DOI: 10.7641/CTA.2015.40228

带扰动控制系统的形式化设计

张晋津[1†], 张　严[2], 朱朝晖[2]

(1. 南京审计学院 计算机科学与技术系, 江苏 南京 211815; 2. 南京航空航天大学 计算机科学与技术学院, 江苏 南京 210016)

摘要: 利用有限抽象进行控制系统的形式化分析与设计是目前研究较多的一类控制系统分析与设计方法. 本文提出两种方法, 使用有限抽象, 构造出两种控制器, 使带扰动的控制系统满足时序逻辑规范. 为此, 首先在时序逻辑规范上引入“弱化”转换函数和“强化”转换函数. 进而, 利用“弱化”转换函数提出一种方法用于构造控制器, 使原系统近似满足给定规范; 利用“强化”转换函数, 提出另一种方法用于构造控制器, 使原系统严格满足给定规范. 本文分析比较上述两种方法与文献中已有的方法, 指出各自的优缺点和适用范围. 最后给出仿真实验, 说明上述两种方法的有效性并展示这些方法的不同适用范围.

关键词: 反馈控制; 控制系统设计; 带扰动控制系统; 时序逻辑; 有限抽象

中图分类号: TP273　　**文献标识码**: A

Formal design of control systems with disturbances

ZHANG Jin-jin[1†], ZHANG Yan[2], ZHU Zhao-hui[2]

(1. Department of Computer Science and Technology, Nanjing Audit University, Nanjing Jiangsu 211815, China;
2. College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing Jiangsu 210016, China)

Abstract: Adopting finite abstraction for the formal analysis and design of control systems is prevailing recently. By applying finite abstractions, we develop two methods for constructing the controller for systems with disturbances so that these systems will satisfy temporal logical specifications. To this end, we first introduce the ”weaken” transformation function and the ”strengthen” transformation function for the temporal logical specifications. By using the ”weaken” transformation function, we develop a method to construct the controller forcing the controlled systems with disturbances to approximately satisfy the specifications. Then, we use the ”strengthen” transformation function to develop another method to construct the other controller enforcing the controlled system to exactly satisfy the specifications. We compare these two methods with some existing methods in modern literature, and find out the advantages and application scopes of these methods. Finally, a simulation example is presented to demonstrate the validity and different application scopes of these two methods.

Key words: feedback control; control system design; control system with disturbances; temporal logic; finite abstraction

1　引言(Introduction)

控制系统的分析与设计是控制理论的一个重要研究方向. 其中, 控制系统分析主要关注于验证系统是否满足规范, 而控制系统设计的目的在于构造控制器使系统在控制器作用下满足给定规范. 传统的控制系统分析与设计主要考虑可达性与稳定性(不变性)等作为其所需满足的规范[1–2]. 近年来, 实际应用中需要使用一些更为复杂的规范. 为此, 研究者们采用了时序逻辑[3–6]、自动机[7]、正规式[8]等计算机领域常用的规范描述语言. 在计算机领域, 特别是形式化方法研究领域已经提出了一些结论和算法用于这些规范的验证和设计. 学术界尝试将这些结论和算法应用于控制论领域, 建立控制系统的形式化分析与设计方法. 但由于控制系统的状态空间一般是连续且无限的, 这些结论和算法无法直接应用于控制系统的分析与设计.

为了降低控制系统的状态空间规模, 研究者们构造了控制系统的有限抽象, 它是控制系统形式化分析与设计的核心概念[9]. 互模拟作为描述控制系统与其有限抽象之间等价性的关键概念曾在这些工作中发

收稿日期: 2014−03−22; 录用日期: 2014−09−01.

†通信作者. E-mail: jinjinzhang@nau.edu.cn; Tel.: +86 13770658202.

国家自然科学基金项目(11426136, 60973045), 江苏省自然科学基金项目(BK20130735), 江苏省高校自然科学基金项目(13KJB520012, 13KJB520011)资助.

Supported by National Natural Science Foundation of China (11426136, 60973045), Natural Science Foundation of Jiangsu Province (BK20130735) and Natural Science Foundation of the Jiangsu Higher Education Institutions (13KJB520012, 13KJB520011).

挥了重要作用. 具体而言, 互模拟的逻辑特征确保了控制系统和与其互模拟等价的有限抽象是逻辑等价的, 从而使控制系统的分析和设计可以通过其有限抽象完成[6]. 然而Girard等人指出, 由于互模拟的要求太过严苛, 对于很多实际应用中常见的控制系统而言, 很难构造与之互模拟的有限抽象[10–11]. 为了克服这一缺陷, Girard等人引入(ε,δ)–近似模拟和近似互模拟等概念, 为众多无扰动控制系统构造了与之近似模拟(或近似互模拟)的有限抽象[10–12], 并证明了当采用可达集、正规语言等描述规范时, 此类控制系统与其有限抽象近似满足相同规范[10,12], 从而使原系统的分析和设计可以归结为其有限抽象的分析和设计. 目前这种方法已经被用于控制系统的安全性和活性验证[13], Girard等人利用这种方法构造了用于确保控制系统满足安全性规范和可达性规范的控制器[14–15], Camara等人使用这种方法解决了几种控制系统的控制器构造问题[16]. 文献[17]和文献[18]分别总结了这种技术路线在控制系统分析与设计中的应用.

由于控制系统在实际运行中都会因环境或系统本身的原因而受到若干扰动的影响, 带扰动控制系统的分析与设计问题是控制论领域的一个研究热点[19–22]. 为了应用上述思路解决带扰动控制系统分析和设计问题, 文献[23–24]构造了交替转换系统作为此类系统的近似有限抽象, 并提出了交替近似互模拟刻画控制系统与其有限抽象之间的近似等价性. 文献[25]为交替近似互模拟建立了模态逻辑特征, 从而为基于与原系统近似交替互模拟的有限抽象的控制器设计方法提供了理论基石. 该文还给出了作用于正线性时序逻辑公式的一个“弱化”转换函数, 并在此基础上提出了一种控制器形式化设计方法.

本文将以一般线性时序逻辑公式作为规范, 提出两种基于抽象构造带扰动控制系统控制器的方法. 具体而言, 本文将针对一般的线性时序逻辑公式定义“弱化”转换函数, 进而提出一种方法用于构造使带扰动控制系统满足“弱化”转换后规范的控制器; 将提出“强化”转换函数, 并基于此函数提出一种控制系统形式化设计方法用于解决如下问题: 基于与原系统近似互模拟的有限抽象, 如何构造使原系统严格满足规范的控制器; 还将比较这两种方法与文献[6]中的方法, 指出各自的优点和适用范围, 并给出仿真实例说明上述两种方法的有效性.

2　控制系统与其有限抽象(Control systems and their finite abstractions)

首先, 本节将回忆带扰动控制系统与其有限抽象的相关概念[23–24], 介绍基于此有限抽象提出的关于正线性时序逻辑规范的控制器构造方法[25]. 在此之前, 需要介绍下文中常用的一些标记的含义.

符号$\mathbb{N},\mathbb{Z},\mathbb{R}$和$\mathbb{R}^0_+$分别表示自然数集合、整数集合、实数集合和非负实数集合. 任意给定集合Q, Q^*和Q^ω分别表示Q上所有有限字符串和所有无限字符串组成的集合. 令$i\in\mathbb{N}$, $s\in Q^*$且$\sigma\in Q^\omega$, 则$s[\mathrm{end}]$表示字符串s的最后一个字符, $\sigma[i]$表示该字符串第i个字符, $\sigma[1,i]$表示$\sigma[1]\sigma[2]\cdots\sigma[i]$. 令$x\in\mathbb{R}^n$, 则$x_i$表示$x$的第$i$项并且$\|x\|\triangleq\max\{|x_1|,|x_2|,\cdots,|x_n|\}$, 其中$|x_i|$表示$x_i$的绝对值. 一个连续函数$\gamma:\mathbb{R}^0_+\to\mathbb{R}^0_+$属于$\mathcal{K}$类当且仅当它是严格递增并且$\gamma(0)=0$; γ属于$\mathcal{K}_\infty$类当且仅当它属于$\mathcal{K}$类并且当$r\to\infty$时, $\gamma(r)\to\infty$. 一个连续函数$\beta:\mathbb{R}^0_+\times\mathbb{R}^0_+\to\mathbb{R}^0_+$属于$\mathcal{KL}$, 当且仅当, 固定$s$, 则映射$\beta(r,s)$关于$r$属于$\mathcal{K}_\infty$类; 固定$r$, 则映射$\beta(r,s)$关于$s$是递减的并且当$s\to 0$, $\beta(r,s)\to 0$.

2.1　控制系统与交替转换系统(Control systems and alternating transition systems)

本小节回顾带扰动控制系统与其有限抽象相关概念, 这些概念的直观背景及构造参见文献[23].

定义 1　带扰动控制系统是一个四元组$\Sigma=(X,W,\mathcal{W},f)$, 其中:

• $X\subseteq\mathbb{R}^n$是状态空间;

• $W=U\times V$是输入空间, 其中$U\subseteq\mathbb{R}^m$是可控输入空间, $V\subseteq\mathbb{R}^k$是扰动输入空间;

• $\mathcal{W}=\mathcal{U}\times\mathcal{V}$是可测且局部本质有界的函数组成的集合的子集, 这些函数的定义域具有如下形式: $[a,b]\subseteq\mathbb{R}$或$[a,b)\subseteq\mathbb{R}$, 其中$0\leqslant a<b$;

• $f:\mathbb{R}^n\times W\to\mathbb{R}^n$是一个满足下面Lipschitz假设的连续映射: 对于任意紧致集合$K\subseteq\mathbb{R}^n$, 存在一个常量$\kappa>0$使得, 对于任意的$x,y\in K$和$w\in W$都有$\|f(x,w)-f(y,w)\|\leqslant\kappa\|x-y\|$.

一个局部绝对连续曲线$\boldsymbol{x}:[a,b]\to\mathbb{R}^n$被称为是$\Sigma$的一条轨迹, 当且仅当, 存在$\boldsymbol{w}\in\mathcal{W}$使得对于几乎所有的$t\in[a,b]$, $\dot{\boldsymbol{x}}(t)=f(\boldsymbol{x}(t),\boldsymbol{w}(t))$. $\boldsymbol{x}(t,x,\boldsymbol{w})$表示系统由$x$状态出发, 在输入$\boldsymbol{w}$作用下$t$时刻到达的状态.

定义 2　一个控制系统Σ被称为是递增全局渐进稳定的, 当且仅当, 它是向前完全并满足以下条件的: 存在$\mathcal{KL}$函数β使得对于任意的$t\in\mathbb{R}$, x_1, $x_2\in\mathbb{R}^n$, $\boldsymbol{w}\in\mathcal{W}$,

$$\|\boldsymbol{x}(t,x_1,\boldsymbol{w})-\boldsymbol{x}(t,x_2,\boldsymbol{w})\|\leqslant\beta(\|x_1-x_2\|,t).$$

定义 3　一个交替转换系统是一个多元组$T=(Q,A,B,\to,O,H)$, 它包括一个状态集合Q, 一个控制标记集合A, 一个扰动标记集合B, 一个转换关系$\to\subseteq Q\times A\times B\times Q$, 一个观察值集合$O$和一个观察函数$H:Q\to O$.

如果观察集合O上附有一个度量, 则称这个交替转换系统是度量化的; 如果对于任意的$q \in Q$, $a \in A$和$b \in B$, 都有$\{q' : q \xrightarrow{a,b} q'\} \neq \varnothing$, 则称其为非死锁的; 如果状态集合$Q$, 控制标记集合$A$和扰动标记集合$B$都是有限的, 则称其为有限的.

一个无限序列$\sigma \in Q^\omega$被称为T的轨迹当且仅当对于任意的$i \in \mathbb{N}$, 存在$a_i \in A$和$b_i \in B$使得$\sigma[i] \xrightarrow{a_i,b_i} \sigma[i+1]$.

在交替转换系统框架下, 控制策略定义如下:

定义 4 令$T = (Q, A, B, \rightarrow, O, H)$是一个交替转换系统. 函数$f : Q^* \rightarrow A$被称为是$T$的一个控制策略. 给定初始状态$q \in Q$, 系统$T$在控制策略$f$作用下生成的轨迹集合定义如下:

$$\begin{aligned}\mathrm{Out}_T(q, f) \triangleq \{&\sigma \in Q^\omega : \sigma[1] = q \ \&\ \forall i \in \mathbb{N},\\ &\exists b_i \in B(\sigma[i] \xrightarrow{f(\sigma[1,i]),b_i} \sigma[i+1])\}.\end{aligned}$$

如果系统T可由上下文确定, 则省略$\mathrm{Out}_T(q, f)$的下标. 文献[23–24]构造交替转换系统作为带扰动控制系统的有限抽象. 其中: 文献[23]证明了递增全局渐进稳定的控制系统存在有限抽象与原系统的取样系统近似等价, 并且给出了线性系统的有限抽象的构造方法; 文献[24]给出了递增输入–状态稳定(incrementally input-to-state stable)的非线性取样–数据(nonlinear sample-data)带扰动控制系统的有限抽象的构造方法. 相关定义参见文献[24]. 在上述工作中, 交替近似互模拟的概念被提出用于刻画控制系统与其有限抽象间的近似等价关系.

定义 5 令$T_i = (Q_i, A_i, B_i, \underset{i}{\rightarrow}, O, H_i)(i = 1, 2)$是两个度量的、非死锁的交替转换系统. 假设这两个转换系统的观测集合上的度量都是d. 给定$\varepsilon \in \mathbb{R}^0_+$, 关系$R \subseteq Q_1 \times Q_2$被称为是$T_1$和$T_2$之间的$\varepsilon$–交替近似互模拟关系, 当且仅当, 对于任意的$(q_1, q_2) \in R$,

1) $d(H_1(q_1), H_2(q_2)) \leqslant \varepsilon$;

2) $\forall a_1 \in A_1$, $\exists a_2 \in A_2$, $\forall b_2 \in B_2$, $\forall q_2' \in Q_2(q_2 \xrightarrow[2]{a_2,b_2} q_2' \Rightarrow \exists b_1 \in B_1, \exists q_1' \in Q_1(q_1 \xrightarrow[1]{a_1,b_1} q_1')$并且$(q_1', q_2') \in R)$;

3) $\forall a_2 \in A_2$, $\exists a_1 \in A_1$, $\forall b_1 \in B_1$, $\forall q_1' \in Q_1(q_1 \xrightarrow[1]{a_1,b_1} q_1' \Rightarrow \exists b_2 \in B_2, \exists q_2' \in Q_2(q_2 \xrightarrow[2]{a_2,b_2} q_2')$并且$(q_1', q_2') \in R)$;

对于任意的$q_1 \in Q_1, q_2 \in Q_2$, 称它们是ε–交替近似互模拟的(记作$q_1 \sim_\varepsilon q_2$), 当且仅当, 存在T_1和T_2之间的ε–交替近似互模拟关系R使得$(q_1, q_2) \in R$. 称T_1和T_2是ε–交替近似互模拟的(记作$T_1 \sim_\varepsilon T_2$), 当且仅当, 存在T_1和T_2之间的ε–交替近似互模拟关系R使得$Q_1 = \{q_1 \in Q_1 : 存\ 在 q_2 \in Q_2 使\ 得 (q_1, q_2) \in R\}$并且$Q_2 = \{q_2 \in Q_2 : 存在 q_1 \in Q_1 使得 (q_1, q_2) \in R\}$.

2.2 正时序逻辑规范的转换及控制器构造(Transformation of positive temporal logical specification and construction of controller)

文献[25]给出了关于正时序逻辑规范的控制器构造方法, 本节简要回顾相关概念和结论.

定义 6 令P是一个有限原子命题集合并且$\varepsilon \in \mathbb{R}^0_+$. 线性时序逻辑$LTL^\varepsilon_+(P)$公式归纳定义如下:

$$\varphi ::= p | < \varepsilon > p | \boldsymbol{X}\varphi | \varphi_1 \wedge \varphi_2 | \varphi_1 \vee \varphi_2 | \varphi_1 \boldsymbol{U} \varphi_2,$$

其中$p \in P$. 如果公式φ中不出现$< \varepsilon >$, 则该公式被称为$LTL_+(P)$公式.

易见上述定义的公式均是正公式. 交替转换系统的轨迹与上述公式间的可满足关系定义如下:

定义 7 令P是一个有限原子命题集合, $\varepsilon \in \mathbb{R}^0_+$, $T = (Q, A, B, \rightarrow, O, H)$是一个交替转换系统, d是O上一个度量并且$\Pi : O \rightarrow P$是一个赋值函数. 轨迹$\sigma \in Q^\omega$在第$i(i \in \mathbb{N})$个位置满足$LTL^\varepsilon_+(P)$公式φ(记作$(T, d), \sigma[i] \models \varphi$)归纳定义如下:

1) $(T, d), \sigma[i] \models p$当且仅当$\Pi(H(\sigma[i])) = p$;

2) $(T, d), \sigma[i] \models < \varepsilon > p$当且仅当存在$q \in Q$使得$d(H(\sigma[i]),\ H(q)) \leqslant \varepsilon$并且$\Pi(H(q)) = p$;

3) $(T, d), \sigma[i] \models \boldsymbol{X}\varphi$当且仅当$(T, d), \sigma[i+1] \models \varphi$;

4) $(T, d), \sigma[i] \models \varphi_1 \wedge \varphi_2$当且仅当$(T, d), \sigma[i] \models \varphi_1$并且$(T, d), \sigma[i] \models \varphi_2$;

5) $(T, d), \sigma[i] \models \varphi_1 \vee \varphi_2$当且仅当$(T, d), \sigma[i] \models \varphi_1$或者$(T, d),\ \sigma[i] \models \varphi_2$;

6) $(T, d), \sigma[i] \models \varphi_1 \boldsymbol{U} \varphi_2$当且仅当存在$j \geqslant i$使得$(T, d),\ \sigma[j] \models \varphi_2$并且对于任意的$i \leqslant k < j$都有$(T, d), \sigma[k] \models \varphi_1$.

本文称轨迹σ满足$LTL^\varepsilon_+(P)$公式φ(记作$(T, d), \sigma \models \varphi$)当且仅当$(T, d), \sigma[1] \models \varphi$.

在下文中, 如果原子命题集合P由上下文可知, 则将$LTL^\varepsilon_+(P)$简记为LTL^ε_+. 为了刻画控制系统与其有限抽象分别可控满足的逻辑规范间关系, 文献[25]中给出了如下转换函数.

定义 8 令P是一个有限原子命题集合并且$\varepsilon \in \mathbb{R}^0_+$. 将$LTL_+$公式映射为$LTL^\varepsilon_+$公式的转换函数$ltr^+_\varepsilon$定义如下: 对于任意的$LTL_+$公式$\varphi$, $ltr^+_\varepsilon(\varphi)$是将$\varphi$中出现的所有原子命题$p$替换为$< \varepsilon > p$得到的公式.

容易验证, 对于任意的轨迹σ, 如果$(T, d), \sigma \models \varphi$则$(T, d), \sigma \models ltr^+_\varepsilon(\varphi)$; 但反之未必成立. 因此, 此转换函数可以称为一个“弱化”转换函数. 在文献[25]中, 笔者说明了如下结论成立:

给定带扰动控制系统与其有限抽象, 如果该控制系统的取样系统与其有限抽象是ε-交替近似互模拟

的, 则以任意线性时序逻辑LTL_+公式φ作为规范, 如果存在控制策略使其有限抽象受控满足规范φ, 则存在控制策略使得原系统的取样系统受控满足转换后的规范$ltr_\varepsilon^+(\varphi)$.

基于该结论, 文献[25]提出了带扰动控制系统的形式化设计方法: 首先利用文献[23]或文献[24]中的方法构造与原系统交替近似互模拟的有限抽象, 进而利用文献[26]所给出的算法求解使有限抽象满足规范的控制策略, 最后利用该控制策略构造原系统的控制器使原系统受控满足“弱化”的规范(即, 近似满足给定规范).

3　近似满足规范的控制器设计(Design of controller enforcing approximate specification)

本节拟将上述工作推广至一般线性时序逻辑规范情形. 即, 本节将针对一般线性时序逻辑公式给出“弱化”转换函数, 刻画带扰动控制系统与其有限抽象分别可控满足规范间的关系, 进而提出方法用于构造控制器使原系统满足“弱化”的规范. 为此, 本文给出含负公式的线性时序逻辑$LTL_l^\varepsilon(P)$.

定义 9　令P是一个有限原子命题集合并且$\varepsilon \in \mathbb{R}_+^0$. 线性时序逻辑$LTL_l^\varepsilon(P)$公式归纳定义如下:

$$\varphi ::= p|<\varepsilon>p|\neg p|<\varepsilon>\neg p|\boldsymbol{X}\varphi|\varphi_1\wedge \varphi_2|\varphi_1\vee\varphi_2|\varphi_1\boldsymbol{U}\varphi_2|\varphi_1\tilde{\boldsymbol{U}}\varphi_2|\Box\varphi|\diamond\varphi,$$

其中$p \in P$. 如果公式φ中不出现$<\varepsilon>$, 则该公式被称为$LTL(P)$公式.

交替转换系统轨迹与$LTL_l^\varepsilon(P)$公式之间的可满足关系定义如下:

定义 10　令P是一个有限原子命题集合, $\varepsilon \in \mathbb{R}_+^0$, $T=(Q,A,B,\rightarrow,O,H)$是一个交替转换系统, d是O上一个度量并且$\Pi: O\to P$是一个赋值函数. 则轨迹$\sigma \in Q^\omega$在第$i(i\in\mathbb{N})$个位置满足$LTL_l^\varepsilon(P)$公式φ(记作$(T,d),\sigma[i]\models\varphi$)归纳定义如下:

1) $(T,d),\sigma[i]\models\neg p$当且仅当$\Pi(H(\sigma[i]))\neq p$;

2) $(T,d),\sigma[i]\models<\varepsilon>\neg p$当且仅当存在$q\in Q$使得$d(H(\sigma[i]),H(q))\leqslant\varepsilon$并且$\Pi(H(q))\neq p$;

3) $(T,d),\sigma[i]\models\varphi_1\tilde{\boldsymbol{U}}\varphi_2$当且仅当对于任意的$j\geqslant i$, 如果$(T,d),\sigma[j]\not\models\varphi_2$, 则存在$k\in\mathbb{N}$使得$i\leqslant k<j$并且$(T,d),\sigma[k]\models\varphi_1$;

4) $(T,d),\sigma[i]\models\Box\varphi_1$当且仅当对于任意的$j\geqslant i$, $(T,d),\sigma[j]\models\varphi_1$;

5) $(T,d),\sigma[i]\models\diamond\varphi_1$当且仅当存在$j\geqslant i$使得$(T,d),\sigma[j]\models\varphi_1$;

6) 当公式φ具有其他形式时, 其可满足性定义与定义7相同.

[1] $\sigma_1\sim_\varepsilon\sigma_2$当且仅当对于任意的$i\in\mathbb{N}$都有$\sigma_1[i]\sim_\varepsilon\sigma_2[i]$.

本文称轨迹σ满足$LTL_l^\varepsilon(P)$公式φ(记作$(T,d),\sigma\models\varphi$)当且仅当$(T,d),\sigma[1]\models\varphi$. 转换系统$T$被称为是受控满足公式$\varphi$的, 当且仅当, 存在$T$的控制策略$f:Q^*\to A$和初始状态$q\in Q$使得对于任意的$\sigma\in\mathrm{Out}(q,f)$都有$(T,d),\sigma\models\varphi$.

易见, 定义6所给出的线性时序逻辑$LTL_+^\varepsilon(P)$是上述定义的一个片段. 如果P由上下文可知, 则简记$LTL_l^\varepsilon(P)$和$LTL(P)$为LTL_l^ε和LTL. “弱化”转换函数定义如下:

定义 11　令P是一个有限原子命题集合并且$\varepsilon\in\mathbb{R}_+^0$. 将$LTL$公式映射为$LTL_l^\varepsilon$公式的转换函数$ltr_\varepsilon$定义如下:

1) $ltr_\varepsilon(p)=<\varepsilon>p$;

2) $ltr_\varepsilon(\neg p)=<\varepsilon>\neg p$;

3) $ltr_\varepsilon(\odot\varphi)=\odot ltr_\varepsilon(\varphi)$, 其中$\odot\in\{\boldsymbol{X},\Box,\diamond\}$;

4) $ltr_\varepsilon(\varphi_1\oplus\varphi_2)=ltr_\varepsilon(\varphi_1)\oplus ltr_\varepsilon(\varphi_2)$, 其中$\oplus\in\{\wedge,\vee,\boldsymbol{U},\tilde{\boldsymbol{U}}\}$.

下文将证明对于ε–交替近似互模拟的交替转换系统, 如果其中之一受控满足LTL公式φ, 则另一个系统受控满足$ltr_\varepsilon(\varphi)$. 为此, 本文需要如下引理:

引理 1[25]　令$T_i=(Q_i,A_i,B_i,\underset{i}{\rightarrow},O,H_i)(i=1,2)$是两个度量的、非死锁的交替转换系统并且$d$是观测集合$O$上的度量. 假设集合$Q_1$是有限的并且$f_1$是$T_1$的控制策略. 对于任意的$q_1\in Q_1$, $q_2\in Q_2$和$\varepsilon\in\mathbb{R}_+^0$, 如果$q_1\sim_\varepsilon q_2$, 则存在控制策略$f_2:Q_2^*\to A_2$使得对于任意的$\sigma_2\in\mathrm{Out}(q_2,f_2)$, 存在$\sigma_1\in\mathrm{Out}(q_1,f_1)$使得$\sigma_1\sim_\varepsilon\sigma_2$.[1]

引理 2　令$T_i=(Q_i,A_i,B_i,\underset{i}{\rightarrow},O,H_i)(i=1,2)$是两个度量的、非死锁的交替转换系统并且$d$是观测集合$O$上的度量. 假设$P$是一个有限原子命题集合, $\Pi:O\to P$是赋值函数并且$\varepsilon\in\mathbb{R}_+^0$. 对于任意的$\sigma_1\in Q_1^\omega$和$\sigma_2\in Q_2^\omega$, 如果$\sigma_1\sim_\varepsilon\sigma_2$, 则对于任意的$LTL$公式$\varphi$, 若$(T_1,d),\sigma_1\models\varphi$则$(T_2,d),\sigma_2\models ltr_\varepsilon(\varphi)$.

证　关于公式φ的结构复杂度归纳证明. 由定义9可知, φ仅可能是如下形式之一: p, $\neg p$, $\boldsymbol{X}\varphi_1$, $\varphi_1\wedge\varphi_2$, $\varphi_1\vee\varphi_2$, $\varphi_1\boldsymbol{U}\varphi_2$, $\varphi_1\tilde{\boldsymbol{U}}\varphi_2$, $\Box\varphi_1$, $\diamond\varphi_1$. 下面仅以$\neg p$和$\varphi_1\tilde{\boldsymbol{U}}\varphi_2$为例给出证明, 其他几种情形可以类似证明.

情形 1　$\varphi=\neg p$. 假设$\sigma_1\in Q_1^\omega$和$\sigma_2\in Q_2^\omega$, $\sigma_1\sim_\varepsilon\sigma_2$并且$(T_1,d),\sigma_1\models\varphi$. 因此, 由定义10可知, $\Pi(H_1(\sigma_1[1]))\neq p$. 另一方面, 因为$\sigma_1\sim_\varepsilon\sigma_2$, 所以$\sigma_1[1]\sim_\varepsilon\sigma_2[1]$. 进而$d(H_1(\sigma_1[1]),H_2(\sigma_2[1]))\leqslant\varepsilon$. 因此, 由定义10可知, $(T_2,d),\sigma_2[1]\models<\varepsilon>\neg p$. 即$(T_2,d),\sigma_2\models<\varepsilon>\neg p$

情形 2　$\varphi=\varphi_1\tilde{\boldsymbol{U}}\varphi_2$. 假设$\sigma_1\in Q_1^\omega$和$\sigma_2\in Q_2^\omega$,

$\sigma_1 \sim_\varepsilon \sigma_2$并且$(T_1,d),\sigma_1 \models \varphi$. 根据定义10, 对于任意的$j \geqslant 1$, 如果$(T_1,d),\sigma_1[j] \not\models \varphi_2$, 则存在$k \in \mathbb{N}$使得$i \leqslant k < j$并且$(T_1,d),\sigma_1[k] \models \varphi_1$. 假设$j \geqslant 1$并且$(T_2,d),\sigma_2[j] \not\models ltr_\varepsilon(\varphi_2)$. 由归纳假设可知, $(T_1,d),\sigma_1[j] \not\models \varphi_2$. 所以, 存在$k \in \mathbb{N}$使得$i \leqslant k < j$并且$(T_1,d),\sigma_1[k] \models \varphi_1$. 根据归纳假设, $(T_2,d),\sigma_2[k] \models ltr_\varepsilon(\varphi_1)$. 因此, 由定义10可知, $(T_2,d),\sigma_2 \models ltr_\varepsilon(\varphi)$.

证毕.

定理 1 令$T_i=(Q_i,A_i,B_i,\underset{i}{\rightarrow},O,H_i)(i=1,2)$是两个度量的、非死锁的交替转换系统, 集合$Q_1$是有限的并且$d$是观测集合$O$上的度量. 假设$P$是一个有限原子命题集合, $\Pi: O \to P$是赋值函数并且$\varepsilon \in \mathbb{R}^0_+$. 如果$T_1$受控满足$LTL$公式$\varphi$, 则$T_2$受控满足$ltr_\varepsilon(\varphi)$.

证 假设T_1受控满足LTL公式φ. 则存在$q_1 \in Q_1$和控制策略$f_1: Q_1^* \to A_1$使得对于任意的$\sigma_1 \in \mathrm{Out}(q_1,f_1)$都有$(T_1,d),\sigma_1 \models \varphi$. 由引理1可知, 存在$q_2 \in Q_2$和控制策略$f_2: Q_2^* \to A_2$使得对于任意的$\sigma_2 \in \mathrm{Out}(q_2,f_2)$都存在$\sigma_1 \in \mathrm{Out}(q_1,f_1)$满足条件$\sigma_1 \sim_\varepsilon \sigma_2$. 进而, 由引理2可知, 对于任意的$\sigma_2 \in \mathrm{Out}(q_2,f_2)$, (T_2,d), $\sigma_2 \models ltr_\varepsilon(\varphi)$. 因此, 根据定义10, T_2受控满足$ltr_\varepsilon(\varphi)$. 证毕.

根据上述定理, 本文给出带扰动控制系统形式化设计方案如下. 如图1所示, 针对线性系统和非线性系统分别采用文献[23]和文献[24]中的方法构造有限交替转换系统作为原系统的有限抽象, 进而利用文献[26]所给出的算法求解使该有限抽象满足规范φ的控制策略, 最后基于该控制策略构造原系统的控制器. 定理1可以确保原系统受控满足$ltr_\varepsilon(\varphi)$. 因为$ltr_\varepsilon(\varphi)$可以视为φ的一个弱化版本, 所以可以称该控制器使原系统近似满足规范φ.

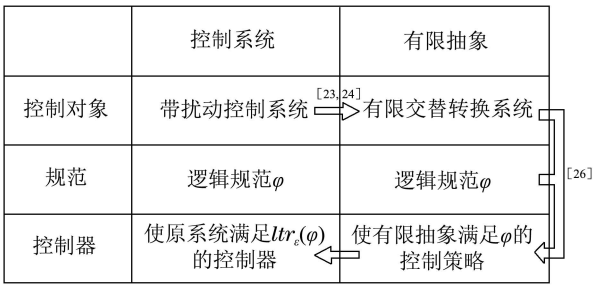

图 1 近似满足规范的控制器设计

Fig. 1 The design of controller enforcing approximate specification

4 严格满足规范的控制器设计(Design of controller enforcing specification exactly)

上一节给出了使控制系统近似满足规范的控制器的构造方法. 然而, 在一些情形下可能要求控制系统严格满足给定规范. 本节将提出基于有限抽象构造使原系统严格满足规范的控制器的方法. 为了实现这种方法, 本节将引入“强化”转换函数将给定规范转换为一个要求“更强”的规范. 这种“更强”的规范由下面这个逻辑语言描述.

定义 12 令P是一个有限原子命题集合并且$\varepsilon \in \mathbb{R}^0_+$. 线性时序逻辑$LTL_s^\varepsilon(P)$公式归纳定义如下:

$$\varphi ::= p|[\varepsilon]p|\neg p|[\varepsilon]\neg p|\boldsymbol{X}\varphi|\varphi_1 \wedge \varphi_2|\varphi_1 \vee \varphi_2|\varphi_1 \boldsymbol{U} \varphi_2|\varphi_1 \tilde{\boldsymbol{U}} \varphi_2|\Box\varphi|\diamond\varphi,$$

其中$p \in P$.

定义 13 令P是一个有限原子命题集合, $\varepsilon \in \mathbb{R}^0_+$, $T=(Q,A,B,\to,O,H)$是一个交替转换系统, d是O上一个度量并且$\Pi: O \to P$是一个赋值函数. 轨迹$\sigma \in Q^\omega$在第$i(i \in \mathbb{N})$个位置满足$LTL_s^\varepsilon(P)$公式φ(记作$(T,d),\sigma[i] \models \varphi$)归纳定义如下:

1) $(T,d),\sigma[i] \models [\varepsilon]p$当且仅当对于任意的$q \in Q$, 如果$d(H(\sigma[i]),H(q)) \leqslant \varepsilon$则$\Pi(H(q))=p$;

2) $(T,d),\sigma[i] \models [\varepsilon]\neg p$当且仅当对于任意$q \in Q$, 如果$d(H(\sigma[i]),H(q)) \leqslant \varepsilon$则$\Pi(H(q)) \neq p$;

3) 当公式φ具有其他形式时, 其可满足性定义与定义10相同.

本文称σ满足$LTL_s^\varepsilon(P)$公式φ(记作$(T,d),\sigma \models \varphi$)当且仅当$(T,d),\sigma[1] \models \varphi$. 转换系统$T$被称为是受控满足公式$\varphi$的, 当且仅当存在$T$的控制策略$f: Q^* \to A$和初始状态$q \in Q$使得对于任意的$\sigma \in \mathrm{Out}(q,f)$都有$(T,d),\sigma \models \varphi$.

“强化”转换函数定义如下, 这个函数将在本节扮演关键角色.

定义 14 令P是一个有限原子命题集合并且$\varepsilon \in \mathbb{R}^0_+$. 将$LTL$公式映射为$LTL_s^\varepsilon$公式的转换函数$str_\varepsilon$定义如下:

1) $str_\varepsilon(p)=[\varepsilon]p$;

2) $str_\varepsilon(\neg p)=[\varepsilon]\neg p$;

3) $str_\varepsilon(\odot\varphi)=\odot str_\varepsilon(\varphi)$, 其中$\odot \in \{\boldsymbol{X},\Box,\diamond\}$;

4) $str_\varepsilon(\varphi_1 \oplus \varphi_2)=str_\varepsilon(\varphi_1) \oplus str_\varepsilon(\varphi_2)$, 其中$\oplus \in \{\wedge,\vee,\boldsymbol{U},\tilde{\boldsymbol{U}}\}$.

容易验证, 对于任意系统T和状态q, 如果φ是一个LTL公式并且$(T,d),\sigma \models str_\varepsilon(\varphi)$, 则$(T,d),\sigma \models \varphi$. 但反之未必成立. 因此, 转换函数$str_\varepsilon$可以视为增强了规范的要求, 所以将其称为“强化”转换函数.

引理 3 令$T_i=(Q_i,A_i,B_i,\underset{i}{\rightarrow},O,H_i)(i=1,2)$是两个度量的、非死锁的交替转换系统并且$d$是观测集合$O$上的度量. 假设$P$是一个有限原子命题集合, $\Pi: O \to P$是赋值函数并且$\varepsilon \in \mathbb{R}^0_+$. 对于任意的$\sigma_1 \in Q_1^\omega$和$\sigma_2 \in Q_2^\omega$, 如果$\sigma_1 \sim_\varepsilon \sigma_2$, 则对于任意的$LTL$公式$\varphi$, 若$(T_1,d),\sigma_1 \models str_\varepsilon(\varphi)$则$(T_2,d),\sigma_2 \models \varphi$.

证 此引理的证明类似于引理2.　　证毕.

定理 2　令$T_i=(Q_i, A_i, B_i, \underset{i}{\rightarrow}, O, H_i)(i=1,2)$是两个度量的、非死锁的交替转换系统, 集合$Q_1$是有限的并且$d$是观测集合$O$上的度量. 假设$P$是一个有限原子命题集合, $\Pi: O\rightarrow P$是赋值函数并且$\varepsilon\in\mathbb{R}_+^0$. 对于任意$LTL$公式$\varphi$, 如果$T_1$受控满足$str_\varepsilon(\varphi)$, 则$T_2$受控满足$\varphi$.

证 类似于定理1, 由引理1和3可证明此定理. 证毕.

根据上述定理, 本文给出一种带扰动控制系统形式化设计方案如下:

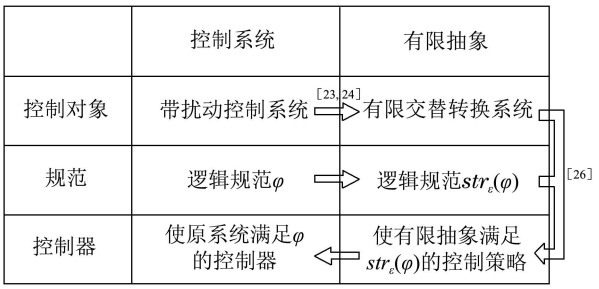

图 2 严格满足规范的控制器设计

Fig. 2 The design of controller enforcing specification exactly

如图2所示, 针对线性系统和非线性系统分别采用文献[23]和文献[24]中的方法构造有限交替转换系统作为原系统的有限抽象, 并将规范φ转换为$str_\varepsilon(\varphi)$, 进而利用文献[26]所给出的算法求解使该有限抽象满足规范$str_\varepsilon(\varphi)$的控制策略, 最后基于该控制策略构造原系统的控制器. 定理2可以确保原系统受控严格满足φ.

5　实例分析(Analysis of example)

本节例子中的控制系统源于文献[27]. 考虑直流电动机的简单模型如下:

$$\Sigma=\begin{cases}\dot{x}=\boldsymbol{A}x+\boldsymbol{B}u+\boldsymbol{G}v,\\ x\in X,\ u\in U,\ v\in V,\end{cases}$$

其中: $x=(x_1,x_2)'$, x_1是电流, x_2是角速度, u是使用的电压, v是多余力的扰动, $X=[0,0.6]\times[0,0.6]$, $U=[0,0.7]$, $V=[-0.01,0.01]$, 并且

$$\boldsymbol{A}=\begin{bmatrix}-R/L & -k_{\rm b}k_{\rm m}/L\\ 1/J & -k_{\rm f}/J\end{bmatrix},$$

$$\boldsymbol{B}=\begin{bmatrix}k_{\rm m}/L\\ 0\end{bmatrix},\ \boldsymbol{G}=\begin{bmatrix}0\\ 1/J\end{bmatrix},$$

其中: $R=0.1$和$L=1$分别是该直流电动机电枢的电阻和电感; $k_{\rm b}=0.2$是电磁力; $k_{\rm m}=0.1$是转矩常数; $k_{\rm f}=0.7$是粘性摩擦力常数; $J=1$是惯性动量.

令原子命题$p_i(i=1,\,2,\,3,\,4)$分别代表下列空间$[0,0.4)\times[0,0.4), [0,0.4)\times[0.4,0.6), [0.4,0.6)\times[0,0.4), [0.4,0.6]\times[0.4,0.6]$. 赋值函数$\Pi$定义为: 对于任意$x\in X$和$i\in\{1,2,3,4\}$, $\Pi(x)=p_i$当且仅当$x\in p_i$. 取公式$\varphi_1=p_1\boldsymbol{U}(p_2\boldsymbol{U}(\neg p_1\wedge\neg p_2))$和$\varphi_2=\Box p_1$作为规范. 下面将构造两个控制器分别使原系统近似满足规范φ_1和严格满足规范φ_2.

按照图1和图2给出的方案, 均需首先构造原系统的有限抽象. 根据文献[23]提出的方法构造上述系统的有限抽象如下: 令取样时间$\tau=5$, $\eta=0.1$且$\mu=0.02$. 则Σ系统的一个有限抽象$T(\Sigma)=(Q,A,B,\rightarrow,O,H)$如下:

• $Q=\{q_i: 0\leqslant i<49\}$, 其中对于$0\leqslant i<49$, $q_i=(\lfloor i/7\rfloor\cdot 0.1\ (i\%7)\cdot 0.1)'$.

• $A=\{a: a\in X_{\rm c}$并且存在$n,m\in\mathbb{Z}$使得$a=(n\cdot 0.02\ \ m\cdot 0.02)'\}$, $X_{\rm c}$如图3所示.

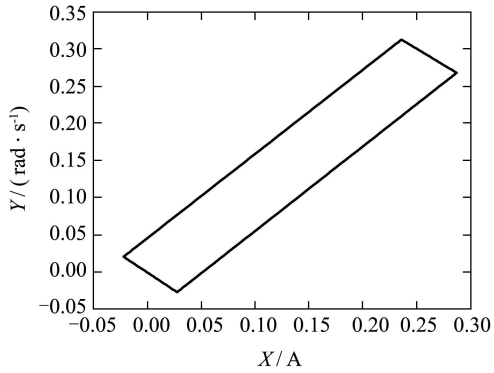

图 3 Σ在输入电压作用下的可达集合的外部近似

Fig. 3 Outer approximation of reachable set of Σ associated with voltage input

• $B=\{b_i: 1\leqslant i\leqslant 3\}$, 其中$b_1=(-0.02\ \ -0.02)'$, $b_2=(0\ \ 0)'$, $b_3=(0.02\ \ 0.02)'$.

• $\longrightarrow\subseteq Q\times A\times B\times Q$. 由于关系$\longrightarrow$的规模较大, 此处仅列举部分(见表1), 其中$a_1=(0.1\ \ 0.1)'$, $a_2=(0.2\ \ 0.2)'$, $a_3=(0.14\ \ 0.14)'$.

表 1 $T(\Sigma)$的部分转换关系

Table 1 Some transitions of $T(\Sigma)$

$q\xrightarrow{a,b}q'$	a_1,b_1	a_1,b_2	a_1,b_3
q_0	q_8	q_8	q_8
$q\xrightarrow{a,b}q'$	a_2,b_1	a_2,b_2	a_2,b_3
q_0	q_{16}	q_{16}	q_{16}
$q\xrightarrow{a,b}q'$	a_1,b_1	a_1,b_2	a_1,b_3
q_8	q_9	q_{16}	q_{16}
$q\xrightarrow{a,b}q'$	a_3,b_1	a_3,b_2	a_3,b_3
q_9	q_{16}	q_{16}	q_{16}

• $O=X$.

• $H=id_X$是一个恒等映射.

根据文献[23]和文献[27], 容易验证上述系统与Σ的取样系统是ε–交替近似互模拟的, 其中$\varepsilon = 0.15$. 需要指出的是, 由于扰动输入的存在, 无法构造与取样系统严格互模拟的有限抽象, 因此Tabuada和Pappas在文献[6]中提出的方法不适用于该问题的求解.

下面将先构造使原系统近似满足规范φ_1的控制器. 为此, 采用文献[26]提供的算法寻找有限抽象$T(\Sigma)$的初始状态和使其满足规范φ_1的控制策略如下: 取$(0\ \ 0)'$作为初始状态, 控制策略$f: Q^* \to A$定义为

$$f(s) = \begin{cases} a_1 & s[\text{end}] = q_0 \text{ 或 } s[\text{end}] = q_8 \\ a_3, & s[\text{end}] = q_9 \text{ 或 } s[\text{end}] = q_{16}, \\ a_2, & s[\text{end}] = q_{17} \text{ 或 } s[\text{end}] = q_{25}, \\ a_4, & s[\text{end}] = q_{41}, \\ a_5, & \text{其他}, \end{cases}$$

其中: $a_1 = (0.1\ \ 0.1)'$, $a_2 = (0.2\ \ 0.2)'$, $a_3 = (0.14\ \ 0.16)'$, $a_4 = (0.26\ \ 0.28)'$并且$a_5 = (0.06\ \ 0.06)'$.

下面将根据上述控制策略构造控制器. 利用文献[28]中的结果和MATSSE工具包[29], 容易验证a_i $(i = 1, 2, 3, 4, 5)$分别是如下定义的输入$\boldsymbol{u}_i (i = 1, 2, 3, 4, 5)$的近似: 对于$t \in [0, \tau]$,

$\boldsymbol{u}_1(t) = 0.25$, $\boldsymbol{u}_2(t) = 0.505$, $\boldsymbol{u}_3(t) = 0.38$, $\boldsymbol{u}_4(t) = 0.685$, $\boldsymbol{u}_5(t) = 0.15$.

因此, 由控制策略f及上述结论可以构造控制器如下: 在取样时间点$n\tau (n \in \mathbb{N})$, 如果当前状态x近似于q_0(即, $\|x - q_0\| \leqslant \eta/2$)或$q_8$则选择输入$\boldsymbol{u}_1$; 如果当前状态$x$近似于$q_9$或$q_{16}$则选择输入$\boldsymbol{u}_3$; 如果当前状态$x$近似于$q_{17}$或$q_{25}$则选择输入$\boldsymbol{u}_2$; 如果当前状态$x$近似于$q_{41}$则选择输入$\boldsymbol{u}_4$; 否则输入$\boldsymbol{u}_5$.

本文利用MATLAB进行了仿真实验, 设置仿真截止时间为1000, 在上述控制器作用下得到的系统Σ的轨迹满足规范$ltr_\varepsilon(\varphi_1)$. 例如, 其中一次实验轨迹如图4所示.

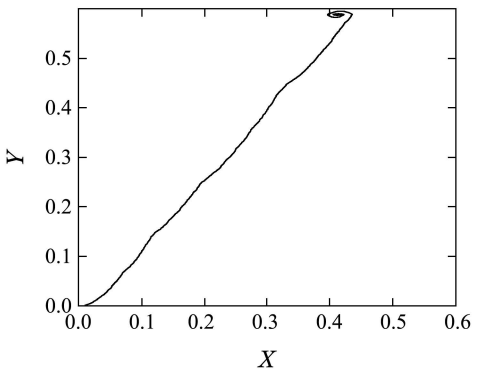

图 4 近似满足规范φ_1的轨迹

Fig. 4 The trajectory satisfying the specification φ_1 approximately

下面将按照图2提供的方案构造使原系统严格满足规范φ_2的控制器. 系统Σ的有限抽象仍取上面构造的有限交替转换系统$T(\Sigma)$. 由文献[26]提供的算法可以验证, 选取初始状态为$q_0 = (0\ \ 0)'$及如下定义的控制策略$f': Q^* \to A$即可使$T(\Sigma)$受控满足规范$str_\varepsilon(\varphi_2)$:

$$f'(s) = \begin{cases} a_2, & s[\text{end}] = q_0, \\ a_5, & \text{其他}. \end{cases}$$

类似地, 可以由此控制策略构造控制器为: 在取样时间点$n\tau (n \in \mathbb{N})$, 如果当前状态x近似于q_0则选择输入$\boldsymbol{u}_2$; 否则输入$\boldsymbol{u}_5$.

本文利用MATLAB进行了仿真实验, 设置仿真截止时间为1000, 在上述控制器作用下得到的系统Σ的轨迹满足规范φ_2. 例如, 其中一次实验轨迹如图5所示.

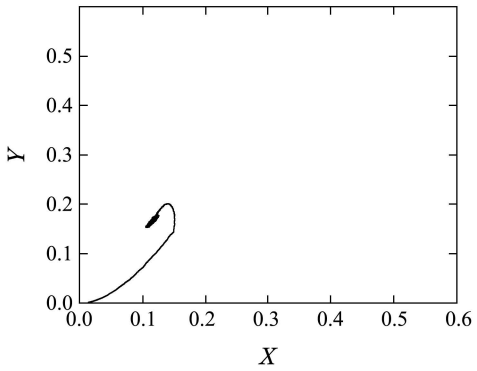

图 5 严格满足规范φ_2的轨迹

Fig. 5 The trajectory satisfying specification φ_2 exactly

但是, 需要指出的是, 按照文献[26]提供的算法可以判定不存在初始状态和控制策略使有限抽象$T(\Sigma)$满足规范$str_\varepsilon(\varphi_1)$. 因此, 按照图2提供的方案无法构造使原系统严格满足规范φ_1的控制器.

6 总结及相关工作比较(Conclusion and comparison with related work)

本文在线性时序逻辑公式上定义了“弱化”转换函数和“强化”转换函数, 分别基于这两个转换函数给出了两种控制器构造方法. 基于“弱化”转换函数ltr_ε, 本文给出了构造使带扰动控制系统近似满足规范的方法(见图1). 其近似程度由“弱化”转换函数ltr_ε所刻画. 基于“强化”转换函数str_ε, 本文建立了构造使带扰动控制系统严格满足规范的方法(见图2). 第5节中的实例分析说明了上述两种方法的有效性.

下面就本文提出的两种方法与文献[6]所给出的方法展开比较, 说明各自的优势及适用的情形. 在文献[6]中, Tabuada和Pappas构造与原系统互模拟的有限转换系统作为其有限抽象, 给出其有限抽象的控制策略, 进而利用此控制策略构造原系统的控制器. 他们对控制系统及其有限抽象采用了相同的逻辑规范,

并基于互模拟的逻辑特征证明了系统在采用其方法构造出的控制器下严格满足给定规范. 为了叙述方便, 下文将这种方法简称为T–P方法. T–P方法与本文第3节和第4节方法之间的主要差异如表2所示.

表 2 T–P方法与本文方法比较

Table 2 Comparing T–P method with the methods provided by this paper

	T–P方法	第3节方法	第4节方法
系统与抽象关系	互模拟	近似互模拟	近似互模拟
系统与抽象的规范	相同	相同	不相同
系统受控满足规范	严格满足	近似满足	严格满足
抽象的构造	相对困难	相对容易	相对容易
求控制策略可能性	不降低	不降低	降低

如表2所示, T–P方法要求构造的有限抽象与原系统互模拟, 而本文的两种方法采用近似互模拟描述控制系统与其有限抽象之间的关系. 由于互模拟的要求比近似互模拟更严格, 这使得构造T–P方法所需的有限抽象相对比较困难. 例如在上一节中, 无法构造与控制系统Σ的取样系统严格互模拟的有限抽象. 此外, 在T–P方法中, Tabuada和Pappas对控制系统及其有限抽象采用了相同规范, 并基于互模拟的逻辑特征证明了系统在采用T–P方法构造出的控制器下严格满足给定规范[6]. 文献[25]指出, 近似互模拟不保证逻辑等价性, 这导致本文的两种方法中的控制系统与其有限抽象未必可控满足相同规范. 这两种方法分别采用不同方案处理这一情况: 第3节的方法将给定规范作为有限抽象的规范, 并证明了如果有限抽象可控满足该规范, 则原系统在构造的控制器作用下近似满足给定规范; 第4节引入“强化”转换函数, 将转换后的规范作为有限抽象的规范, 并证明了有限抽象可控满足转换后规范蕴涵原系统可控严格满足给定规范. 由此可见, 第4节的方法既保证了有限抽象的易构性, 又确保了控制系统控制器的精准性. 然而, 有得必有失, 如第5节中实例分析中所示, 该方法付出的代价是降低了有限抽象控制策略存在的可能性.

总的来说, 如表2所示, 第4节的方法可以确保有限抽象的易构性并保证控制系统在构造的控制器下严格地满足原规范, 为此付出的代价是降低了有限抽象控制策略存在的可能性; 第3节方法不会降低有限抽象的易构性及有限抽象控制策略存在的可能性, 但牺牲了控制系统控制器的精确性; T–P方法既不会降低有限抽象控制策略存在的可能性, 也可以保证控制器的准确性, 但所需的有限抽象较难构造. 总之, 这3种不同方法是对如下3种因素做出不同权衡提出的: 1) 控制器的精准性, 2) 有限抽象的易构性, 3) 获得有限抽象控制策略的可能性. 这3种方法各有优缺点, 适用于不同的场合. 给定控制系统, 如果与之互模拟的有限抽象容易构造, 则T–P方法可以兼顾上述3种因素, 是最适用的方法. 当与给定控制系统互模拟的有限抽象很难构造时, 为了确保形式化设计的可行性, 需要降低有限抽象的构造难度, 可选择本文的方法. 此时, 具体选择何种方法依赖于实际需求对控制器精确性的要求, 即, 如果实际需求对控制器精确性要求很高, 则首先尝试使用第4节的方法为宜.

参考文献(References):

[1] HABETS L, VAN SCHUPPEN J H. A control problem for affine dynamical systems on a full-dimensional polytope [J]. *Automatica*, 2004, 40(1): 21 – 35.

[2] HABETS L, VAN SCHUPPEN J H. Control of piecewise-linear hybrid systems on simplices and rectangles [C] //*Proceedings of Hybrid Systems: Computation and Control*. New York: Springer-Verlag, 2001, 2034: 261 – 274.

[3] KRESS-GAZIT H, FAINEKOS G E, PAPPAS G J. Temporal logic motion planning for mobile robots [J]. *IEEE Transactions on Robotics*, 2005, 21(5): 2020 – 2025.

[4] FAINEKOS G E, KRESS-GAZIT H, PAPPAS G J. Hybrid controllers for path planning: a temporal logic approach [C] //*Proceedings of the 44th IEEE Conference on Decision and Control, and the European Control Conference 2005*. Seville, Spain: IEEE, 2005: 4885 – 4890.

[5] KLOETZER M, BELA C. A Fully Automated framework for control of linear systems from LTL specifications [J]. *IEEE Transactions on Automatic Control*, 2008, 53(1): 287 – 297.

[6] TABUADA P, PAPPAS G J. Linear time logic control of discrete-time linear systems [J]. *IEEE Transactions on Automatic Control*, 2006, 51(12): 1862 – 1877.

[7] KOUTSOUKOS X, ANTSAKLIS P, STIVER J, et al. Supervisory control of hybrid systems [J]. *Proceedings of the IEEE*, 2002, 88(7): 1026 – 1049.

[8] TABUADA P, PAPPAS G J. From discrete specifications to hybrid control [C] //*Proceedings of the 42nd IEEE Conference on Decision and Control*. Hawaii, USA: IEEE, 2003: 3366 – 3371.

[9] ALUR R, HENZINGER T A. Discrete abstractions of hybrid systems [J]. *Proceedings of the IEEE*, 2000, 88(7): 971 – 984.

[10] GIRARD A. Approximately bisimilar finite abstractions of stable linear systems [C] //*Proceedings of Hybrid Systems: Computation and Control*. New York: Springer-Verlag, 2007, 4416: 231 – 244.

[11] POLA G, GIRARD A, TABUADA P. Approximately bisimilar symbolic models for nonlinear control systems [J]. *Automatica*, 2008, 44(10): 2508 – 2516.

[12] TABUADA P. An approximate simulation approach to symbolic control [J]. *IEEE Transactions on Automatic Control*, 2008, 53(6): 1406 – 1418.

[13] LERDA F, KAPINSKI J, CLARKE E. M, et al. Verification of supervisory control software using state proximity and merging [C] // *Proceedings of the 11th International Workshop of Hybrid Systems: Computation and Control*. New York: Springer-Verlag, 2008, 4981: 344 – 357.

[14] GIRARD A. Controller synthesis for safety and reachability via approximate bisimulation [J]. *Automatica*, 2012, 48(5): 947 – 953.

[15] JULIUS A, WINN A K. Safety controller synthesis using human generated trajectories: nonlinear dynamics with feedback linearization and differential flatness [C] //*Proceedings of the 2012 American Control Conference*. Montréal, Canada: IEEE, 2012, 709 – 714.

[16] CAMARA J, GIRARD A, GOESSLER G. Synthesis of switching controllers using approximately bisimilar multiscale abstractions [C] // *Proceedings of the 14th International Conference on Hybrid Systems: Comput Control*. New York: ACM, 2011: 191 – 200.

[17] ALUR R. Formal verification of hybrid systems [C] //*Proceedings of International Conference on Embedded Software*. Taipei: IEEE, 2011: 273 – 278.

[18] GIRARD A, PAPPAS G J. Approximate bisimulation: a bridge between computer science and control theory [J]. *European Journal of Control*, 2011, 17(5/6): 568 – 578.

[19] KUO B C. *Auotmatic Control Systems* [M]. New York: Prentice-Hall, 1975.

[20] 程春华, 胡云安, 吴进华, 等. 非仿射系统的自适应观测器自抗扰控制 [J]. 控制理论与应用, 2014, 31(2): 148 – 158.
(CHENG Chunhua, HU Yunan, WU Jinhua, et al. Auto disturbance rejection controller for non-affine nonlinear systems with adaptive observers [J]. *Control Theory & Applications*, 2014, 31(2): 148 – 158.)

[21] 高志强. 自抗扰控制思想探究 [J]. 控制理论与应用, 2013, 30(12): 1498 – 1510.
(GAO Zhiqiang. On the foundation of active disturbance rejection control [J]. *Control Theory & Applications*, 2013, 30(12): 1498 – 1510.)

[22] 王丽君, 李擎, 童朝南, 等. 时滞系统的自抗扰控制综述 [J]. 控制理论与应用, 2013, 30(12): 1521 – 1533.
(WANG Lijun, LI Qing, TONG Chaonan, et al. Overview of active disturbance rejection control for systems with time-delay [J]. *Control Theory & Applications*, 2013, 30(12): 1521 – 1533.)

[23] POLA G, TABUADA P. Symbolic models for nonlinear control systems: alternating approximate bisimulations [J]. *SIAM Journal on Control and Optimization*, 2009, 48(2): 719 – 733.

[24] BORRI A, POLA JG, BENEDETTO D M. Symbolic models for nonlinear control systems affected by disturbances [J]. *International Journal of Control*, 2012, 85(10): 1422 – 1432.

[25] ZHANG J J, ZHU Z H. A modal characterization of alternating approximate bisimilarity [J]. *Formal Methods in System Design*, 2014, 44(3): 240 – 263.

[26] KLOETZER M, BELTA C. Dealing with nondeterminism in symbolic control [C] //*Proceedings of the 11th International Workshop on Hybrid Systems: Computation and Control*. New York: Springer-Verlag, 2008, 4981: 287 – 300.

[27] POLA G, TABUADA P. Symbolic models for nonlinear control systems affected by disturbances [C] //*Proceedings of IEEE Conference on Decision and Control*. Cancun, Mexico: IEEE, 2008: 251 – 256.

[28] GIRARD A. Reachability of uncertain linear systems using zonotopes [C] //*Proceedings of the 8th International Workshop on Hybrid Systems: Computation and Control*. Berlin: Springer, 2005, 3414: 291 – 305.

[29] GIRARD A. Metrics for approximate transition systems simulation and equivalence (MATSSE) [EB/OL]. http://ljk.imag.fr/membres/Antoine. Girard/Software/Matisse/index.html.

作者简介:

张晋津 (1981–), 男, 讲师, 博士, 目前研究方向为形式化方法、控制系统形式化分析与设计等, E-mail: jinjinzhang@nau.edu.cn;

张 严 (1983–), 男, 博士研究生, 目前研究方向为形式化方法、计算机科学中的逻辑学, E-mail: yanzhang_nuaa@nuaa.edu.cn;

朱朝晖 (1970–), 男, 教授, 博士生导师, 目前研究方向为形式化方法、计算机科学中的逻辑学等, E-mail: zhaohui@nuaa.edu.cn.