Approximate Simulation for Algebraic Transition Systems

Ning Zhou[1,a,*], Jun Fu[2,b] and Xiao-gang Wang[1,c]

[1]School of Electronic and Information Engineering, Lanzhou Jiaotong University
Lanzhou, China

[2] Huawei Nanjing R&D center, Nanjing, China

[a]tomzhou@gmail.com, [b]jeff.fujun@huawei.com, [c]reswxg@mail.lzjtu.cn

*Corresponding author

Abstract. As the real-time systems and embedded systems are developing, behaviors of systems has become hybrid with the fusion of discrete and continuous components. Traditional labeled transition system could only describe discrete systems. In this paper, we proposed a new type of labeled transition system which called algebraic transition system. The algebraic transition system can describe behaviors of hybrid systems. On the algebraic transition system, an approximate simulation relation was defined, which is a better choice for reducing complexity and providing more robust relationships between systems.

Keywords: Metric, Algebraic Transition System, Simulation.

Introduction

Labeled transition systems are useful for giving semantics to programming programs characterized with discrete structures. As the development of real-time systems and embedded systems, behaviors of systems become hybrid with the fusion of discrete and continuous components [1]. Breugel [2, 3] generalized the theory for proving the equivalence of semantic models of programming languages by means of labeled transition systems with metric.

In our proposed algebraic transition system, we using the approximate method of polynomials: Taylor approximations [4]. When we build the metric of algebraic transition systems, we refer the theory of metric labeled transition systems [3]. In [5], the decision result on first-order arithmetic formulas was proposed. In model checking [6, 7], labeled transition system is used to describe the potential behavior of discrete systems, and we extend the labeled transition systems with polynomials, which can describe the behaviors of a kind of hybrid systems. For weighted transition systems, Larsen has proposed the approximate simulation relation [9].

Preliminaries

We start with some terminology and notion which we will use heavily. Let R be the set of real numbers, N be the set of naturals including the 0, and $\mathrm{R}_{\geq 0}$ be the set of non-negative reals. The cardinality of a set A is the number of elements in A and is denoted $|A|$.

Definition 1 (Metric space) A metric space is given by a nonempty set S and a distance function $d : S \times S \rightarrow \mathrm{R}_{\geq 0}$, called metric, such that

1. for all $x, y \in S$, $d_S(x, y) = 0 \Leftrightarrow x = y$,
2. (symmetry) $d(x, y) = d(y, x)$ for all $x, y \in S$, and
3. (triangle inequality) $d(x, z) \leq d(x, y) + d(y, z)$ for all $x, y, z \in S$.

The metric d is pseudo if $d(x, y) = 0$ does not necessarily means that $x = y$. A hemimetric is a metric without the symmetry, i.e., there exists some $x, y \in S$ such that $d(x, y) \neq d(y, x)$. The pair (S, d) with a pseudo metric d is called a pseudo metric space. Similarly, (S, d) is a hemimetric space if d is a hemimetric.

A sequence $\{s_n\}$ in a metric space (S, d) is a Cauchy sequence if for any $\varepsilon > 0$ there exists an integer $N \in \mathrm{N}$ such that for all $n, m > N$, $d(s_n, s_m) < \varepsilon$. In addition, the sequence $\{s_n\}$ converges to X if there exists an $M \in \mathrm{N}$ such that for all $n > M$, $d(s_n, X) < \varepsilon$. The metric space (S, d) is complete if every Cauchy sequences converges to an element in S.

Let (S, d) be a metric space, and $f : S \to S$ be a function. The function is a contraction with a Lipschitz constant λ if for all $x_1, x_2 \in S$, $d(f(x_1), f(x_2)) \le \lambda \cdot d(x_1, x_2)$ with $0 \le \lambda < 1$. If $f(x) = x$ with $x \in S$, then x is a fixed point of f in S.

Algebraic Transition Systems and Simulation

In this section we introduce relationships between algebraic transition systems [10], which are specific transition systems labeling transitions with algebraic expressions. We concentrate on the relationships here, simulation, but other kinds may be defined by algebraic expressions labeled on transitions. Algebraic expressions, called algebraic formulas, are defined with polynomials and inequalities which are used to specify transition relation between system states.

Firstly, we introduce the notion of algebraic transition system (ATS) that is a kind of transition systems with transitions labeled by algebraic formulas, and extend it to a metric version, where the state space is endowed with a metric as well as labels.

Definition 2 (Algebraic Transition Systems) For the signature (V, F), a metric algebraic transition system is a tuple $\mathrm{A} = (\mathrm{S}, \mathrm{L}, \mathrm{T}, S_0, \psi_0)$ such that

- S is a set of locations,
- $\mathrm{L} \subseteq \Psi(V \cup V', F)$ is a set of algebraic formulas labeled on transitions, where the set $V' = \{x_1', \mathrm{K}, x_n'\}$ represents the new values taken by the variables $x_1, \mathrm{K}, x_n \in V$ after transitions,
- $\mathrm{T} \subseteq \mathrm{S} \times \mathrm{L} \times \mathrm{S}$ is a set of transitions,
- $S_0 \in \mathrm{S}$ is a set of initial locations, and
- $\psi_0 \in \Psi(V, F)$ is an initial conditions.

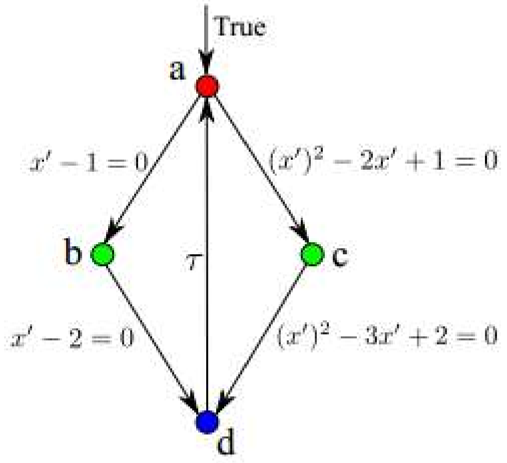

Fig 1: an example which gives a transition system

A transition system given by the example in Fig. 1 is an algebraic transition system in the form of the following

$$\mathrm{S} = \{a, b, c, d\}$$
$$\mathrm{L} = \{\tau\} \cup \left\{x' - 1 = 0, x' - 2 = 0\right\}$$
$$\cup \left\{(x')^2 - 2x' + 1 = 0, (x')^2 - 3x' + 2 = 0\right\}$$
$$\mathrm{L} = \left\{\left(a, x' - 1 = 0, b\right)\right.$$

$$(a, (x^{'})^2 - 2x^{'} + 1 = 0, c)$$
$$(b, x^{'} - 2 = 0, d)$$
$$(c, (x^{'})^2 - 3x^{'} + 2 = 0, d)$$
$$(d, \tau, a)\}$$
$$S_0 = \{a\}$$
$$\psi_0 = \{True\}$$

where the label τ represents a null transition which leaves all variables unchanged.

Let us explain the semantics of an algebraic transition systems $\mathrm{A} = (\mathrm{S}, \mathrm{L}, \mathrm{T}, S_0, \psi_0)$. A state $(s, \vec{u})$ is a vector $\vec{u} \in \mathrm{R}^{|V|}$ paired with a location $s \in \mathrm{S}$. The set of all possible states are usually understood as the state space of A denoted by $State(\mathrm{A})$. Let us remark that the state space can be discrete, continuous, or hybrid. This makes it possible to cover a wide range of complex systems including discrete, continuous, or hybrid states.

We say there is a transition labeled by $\alpha \in \mathrm{L}$ from location s_1 to location s_2, if there exists an evolution from state $(s_1, \vec{u}_1)$ to $(s_2, \vec{u}_2)$, denoted by $(s_1, \vec{u}_1) \xrightarrow{\alpha} (s_2, \vec{u}_2)$, such that

- $(s_1, \alpha, s_2) \in \mathrm{T}$,
- $[\vec{x}\ \alpha\ \vec{u}_1, \vec{x}'\ \alpha\ \vec{u}_2]\ \ \alpha$ with $\vec{x} \in V^{|\vec{x}|}$, $\vec{x}' \in V'^{|\vec{x}'|}$, $\vec{u}_1 \in \mathrm{R}^{|\vec{x}|}$ and $\vec{u}_2 \in \mathrm{R}^{|\vec{x}'|}$.

Moreover, the state $(s_2, \vec{u}_2)$ is a successor of the state $(s_1, \vec{u}_1)$. If there are finitely many successors for each state in $State(\mathrm{A})$, the system A is called finitely branching. The system A is called nonblocking if there exists at least one successor for all states in $State(\mathrm{A})$. In addition, the initial states of A, denote by C_{ini}, are determined by locations in S_0 and the initial condition ψ_0 such that $C_{ini} = \{(s_0, \vec{u}_0) \mid s_0 \in S_0 \wedge [\vec{x}\ \alpha\ \vec{u}_0]\ \ \psi_0\}$. For instance, the initial states of the system shown in Fig. 1 is denoted by $\{(a, \vec{u}) \mid \vec{u} \in \mathrm{R}^{|V|}\}$.

Theorem 1 A state $(s, \vec{u})$ is reachable in n step iff $(s, \vec{u}) \in Reach^n(\mathrm{A})$. And, $(s, \vec{u})$ is reachable iff $(s, \vec{u}) \in Reach(\mathrm{A})$.

Proof. This proof is a quite trivial. If the state $(s, \vec{u})$ is reachable in n steps, then there is a run $(s_0, \vec{u}_0) \xrightarrow{\alpha_0} (s_1, \vec{u}_1) \xrightarrow{\alpha_1} \Lambda \xrightarrow{\alpha_{n-1}} (s_n, \vec{u}_n) \xrightarrow{\alpha_n} \Lambda$ such that $(s_n, \vec{u}_n) = (s, \vec{u})$ and $(s_0, \vec{u}_0) \in C_{ini}$. Since $(s_0, \vec{u}_0) \in C_{ini}$ and $(s_0, \vec{u}_0) \xrightarrow{\alpha_0} (s_1, \vec{u}_1)$, we have $(s_1, \vec{u}_1) \in Reach(C_{ini})$ by the definition of $Reach(\cdot)$. Likewise, we can conclude $(s_2, \vec{u}_2) \in Reach^2(C_{ini})$ since $(s_2, \vec{u}_2) \in Reach(Reach(C_{ini}))$ can be obtained from $(s_1, \vec{u}_1) \xrightarrow{\alpha_1} (s_2, \vec{u}_2)$. Therefore, $(s_n, \vec{u}_n) \in Reach^n(C_{ini}) = Reach^n(\mathrm{A})$ can be concluded likewise.

Conversely, assume that $(s, \vec{u}) \in Reach^n(\mathrm{A}) = Reach^n(C_{ini})$. If $n = 0$, then

$$(s, \vec{u}) \in Reach^0(C_{ini}) = C_{ini}.$$

Hence $(s, \vec{u})$ is an initial state which is reachable in 0 steps. In the case of $n > 0$,

$$(s, \vec{u}) \in Reach^n(C_{ini})$$
$$\Rightarrow (s, \vec{u}) \in Reach(Reach^{n-1}(C_{ini}))$$
$$\Rightarrow \exists (s_{n-1}, \vec{u}_{n-1}) \xrightarrow{\alpha_{n-1}} (s, \vec{u})\ (s_{n-1}, \vec{u}_{n-1}) \in Reach^{n-1}(C_{ini})$$
$$\Rightarrow \exists (s_{n-2}, \vec{u}_{u-2}) \xrightarrow{\alpha_{u-2}} (s_{n-1}, \vec{u}_{n-1}) \xrightarrow{\alpha_{n-1}} (s, \vec{u})\ (s_{n-2}, \vec{u}_{n-2}) \in Reach^{n-2}(C_{ini})$$

$$\Rightarrow \Lambda$$

$$\Rightarrow \exists (s_0, \overset{\rho}{u}_0) \xrightarrow{\alpha_0} (s_1, \overset{\rho}{u}_1) \xrightarrow{\alpha_1} \Lambda \xrightarrow{\alpha_{n-2}} (s_{n-1}, \overset{\rho}{u}_{n-1}) \xrightarrow{\alpha_{n-1}} (s, \overset{\rho}{u})$$

$$(s_0, \overset{\rho}{u}_0) \in C_{ini}$$

Hence the state $(s, \overset{\rho}{u})$ is reachable in n steps.

By the definition of reachability, $(s, \overset{\rho}{u})$ is reachable if and only if it is reachable in n steps with all $n \in \mathrm{N}$. For any $n \geq 0$, $(s, \overset{\rho}{u})$ is reachable in n steps if and only if $(s, \overset{\rho}{u}) \in Reach^n(\mathrm{A})$ by the proof above. Hence, $(s, \overset{\rho}{u})$ is reachable if and only if $(s, \overset{\rho}{u}) \in \mathrm{Y}_{n \in \mathrm{N}} Reach^n(\mathrm{A}) = Reach(\mathrm{A})$.

The reachable states of an algebraic transition system play an important role in the verification of safety and liveness . The high cardinality of reachable states has motivated the development of various notion of system relationships that potentially reduce the complexity of verification [8].

Now, we introduce simulation for algebraic transition systems. Simulation is an important system relationships well established in the formal method community. The simulation between two systems reflects the relationship that a system is refined by the other one. We introduce the simulation of algebraic transition systems based on syntactic identity that requires the algebraic formulas labeled on transitions are strictly identical.

Definition 3 (Syntactic Simulation) Let $\mathrm{A} = (\mathrm{S}, \mathrm{L}, \mathrm{T}, S_0, \psi_0)$ and $\mathrm{A}' = \left(\mathrm{S}', \mathrm{L}, \mathrm{T}', S_0', \psi_0'\right)$ be algebraic transition systems with the same label set. A simulation for A by A' is a binary relation $\mathrm{R} \subseteq \mathrm{S} \times \mathrm{S}'$ such that for all $(s_1, s_2) \in \mathrm{R}$:

- For each $s_0 \in \mathrm{S}_{10}$ there exists a $s_0' \in \mathrm{S}_{20}$ such that $(s_0, s_0') \in \mathrm{R}$, and
- If there is a transition $s_1 \xrightarrow{\alpha} s_1'$ of L_1, then there exists a transition $s_2 \xrightarrow{\alpha} s_2'$ of L_2 with $(s_1', s_2') \in \mathrm{R}$.

We say the system A_1 is syntactically simulated by system A_2, denoted by $\mathrm{A}_1 {}^{\circ}_{syn} \mathrm{A}_2$, if there is a syntactic simulation for A_1 by A_2. The syntactic version of simulation for algebraic transition systems shows that each transition of the system A_1 can be matched by a transition of the system A_2 with an identical label.

Since algebraic formulas are labeled on algebraic transition systems, the notion of simulation can be refined according to the semantics of algebraic formulas, which leads to the semantical simulation.

Definition 4 (Semantical Simulation) Let $\mathrm{A}_i = (\mathrm{S}_i, \mathrm{L}_i, \mathrm{T}_i, d_{\mathrm{L}}, S_{i0})$ with $i = 1, 2$, be two algebraic transition systems. The semantical simulation for A_1 by A_2 is a binary relation $\mathrm{R} : \mathrm{S}_1 \times \mathrm{S}_2$ which satisfies that

- For each $s_0 \in \mathrm{S}_{10}$ there is a $s_0' \in \mathrm{S}_{20}$ with $(s_0, s_0') \in \mathrm{R}$, and
- If there is $s \xrightarrow{\alpha} t$ with $(s, s') \in \mathrm{R}$, then there exists a transition $s' \xrightarrow{\alpha'} t'$ with $\alpha \subseteq \alpha'$.

The system A_1 is semantically simulated by system A_2 ($\mathrm{A}_1 {}^{\circ}_{sem} \mathrm{A}_2$) if there exists a semantical simulation relation for A_1 by A_2.

Proposition 1 Let A_1, A_2 be algebraic transition systems.

$$\mathrm{A}_1 {}^{\circ}_{syn} \mathrm{A}_2 \Rightarrow \mathrm{A}_1 {}^{\circ}_{sem} \mathrm{A}_2 \tag{1}$$

$$\mathrm{A}_1 {}^{\circ}_{syn} \mathrm{A}_2 \Rightarrow Reach(\mathrm{A}_1) \subseteq Reach(\mathrm{A}_2) \tag{2}$$

$$\mathrm{A}_1 {}^{\circ}_{sem} \mathrm{A}_2 \Rightarrow Reach(\mathrm{A}_1) \subseteq Reach(\mathrm{A}_2) \tag{3}$$

Proof. The proof of (1) is trivial since for any $\alpha \in \mathrm{L}$ there is $\alpha \subseteq \alpha$.

If $\mathrm{A}_1{}^{\circ}{}_{syn}\mathrm{A}_2$, then there exists a syntactic simulation for A_1 by A_2. By this syntactic simulation, a run $(s_0, \overset{\rho}{u}_0) \xrightarrow{\alpha_0} (s_1, \overset{\rho}{u}_1) \xrightarrow{\alpha_1} \Lambda \xrightarrow{\alpha_{i-1}} (s_i, \overset{\rho}{u}_i) \xrightarrow{\alpha_i} \Lambda$ of A_1 can be matched by a run of A_2. The reachable set of A_1 is included in $Reach(\mathrm{A}_2)$. The proof of 3 is similar.

Approximate Simulation

Since classical relationships between labeled transition systems do not permit any error, the reduction of systems is clearly limited. Approximate relationships, which allow for error, will improve the reduction of systems. Notions of system approximation are not only better choice for reducing complexity but also provide more robust relationships between systems. The challenge of approximate relationships is to quantify the quality of the approximation.

A metric for action labels defines the distance between labels such as

$$d(\alpha, \beta) = \sup_i \mid \alpha(i) - \beta(i) \mid$$

To construct the notions of approximate relationships, we equip labeled transition systems with metrics on the state space and the set of action labels.

Definition 5 (Metric Labeled Transition Systems) A metric labeled transition system is a labeled transition system $(\mathrm{S}, \mathrm{L}, \mathrm{T})$ such that the set of states S is endowed with a metric d_s, and the set of labels L is equipped with a metric d_l, such that

1. (S, d_s) is a metric space,
2. (L, d_l) is a metric space as defined in Def. 1.

There are different choices between state space and action labels on which metrics are defined. Most transition systems define their state space as a metric space by equipping the state metric d_s [6, 7, 1]. Another choice is to label their transitions with certain constants as the costs or the probabilities of performing the corresponding transitions [9].

The metric d_s specifies the distance between states, and the metric d_l reflects the distance between transitions. Note that d_s and d_l do not need to strictly satisfy all conditions in the definition of metrics shown in Def. 1. Particularly, the metrics d_s and d_l are chosen to be pseudo or hemimetric under distinct circumstances [6, 1, 9,].

For labeled transition systems with finite states, we investigate the distances between states. Inspired by [9, 1] and [6], we present the definition of d_s by d_l which captures the notions of distances between states that how far they are from being similar and bisimilar.

Definition 6 (Simulation Distances) Let $\mathrm{L} = (\mathrm{S}, \mathrm{L}, \mathrm{T})$ be a labeled transition system with a metric $d_l : \mathrm{L} \times \mathrm{L} \to \mathrm{R}_{\geq 0}$ such that S is finite. For states $s_1, s_2 \in \mathrm{S}$, the simulation distance from state s_1 to s_2 is defined to be the least fixed point of the following functions

$$d_s(s_1, s_2) = \sup_{s_1 \xrightarrow{\alpha_1} t_1} \inf_{s_2 \xrightarrow{\alpha_2} t_2} \left\{ d_l(\alpha_1, \alpha_2) + \lambda d_s(t_1, t_2) \right\} \tag{4}$$

where $\lambda \in \mathrm{R}$ and $0 \leq \lambda < 1$.

Simulation distances between states in a labeled transition system can be denoted by a matrix. Let $\mathrm{S} = \{s_1, \mathrm{K}\ , s_n\}$ be the state set of a labeled transition system $\mathrm{L} = (\mathrm{S}, \mathrm{L}, \mathrm{T})$, define a function $D : \mathrm{R}_{\geq 0}^{n \times n} \to \mathrm{R}_{\geq 0}^{n \times n}$ as follows

$$D(\mathrm{s})_{ij} = \sup_{s_i \xrightarrow{\alpha} s_g} \inf_{s_j \xrightarrow{\beta} s_h} \{ d_l(\alpha, \beta) + \lambda\ \mathrm{s}_{gh} \} \tag{5}$$

where s_{gh} indicates the entry of matrix s in its gth row and hth column. The matrix of simulation distances over S can be written as

$$\begin{bmatrix} s_{11} & s_{12} & \Lambda & s_{1n} \\ s_{21} & s_{22} & \Lambda & s_{2n} \\ \mathrm{M} & \mathrm{M} & \mathrm{O} & \Lambda \\ s_{n1} & s_{n2} & \Lambda & s_{nn} \end{bmatrix} = D \begin{bmatrix} s_{11} & s_{12} & \Lambda & s_{1n} \\ s_{21} & s_{22} & \Lambda & s_{2n} \\ \mathrm{M} & \mathrm{M} & \mathrm{O} & \Lambda \\ s_{n1} & s_{n2} & \Lambda & s_{nn} \end{bmatrix}$$

For two matrices $\mathrm{s}, \mathrm{t} \in \mathrm{R}^{n\times n}_{\geq 0}$, the distance between s and t is defined by the metric $d(\mathrm{s}, \mathrm{t}) = \mathrm{max}_{i,j=1}^{n} \mid \mathrm{s}_{ij} - \mathrm{t}_{ij} \mid$.

Summary

In this paper, we present the approximation simulation definition on algebraic transition systems. Using algebraic transition systems, we can abstract a kind of hybrid systems, especially embedded systems. Then we construct the approximate simulation relationship between algebraic transition systems, which allow for error, will improve the reduction of systems. Next, we will study the topics of other relationships in algebraic transition systems, like bisimulaiton relationship, and trace equivalence relationship, etc.

Acknowledgement

This research was supported by the National Science Foundation of China (61650207), and the Science and Technology Foundation of Gansu Province (1610RJZA059).

References

[1] De Alfaro, Luca, Marco Faella, and Mariëlle Stoelinga. Linear and branching system metrics. IEEE Transactions on Software Engineering 35.2 (2009): 258-273.

[2] Girard, Antoine, A. Agung Julius, and George J. Pappas. Approximate simulation relations for hybrid systems. Discrete event dynamic systems 18.2 (2008): 163-179.

[3] Haghverdi, Esfandiar, Paulo Tabuada, and George J. Pappas. Bisimulation relations for dynamical, control, and hybrid systems. Theoretical Computer Science 342.2-3 (2005): 229-261.

[4] Thomas A Henzinger and Joseph Sifakis. The Embedded Systems Design Challenge, volume 4085 of Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2006, pp.1-15.

[5] Vasile I. Istratescu. Fixed Point Theory: An Introduction. Springer Netherlands, 1981.

[6] Girard, Antoine, and George J. Pappas. Approximation metrics for discrete and continuous systems. IEEE Transactions on Automatic Control 52.5 (2007): 782-798.

[7] Girard, Antoine, and Gang Zheng. Verification of safety and liveness properties of metric transition systems. ACM Transactions on Embedded Computing Systems (TECS)11.S2 (2012): 54.

[8] Rob J. van Glabbeek. The linear time - branching time spectrum ii. In Book The Linear Time - Branching Time Spectrum II, Proceedings of the 4th International Conference on Concurrency Theory, Springer-Verlag, 1993, pp.66-81.

[9] Larsen, Kim G., Uli Fahrenberg, and Claus Thrane. Metrics for weighted transition systems: Axiomatization and complexity. Theoretical Computer Science 412.28 (2011): 3358-3369.