文章编号:1006-9348(2009)05-0092-04

时间自动机的 LTL性质模型检测研究

彭云全[1,2],魏绪凯[1,2],李广元[1]
(1. 中国科学院软件研究所,北京 100080;2. 中国科学院研究生院,北京 100049)

摘要:为了增强模型检测工具的检测能力,拓宽模型检测技术的应用范围,对基于时间自动机的 LTL性质模型检测进行了研究,对自动机的状态空间的存储方式和状态空间的展开过程进行了分析,讨论了 LTL性质模型检测工具的检测流程和检测算法的实现策略对工具检测性能的影响,针对制约模型工具的检测能力和检测效率的因素,采取了一些相应的优化改进策略。采用了 BDD(二叉决策图)共享存储技术和位编码压缩存储,较有效地减小了空间消耗,缓解了模型检测中状态爆炸引起的内存空间不足问题。与 DTSpin等著名的模型检测工具进行了实验比较,取得了较好的实验结果。

关键词:时间自动机;模型检测;线性时序逻辑性质;二叉决策图共享存储
中图分类号:N945.12 **文献标识码**:B

LTL Model Checking for Timed Automata

PENG Yun-quan[1,2], WEI Xu-kai[1,2], LI Guang-yuan[1]
(1. Institute of Software, Chinese Academy of Sciences, Beijing 100080, China;
2. Graduate School, Chinese Academy of Sciences, Beijing 100049, China)

ABSTRACT: The research on model checking based on timed automata is done in order to enhance the model checking tool's ability and efficiency. The process of the state-space's generation is further analyzed. The design and implementation of the model checking tool that checks LTL properties is well studied, and the results of different strategies are discussed. Some improvements of the generation and storage of the state-space are made to enhance the model checking tool's ability and efficiency. A data structure named BDD(Binary Decision Diagram) is used to reduce the consumption of memory in the process of state-space generation. The experimental results show that this tool is more effective than other similar tools, such as the famous DTSpin.

KEYWORDS: Timed automata; Model checking; LTL property; Binary decision diagram

1 引言

模型检测[1](model checking)技术的发展已经有相当长的一段历史,理论日趋成熟,模型检测工具的种类也越来越丰富。时间自动机[2](Timed Automata)是广泛使用的一种数学模型,LTL(线性时序逻辑[3])是最常用的时序逻辑之一,但是目前基于时间自动机的 LTL性质模型检测工具却比较少,并且已有的这些检测工具它们的性能表现也不是很理想,最主要的制约因素是状态爆炸问题,即时间自动机的状态空间完全展开存储所需要的内存空间过大的问题。目前已经存在的基于时间自动机的 LTL性质模型检测工具采用变量组合来存储表示状态信息,信息存储不够紧凑,信息压缩和共享程度不够高,内存消耗问题比较严重。本文研究了一种新的基于时间自动机的 LTL性质模型检测工具 CTAV,该工具的创新之处在于将 BDD[4](二叉判定图)的共享存储技术引入到了 LTL性质模型检测的状态空间存储当中,给出了状态空间生成过程和状态空间的存储表示的一些优化方法,有效地缓解了状态爆炸问题,提高了检测工具的性能。与目前已经存在的同类型工具相比较,该工具的性能表现取得了非常明显的优势。

基金项目:国家自然科学基金(60673051, 60736017, 60721061);
国家 973计划资助(2002cb312200)
收稿日期:2008-03-19 修回日期:2008-04-21

2 基本概念和原理

2.1 实时系统和时间自动机

实时系统是能及时响应外部发生的事件,并以足够快的速度完成对事件处理的计算机应用系统。实时系统要求对外部事件的响应必须在一定时间内完成,保证在规定的时间限度之内做出响应是实时系统设计的关键。航天控制系统、实时通信系统等都是实时系统的代表。实时系统的特点和应用场合决定了其正确性可靠性至关重要。为了确保实时系统的正确性可靠性,更改系统设计中可能存在的缺陷,利用模型检测技术对其进行分析检测是十分必要的。

时间自动机是对实时系统建模的一种形式化方法。时间自动机是一个六元组 $<L, l_0, \Sigma, X, I, E>$，其中：

1)X为时钟变量的有限集合，C(X)为 X上时钟约束的集合，其语法定义如下：

$\Phi ::= x \sim c \mid \phi_1 \wedge \phi_2 \mid true$ 其中 $x \in X$, $\sim \in \{<, \leqslant, =, \geqslant, >\}$, $c \in N^+$

2)L为状态的非空有限集合，$l_0 \in L$为初始状态；

3)映射 $I: L \to C(X)$为每个状态指定时间约束，称为状态的不变量；

4)Σ为字母的有限集合；

5)$E \subseteq L \times C(X) \times \Sigma \times 2^X \times L$是迁移的集合。迁移 $(l, \phi, \sigma, Y, l') \in E$表示在满足约束条件 ϕ的前提下，通过标号为 $\sigma \in \Sigma$的迁移，状态 l可以迁移到它的后继状态 l'。与此同时，属于重置时钟集 Y($Y \subseteq X$)的时钟被重置。

2.2 LTL性质的模型检测原理

给定时间自动机 $M = <L, l_0, \Sigma, X, I, E>$，当时钟变量的值超过 M中出现的最大常数时，可以看作是处于同一个等价类中，这样时钟赋值集 μ_X可以划分成有限个等价类，利用该等价类做商自动机可以得到一个与 M具有相同接受语言的 Büchi自动机 M_B。

给定 LTL公式 φ，要检验性质 φ是否被时间自动机 M所满足，可以先将公式 $\neg\varphi$转化为一个自动机 $M_{\neg\varphi}$[6]，然后检验 M_B与 $M_{\neg\varphi}$的合成 $M_B \| M_{\neg\varphi} \|$。若 $M_B \| M_{\neg\varphi}$为空，则性质 φ被自动机 M所满足；反之若 $M_B \| M_{\neg\varphi}$不为空，则性质 φ不被自动机 M所满足。

在模型检测过程中，检测 $M_B \| M_{\neg\varphi}$是否为空相当于寻找是否存在一个从初始状态出发可达的强连通图，且此强连通图的边覆盖所有的可接受条件。若能找到这样的强连通图，则 $M_B \| M_{\neg\varphi}$非空。

对模型进行检测的过程中要对状态空间进行遍历搜索，最主要的两个数据结构是一个名为 todo的栈记录待展开的状态和一个名为 past的栈记录已经访问的状态。检测的流程可由图 1来表示。

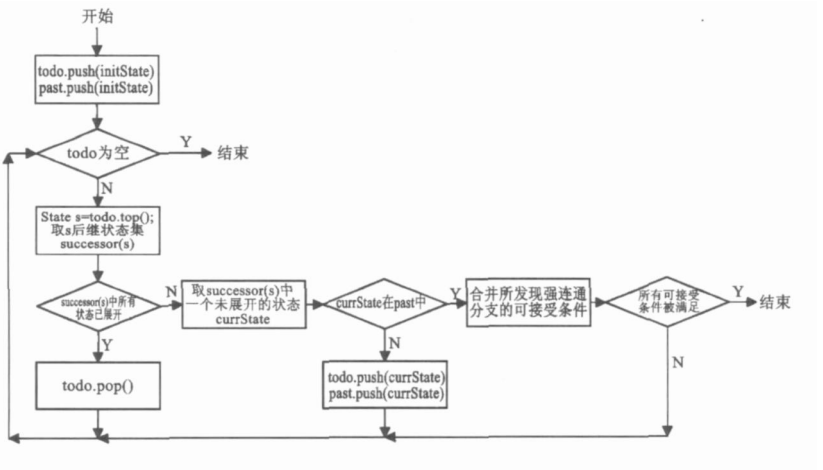

图 1 检测流程图

如果 todo栈为空则状态空间已经完全展开，没有找到满足所有可接受条件的强连通分支，检测过程结束。如果在状态空间遍历的过程中找到了满足所有可接受条件的强连通分支，则记录该强连通分支，检测过程结束。

2.3 模型检测工具

模型检测工具是模型检测算法的具体实现，通过对时间自动机状态空间的穷举搜索，检验时间自动机是否会到达满足性质的状态，来完成性质验证。评价一个检测工具的检测能力，主要是看检测工具对模型规模增长的适应能力。检测工具所能检测的模型规模越大，说明该工具检测能力越强。利用模型检测工具进行性质验证一般需经三个步骤：①系统建模，对要进行验证的系统进行深入分析，对其进行抽象，建立其形式化模型。②性质描述，对系统要满足的性质进行描述，使用逻辑公式来表示。③模型检测，利用模型检测工具验证模型是否满足给定的性质描述。

3 建立模型

要使用模型检测工具解决实际问题，首先要把自然语言能够描述的问题建立合适的仿真模型，即需要用模型检测工具能够识别的语言来描述。对于基于时间自动机的 LTL性质模型检测工具而言，就是要把具体的问题抽象为时间自动机的描述。

下面讨论这样一个问题的模型建立过程。假定有一种只能同时供一人使用的资源，有一个 n个人组成的团队，每个人都随时可能提出使用该种资源的申请，并且申请会在 a时间单位内被处理，申请者进入等待使用资源的队列中。为了防止出现冲突，规定等待者至少等待 b时间单位。若等待的这段时间里没有其他人申请资源，则等待者随时可以使用资源一段时间后释放资源；若有其他人提出资源申请，则等待者重新申请。会不会出现两个人同时使用资源的情况呢？即采用这样的策略能否保证资源的互斥使用，确保在同一段时间里只有一个人在使用资源？这个问题可以由图 2的时间自动机来描述。

图中的时间自动机除 observer外的每个 Process描述了每个人的行为。全局变量 Id记录了当前谁拥有资源使用权，另一全局变量 k记录了资源使用者的个数。每个 Process的状态 idle、req、wait、critical分别代表了空闲、申请资源、等待资源、使用资源几个状态。observer是一个监视进程，一旦使用资源的人数大于或等于 2个，就把标志变量 p置 1。需要检测的 LTL性质是 $<>p$即检测是否有把标志变量 p置 1。

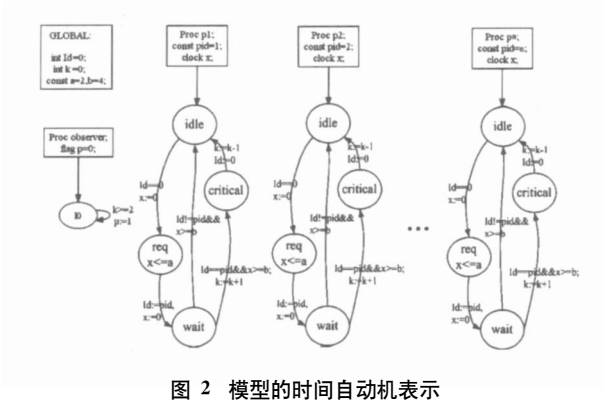

图 2 模型的时间自动机表示

4 检测的策略改进

影响工具检测能力最主要的因素在于时间自动机状态完全展开导致的状态空间爆炸问题。由于状态数目过多,会导致 past栈深度过大,占用的内存资源超过计算机的承受能力时就不能得出有效的检测结果。为此,引入了 BDD[4] (二叉判定图)来存储已经遍历的状态空间。首先要完成的工作是将状态用 BDD符号化表示,即对状态的所有信息进行 BDD编码。BDD用来表示布尔函数,要使用 ROBDD来表示状态,就需要把状态的信息与布尔函数关联起来。状态信息在内存中都可以表示为比特流,一个长度为 m的比特流可以理解为 m个布尔变量进行与运算得到的函数。编码之前需要预先计算状态信息所需要的比特流的长度,对于状态中的某个变量 v,根据其取值范围确定该变量编码所需比特数。BDD的存储效果跟变量的顺序有较大的关系,已有的经验表明为属于同一个进程的变量分配相邻的比特位有助于 BDD的约减,能取得较好的空间压缩效果。影响 BDD存储效果的另一个极为重要的因素是 BDD的存储粒度。BDD存储的状态越多,这些状态在合并约减的过程中所消减的节点可能也越多,BDD的共享存储性能利用得越充分。在状态展开的过程中,为了识别新生成的状态所属的强连通分支,需要记录状态生成的先后顺序,各个状态需要区分存储。当已经确定某些状态属于同一个强连通分支之后,这些状态就可以不再彼此区分,而改用其所在的强连通分支来记录。因此,把 past栈中属于同一个强连通分支的状态合并为状态集,把表示这些状态的 BDD合并为一个 BDD,能极大地降低内存空间的消耗,有效增强工具的检测能力。

5 实验研究

本文所研究的工具称为 CTAV,在采用了一些优化策略进行改进之后,通过实验来验证了这些改进策略对 CTAV性能的影响。实验所使用的检测模型是前文所述的资源互斥使用的模型,模型参数取 a=2, b=4。下面将列出针对上文所述改进策略所进行的实验以及实验所取得的数据,并对数据作简单分析。

5.1 使用 BDD前后比较

引入 BDD作为状态空间的存储数据结构,并没有改变检测算法的流程,因此优化策略并不改变检测结果,检测算法引入优化策略之后的正确性可以得到保证。状态空间采用 BDD存储之后就可以有效利用 BDD的共享存储性能,使得状态信息的存储更紧凑,信息压缩程度更高,可以预期采用改进策略之后的检测工具在空间性能表现上将会有很大的提升,表 1的实验数据和预期的结果取得了一致。

表 1 状态空间展开、存储表示使用 BDD前后结果比较

进程数	不使用 BDD		使用 BDD	
	时间 (s)	空间 (K)	时间 (s)	空间 (K)
2	0. 82	23176	0. 73	35156
3	0. 73	24352	0. 56	30672
4	1. 03	24880	0. 77	35152
5	2. 69	29360	2. 85	33964
6	10. 49	59476	18. 68	38712
7	70. 00	266644	141. 45	66344
8	629. 83	1698812	1346. 73	159440
9	—	—	9986. 56	373828

采用 BDD存储表示状态集合后,有效地利用了 BDD的数据共享效果取得了较为理想的空间表现。进程数较小的时候由于引入 BDD结构带来的附加空间消耗,使用 BDD占用的空间反而可能增大。进程数较大的时候使用 BDD的优势较为明显,使用 BDD的空间消耗可以减少 90%以上。以上实验结果说明 BDD的数据共享技术应用于 LTL性质模型检测工具取得了明显的降低空间消耗的效果。

5.2 与 DTSpin的比较

Spin是由贝尔实验室开发的用于验证并发系统的工具,DTSpin是 Spin的带离散时间变量的扩展,可以用来验证带时间参数的并发系统。表 2给出了 DTSpin和 CTAV分别验证互斥模型所得到的实验数据。

表 2 CTAV与 DTSPin的比较

进程数	DTSpin		CTAV	
	时间 (s)	空间 (KB)	时间 (s)	空间 (KB)
2	0. 12	1493	0. 41	29924
3	0. 15	1698	0. 55	25116
4	0. 32	6596	0. 72	31660
5	3. 67	65104	2. 71	32192
6	—	—	21. 86	35964
7	—	—	127. 04	54168
8	—	—	1226. 49	113776
9	—	—	13081. 58	212952
10	—	—	197962. 39	549448

从表 2互斥模型的检测结果可以看出,当进程数目达到 6个的时候 DTSpin已经不能得出检测结果,而 CTAV仍然可以有效得出检测结果并且检测效率表现良好。随着进程数目增多模型规模增大,CTAV在检测能力和检测效率方面都取得了优于 DTSpin的表现,在空间和时间方面都取得了一

定的优势。当进程数达到 9个以上的时候，CTAV在时间上性能降低明显，但空间消耗仍然控制得较为理想。

6 结论

本文主要介绍了对基于离散时间自动机的 LTL性质检测的一些研究工作，对模型检测工具 CTAV作了改进，通过引入 BDD和采用状态编码压缩降低了内存消耗，提高了CTAV的性能。通过与 DTSpin的比较，可以看出改进后的CTAV在检测能力和检测效率方面都取得了不错的表现。下一步的主要工作为对状态空间的展开过程作进一步优化，减少显式状态到 BDD的转化次数和对 BDD之间逻辑操作进行优化以期获得较好的时间效率。

参考文献：

[1] E M Clarke O Grumberg and D A Peled. Model checking[M]. The MIT Press 1999.

[2] R Alur D L Dill A Theory of Timed Automata[J]. Theoretical Computer Science 1994, 126(2): 183－226.

[3] 李广元，唐稚松. 带有时钟变量的线性时序逻辑与实时系统验证[J]. 软件学报，2002, (1): 33－41.

[4] R E Bryant Symbolic Boolean Manipulation with Ordered Binary－decision Diagrams[J]. ACM Computing Surveys (CSUR) Archive ACM Press 1992, 24(3): 293－318.

[5] Kim Guldstrand Larsen Paul Pettersson and Wang Yi UPPAAL in a nutshell[J]. International Journal on Software Tools for Technology Transfer 1997, 1(1－2): 134－152.

[6] T A Henzinger Pei－Hsin Ho and Howard Wong－Toi HY-TECH: A model checker for hybrid systems[J]. International Journal on Software Tools for Technology Transfer 1997, 1(1－2): 110－122.

[7] C Daws et al The tool KRONOS[C]. In Hybrid Systems III: Verification and Control volume 1066, Rutgers University New Brunswick NJ USA. Springer 1996. 208－219.

[8] A Duret－Lutz D Poitrenaud Spot: an extensive model checking library using transition－based generalized Büchi automata[C]. Volendam, The Netherlands IEEE Computer Society Process 2004. 76－83.

[9] G Behrmann P Bouyer K Larsen and R Pelnek. Lower and upper bounds in zone based abstractions of timed automata[C]. Lecture Notes in Computer Science, Proceeding of TACAS 2004.

[作者简介]

彭云全 (1982－)，男 (汉族)，四川简阳人，硕士研究生，研究方向为实时系统的模型检测理论与工具；

魏绪凯 (1983－)，男 (汉族)，辽宁大连人，硕士研究生，研究方向为实时系统的模型检测理论与工具；

李广元 (1962－)，男 (汉族)，北京人，中国科学院软件研究所副研究员，研究方向为实时系统的模型检测理论与工具。

(上接第 87页)

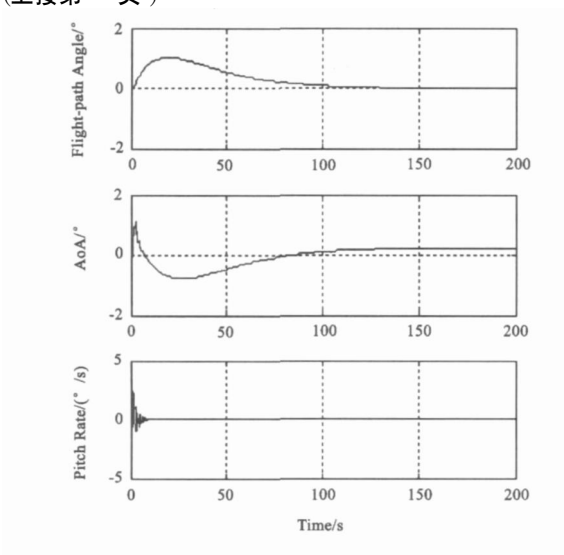

图 7 飞行航迹角、攻角和俯仰角速率随时间变化曲线

AIAA Guidance Navigation and Control Conference and Exhibit Austin Texas Aug 2003.

[4] H Xu M Mirmirani Robust Adaptive Sliding Control for a Class of MIMO Nonlinear Systems[C]. AIAA Guidance Navigation and Control Conference and Exhibit Montreal Canada Aug 2001.

[5] 郭锁凤，等. 先进飞行控制系统[M]. 北京：国防科技出版社，2003.

[6] P G Kevin O S David S Andrea Y Stephen A B Michael B D David Reference Command Tracking for a Linearized Model of an Airbreathing Hypersonic Vehicle[C]. AIAA Guidance Navigation and Control Conference and Exhibit San Francisco California Aug 2005.

[作者简介]

鹿存侃 (1983－)，男 (汉族)，江苏徐州人，博士研究生，研究方向：飞行器制导与控制；

闫 杰 (1961－)，男 (汉族)，陕西西安人，博士，教授，研究方向：飞行器制导与控制。