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

为IC3算法深度优化SAT求解器

Deeply Optimizing the SAT Solver for the IC3 Algorithm

37th International Conference on Computer Aided Verification (CAV 2025)

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

摘要

IC3/PDR算法，由于其高效性、可扩展性和完备性，近年来在模型检测领域产生了重大影响。我们针对IC3模型检测算法中的SAT求解过程提出多项优化，旨在提升其效率和可扩展性。通过分析SAT查询的特点，我们提出仅对部分变量做决策以减少不必要的搜索；用常数时间的桶结构替代VSIDS中的二叉堆；并引入无需激活变量的临时子句机制，避免频繁重置求解器。基于这些优化，我们实现了轻量级SAT求解器GipSAT。实验证明，GipSAT支持的IC3实现相比基于MiniSat的版本在求解时间上平均加速3.61倍。

简介

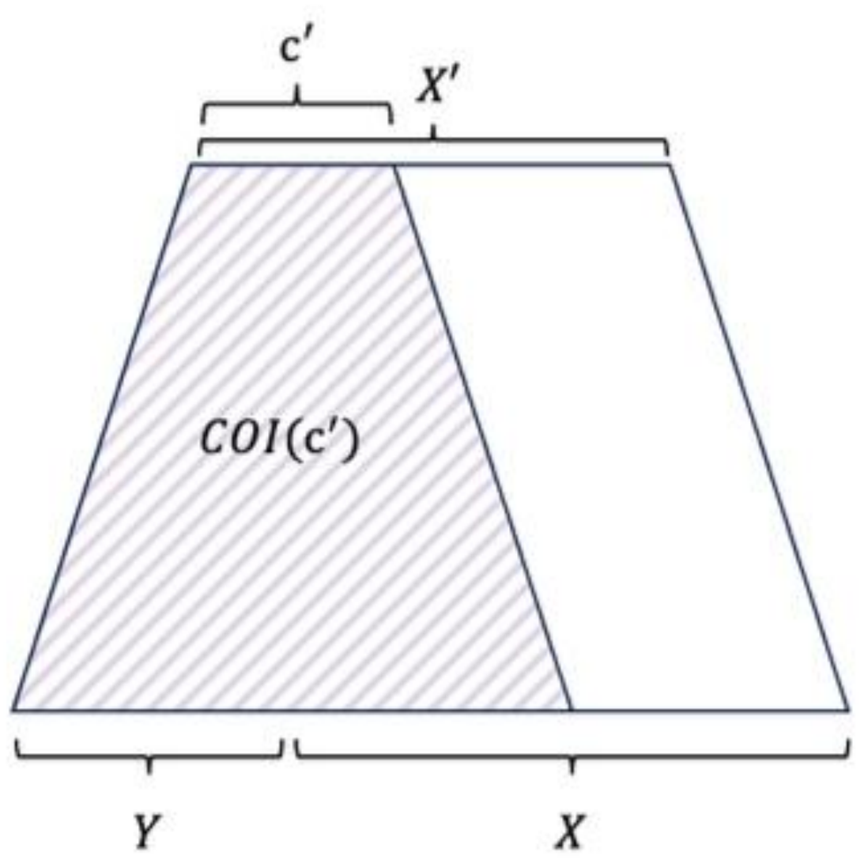
IC3算法是一个在硬件模型检测中广泛使用的基于SAT的算法，它是许多最先进的模型检测器的主要引擎，具有很高的影响力。它致力于寻找归纳不变式，这个不变式是从一系列帧$F_0 \dots F_k$中推导出来的，其中每个F_i代表迁移系统经过小于等于i步的状态空间的过近似。当存在某个i，使$F_i = F_{i+1}$，表示已经找到了归纳不变式，证明迁移系统满足安全属性，或者当找到一个真正的反例时，证明系统不满足，该过程终止。

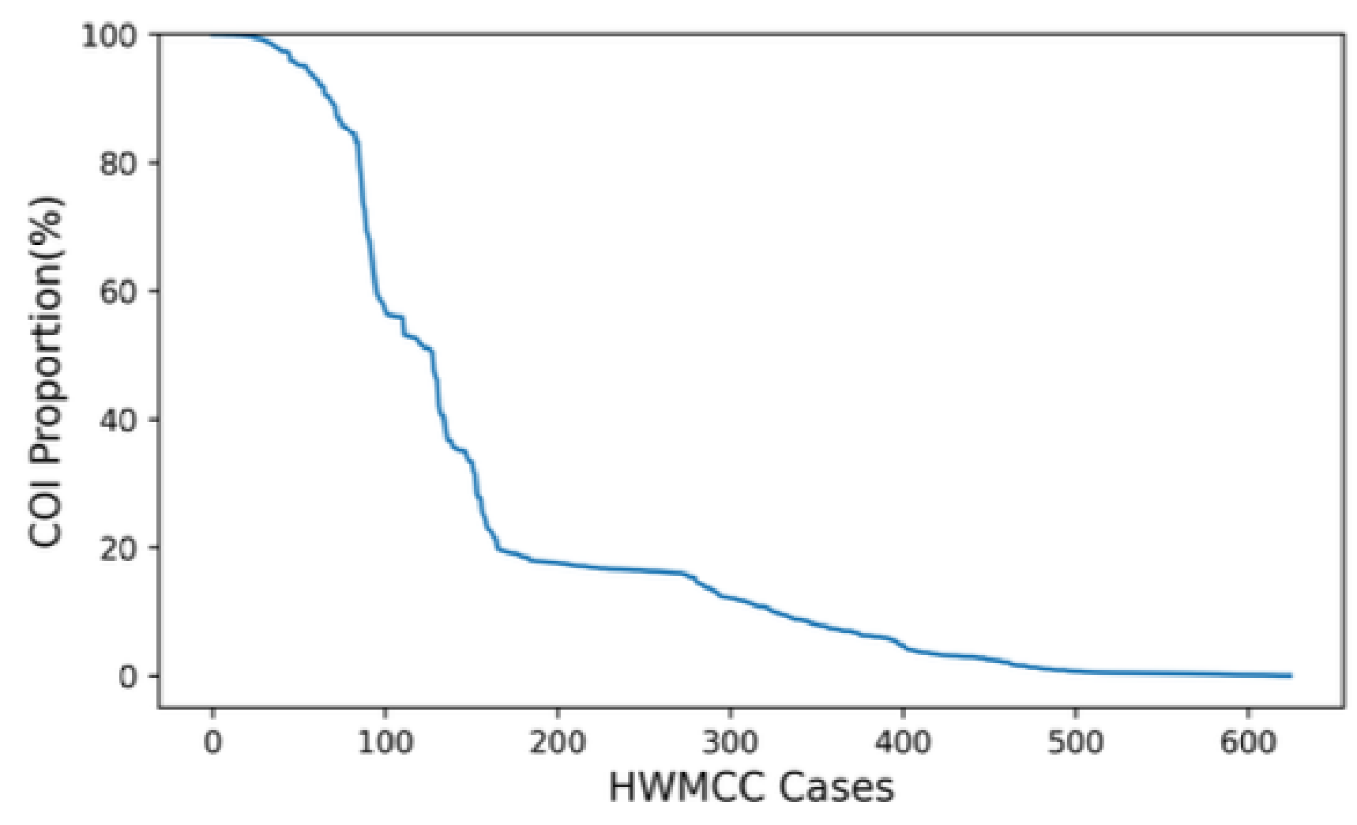
IC3算法是一个基于SAT求解器的模型检测算法，目前的IC3算法通常是一个两层结构，上层为IC3算法层，下层为SAT求解器层。算法层通过不断构造SAT问题并交给求解器，拿到求解器的结果后再进一步决策。提升IC3所依赖的SAT求解器性能可以有效的提升IC3算法的整体性能。

优化方法

在 IC3 中，Q_{relind}：$F_i \wedge c \wedge T \wedge \neg c'$ 表示用于判断是否存在某个满足 $F_i \wedge c$ 的 $\neg c'$ 的前继状态。我们发现，求解 Q_{relind} 并不需要考虑所有变量的赋值。如下图所示，整个梯形是一个电路的结构，由于$\neg c'$只依赖其 逻辑锥（COI）内的变量，如紫色区域所示，其他变量的取值不会影响结果，因此我们在每次求解中并不需要对所有变量进行赋值。右图展示了我们对一些测试用例的求解过程中COI所占全部变量比例的平均值的统计结果，可以看到在大部分测试用例中，COI只占20%左右，这意味着我们可以在求解时只关注一小部分变量，从而提升求解效率。

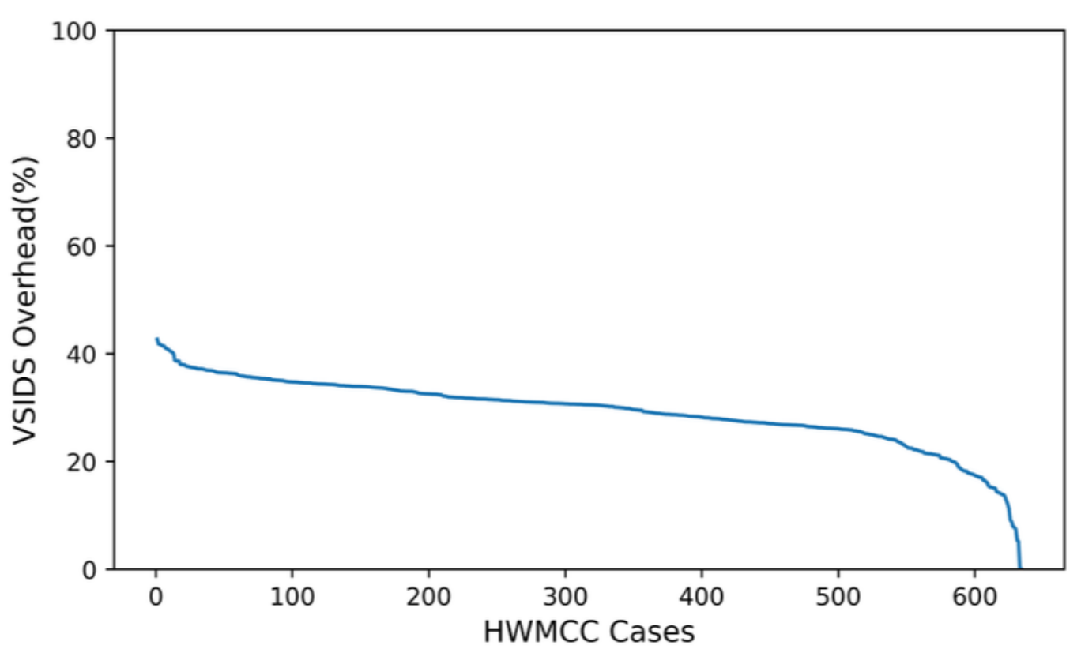
对于 $F_i \wedge c$，我们只需要关注公式中存在的变量就可以知道可满足性。而对于 $T \wedge \neg c'$，我们只需要关注紫色区域的变量，也就是$COI(c')$的变量。每次求解前动态计算当前的需要考虑的变量，并将其中变量加入 VSIDS 的决策候选集，限制布尔约束传播仅对需要考虑的变量的传播与赋值。该策略有效避免无关变量的传播，显著减少 SAT 求解中的开销。





SAT 求解器通常使用 VSIDS 启发式通过二叉堆进行变量决策，我们测量了其操作开销，如下图。结果表明 VSIDS 的开销不可忽略，大多数用例约为 30%。这可能是由于 IC3 查询较简单，而 VSIDS 的对数级堆操作相较于常数时间的赋值操作开销更大，因而显得突出。受桶排序启发，我们设计了一种新的 VSIDS 数据结构，将变量按得分分配到预设的多个桶中，桶号越小得分越高。桶之间保证有序，但桶之内是无序的。每次在决策变量时，从分数最大的桶中拿一个变量，这一方法可以有效的将VSIDS操作将地位常数时间。

同时由于 Q_{relind} 每次需要引入临时子句，目前主流的方法通过引入激活变量来实现。但是每次求解需要创建一个新的变量，随着多次调用后会降低求解性能。我们提出了一种支持临时子句的方法，可以证明如果学习子句依赖临时子句，也一定会包含激活变量，我们通过单独记录这些子句并在求解后删掉，可以反复利用一个激活变量，避免了重启。



实验评估

我们将优化后的 SAT 求解器 GipSAT 集成到 rIC3 模型检测器中，并与 MiniSat、CryptoMiniSat 和 CaDiCaL 进行了对比。同时，我们还比较了 ABC 和 nuXmv 中的 IC3 引擎。实验采用硬件模型检测竞赛中的 635 个基准用例，设置内存上限为 16GB，时间限制为 1 小时。

实验结果如图所示。从运行时间来看，GipSAT 相比表现最好的常规求解器 Minisat 多解决了 23 个用例，显著提升了 IC3 算法的求解效率。下表最后一列给出了 GipSAT 相对于各常规求解器在求解时间上的几何平均加速比。结果表明，GipSAT 在 rIC3 中相较于 Minisat 平均加速达到 3.61 倍，显示出明显的效率优势。这些实验结果充分验证了所提出优化方法的有效性。

Configuration	#Solved	ΔSolved	#Safe	#Unsafe	Avg. ST Ratio	PAR-2
rIC3-GipSAT	392	0	326	66	x1.00	2843.50
rIC3-Minisat	369	-23	309	60	x3.61	3140.95
rIC3-CryptoMinisat	364	-28	310	54	x4.83	3216.31
rIC3-CaDiCaL	366	-26	311	55	x5.99	3189.09
ABC	357	-	305	52	-	3258.97
nuXmv	353	-	301	52	-	3289.72