计算机科学 1998 Vol. 25№. 2

混合系统的分析

Analysis of Hybrid Systems

侯建民　李宣东　樊晓聪　郑国梁

（南京大学计算机科学系　南京 210093）

摘　要　The paper first provides the definition of hybrid system. It then defines syntax structure of hybrid automaton in detail and fully analyses the automaton that is a model of the hybrid system. Thirdly, It introduces some verification problems of hybrid automaton and transformation algorithms to timed automaton. At last, it gives some future research directions for hybrid automaton.

关键词　Hybrid system, Hybrid automaton, Linear, Verification, Bisimulation

在人们日常生活中，混合系统（Hybrid System）应用的实例很多，如汽车中的计算机控制系统、飞机中的平稳飞行控制系统等都属于混合系统的范畴，并且随着计算机技术的发展，混合系统的应用范围会更加广泛，人们的生活会更加依赖于混合系统，因此社会应用的需求要求研究人员对混合系统进行比较深入的研究，保证混合系统运行的正确性。

什么是混合系统呢？不同的人有着不完全一致的看法。Grossman 等认为混合系统是数字设备与连续设备的交互网络[1]，Manna 等认为混合系统是将离散部件和连续部件融合在一起的反应系统[2]，Alur 等认为混合系统是由模拟环境中的离散程序组成的[3]。在上述不同的定义中，相同的一点是混合系统都涉及到了离散系统和连续系统（模拟系统），我们认为比较贴切的定义是，混合系统是运行于物理环境中的数字系统。事实上，混合系统是介于控制论和计算机科学之间的研究对象，因为控制论研究的对象大多是连续变化系统，而计算机科学的研究对象大多是离散系统。

大多数混合系统都涉及到实时控制，因此人们常常采用混合自动机作为这类混合系统的模型。混合自动机是由有限节点及节点上的离散变量和连续变量组成的，离散变量在混合自动机发生节点变更的状态转换时更新，节点内的连续变量随着时间推移按照系统要求的微分方程连续变化。各节点中的微分方程是由系统在该节点的状态及系统需求确定的。通过对混合系统模型—混合自动机—的深入分析和研究，就可以全面、细致地理解混合系统的性能。

1　混合自动机的定义

1.1　定义

混合自动机是一个五元组$\langle S, S_0, X, E, \Phi\rangle$，其中：

· S 是有限节点的集合，用 s、s′ 等表示节点。$S_0 \subseteq S$，是初始节点的集合。

· X 是有限变量的集合，其中包含连续变量和离散变量，统称状态变量。各状态变量取值均为实数，即对任意的 $x \in X$，都有 $x \in R$。节点 s 上某变量 x 的取值用 $x_s(t)$ 表示，t 表示混合自动机从进入节点 s 开始且一直保持在节点 s 直到当前时刻的时间间隔，$X_s(t)$ 表示节点 s 上所有状态变量的取值。

· E 是有限边的集合。对于任意 $e \in E$，都有 $(s, \alpha_e, \Psi_e, \upsilon_e, s')$ 的形式，其中 s 是源节点，s′ 是目标节点，α_e 是 e 上的标号。Ψ_e 是状态转换使能条件，简称使能条件，又称警卫条件，一般由 X 中元素与常数的线性等式或线性不等式的布尔组合构成，表示形式为 $\Psi_e ::= x=k \mid x<u \mid v<x \mid \Psi 1_e \wedge \Psi 2_e \mid \Psi 1_e \vee \Psi 2_e$，k，u，v 都是常数。$\upsilon_e$ 是节点变更的状态转换发生时变量赋值函数，表示形式为 $x := \upsilon_e(x \in Y \subseteq X)$，是指当系统进入节点 s′ 时 X 的子集 Y 中所有变量都以新值作为初值，X\Y 中的变量仍以原值作为初值，即 $X[Y \rightarrow \upsilon_e(Y)]$。同时边 e 表示为 $e=(s, s')$。

· Φ 是每个节点 $s(s \in S)$ 上线性不变式 φ_s 的集

合。φ_s 表示在节点 s 上所有变量应满足的约束条件，φ_s 的表示形式为 $M_s(X_s)+N_s \leqslant L_s$，其中 M_s、N_s、L_s 都是只与节点 s 有关的常数矩阵。

节点 s 中变量 X_s 的变化规律(微分方程)反映了混合系统不同的变化特征。对于形如 $\dot{X}_s=f_s(X_s)$ 的微分方程，如果在混合自动机的任意节点 $s(s\in S)$ 中，上述微分方程都存在线性解，那么这类混合自动机称为线性混合自动机，否则称为非线性混合自动机。在线性混合自动机中，如果对于任意节点 $s(s\in S)$，都有 $f_s(X_s)=K_s \cdot X_s+C_s$ 的形式，K_s 取值为 $[A_s,B_s]$中的任一常数，A_s、B_s、C_s 是只与节点 s 有关的常数矩阵，并且 $A_s \leqslant B_s$(表示 A_s 的每一个元素都不大于 B_s 中对应的元素)，那么称这类线性混合自动机为常微分包含线性混合自动机(Constant Differential Inclusion Linear Hybrid Automaton)，又称为有界比率线性混合自动机(Bounded-rate Linear Hybrid Automaton)，K_s 称为比率；如果 $A_s=B_s$，那么称为常斜率线性混合自动机(Constant Slope Linear Hybrid Automaton)，如果所有节点上微分方程中数值不等的比率有 n 个，那么这类混合自动机又称作 n-rate 线性混合自动机。如果对任意的节点 s、$s'\in S$ 都有 $A_s=B_s=A_{s'}=B_{s'}=k\neq 0$ 成立时，我们称这类线性混合自动机为 k-时间图(k-timed Graph)。特别地，对任意的节点 $s(s\in S)$都有 $k=1$ 并且 $\upsilon_s=0$ 时，这类常斜率线性混合自动机就成为时间自动机。当 $K_s\in\{0,1\}$时，线性混合自动机成为积分自动机，积分自动机也是 2-rate 线性混合自动机的一种特例。如果线性混合自动机中的使能条件、约束条件和变量赋值函数都是简单的线性形式，如 $x<c$、$x>c$ 或 $x=c$ 等形式时，我们称这样的线性混合自动机为简单线性混合自动机。类似地，其它类型的线性混合自动机也都分别有简单的形式。

混合自动机的状态用二元关系 (s,X_s) 表示，X_s 反应了节点 s 上所有状态变量在某一时刻的取值情况。混合自动机状态变化有两种情况：一种是状态转换，另一种是随着时间推移节点上状态变量的更新。为叙述方便，将前一种变化称为转换步变化，将后一种变化称为时间步变化。

• 转换步变化：如果节点 s 的变量 X_s 在某一时刻满足 $\Psi_s(X_s)$的条件，并且有标号 a_s 发生，那么就会发生节点变更和状态变量变化的状态转换，即存在目标节点 s′ 使得 $(s,a_s,\Psi_s,\upsilon_s,s')\in E$。表示为：

$$\frac{(s,a_s,\Psi,\upsilon,s')\in E,\Psi_s(X_s),\upsilon_s(X_{s'})[Y\rightarrow\upsilon_s(Y)]=X_{s'}}{(s,X_s)\xrightarrow{a_s}(s',X_{s'})}$$

• 时间步变化：混合自动机的状态 (s,X_s) 随着时间的推移，在节点 s 上保持了 t_s 的时间长度，简称时段，节点 s 上的变量值由 $X_s(0)$变化到 $X_s(t_s)$，即仅仅是节点上状态变量发生了变化。设 $\dot{X}_s=f_s(X_s)$ 的解是 $F_s(t)$，且 $F_s(0)=X_s(0)$，那么有：

$$\frac{X_s(t)=F_s(t),\forall\, t,0\leqslant t\leqslant t_s,\varphi_s(F_s(t))}{(s,X_s(0))\xrightarrow{t}(s,X_s(t))}$$

混合自动机的一个数据迹是由非负时段 t_s 和微分方程 f_s 构成的，表示为 (t_s,f_s)的形式。对于任意 $t'_s\in[0,t_s]$，$F(t'_s)$都满足节点 s 上的线性不变式 φ_s 的要求。混合自动机的一条迹 τ，即混合自动机能够接受的语言，表示形式为：$(s_0,t_0,f_0)\rightarrow(s_1,t_1,f_1)\rightarrow\cdots\rightarrow(s_n,t_n,f_n)\rightarrow\cdots$，$t_i$ 表示混合自动机在节点 s_i 上的时段，并且在 (s_i,s_{i+1})之间都存在一个转换关系，即有 $(s_i,s_{i+1})\in E$。通过迹的计算，能够准确地判断混合自动机中有关节点上的时间性能。迹 τ 中的一个状态表示为 (s_i,t'_i)的形式，且 $0\leqslant t'_i\leqslant t_i$。迹 τ 中两个状态 (s_i,t'_i)、(s_j,t'_j)的排序关系定义为：如果 $i\leqslant j$ 或者 $i=j$ 且 $t'_i<t'_j$，那么 (s_i,t'_i)排在 (s_j,t'_j)的前面。混合自动机沿着迹 τ 到达状态 (s_i,t'_i)的时间长度是：$T(s_i,t'_i)=\sum_{0\leqslant j<i}t_j+t'_i$，迹 τ 上的无限时间长度是：$T_\tau=\sum_{0\leqslant j}t_j$，如果 $T_\tau=\infty$，那么我们称迹 τ 是发散的。

1.2 实例

图 1 就是一个混合系统—温控系统的混合自动

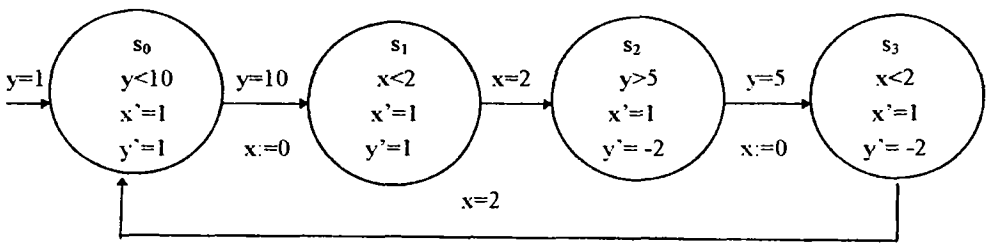

图 1

机模型[4]。该混合自动机是线性的，共有四个节点 s_0、s_1、s_2、s_3，两个变量 x、y。每个变量在各个节点内的微分方程以及各节点的线性不变式、各节点间状态转换的使能条件和变量赋值函数都如图中所示。在图 1 所示的混合自动机中，没有定义标号。

在图 1 的混合自动机中，x 表示时间，其变化率始终保持为 $x=1$，y 表示温度。初始时，$x=0$，$y=1$。进入 s_0 节点后，如果温度 $y<10$，那么温升速率是 1，即 $y=1$。当温度 $y=10$ 时，由 s_0 节点进入 s_1 节点，同时时间变量 x 清零。自动机在 s_1 节点内停留的最长时间小于 2 秒，温升速率仍然是 1。当时间变量 $x=2$ 时，自动机进入 s_2 节点，此时温度开始下降，下降的速率是 2。当温度降至 5 时，自动机进入 s_3 节点，同时时间变量 x 清零。自动机在 s_3 节点内停留的最长时间小于 2 秒，温降速率仍是 2。当时间变量 $x=2$ 时，自动机又进入 s_0 节点，重新开始升温。该混合自动机描述了一个温控系统试图将温度控制在[1,12]范围内的运行情况，因此对其验证的目标就是：该混合自动机的运行过程是否满足温控系统的规约，即在任意时刻是否都有 $y\in[1,12]$。

2 混合自动机的性质

2.1 判定性和不可判定性

对于给定的混合自动机 A，定义其 Muller 接受条件是 $F_A\subseteq 2^S$，A 的一条 Muller 接受迹 τ 首先是 A 的一条迹，并且有 $\tau_\infty\in F_A$，τ_∞ 表示在迹 τ 中无限多次出现的节点。Muller 空问题是指混合自动机 A 是否有一个 Muller 接受迹。因此，关于混合自动机的验证，有下面的定理。

定理：对于 2-rate 自动机和简单的积分自动机，Muller 空问题是不可判定的[5]。

事实上，对于简单的 n-rate 混合自动机(比率不等于零)而言，Muller 空问题是可判断的。这是由于简单的 n-rate 混合自动机可以通过比率的比例处理转化为时间自动机，而时间自动机的 Muller 空问题是 PSPACE 完全问题。

2.2 有关验证的几个问题

就一个自动机而言，通常意义下的安全性是指该自动机的迹不包含不好的状态，或者是不好的状态对于该自动机是不可达的。活性是指该自动机的迹包含好的状态无限多次。对混合自动机而言，安全性和活性问题是通过可达性和空问题来进行验证的。

混合自动机的可达性问题是验证安全性需求的基本问题，它是指对于给定的混合自动机及某节点，是否存在一条始于初始状态的迹可以到达该节点。如果该节点上的性能不满足系统安全性要求，那么设计出来的混合自动机的所有迹都应不包含该节点。混合自动机的空问题是验证活性需求的基本问题，它是指对于给定的混合自动机，是否存在一条始于初始状态的迹是发散的。如果满足活性要求的节点集合为 F_A，那么设计出来的混合自动机的所有迹应包含 F_A 中所有元素无限多次，故迹必是发散的。混合自动机的迹包含问题(trajectory inclusion problem)在验证混合自动机是否满足其规约时具有重要的作用，它是指当规约可以用一个混合自动机 A 表示并且实现模型也是另一个混合自动机 A′ 时，如果 A′ 的所有迹也都是 A 的迹，说明实现模型正确地实现了系统的规约。

由于混合自动机的种类较多，不便于分别进行分析、研究，于是人们提出了双模拟性(Bisimulation)的概念，凡是满足双模拟性的两个自动机(转换系统)都具有相同的性质。为描述方便，我们根据自动机的语义模型—转换系统—来定义双模拟性。

对于转换系统 $T_1=(S_1,\rightarrow_1)$，$T_2=(S_2,\rightarrow_2)$及其共同的标号集 L 和定义在 S_1,S_2 上的二元关系 $\rho\subseteq S_1\times S_2$，当 $\rho(s_1,s_2)$成立并且对任意的 $a\in L$，都有：

(1)如果 $s_1\xrightarrow{a}_1 s'_1$，那么存在 s'_2 使得 $s_2\xrightarrow{a}_2 s'_2$，并且有 $\rho(s_1',s_2')$成立；

(2)如果 $s_2\xrightarrow{a}_2 s_2'$，那么存在 s_1' 使得 $s_1\xrightarrow{a}_1 s_1'$，并且有 $\rho(s_1',s_2')$成立。

那么我们称 T_1、T_2 具有双模拟性。类似地，如果 T_1、T_2 都是混合自动机，并且满足上述性质时，我们亦称这两个混合自动机具有双模拟性。十分显然，双模拟性的两个混合自动机具有相同的性质，因此我们只要了解了比较简单混合自动机的性质，就可以推测出较复杂混合自动机的性能。

文[6]对时间自动机的性质及其判定性等许多问题进行了详尽的分析和介绍，使得时间自动机作为实时系统的一个基本模型，在系统设计、系统(或软件)验证和理论推导方面具有重要的作用和意义。

同时，一些混合自动机通过某些具体的变换可以转换成时间自动机的形式，即与时间自动机是双模拟的，这为分析混合自动机的性能提供了便利的条件。

对于简单的常微分包含线性混合自动机、简单的常斜率线性混合自动机以及简单的 k-时间图，通过对各节点中微分方程的比率进行比例处理(线性变换)，同时相应地修改节点上线性不变式、赋值函数和使能条件，那么这些混合自动机都可以逐步地转化到时间自动机[7,8]。另外，对于某一类的非线性混合自动机，通过采用 ε-近似变换方法以及比例变换方法，也可以逐步地转化到时间自动机的形式[9]。这些变换方法对于简化复杂的混合自动机、寻找可判定混合自动机的子集都具有十分显著的意义。

2.3 混合自动机的组合

当一个混合系统由多个并行运行的部件组成时，我们往往首先采用混合自动机作为混合系统各个部件的模型，然后再将这些混合自动机组合起来作为整个混合系统的模型。混合自动机之间通过共享变量或同步标号来保持协同。

设 $A_1=\langle S_1,S_{10},X_1,E_1,\Phi_1\rangle$、$A_2=\langle S_2,S_{20},X_2,E_2,\Phi_2\rangle$是两个混合自动机，其中 X_1,X_2 中变量的维数分别是 n_1 和 n_2。组合后的混合自动机定义为 $A=\langle S,S_0,X,E,\Phi\rangle$，其中 $S=S_1\times S_2$，$S_0=S_{10}\times S_{20}$，$X=X_1\cup X_2$，$\Phi=\Phi_1\wedge\Phi_2$。

对于 A 中每个节点 $(s_1,s_2)\in S_1\times S_2$，节点上的线性不变式为 $\phi_{(s1,s2)}=\phi_{s1}\wedge\phi_{s2}$，微分方程 $f_{(s1,s2)}=f_{s1}\wedge f_{s2}$。E 的元素 e 定义为 $e=((s_1,s_2),(s_1',s_2'))$当且仅当下面三种情况中有一种成立：如果 $s_1=s_1'$ 时，存在 $e_2=(s_2,s_2')\in E_2$ 并且 e_2 上标号 a_2 不是 A_1 的标号；如果 $s_2=s_2'$ 时，存在 $e_1=(s_1,s_1')\in E_1$ 并且 e_1 上标号 a_1 不是 A_2 的标号；如果 $e_1=(s_1,s_1')\in E_1$，$e_2=(s_2,s_2')\in E_2$ 并且 e_1,e_2 上标号相同，即 $a_1=a_2$。由于 X_1,X_2 之间可能存在共享变量，因此 X 的维数在 $\max(n_1,n_2)$ 和 n_1+n_2 之间。如果 A_1,A_2 标号集的合取为空，那么构成混合自动机 A 的两个混合自动机 A_1,A_2 的状态转换是交替进行的；如果 A_1,A_2 标号集的合取非空，那么公共的标号必须同步，使得两个混合自动机的状态同时变更。

3 研究方向

混合自动机作为实际工作中的一种重要模型，其实现结果直接影响到对实际混合系统的理解和设计。特别地，混合自动机的验证问题是保证实际混合系统正确实现的一种重要手段，因此一直是计算机界人士关注和研究的热点[3,5,10,11]。有关混合自动机验证比较成熟的工具主要有 SMC、UPPAAL、HyTech(Cornell)等，这些基本上都是由大学的研究机构完成的。当前，有关混合自动机的研究主要有以下几个方面：

(1)在嵌入混合系统的系统中对混合自动机的识别和快速生成，以及通过混合自动机对真实系统的有效模拟和仿真。

(2)寻找混合自动机中可判定的子集，为此往往需要在混合自动机上增加一些限制性条件。

(3)是否存在某一种验证方法，可以有效地解决某一类混合自动机的正确性问题。

(4)对可判定的混合自动机，寻找一种验证效率较高的算法，从而可以在较短的时间里完成验证工作。

参考文献

[1] Grossman R. L., Larson R. G., An algebraic approach to hybrid systems, Theoretical Computer Science, 138(1)1995

[2] Manna Z., Pnueli A., Verifying hybrid systems. LNCS 736, Springer-Verlag, 1993

[3] Alur R. et al., Hybrid automata: an algorithmic approach to the specification and verification of hybrid systems, Same to[2]

[4] Nicollin X. et al., From ATP to timed graphs and hybrid systems, LNCS 600, Springer-Verlag, 1992

[5] Henzinger T. A. et al., What's decidable about hybrid automata, Proc. of the 27th Annual Symposium on Theory of Computing, ACM Press, 1995

[6] Alur R. and Dill D. L., A theory of timed automata, Theoratical Computer Science, Vol. 126, 1994

[7] Olivero A. et al., Using abstractions for the verification of linear hybrid systems, Proc. of 6th Intl. Conf. on Computer Aided Verification(CAV'94), Springer-Verlag, 1994

[8] Puri A. and Varaiya P., Decidability of hybrid systems with rectangular differential inclusion, Same to [7]

[9] Henzinger T. A. and Ho P. H., Algorithmic analysis of nonlinear hybrid systems, Proc. of the 7th Intl. Conf. on Computer Aided Verification (CAV'95), Springer, 1995

[10] Alur R. et al., Automatic symbolic verification of embedded systems, Proc. of the 14th Annual Real-time System Symposium, IEEE Computer Society Press, 1993

[11] Nicollin X. et al., An approach to the description and analysis of hybrid systems, Same to[2]