УДК 681.3

А. АЛИБЕК[1], А.Б. АЛТАЕВА[2], Б.Ш. КУЛПЕШОВ[2]

([1]Институт проблем информатики и управления, Алматы, Казахстан,
[2]Международный университет информационных технологий, Алматы, Казахстан)

ЗАДАЧИ ДОСТИЖИМОСТИ И ВЕРИФИКАЦИИ ГИБРИДНЫХ СИСТЕМ

Аннотация. Настоящая статься посвящена исследованию вопросов достижимости и верификации упорядоченных гибридных систем. Здесь мы вводим понятие слабо о-минимальных гибридных систем и исследуем их свойства.

Ключевые слова: гибридная система, бисимуляция, дискретный переход, непрерывная динамика, о-минимальность.

Тірек сөздер: гибрид жүйесі, бисимуляция, дискреттік ауысу, үздіксіз динамика, о-минималдық.

Keywords: hybrid system, bisimulation, discrete transition, continuous dynamics, o-minimality.

Гибридные системы – это математические модели систем управления, в которых непрерывная динамика, порождаемая в каждый момент времени одной из априорно заданного набора непрерывных систем, перемежается с дискретными операциями, подающими команды либо на мгновенное переключение с одной системы на другую, либо на мгновенную перестройку с заданных текущих координат на другие координаты, либо на то и другое одновременно. Гибридная динамика системы заключается в альтернативной комбинации непрерывной динамики с дискретной. Непрерывная и дискретная составляющие системы могут включать некоторые параметры, влияющие на поведение системы.

Гибридные системы часто встречаются в различных прикладных задачах из таких областей знания, как автомобилестроение, авиастроение, робототехника, электроэнергетика, обеспечение безопасного движения в пространстве, на суше, на воде и др. Математическая модель гибридной системы возникает каждый раз, когда необходимо исследовать взаимодействие среды, непрерывно изменяющейся в соответствии с некоторыми физическими законами, и управляющих элементов, срабатывающих в дискретные моменты времени. Примерами таких комплексов могут служить электронные системы автоматического управления самолетом, либо автомобилем, системы автоматического регулирования температуры, влажности в помещении и др. Возможности подобных систем проявляются шире, чем обычных.

В данной работе рассматриваются задачи достижимости и верификации для упорядоченной гибридной системы. Задача достижимости состоит в построении множества достижимости гибридной системы, состоящем из всевозможных состояний системы, в которые можно перейти при помощи соответствующего допустимого управляющего воздействия из фиксированного в заданный начальный момент времени состояния (или множества таковых). К задачам достижимости примыкают задачи верификации, в которых необходимо узнать, может ли анализируемая система попасть (или, наоборот, не попасть) в одно из предписанных состояний («желательных» или «нежелательных»). Такая постановка задачи может быть обусловлена, например, проблемами обеспечения безопасности движения в пространстве.

Важным подходом к вопросам разрешимости для алгоритмов верификации гибридных систем является построение бисимуляции. Бисимуляции – это фактор-пространства с конечным числом состояний, в которых свойства достижимости эквивалентны этим же свойствам в первоначальной гибридной системе с бесконечным числом состояний. Ранее в [1] были введены о-минимальные

гибридные системы, являющиеся гибридными системами, у которых соответствующие множества и потоки являются определимыми в о-минимальной теории. В настоящее время данные системы являются активным объектом исследования, например, приведем одну из последних работ [2]. Здесь мы вводим понятие слабо о-минимальных гибридных систем и исследуем их свойства.

Гибридные системы состоят из машин с конечным числом состояний, взаимодействующих с дифференциальными уравнениями. Различные формализмы моделирования, методологии анализа, дизайна и управления, а также приложения, могут быть найдены в [3-5]. Теория формальной верификации является одним из главных подходов при анализе свойств гибридных систем.

Алгоритмы верификации существенным образом являются алгоритмами достижимости, которые проверяют, могут ли траектории гибридной системы достичь некоторых нежелаемых регионов пространства состояний. Поскольку гибридные системы имеют пространства с бесконечным числом состояний, разрешимость алгоритмов верификации очень важна. Бисимуляции – это системы, сохраняющие достижимость в том смысле, что проверка какого-либо свойства на фактор-системе эквивалента проверка этого свойства на оригинальной системе. Хотя даже фокусом этой статьи являются свойства достижимости, бисимуляции сохраняют многие другие сложные свойства, выразимые в разветвляющихся временных логиках. В этом подходе, доказательство того, что гибридная система с бесконечным числом состояний имеет бисимуляцию с конечным числом состояний, является первым шагом для доказательства разрешимости процедур верификации.

Общим подходом для получения бисимуляций является использование алгоритма, утончающего начальное разбиение пространства состояний до тех пор, пока оно не станет вычислимым посредством динамики системы и это свойство должно сохраняться.

Мы адаптируем терминологию [6], слегка модифицируя для наших целей. Система перехода $T = (Q, \Sigma, \rightarrow, Q_O, Q_F)$ состоит из множества (необязательно конечного) состояний Q, алфавита событий Σ, отношения перехода $\rightarrow \subseteq Q \times \Sigma \times Q$, множества начальных состояний $Q_O \subseteq Q$ и множества конечных состояний $Q_F \subseteq Q$. Переход от q_1 к q_2 посредством σ обозначается через $q_1 \xrightarrow{\sigma} q_2$. Система перехода является *конечной*, если мощность множества Q конечна, и *бесконечной* в противном случае. *Регионом* называется подмножество $P \subseteq Q$. Для данного $\sigma \in \Sigma$ мы определяем предшественника $\mathrm{Pr}e_\sigma(P)$ региона P следующим образом: $\mathrm{Pr}e_\sigma(P) := \{q \in Q \mid \exists p \in P : q \xrightarrow{\sigma} p\}$.

Для данного отношения эквивалентности $\approx \subseteq Q \times Q$ на пространстве состояний может быть определена фактор-система перехода следующим образом: Пусть $Q/_\approx$ – фактор-пространство. Для региона P мы обозначаем через $P/_\approx$ совокупность всех классов эквивалентности, которые пересекают P. Отношение перехода $\rightarrow_\approx$ на фактор-пространстве определяется следующим образом: для $Q_1, Q_2 \in Q/_\approx$ $Q_1 \xrightarrow{\sigma}_\approx Q_2$ тогда и только тогда, когда существуют $q_1 \in Q_1$ и $q_2 \in Q_2$ такие, что $q_1 \xrightarrow{\sigma} q_2$. Фактор-системой перехода тогда является $T/_\approx = \left(Q/_\approx, \Sigma, \rightarrow_\approx, Q_0/_\approx, Q_F/_\approx\right)$.

Для данного отношения эквивалентности ≈ на Q мы называем какое-либо множество ≈-*блоком*, если оно является объединением классов эквивалентности. Отношение эквивалентности ≈ называется *бисимуляцией* системы T тогда и только тогда, когда Q_O, Q_F являются ≈-блоками и для всех $\sigma \in \Sigma$ и всех ≈-блоков какого-либо региона P регион $\mathrm{Pr}e_\sigma(P)$ является ≈-блоком. В этом случае системы T и $T/_\approx$ называются *биподобными*.

Мы также говорим, что разбиение является бисимуляцией, когда его индуцированное отношение эквивалентности является бисимуляцией. Бисимуляция называется конечной, если она имеет конечное число классов эквивалентности. Бисимуляции очень важны, поскольку биподобные системы перехода сохраняют свойства достижимости в дополнение к другим более сложным свойствам, выразимым в разветвляющихся временных логиках [6]. Поэтому проверка свойств на биподобной системе перехода эквивалентна проверке свойств оригинальной (первоначальной) системы перехода. Это очень полезно при сокращении сложности различных алгоритмов верифи-

кации, где Q конечно, но очень большое. Кроме того, если T бесконечно, а $T/_{\approx}$ является конечной бисимуляцией, то алгоритмы верификации для бесконечных систем гарантированно завершатся. Этот подход был успешно применен к временным автоматам [7]. Следует заметить, что понятие бисимуляции аналогично понятию динамической совместимости.

Если ≈ является бисимуляцией, то легко может быть показано, что если $p \approx q$, то

B1: $p \in Q_F \Leftrightarrow q \in Q_F$ и $p \in Q_O \Leftrightarrow q \in Q_O$,

B2: если $p \xrightarrow{\sigma} p'$, то существует q' такой, что $q \xrightarrow{\sigma} q'$ и $p' \approx q'$.

Основываясь на вышеприведенной характеризации, для произвольной системы перехода T следующий алгоритм вычисляет возрастающее утончаемые разбиения пространства состояний Q. Если этот алгоритм завершается, то результирующая фактор-система перехода является конечной бисимуляцией.

Алгоритм 1 (Алгоритм бисимуляции для систем перехода)

Set: $Q/_{\approx} = \{Q_O \cap Q_F, Q_O \setminus Q_F, Q_F \setminus Q_O, Q \setminus (Q_O \cup Q_F)\}$

while: $\exists P, P' \in Q/_{\approx}$ и $\sigma \in \Sigma$ такие, что $\varnothing \neq P \cap \mathrm{Pr}\, e_\sigma(P') \neq P$

set: $P_1 = P \cap \mathrm{Pr}\, e_\sigma(P'), P_2 = P \setminus \mathrm{Pr}\, e_\sigma(P')$

refine: $Q/_{\approx} = \left(Q/_{\approx} \setminus \{P\}\right) \cup \{P_1, P_2\}$

end while:

Заметим, что каждый раз, когда разбиение пространства $Q/_{\approx}$ утончается, переходы обновляются относительно вновь разделенных множеств. При проверке специфических свойств таких, как достижимость до множества Q_F, можно было бы упростить алгоритм, стартуя с более крупного разбиения, например, $\{Q_F, Q \setminus Q_F\}$. В общем случае в начальное разбиение следует включать все дополнительные множества, относящиеся к проблеме верификации (такие как безопасные или опасные регионы). Чем больше начальный класс множеств, тем трудней для алгоритма завершиться.

Мы сфокусируемся на системах перехода, порожденных следующим классом гибридных систем. Гибридная система – это кортеж $H = \left(X, X_O, X_F, F, E, I, G, R\right)$, где:

- $X = X_D \times X_C$ - пространство состояний с $X_D = \{q_1, \ldots, q_n\}$ и многообразием X_C.
- $X_O \subseteq X$ - множество начальных состояний.
- $X_F \subseteq X$ - множество конечных состояний.
- $F : X \to TX_C$ присваивает каждому дискретному месторасположению $q \in X_D$ векторное поле $F(q,\cdot)$.
- $E \subseteq X_D \times X_D$ - множество ребер (которые индуцируют дискретные переходы как показано ниже).
- $I : X_D \to 2^{X_C}$ присваивает каждой локации множество $I(q) \subseteq X_C$, называемое инвариантом.
- $G : E \to X_D \times 2^{X_C}$ присваивает ребру $e = (q_1, q_2) \in E$ предохранитель вида $\{q_1\} \times U$, где $U \subseteq I(q_1)$.
- $R : E \to X_D \times 2^{X_C}$ присваивает ребру $e = (q_1, q_2) \in E$ перезапуск вида $\{q_2\} \times V$, где $V \subseteq I(q_2)$.

Траектории гибридной системы H начинаются в любой точке $(q, x) \in X_O$ и состоят либо из непрерывных эволюций, либо из дискретных прыжков. Непрерывные траектории сохраняют дискретную часть состояний постоянной, а непрерывная часть эволюционирует относительно векторного поля $F(q,\cdot)$ столько, сколько траектория остается внутри инвариантного множества $I(q)$. Если траектория выходит из $I(q)$, тогда *навязывается* дискретный переход. Если во время непрерывной эволюции состояние $(q, x) \in G(e)$ достигается для некоторого $e \in E$, тогда *допускается*

дискретный переход, индуцированный с помощью e. Состояние гибридной системы может тогда (затем) мгновенно прыгнуть с (q,x) на $(q',x') \in R(e)$, а непрерывная часть траектории затем эволюционирует относительно векторного поля $F(q',\cdot)$. Заметим, что даже при том, что непрерывная эволюция является детерминированной, дискретная эволюция может быть недетерминированной.

Определим для любого региона $P \subseteq X$ и $q \in X_D$ следующее множество:

$$P_q = \{x \in X_C : (q,x) \in P\}.$$

Для каждой позиции $q \in X_D$ рассмотрим конечную совокупность множеств

$$A_q = \{I(q), (X_O)_q, (X_F)_q\} \cup \{G(e)_q, R(e)_q : e \in E\} \qquad (2)$$

которая описывает начальные и конечные состояния, предохранители, инварианты и перезапуски, связанные с локацией q. Пусть L_q – самое крупное разбиение множества X_C, совместимое с совокупностью A_q (под совместимостью мы понимаем, что каждое множество в A_q является объединением множеств в L_q). (Конечное) разбиение L_q может быть легко вычислено последовательным нахождением пересечений между каждым из множеств в A_q и их дополнениями. Мы определяем $(q, L_q) := \{\{q\} \times P \mid P \in L_q\}$. Эти совокупности (q,L_q) будут стартующими разбиениями алгоритма бисимуляции. Кроме того, поскольку по определению $\mathrm{Pr}\, e_\tau(P)$ применяется к регионам $P \subseteq X$, а не к его непрерывной проекции P_q, мы определяем для $Y \subseteq X_C$ следующий оператор: $\mathrm{Pr}\, e_q(Y) = \left(\mathrm{Pr}\, e_\tau(\{q\} \times Y)\right)_q$. Общий алгоритм бисимуляции для систем перехода тогда принимает следующую форму для класса гибридных систем:

Алгоритм 2 (Алгоритм бисимуляции для гибридных систем)

Set: $X/_{\approx} = \bigcup_q (q, L_q)$

for: $q \in X_D$

while: $\exists P, P' \in L_q$ такие что $\varnothing \neq P \cap \mathrm{Pr}\, e_q(P') \neq P$

Set: $P_1 = P \cap \mathrm{Pr}\, e_q(P')$; $P_2 = P \setminus \mathrm{Pr}\, e_q(P')$

refine: $L_q = (L_q \setminus \{P\}) \cup \{P_1, P_2\}$

end while:

end for:

Следующий пример показывает, что даже в очевидно простых ситуациях Алгоритм 2 не завершается.

Пример 1. Рассмотрим гибридную систему только с одной дискретной позицией q и пусть F – линейное векторное поле $\begin{pmatrix} -1 & 1 \\ -1 & -1 \end{pmatrix} x$ на R^2. Предположим, что разбиение множества R^2 состоит из следующих трех множеств:

$$P_1 = \{(x,0) : 0 \le x \le 4\},\ P_2 = \{(x,0) : -4 \le x < 0\},\ P_3 = R^2 \setminus (P_1 \cup P_2).$$

Траекториями поля F являются спирали, движущиеся прочь от начала координат. Первая итерация алгоритма разбивает P_2 на $P_4 = P_2 \cap \mathrm{Pr}\, e_q(P_1) = \{(x,0) : x_1 \le x < 0\}$ и $P_2 \setminus \mathrm{Pr}\, e_q(P_1)$. Здесь $x_1 < 0$ – x-координата первой точки пересечения спирали через (4, 0) с P_2. Вторая итерация делит P_1 на $P_5 = P_1 \cap \mathrm{Pr}\, e_q(P_4) = \{(x,0) : 0 \le x \le x_2\}$ и $P_1 \setminus \mathrm{Pr}\, e_q(P_4)$, где $x_2 > 0$ – x-координата следующей точки пересечения спирали с P_1. Этот процесс продолжается неопределенным образом, поскольку спираль пересекает P_1 в бесконечном числе точек, и поэтому алгоритм не завершается.

Из вышеприведенного примера ясно, что критической проблемой (задачей) должно являться исследование как траектории поля $F(q,\cdot)$ взаимодействуют с множествами L_q для единственной позиции q. Это требует того, чтобы траектории векторного поля $F(q,\cdot)$ имели «хорошие» свойства пересечения с такими множествами. Поскольку целью является получение конечных разбиений, станет важным, что мы ограничиваемся на изучение классов множеств со свойствами глобальной «конечности», например, множества с конечным числом связанных компонент.

Определение 2. Пусть $F : R^n \to R^n$ – гладкое векторное поле на R^n. Для каждого $x \in R^n$ пусть $\gamma_x(t)$ обозначает интегральную кривую поля F, которая проходит через точку x при $t = 0$, т.е. $\dot{\gamma}_x(t) = F(\gamma_x(t))$ и $\gamma_x(0) = x$. Мы говорим, что поле F является *полным*, если для каждого x $\gamma_x(t)$ определяется для всех t. *Потоком* поля F является функция $\Phi : R^n \times R \to R^n$, определяемая как $\Phi(x,t) = \gamma_x(t)$.

Определение 3. Гибридная система $H = (X, X_O, X_F, F, E, I, G, R)$ называется *слабо о-минимальной*, если X_C является многообразием; для каждого $q \in X_D$ векторное поле $F(q,\cdot)$ является полным, и для каждого $q \in X_D$ семейство множеств $A_q = \{I(q), (X_O)_q, (X_F)_q\} \cup \{G(e)_q, R(e)_q : e \in E\}$ и поток поля $F(q,\cdot)$ являются определимыми в слабо о-минимальном обогащении линейно упорядоченной группы.

Теорема 4. Каждая слабо о-минимальная гибридная система ранга выпуклости 1 допускает конечную бисимуляцию. В частности, алгоритм бисимуляции (Алгоритм 2) завершается для слабо о-минимальных гибридных систем ранга выпуклости 1.

REFERENCES

1 Lafferriere G., Pappas G.J., Sastry S. O-minimal hybrid systems. Mathematics of Control, Signals and Systems. 2000. Vol. 13, N 1. P. 1-21.

2 Bouyer P., Brihaye T., Chevalier F. O-minimal hybrid reachability games, Logical Methods in Computer Science. 2010. Vol. 6, N 1. P. 1-48.

3 Alur R., Henzinger T.A., Sontag E.D., editors, Hybrid Systems III, volume 1066 of Lecture Notes in Computer Science. Springer-Verlag, Berlin, 1996.

4 Henzinger T.A., Sastry S., editors. Hybrid Systems: Computation and Control, volume 1386 of Lecture Notes in Computer Science. Springer-Verlag, Berlin, 1998.

5 Maler O., editor. Hybrid and real-Time Systems, volume 1201 of Lecture Notes in Computer Science. Springer-Verlag, Berlin, 1997.

6 Henzinger T.A. Hybrid automata with finite bisimulations. In Z. Fulop and F. Gecseg, editors. ICALP 95: Automata, Languages, and Programming, pages 324-335. Springer-Verlag, Berlin, 1995.

7 Alur R., Dill D.L. A theory of timed automata. Theoretical Computer Science, 126: 183-235, 1994.

Резюме

А. Әлібек[1], А. Б. Алтаева[2], Б. Ш. Күлпешов[2]

([1]Информатика және басқару проблемалар институты, Алматы, Қазақстан,
[2]Халықаралық ақпараттық технологиялар университеті, Алматы, Қазақстан)

ГИБРИД ЖҮЙЕЛЕРДІҢ ҚОЛ ЖЕТЕРЛІКТІК ПЕН ВЕРИФИКАЦИЯ МӘСЕЛЕЛЕРІ

Мақала реттелген гибрид жүйелерінде қол жетерліктік пен верификация мәселелерін зерттеуіне арналған. Осы мақалада біз босаң о-минималды гибрид жүйелер ұғымын енгіземіз және олардың қасиеттерін зерттейміз.

Тірек сөздер: гибрид жүйесі, бисимуляция, дискреттік ауысу, үздіксіз динамика, о-минималдық.

Summary

A. Alibek[1], A.B. Altayeva[2], B.Sh. Kulpeshov[2]

([1]Informatics and Control Problems Institute, Almaty, Kazakhstan,
[2]International Information Technology University, Almaty, Kazakhstan)

REACHABILITY AND VERIFICATION PROBLEMS OF HYBRID SYSTEMS

The present article is devoted to studying reachability and verification questions in ordered hybrid systems. Here we introduce the notion of weakly o-minimal hybrid systems and study their properties.

Keywords: hybrid system, bisimulation, discrete transition, continuous dynamics, o-minimality.

Поступила 03.03.2014 г.