ВЕСТНИК НОВОСИБИРСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА
Серия «Математика, механика, информатика»
Том VI, 2006 г. Выпуск 3. С. 88–97

УДК 004.021

Локальный тест на включение в задаче о достижимости для вполне структурированных систем переходов[1]

Д. Л. Чубаров

§ 1. Введение

Процедуры построения множества достижимых состояний в символьном представлении нередко применяются для анализа дискретных систем переходов с бесконечным числом состояний. Самым простым примером является процедура построения дерева достижимости Карпа и Миллера, где некоторые узлы представляют бесконечные множества состояний. В общем случае аналогичные процедуры строятся на основе автоматного представления регулярных множеств [5]. Однако, их широкому применению препятствует отсутствие гарантий остановки и высокая вычислительная сложность отдельных операций.

Решению первой проблемы — поиску классов систем переходов для которых отдельные задачи анализа разрешимы — посвящены работы по изучению вполне структурированных систем переходов [2, 4, 9].

Один вариант решения второй проблемы — ускорения отдельных операций — в контексте систем переходов, представленных символьно с помощью бесквантворных формул арифметики Пресбургера, состоит в применении локального теста на включение вместо более сильного, но вместе с тем более сложного теста [6, 14].

Естественным образом возникает вопрос о том, сохранятся ли результаты о разрешимости для вполне структурированных систем переходов при построении дерева достижимости с применением локального теста. В настоящей работе ответ на этот вопрос получен для задачи о покрываемости.

Для ответа на вопрос потребовался один факт из теории нетеровых предпорядков,

[1]Работа поддержана грантом РФФИ 06-01-00464-а

который не удалось найти в литературе. В статье приводится полное доказательство, полученное модификацией одного доказательства из книги [1].

§ 2. Используемые обозначения

Мы будем использовать следующее соглашение. Переменные и функциональные символы будут обозначены буквами латинского алфавита $a, \ldots, z$ возможно с индексами. Множества будут обозначаться либо заглавными буквами $A, \ldots, Z$, либо прописными буквами полужирного шрифта $\mathbf{x}, \mathbf{y}, \mathbf{z}$. Символы в калиграфическом написании $\mathcal{S}, \mathcal{T}$ будем обозначать алгебраические структуры.

Если $\varphi(x)$ является формулой в некотором языке L, содержащей свободное вхождение переменной x, а t термом того же языка, то $\varphi(x)[{}^{t}/_{x}]$ будет обозначать формулу полученную из $\varphi(x)$ подстановкой t вместо всех свободных вхождений x.

Алгебраические структуры будем обозначать как пару $\mathcal{S} = \langle S; \Sigma \rangle$, состоящую из носителя S и сигнатуры Σ. Если φ — формула сигнатуры Σ, а θ — интерпретация ее свободных переменных, то символом $\mathcal{S}, \theta \models \varphi$ будем обозначать выполнимость формулы φ при интерпретации θ.

Пусть $R(x, y)$ — бинарное отношение на множестве S, а X — подмножество в S. Прообразом X по отношению R будем называть множество $\mathrm{pre}_R(X) = \{x \mid R(x, y)$ для некоторого $y \in X\}$. Там, где отношение можно однозначно определить из контекста, нижний индекс будем опускать. Когда обозначение $\mathrm{pre}(X)$ используется без нижнего индекса, будем писать $\mathrm{pre}^*(X)$ вместо $\mathrm{pre}_{R^*}(X)$ для прообраза по отношению к рефлексивному и транзитивному замыканию отношения R.

§ 3. Символьное представление для систем переходов

Системой переходов будем называть структуру $\mathcal{S} = \langle S; \{\dashrightarrow\} \rangle$ с носителем S и сигнатурой, содержащей символ бинарного отношения $\dashrightarrow$. Множество S называется *множеством состояний* системы переходов, а отношение $\dashrightarrow$ называется *отношением перехода*.

При необходимости мы будем добавлять в сигнатуру новые символы, получая таким образом системы переходов с более богатой структурой. Расширение сигнатуры позволяет также изучать системы переходов в символьном представлении. В продолжение этого раздела мы определим символьное представление систем переходов, следуя [14].

Пусть $\mathcal{X} = \langle X; \Sigma \rangle$ является структурой с сигнатурой Σ, не содержащей символа $\dashrightarrow$. Будем говорить, что задано символьное представление системы переходов $\mathcal{S}$ над $\mathcal{X}$, если задано отображение $\nu : S \to X^n$ и формула ϕ со свободными переменными $x_1, \ldots, x_n$ и $x'_1, \ldots, x'_n$, такая что если θ_{s_1,s_2} — интерпретация, которая переменной x_1 ставит в соответствие значение $\nu(s_1)_1$, переменной x_2 ставит в соответствие значение $\nu(s_1)_2$ и

так далее, и аналогично переменной x'_i соответствует значение $\nu(s_2)_i$, то

$$s_1 \dashrightarrow s_2, \text{ если и только если } \mathcal{X}, \theta_{s_1,s_2} \models \varphi.$$

Будем говорить, что формула φ определяет отношение переходов.

Если $s \in S$ — элемент множества состояний, то пусть θ_s обозначает некоторую интерпретацию, которая ставит переменным $x_1, \ldots, x_n$ в соответствие значения $\nu(s)_1$, ..., $\nu(s)_n$. Будем говорить, что подмножество Z, содержащееся в множестве S, определено формулой ψ со свободными переменными $x_1, \ldots, x_n$, если

$$s \in Z \quad \text{тогда и только тогда, когда} \quad \mathcal{X}, \theta_s \models \psi.$$

Пусть L — множество формул сигнатуры Σ, замкнутое относительно замены переменных и конъюнкции, такое что отношение переходов определяется дизъюнкцией формул из L. Тогда имеет место следующее утверждение.

Предложение 1 [14]. *Пусть Z — некоторое подмножество множества состояний, определимое формулой из L, тогда прообраз Z относительно $\dashrightarrow$ является объединением конечного числа множеств, определимых формулами из L.*

Если отношение перехода определяется дизъюнкцией формул языка L, то совокупность множеств определимых формулами языка L задает *абстрактное представление* системы переходов.

Приведем несколько примеров систем переходов, имеющих символьное представление.

§ 3.1. *Системы переходов с конечным числом состояний*

Рассмотрим систему переходов $\langle S_F; \{\dashrightarrow_F\}\rangle$ с конечным множеством состояний. В этом случае символьное представление можно получить, введя для каждого элемента $s \in S_F$ в язык предикаты $P_s(x)$, такие что $\theta \models P_s(x)$ если и только если $\theta(x) = s$.

Язык составленный из атомов P_s и их отрицаний, очевидно удовлетворяет требованию замкнутости относительно конъюнкции и требованию определимости отношения переходов.

§ 3.2. *Языки программирования в ограничениях*

Рассмотрим систему переходов $\langle S_C; \{\dashrightarrow_C\}\rangle$ и сигнатуру Σ, имеющую символьное представление над структурой $\mathcal{X}$ сигнатуры Σ. Множество L формул сигнатуры Σ является языком программирования в ограничениях, если L замкнуто относительно экзистенциальной квантификации, конъюнкции и переименования переменных [11].

Рассмотрим совокупность Z всех подмножеств множества S, определимых формулами языка L. Потребуем дополнительно, чтобы отношение перехода $\dashrightarrow_C$ было определимо дизъюнкцией формул языка L. В этом случае Z задает абстрактное представление системы переходов в соответствии с определением.

§ 3.3. *Монотонные системы переходов*

Рассмотрим систему переходов $\langle S_U; \{\dashrightarrow_U, \precsim\}\rangle$, обогащенную рефлексивным и транзитивным бинарным отношением $\precsim$. *Верхним конусом элемента* $s \in S_U$ называется множество $\{t \mid s \precsim t\}$. Объединение верхних конусов элементов называется *верхним конусом*.

Будем говорить, что отношение переходов *совместно* с отношением $\precsim$, если для любых элементов $x, y, z \in S_U$, таких, что $x \dashrightarrow_U y$ и $x \precsim z$ найдется элемент w, такой что $y \precsim w$ и $z \dashrightarrow_U w$. Системы переходов, в которых выполняется условие совместности называются монотонными.

Рефлексивное и транзитивное бинарное отношение является *нетеровым предпорядком*, если оно не содержит бесконечных убывающих цепей и не содержит бесконечных антицепей. В этом случае всякий верхний конус является объединением конечного числа верхних конусов элементов.

Допустим, что условие совместности выполняется, тогда множество всех верхних конусов замкнуто относительно прообраза. Допустим, кроме того, что отношение переходов само является верхним конусом в декартовом произведении $S \times S$. Тогда выполняется и условие определимости отношения переходов в абстрактном представлении, состоящем из совокупности всех верхних конусов элементов.

Примером монотонных систем переходов являются сети Петри с отношением покомпонентного порядка на разметках. Другие варианты определения совместности, позволяющие включить в класс монотонных систем ряд интересных примеров, не являющихся монотонными в указанном выше смысле, рассматриваются в статье [9]. Для таких систем возможно с незначительными изменениями перенести приведенную здесь конструкцию абстрактного представления.

§ 4. Построение множества достижимых состояний

Мы последовательно рассмотрим два описания процедуры построения множества достижимых состояний. Первое описание является традиционным и в общих чертах следует работе [9]. Другое описание дается в терминологии абстрактного представленния определенной выше. Последнее описание имеет несколько параметров, изменяя которые, можно получить новые варианты традиционной процедуры.

§ 4.1. *Два варианта процедуры*

Рассмотрим систему переходов $\mathcal{S} = \langle S; \{\dashrightarrow\}\rangle$ и подмножество X в множестве состояний. Положим $I_0 = X$ и рассмотрим возрастающую последовательность множеств $I_0, I_1, \ldots$, полученную по правилу $I_{i+1} \cup \mathrm{pre}(I_i)$. Последовательность обрывается на ша-

ге n, если $I_{n+1} = I_n$. Если последовательность обрывается на некотором шаге n, то $I_n = \mathrm{pre}^*(X)$, таким образом построено множество всех элементов в S из которых достижим некоторый элемент множества X в результате конечной последовательности переходов.

В применении этой процедуры возникают две трудности. Во-первых, при вычислении прообраза необходимо избежать повторного выполнения одних и тех же вычислений в связи с тем, что каждое вновь построенное множество содержит предыдущее. Для того, чтобы описать процедуру более детально, мы будем предполагать, что система переходов имеет абстрактное представление совокупностью множеств Z.

Пусть X — такое подмножество множества S, что существует конечное подмножество $J = \{\mathbf{z}_1, \ldots, \mathbf{z}_n\}$ в Z, такое что $X = \mathbf{z}_1 \cup \ldots \cup \mathbf{z}_n$.

Процедура построения множества достижимости оперирует конечными подмножествами Z. Когда новое подмножество a конструируется посредством объединения подмножеств a_1 и a_2, процедура должна избегать дублирования. Возможно применение различных критериев избыточности, которые влекут различные критерии остановки. Операцию объединения с применением критерия избыточности будем обозначать как $a = \sigma(a_1, a_2)$. Единственным условием, которое накладывается на операцию σ является следующее:

$$\bigcup \sigma(a_1, a_2) = \bigcup a_1 \cup \bigcup a_2$$

В следующем подразделе мы рассмотрим два различных критерия избыточности, а текущий раздел завершим описанием процедуры построения множества достижимости.

Следующий вариант процедуры построения множества достижимости строит последовательность $P_0, P_1, \ldots$ конечных подмножеств в Z. Пусть $P_0 = X$ и пусть $\delta_0 = P_0$. Множества $P_1, P_2, \ldots$ строятся следующим образом.

(1) Определим $\alpha_i = \{\mathrm{pre}(\mathbf{z}) \mid \mathbf{z} \in \delta_i\}$.
(2) Пусть $\delta_{i+1} = \sigma(P_i, \alpha_i)$.
(3) Если множество δ_{i+1} пусто, процедура останавливается.
(4) Пусть $P_{i+1} = \sigma(\delta_{i+1}, P_i) \cup \delta_{i+1}$.
(5) Повторить процедуру, начиная с первого пункта.

На каждом шаге процедуры объединение всех множеств, содержащихся в P_i совпадает с множеством I_i, определенном в первом варианте процедуры. Таким образом, в случае, если второй вариант процедуры останавливается на шаге n, то $\bigcup P_n = \mathrm{pre}^*(X)$.

§ 4.2. *Критерии избыточности*

Применение критерия избыточности может быть наиболее вычислительно интенсивной частью процедуры, поскольку операция σ вычисляется на каждой итерации. В

случае, когда множества совокупности Z заданы линейными неравенствами в рациональных числах, в работе [15] приведены несколько вариантов критерия избыточности и соответствующие оценки сложности. Варианты, предложенные в этой работе, позволяют получить более эффективную процедуру вычисления критерия за счет потери в полноте.

Стандартный критерий избыточности можно сформулировать следующим образом:

$$\sigma_1(X, Y) = Y \setminus \{\mathbf{y} \mid \mathbf{y} \subseteq \bigcup X\}. \tag{1}$$

Другой, более слабый критерий мы будем называть локальным критерием избыточности

$$\sigma_2(X, Y) = Y \setminus \{\mathbf{y} \mid \mathbf{y} \subseteq \mathbf{x} \text{ для некоторого } \mathbf{x} \in X\}. \tag{2}$$

Применение локального критерия гарантирует выполнение следующих условий на каждом шаге процедуры построения множества достижимых состояний:

(1) $\bigcup P_{i+1} = \bigcup P_i \cup \bigcup \alpha_i$
(2) Множество P_{i+1} не содержит двух элементов $\mathbf{x}$ и $\mathbf{y}$, таких что $\mathbf{x}$ и $\mathbf{y}$ различны, и $\mathbf{x} \subseteq \mathbf{y}$.

Критерий σ_2 слабее, чем критерий σ_1. Таким образом, процедура, использующая критерий σ_2, может не остановиться за конечное число шагов, в то время как процедура, использующая σ_1, останавливается. В продолжение этой статьи мы будем называть вариант процедуры с критерием σ_2 *процедурой с локальным критерием избыточности.*

Одним важным классом задач, на котором процедура построения множества достижимых состояний останавливается, является вычисление множества достижимости для верхних конусов для вполне структурированных систем. Мы завершим этот раздел описанием этого класса задач.

§ 4.3. *Вполне структурированные системы переходов*

В случае если система переходов S является вполне структурированной системой переходов, а множесто X является верхним конусом, процедура построения множества достижимости останавливается [4, 9, 10].

Определение 1. Монотонная система переходов $\mathcal{S} = \langle S; \{\dashrightarrow, \precsim\}\rangle$ является *вполне структурированной системой переходов* тогда и только тогда, когда отношение $\precsim$ является нетеровым предпорядком, то есть предпорядком, не содержащим бесконечных антицепей и бесконечных убывающих цепей.

Процедура построения множества достижимых состояний для вполне структурированных систем переходов определяется в абстрактном представлении совокупностью верхних конусов элементов.

Пусть X — верхний конус в S. Будем говорить, что система переходов с начальным состоянием s_0 удовлетворяет *свойству покрываемости* X, если начальное состояние принадлежит множеству достижимых состояний множества X.

В качестве примера задач, в которых требуется проверка свойства покрываемости для вполне структурированных систем переходов, можно упомянуть процедуру для анализа свойств безопасности протоколов с широковещательными посылками, предложенную в работе [7].

Доказательство остановки процедуры при применении критерия σ_1 хорошо известно и основано на том факте, что покомпонентный порядок на множестве k-мерных векторов с положительными целыми компонентами является нетеровым предпорядком. Ситуация с локальным критерием несколько сложнее. Для того, чтобы доказать остановку в этом случае, нам потребуется следующая теорема.

§ 5. Одна теорема о нетеровых предпорядках

В этом разделе приводится доказательство утверждения о том, что множество верхних конусов в нетеровом предпорядке образует нетеров предпорядок по включению.

Сначала докажем следующую лемму.

Лемма 1. *Пусть $\alpha = \alpha_1, \alpha_2, \ldots$ является последовательностью элементов в нетеровом предпорядке $\mathcal{A} = \langle A; \leq \rangle$, а $\beta = \beta_1, \beta_2, \ldots$ является последовательностью элементов в предпорядке $\mathcal{B} = \langle B; \leq \rangle$, такая что последовательность β содержит возрастающую подпоследовательность, тогда последовательность $\gamma = (\alpha_1, \beta_1), (\alpha_2, \beta_2), \ldots$ в $\mathcal{A} \times \mathcal{B}$ содержит возрастающую подпоследовательность.*

ДОКАЗАТЕЛЬСТВО. Пусть последовательность $b_{i_1}, b_{i_2}, \ldots$ является возрастающей подпоследовательностью в β. В силу того, что $\mathcal{A}$ является нетеровым предпорядком, подпоследовательность $a_{i_1}, a_{i_2}, \ldots$ в свою очередь содержит возрастающую подпоследовательность $a_{j_1}, a_{j_2}, \ldots$. Таким образом, последовательность $(a_{j_1}, b_{j_1}), (a_{j_2}, b_{j_2}), \ldots$ является возрастающей подпоследовательностью в γ.

Напомним, что верхним конусом в предпорядке называется любое множество которое со всяким элементом содержит и все большие его элементы. Теперь мы можем доказать следующую теорему.

Теорема 1. *Любая бесконечная последовательность $X_1, X_2, \ldots$ верхних конусов в нетеровом предпорядке содержит некоторую подпоследовательность $X_{i_1} \supseteq X_{i_2} \supseteq \ldots$, состоящую из вложенных верхних конусов.*

ДОКАЗАТЕЛЬСТВО. Допустим, что существует последовательность верхних конусов, не содержащая бесконечной подпоследовательности вложенных конусов. Среди всех таких последовательностей $A_1, A_2, \ldots$ выберем ту, в которой множество A_1 содержит

наименьшее число минимальных элементов. Такой выбор возможен в силу того, что в нетеровом предпорядке любой верхний конус содержит лишь конечное число минимальных элементов.

Множество минимальных элементов в конусе A_i обозначим как B_i. В каждом из множеств B_i в свою очередь выберем по одному элементу a_i и пусть C_i обозначает конус, минимальными элементами которого являются элементы множества $B_i \setminus \{a_i\}$.

Число минимальных элементов в верхнем конусе C_1 строго меньше числа минимальных элементов в верхнем конусе A_1, следовательно последовательность $C_1, C_2, \ldots$ содержит подпоследовательность, состоящую из вложенных конусов.

Определим на множестве верхних конусов предпорядок $\sqsubseteq$ так, что $A \sqsubseteq B$ тогда и только тогда, когда $B \subseteq A$.

К последовательностям $C_1, C_2, \ldots$ и $a_1, a_2, \ldots$ применима лемма 1, следовательно последовательность $\gamma = (C_1, a_1), (C_2, a_2), \ldots$ содержит возрастающую покомпонентно подпоследовательность.

Заметим, что если $C_i \sqsubseteq C_j$ и $a_i \precsim a_j$, то $A_j \subseteq A_i$. Таким образом последовательность верхних конусов A_i, соответствующая возрастающей покомпонентно подпоследовательности в γ является подпоследовательностью вложенных конусов.

§ 6. Остановка процедуры с локальным критерием защиты от дублирования

Рассмотрим вполне структурированную систему переходов $\mathcal{S} = \langle S; \{\dashrightarrow, \precsim\}\rangle$. Пусть Z обозначает совокупность всех верхних конусов элементов над S, а X является верхним конусом, то есть, в силу нетеровости предпорядка $\precsim$, является объединением конечного числа верхних конусов элементов.

Рассмотрим последовательность множеств, $P_0, P_1, \ldots$, которая строится локальным вариантом процедуры построения множества достижимых элементов. Критерий избыточности гарантирует, что в этой последовательности не встретится пара множеств P_i и P_j, такая что $i < j$ и найдутся верхние конусы $\mathbf{x_i} \in P_i$ и $\mathbf{x_j} \in P_j$, такие что $x_j \subseteq x_i$.

В силу теоремы 1. Такая последовательность не может быть бесконечной. Таким образом доказана остановка процедуры построения множества достижимых состояний для задачи о покрываемости для вполне структурированных систем переходов.

§ 7. Историческая справка

Ряд доказательств нетеровости для различных предпорядков собраны в книге [1]. Приведенное доказательство теоремы 1 основано на модификации одного из доказательств, из этой книги. Теме исследования свойств нетеровых предпорядков посвящен

целый ряд статей, многие из которых упомянуты в обзоре [12].

Процедура построения дерева достижимости с локальным тестом на включение применяется в ряде систем для проверки моделей [6, 13]. Локальный тест на включение также применяется в контексте программирования в ограничениях [15].

Понятие вполне структурированных систем переходов предложено независимо в работах [4] и [8]. Изучению этого класса систем посвящены книги [2] и [3]. В этих книгах, в частности, речь идет о проверке моделей для более сложных свойств, чем свойство покрываемости, таких как свойства, описываемые темпоральными логиками линейного и ветвящегося времени.

§ 8. Заключение

Мы показали, что описанная процедура построения множества достижимых состояний с локальным критерием избыточности является разрешающей процедурой для задачи о покрываемости для вполне структурированных систем переходов.

В общем случае применение локального критерия позволяет получить более эффективную реализацию процедуры за счет потери в полноте критерия остановки. Следует заметить, что для задачи о покрываемости для вполне структурированных систем переходов стандартный критерий избыточности может быть реализован также эффективно как и локальный при условии, что минимальные элементы верхних конусов могут быть эффективно вычислены.

С другой стороны, существуют ситуации в которых локальный критерий избыточности может быть реализован значительно быстрее. Описание некоторых таких ситуаций и возможностей использования неполного метода может быть предметом дальнейших исследований и экспериментов.

§ 9. Благодарности

Автор благодарит А. Воронкова, Т. Рыбину за помощь в постановке задачи, а также В.А. Непомнящего за помощь в подготовке статьи.

Литература

[1] *Ю. Л. Ершов, С. С. Гончаров*, Конструктивные модели, Сибирская школа алгебры и логики, Новосибирск, Научная книга, 1999.

[2] *Е. В. Кузьмин, В. А. Соколов*, Вполне структурированные системы помеченных переходов, Физматлит, 2005.

[3] *Е. В. Кузьмин, В. А. Соколов*, Структурированные системы переходов, Физматлит, 2006.

[4] *P. A. Abdulla, K. Čerāns, B. Jonsson, Y.-K. Tsay*, General decidability theorems for infinite state systems, In LICS, 1996, 313–321.

[5] *S. Bardin, A. Finkel, J. Leroux, L. Petrucci*, FAST: Fast Accelereation of Symbolic Transition systems, In Proc. 15th Conf. Computer Aided Verification (CAV'2003), vol. 2725 of Lect. Notes in Comput. Sci., Springer, 2003, 118–121.

[6] *G. Delzanno, A. Podelski*, Constraint-based deductive model checking, STTT, **3**, No. 3 (2001), 250–270.

[7] *J. Esparza, A. Finkel, R. Mayr*, On the verification of broadcast protocols, In LICS, 1999, 352–359.

[8] *A. Finkel*, A generalization of the procedure of Karp and Miller to well structured transition system, In ICALP, 1987, 499–508.

[9] *A. Finkel, Ph. Schnoebelen*, Fundamental structures in well-structured infinite transition systems, In LATIN, 1998, 102–118.

[10] *A. F*, Reduction and covering of infinite reachability trees, Inf. Comput., **89**, No. 2 (1990), 144–179.

[11] *J. Jaffar, M. J. Maher*, Constraint logic programming: A survey. J. Log. Program., **19**–**20** (1994), 503–581.

[12] *J. Kruskal*, The theory of well-quasi-ordering: a frequently discovered concept, J. Comb. Theory, Ser. A, **13** (1972), 297–305.

[13] *T. Rybina, A. Voronkov*, BRAIN: Backward reachability analysis with integers, In AMAST, vol. 2422 of Lect. Notes Comput. Sci., 2002, 489–494.

[14] *T. Rybina, A. Voronkov*, A logical reconstruction of reachability, In Ershov Memorial Conference, 2003, 222–237.

[15] *Divesh Srivastava*, Subsumption and indexing in constraint query languages with linear arithmetic constraints, Ann. Math. Artif. Intell., **8**, No. 3–4 (1993), 315–343.

Поступило 1 июня 2006 г.

Адрес автора:
ЧУБАРОВ Дмитрий Леонидович,
РОССИЯ, 630090, г. Новосибирск,
просп. Академика М. А. Лаврентьева, 6
ИВТ СО РАН
e-mail: dchubarov@ict.nsc.ru