定性推理在矩形 phase-portrait 近似中的应用*)

刘保罗　裴海龙　李坚强

(华南理工大学自动化科学与工程学院　广州 510640)

摘　要　抽象近似是验证混合系统安全性的主要方法，矩形 phase-portrait 近似是通过构造简单的线性混合自动机来近似原混合自动机。phase-portrait 近似的关键步骤是如何划分状态空间。本文采用定性推理的方法，叙述了如何根据系统动态特征来划分状态空间及如何精化抽象模型。

关键词　混合自动机，phase-portrait 近似，李导数

Application of Qualitative Reasoning in Rectangular Phase-portrait Approximation

LIU Bao-luo　PEI Hai-long　LI Jian-qiang

(College of Automation Science and Engineering, South China University of Technology, Guangzhou 510640, China)

Abstract　Abstraction is a dominant approach for verification of hybrid systems; rectangular phase-portrait approximation is to construct simpler linear hybrid automaton to over-approximate the original automaton. The key procedure of phase-portrait approximation is the decomposition of the control model. In this paper, we adopt qualitative reasoning method to show how to partition the state space with respect to the dynamical property and how to refine the abstract model.

Keywords　Hybrid automaton, Phase-portrait approximation, Lie-derivative

1　引言

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，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及离散动态，安全性验证的可判定性仅限于一些简单混合系统，如时间自动机、矩形自动机等。对于大多数混合系统，安全性问题是不可判定的[1]。基于这个问题，研究者提出了许多种方法，旨在寻找验证安全性的充分条件。T. A. Henzinger 提出 phase-portrait 近似概念，这种方法是利用抽象的方法将复杂的混合动态模型转化为简单的可计算自动机模型，如线性自动机(LHA)。

phase-portrait 近似的关键是控制模态空间的划分，它直接影响着近似自动机模拟原系统的程度。虽然文献[4]中给出了 phase-portrait 近似的完备性，但盲目的划分可能由于抽象模型的精化而引起模态数目的剧增，因此，如何划分是运用这种方法的关键。本文基于这种考虑，采用定性推理[2]的方法，叙述了一种基于动态特性的模态空间划分方法。本文所考虑的对象为分段仿射混合系统。

2　基本术语

假定 $X=\{x_1,\cdots,x_n\}$ 是有限变量集，X 上的线性项定义为表达式 $y\equiv a_i+\Sigma_{x_i\in X}a_ix_i$，其中 $a_i\in\mathbb{Q}$。线性项集合表示为 $LTerm(X)$。线性约束为公式 $y\sim 0$，其中 $y\in Lterm(X)$，$\sim\in\{\leqslant,\geqslant,=,<,>\}$。线性谓词定义为线性约束的合取。$X$ 上的线性谓词集表示为 $Lin(X)$。实数域上的闭区间 I 定义为公式 $l_I\leqslant x\leqslant r_I$，其中 $l_I\in\mathbb{R}$，$r_I\in\mathbb{R}$ 分别称为区间的左端点和右端点。X 上的矩形谓词定义为公式 $\wedge_{x_i\in X}x_i\in I_{x_i}$，其中 $I_{x_i}(x_i\in X)$ 是实数域上的闭区间。X 上的矩形谓词公式集表示为 $Rect(X)$。X 的仿射动态定义为：$\wedge_{x_i\in X}\dot{x}_i=t_{x_i}$，其中 $t_x\in LTerm(X)$ 是 X 上的线性项，$\dot{x}_i$ 是一阶导数。仿射动态谓词集表示为 $Affine(X,\dot{X})$。矩形动态谓词 $Rect(\dot{X})$)。给定谓词公式 P，$[\![p]\!]$表示使 P 为真的点的集合。

3　分段仿射混合自动机的线性 phase-portrait 近似

3.1　分段仿射混合自动机

定义 1(分段仿射混合自动机)　分段仿射混合自动机是元组 $H=(L,X,Lab,E,Init,Inv,Flow,J,U)$ 其中：

L 是离散位置的集合，离散位置又称为控制模态。

$X=\{x_1,\cdots,x_n\}$ 是连续变量。

Lab 标签集，包括静默迁移标签 τ。

$E\subseteq L\times Lab\times L$ 是离散迁移关系。

$Init:L\rightarrow Lin(X)$ 是初始条件。

$Inv:L\rightarrow Lin(X)$ 赋予每个离散位置不变集。

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

$J:E\rightarrow Lin(X,X')$ 是迁移条件。X' 表示迁移后的变量值。

$U:L\rightarrow Lin(X)$，最终状态，表示不安全集。

混合自动机的离散位置代表离散的控制模态，在每个模态中的动态由仿射向量场、不变集来控制约束，模态间的切换由迁移条件给定，因此混合系统的运行由一个或多个与离散跳转相交替的连续运行轨迹组成，由初始状态出发按照动态运行直至到达，按照关系进行复位离散跳转到 l'，然后在 l' 中按照上述方式继续进行。混合自动机的可达集定义为由初始

*)本文受国家自然科学基金(60374036)(60574004)，广东省自然科学基金(031407)项目资助。刘保罗　博士生，研究方向为混合系统安全性验证；裴海龙　教授，博士生导师，研究方向为混合系统分析与综合。

状态出发的运行轨迹所经历的状态点的集合，表示为 Reach($[\![H]\!]$)$\subseteq L\times\mathbb{R}^n$。混合自动机 H 称为是安全的，如果在 H 中不存在从初始状态$(l_0,x_0)\in[\![Init]\!]$到不安全状态$(l_f,x_f)\in[\![U]\!]$的轨迹，即 Reach($[\![H]\!]$)$\cap Q_f=\emptyset$。

例 1　考虑一个温控加热器，其建模自动机如图 1 所示，其中变量 x 表示温度。自动机有两个控制模态，位置 on 表示温控加热器开始加热，其连续动态为 $\dot{x}=5-0.1x$，位置 off 表示温控加热器停止加热，其动态方程为 $\dot{x}=-0.1x$。初始状态为(off,x=20)，当 $x<19$ 时，加热器启动；当 $x>21$ 时，加热器停止。

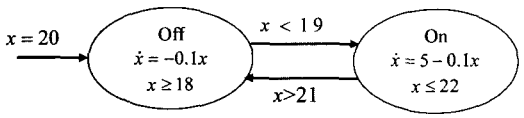


图 1　温控加热器建模混合自动机

3.2　线性 phase-portrait 近似

混合自动机的 Hphase-portrait 近似就是针对每个离散控制模态 l，寻找合适的状态空间划分 $\psi(l)=\{\psi_1^l,\cdots,\psi_k^l\}$，然后在每个区域$(l,\psi_i^l)$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，构造线性自动机 H'，使得 Reach($[\![H]\!]$)$\subseteq$Reach($[\![H']\!]$)。其形式化定义如下：

定义 2(线性 phase-portrait 近似)　给定仿射自动机 $H=(L,X,Lab,E,Init,Inv,Flow,J,U)$ 及其状态划分函数 $\psi:L\to 2^{\mathbb{R}^n}$，构造 H 的 phase-portrait 线性自动机 $H'=(L',X',Lab',E',Init',Inv',Flow',J',U')$，使其满足：

(a)$L'=\{(l,\varphi)\mid l\in L,\varphi\in\psi(l)\}$。

(b)$X'=X$。

(c)$Lab'=Lab$。

(d)$E'=E_1\cup E_2$，其中 $E_1=\{((l,\varphi),\sigma,(l',\varphi'))\mid\varphi\in\psi(l)\wedge\varphi'\in\psi(l')\wedge(l,\sigma,l')\in E\}$。$E_2=\{((l,\varphi),\tau,(l,\varphi'))\mid\varphi,\varphi'\in\psi(l)\wedge l\in L\}$。

(e)$\forall(l,\varphi)\in L'.\ Init'(l,\varphi)=Init(l)\wedge\varphi$。

(f)$\forall(l,\varphi)\in L'.\ Inv'(l,\varphi)=Inv(l)\wedge\varphi$。

(g)$\forall(l,\varphi)\in L'$，$Flow'(l,\varphi)=Rflow(l,\varphi)$。

(h)$\forall e\in E_1$，$J'((l,\varphi),\sigma,(l',\varphi'))=J(l,\sigma,l')$，$\forall e\in E_2$，$J'((l,\varphi),\tau,(l,\varphi'))=stable(X)$。$stable(x)$表示 $x=x'$。

(i)$\forall(l,\varphi)\in L'$，$U'(l,\varphi)=U(l)\wedge\varphi$。

其中 $Rflow(l,\varphi)$是利用微分包含来近似仿射动态。给定仿射自动机 H 模态 l 的仿射向量场 $Flow(l)$，则子模态(l,φ)的 $Rflow(l,\varphi)\in$Rect(X)定义为

$$Rflow(l,\varphi)=[\min_{x\in Inv(l,\varphi)}Flow(l),\ \max_{x\in Inv(l,\varphi)}Flow(l)]$$

对于仿射自动机 H，模态 l 的仿射向量场可表示为 $\dot{x}_i=a_0+\sum_i a_i x_i$，$a_i\in\mathbb{Q}$ $(0\leqslant i\leqslant n)$，不变集 $Inv(l)\in Lin(X)$，因此矩形向量场 $Rflow(l,\varphi)$的求解是一个线性规划问题，$Rflow(l,\varphi)$的右端点可表述为：

maximize $\dot{x}_i=a_0+\sum_i a_i x_i$，$a_i\in\mathbb{Q}$ $(0\leqslant i\leqslant n)$

subject to $Inv(l)$

$Rflow(l,\varphi)$左端点的求解与此类似。

定理 1　按照上述步骤所构造的线性自动机 H'是仿射自动机 H 的近似，且如果 H'是安全的，则 H 也是安全的。

混合自动机 H'是 H 的外近似，这种关系记为 $H\leq H'$。基于线性 phase-portrait 近似的验证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进行验证的过程，其步骤如图 2 所示：首先构造原系统 H 的 phase-portrait 线性自动机 H'，然后利用已有的工具(如 Hytech)验证 H'。如果 H'是安全的，则 H 也是安全的。如果 H'是不安全的，不能依此推断出 H 的安全性，H'模型进一步调整得模型 H''，然后再验证 H''。整个过程按照模型抽象-验证-再做模型抽象的方式迭代循环，直至得出验证结论，或者迭代的次数超于用户给定的阈值，系统退出。

因此，如何进行合适的状态空间划分，使得矩形动态较好地近似仿射动态，是 phase-portrait 自动机近似的关键，在下文中使用定性推理来指导状态空间的划分。

```
H′=appLHA( ); //构造 H 的 phase-portrait LHA: H′
repeat do
  verify(H′);
  if(H′是安全的) do
    printf("H′是安全的");
    return;
  else
    H′=refine(B′);
  endif
until(精化验证次数不大于用户给定值)
```

图 2　线性 phase-portrait 近似验证过程

4　基于定性推理的状态空间划分

划分状态空间实质上是寻找以满足某种特定性质的等价类求取熵空间的过程。考虑混合自动机 H，如果模态 l 存在着一个等价类集 $\psi(l)=\{\psi_1^l,\cdots,\psi_k^l\}$，$\psi(l)$是状态空间 $S=(l,inv(l))$的一个划分，模态 l 基于 $\psi(l)$的熵空间为 $S/\lambda(l)$。由文献[1]可知，在混合自动机可达性运算中由多项式定义的集合是可计算的，因此考虑等价类由多项式来表示。因此模态空间划分就是针对每一个控制模态 l，寻找合适的多项式集 P，使其构成模态 l 的一个划分等价类集：$\psi(l)=\{\psi_1^l,\cdots,\psi_k^l\}$，其中$[\![\psi_i^l]\!]=\{x\in X\mid\wedge_{\alpha\in m_1}p_\alpha(x)\geqslant 0\wedge\wedge_{\beta\in m_2}p_\beta(x)\leqslant 0\wedge Inv(l)\}$，$i=1,2,\cdots,k$，这里 $m_1\cup m_2$ 是集合$\{1,2,\cdots,|P|\}$的划分。

因此，如何进行合适的状态空间划分，就是如何寻找合适的模态划分多项式。在下文依据定性推理的方法选用恰当的多项式集。

4.1　基于向量场特性划分状态空间

线性 phase-portrait 近似用微分包含的方法将区域内所有点的动态都统一为矩形动态，因此考虑将具有相似动态特性的状态进行划分。

给定仿射混合自动机 H，其模态 l 的仿射向量场为 $\dot{x}_i=t_i$，$t_i\in Lterm(x)$，$(i=1,\cdots,n)$，选用向量 X 的一阶，二阶…K 阶导数做划分多项式。易知，一阶导数描述了变量变化的单调性，二阶导数描述了凸性，等等。因此，导数多项式定性地刻画了轨迹的动态特性，且高阶导数多项式所决定的划分是低阶导数的精化，即高阶导数多项式比低阶导数多项式保证了更精确的定性性质。

4.2　基于感兴趣多项式及其李导数划分状态空间

定义 3(李导数)　给定仿射自动机 H，其模态 l 的向量场为 $Flow(l)$，多项式 p 关于 $Flow(l)$的李导数定义为

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

多项式 p 的李导数刻画了动态轨迹关于多项式 p 的变化方向。给定多项式及李导数的符号，可以推断出系统向量场流的方向，因此可以选用感兴趣的多项式集 p_i $(i=1,\cdots,k)$，以$\{p_i,L_{Flow}(p_i)\}$做空间划分多项式，在划分后的每个区

域内，每个多项式的符号及其李导数的变化方向保持不变。每个区域内的流针对多项式 $p_i(i=1,\cdots,k)$具有相同的流向。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。

4.3 精化多项式

基于 phase-portrait 近似所构造的模型是原系统的外近似。因此，如果抽象模型经验证不满足安全性要求，不能推理出原系统的安全性，抽象模型需要作进一步的精化。假设仿射自动机 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 $p_i\in P_i$ 求其关于 $Flow(l)$的李导数 $L_{Flow(l)}(p_i)$多项式。如果 $L_{Flow(l)}(p_i)$不是常数而且与集合 P_l 中的所有多项式不存在常数倍关系，则将 $L_{Flow(l)}(p_i)$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'。由上节易知，基于 P_l'划分所得的 $H_{P'}$ 满足 $H\leq H_{P'}\leq H_P$[2]，其中 H_P 是 H 基于 P_l，$(l\in L)$的 phase-portrait 近似。P_l'称为 P_l 的精化多项式集。

例 2　考虑例 1 所示的混合自动机，按本节所述的方法选定模态 on 的初始多项式集为 $P_{on}\equiv\{x,x-22,x-19,x-18\}$。对 P_{on}中的每个多项式求导，构造精化多项式集为 $P_{on}'\equiv\{x,x-22,x-19,x-18,0.1x-5\}$。依此类推，可以求得 P_{on}'的精化多项式为 $P_{on}''\equiv\{x,x-22,x-19,x-18,0.1x-5,0.01x+4.5\}$。

5 实现算法及实例

本文所述的验证算法是基于 PHAVer[3] 实现的，PHAVer 实现了线性混合自动机的精确验证。对于仿射自动机，PHAVer 使用 phase-portrait 近似将分段仿射自动机近似为线性自动机，它的划分策略是由用户指定划分平面的方向来进行矩形划分。而本文是基于系统的动态特性进行划分，其主要实现代码如图 3 所示，其中函数 get_split_constraints 构造划分多项式集，在初次调用时参数 cons 为空。get_split_constraints 选定各变量的零阶导数及感兴趣多项式作为初始多项式集。当 cons 不为空时，则按上节的方法精化多项式集。reachint(H,U)判断自动机 H 的不安全集 U 是否可由初始状态可达。rectangularflow(H)求解 H 的矩形动态近似。Itercount 表示迭代次数，如果 Itercount 不大于用户设定值 partnumber 时，则采用基于定性推理的多项式划分，否则继续采用 PHAVer 的方法进行矩形划分。

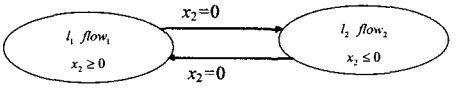
```
while itercount <= partnumber do
  constraints=get_split_constraints(H,cons);
  cons'= unin(cons,constraints);
  if ! equal(cons',cons) do
    cons =cons';
  else break;
  endif
  for each loc∈locations(H) do
    H'=split_location(loc,constraints);
  endfor
  rectangularflow(H');
  if ! ( reachinit(H',U')) do
    printf("His safe");
    return;
  endif
  itercount = itercount+1;
endwhile
```

图 3　基于定性推理划分验证的主要代码实现

例 3　设一个具有不确定参数的连续动态系统，其动态方程为

$$\begin{pmatrix}\dot{x}_1\\ \dot{x}_2\end{pmatrix}=\begin{pmatrix}-4 & a\\ 6 & -4\end{pmatrix}\begin{pmatrix}x_1\\ x_2\end{pmatrix}$$

其中参数 a 的变化范围为 $1.9\leqslant a\leqslant 2.1$。如果假定初始状态为 $0.7\leqslant x_1\leqslant 1\wedge 0.2\leqslant x_2\leqslant 0.25$，不安全集为 $x_2\geqslant 0.81$，求解系统的安全性。这种带有参数的连续系统验证问题可以转换为混合自动机的验证，其混合自动机模型如图 4 所示。利用图 3 算法进行验证的实验结果如表 1 所示，其中 partnumber 设定不同的定性迭代次数。当 partnumber 为零时，表示直接使用 PHAVer 进行验证。从实验结果可以看出，基于定性推理的划分较大地提高了验证的效率。



$$flow_1\equiv -4x_1+1.9x_2\leqslant\dot{x}_1\leqslant -4x_1+2.1x_2\wedge\dot{x}_2=6x_1-4x_2$$

$$flow_2\equiv -4x_1+2.1x_2\leqslant\dot{x}_1\leqslant -4x_1+1.9x_2\wedge\dot{x}_2=6x_1-4x_2$$

图 4　具有不确定参数连续动态的混合自动模型

表 1　实验结果

Partnumber	内存(KB)	时间(秒)	划分多面体(个)
0	56676	96.61	988
2	11640	9.53	254
3	12720	6.46	145
4	12728	6.8	151

结束语　矩形 phase-portrait 近似是通过构造简单的线性混合自动机来模拟原混合自动机，其关键步骤是如何划分模态。本文采用定性推理的方法，叙述了如何根据系统动态特征来划分状态空间，并给出了实现算法。经实验表明，基于定性推理的划分验证可以较好地提高验证效率。

参 考 文 献

[1] Alur R, Henzinger T A. Discrete Abstractions of Hybrid Systems. Proceedings of the IEEE, 2000, 88(7): 971-984

[2] Tiwari A, Khanna G. Series of abstractions for hybrid automata // HSCC, LNCS. 2002, 2289: 465-478

[3] Frehse G. PHAVer: Algorithmic Verification of Hybrid Systems past HyTech // HSCC, LNCS. 2005, 3414: 258-273

[4] Henzinger P, Ho H, Wong-Toi H. Algorithmic analysis of nonlinear hybrid systems. IEEE Transactions on Automatic Control, 1998, 43: 540-554

[5] Doyen L, Henzinger T A. Automatic Rectangular Refinement of Affine Hybrid Systems // FORMATS, LNCS. 2005, 3829: 144-161