

实时模型检测中基于驻留环的精确加速

尹传龙¹, 庄 雷¹, 王从银^{1,2}

(1. 郑州大学信息工程学院, 河南郑州 450052; 2. 吉首大学数学与计算机科学学院, 湖南吉首 416000)

摘 要: 在控制系统和外界环境之间经常会出现时间度量差距. 对这些系统用时间自动机建模, 并运用符号模型检测技术进行验证时, 会引起符号状态空间的片段问题. 精确加速技术在不改变系统可达性的前提下解决了片段问题. 针对可加速环引起的片段问题, 本文提出一种基于驻留环实现精确加速的方法. 驻留环的长度固定, 不依赖于可加速环的窗口, 因而构造的自动机模型更简单, 能提高精确加速的速度, 并能够降低精确加速的时间和空间开销.

关键词: 模型检测; 时间自动机; 可加速环; 精确加速; 驻留环

中图分类号: TP301.1 **文献标识码:** A **文章编号:** 0372-2112 (2011) 03-0489-05

Exact Acceleration of Real-Time Model Checking Based on Parking Cycle

YIN Chuan-long¹, ZHUANG Lei¹, WANG Cong-yin^{1,2}

(1. School of Information Engineering, Zhengzhou University, Zhengzhou, Henan 450052, China;

2. College of Maths and Computer Science, Jishou University, Jishou, Hunan 416000, China)

Abstract: Different time scales are often found between control systems and their environments. When these systems are modeled as timed automata, such difference can lead to fragmentation of the symbolic state space in the process of applying symbolic model checking techniques to the validation of them. Exact acceleration addresses the fragmentation problem without any side-effect to the reachability properties of the system under consideration. To address the fragmentation problems caused by the acceleratable cycles, this paper introduces an exact acceleration technique based on parking cycle. The length of the parking cycle is constant, without dependency on the window of the acceleratable cycles, and so makes the constructed acceleration simpler, the process of the exact acceleration faster, and both the time cost and the space cost of exact acceleration can be greatly reduced.

Key words: model checking; timed automata; acceleratable cycle; exact acceleration; parking cycle

1 引言

时间自动机^[1,2]是实时系统建模的有效工具, 可当用时间自动机对含有不同时间度量的系统进行建模, 然后运用符号模型检测技术进行验证时, 可能会出现片段问题(即符号状态空间的片段化现象), 导致模型检测时间明显增加^[3]. 事实上, Hune 和 Iversen 在使用 UPPAAL 工具对 LEGO 程序进行验证的时候, 就已发现并描述了片段问题^[4,5]. 此外, 在实时轮询系统^[6](如可编程的逻辑控制器)以及考虑上下文的通信协议的验证中也会出现片段问题.

文献[7]在线性关系分析中表明了抽象加速应用在合并扩展中可以提高分析的精确性, 同时加速的应用也从符号证明扩展到数据流分析中的最小固定点的计算, 最近也提出将加速技术和基于插补模型检测合并应用,

基于插补的模型检测可以提供有效的自动抽象方案, 帮助加速技术处理更小的块. 同样加速技术可以帮助基于插补的模型检测处理更复杂的行为^[8].

文献[3]提出通过构造附加环的方法对可加速环引起的片段问题进行精确加速, 与其它加速技术^[9,10]相比, 该方法不改变时间自动机的可达性, 并可以有效地加速前向搜索可达性分析. 设可加速环窗口为 $[a, b]$, 则附加环的长度是可加速环长度的 $\lceil a/(b-a) \rceil$ 倍. 随着边界比值 a/b 接近1时, 附加环的长度会大大增加, 这意味着不仅大大增加了时间自动机的位置的数目, 还大大增加模型检测时的状态空间, 使得加速的代价随之增大.

本文针对文献[3]中定义的可加速环提出了一种通过构造驻留环实现精确加速的方法. 驻留环的构造简单, 长度固定, 使得构造时间自动机的精确加速模型时

更加的简单快捷.在模型检测时驻留环增加的状态空间远小于附加环,从而大大减少了加速的代价.

本文第2节介绍了时间自动机的基本知识,用前向符号搜索^[11]说明了片段问题,以及描述了基于附加环的精确加速方法及其存在的问题.第3节提出了基于驻留环的精确加速方法,给出了长度固定的驻留环的构造方法,并证明了添加驻留环的时间自动机能够对具有可加速环的时间自动机的可达性分析过程进行精确加速.最后,第4节对基于驻留环的精确加速方法进行总结,并对未来的工作进行了展望.

2 基本知识及相关背景

2.1 时间自动机

假定 X 是时钟集,时钟约束 δ 的集合 $\Phi(X)$ 定义如下:

$$\delta: x \sim c \mid \delta_1 \wedge \delta_2$$

其中 $x \in X, c \in \mathbb{N}, \sim$ 表示二元关系 $<, \leq, =, \geq$ 或 $>$.

时钟集 X 的时钟解释 v 是从 X 到 $\mathbb{R}^+$ 的映射,其中 $\mathbb{R}^+$ 是包含 0 的正实数集.时钟解释 v 满足时钟约束 δ , 记作 $v \models \delta$, 当且仅当 δ 满足 v 给定的值.对于正实数 t , $v + t$ 也是一个时钟解释,它将每一个时钟变量赋值为 $v(x) + t$; 对于 X 的子集 $Y, v[Y: 0]$ 也是一个时钟解释,它将每一个属于 Y 的时钟变量 x 复位为 0, 而不属于 Y 的时钟变量的时钟值保持不变.

定义 1^[1] (时间自动机) 时间自动机 M 是一个六元组 $\langle L, L_0, \Sigma, X, I, E \rangle$, 其中 L 是有穷位置集, 初始位置集 L_0 是 L 的子集, Σ 是有穷事件集, X 是时钟集, I 是映射, 它为 L 中的每个位置 l 分配了一个位置不变式, 转换规则集 E 是 $L \times \Sigma \times \Phi(X) \times 2^X \times L$ 的子集. 一条转换 $\langle l, a, \delta, \lambda, l' \rangle$ 表示如果当前位置 l 的时钟解释满足时钟约束 δ , 那么系统可以通过实现事件 a 从位置 l 转换到另一个位置 l' , 同时把 λ 中的所有时钟复位.

例 1 实时系统通常包含一个控制程序, 它通过传感器来控制并监管外界环境. 用时间自动机对实时系统进行建模和验证不仅需要控制程序模型, 还需要一个环境模型^[4]. 图 1 的时间自动机 M_p 表示一个控制程序和外界环境的简化模型. 由位置 l_0, l_1, l_2 组成的

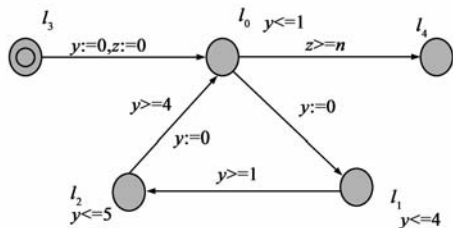


图1 时间自动机 M_p

控制环对应控制程序. 在位置 l_0 , 外界环境的时钟 z 被考察, 如果满足条件 $z \geq n$, 就有可能跳出控制环.

2.2 片段问题

表 1 为时间自动机 M_p 从初始位置 l_3 开始利用前向符号搜索执行控制环两次得到的符号状态. 当搜索到第 5 个符号状态时, 虽然位置是 l_0 , 但由于时钟带并不包含在第 2 个符号状态的时钟带中, 应该进一步搜索这个状态. 当搜索到第 8 个状态时, 第 8 个状态的时钟带不包含在第 2 个符号状态或第 5 个符号状态的时钟带中, 也应该进一步搜索.

由于阈值 n 较大, 而时钟 z 增长又比较缓慢, 当模型检测位置 l_4 是否可达时, 自动机 M_p 必须执行控制环很多次才能使得时钟 z 得到足够的增长, 才能判断位置 l_4 是否可达. 这表明由于模型中出现了不同的时间度量, 时间自动机在前向符号搜索进行模型检测时, 会出现大量的时钟带片段, 从而形成了不必要的符号状态空间分裂(片段问题).

表 1 前向符号搜索时间自动机 M_p 得到的部分结果

状态	位置	时钟带		
1	l_3	$y = 0$	$z = 0$	$z - y = 0$
2	l_0	$0 \leq y \leq 1$	$0 \leq z \leq 1$	$z - y = 0$
3	l_1	$0 \leq y \leq 4$	$0 \leq z \leq 5$	$0 \leq z - y \leq 5$
4	l_2	$1 \leq y \leq 5$	$1 \leq z \leq 6$	$0 \leq z - y \leq 5$
5	l_0	$0 \leq y \leq 1$	$4 \leq z \leq 7$	$3 \leq z - y \leq 7$
6	l_1	$0 \leq y \leq 4$	$4 \leq z \leq 11$	$0 \leq z - y \leq 11$
7	l_2	$1 \leq y \leq 5$	$5 \leq z \leq 12$	$0 \leq z - y \leq 11$
8	l_0	$0 \leq y \leq 1$	$8 \leq z \leq 13$	$7 \leq z - y \leq 13$

图 2 是前向符号状态搜索时间自动机 M_p 在位置 l_0 得到的时钟带, 其中, D_i 为前向符号搜索时第 i 次到达位置 l_0 时所得到的时钟带. 从 D_4 开始的每个时钟带都与其前面那个时钟带有重叠, 这是由于控制环较小的时间度量导致时钟带 $\{0 \leq y \leq 1, z \geq 8\}$ 被分割成无穷多个片段.

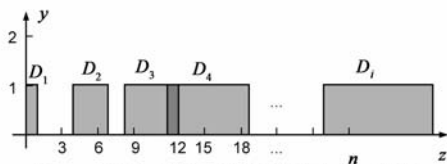


图2 时间自动机 M_p 在复位位置 l_0 的时钟带

2.3 基于附加环的精确加速

定义 2^[3] (可加速环) 假设 $M = \langle L, L_0, \Sigma, X, I, E \rangle$ 是一个时间自动机, $E_c = (e_0, e_1, \dots, e_{n-1}) \in E^n$ 且 $y \in X$. 二元组 (E_c, y) 是一个可加速环, 当

- (1) E_c 是一个环,
- (2) 对于所有出现在 E_c 中的位置 $l, I(l)$ 为空或都是 $\{y \leq c\}$ 的形式,
- (3) 如果 $\langle l, a, \delta, \lambda, l' \rangle \in E_c$, 那么 δ 或者为空或

不间断的时钟带片段. 证毕

推论 3 假定时间自动机 M 中存在窗口为 $[a, b]$ 的可加速环, 时钟 z 是可加速环以外的时钟, 且在执行可加速环前时钟 z 的最大值是 n_0 . 如果 $a < b$, 那么在前向符号状态搜索过程中, 当 $z - n_0 \geq a * a / (b - a)$ 时, 可加速环中的任意位置都将会得到连续的时钟带.

证明 因为时钟 z 是可加速环以外的时钟, 根据可加速环的定义, 在可加速环中的任意位置中的不变式或约束条件都不会包含时钟 z , 所以根据时间自动机的性质, 在执行可加速环时, 时钟 z 是单调增长的. 因此, 当 $z - n_0 \geq a * a / (b - a)$, 根据推论 2, 复位位置上的时钟带开始连续, 可加速环中的其他任意位置都将会得到连续的时钟带. 证毕

我们利用得出的定理和推论, 提出一种基于驻留环实现精确加速的方法, 向时间自动机添加仅由一个位置及其边界条件构成的驻留环. 只有当可加速环以外的时钟 z 的增量大于等于 $a * a / (b - a)$ 后, 才能进入驻留环. 一方面由于驻留环中的位置没有不变式, 可以保证时钟在此位置驻留, 达到加速的目的. 另一方面驻留环包含边界条件, 这样可以保证进入驻留环前, 可加速环的任意位置都得到了连续的时钟带, 从而达到保证可达性的目的. 这样驻留环通过控制加速的时机, 既加速了符号状态前向搜索, 也保证了时间自动机的可达性, 实现了精确加速.

定义 4 (基于驻留环的加速自动机) 假设时间自动机 $M = \langle L, L_0, \Sigma, X, I, E \rangle$, $C_a = ((e_0, e_1, \dots, e_{n-1}), y)$ 是一个可加速环, 其窗口为 $[a, b]$, z 是可加速环 C_a 以外的时钟, 且进入可加速环前 z 的最大值为 n_0 . 假定 $L = \{l_0, l_1, \dots, l_m\}$, 且 $e_i = (l_i, a_i, \delta_i, \lambda_i, l_{i+1})$. 定义基于驻留环的加速自动机 $A_p(M, C_a) = \langle L', L_0, \Sigma, X, I', E' \rangle$, 其中

$$L' = L \cup \{l'_0\},$$

$$I'(l_i) = I(l_i), \text{ 其中 } 0 \leq i \leq m$$

$$I'(l'_0) = \Phi,$$

$E' = E \cup \{(l_0, \Phi, \delta', \Phi, l'_0), (l'_0, \Phi, \Phi, \lambda_0, l_0)\}$, 其中 δ' 为 $z \geq a * a / (b - a) + n_0$.

我们利用驻留环入口的边界条件 $z \geq a * a / (b - a) + n_0$ 控制加速的时机, 只有可加速环至少被执行了 $a / (b - a)$ 次后, 才能进入位置 l'_0 , 从而保证复位位置上以后得到的时钟带是连续的, 这样才进入加速阶段, 否则时间自动机会一直执行可加速环直到符合边界条件. 对于进入可加速环前时钟 z 的最大值 n_0 , 可以通过分析计算得到. 当然用实际的模型检测工具建模时, 可以定义一个有界整数变量 i 用来计算并控制至少执行 $a / (b - a)$ 次可加速环, 这样我们的边界条件就变成了 i

$$\geq a / (b - a).$$

定理 3 假定时间自动机 $M = \langle L, L_0, \Sigma, X, I, E \rangle$, C_a 是 M 的一个窗口为 $[a, b]$ 的可加速环, φ 是 M 的一个可达性属性, 那么

$$a < b \Rightarrow (M \models \varphi \Leftrightarrow A_p(M, C_a) \models \varphi).$$

证明 当 $a < b$ 时, 因为 $A_p(M, C_a)$ 是通过向时间自动机 M 添加一个驻留环得到的, 显然, 时间自动机 M 能满足的任意可达状态 S , 时间自动机 $A_p(M, C_a)$ 也可以通过执行同样的时间轨迹到达状态 S , 即 M 相关的状态转换系统 $T(M)$ 包含在 $A_p(M, C_a)$ 相关的状态转换系统 $T(A_p(M, C_a))$ 中. 得证.

当 $a < b$ 时, 假设时间自动机 $A_p(M, C_a)$ 的边界条件为 $z < a * a / (b - a) + n_0$. 当 $z < a * a / (b - a) + n_0$ 时, 时间自动机 $A_p(M, C_a)$ 未执行驻留环, 此时 $A_p(M, C_a)$ 可达的状态, 时间自动机 M 也是可达. 当 $z \geq a * a / (b - a) + n_0$, 根据推论 3, 时间自动机 M 的可加速环中的任意位置都将会得到连续的不间断的时钟带片段, 即, 在 $z \geq a * a / (b - a) + n_0$ 后的任意时刻都可以到达可加速环中的任意位置. 因此当 $z \geq a * a / (b - a) + n_0$ 时, $A_p(M, C_a)$ 满足边界条件执行驻留环后又回到复位位置的任意状态, 时间自动机 M 也是可达的. 这就证明了基于驻留环的加速自动机 $A_p(M, C_a)$ 不会改变 M 的可达性属性 φ . 得证.

例 3 对于例 1 中含有可加速环的时间自动机 M_p , 向自动机 M_p 添加一个驻留环, 构造基于驻留环的加速自动机 M'_p , 如图 4 所示. 与图 3 相比, 在图 4 中仅添加新的位置 l'_0 .

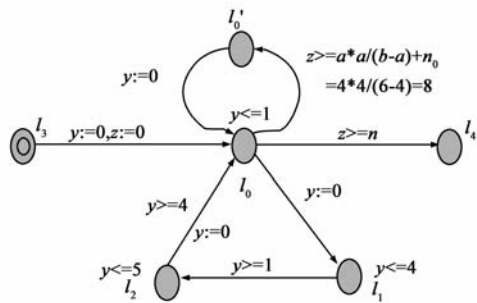


图4 时间自动机 M_p 基于驻留环的加速自动机 M'_p

在例 3 中, 可加速环的窗口为 $[4, 6]$, 求得边界条件 $z \geq 8$. 当 $z < 8$ 时, 时间自动机只能执行可加速环, 只有执行了两次可加速环, 满足加速条件时才开始进入 l'_0 . 同附加环的作用一样, 执行一次驻留环所得到的符号状态包括了执行多次可加速环所得到的符号状态, 因而实现了加速, 解决了片段问题.

相比基于附加环的精确加速方法, 首先, 基于驻留环的精确加速方法是建立在精确加速原理之上的, 同样也加速了前向符号状态搜索, 且不改变可达性, 实现

了精确加速.其次,向时间自动机添加的驻留环的大小是固定的,这样就解决了附加环的长度依赖可加速环窗口的问题.再次,驻留环是简单的,仅由一个位置及其边界条件组成,这也会大大节省存储空间.最后,基于驻留环的方法和附加环的构造方法一样需要计算可加速环窗口.不同的是,基于附加环的精确加速方法中用可加速环的窗口确定构造附加环需要展开可加速环的次数,这里我们利用窗口计算驻留环入口的边界条件.

4 结论

为了解决可加速环引起的片段问题,本文提出一种基于驻留环的精确加速方法用以加速前向符号可达性分析过程.相比基于附加环的精确加速,该方法向系统的时间自动机模型添加一个长度固定的驻留环.添加驻留环引入的符号状态远少于添加附加环.我们未来的工作是研究适合求解可加速环的算法,以及研发能自动添加驻留环构造精确加速模型的程序.

参考文献

- [1] Alur R, Dill D L. A theory of timed automata[J]. Theoretical Computer Science, 1994, 126(2): 183 – 236.
- [2] 林惠民, 张文辉. 模型检测: 理论、方法与应用[J]. 电子学报, 2002, 30 (12A): 1907 – 1912.
Lin Hui-min, Zhang Wen-hui. Model checking: theories, techniques and applications[J]. Acta Electronica Sinica, 2002, 30 (12A): 1907 – 1912. (in Chinese)
- [3] Hendriks M, Larsen K G. Exact acceleration of real-time model checking[A]. Electronic Notes in Theoretical Computer Science [C]. Amsterdam: Elsevier Science, 2002. 120 – 139.
- [4] Hune T S. Modeling a language for embedded systems in timed automata[R]. Aarhus: Basic Research in Computer Science, 2000.
- [5] Iversen T K, Kristoffersen K J, et al. Model checking real-time control programs — Verifying LEGO mindstorms systems using uppaal[A]. IEEE Euromicro Conference on Real-Time Systems [C]. Stockholm: IEEE Computer Society, 2000. 147 – 155.

- [6] Dierks H. Specification and verification of polling real-time systems[D]. Oldenburg: Carl von Ossietzky University, 1999.
- [7] Leroux J, Sutre G. Accelerated data-flow analysis[A]. 14th Int Static Analysis Symposium [C]. Kongens Lyngby: Springer Press, 2007. 184 – 199.
- [8] Caniart N, Fleury E, Leroux J, Zeitoun M. Accelerating interpolation-based model checking[A]. 14th International Conference on Tools and Algorithms for Construction and Analysis of Systems [C]. Budapest: Springer Press, 2008. 428 – 443.
- [9] Möller M O. Parking can get you there faster[A]. The Workshop on Theory and Practice of Timed Systems, Electronic Notes in Theoretical Computer Science [C]. Amsterdam: Elsevier Science, 2002.
- [10] Gonnord L, Halbwachss N. Combining widening and acceleration in linear relation analysis[A]. 13th International Static Analysis Symposium [C]. Seoul: Springer Press, 2006. 144 – 160.
- [11] Bengtsson J, Wang Yi. Timed automata: semantics, algorithms and tools[A]. Reisig W, Rozenberg. Lecture Notes on Concurrency and Petri Nets [C]. Eichsatt: Springer Press, 2004.

作者简介



尹传龙 男, 1985 年 11 月出生于山东省临沂市. 硕士研究生, 研究方向为模型检测.

E-mail: dragonyinel@163.com



庄雷 女, 1963 年 2 月出生于河南省郑州市. 现为郑州大学信息工程学院教授、博士生导师, 主要研究方向为模型检测、对等计算.

E-mail: ielzhuang@zzu.edu.cn