文章编号: 1001-0920(2001)05-0637-04

具有定时器连续系统的阈值切换面划分离散近似

张苗苗, 谢剑英, 张学军
(上海交通大学 自动化系, 上海 200030)

摘 要: 若混合系统的连续部分存在定时器, 则无法应用基于阈值切换面划分的验证方法。为此, 首次提出了综合流管道近似和阈值切换面划分的方法以及过渡状态的概念。在流管道近似过渡状态集合时, 扩大其在时间上的分析范围, 便可自动得到定时器的合理设定范围。最后通过实例验证了上述方法的可行性, 以及形式验证相对于仿真方法的优越性。

关键词: 流管道; 阈值切换面; 分析区域; 过渡状态
中图分类号: TP 301 **文献标识码**: A

Discrete Approximation of Continuous Systems with Timers Based on Partition of Threshold Switching Surfaces

ZHANG Miao-miao, XIE Jian-ying, ZHANG Xue-jun
(Department of Automation, Shanghai Jiaotong University, Shanghai 200030, China)

Abstract: A method of integrating Partition of Threshold Switching Surfaces (PTSS) and Segmenting Approximation of Flow Pipe (SAFP) is proposed to solve the problem that PTSS is not applicable if there exist timers in continuous blocks, and the notion of interim states is put forward. Enlarging the analysis time domain when interim states are approximated by SAFP, the timer's reasonable range can be got, which expands the application scope of the method. An example of chemical process control shows that the method is effective and superior to the simulation method.

Key words: flow pipe; threshold switching surface; analysis region; interim states

1 引 言

混合系统形式验证技术的丰富成果, 为解决现代工业过程逻辑控制程序的验证问题提供了新的手段, 但目前仍存在状态爆炸问题。采用离散整个连续状态空间的方法来进行可达性验证[1,2], 虽可简化空间划分, 但维数的增长仍会使小室数目发生爆炸。考虑到混合系统发生切换时的信息, 文献[3]给出了仅在阈值切换表面离散化的方法, 可节省计算开销, 降低系统维数, 但当连续系统存在定时器时, 此方法则遇到了很大困难。定时器事件发生时, 连续部分的轨迹不一定正好落在切换面上(很可能位于两个切换面之间); 并且由于初始区域存在一定范围, 当系统轨迹在发生定时器事件时, 由位置组成的切换面很不规则, 一般无法进行划分。对存在定时器的情况, 文献[2]采用了离散整个空间的方法, 但计算量非常大。

针对上述问题, 本文提出具有定时器事件的连续部分划分时的过渡状态概念, 将变时间间隔的流

收稿日期: 2000-04-13; 修回日期: 2000-06-28

作者简介: 张苗苗(1971—), 女, 安徽宿州人, 博士生, 从事混合系统的分析与验证研究; 谢剑英(1940—), 男, 福建龙岩人, 教授, 博士生导师, 从事复杂过程控制、离散事件系统等研究。

管道近似与基于阈值切换面划分的方法相结合, 很好地解决了含有定时器连续部分的离散近似问题, 扩展了基于阈值切换面划分的混合系统即时验证的应用范围。

2 过渡状态的提出和解决问题的基本思路

2.1 过渡状态

定义 **1**(过渡状态集合) 从一定初始区域出发的连续系统发生某定时器事件时的所有可能状态的集合, 称为该定时器事件的过渡状态集合, 表示为

$$S_{\text{interim}} = \{(x_1, x_2, \cdots, x_n) \mid \dot{x} = f_A(x, t) \wedge x_0 = x(0) \wedge t = t_{\text{timer}}\} \quad (1)$$

其中, f_A 为定时器事件发生前连续部分的向量场, t_{timer} 为定时器的设定值。

由定义 1 可以看出, 某定时器的过渡状态与一定初始区域相关, 因而是不确定的, 即事先无法准确知道其位置。

定义 **2**(过渡状态集合的保守近似) 对于过渡状态集合 S_{interim}, 如果存在状态集合 $\hat{S}_{\text{interim}}$ 并满足

$$\hat{S}_{\text{interim}} \supseteq S_{\text{interim}} \quad (2)$$

则称 $\hat{S}_{\text{interim}}$ 为 S_{interim} 的保守近似。

定时器事件发生时, 连续状态形成的几何形状大多不规则, 无法划分。如果其保守近似集合形成的切换面是规则的, 则可对其进行划分, 据此得到的验证结论是充分的。流管道近似方法[3] 采用了时间概念, 通过扩大定时器时刻附近的时间范围, 可方便地获得过渡状态集合的保守近似。

$$\hat{S}_{\text{interim}} = \{(x_1, x_2, \cdots, x_n) \mid \dot{x} = f_A(x, t) \wedge x_0 = x(0) \wedge t \in [t_{\text{timer}} - \epsilon, t_{\text{timer}} + \delta] \wedge \epsilon \geq 0 \wedge \delta \geq 0 \wedge \neg(\epsilon = 0 \wedge \delta = 0)\} \quad (3)$$

若 $\epsilon = 0 \wedge \delta > 0$, 则称近似结果为前向近似; 若 $\epsilon > 0 \wedge \delta = 0$, 则称近似结果为反向近似。

2.2 解决问题的思路

本文将定时器事件产生的阈值切换面视为一种特殊的阈值切换面, 采用特殊的方法来处理。即在定时器事件发生前, 用基于阈值切换面划分的方法得到一个离散近似模型; 定时器事件发生后, 则根据系统的动态同样得到另一个离散模型; 然后将这两个模型通过中间过渡状态联接起来。由于每个连续模型规模一般不是很大, 定时器数目不会很多, 新的离散方法是可行的。实际上, 该方法与整个空间离散化方法相比具有许多优势。

图 1 是基于阈值切换划分的具有单个定时器的连续系统示意图。其中, A 为根据定时器事件发生前的系统方程进行的划分, 称为第 1 阶段; B 为根据定时器事件发生后的系统方程进行的划分, 称为第 2 阶段; 中间是过渡状态集合, 可通过流管道近似获得。虚线代表省略状态。

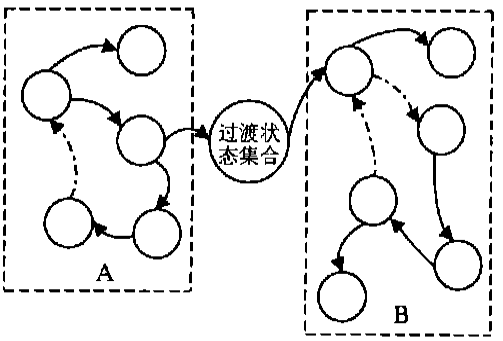

图 **1** 具有定时器的阈值切换面划分

当通过流管道近似计算得到的过渡状态集合较大时, 为得到较好的近似结果, 将其分裂为几个较小的集合, 分别进行划分。将过渡状态集合看成一个初始区域, 其表面作为 B 划分的初始区域, 类似于文献[2] 的矩形划分。由于流管道近似的每一段都是凸壳, 作为新的初始区域较为容易实现计算。

基于变时间间隔的流管道近似, 可根据要求调整时间间隔, 即在定时器发生事件的附近细化, 而其它部分可采用稍大的时间间隔以适应不同的需求。

3 混合系统的验证实例

下面举例证明上述方法的可行性, 以及混合系统相对于仿真方法的优点。

3.1 实例的系统描述

采用文献[1] 的实例(见图 2), 其过程如下: 首先在蒸发器 T_1 中装入溶液并蒸发, 要求达到合理浓度; 一旦反应器 T_2 为空, 则将 T_1 中的物质泄入 T_2。为安全起见, 当系统故障导致 T_1 内温度高于报警温度 T_{alarm} 时, 系统安全关闭。但关闭 T_1 加热器过早将导致蒸馏塔内的产品发生晶化。

采取的控制策略有以下两种: 1) 当 T_1 内温度超过报警温度 T_{alarm}(单位 K) 时关闭加热器; 2) 在系统发生故障时立即启动一定时器, 等待一段时间 t_{timer}(单位 s) 后, 再关闭加热器。因此, PLC 控制程序中选定的报警温度 T_{alarm} 或定时器的报警时间 t_{timer} 是否恰当, 便成为系统设计的关键因素, 也是我们的

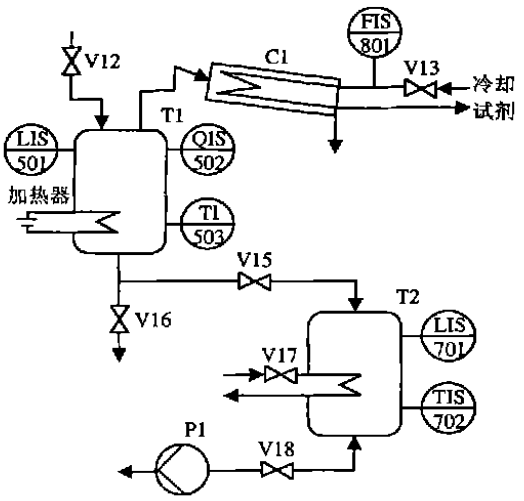

图 2　化工过程的验证模型

验证目的。

在 u_1 状态下,H_1,H_2 和 T 满足

$$\dot{H}_1 = 0$$

$$\dot{H}_2 = -3.333 \times 10^{-4}\sqrt{19.62H_2}$$

$$\dot{T} = \frac{5\,000 - \dfrac{24(T-283)}{2.819 \times 10^{6}T^{-1} + 6.433 \times 10^{3} - 10.513T}}{1.23 \times 10^{5}H_1 - 1.327 \times 10^{9}T^{-2} + \cdots} \rightarrow$$

T_1 内的晶化温度 $T_{crys} = 338$ K,塔内物质的最小高度分别为 $H_{1min} = 0.04$ m 和 $H_{2min} = 0.04$ m,最大高度分别为 $H_{1max} = 0.22$ m 和 $H_{2max} = 0.30$ m,系统中的最高温度 $T_{max} = 405$ K。不变集 $\mathrm{Inv} = \{H_{1min} \le H_1 \le H_{1max} \wedge H_{2min} \le H_2 \le H_{2max} \wedge T_{crys} \le T \le T_{max}\}$ 是基于切换面划分的分析区域。

3.1.1　实例的混合自动机模型

状态变量 $X = (H_1, H_2, T)$,离散输入变量 $u = (\mathrm{Heat}, \mathrm{V15}, \mathrm{V18})$,其中 T 为 T_1 的温度,H_1 和 H_2 分别为 T_1 和 T_2 内物质的高度。$u_1 \sim u_5$ 代表系统不同的工作区域,可看成是对系统状态空间的粗略划分。其中 u_4 为故障状态,u_5 为系统的安全关闭状态。设压缩机故障时的蒸发温度 $T = 373$ K,T_1 和 T_2 内物质的高度 $H_1 \in [0.2, 0.22]$,$H_2 \in [0.28, 0.3]$。验证的目的是证明从上述初始状态集合出发的所有轨迹是否最终到达 u_5,而不是 u_4。当采用定时器控制方式时,系统混合自动机模型如图 3 所示。

3.1.2　仿真结果

在 Matlab 中建立了该系统的仿真模型。采用定时器控制方式并设定 $t_{timer} = 300$ s,温度仿真曲线 T 如图 4 所示。经过大量仿真试验可知,系统的定时器

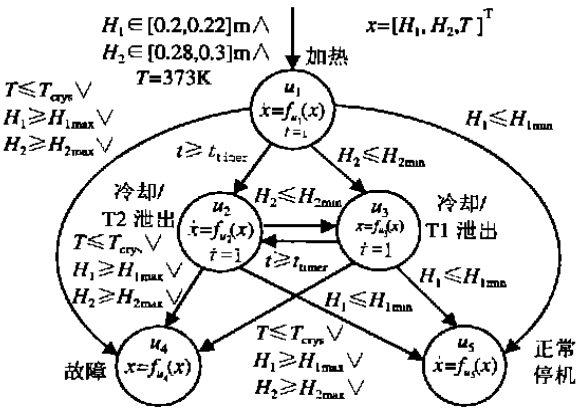

图 3　实例的混合计时自动机模型

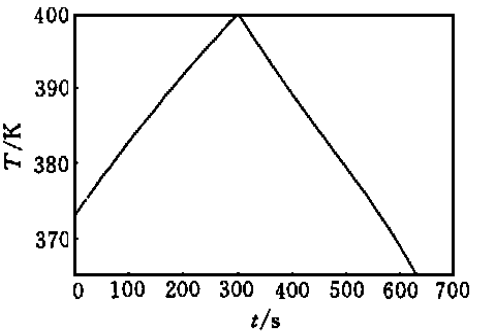

图 4　当 $t_{timer} = 300$ s 时的仿真曲线

设定在 240 ～ 300 s 之间时,系统不会进入故障状态;时间小于 240 s 时系统可能发生晶化,时间大于 300 s 时蒸发器的压力将高于阈值 $T_{max} = 405$ K,这两种情况是不允许出现的。可以看出,采用仿真方法确定参数的合理范围非常繁琐,需要进行大量的仿真试验,且无法保证结论的可靠性。

3.1.3　验证过程

这里给出采用定时器控制方式的验证过程。将切换面事件产生的切换面视为一新的初始集合(过渡状态集合),并用流管道近似得到该集合的保守近似。

3.1.4　第 1 阶段划分

在用流管道近似时,若初始区域比较大,则必须先划分为较小的初始区域,再分别进行流管道近似。为突出主要问题,选定的初始区域比较小,因而可省略先将初始区域分成几部分再分别计算的步骤。当 $0 \le t \le 310$ s 时,流管道近似的结果如图 5 所示。通过流管道近似可知,当 $t = 310$ s 时,系统的演化轨迹仍未到达常规阈值切换面 $T < T_{crys} \vee T > T_{max} \wedge H_1 < H_{1min} \vee H_1 > H_{1max} \vee H_2 < H_{2min} \vee H_2 > H_{2max}$。根据移去不可达状态的验证策略,在定时器

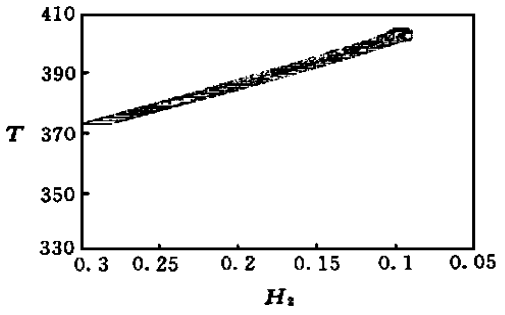

图 5 实例的第 1 阶段流管道近似

事件发生前, 无需进行阈值切换面划分。

3.1.5 过渡状态集合的近似

当 295 s $\leq t \leq$ 300 s 和 300 s $\leq t \leq$ 305 s 时, 两段的流管道近似结果如图 6 所示。选定 295 s $\leq t \leq$ 300 s 段作为 t_{timer} 定时器事件的过渡状态集合(反向近似), 并将该段流管道的 6 个面作为第 2 阶段划分改进的初始区域。

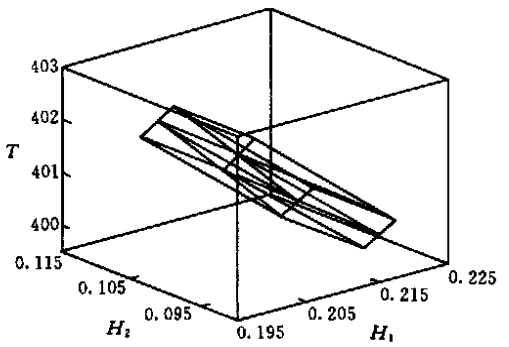

图 6 过渡状态的流管道近似

3.1.6 第 2 阶段划分改进

当系统发生定时器事件后, 在 295 s $\leq t \leq$ 300 s 范围内流管道段的一个面根据 u_2 演化, 其轨迹与 $H_2 = 0.04$ 阈值切换面相交, 以相交面作为初始区域并根据 u_3 演化, 最终到达安全区域 u_5。同样, 采用上述方法可处理其它 5 个面。如果每个面均如此处理, 计算量仍较大。可先对过渡状态集合到达切换面的情况进行汇总, 以找出合适的划分方法, 从而不需要对每个面均进行一次划分改进。由于系统在 $t_{timer} \in [295, 300]$ 时产生的过渡状态集合均进入安全状态 u_5, 满足规范, 所以系统在 $t_{timer} = 300$ s 时产生的过渡状态集合也进入安全状态 u_5, 系统的安全性质得到验证。

采用在 300 s $\leq t \leq$ 305 s 范围的流管道段作为过渡状态的前向近似集合, 经分析可知, 存在不满足规范的状态。

3.2 定时器的合理范围

前面已验证了在 295 s $\leq t \leq$ 300 s 时系统是满足规范的。如果扩大流管道近似范围, 从正、反两个方向扩大流管道近似范围, 且每段均采用上述方法近似, 则可得到系统定时器的安全范围设定为 240 s $\leq t_{timer} \leq$ 300 s 时, 系统能安全关闭的结论, 这与文献[1] 得到的结论是一致的。

4 结 论

本文提出的综合流管道近似和阈值切换面划分的方法, 可解决连续系统存在定时器时阈值切换面划分离散近似方法的实现问题。采用所提出的过渡状态的概念, 可自动得到定时器的合理设定范围, 为 PLC 应用程序的验证提供了新思路。通过化工过程控制中混合系统实例的形式验证, 证明了上述方法的可行性以及形式验证相对于仿真方法的优越性。

参考文献:

[1] S Kowalewski, S Engell, J Preubig *et al*. Verification of logic controllers for continuous plants using timed condition/event-system models[J]. Automatica, 1999, 35(3): 505–518.

[2] O Stursberg, S Kowalewski, I Hoffmann *et al*. Comparing timed and hybrid automata as approximations of continuous systems: Hybrid systems IV[M]. New York: Springer, 1997. 361–377.

[3] A Chutinan, B H Krogh. Verification of polyhedral-invariant hybrid automata using polygonal flow pipe approximations[A]. Second Int Workshop, HSCC 99[C]. Netherlands: Springer-Verlag, 1999. 76-90.

[4] A Chutinan, B H Krogh. Computing polyhedral approximations to flow pipes for dynamic systems[A]. The 37th IEEE Conf on Decision and Control[C]. Tampa, 1998. 2089-2094.