文章编号: 1001-0920(2001)02-0203-04

混合系统的形式验证技术及其在化工过程控制中的应用

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

摘 要: 针对 PLC 等逻辑控制器控制连续对象的可靠性问题, 给出了混合系统的形式验证的方法, 即用混合矩形自动机建模, 通过其商迁移的可达性分析, 证明了控制程序的正确性。应用实例表明该方法是可行和有效的。

关键词: 混合系统; 矩形自动机; 形式验证; 可达性
中图分类号: TP 301 文献标识码: A

Formal Verification of Hybrid Systems and Its Application on Chemical Process Control

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

Abstract: Aiming at reliability of programmable logic controller for continuous plants, an approach is presented to make the hybrid systems' formal verification. The model is given out by using hybrid rectangular automata and the analysis of its quotient transition system's reachability is presented. The principles of verification are given. The method is illustrated by an example of chemical process control.

Key words: hybrid systems; rectangular automata; formal verification; reachability

1 引 言

现代工业已大量采用可编程逻辑控制器和计算机分布式控制系统。当数字控制装置与模拟量的对象打交道时, 应很好地分析和理解所出现的现象, 同时也应保障控制程序的正确性和操作安全性。由于现有的软件工具只能检查控制程序中的逻辑错误, 而对物理对象的控制是否符合要求则无能为力, 因此对于这类逻辑控制系统的正确性和安全性问题, 大多依靠编程者的实际经验和大量的仿真运行进行分析, 缺乏比较合适可信的验证工具。

近年来, 混合系统的形式验证技术获得了丰硕的研究成果, 为现代工业过程逻辑控制程序的验证提供了新的手段。混合系统是连续变量过程和离散事件过程并存且相互交换信息的动态系统。在化工过程控制等应用中, 运行于控制系统的软件的主体是执行逻辑控制函数。即使软件的主体是连续控制, 其程序也往往包括故障紧急处理和运行模式的切换等, 且受控对象中包含大量的离散元件(如阀门、开关、继电器、传感器等)。可以说, 这类系统是混合系

收稿日期: 1999-08-20; 修回日期: 2000-02-14
作者简介: 张学军(1972—), 男, 河北滦南人, 博士生, 从事混合系统的分析与控制等研究; 谢剑英(1940—), 男, 福建龙岩人, 教授, 博士生导师, 从事复杂工业过程控制、智能控制等研究。

统的典型实例。

仿真方法每次只能产生特定初始条件和输入信号的一条轨迹, 其完备性难以从理论上得到保障, 因而可信度较低。混合系统的形式验证技术是通过穷举算法对系统进行可达性分析, 即在一次运行中, 给定初始状态和输入信号的集合, 模型检查系统的每一种可能行为, 以证明所有的可达状态是否满足预定的规范, 从而为控制程序的可靠性提供了科学分析的依据。

2 混合系统的形式验证技术

混合系统的形式验证技术是利用混合矩形自动机对控制系统建模, 将原系统的可达性分析转化为有限状态商迁移系统的可达性分析, 从而大大降低了计算量, 使全空间搜索成为可能。

2.1 迁移系统

定义 **1**(迁移系统) 迁移系统是集合

$$T = (S, \Sigma, \rightarrow, S_0, S_F) \tag{1}$$

其中, S 是状态集合, Σ 是事件的字母表, $\rightarrow \subseteq S \times \Sigma \times S$ 是迁移关系, $S_0 \subseteq S$ 是初始状态集合, $S_F \subseteq S$ 是终止状态集合。

定义 **2**(等价关系) 称某个关系 $\sim \subseteq S \times S$ 是等价的, 如果满足:

1) 自反性: 对于所有的 s, 有 $(s, s) \in \sim$;

2) 对称性: 若 $(s, s') \in \sim$, 则 $(s', s) \in \sim$;

3) 传递性: 若 $(s, s') \in \sim$ 和 $(s', s'') \in \sim$, 则 $(s, s'') \in \sim$。

给定一个等价关系 $\sim$, 则 $S/\sim = \{S_i\}$ 代表了 S 的商空间, 即包含其所有等价类的集合。迁移系统 (1) 的商迁移系统记为

$$T/\sim = (S/\sim, \Sigma/\sim, \rightarrow/\sim, S_0/\sim, S_F/\sim) \tag{2}$$

2.2 仿真对

定义 **3**(仿真对) 对于迁移系统 (1), S 上的等价关系 $\sim$ 是仿真对, 如果满足:

1) S_0 是等价类的并集;

2) S_F 是等价类的并集;

3) 对于所有的 $\sigma \in \Sigma$, 如果 P 是等价类的并集, 则 $\mathrm{Pre}_\sigma(P)$ 也是等价类的并集。

这里 $\mathrm{Pre}_\sigma(P) = \{s \in S: \exists\, s' \in P$, 满足 $(s, \sigma, s') \in \rightarrow\}$。

2.3 混合矩形自动机

定义 **4**(混合矩形自动机) 混合自动机是一个多元组, 即

$$H = (Q, X, \mathrm{Init}, f, \mathrm{Inv}, E, G, R) \tag{3}$$

其中, Q 是有限个离散状态变量的集合, $Q = \{q_1, q_2, \cdots, q_m\}$; X 是有限个连续变量的集合, $X = \{X_1, X_2, \cdots, X_n\}$, $X = \boldsymbol{R}^n$; $\mathrm{Init} = \bigcup_{i=1}^{m}\{q_i\} \times \mathrm{Init}(q_i) \subseteq Q \times X$ 是初始状态的集合, $\mathrm{Init}(q_i) = \mathrm{Init}_1(q_i) \times \cdots \times \mathrm{Init}_n(q_i)$ 是矩形; 对于所有的 (q, x), 有 $f(q, x) = F(q)$, $F(q) = F_1(q) \times \cdots \times F_n(q)$ 是一个矩形; $\mathrm{Inv}: Q \rightarrow 2^{X \times V}$ 是对每一个 $q \in Q$ 赋予不变集; $E \subset Q \times Q$ 是离散迁移的集合; 对每一个 $e = (q, q') \in E$, $G(e) = G_1(e) \times \cdots \times G_n(e)$ 是矩形; $R(e, x) = R_1(e, x) \times \cdots \times R_n(e, x)$ 是对每一个 $e = (q, q') \in E$, $x \in X$ 进行复位。

定义 **5** 始化矩形自动机称为初始化的, 如果对于所有的转移 $e = (q, q') \in E$ 满足

$$F_i(q) \neq F_i(q') \Rightarrow R_i(e, x) \neq \{x_i\} \tag{4}$$

其中 $F_i(q)$ 和 $F_i(q')$ 为微分包。

定理 **1** 始化矩形自动机的可达性问题是 PSPACE 完备的[3]。

PSPACE 完备性表明, 存在某种算法, 可在有限步内计算出始化矩形自动机的可达集。基于上述原理, 目前已有多种混合控制系统的形式验证工具, 大致可分为两类: 1) HyTech 为代表的模型检查方法; 2) 以 STeP 为代表的定理证明。它们的共同目标是: 给定系统描述, 确定系统是否满足特定的性质。HyTech 作为分析混合系统的形式验证工具, 能计算出线性混合系统满足时态要求的条件, 通过检查符号化模型的准确性来实现。在进行逻辑控制程序的形式验证时, 可直接利用 HyTech 软件。

3 验证过程举例

现在结合实例来说明验证在化工过程控制中的应用。图 1 是整个验证过程的流程图, 虚线框内的受控对象编辑器和流程图编辑器是混合自动机建模的前期工作, 限于篇幅, 这里不再赘述。

3.1 系统描述

本文采用文献[2] 中的实例(见图 2), 其过程如下:

1) 首先在蒸发器 T1 中装入溶液并蒸发, 要求达到合理浓度;

2) 一旦反应器 T2 为空, 则将 T1 中的物质泄入 T2。

为安全起见, 当系统故障(如压缩机 C1 停机)

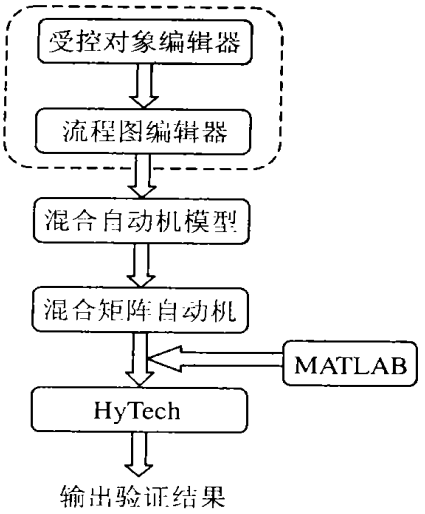

图 1　形式验证流程图

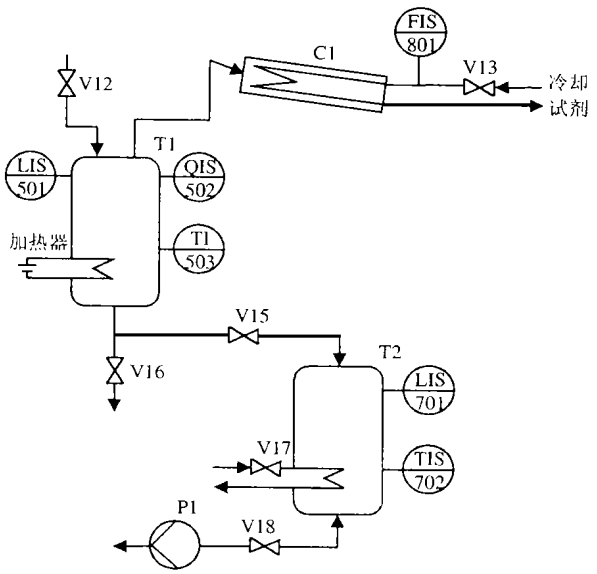

图 2　化工过程的验证模型图

导致 T1 内温度高于报警温度 T_{alarm} 时, 应使系统安全关闭。首先打开阀门 V18, 启动电泵 P1, 泄出 T2 中的物质; 当 T2 变空后, 打开阀门 V15, 抽出 T1 中的物质, 此时系统即可安全关闭。这期间蒸馏塔 T1 内的温度将升高, 压力增大, 因而必须适时关掉 T1 加热器。但关闭加热器过早将使蒸馏塔内的产品发生晶化。因而 PLC 控制程序中选定的报警温度是否恰当, 便成为系统设计的关键因素, 也是验证的目的。系统的输入情况如表 1 所示。

表 1　系统的输入情况

	加热器	V15	V18	描　述
u_1	打开	关闭	打开	T1 加热
u_2	关闭	关闭	打开	T1 冷却 / T2 泄出
u_3	关闭	打开	关闭	T1 冷却 / 泄出

3.2　混合系统模型的建立

对于该实例, 状态变量为 $X = (H_1, H_2, T)$, 离散输入变量为 $u = (\text{Heat}, \text{V15}, \text{V18})$, 其中 T 为 T1 的温度, H_1 和 H_2 分别为 T1 和 T2 内物质的高度。系统的混合自动机模型如图 3 所示。u_1, u_2, u_3, u_4 和 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。T1 内的晶化温度 $T_{crys} = 338\text{K}$, 蒸发温度 $T = 373\text{K}$。T1 和 T2 内部 "空" 均记为 H_{empty}, 运行时塔内物质的最小高度分别为 $H_{1min} = 0.2\text{m}$ 和 $H_{2min} = 0.28\text{m}$, 最大高度分别为 $H_{1max} = 0.22\text{m}$ 和 $H_{2max} = 0.30\text{m}$, 这里选定报警温度 $T_{alarm} = 395\text{K}$。

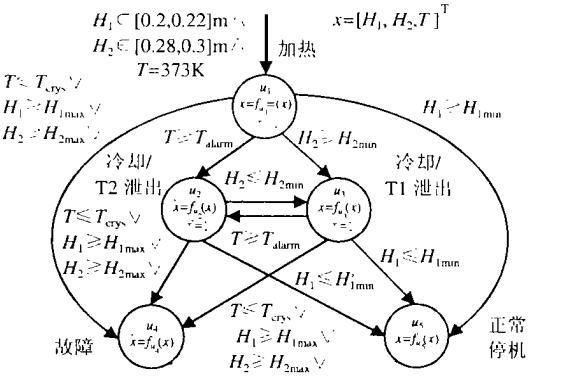

图 3　混合计时自动机模型

综上所述, 容易写出该系统的不变集为

$$\text{Inv} = \{H_{1min} \le H_1 \le H_{1max} \wedge H_{2min} \le H_2 \le H_{2max} \wedge T_{crys} \le T \le T_{alarm}\} \quad (5)$$

本实例的目的是验证从初始状态集合 $X_0 = \{0.2 \le H_1 \le 0.22, 0.28 \le H_2 \le 0.3, T = 373\}$ 出发的所有轨迹是否最终到达 u_5, 而不是 u_4。

在混合自动机模型中直接引入本地时钟, 既便于连续系统的标定, 又符合 PLC 中定时器的实际情况。如果某个状态不需要时钟(比如 u_4 和 u_5), 则自动省略本地时钟, 以降低模型的复杂程度; 如果在模型中单独引入计时时钟, 则不利于模型的统一表达。

3.3　混合自动机模型的转化

HyTech 中自动机的状态包括位置和时钟, 其可达性分析是通过迭代方法确定系统是否可从初始状态到达某个状态集合。但是 HyTech 只能检查线性混合自动机, 所以图 3 中的自动机模型在输入 HyTech 之前应转化为其可接受的形式。本文采用对系统状态空间进行矩形划分的方法, 即划分为矩形自动机。下面以 u_1 为例说明其基本过程。

在 u_1 状态下, H_1, H_2 和 T 满足

$$\begin{cases} \dot{H}_1 = 0 \\ \dot{H}_2 = -3.333 \times 10^{-4} \sqrt{19.62 H_2} \\ \dot{T} = \dfrac{5\,000 - (1.23 \times 10^5 H_1 - 1.327 \times 10^9 T^{-2} + \rightarrow}{\leftarrow \dfrac{24(T - 283)}{2.819 \times 10^6 T^{-1} + 6.433 \times 10^3 - 10.513 T}} \end{cases} \tag{6}$$

其中, $H_1 \in [0.2, 0.22]$ m, $H_2 \in [0.28, 0.3]$ m, $T \in [338, 395]$ K。

容易看出, H_1 保持不变, H_2 的变化速率很小且基本恒定(最小变化率约为最大变化率的 96.6%), 因而划分间隔可以大些; 而 T 的变化较为复杂, 划分间隔应小些。这里 H_1 取点 0.2, 0.21 和 0.22; H_2 取点 0.28, 0.29 和 0.30; T 取点 338, 350, 373, 384 和 395。把 u_1 细化为 16 个子空间, 划分出的每个子空间为小室(cell); 再根据系统的状态方程用 Matlab 估算各小室间所有可能的迁移, 便完成了 u_1 的转化。

当图 3 中的其它自动机也完成同样的转化后, 模型便成为线性自动机, 满足 HyTech 对模型的要求。当然也可用另一种观点来看待该转化过程: 建模阶段是对连续变量空间的粗略矩形划分, 由于空间划分的粗粒度对系统的描述精度有较大影响, 为保障精度, 需进一步减小划分间隔。这种先粗划再细分的方法, 比直接考虑整个变量范围的方法降低了计算各个子空间转移的难度。

3.4 用 HyTech 进行形式验证

将上述从 Matlab 获得的状态转移数据直接输入 HyTech, 以实现形式验证。HyTech 输出结果表明, 系统的报警温度 T_{alarm} 选定为 395K 时, 系统不会进入故障状态 u_4, 因而验证所选定的报警温度值是合适的。若 T_{alarm} 选定为 385K, 则 HyTech 输出结果表明 u_4 状态可以到达, 这是不允许出现的情况; 若 T_{alarm} 选定为 343K, 则 HyTech 输出结果表明 u_4 状态也可以到达。报警温度的选择有一个合适的范围。

由于自动机形式验证的固有原因, 验证的计算量相对于离散状态数量的增加呈指数增长。混合系统进行验证时尽管采取了一些措施以降低计算量, 但仍不适于大规模复杂系统的分析。目前针对可达计算的复杂性问题, 人们正在寻找高效的解决方法。如何在不同的建模层次上抽取合适的模型动态, 是解决该问题的一个值得研究的方向。

4 结 论

本文给出了混合系统形式验证技术的原理及其在化工自动控制中的应用方法, 为 PLC 应用程序的验证提供了新思路。该验证方法是可行而有效的, 但仍需进一步改进, 以适应大规模系统验证的迫切需要。

参考文献:

[1] A Chutinan. Hybrid system verification using discrete model approximations[D]. Pittsburgh: PhD Thesis, Carnegie Mellon University, 1999. 9–29.

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

[3] A Puri, P Varaiya. Decidability of hybrid systems with rectangular inclusions[A]. Proc of the 6th Workshop on Computer-aided Verification[C]. Germany: Springer-Verlag, 1994. 95–104.