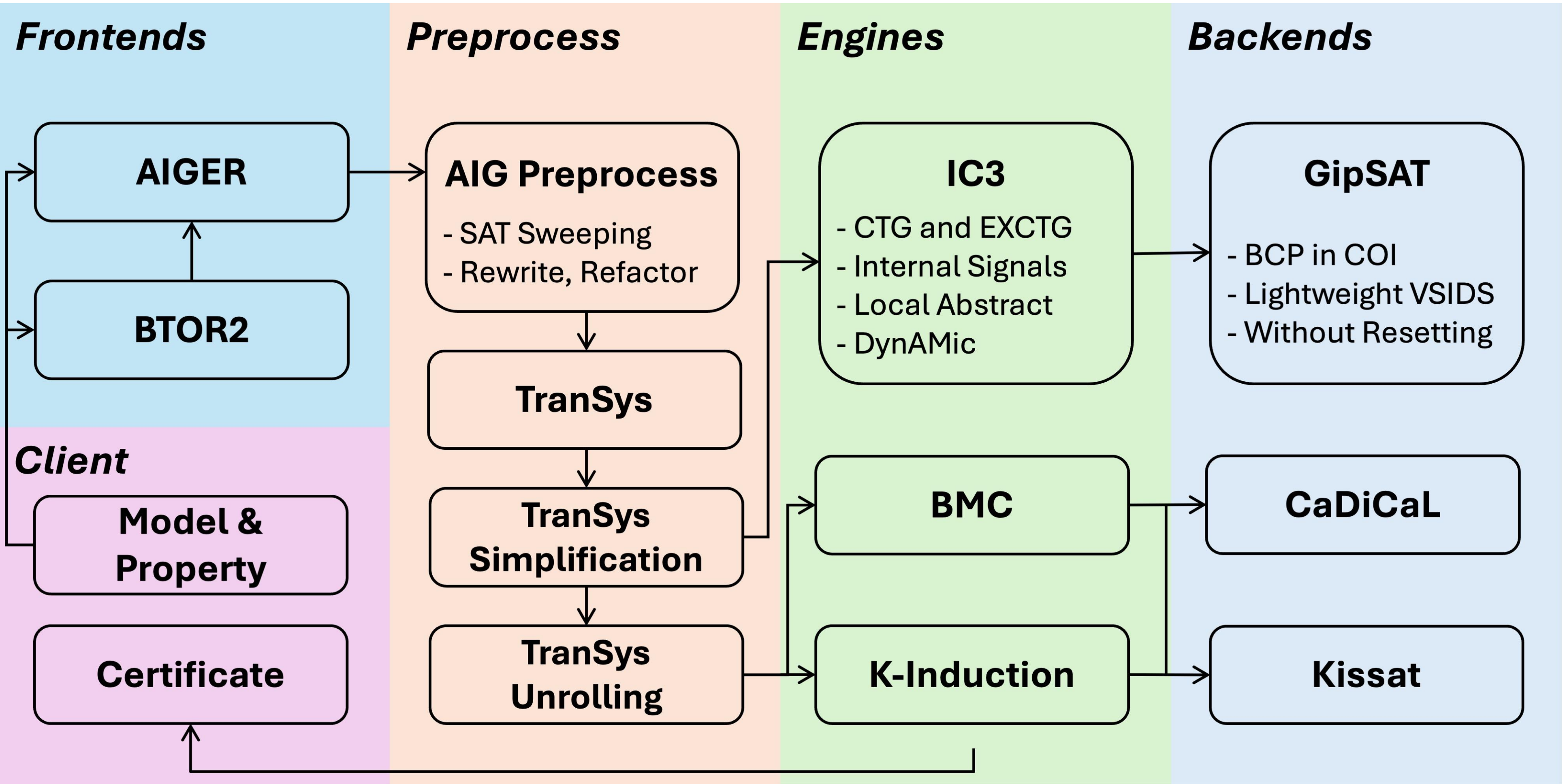
苏宇恒 杨秋松 慈轶为 卜天峻
中科院软件所基础软件国家工程研究中心
{suyuheng2021, qiusong, yiwei, butianjun2024}@iscas.ac.cn

简介

模型检测是一种形式化验证方法，它通过全自动地遍历设计的所有可能状态空间，能够给出证明结果或不满足反例。然而，模型检测的状态空间随着设计规模呈指数增长，因此提升求解器的验证能力和性能一直是一个重要且持续的研究方向。rIC3是一个硬件模型检测求解器，融合了多种近期提出的优化技术，如专门优化的 SAT 求解器、动态推广策略调整机制等。该工具在2024硬件模型检测竞赛（HWMCC24）取得了两个赛道的第一名，相比其他开源工具有较大的领先。rIC3 同时可作为 SymbiYosys 平台验证 RTL 设计的后端工具。其源码模块化程度高，其中 IC3 算法模块结构简洁，便于学术研究。

CAV 2025

DISTINGUISHED PAPER AWARD



Frontends

AIGER

BTOR2

Client

Model & Property

Certificate

Preprocess

AIG Preprocess
- SAT Sweeping
- Rewrite, Refactor

TranSys

TranSys Simplification

TranSys Unrolling

Engines

IC3
- CTG and EXCTG
- Internal Signals
- Local Abstract
- DynAMic

BMC

K-Induction

Backends

GipSAT
- BCP in COI
- Lightweight VSIDS
- Without Resetting

CaDiCaL

Kissat

采用的技术

- 深度优化的SAT求解器：rIC3 针对 IC3 中简单、高频的查询开发了深度优化的轻量级 SAT 求解器。它通过分析影响锥限制变量赋值范围，并用常数时间桶结构替代 VSIDS 的堆操作，显著降低了求解开销，还支持临时子句，避免频繁重置。
- 更强的泛化方法：CTG与EXCTG。IC3 中的 CTG 推广在传统基础上引入了阻断反例的机制。rIC3 还采用了 EXCTG 作为进一步优化，它不仅阻断当前前驱，还递归向上传播，能覆盖更多不可达状态，提升泛化效果。
- 动态调整泛化策略：CTG 和 EXCTG 虽然效果更好，但计算代价更高。rIC3 引入动态策略，根据阻塞坏状态的“难度”自动调整使用何种泛化方法，既保证了泛化效果，又控制了性能开销。
- 基于内部信号的谓词抽象：传统 IC3 只使用状态变量构造不变式，rIC3 扩展为同时考虑设计中的内部信号，能生成更精简的不变式，提升在复杂电路上的验证效率。
- 基于约束的局部抽象：为降低验证难度，rIC3 初始阶段会抽象掉全部约束，仅在反例触发后逐步添加必要部分。相比对转移关系抽象，这种方法更轻量，也更灵活。

实验评估

我们将 rIC3 与当前主流的开源 IC3 实现进行了对比实验，使用了来自硬件模型检测竞赛的 840 个基准用例，设定时间限制为 1 小时，内存限制为 32GB。实验结果如图所示，rIC3 在可扩展性和求解效率方面均显著优于其他求解器，展现出强大的求解能力。

Tools	Solved(840)	TO	MO	PAR-2	Unique	Best
rIC3-ic3	606	225	9	2147.70	61	398
nuXmv-cav23	533	302	5	2777.30	8	41
ABC-pdr	516	320	4	2900.99	1	80
Avy	488	350	2	3142.87	29	38
IC3ref	486	353	1	3169.29	1	59
AVR-ic3sa	353	481	6	4305.24	22	53
Pono-ic3ia	311	518	11	4652.29	1	7
Pono-ic3sa	212	614	14	5459.96	0	5