中国科学院软件研究所学术年会’2017
暨计算机科学国家重点实验室开放周

学术论文

面向概率时间自动机模型检测的判定图

纪玮　王凡　吴鹏 (wp@ios.ac.cn)　吕毅

中国科学院软件研究所计算机科学国家重点实验室　國立臺灣大學電機工程學系

Wei Ji, Farn Wang, Peng Wu, Yi Lv: An Experiment on Decision Diagrams for Model Checking Probabilistic Timed Automata. ICECCS 2016: 111-121

我们的工作

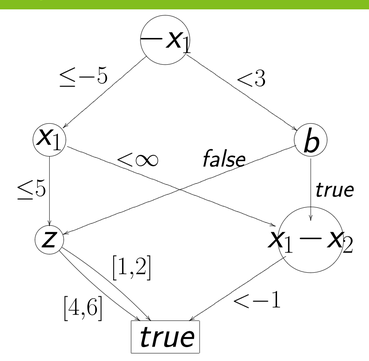
- 提出基于 RED 判定图的概率时间自动机符号模型检测方法及工具 PROB-RED
  - RED 判定图的概率扩展
  - RED 建模语言的概率扩展
  - 下载网址：https://github.com/wolvre/probred
- 与主流概率时间自动机验证工具对比，有效降低时间开销，并提高可扩展性（scalability）

概率时间自动机模型检测

- 经典方法
  - 基于时间自动机的模型检测算法，如 UPPAAL
  - 基于 Markov 判定过程的模型检测算法，如 PRISM
- 对概率时间自动机状态的离散和连续部分的表示是分离的.
  - BDD、MTBDD 等表示离散状态变量和概率
  - DBM、CDD、DDD 等表示连续时钟（clock）约束
- 我们基于 RED 判定图提出概率时间自动机状态的**集成**表示方法 - 概率 RED 判定图
  - 以改进概率时间自动机模型检测方法的效率和可扩展性
  - “集成”思路源于 RED 判定图在时间自动机模型检测方面取得的成功

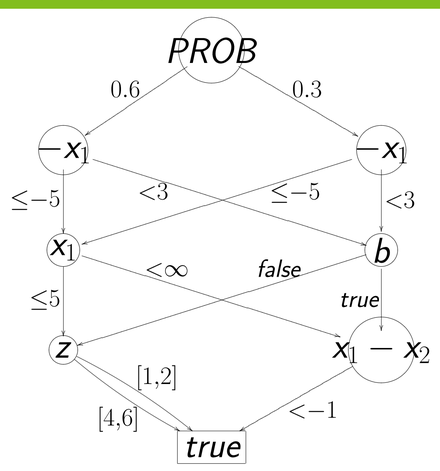
“集成”的秘密 - 结构共享

- RED - 时间自动机符号模型检测工具
- RED 判定图 - 时间自动机状态的集成表示，包含：
  - 多值判定图（Multi-value Decision Diagram，MDD）
  - 时钟限定图（Clock-Restriction Diagram，CRD）
- 高效的结构共享

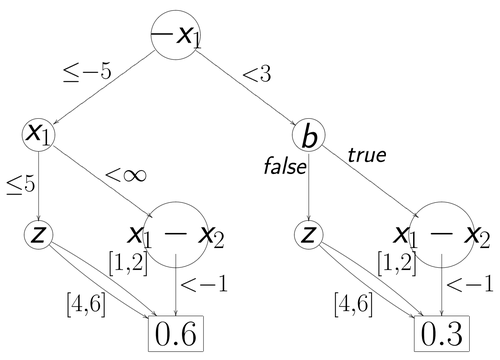


Farn Wang, Efficient Verification of Timed Automata with BDD-like Data-Structures. International Journal on Software Tools for Technology Transfer (STTT), 2004, 6(1):77-97

我们提出的 RED 判定图概率扩展方式与主流方式不同



概率 RED 判定图 ☺



与 MTBDD 类似的扩展方式 ☹

RED 建模语言的概率扩展

- PRISM 模块（Modules）对应于 RED 模式（Modes）
- PRISM 卫式（Guarded）概率分支（branches）对应于 RED 卫式语句（statements）
- 概率值单独声明
- PRISM 动作标签（labels）对应于 RED 通道（Channels）
- 在 RED 模型中引入 *Signal* 进程模拟 PRISM 模块间的同步

PRISM 概率时间自动机基准模型（Benchmarks）

5 个网络 / 安全协议

- IEEE 1394 firewire root contention protocol (*fw*,*fw_a*)
- IEEE 802.3 CSMA/CD protocol (*csma*)
- Non-repudiation service protocol, with honest recipients (*nrp_h*)
- Non-repudiation service protocol, with malicious recipients (*nrp_m*)
- IPv4 Zeroconf network configuration protocol (*zeroconf*)

后向可达性（Backwards Reachability）分析

- 量化可达性

$$P_{\max=?}[F\ \phi] \quad P_{\min=?}[F\ \phi]$$

- 值迭代算法

$$\bigwedge_{\eta \in V} P^+_{k+1}(\eta) = \max_{\eta \xrightarrow{b} \mu} \sum_{\alpha \in Assigns(\mathcal{X},\mathcal{Y})} \mu(\alpha) \cdot P^+_k(\eta\alpha)$$

$$P^+_0(\eta \wedge \langle\phi\rangle) = 1.0$$

- 有限时钟变量集 $\mathcal{X}$, 有界时钟区间（zones）
- 有限离散变量集 $\mathcal{Y}$, 有界值域
- 因此，有限符号状态集 V
- 与 PRISM 概率时间自动机后向可达性模型检测引擎类似

实验 1：不同参数（变量值域）

Model	*K*	*C*	PROB-RED *time*(s)	PROB-RED *CPU*(s)	PROB-RED *prob.*	PRISM (Backwards Reachability) *time*(s)	PRISM (Backwards Reachability) *CPU*(s)	PRISM (Backwards Reachability) *prob.*	PRISM (Stochastic Games) *time*(s)	PRISM (Stochastic Games) *CPU*(s)	PRISM (Stochastic Games) *prob.*
csma	2	4	0.647	0.527	0.143555	0.795	0.687	0.143555	4.214	3.239	0.143555
	2	5	0.814	0.691	0.062805	0.954	0.813	0.062805	7.308	4.686	0.062805
	2	6	0.895	0.748	0.027477	1.077	0.896	0.027477	10.022	7.679	0.027477
	2	7	1.122	0.993	0.012021	1.355	1.190	0.012021	12.286	10.107	0.012021
	2	8	1.348	1.186	0.005259	1.484	1.223	0.005259	17.321	14.584	0.005259
	4	4	2.273	1.855	0.076904	3.274	3.023	0.076904	23.835	20.997	0.076904
	4	5	2.734	2.418	0.009313	3.947	3.421	0.009313	112.541	100.983	0.009313
	4	6	3.105	2.720	0.001127	4.512	4.240	0.001128	202.450	190.763	0.001128
	4	7	3.445	3.127	0.000137	4.984	4.521	0.000137	314.087	291.375	0.000137
	4	8	3.781	3.397	0.000017	5.379	4.864	0.000017	821.337	782.512	0.000017
	6	4	5.766	5.013	0.076904	10.445	9.521	0.076904	272.488	255.786	0.076904
	6	5	8.748	6.082	0.009313	16.160	14.335	0.009313	7786.092	7637.475	0.009313
	8	4	14.245	13.115	0.076904	170.953	154.474	0.076904	×		
	8	5	31.830	22.580	0.009313	391.266	362.177	0.009313	×		

Model	PROB-RED *time*(s)	PROB-RED *CPU*(s)	PROB-RED *prob.*	PRISM (Backwards Reachability) *time*(s)	PRISM (Backwards Reachability) *CPU*(s)	PRISM (Backwards Reachability) *prob.*	PRISM (Stochastic Games) *time*(s)	PRISM (Stochastic Games) *CPU*(s)	PRISM (Stochastic Games) *prob.*
nrp_h_{min}	0.274	0.228	1.000000	×			0.487	0.442	1.000000
nrp_m_{max}	0.301	0.264	0.105658	0.449	0.408	0.105658	0.516	0.427	0.105658

实验 2：不同模型大小 (*zeroconf*)

#h.	*#s.*	PROB-RED *time*(s)	PROB-RED *CPU*(s)	PROB-RED *prob.*	PRISM (Backwards Reachability) *time*(s)	PRISM (Backwards Reachability) *CPU*(s)	PRISM (Backwards Reachability) *prob.*	PRISM (Backwards Reachability) *#st.*	PRISM (Backwards Reachability) *#tr.*
1	1	0.291	0.232	0.001298	0.343	0.302	0.001298	31	43
2	2	3.521	2.876	0.002595	×				
3	3	64.096	57.410	0.003889	×				
4	4	1057.016	989.354	0.005184	×				

#h.	*#s.*	PRISM (Stochastic Games) *time*(s)	PRISM (Stochastic Games) *CPU*(s)	PRISM (Stochastic Games) *prob.*	PRISM (Stochastic Games) *#st.*	PRISM (Stochastic Games) *#tr.*	PRISM (Digital Clocks) *time*(s)	PRISM (Digital Clocks) *CPU*(s)	PRISM (Digital Clocks) *prob.*	PRISM (Digital Clocks) *#st.*	PRISM (Digital Clocks) *#tr.*
1	1	0.321	0.272	0.001302	27	38	0.467	0.404	0.001301	519	684
2	2	94.833	88.018	0.002601	69,853	160,697	×				
3	3	×					×				
4	4	×					×				

总结

	可验证模型数	PROB-RED 降低的 total 时间开销	PROB-RED 降低的 CPU 时间开销
PRISM-Stochastic Games	24	64.0%	66.1%
PRISM-Digital Clocks	9	32.1%	28.4%
PRISM-Backwards Reachability	20	34%	37.1%
PROB-RED	可验证全部 28 个模型		

- 面向概率时间自动机的集成量化状态空间表示 - 概率 RED 判定图
- 保持了 CRD 在表示连续时钟方面的效率优势
- 能够一致处理符号状态及其概率的分析算法
- 更多细节详见以下论文：
  Wei Ji, Farn Wang, Peng Wu, Yi Lv: An Experiment on Decision Diagrams for Model Checking Probabilistic Timed Automata. ICECCS 2016: 111-121

未来工作

- 进一步支持概率时序逻辑
- 进一步优化概率模型检测算法的效率和性能
- 探索验证概率时间自动机其它量化性质，如期望效益（rewards）或成本（costs）等