P.O.Box 8718, Beijing 100080, China	Journal of Software, Jan 2006,17(1):1-10
E-mail: jos@iscas.ac.cn	ISSN 1000-9825, CODEN RUXUEW, CN 11-2560/TP
http://www.jos.org.cn	Copyright © 2006 by *Journal of Software*

有限精度时间自动机的可达性检测

晏荣杰, 李广元, 徐雨波, 刘春明, 唐稚松

晏荣杰1,2, 李广元1, 徐雨波1,2, 刘春明1,2, 唐稚松1
1(中国科学院 软件研究所 计算机科学重点实验室,北京 100080)
2(中国科学院 研究生院,北京 100049)
作者简介: 晏荣杰(1977－),女,河北保定人,博士生,主要研究领域为形式化方法,时序逻辑,实时系统的模型检测方法.李广元(1962－),男,博士,副研究员,CCF高级会员,主要研究领域为时序逻辑,实时及混成系统的建模,形式化验证及模型检测.徐雨波(1980－)男,硕士生,主要研究领域为实时系统的模型检测.刘春明(1979－),男,硕士生,主要研究领域为实时系统的模型检测.唐稚松(1925－),男,研究员,博士生导师,中国科学院院士,主要研究领域为时序逻辑,程序验证,数理逻辑,自动机理论及软件工程.
联系人: 晏荣杰 Phn: +86-10-62562796, Fax: +86-10-62563894, E-mail: yrj@ios.ac.cn, http://www.ios.ac.cn

Received 2004-04-28; Accepted 2005-07-11

Abstract
To relieve the state space explosion problem, and accelerate the speed of model checking, this paper introduces the concept of finite precision timed automata (FPTAs) and proposes a data structure to represent its symbolic states. FPTAs only record the integer values of clock variables together with the order of their most recent resets to reduce the state space. The constraints under which the reachability checking of a timed automaton can be reduced to that of the corresponding FPTA are provided, and then an algorithm for reachability analysis is presented. Finally, the paper presents some preliminary experimental results, and analyzes the advantages and disadvantages of the new data structure.

Yan RJ, Li GY, Xu YB, Liu CM, Tang ZS. Reachability checking of finite precision timed automata. *Journal of Software*, 2006,17(1):1-10.
DOI: 10.1360/jos170001
http://www.jos.org.cn/1000-9825/17/1.htm

摘要
为了缓解状态空间爆炸问题,减小模型检测过程中生成的状态空间,加快模型检测速度,引入有限精度时间自动机(finite precision timed automata,简称FPTA)作为实时系统的形式模型,并提出了一种数据结构SDS(series of delay sequence)符号化表示状态空间中的状态集.FPTA只记录时钟变量的整数值及时钟变化的先后次序,从而减小生成的状态空间.在一定的时间约束下,Alur与Dill提出的时间自动机的可达性检测可简化为FPTA的可达性检测.举例描述了状态空间的生成过程和表示方法.最后,列出部分初步的实验结果,分析了SDS的特点及不足.

基金项目: the National Natural Science Foundation of China under Grant Nos.60273025, 60223005, 60421001 (国家自然科学基金); the National Grand Fundamental Research 973 Program of China under Grant No.2002cb312200 (国家重点基础研究发展规划(973))

References:

[1] Alur R, Dill, DL. A theory of timed automata. Theoretical Computer Science, 1994,126(2):183-235.

[2] Larsen KG, Pettersson P, Wang Y. UPPAAL in a nutshell. Int'l Journal on Software Tools for Technology Transfer, 1997,1(1?2): 134-152.

[3] Daws C, Olivero A, Tripakis S, Yovine S. The tool KRONOS. In: Hybrid Systems III. LNCS 1066, New Brunswick: Springer-Verlag, 1996. 208-219.

[4] Bozga M, Daws C, Maler O, Olivero A, Tripakis S, Yovine S. Kronos: A model-checking tool for real-time systems. In: Hu AJ, Vardi MY, eds. CAV. London: Springer-Verlag, 1998. 298-302.

[5] Wang F. Efficient data structure for fully symbolic verification of real-time software systems. In: TACAS. LNCS 1785, London: Springer-Verlag, 2000. 157-171.

[6] Wang F. Region encoding diagram for fully symbolic verification of real-time systems. In: COMPSAC. Taipei: IEEE Computer Society, 2000. 509-515.

[7] Wang F. Efficient verification of timed automata with BDD-like data-structures. In: VMCAI. London: Springer-Verlag, 2003. 189-205.

[8] Beyer D, Lewerentz C, Noack A. Rabbit: A tool for BDD-based verification of real-time systems. In: CAV. LNCS 2725, London: Springer-Verlag, 2003. 122-125.

[9] Katoen JP. Concepts, Algorithms and Tools for Model Checking. Erlangen-Nurnberg: Friedrich-Alexander University, 1999.

[10] Bosnacki D, Dams D, Holenderski L. A heuristic for symmetry reductions with scalarsets. In: FME. LNCS 2021, London: Springer-Verlag, 2001. 518-533.

[11] Hendriks M, Behrmann G, Larsen KG, Vaandrager F. Adding symmetry reduction to uppaal. In: Larsen KG, Niebert P, eds. FORMATS. London: Springer-Verlag, 2003. 46-59.

[12] Bengtsson J, Jonsson B, Lilius J, Wang Y. Partial order reductions for timed system. In: Sangiorgi D, de Simone R, eds. CONCUR. London: Springer-Verlag, 1998. 485-500.

[13] Daws C, Yovine S. Reducing the number of clock variables of timed automata. In: IEEE RTSS. IEEE Computer Society, 1996. 208-219.

[14] Asarin E, Bozga M, Kerbrat A, Maler O, Pnueli A, Rasse A. Data-Structures for the verification of timed automata. In: Proc. of the Int'l Workshop on Hybrid and Real-Time Systems. LNCS 1201, London: Springer-Verlag, 1997. 346-360.

[15] Alur R, Henzinger TA. A really temproal logic. In: IEEE FOCS. IEEE Computer Society, 1989. 164-169.

[16] Wang F. Formal verification of timed systems: A survery and perspective. Proc. of the IEEE, 2004,92(8):1283-1307.

[17] Bryant R. Graph-Based algorithms for boolean function manipulation. IEEE Trans. on Computers, 1986,35(8):677-691.

[18] Behrmann G, Larsen KG, Weise C, Wang Y, Pearson J. Efficient timed reachability analysis using clock difference diagrams. In: CAV. LNCS 1633, London: Springer-Verlag, 1999. 341-353.

[19] Bozga M, Maler O, Pnueli A, Yovine S. Some progress in the symbolic verification of timed automata. In: CAV. LNCS 1254, London: Springer-Verlag, 1997. 179-190.

[20] Berard B, Bidoit M, Finkel A, Laroussinie F, Petit A, Petrucci L, Schnoebelen P. Systems and Software Verification: Model Checking Techniques and Tools. Springer-Verlag, 2001.

[21] G?llü A, Puri A, Varaiya P. Discretization of timed automata. In: Proc. of the 33rd IEEE Conf., 1994,1(14-16):957-958.

[22] Raskin JF, Schoebbens P. Real-Time logics: Fictitious clock as an abstraction of dense time. In: Tools and Algorithms for the Construction and Analysis of Systems. LNCS 1217, London: Springer-Verlag, 1997. 165-182.

[23] Dang Z, Ibarra OH, Bultan T, Kemmerer RA, Su J. Binary reachability analysis of discrete pushdown timed automata. In: CAV. LNCS 1855, London: Springer-Verlag, 2000. 69-84.

[24] Strehl K, Thiele L. Symbolic model checking of process networks using interval diagram techniques. In: ICCAD. New York: ACM Press, 1998. 686-692.

[25] Bengtsson J, Wang Y. Timed automata: Semantics, algorithms and tools. Technical Report, UNU-IIST No. 316, 2004.

[26] Lamport L. A fast mutual exclusion algorithm. ACM Trans. on Computer Systems, 1987,5(1):1-11.

[27] Gerd B, Johan B, Alexandre D, Larsen KG, Paul P, Wang Y. UPPAAL implementation secrets. In: FTRTFT. LNCS 2469, London: Springer-Verlag, 2002. 3-22.