第 27 卷第 3 期
2010 年 3 月
控 制 理 论 与 应 用
Control Theory & Applications
Vol. 27 No. 3
Mar. 2010

文章编号: 1000−8152(2010)03−0317−06

基于定性推理的矩形phase-portrait近似

刘保罗[1,2], 裴海龙[2]

(1. 洛阳理工学院 计算机与信息工程系, 河南 洛阳 471023; 2. 华南理工大学 自动化科学与工程学院, 广东 广州 510640)

摘要: 矩形phase-portrait近似的关键是控制模态的有效划分. 本文提出了基于定性推理的phase-portrait近似, 给出了一种基于向量场、感兴趣多项式及其李导数动态特性的模态空间划分方法, 并进一步给出了基于精化多项式的抽象模型精化方法. 实验结果表明, 基于定性推理划分的phase-portrait近似验证明显地减少了模态空间的划分数目, 提高了验证的效率.

关键词: 混合自动机; 时间模拟; phase-portrait近似

中图分类号: TP271　　**文献标识码**: A

Rectangular phase-portrait approximation based on qualitative reasoning

LIU Bao-luo[1,2], PEI Hai-long[2]

(1. Department of Computer and Information Engineering, Luoyang Institute of Science and Technology, Luoyang Henan 471023, China;
2. College of Automation Science and Technology, South China University of Technology, Guangzhou Guangdong 510640, China)

Abstract: The core of the rectangular phase-portrait approximation is the efficient partition of the control model. The phase-portrait approximation based on quality reasoning is proposed. An approach for mode partition is then presented based on the characteristic of the vector field, interesting polynomials and their Lie-derivative. A method for the refinement of the abstract model based on the refined polynomials is also given. Experiment shows that the phase-portrait approximation based on the qualitative-reasoning partition obviously reduces the partition number of the mode state space, and enhances the verification efficiency.

Key words: hybrid automaton; time simulation; phase-portrait approximation

1 引言(Introduction)

混合系统是连续动态和离散事件过程并存且相互交换信息的动态系统, 如数字嵌入式系统. 安全性保证是混合系统设计的主要要求之一. 由于混合系统涉及复杂的连续动态和离散动态, 安全性验证问题的可判定性仅限于一些的简单混合系统, 如时间自动机、矩形自动机等. 对于一般的混合系统, 安全性问题是不可判定的[1,2]. 基于这个问题, 研究者提出了许多方法, 旨在寻找验证安全性的充分条件, 抽象近似是验证的主要方法之一. 抽象验证是基于所要验证的性质[3,4], 首先将复杂系统映射到保持兴趣行为的简化模型上, 然后在简化模型进行验证以推理出原系统的性质. phase-portrait近似是抽象近似方法在混合系统安全性验证的典型应用, 它以可判定或可计算的混合自动机(如线性自动机)为目标模型进行模型转换, 抽象近似自动机模拟原系统.

Phase-portrait近似的关键是控制模态状态空间的划分, 它直接影响着近似自动机模拟原系统的精确程度. 现有文献缺乏对模态空间划分策略的研究, 在文献[5]给出一种均匀矩形划分策略, 这种均匀静态划分在模型精化过程中往往会引起模态数量的剧增. 针对这个问题, 本文提出了基于定性推理的phase-portrait近似方法, 依据系统的动态特性来指导状态空间的划分, 给出了一种基于向量场动态特性、感兴趣多项式及其李导数的状态空间划分方法. 本文所考虑的对象为仿射混合系统.

2 预备知识(Preliminaries)

设$X = \{x_1, \cdots, x_n\}$为有限变量集, X上的线性项为表达式$y \equiv a_0 + \sum\limits_{x_i \in X} a_i x_i$, 其中$a_i \in \mathbb{Q}(0 \leqslant i \leqslant n)$是有理常数. X上线性项的全体表示为$\mathrm{LTerm}(X)$. 线性约束定义为$y \sim 0$, 其中$y \in$

收稿日期: 2008−05−30; 收修改稿日期: 2008−11−10.
基金项目: 国家自然科学基金重点资助项目(60736024).

$\mathrm{Lterm}(X)$, $\sim\in\{<,\leqslant,=,>,\geqslant\}$. 线性谓词定义为线性约束的合取. X上线性谓词的全体记为$\mathrm{Lin}(X)$. X的仿射动态定义为: $\bigwedge\limits_{x_i\in X}\dot{x}_i=t_{x_i}$, 其中$t_{x_i}\in \mathrm{LTerm}(X)$是$X$上的线性项. X上的全体仿射动态谓词集表示为$\mathrm{Affine}(\dot{X},X)$. X的矩形动态定义为: $\bigwedge\limits_{x_i\in X}\dot{x}_i\in I_{x_i}$, 其中$I_{x_i}(x_i\in X)$是实数域上的闭区间. X上矩形动态谓词的全体记为$\mathrm{Rect}(\dot{X})$. 给定X上的任意谓词公式p, 以符号$[\![p]\!]$表示使谓词p取真值的值集.

3 仿射混合自动机的矩形phase-portrait近似(Rectangular phase-portrait approximation of affine hybrid automata)

3.1 仿射混合自动机(Affine hybrid automata)

定义 1 分段仿射混合自动机是一个元组$H=(L,X,\mathrm{Lab},E,\mathrm{Init},\mathrm{Inv},\mathrm{Flow},J,U)$, 其中:

· L是离散位置集, 离散位置又称为控制模态.

· $X=\{x_1,\cdots,x_n\}$是有限变量集.

· Lab是标签集, 其中包括静默迁移标签τ.

· $E\subseteq L\times\mathrm{Lab}\times L$是离散迁移关系.

· $\mathrm{Init}:L\to\mathrm{Lin}(X)$是初始条件.

· $\mathrm{Inv}:L\to\mathrm{Lin}(X)$赋予每个离散位置不变集.

· $\mathrm{Flow}:L\to\mathrm{Affine}(\dot{X},X)$赋予每个离散位置仿射向量场.

· $J:E\to\mathrm{Lin}(X,X')$是迁移条件, X'表示迁移后变量的更新值.

· $U:L\to\mathrm{Lin}(X)$是最终状态, 表示不安全集.

例 1[6] 一个燃气供热系统, 由单个燃气炉为两个水箱供热, 其动力系统的建模为仿射混合自动机, 如图1所示. 燃气炉有两种工作模式: 停止运转(模态l_0)和运转加热, 分别为两个水箱之一供热(模态l_1,l_2), 变量x_1,x_2分别表示两个水箱的温度, 模态的动态由ON_i和$\mathrm{OFF}_i(i=1,2)$给定, 其中常数a_i表示水箱i与房间之间的温度交换率, b_i表示水箱间的温度交换率, h为燃气炉的功率. 设定$h=2$, $a_1=a_2=0.01$, $b_1=b_2=0.005$. 由图1可知建模自动机的各个模态具有仿射动态.

仿射混合自动机H的语义是一个赋时迁移系统[5](timed transition systems, TTS)$[\![H]\!]=(Q,Q_0,Q_{\mathrm{f}},\varSigma,\to)$, 其中: Q,Q_0和Q_{f}分别为状态集、初始状态集和不安全状态集, $\varSigma$是包含静默标签τ的标签集, $\to$是迁移关系. 混合自动机H称为安全的, 如果从初始状态出发的所有轨迹永远不会进入不安全区域, 即$\mathrm{Reach}([\![H]\!])\cap\bigcup\limits_{l\in L}[\![U(l)]\!]=\emptyset$.

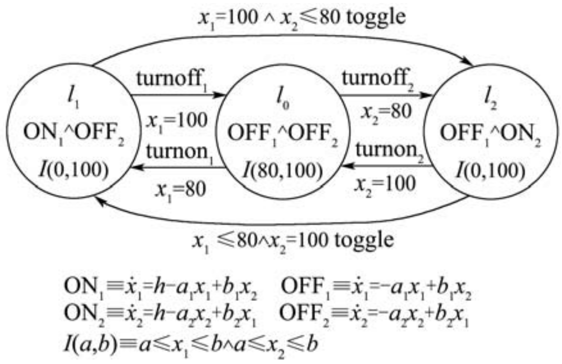

图 1 燃气供热系统建模混合自动机

Fig. 1 Hybrid automaton for gas-heating system

给定赋时迁移系统$T=\{Q,Q_0,Q_{\mathrm{f}},\varSigma,\to\}$, 定义关系[5]$\twoheadrightarrow\subseteq Q\times(\varSigma\backslash\{\tau\}\cup\mathbb{R}^{\geqslant 0})\times Q$, 如果$q\overset{\sigma}{\twoheadrightarrow}q'$, $\sigma\in\varSigma\backslash\{\tau\}$, 则存在有限序列$q_1,\cdots,q_k$, 使得$q\xrightarrow{\tau}q_1\xrightarrow{\tau}\cdots\xrightarrow{\tau}q_k\xrightarrow{\sigma}q'$, 如果$q\overset{t}{\twoheadrightarrow}q'$, $t\in\mathbb{R}^{\geqslant 0}$, 则存在有限序列$t_1,\cdots,t_k$使得$q\xrightarrow{t_0}q_1\xrightarrow{\tau}q_2\xrightarrow{t_1}\cdots\xrightarrow{\tau}q_{2k}\xrightarrow{t_k}q'$, 且$t=t_1+\cdots+t_k$.

定义 2[5] 给定两个赋时迁移系统TTS: $T_1=(Q^1,Q^1_0,Q^1_{\mathrm{f}},\varSigma,\to^1)$ 和$T_2=(Q^2,Q^2_0,Q^2_{\mathrm{f}},\varSigma,\to^2)$, 如果在$T_1$与$T_2$之间存在关系$R\subseteq Q^1\times Q^2$满足:

· 对于任意的$(q_1,q_2)\in\mathbb{R}$, $\sigma\in\varSigma\backslash\{\tau\}\cup\mathbb{R}^{\geqslant 0}$, 如果$q_2\overset{\tau}{\twoheadrightarrow}q'_2$, 则存在$q'_1\in\mathbb{Q}^1$, 满足$q_1\overset{\sigma}{\twoheadrightarrow}q'_1$且$(q'_1,q'_2)\in\mathbb{R}$.

· 对于任意的$q_2\in\mathbb{Q}^2_0$, 存在$q_1\in\mathbb{Q}^1_0$满足$(q_1,q_2)\in\mathbb{R}$.

· 对于任意的$q_2\in\mathbb{Q}^2_{\mathrm{f}}$, 存在$q_1\in\mathbb{Q}^1_{\mathrm{f}}$满足$(q_1,q_2)\in\mathbb{R}$.

则称T_1弱时间模拟T_2, 记为: $T_2\preceq_{wT}T_1$.

给定混合自动机H_1和H_2, 其TTS分别为$[\![H_1]\!]$, $[\![H_2]\!]$, 如果$[\![H_1]\!]\preceq_{wT}[\![H_2]\!]$, 则称混合自动机$H_2$弱时间模拟混合自动机$H_1$, 简记为: $H_1\preceq_{wT}H_2$.

基于抽象近似进行验证的理论依据为:

定理 1[5] 如果混合自动机H_1和H_2满足$H_1\preceq_{wT}H_2$, 且H_2是安全的, 则H_1是安全的.

混合自动机H的矩形phase-portrait近似是通过抽象近似过程构建混合自动机H', 使得$H\preceq_{wT}H'$且H'具有矩形动态. 由定理1可知, 如果H'是安全的, 则可得出H是安全的.

3.2 矩形phase-portrait近似(Rectangular phase-portrait approximation)

矩形phase-portrait近似是以线性自动机为目标

模型, 将复杂的混合自动机转化为简单的线性自动机的过程. Phase-portrait近似验证的关键是近似线性自动机H'的构造, 其构造过程可分为两个步骤: 1) 针对H的每个离散模态l, 寻找合适的状态空间划分$\Psi(l)=\{\Psi_1^l,\cdots,\Psi_k^l\}$; 2) 在每个划分子区域$(l,\Psi_i^l)$内构造合适的初始集、不变集、矩形向量场、不安全集等元素及区域间的迁移关系, 使得所构造的LHAH'满足$H\preceq_{wT}H'$.

因此如何划分状态空间, 使得矩形动态较好地近似仿射动态, 是phase-portrait近似的关键, 在下文中使用定性推理来指导状态空间的划分.

4 基于定性推理的模态划分(Mode partition based on qualitative reasoning)

考虑混合自动机H的任意模态l, 其状态空间为$S_l=\{(l,\boldsymbol{x})|\boldsymbol{x}\in[\![\mathrm{Inv}(l)]\!]\}$, 基于多项式模态空间划分的定义为:

定义 3　混合自动机H的多项式模态划分是针对H的任意控制模态l, 寻找合适的多项式集P, 使得基于多项式集P模态l的划分$\Psi(l)=\{\Psi_1^l,\cdots,\Psi_k^l\}$构成模态$l$的一个状态空间覆盖, 即满足

$$[\![\mathrm{Inv}(l)]\!]\subseteq\cup[\![\Psi(l)]\!],$$

其中

$$\begin{aligned}[\![\Psi_i^l]\!]=\{\boldsymbol{x}\in\mathbb{R}^n|&\bigwedge_{\alpha\in m_1}p_\alpha(\boldsymbol{x})\geqslant\\&0\wedge\bigwedge_{\beta\in m_2}p_\beta(\boldsymbol{x})\leqslant0\wedge\mathrm{Inv}(l)\},\\&i=1,2,\cdots,k,\end{aligned}$$

$m_1\cup m_2$是集合$\{1,2,\cdots,|P|\}$[1]的划分.

基于多项式集P的模态空间划分定义了多项式模态划分函数$\Psi:L\to2^{\mathbb{R}^n}$, 多项式集$P$称为模态划分多项式集. 模态$l$被划分成$2^{|P|}$个子模态(子区域), 即$k=2^{|P|}$.

确定了划分多项式集就确定了模态的划分, 在下文依据定性推理的方法来选取划分多项式.

4.1 基于向量场特性的划分(Partition based on characteristic of vector fields)

Phase-portrait近似将模态划分成多个子模态(子区域), 在每个子模态内使用微分包含将仿射动态近似为矩形动态. 因此, 子模态内向量场的变化量越大, 则近似矩形动态区间越大, 近似的误差就越大. 考虑依据动态向量场的变化特性来划分状态空间, 使得划分后的状态子空间具有相似的动态特性, 具体叙述如下:

仿射自动机H模态l的向量场为: $\dot{x}_i=t_i$, $t_i\in\mathrm{Lterm}(X)(i=1,\cdots,n)$, 选用多项式集$P=\{x_i,t_i\}_{1\leqslant i\leqslant n}$作为划分多项式集.

基于仿射集P将模态l划分成子模态集$\Psi(l)=\{\Psi_1^l,\cdots,\Psi_k^l\}$. 在每个子模态$\Psi_j^l$内, 变量$x_i(1\leqslant i\leqslant n)$及1阶导数$t_i(1\leqslant i\leqslant n)$的符号保持不变. 因此, 变量$x_i$在每个区域内具有单调性. 同样地, 若在集合$P$增加$x_i$的2阶导数多项式, 则在每个子模态内不仅保持$x_i$变化单调性而且保持了凸性, 此时的模态划分具有更精确的定性性质. 依此类推, 可以在仿射集P中增加x_i的3阶、4阶$\cdots$ K阶导数多项式. 后一级的划分相比前一级具有更精确的定性性质, 精化了前一级的状态空间划分. 因此基于向量场特性来划分状态空间实质上是以具有相同动态特性的状态集合为等价集求取熵空间的过程.

例 2　例1所示的自动机模态l_1的向量场为

$$\dot{x}_1=2-\frac{1}{100}x_1+\frac{1}{200}x_2,$$
$$\dot{x}_2=-\frac{1}{100}x_2+\frac{1}{200}x_1.$$

选择x_i及1阶导数作为划分多项式集P_1为

$$P_1=\{x_1,x_2,400-2x_1+x_2,x_1-2x_2\}.$$

4.2 基于感兴趣多项式及其李导数的划分(Partition based on interesting polynomials and their Lie-derivatives)

定义 4[8]　给定仿射自动机H, 其模态l的向量场为$\mathrm{Flow}(l)$, 多项式p关于$\mathrm{Flow}(l)$的李导数定义为

$$L_{\mathrm{Flow}(l)}(p)=\frac{\partial p}{\partial x_1}\dot{x}_1+\frac{\partial p}{\partial x_2}\dot{x}_2+\cdots+\frac{\partial p}{\partial x_n}\dot{x}_n.$$

李导数是系统动态变化特征在多项式p上的反映. 给定多项式的值及李导数的方向, 可以推断出系统向量场的流向. 具体地讲, 若在某点s上有$p\geqslant0$, $L_{\mathrm{Flow}}(p)\geqslant0$, 则经该点的动态轨迹只会呆在$p\geqslant0$的状态区域, 而不会进入$p\leqslant0$区域; 若$L_{\mathrm{Flow}}(p)\leqslant0$, 则轨迹不仅可以呆在$p\geqslant0$区域内, 也可以进入$p\leqslant0$区域.

因此可以选用感兴趣的多项式集$p_i(i=1,\cdots,k)$, 以$p_i,L_{\mathrm{Flow}}(p_i)$做模态划分多项式. 这种划分不仅体现了系统针对特定多项式的动态变化特性, 而且根据多项式及李导数的符号, 可以判定子模

[1] $|P|$是集合P的势.

态间的迁移关系. 感兴趣集可以是模态的迁移条件多项式、初始集多项式、不变集多项式及不安全集多项式等. 模态间迁移关系tran的计算算法如Algorithm 1所示, 其中poly(q)表示定义模态q的多项式集.

Algorithm 1 迁移关系tran的计算算法:

for every two adjacent modes $q \in L \times \Psi_l$, $q' \in L \times \Psi_l$ do
  for $p_q \in \mathrm{poly}(q)$ and the corresponding $p_{q'} \in \mathrm{poly}(q')$
  do
    if $p_q \geqslant 0$ then
    if $\mathbb{R} \models \mathrm{Inv}(q) \Rightarrow L_{\mathrm{Flow}(q)}(p) \leqslant 0 \wedge p_{q'} \leqslant 0$ then
      tran $\leftarrow (q, q')$;
     else if $\mathbb{R} \models \mathrm{Inv}(q) \Rightarrow L_{\mathrm{Flow}(q)}(p) \geqslant 0$ then
      tran $\leftarrow (q, q')$;
     end if
    else if $p_q \leqslant 0$ then
     if $\mathbb{R} \models \mathrm{Inv}(q) \Rightarrow L_{\mathrm{Flow}(q)}(p) \geqslant 0 \wedge p_{q'} \geqslant 0$
      then tran $\leftarrow (q, q')$;
     else if $\mathbb{R} \models \mathrm{Inv}(q) \Rightarrow L_{\mathrm{Flow}(q)}(p) \leqslant 0$ then
      tran $\leftarrow (q, q')$
     end if
   end if
  end for
end for

例 3 考察例1所示的仿射自动机模态l_1, 选择感兴趣多项式集及其李导数为

$$P_2 = \{x_1 - 100, x_1 - 80, x_2 - 100, x_2 - 80, 400 - 2x_1 + x_2, x_1 - 2x_2\}.$$

4.3 多项式精化(Refinement of polynomials)

基于phase-portrait近似所构造的模型是原系统的外近似, 如果抽象模型经验证不满足安全性要求时, 不能推理出原系统的安全性, 抽象模型需作进一步的精化. 设仿射自动机H任意模态l有划分多项式集$P_l = \{p_i\}_{1 \leqslant i \leqslant k}$, 对任意$p_i \in P_l$求其关于Flow($l$)的李导数$L_{\mathrm{Flow}(l)}(p_i)$, 如果$L_{\mathrm{Flow}(l)}(p_i)$不是常数且与集合$P_l$中的任意多项式不存在常数倍关系, 则将$L_{\mathrm{Flow}(l)}(p_i)$加入多项式集$P_l$中, 以此方式构造所得的多项式集记为$P_l'$, P_l'称为P_l的精化多项式集.

例 4 考虑例1所示自动机模态l_1, 选定初始多项式集为

$$P = \{x_1, x_2, x_1 - 100, x_1 - 80, x_2 - 80, x_2 - 100\},$$

P的精化多项式集P'为

$$P' = \{x_1, x_2, x_1 - 100, x_1 - 80, x_2 - 100, x_2 - 80, 400 - 2x_1 + x_2, x_1 - 2x_2\}.$$

以此类推, 构造P'的精化多项式集, 即P的二次精化多项式集.

5 矩形动态近似(Rectangular dynamics approximation)

模态l经划分之后, phase-portrait近似的第2步骤是为每个子模态(l, Ψ_i^l)构造近似线性初始集、不变集、不安全集及矩形向量场. 分段仿射混合自动机的初始集、不变集和不安全集已是线性谓词公式, 因此重点考虑矩形向量场的构造.

矩形向量场的构造是用矩形动态来外近似仿射动态. 仿射自动机H模态l的仿射向量场为

$$\bigwedge_{x_i \in X} \dot{x}_i = t_{x_i} = a_0 + \sum_{x_j \in X} a_j x_j,$$

其中$a_j \in \mathbb{Q}(1 \leqslant j \leqslant n)$. 利用微分包含确定子模态$(l, \Psi_i^l)$的矩形向量场$R_{\mathrm{flow}}(l, \Psi_i^l)$为

$$\bigwedge_{x_i \in X} \dot{x}_i \in I_{x_i} = [l_{x_i}, r_{x_i}].$$

I_{x_i}是$\{[\![t_{x_i}]\!]_{\boldsymbol{x}} | \boldsymbol{x} \in [\![\mathrm{Inv}(l, \Psi_i^l)]\!]\}$的紧致包含. I_{x_i}的求解是一个线性规划问题, 右端点r_{x_i}的求解可表述为

$$\max\ \dot{x}_i = a_0 + \sum_{x_j \in X} a_j x_j,$$
$$\text{s.t. } \boldsymbol{x} \in [\![\mathrm{Inv}(l, \Psi_i^l)]\!].$$

左端点l_{x_i}的求解同理.

综上所述, 给出了多项式模态划分函数$\Psi: L \to 2^{\mathbb{R}^n}$的映射方式, $R_{\mathrm{flow}}(l)$及迁移tran的求解. 结合这些具体过程给出矩形phase-portrait近似的具体实现如下:

给定分段仿射自动机$H = (L, X, \mathrm{Lab}, E, \mathrm{Init}, \mathrm{Inv}, \mathrm{Flow}, J, U)$及其多项式覆盖函数$\Psi$: $L \to 2^{\mathbb{R}^n}$, 构造H的phase-portrait线性自动机$H' = (L', X', \mathrm{Lab}', E', \mathrm{Init}', \mathrm{Inv}', \mathrm{Flow}', J', U')$使其满足:

· $L' = \{(l, \varphi) | l \in L, \varphi \in \Psi(l)\}$.
· $X' = X$.
· $\mathrm{Lab}' = \mathrm{Lab}$.
· $E' = E_1 \cup E_2$,

其中:

$$E_1=\{((l,\varphi),\sigma,(l',\varphi'))|((l,\varphi),(l',\varphi'))\in \text{tran}\wedge(l,\sigma,l')\in E\};$$

$$E_2=\{((l,\varphi),\tau,(l',\varphi'))|((l,\varphi),(l',\varphi'))\in \text{tran}\wedge l\in L\}.$$

· $\forall(l,\varphi)\in L',\text{Init}'(l,\varphi)=\text{Init}(l)\wedge\varphi$.

· $\forall(l,\varphi)\in L',\text{Inv}'(l,\varphi)=\text{Inv}(l)\wedge\varphi$.

· $\forall(l,\varphi)\in L',\text{Flow}'=R_{\text{flow}}(l,\varphi)$.

· $\forall e\in E_1,J'((l,\varphi),\sigma,(l',\varphi'))=J(l,\sigma,l')$;

$\forall e\in E_1,J'((l,\varphi),\tau,(l',\varphi'))=\text{stable}(X)$, 其中stable$(X)$表示$X'=X$.

· $\forall(l,\varphi)\in L',U'(l,\varphi)=U(l,\varphi)\wedge\varphi$.

由H'的构造过程, 显然可得出下述结论:

定理 2 混合线性自动机H'弱时间模拟混合自动机H, 即$H\preceq_{wT}H'$.

混合自动机H'是依据多项式模态划分函数Ψ而实现的, 假定Ψ的划分多项式集为P', 精化P'得P'', 依据P''构造H的 phase-portrait 近似H'', 有下述定理:

定理 3 $H\preceq_{wT}H''\preceq_{wT}H'$.

证 由定理2显然有$H\preceq_{wT}H',H\preceq_{wT}H''$. 又由于$H''$的划分多项式集$P''$是$H'$的划分多项集$P'$的精化, 即有$P'\subseteq P''$成立, 因此$H''\preceq_{wT}H'$, 即$H''$是$H$的精化模型. 证毕.

例 5 在例1中的仿射自动机H, 综合例2,3的多项式集P_1,P_2, 构造模态l_1的划分多项式集P为

$$P=P_1\cup P_2=\{x_1,x_2,400-2x_1+x_2,x_1-2x_2,x_1-100,x_1-80,x_2-100,x_2-80\},$$

多项式集P将模态l_1的状态空间划分为6个区域, 如图2所示. 在每个区域中的矩形向量场分别为

$$(l_1,\psi_1):\dot{x}_1\in\left[\frac{8}{5},\frac{5}{2}\right],\ \dot{x}_2\in\left[-1,-\frac{2}{5}\right],$$

$$(l_1,\psi_2):\dot{x}_1\in\left[\frac{7}{5},\frac{17}{10}\right],\ \dot{x}_2\in\left[-\frac{3}{5},-\frac{3}{10}\right],$$

$$(l_1,\psi_3):\dot{x}_1\in\left[\frac{7}{5},\frac{8}{5}\right],\ \dot{x}_2\in\left[-\frac{4}{5},0\right],$$

$$(l_1,\psi_4):\dot{x}_1\in\left[\frac{5}{4},\frac{8}{5}\right],\ \dot{x}_2\in\left[-\frac{2}{5},0\right],$$

$$(l_1,\psi_5):\dot{x}_1\in\left[\frac{8}{5},2\right],\ \dot{x}_2\in\left[0,\frac{2}{5}\right],$$

$$(l_1,\psi_6):\dot{x}_1\in\left[\frac{7}{5},1\right],\ \dot{x}_2\in\left[0,\frac{1}{2}\right].$$

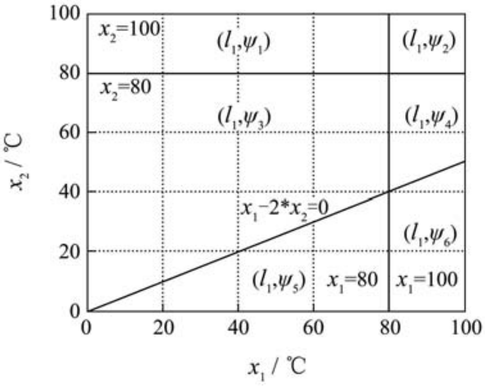

图 2 模态l_1的划分区域图

Fig. 2 Partition of the mode l_1

子模态间的迁移关系及模态的矩形phase-portrait近似如图3所示.

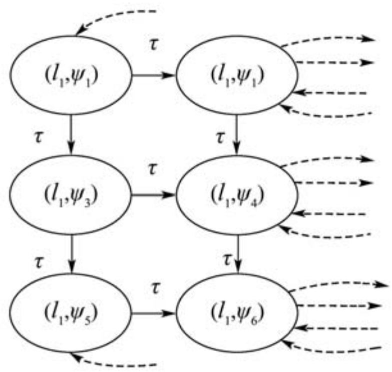

图 3 模态l_1的矩形phase-portrait近似

Fig. 3 Rectangular phase-portrait approximation of the mode l_1

6 实现及实例(Implementation and example)

本文所叙述的验证算法是基于验证工具PHAVer[9]实现的. PHAVer实现了线性phase-portrait近似, 所采用的划分策略是依据用户所指定的划分方向进行均匀矩形划分, 而本文依据系统的动态特性进行划分. 算法的实现简述如下:

验证的过程按照模型抽象–验证–模型精化的方式迭代循环, 用户可以通过变量$partnumber$来设定依据定性推理划分的迭代层数, 即划分多项式集可精化的深度. 初始模态划分多项式集P选用模态连续变量的零阶导数及感兴趣多项式(即不变集, 不安全集, 迁移条件集等). 当模型精化调整的迭代次数不大于用户设定值$partnumber$时, 采用定性推理多项式划分, 否则采用PHAVer的矩形划分. 特别地, $partnumber$为零时, 表示直接使用PHAVer进行矩形划分验证.

将本文所叙述的验证算法应用于文献[10]的基准验证实验中, 实验简述如下: 一个物体在具有$N \times M$栅格的平台上运行, 物体的期望速度控制$\boldsymbol{v}_{\rm d}(i) = (\sin(i\pi/4), \cos(i\pi/4))$随物体所处的单元格而发生变化. 设物体在单元格内具有相同的$\boldsymbol{v}_{\rm d}$. 使用映射矩阵M赋予每个单元格一个整数$i \in \{1, \cdots, 7\}$或特殊符号$\{A, B\}$, 符号A表示目标区域, B表示禁止区域. 设$N = M = 3$, 系统的动态方程为

$$\begin{pmatrix} \dot{\boldsymbol{x}} \\ \dot{\boldsymbol{v}} \end{pmatrix} = \begin{pmatrix} 0 & I \\ 0 & A \end{pmatrix} \begin{pmatrix} \boldsymbol{x} \\ \boldsymbol{v} \end{pmatrix} - \begin{pmatrix} 0 \\ A \end{pmatrix} \begin{pmatrix} 0 \\ \boldsymbol{v}_{\rm d}(i) \end{pmatrix}.$$

其中

$$A = \begin{pmatrix} -1.2 & 0.1 \\ 0.1 & -1.2 \end{pmatrix}.$$

物体的初始位置为$\boldsymbol{x}_0 \in [2, 3] \times [1, 2]$, 初始速度为$\boldsymbol{v}_0 \in [-0.3, 0.3] \times [-0.3, 0.3]$. 验证在有如下的速度映射矩阵时物体不会驶入禁止区域.

$$M = \begin{pmatrix} B & 2 & 4 \\ 2 & 3 & 4 \\ 2 & 4 & A \end{pmatrix}.$$

实验结果如表1所示, 其实验环境为: AMD 1.4 GHz, 512 MB RAM和Linux操作系统平台. 表1比较了当$partnumber$分别取0,2,3,4,5时, 为验证系统是安全的所需的内存、时间及所划分的多面体个数. 当$partnumber$为0时, 表示使用矩形划分的phase-portrait近似验证. 从实验结果可以看出, 当$partnumber$取值为4时, 取得最佳效果, 相比$partnumber$为0时, 验证所需划分的多面体个数减少了1060, 验证时间减少了78.24%. 因此, 与矩形划分相比较, 使用定性推理划分的验证明显地减少了模态空间划分的数目, 较大地提高了验证的效率.

表 1 实验结果

Table 1 Results of the experiment

$partnumber$	内存/MB	t/s	划分多面体/个
0	89767	67.13	1406
2	37452	28.87	524
3	21910	18.79	402
4	22340	14.61	346
5	22352	16.04	353

7 结论(Conclusion)

模态空间划分是 phase-portrait 近似的关键步骤. 本文提出了定性推理的划分策略, 根据系统的动态特性来指导模态空间的划分. 经实验表明, 基于定性推理的矩形phase-portrait近似验证显著地减少了模态空间的划分数目, 较大地提高了验证的效率. 本文的研究对象是仿射混合自动机, 然而在本文中所阐述的方法同样可适用于多项式混合自动机[11].

参考文献(References):

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

[2] HENZINGER T A, KOPKE P W, PURI A, et al. What's decidable about hybrid automata[C] //*Proceedings of the 27th Annual Symposium on Theory of Computing*. New York: ACM Press, 1995: 373 – 382.

[3] TIMARI A, KHANNA G. Series of abstractions for hybrid automata[C] //*Hybrid Systems: Computation and Control*. LNCS 2289, Berlin: Spring-Verlag, 2002: 465 – 478.

[4] ALUR R, DANG T, IVANCIC F. Counter-example guided predicate abstraction of hybrid systems[C] //*Ninth International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS)*. LNCS 2619, Berlin: Springer-Verlag, 2003: 208 – 223.

[5] HENZINGER T A, HO P H, WONG-TOI H. Algorithmic analysis of nonlinear hybrid systems[J]. *IEEE Transactions on Automatic Control*, 1998, 43(4): 540 – 554.

[6] DOYEN L, HENZINGER T A. Automatic rectangular refinement of affine hybrid systems[C] //*Formal Modeling and Analysis of Timed Systems(FORMATS)*. LNCS 3829, Berlin: Spring-Verlag, 2005: 144 – 161.

[7] HENZINGER T A, HO P H, WONG-TOI H. HyTech: A model checker for hybrid systems[J]. *International Journal on Software Tools for Technology Transfer*, 1997, 1(1/2): 110 – 122.

[8] 韩茂安, 顾圣士. 非线性系统的理论和方法[M]. 北京: 科学出版社, 2001.

[9] FREHSE G. PHAVer: Algorithmic verificatin of hybrid systems past HyTech[C] //*Hybrid Systems: Computation and Control*. LNCS 3414, Berlin: Spring-Verlag, 2005: 258 – 273.

[10] FEHNKER A, IVANCIC F. Benchmarks for hybrid systems verification[C] //*Hybrid Systems: Computation and Control*. LNCS 2293, Berlin: Spring-Verlag, 2004: 326 – 341.

[11] 刘保罗, 裴海龙. 混合自动机的多项式phase-portrait近似[J]. 计算机科学, 2008, 35(5): 180 – 183.

作者简介:

刘保罗 (1976—), 女, 博士研究生, 研究方向为形式化验证、离散系统控制, E-mail: ieliubl@163.com;

裴海龙 (1958—), 男, 教授, 博士生导师, 长期从事嵌入式系统分析与应用、智能机器人系统等的研究, E-mail: auhlpei@scut.edu.cn.