Моделирование и анализ поведения последовательных реагирующих программ

В.А.Захаров <zakh@cs.msu.su>
Институт системного программирования РАН,
109004, Россия, г. Москва, ул. А. Солженицына, дом 25;
НИУ Высшая школа экономики, Россия, Москва, 101000, ул. Мясницкая, д. 20.

Аннотация. Автоматы-преобразователи с конечным числом состояний над полугруппами могут служить простой моделью последовательных реагирующих программ. Эти программы работают во взаимодействии с окружающей средой, получая на входе поток управляющих сигналов и выполняя последовательности действий. Как только программа достигает определенного состояния управления, она выдает на выходе текущий результат вычисления. Элементарные действия реагирующей программы можно рассматривать как порождающие элементы некоторой полугруппы, а результат последовательного выполнения этих действий расценивается как элемент полугруппы, представляющий собой композицию этих действий. В данной статье предложен общий подход к решению двух задач анализа вычислений преобразователей такого вида – задачи проверки k-значности конечных преобразователей и задачи проверки эквивалентности k-значных преобразователей. Показано, что обе указанные задач можно свести к задаче поиска опровергающих вершин в ограниченных фрагментах размеченных системах переходов. При помощи предложенного подхода показано, что задача проверки эквивалентности детерминированных конечных преобразователей над полугруппами, которые могут быть вложены в конечно порожденные разрешимые полугруппы, и задача проверки k-значности таких преобразователей разрешимы за полиномиальное время. Кроме того, установлено, что задача проверки эквивалентности k-значных преобразователей разрешима за время, экспоненциальное относительно их размеров.

Ключевые слова: реагирующая программа; автомат-преобразователь; полугруппа; размеченная система переходов; эквивалентность; свойство k-значности; разрешающий алгоритм; сложность.

DOI: 10.15514/ISPRAS-2015-27(2)-13

Для цитирования: Захаров В.А. Моделирование и анализ поведения последовательных реагирующих программ. Труды ИСП РАН, том 27, вып. 2, 2015 г., стр. 221-250. DOI: 10.15514/ISPRAS-2015-27(2)-13.

1. Введение

Автоматы-преобразователи (transducers) с конечным числом состояний естественным образом расширяют широко известную модель вычислений конечных автоматов Рабина-Скотта. В отличие от конечных автоматов, способных распознавать регулярные языки $L, L \subseteq \Sigma^*$, конечные преобразователи позволяют распознавать регулярные (рациональные) отношения $R, R \subseteq \Sigma^* \times \Delta^*$, на множествах конечных слов. Поэтому их область применения гораздо обширнее. Конечные преобразователи используются в системном программировании для построения простейших компиляторов [2], драйверов, осуществляющих фильтрацию и преобразования строк, изображений, потоков данных [3,21], в системах автоматизированного проектирования управляющих систем для разработки контроллеров [16], в компьютерной лингвистике для создания программ распознавания речи [14] и др. Для практического использования этой модели вычислений в столь разнообразных областях, нужны эффективные алгоритмы построения композиций, проверки эквивалентности и минимизации преобразователей.

Преобразователи могут служить простой моделью некоторого класса специальных программ. Эти программы работают во взаимодействии с окружающей средой, получая на входе поток управляющих сигналов, запросов или показаний датчиков. После приема очередной порции входных данных такая программа выполняет некоторую конечную последовательность действий и переходит в новое состояние управления. Как только программа достигает определенного состояния управления, она выдает на выходе текущий результат вычисления. Программы такого рода называются реагирующими программами. Их функция состоит в том, чтобы вырабатывать правильные отклики в ответ на внешние воздействия. К числу программ такого рода относятся операционные системы, сетевые протоколы, драйверы, контроллеры. При выборе подходящей математической модели важным обстоятельством являются два факта. Во-первых, разные последовательности действий, выполняемые такой программой, могут приводить к одному и тому же результату. Поэтому элементарные (базовые) действия реагирующей программы можно рассматривать как порождающие элементы некоторой полугруппы, а результат последовательного выполнения этих действий расценивается как элемент полугруппы, представляющий собой композицию этих действий. Во-вторых, одна и та же последовательность входных данных (запросов, управляющих сигналов) может приводить к разным результатам, поскольку на поведение программы помимо входных данных могут также влиять внешние факторы, скрытые от внешнего наблюдателя. Для моделирования такой реагирующей программы можно воспользоваться конечным автоматом-преобразователем (в общем случае недетерминированным), который преобразует слова входного алфавита Σ (алфавита управляющих сигналов) в полугрупповые выражения

Представим себе в качестве примера, что радиоуправляемый робот движется по поверхности планеты. Он может делать шаги в любом из четырех направлений N, E, S, W. Если этот робот получает некоторый управляющий сигнал syg, пребывая при этом в состоянии q, то он может выбрать и совершить некоторую серию шагов (скажем, N, N, W, S), а также перейти в следующее состояние q'. В особых состояниях управления q_{fin} робот оповещает о своем текущем местоположении. Существенными являются две особенности этого робота: 1) робот может достичь одного и того же места, совершая разные последовательности шагов (например N, N, W, W, S, E и W, N), и 2) выбор допустимой последовательности шагов может зависеть от случайных, не поддающихся контролю обстоятельств (например, от освещенности местности, погодных условий, состояния грунта и пр.). Наиболее простой моделью вычислений, пригодной для проектирования и анализа программы управления движением такого робота может служить недетерминированный конечный преобразователь, работающий над абелевой группой ранга 2.

Так мы приходим к концепции автомата-преобразователя, который принимает на входе слова некоторого алфавита Σ и выдает на выходе элементы некоторой конечно порожденной полугруппы S. Для преобразователей такого вида нужно уметь решать тот же самый набор алгоритмических задач, что и для конечных автоматов Рабина-Скотта и традиционных автоматов-преобразователей, а именно

- задачу синтеза преобразователя по заданному алгебраическому или логическому описанию рационального отношения $R, R \subseteq \Sigma^* \times S$;
- задачу верификации заданного преобразователя относительно заданных алгебраических или логических спецификаций его поведения;
- задачу проверки эквивалентности двух заданных преобразователей;
- задачи детерминизации и минимизации преобразователей.

В данной статье приводятся некоторые результаты исследования проблемы эквивалентности для конечных преобразователей над полугруппами. Изучение этой проблемы и ряда смежных задач для классических автоматов-преобразователей началось в 60-х годах XX века. Вначале было установлено, что проблема эквивалентности для недетерминированных автоматов-преобразователей (generalized finite state machines) неразрешима [8,9] и при этом даже для однобуквенного входного алфавита [11]. Однако неразрешимость возникает только для таких недетерминированных преобразователей, у которых входные слова могут иметь неограниченно много выходных образов. На следующем этапе проблема эквивалентности изучалась для класса ограниченно недетерминированных преобразователей, у которых для любого входного слова количество его различных выходных образов не превосходит некоторого фиксированного числа k. Было

установлено, что свойство ограниченной недетерминированности преобразователей можно проверять за полиномиальное время [22]. В статье [10] было показано, что столь же эффективно можно проверять и свойство -значности недетерминированных преобразователей для любого заданного числа k. Разрешимость проблемы эквивалентности была установлена для детерминированных автоматов-преобразователей [5], функциональных (однозначных) преобразователей [4,19] и k-значных недетерминированных преобразователей [7,23]. В серии работ [6,17,18,20] авторы предложили метод декомпозиции произвольного -значного недетерминированного преобразователя в сумму функциональных и недвусмысленных (unambiguous) преобразователей. Этот метод был использован для построения алгоритмов проверки ограниченной недетерминированности, -значности и эквивалентности классических преобразователей, работающих над словами.

В данной статье предложен новый универсальный метод решения задач, связанных с проверкой эквивалентности конечных автоматов-преобразователей, работающих над полугруппами. Для проверки эквивалентности преобразователей π_1 и π_2 предлагается исследовать свойства размеченной системы переходов (Labeled Transition System, LTS) Γ_{π_1,π_2}, ассоциированной с этими преобразователями. Маршруты в этой LTS представляют все возможные пары вычислений преобразователей π_1 и π_2 на одном и том же входном слове. Каждая вершина u LTS Γ_{π_1,π_2}содержит информацию о том, в каких состояниях оказываются преобразователи π_1 и π_2 после прочтения некоторого входного слова, и том, каково расхождение выходных полугрупповых элементов, вычисленных преобразователями к этому моменту. Если оба преобразователя достигают своих заключительных состояний и дефицит вычисленных ими выходных результатов оказывается ненулевым, то это служит признаком того, что преобразователи π_1 и π_2 на некотором входном слове вычисляют разные результаты, т.е. не являются эквивалентными. Вершины LTS Γ_{π_1,π_2}, в которых проявляется указанный эффект, называются *опровергающими* вершинами. Таким образом, проверка эквивалентности преобразователей π_1 и π_2 сводится к проверке достижимости опровергающих вершин в LTS Γ_{π_1,π_2}. Оказывается, что для проверки достижимости опровергающих вершин достаточно исследовать лишь ограниченный фрагмент LTS Γ_{π_1,π_2}. Если анализируемые преобразователи π_1 и π_2 являются детерминированными, то размер этого фрагмента ограничен полиномом, зависящим от размера π_1 и π_2, и поэтому проблема эквивалентности для преобразователей такого рода может быть решена за полиномиальное время. Если же анализируемые преобразователи являются ограниченно недетерминированными, то размер этого фрагмента ограничен экспонентой, зависящей от размера π_1 и π_2 . Поскольку проблема эквивалентности недетерминированных конечных автоматов Рабина-Скотта является PSPACE-полной, эта оценка вряд ли может быть существенно улучшена. Тот же самый подход можно использовать и для проверки свойства

-значности недетерминированности конечных преобразователей, работающих над полугруппами.

Используемый в данной статье подход был впервые предложен в работе [24] для разработки полиномиальных по времени алгоритмов проверки эквивалентности программ. Сходные идеи были развиты также в статьях [6,17,18] и применены для анализа вычислений традиционных автоматов-преобразователей. Основные преимущества нашего подхода (помимо того очевидного факта, что он применим к автоматам-преобразователям более общего вида) таковы. Во-первых, в отличие от метода проверки свойств вычислений автоматов-преобразователей, впервые предложенного в статье [23] и затем развитого в статье [17], наш подход не требует предварительной декомпозиции анализируемых преобразователей и может быть применен к любым преобразователям без предварительной их подготовки. Во-вторых, предложенные нами процедуры верификации преобразователей, в отличие от методов, описанных в работах [18,20], не опираются ни на какие особенности устройства отношения переходов анализируемых преобразователей. Фактически, все рассматриваемые далее задачи, связанные с проблемой эквивалентности, решаются одной и той же процедурой обхода размеченной системы переходов в глубину с возвратом с целью обнаружения опровергающих вершин. Специфика решаемой задачи отражается лишь в устройстве самой системы переходов. Вследствие этого сложность разработанных нами алгоритмов проверки эквивалентности и ограниченной недетерминированности автоматов преобразователей существенно меньше сложности алгоритмов, описанных в статьях [4-7,17,18,20]. Разработанный нами подход применим к автоматам-преобразователям, проводящих вычисления в произвольной конечно порожденной полугруппе, которая может быть вложена в группу с разрешимой проблемой равенства слов.

Статья устроена следующим образом. В разделе 2 введены основные известные понятия, относящиеся к теории конечных последовательных автоматов-преобразователей. В разделе 3 описан алгоритм проверки эквивалентности детерминированных автоматов-преобразователей, работающих над полугруппами. В разделе 4 описаны сходные по устройству алгоритмы решения двух задач – проверки свойства функциональности преобразователей и проверки эквивалентности функциональных преобразователей. В разделе 5 предложен метод проверки свойства -значности недетерминированных преобразователей. Для большей наглядности в этом разделе подробно описан и обоснован алгоритм проверки свойства 2-значности преобразователей. Из описания этого алгоритма легко выводится и общий способ построения алгоритмов проверки свойства -значности недетерминированности преобразователей для любого значения параметра k. В разделе 6 описан алгоритм проверки эквивалентности 2-значных недетерминированных автоматов преобразователей. В разделе 7 приведены оценки сложности предложенных разрешающих алгоритмов для конечных

преобразователей над свободной полугруппой и свободной коммутативной полугруппой. В заключительном разделе проведен сравнительный анализ полученных результатов, а также обозначены перспективы решения других задач синтеза и анализа автоматов-преобразователей над полугруппами.

2. Основные понятия

Пусть задан конечный алфавит Σ. Записью Σ^* обозначим множество всех конечных слов над алфавитом Σ. Буквы алфавита Σ могут быть истолкованы как элементарные события, происходящие во внешней среде и оказывающие влияния на информационную систему, взаимодействующую с этой средой. В этом случае слова можно истолковывать как возможный сценарий поведения внешней среды по отношению к информационной системе.

Конечным автоматом над алфавитом Σ назовем систему $M = \langle \Sigma, Q, init, F, \varphi \rangle$, в которой

- Q – конечное множество *состояний*;
- $init$ – *начальное состояние*, $init \in Q$;
- F – подмножество *финальных состояний*, $F \subseteq Q$;
- $\varphi \subseteq Q \times \Sigma \times Q$ – *отношение переходов*.

Автомат M допускает слово $w = a_1 a_2 \dots a_n$, если существует такая последовательность состояний $q_0, q_1, \dots, q_n$, в которой $q_0 = init$, $q_n \in F$, и $(q_{i-1}, a_i, q_i) \in \varphi$ выполняется для каждого $i, 1 \leq i \leq n$. Язык $L(M)$ автомата M – это множество всех слов, допускаемых автоматом M. Запись $M[q]$ будет использоваться для обозначения автомата $\langle \Sigma, Q, q, F, \varphi \rangle$, в котором начальным состоянием служит состояние q.

Рассмотрим полугруппу $S = (B, \cdot, e)$, порожденную множеством элементов B и имеющую единичный (нейтральный) элемент e. Порождающие элементы полугруппы можно рассматривать как элементарные операторы (действия), которые выполняет информационная система в ответ на внешние воздействия. Бинарная операция полугруппы в этом случае соответствует последовательной композиции этих операторов. Если два полугрупповых выражения s_1 и s_2 имеют одинаковое значение, то это означает, что соответствующие этим выражениям последовательности операторов вычисляют одинаковый результат.

Конечным преобразователем (далее просто преобразователем) над полугруппой S называется система $\pi = \langle \Sigma, S, Q, q_0, F, T \rangle$, в которой

- Q – конечное множество состояний;
- q_0 – начальное состояние, $q_0 \in Q$;
- F – подмножество финальных состояний, $F \subseteq Q$;

- $T \subseteq Q \times \Sigma \times S \times Q$ – конечное отношение переходов.

Четверки (q, a, s, q') из множества T называются *переходами*; для их обозначения используем запись $q \xrightarrow{a/s} q'$. Для каждого состояния $q, q \in Q$, запись $\pi[q]$ будет обозначать преобразователь $\langle \Sigma, S, Q, q, F, T \rangle$, в котором состояние q играет роль начального состояния. Мы будем использовать запись M_π для обозначения *автомата-подложки* $\langle \Sigma, Q, q_0, F, \varphi_\pi \rangle$, в котором $\varphi_\pi = \{(q, a, q') : q \xrightarrow{a/s} q' \text{ для некоторого } s \text{ из } S\}$. Для конечного автомата $M = \langle \Sigma, Q', init, F', \varphi' \rangle$ и преобразователя $\pi = \langle \Sigma, S, Q, q_0, F, T \rangle$ *проекцией преобразователя* π *на автомат* M называется преобразователь $\pi|_M = \langle \Sigma, S, Q \times Q', (q_0, init), F \times F', \hat{T} \rangle$, в котором отношение переходов $\hat{T}$ определяется требованием: $(q, p) \xrightarrow{a/s} (q', p') \Leftrightarrow q \xrightarrow{a/s} q' \wedge (p, a, p') \in \varphi$.

Вычислением преобразователя π на входном слове $w = a_1 a_2 \dots a_n$ называется всякая последовательность переходов

$$run = q_i \xrightarrow{a_1/s_1} q_{i+1} \xrightarrow{a_2/s_2} \cdots \xrightarrow{a_{n-1}/s_{n-1}} q_{i+n-1} \xrightarrow{a_n/s_n} q_{i+n} .$$

Конечный преобразователь служит моделью последовательной реагирующей программы. Каждый переход $q \xrightarrow{a/s} q'$ означает, что при получении внешнего воздействия a в состоянии управления q эта программа совершает переход в состояние управления q' и выполняет последовательность операторов s. Последовательность таких переходов образует вычисление реагирующей программы.

Элемент $s = s_1 \cdot s_2 \cdots s_n$ полугруппы S называется *образом* входного слова w, а пара (w, s) называется *меткой* вычисления run. Запись $q_i \xrightarrow{w/s} q_{i+n}$,будет использоваться для сокращенного обозначения вычисления преобразователя на входном слове w. Если $q_i = q_0$, то вычисление run называется *начальным вычислением*. Если $q_{i+n} \in F$, то вычисление run называется *финальным вычислением*. *Полным вычислением* называется всякое вычисление преобразователя, которое является как начальным, так и финальным. Записью $Lab(\pi)$ обозначим множество меток (w, s) всех полных вычислений преобразователя π; это множество является отношением, которое реализует преобразователь π. Преобразователи π' и π'' считаются *эквивалентными* (и обозначаются записью $\pi' \sim \pi''$), если $Lab(\pi') = Lab(\pi'')$.

Образ входного слова представляет собой результат вычисления реагирующей программы в ответ на последовательность воздействий среды. Внешний наблюдатель регистрирует результаты лишь тех вычислений, которые достигают финальных состояний управления. Поэтому наблюдаемое поведение реагирующей программы π полностью определяется множеством меток $Lab(\pi)$. Таким образом, эквивалентность преобразователей означает, что соответствующие реагирующие программы имеют одинаковое наблюдаемое поведение.

Состояние q преобразователя π считается *полезным*, если хотя бы одно полное вычисление проходит через это состояние. Далее будем полагать, что все состояния преобразователя полезны, поскольку от бесполезных состояний можно избавиться, сохранив при этом реализуемое преобразователем отношение. Преобразователи такого рода будем называть *правильными*. Преобразователь считается *детерминированным*, если для любой буквы a и для любого состояния q множество T содержит не более одного перехода вида $q \xrightarrow{a/s} q'$. Преобразователь π называется -*значным*, где k – положительное целое число, если для любого входного слова w отношение $Lab(\pi)$ содержит не более k меток вида (w, s). Однозначный преобразователь также называется *функциональным*.

Далее в статье будет описан общий метод построения разрешающих процедур для задач проверки эквивалентности и -значности преобразователей на полугруппами S , вложимыми в конечно порожденные разрешимые группы. Полугруппа S называется *вложимой* в группу G, если эта группа содержит подполугруппу S' , изоморфную полугруппе S. Необходимые и достаточные условия вложимости полугруппы в группу были установлены А.П. Мальцевым в статье [12]. В последующей статье [13] было доказано, что никакой критерий вложимости полугруппы в группу не может представлен конечным множеством условий. Однако для полугрупп специального вида условия их вложимости в группу могут быть сформулированы сравнительно просто. Например, свободная полугруппа всегда вложима в свободную группу. Для вложимости в группу коммутативной полугруппы необходимо и достаточно, чтобы она обладала свойствами левого и правого сокращения. Группа называется разрешимой, если в ней разрешима *проблема равенства слов*, т.е. существует алгоритм, который для любой пары выражений, составленных из порождающих элементов группы, может определить, представляют ли эти выражения один и тот же элемент группы. В этой статье мы будем полагать, что G является конечно порожденной разрешимой группой, содержащей полугруппу S в качестве подполугруппы. Поэтому для всякого элемента s полугруппы S запись s^- будет обозначать элемент группы G, обратный групповому элементу s.

3. Проверка эквивалентности детерминированных преобразователей

Пусть заданы пара детерминированных преобразователей $\pi' = \langle \Sigma, S, Q', q_0', F', T' \rangle$ и $\pi'' = \langle \Sigma, S, Q'', q_0'', F'', T'' \rangle$ над полугруппой S, которая вложена в конечно порожденную разрешимую группу G. Для проверки эквивалентности этих преобразователей рассмотрим размеченную систему переходов (LTS) $\Gamma^0_{\pi',\pi''} = \langle Q' \times Q'' \times G, \Rightarrow \rangle$. Ее вершинами являются тройки вида (q', q'', g), где $q' \in Q', q'' \in Q''$, и $g \in G$. Отношение переходов $\Rightarrow$ определяется следующим образом: для каждой пары вершин $v_1 = (q_1', q_1'', g_1)$

и $v_2 = (q_2', q_2'', g_2)$, и произвольной буквы a отношение $v_1 \overset{a}{\Rightarrow} v_2$ имеет место тогда и только тогда, когда в преобразователях π' и π'' есть переходы $q_1' \xrightarrow{a/s'} q_2'$ и $q_1'' \xrightarrow{a/s''} q_2''$ соответственно, и при этом $g_2 = (s')^- g_1 s''$.

Пусть задано слово $w = a_1 a_2 \dots a_n$ и пара вершин $v = (q_1', q_1'', g_1)$ и $u = (q_2', q_2'', g_2)$. Запись $v \overset{w}{\Rightarrow} u$ будет обозначать последовательность переходов $v \overset{a_1}{\Rightarrow} v_1 \overset{a_2}{\Rightarrow} v_2 \overset{a_3}{\Rightarrow} \cdots \overset{a_{n-1}}{\Longrightarrow} v_{n-1} \overset{a_n}{\Rightarrow} u$, которую будем называть маршрутом в LTS $\Gamma^0_{\pi',\pi''}$. В этом случае будем говорить, что вершина u достижима из вершины v. Нетрудно видеть, что в LTS $\Gamma^0_{\pi',\pi''}$ существует маршрут $v \overset{w}{\Rightarrow} u$ в том и только том случае, если ${q'}_1 \xrightarrow{w/s'} {q'}_2$, ${q''}_1 \xrightarrow{w/s''} {q''}_2$, и $(s')^- g_1 s'' = g_2$.

Вершину $v_{src} = (q_0', q_0'', e)$, где e – единичный элемент группы G, назовем *стартовой вершиной* LTS $\Gamma^0_{\pi',\pi''}$. Используем запись $\mathrm{V}^0_{\pi',\pi''}$ для обозначения множества вершин LTS $\Gamma^0_{\pi',\pi''}$, достижимых из стартовой вершины. Всякую вершину (q_1, q_2, g) будем называть *опровергающей*, если она удовлетворяет одному из следующих требований:

- q_1 и q_2 – финальные состояния преобразователей π' и π'', и при этом $g \neq e$;
- одно из состояний q_σ, $\sigma \in \{1,2\}$, является финальном, тогда как другое состояние $q_{3-\sigma}$ не является финальным;
- для некоторой буквы a одно из состояний q_σ, $\sigma \in \{1,2\}$, имеет a-переход $q_\sigma \xrightarrow{a/s} q'_\sigma$, тогда как другое состояние $q_{3-\sigma}$ не имеет a-переходов.

Множество всех опровергающих вершин LTS $\Gamma^0_{\pi',\pi''}$ обозначим записью $R^0_{\pi',\pi''}$. Значение множеств вершин $\mathrm{V}^0_{\pi',\pi''}$ и $R^0_{\pi',\pi''}$ для проверки эквивалентности детерминированных преобразователей проясняют следующие две леммы.

Лемма 1. Детерминированные преобразователи π' и π'' эквивалентны тогда и только тогда, когда $\mathrm{V}^0_{\pi',\pi''} \cap R^0_{\pi',\pi''} = \emptyset$.

Доказательство. Следует непосредственно из определений LTS $\Gamma^0_{\pi',\pi''}$, и множества вершин $\mathrm{V}^0_{\pi',\pi''}$, $R^0_{\pi',\pi''}$. Детерминированные правильные преобразователи π' и π'' неэквивалентны тогда и только тогда, когда для некоторого слова w выполняется хотя бы одно из двух условий:

1) $(w, s') \in Lab(\pi')$, $(w, s'') \in Lab(\pi'')$, и при этом $s' \neq s''$;
2) Для одного из преобразователей, множество его меток содержит пару (w, s), тогда как другой преобразователь не имеет никаких образов для слова w.

Первое из указанных условий выполняется в том и только том случае, если из стартовой вершины LTS $\Gamma^0_{\pi',\pi''}$, по маршруту с пометкой w достижима вершина (q_1, q_2, g), где q_1 и q_2 – финальные состояния преобразователей π' и π'', и при этом $g = (s')^- s'' \neq e$. Второе из указанных условий выполняется в том и только том случае, если либо из стартовой вершины LTS $\Gamma^0_{\pi',\pi''}$ по маршруту с пометкой w достижима некоторая вершина (q_1, q_2, g), в которой только одно из двух состояний q_1, q_2 является финальным, либо $w = w'aw''$, и при этом из стартовой вершины LTS $\Gamma^0_{\pi',\pi''}$ по маршруту с пометкой w' достижима некоторая вершина (q_1, q_2, g), в которой только одно из двух состояний q_1, q_2 имеет -переход.

QED

Таким образом, проверка эквивалентности детерминированных преобразователей сводится к проверке достижимости опровергающих вершин из стартовой вершины LTS $\Gamma^0_{\pi',\pi''}$. Следующая лемма показывает, что для проверки достижимости опровергающих вершин достаточно исследовать лишь ограниченный фрагмент LTS.

Лемма 2. Если множество $V^0_{\pi',\pi''}$ содержит пару вершин $v_1 = (q_1', q_1'', g_1)$ и $v_2 = (q_1', q_1'', g_2)$, удовлетворяющую соотношению $g_1 \neq g_2$, то $\mathrm{V}^0_{\pi',\pi''} \cap R^0_{\pi',\pi''} \neq \emptyset$.

Доказательство. Предположим, что, вопреки утверждению леммы, $\mathrm{V}^0_{\pi',\pi''} \cap R^0_{\pi',\pi''} = \emptyset$, и, следовательно, $\pi' \sim \pi''$. По определению LTS $\Gamma^0_{\pi',\pi''}$ достижимость вершины v_1 означает, что существует такое слово w_0, для которого имеются начальные вычисления $q_0' \xrightarrow{w_0/s_0'} q_1'$ и $q_0'' \xrightarrow{w_0/s_0''} q_1''$, и при этом $g_1 = (s_0')^- s_0''$. Поскольку состояние q_1' является полезным, существует такое слово w, для которого вычисление $q_0' \xrightarrow{w_0/s_0'} q_1' \xrightarrow{w/s'} q_3'$ является полным вычислением преобразователя π'. Предполагая, что $\pi' \sim \pi''$, и принимая во внимание детерминированность преобразователя π'', приходим к заключению о том, что преобразователь π'' имеет такое полное вычисление $q_0'' \xrightarrow{w_0/s_0''} q_1'' \xrightarrow{w/s''} q_3''$, для которого $s_0' s' = s_0'' s''$. Значит, $(s_0')^- s_0'' = s'(s'')^-$, и поэтому $g_1 = s'(s'')^-$. По определению LTS $\Gamma^0_{\pi',\pi''}$ существование вычислений $q_1' \xrightarrow{w/s'} q_3'$ и $q_1'' \xrightarrow{w/s''} q_3''$ означает, что в LTS имеется маршрут $v_2 \overset{w}{\Rightarrow} (q_3', q_3'', g)$, причем $g = (s')^- g_2\, s''$. Учитывая, что (q_3', q_3'', g) принадлежит множеству $\mathrm{V}^0_{\pi',\pi''}$, а также то, что оба состояния q_3' и q_3'' являются финальными, и предполагая, что $\mathrm{V}^0_{\pi',\pi''} \cap R^0_{\pi',\pi''} = \emptyset$, мы приходим к равенству $g = e$. Следовательно, $g_2 = s'(s'')^- = g_1$, а это противоречит условию данной леммы. QED

Из лемм 1 и 2 вытекает, что для проверки эквивалентности правильных детерминированных преобразователей π' и π'' достаточно проанализировать не более $|Q'||Q''|+1$ вершин, достижимых из стартовой вершины LTS $\Gamma^0_{\pi',\pi''}$. Итак, мы приходим к следующей теореме.

Теорема 1. Если полугруппа S вложима в конечно порожденную разрешимую группу G, то проблема эквивалентности детерминированных преобразователей над S разрешима. Кроме того, если проблема равенства слов в группе G разрешима за полиномиальное время, то и проблема эквивалентности детерминированных преобразователей над S разрешима за полиномиальное время.

4. Проверка эквивалентности функциональных преобразователей

Для проверки того, является ли преобразователь $\pi = \langle A, S, Q, q_0, F, T\rangle$ функциональным, мы воспользуемся размеченными системами переходов подобно тому, как это было сделано для проверки эквивалентности детерминированных преобразователей. Но для недетерминированных преобразователей соответствующие LTS нуждаются в некоторых изменениях.

Пусть заданы преобразователи $\pi' = \langle A, S, Q', q'_0, F', T'\rangle$ и $\pi'' = \langle A, S, Q'', q''_0, F'', T''\rangle$ над полугруппой S, которая вложена в конечно порожденную разрешимую группу G. Отношение переходов в LTS $\Gamma^1_{\pi',\pi''} = \langle\, Q' \times Q'' \times G, \Rightarrow \rangle$ определим так: для каждой пары вершин $v_1 = (q'_1, q''_1, g_1)$ и $v_2 = (q'_2, q''_2, g_2)$ и буквы a отношение $v_1 \overset{a}{\Rightarrow} v_2$ имеет место тогда и только тогда, когда в преобразователях π' и π'' есть переходы $q'_1 \xrightarrow{a/s'} q'_2$ и $q''_1 \xrightarrow{a/s''} q''_2$ соответственно, и при этом $g_2 = (s')^- g_1 s''$ и $L(M_{\pi'}[q'_2]) \cap L(M_{\pi''}[q''_2]) \neq \emptyset$. Множество всех вершин LTS $\Gamma^1_{\pi',\pi''}$, достижимых из стартовой вершины (q'_0, q''_0, e) обозначим записью $V^1_{\pi',\pi''}$. Будем говорить, что вершина (q_1, q_2, g) является опровергающей, если q_1 и q_2 – финальные состояния и при этом $g \neq e$. Множество всех опровергающих вершин LTS $\Gamma^1_{\pi',\pi''}$ обозначим записью $R^1_{\pi',\pi''}$. Для проверки свойства функциональности преобразователя π рассмотрим LTS $\Gamma^1_{\pi,\pi}$ и множества вершин $V^1_{\pi,\pi}$ и $R^1_{\pi,\pi}$.

Лемма 3. Правильный преобразователь π является однозначным тогда и только тогда, когда $V^1_{\pi,\pi} \cap R^1_{\pi,\pi} = \emptyset$.

Доказательство. Проводится также, как и доказательство леммы 1 на основании определений LTS $\Gamma^1_{\pi,\pi}$ и множеств $V^1_{\pi,\pi}$ и $R^1_{\pi,\pi}$ QED

Лемма 4. Если множество $V^1_{\pi,\pi}$ содержит такую пару вершин $v_1 = (q'_1, q''_1, g_1)$ и $v_2 = (q'_1, q''_1, g_2)$, для которой имеет место соотношение $g_1 \neq g_2$, то $V^1_{\pi,\pi} \cap R^1_{\pi,\pi} \neq \emptyset$.

Доказательство. Проводится также, как и доказательство леммы 2. QED

Из лемм 3 и 4 вытекает, что для проверки свойства функциональности преобразователя π достаточно рассмотреть не более $|Q|^2 + 1$ вершин, достижимых из стартовой вершины LTS $\Gamma^1_{\pi,\pi}$.

Теорема 2. Если полугруппа S вложима в конечно порожденную разрешимую группу G, то свойство функциональности преобразователя над полугруппой S разрешимо. Кроме того, если проблема равенства слов в группе G разрешима за полиномиальное время, то и проверку свойства функциональности преобразователей над S можно провести за полиномиальное время.

Эквивалентность функциональных преобразователей π' и π'' можно проверить точно так же, как и свойство функциональности, при помощи LTS $\Gamma^1_{\pi',\pi''}$. Но для этого нам вначале нужно убедиться, что $L(M_{\pi'}[q'_0]) = L(M_{\pi''}[q''\_0])$. Проверку этого соотношения необходимо проводить потому, что в случае функциональных преобразователей, в отличие от детерминированных преобразователей, достижимость вершин (q_1, q_2, g), в которой одно из состояний q_σ, $\sigma \in \{1,2\}$, является финальном, а другое нет, не является признаком неэквивалентности. Это, в частности, означает, что задача проверки эквивалентности для функциональных преобразователей является PSPACE-трудной независимо от того, над какой полугруппой работают эти преобразователи.

Лемма 5. Если $L(M_{\pi'}[q'_0]) = L(M_{\pi''}[q''_0])$, то функциональные преобразователи π' и π'' эквивалентны тогда и только тогда, когда $V^1_{\pi',\pi''} \cap R^1_{\pi',\pi''} = \emptyset$.

Лемма 6. Если множество $V^1_{\pi',\pi''}$ содержит такую пару вершин $v_1 = (q'_1, q''_1, g_1)$ и $v_2 = (q'_2, q''_2, g_2)$, для которой $g_1 \neq g_2$, то $V^1_{\pi',\pi''} \cap R^1_{\pi',\pi''} \neq \emptyset$.

Из лемм 5 и 6 вытекает, что для проверки эквивалентности функциональных преобразователей π' и π'' достаточно рассмотреть не более $|Q'||Q''| + 1$ вершин, достижимых из стартовой вершины LTS $\Gamma^1_{\pi',\pi''}$. Таким образом, верна

Теорема 3. Если полугруппа S вложима в конечно порожденную разрешимую группу G, то проблема эквивалентности для функциональных преобразователей над полугруппой S разрешима. Кроме того, если проблема равенства слов в группе G разрешима за полиномиальное время, то проблема эквивалентности функциональных преобразователей над S является PSPACE-полной.

5. Проверка свойства двухзначности моделей реагирующих программ

Метод анализа поведения преобразователей, основанный на размеченных системах переходов, предложенный в предыдущих разделах статьи для проверки эквивалентности детерминированных и функциональных преобразователей, можно развить далее для проверки свойств

конечнозначных преобразователей. Для простоты изложения мы ограничимся рассмотрением 2-значных преобразователей.

Вначале обратимся к задаче проверки свойства 2-значности конечных преобразователей, работающих над полугруппами, которые вложены в группы. Для заданного преобразователя $\pi = \langle A, S, Q, q_0, F, T\rangle$ определим LTS $\Gamma_\pi^2 = \langle Q \times (Q \times G)^2, \Rightarrow \rangle$ следующим образом: для каждой пары вершин $v_1 = (q_1, (q_2, g_{12}), (q_3, g_{13}))$ и $v_2 = (q_1', (q_2', g_{12}'), (q_3', g_{13}'))$, и произвольной буквы a отношение $v_1 \underset{a}{\Rightarrow} v_2$ имеет место тогда и только тогда, когда в преобразователе π существуют такие переходы $q_1 \xrightarrow{a/s_1} q_1'$, $q_2 \xrightarrow{a/s_2} q_2'$, и $q_3 \xrightarrow{a/s_3} q_3'$, для которых выполняются равенства $g_{12}' = (s_1)^{-} g_{12} s_2$ и $g_{13}' = (s_1)^{-} g_{13} s_3$, и при этом $L(M_\pi[q_1']) \cap L(M_\pi[q_2']) \cap L(M_\pi[q_3']) \neq \emptyset$.

Тройку состояний (q_1, q_2, q_3) будем называть *типом* вершины $(q_1, (q_2, g_{12}), (q_3, g_{13}))$. Как и в случае $k = 1$, обозначим записью V_π^2 множество всех вершин LTS Γ_π^2, достижимых из стартовой вершины $(q_0, (q_0, e), (q_0, e))$. Как следует из определений LTS Γ_π^2 и множества V_π^2, вершина $v = (q_1, (q_2, g_{12}), (q_3, g_{13}))$ содержится в множестве V_π^2 тогда и только тогда, когда для некоторого слова w преобразователь π имеет вычисления $q_0 \xrightarrow{w/s_1} q_1$, $q_0 \xrightarrow{w/s_2} q_2$, $q_0 \xrightarrow{w/s_3} q_3$, удовлетворяющие равенствам $g_{12} = (s_1)^{-} s_2, g_{13} = (s_1)^{-} s_3$. Поэтому, если некоторая вершина $v = (q_1, (q_2, g_{12}), (q_3, g_{13}))$ содержится в множестве V_π^2, то в этом же множестве содержатся так же и вершины $(q_1, (q_1, e), (q_3, g_{13}))$, $(q_1, (q_2, g_{12}), (q_1, e))$, $(q_1, (q_2, g_{12}), (q_2, g_{12}))$, и т. д..

Множество опровергающих вершин R_π^2 состоит из всех тех вершин $(q_1, (q_2, g), (q_3, h))$, для которых состояния q_1, q_2, q_3 являются финальными, и при этом $g \neq e, h \neq e, g \neq h$.

Лемма 7. Преобразователь π является 2-значным тогда и только тогда, когда $V_\pi^2 \cap R_\pi^2 = \emptyset$.

Доказательство. Следует непосредственно из определений множеств V_π^2, R_π^2, а также определения свойства 2-значности конечных преобразователей. QED

В общем случае множество достижимых вершин V_π^2 бесконечно, и поэтому, чтобы воспользоваться леммой 7 для построения эффективной процедуры проверки свойства 2-значности преобразователя, нужно каким-то образом выделить в этом множестве ограниченный фрагмент, анализ которого позволил бы решить вопрос о выполнимости равенства $V_\pi^2 \cap R_\pi^2 = \emptyset$. Для этой цели воспользуемся следующими тремя леммами, доказательство которых по существу опирается на принцип Дирихле и простейшие тождества теории групп.

Лемма 8. Предположим, что множество V_π^2 содержит четыре вершины $v_i = \big(q', (q'', h_i), (q''', g_i)\big)$, $1 \le i \le 4$, одного и того же типа, удовлетворяющие соотношениям $h_i \neq h_j, g_i \neq g_j$ и $h_i g_i^- \neq h_j g_j^-$ для каждой пары индексов $i, j, 1 \le i \le 4$. Тогда $V_\pi^2 \cap R_\pi^2 \neq \emptyset$.

Доказательство. Поскольку все вершины $v_i, 1 \le i \le 4$, принадлежат множеству V_π^2, верно соотношение $L(M_\pi[q']) \cap L(M_\pi[q'']) \cap L(M_\pi[q''']) \neq \emptyset$. Значит, есть такое слово w, для которого преобразователь π имеет финальные вычисления $q' \xrightarrow{w/s'} p'$, $q'' \xrightarrow{w/s''} p''$ и $q''' \xrightarrow{w/s'''} p'''$. Тогда, по определению LTS Γ_π^2, множество V_π^2 содержит четыре вершины $u_i = (p', (p'', (s')^- h_i\, s''), (p''', (s')^- g_i s'''))$, $1 \le i \le 4$. Если вершина u_1 не является опровергающей, то верно одно из трех равенств: $(s')^-\, h_1\, s'' = e, (s')^- g_1 s''' = e$, or $(s')^- h_1 s'' = (s')^- g_1 s'''$. Не ограничивая общности, рассмотрим лишь случай $(s')^- h_1 s'' = e$ (в двух других случаях рассуждения проводятся аналогичным образом). Так как $h_1 \neq h_2$, справедливо соотношение $(s')^- h_2 s'' \neq e$. Значит, если u_2 не является опровергающей вершиной, то верно одно из двух равенств $(s')^- g_2 s''' = e$ или $(s')^- h_2 s'' = (s')^- g_2 s'''$. Рассмотрим случай $(s')^- g_2 s''' = e$ (те же самые рассуждения можно провести и в случае другого равенства). Так как $h_1 \neq h_3$ и $g_2 \neq g_3$, из равенств $(s')^- h_1 s'' = e$ и $(s')^- g_2 s''' = e$ следует соотношение $(s')^- h_3 s'' \neq e$ и $(s')^- g_3 s''' \neq e$. Поэтому, если u_3 не является опровергающей вершиной, то $(s')^- h_3 s'' = (s')^- g_3 s'''$. Ввиду того, что $h_1 \neq h_4, g_2 \neq g_4$ и $h_3 g_3^- \neq h_4 g_4^-$, мы приходим к заключению, что следствием равенств $(s')^- h_1 s'' = e, (s')^- g_2 s''' = e$ и $(s')^- h_3 s'' = (s')^- g_3 s'''$ являются соотношения $(s')^- h_4 s'' \neq e, (s')^- g_4 s''' \neq e$ и $(s')^- h_4 s'' \neq (s')^- g_4 s'''$. Согласно определению опровергающей вершины, это означает, что $v_4 \in R_\pi^2$. QED

Лемма 9. Предположим, что в LTS Γ_π^2 есть четыре различные вершины $v_i = (q', (q'', g'')), (q'', g_i''')\big)$, $1 \le i \le 4$, удовлетворяющие одному из следующих трех условий:

a) равенство $g_i'' = g_j''$ выполняется для любой пары индексов $i, j,\ 1 \le i < j \le 4$;

b) равенство $g_i''' = g_j'''$ выполняется для любой пары индексов $i, j,\ 1 \le i < j \le 4$;

c) равенство $(g_i'')^- g_i''' = \big(g_j''\big)^- g_j'''$ выполняется для любой пары индексов $i, j,\ 1 \le i < j \le 4$.

Тогда, если опровергающая вершина достижима из вершины v_4, то некоторая вершина также достижима из одной из вершин v_1, v_2, v_3.

Доказательство. Ограничимся рассмотрением случая, когда все вершины удовлетворяют первому из перечисленных условий; аналогичные рассуждения применимы и в случае выполнимости любого из двух других условий.

Предположим, что в LTS Γ_π^2 существует путь, помеченный словом w и позволяющий достичь опровергающую вершину $u_4 = (p', (p'', h''), (p''', h_4'''))$ из вершины v_4. Тогда преобразователь π имеет три таких финальных вычисления $q' \xrightarrow{w/s'} p'$, $q'' \xrightarrow{w/s''} p''$и $q''' \xrightarrow{w/s'''} p'''$, для которых выполняются равенства $h'' = (s')^- g'' s''$ и $h_4''' = (s')^- g_4''' s'''$. Поскольку вершина u_4 является опровергающей, должно быть соблюдено соотношение $h'' \neq e$.

По определению LTS Γ_π^2 для каждого значения индекса $i, 1 \leq i \leq 3$, в этой системе переходов есть путь из вершины v_i в такую вершину $u_i = (p', (p'', h''), (p''', h_i'''))$, для которой имеет место равенство $h_i''' = (s')^- g_i''' s'''$. Если $u_1 \notin R_\pi^2$, то либо $h_1''' = e$, либо $(h'')^- h''' = e$. Проанализируем случай $h_1''' = e$ (в другом случае мы также можем воспользоваться аналогичными рассуждениями). Ввиду того, что $g_2''' \neq g_1'''$ и $g_1''' \neq g_3'''$, верны соотношения $h_2''' \neq e$ и $h_3''' \neq e$. Значит, если $u_2 \notin R_\pi^2$, то $(h'')^- h_2''' = e$. Однако, коль скоро $g_2''' \neq g_3'''$, справедливо соотношение $(h'')^- h_3''' \neq e$, и в результате мы приходим к заключению о том, вершина u_3 является опровергающей. QED

При помощи лемм 8 и 9 можно доказать следующую теорему.

Теорема 4. Если полугруппа S вложим в конечно порожденную разрешимую группу G, то свойство 2-значности конечных преобразователей над полугруппой S разрешимо. Кроме того, если проблема равенства слов в группе G разрешима за полиномиальное время, то и свойство 2-значности конечных преобразователей над S разрешима за полиномиальное время.

Доказательство. Как следует из леммы 7, для проверки 2-значности преобразователя π достаточно провести проверку достижимости опровергающих вершин из стартовой вершины в LTS Γ_π^2. Поиск опровергающих вершин можно проводить методом обхода вершин LTS по стратегии поиска в глубину с возвратом. Обход начинается из стартовой вершины $(q_0, (q_0, e), (q_0, e))$; при этом продвижение в глубину проводится только из значимых вершин, которые определяются на основании леммы 9. Указанный обход вершин LTS Γ_π^2 может быть прерван досрочно, если будет обнаружено, что выполнены условия леммы 8. В этом случае факт достижимости опровергающей вершины устанавливается без явного предъявления пути, ведущего в нее из стартовой вершины.

Предположим, что на некотором этапе предложенного обхода LTS Γ_π^2 была достигнута ранее не встречавшаяся вершина $v = (q', (q'', g''), (q''', g'''))$. Возможны следующие четыре альтернативы.

1) Если вершина v является опровергающей, то обход прекращается, и выносится вердикт о том, что преобразователь π не является 2-значным.

2) В противном случае, если ранее были пройдены 3 значимых вершины $v_i = \left(q', (q'', g_i''), (q''', g_i''')\right)$, $1 \leq i \leq 3$, одного и того же типа, для которых выполняется одно из трех следующих условий:

а) $g'' = g_i''$ для каждого значения индекса i, $1 \leq i \leq 3$;

b) $g''' = g_i'''$ для каждого значения индекса $i,\ 1 \le i \le 3$;

c) $(g'')^- g''' = (g_i'')^- g_i'''$ для каждого значения индекса $i,\ 1 \le i \le 3$,

то вершина v объявляется незначимой, и из нее совершается откат к ее предшественнику в этом обходе.

3) В противном случае, если ранее были пройдены 27 значимых вершин $v_i = (q', (q'', g_i''), (q''', g_i'')), i,\ 1 \le i \le 27$, того же самого типа, что и вершина v, то обход прекращается, и выносится вердикт о том, что преобразователь π не является 2-значным.

4) В противном случае вершина v объявляется значимой, и процедура обхода LTS Γ_π^2 продолжается из этой вершины.

Если процедура обхода завершается в стартовой вершине, преобразователь π признается 2-значным.

Как видно из приведенного описания процедуры обхода, она всегда завершается после посещения не более $27|Q|^3$ значимых вершин LTS Γ_π^2. Лемма 9 обеспечивает гарантию того, что игнорирование незначимых вершин не приводит к потере возможности достичь опровергающую вершину. Это обстоятельство гарантирует полноту нашей процедуры поиска. Чтобы убедиться в корректности этой процедуры нужно показать, что третья альтернатива приводит к правильному решению. Действительно, как следует из простых комбинаторных соображений, если имеются 28 вершин (v и v_i, $1 \le i \le 27$), и из которых никакие четыре вершины не удовлетворяют ни одному из условий леммы 9 (а это объясняется тем, что все пройденные в нашем обходе вершины являются значимыми), то в этом множестве вершин найдутся такие четыре вершины, которые удовлетворяют предпосылкам леммы 8. QED

Обход LTS Γ_π^2 может быть еще более сокращен, если воспользоваться следующей леммой.

Лемма 10. Пусть $q \in \{q', q'', q'''\}$. Предположим, что существует такое входное слово w, принадлежащее множеству слов $L(M_\pi[q']) \cap L(M_\pi[q'']) \cap L(M_\pi[q'''])$, для которого преобразователь π имеет два финальных вычисления $q \xrightarrow{w/s_1} p_1$ и $q \xrightarrow{w/s_2} p_2$, удовлетворяющих соотношению $s_1 \ne s_2$. Тогда если в множестве V_π^2 есть пять вершин $v_i = (q', (q'', g_i), (q''', h_i)), 1 \le i \le 5$, то $V_\pi^2 \cap R_\pi^2 \ne \emptyset$.

Доказательство. Для определенности будем считать, что $q = q'$. Так как все вершины $v_i,\ 1 \le i \le 5$, принадлежат множеству V_π^2, это множество содержит также 10 вершин $u_{1i} = (q', (q', e), (q'', g_i)),\ u_{2i} = (q', (q', e), (q''', h_i)), 1 \le i \le 5$. Коль скоро слово w принадлежит множеству $M_\pi[q']) \cap L(M_\pi[q'']) \cap L(M_\pi[q'''])$, преобразователь π имеет финальные вычисления $q'' \xrightarrow{w/s''} p''$, $q''' \xrightarrow{w/s'''} p'''$. Таким образом, из стартовой вершины LTS Γ_π^2 достижимы следующие 10 вершин: $u_i'' = (p_1, (p_2, s_1^- s_2), (p'', s_1^- g_i s''))$ и $u_i''' = (p_1, (p_2, s_1^- s_2), (p''', s_1^- h_i))$, где $1 \le i \le 5$.

Предположим, что ни одна из вершин $u_i'', u_i''', 1 \le i \le 4$, не является опровергающей. Следует заметить, что $s_1 \neq s_2$, и, следовательно, $s_1^- s_2 \neq e$. Поэтому, по определению опровергающей вершины, для каждого i, $1 \le i \le 4$, элемент g_i группы G либо равен $s_1(s'')^-$, либо равен $s_2(s'')^-$, а элемент h_i либо равен $s_1(s''')^-$, либо равен $s_2(s''')^-$. Принимая во внимание, что вершины $v_i, 1 \le i \le 5$, попарно различны, мы приходим к выводу о том, что ни одно из двух равенств $g_5 = s_1(s'')^-$ и $g_5 = s_2(s'')^-$ не может быть выполнено. Таким образом, $u_5'' = (p_1', (p_2', s_1^- s_2), (p'', s_1^- g_5 s''))$ является опровергающей вершиной, достижимой из стартовой вершины LTS Γ_π^2. QED

Чтобы проверить основное требование предпосылки леммы 10 – существование двух финальных вычислений $q \xrightarrow{w/s_1} p_1$ и $q \xrightarrow{w/s_2} p_2$ с разными образами, – можно воспользоваться алгоритмом проверки свойств функциональности конечных преобразователей. Условия леммы 10 выполнены для состояния q тогда и только тогда, когда проекция преобразователя $\pi[q]$ на конечный автомат, распознающий язык $M_\pi[q']) \cap L(M_\pi[q'']) \cap L(M_\pi[q''']),$ обладает свойством функциональности. Таким образом, алгоритм обхода LTS Γ_π^2, описанный в доказательстве теоремы 4 можно модифицировать, введя следующую дополнительную альтернативу:

3') В противном случае, если ранее были пройдены 4 значимых вершины $v_i = \left(q', (q'', g_i''), (q''', g_i''')\right), 1 \le i \le 4$, одного и того же типа, для которых выполняется условие леммы 10, то обход прекращается, и выносится вердикт о том, что преобразователь π не является 2-значным.

Предложенный метод проверки 2-значности недетерминированности преобразователей – леммы 9, 10 и процедуру поиска опровергающих вершин, описанную в доказательстве теоремы 4, – можно использовать и для проверки -значности конечных преобразователей при любом $k > 1$. В этом случае вершинами LTS служат наборы вида $(q_0, (q_1, h_1), \dots, (q_k, h_k))$, и для проверки достижимости опровергающей вершины в LTS Γ_π^2 достаточно совершить обход не более $\binom{k+1}{2}^{\binom{k+1}{2}} |Q|^{k+1} + 1$ значимых вершин.

6. Проверка эквивалентности двухзначных моделей реагирующих программ

Вместо решения проблемы эквивалентности для конечных преобразователей мы исследуем более общую задачу проверки включения: для заданной пары преобразователей π и π' проверить выполнимость включения $Lab(\pi') \subseteq Lab(\pi)$. Решение этой задачи также проведем на основе размеченных систем переходов.

Пусть задана пара 2-значных преобразователей $\pi = \langle A, S, Q, q_0, F, T\rangle$ и $\pi' = \langle A, S, Q', q_0', F', T'\rangle$. Ясно, что $Lab(\pi') \subseteq Lab(\pi)$ влечет $L(M_{\pi'}) \subseteq L(M_\pi)$. Поэтому проверку включения преобразователей начнем с проверки

включения соответствующих автоматов-подложек, и далее в этом разделе будем считать, не оговаривая этого особо всякий раз, что для анализируемых преобразователей π и π' имеет место включение $L(M_{\pi'}) \subseteq L(M_\pi)$.

Чтобы дать определение LTS $\Gamma^3_{\pi,\pi'}$, соответствующей проблеме включения для преобразователей π и π', нам понадобится ввести вспомогательное понятие блока состояний. Рассмотрим некоторое мультимножество состояний $\hat{Q}$ преобразователя π. *Блоком состояний* в мультимножестве $\hat{Q}$ называется всякое максимальное по включению (т.е. нерасширяемое) подмножество B множества $\hat{Q}$, удовлетворяющее условию $\bigcap_{q\in B} L(M_\pi[q] \neq \emptyset)$, которое подразумевает существование хотя бы одного слова, которое допускается каждым автоматом $M_\pi[q], q \in B$.

LTS $\Gamma^3_{\pi,\pi'} = \langle V, \Rightarrow \rangle$ определяется следующим образом. Множество вершин V образуют всевозможные пары $u = (q', X)$, где $q' \in Q'$, $X = \{(q_1, g_1), \dots, (q_m, g_m)\} \subseteq Q \times G$, и при этом выполнено условие $L(M_{\pi'}\{q'\]) \cap \bigcap_{i=1}^{m} L(M_\pi[q_i]) \neq \emptyset$. Пару $(q', \{q_1, \dots, q_m\})$ будем называть типом вершины u. Для каждой буквы a и пары вершин $u = (q', X)$ и $v = (p', Y)$, имеющих типы (q', B_u) и (p', B_v) соответственно, переход $u \overset{a}{\Rightarrow} v$ возможен тогда и только тогда, когда выполнены следующие требования:

1) в преобразователе π' есть переход $q' \xrightarrow{a/s'} p'$,
2) B_v – это блок состояний в мультимножестве $\hat{Q} = \{\hat{q} : \exists\, q\ (q \in B_u \wedge q \xrightarrow{a/s} \hat{q})\}$,
3) пара (p, h) принадлежит множеству Y в том и только том случае, если $p \in B_v$ и при этом для некоторой пары (q, g) из множества X в преобразователе π есть переход $q \xrightarrow{a/s} p$, для которого верно равенство $h = (s')^- g s$.

Как обычно, для любого заданного слова w мы будем обозначать записью $u \overset{w}{\Rightarrow} v$ композицию соответствующих однобуквенных переходов в LTS. Вершина $v_{src} = (q'_0, \{(q_0, e)\})$ объявляется стартовой вершиной LTS $\Gamma^3_{\pi,\pi'}$. Запись $\mathrm{V}^3_{\pi,\pi'}$ служит обозначением множества всех вершин, достижимых из стартовой вершины v_{src}. Опровергающей вершиной назовем всякую вершину (q', X), в которой $q' \in F'$, и для каждой пары (q, g) из X либо $q \notin F$, либо $g \neq e$. Множество всех опровергающих вершин LTS $\Gamma^3_{\pi,\pi'}$ обозначим записью $\mathrm{R}^3_{\pi,\pi'}$.

Содержательный смысл LTS $\Gamma^3_{\pi,\pi'}$ применительно к задаче проверки включения преобразователей π и π' проясняют следующие утверждения.

Утверждение 1. Пусть w_0 и w_1 – произвольные слова, и $q_0' \xrightarrow{w_0/s_0'} q_1' \xrightarrow{w_1/s_1'} q_2'$ – полное вычисление преобразователя π'. Тогда существует такая вершина $v = (q_1', X)$, что $v_{src} \overset{w_0}{\Rightarrow} v$, и для каждого полного вычисления $q_0 \xrightarrow{w_0/s_0} q_1 \xrightarrow{w_1/s_1} q_2$ преобразователя π мультимножество X содержит пару $(q_1, (s_0')^{-}s_0)$.

Утверждение 2. Предположим, что $v_{src} \overset{w_0}{\Rightarrow} (q_1', X)$. Тогда существует такое слово w_1 и полное вычисление $q_0' \xrightarrow{w_0/s_0'} q_1' \xrightarrow{w_1/s_1'} q_2'$ преобразователя π', что для любого полного вычисления $q_0 \xrightarrow{w_0/s_0} q_1 \xrightarrow{w_1/s_1} q_2$ преобразователя π мультимножество X содержит пару $(q_1, (s_0')^{-}s_0)$.

Оба эти утверждения нетрудно доказать, воспользовавшись индукцией по длине слова w_0 и опираясь лишь на определение отношения переходов $\Rightarrow$ в LTS $\Gamma^3_{\pi,\pi'}$. Здесь нужно особо отметить, что справедливость приведенных утверждений обусловлена тем фактом, что тип каждой вершины связан именно с блоком состояний как максимальным множеством пар, удовлетворяющих определенному условию.

Лемма 11. $Lab(\pi') \subseteq Lab(\pi) \Leftrightarrow \mathrm{V}^3_{\pi,\pi'} \cap \mathrm{R}^3_{\pi,\pi'} = \emptyset$.

Доказательство. Следует из утверждений 1 и 2 на основании определения опровергающей вершины LTS $\Gamma^3_{\pi,\pi'}$. QED

Мы покажем, что даже в том случае, когда множество $\mathrm{V}^3_{\pi,\pi'}$ оказывается бесконечным, нужно исследовать только конечный его фрагмент, чтобы убедиться в (не)достижимости опровергающих вершин.

Рассмотрим произвольную достижимую вершину v типа (q', B). Поскольку π – это 2-значный преобразователь, для каждого его состояния q в мультимножестве B может содержаться не более двух копий состояний q. Поэтому, $|B| \leq 2|Q|$, и общее число типов вершин LTS $\Gamma^3_{\pi,\pi'}$, достижимых из стартовой вершины, не превосходит величины $|Q'|3^{|Q|}$.

Рассмотрим язык $L = L(M_{\pi'}[q']) \cap \bigcap_{q \in B} L(M_{\pi}[q])$; будем называть его языком типа (q', B). По определению LTS $\Gamma^3_{\pi,\pi'}$, этот язык непуст. Семейство типов всех достижимых вершин можно разделить на три класса в зависимости от свойств языка L. Тип (q', B) будет называться A-типом в том случае, когда язык L содержит такое слово w, которое имеет два разных образа s_1' и s_2' в двух финальных вычислениях $q' \xrightarrow{w/s_1'} p_1'$ и $q' \xrightarrow{w/s_2'} p_2'$ преобразователя π'. Тип (q', B) будет называться B-типом в том случае, когда он не относится к классу A, и при этом в мультимножестве B существует такое состояние q, а в языке L найдется такое слово w, которое имеет два разных образа s_1 и s_2 в двух финальных вычислениях $q \xrightarrow{w/s_1} p_1$ и $q \xrightarrow{w/s_2} p_2$ преобразователя π. Все остальные типы будем называть C-типами. Леммы, которые приводятся далее,

раскрывают некоторых характерные свойства этих классов, важные для решения проблемы включения.

Лемма 12. Предположим $Lab(\pi') \subseteq Lab(\pi)$, и пара (q', B) является A-типом. Тогда из стартовой вершины LTS $\Gamma^3_{\pi,\pi'}$ достижимо не более $2^{|B|}$ вершин этого типа.

Доказательство. Рассмотрим язык L типа (q', B), произвольную вершину $v = (q', X)$ типа (q', B), для которой имеется путь $v_{src} \overset{w_0}{\Rightarrow} v$. Пусть (q, g) – произвольная пара из множества X. Так как тип (q', B) является A-типом, в языке L найдется такое слово w, которое имеет два разных образа s'_1 и s'_2 в двух финальных вычислениях $q' \xrightarrow{w/s'_1} p'_1$ и $q' \xrightarrow{w/s'_2} p'_2$ преобразователя π'. По определению языка L, преобразователь π имеет финальное вычисление $q \xrightarrow{w/s} q_1$. Заметим, что элементы s'_1, s'_2 и s группы G зависят только от типа (q', B) и состояния q. Согласно утверждению 2, преобразователи π и π' имеют такие начальные вычисления $q_0 \xrightarrow{w_0/s_0} q$ и $q'_0 \xrightarrow{w_0/s'_0} q'$, для которых верно равенство $g = (s'_0)^- s_0$. Но тогда преобразователь π' имеет два полных вычисления $q'_0 \xrightarrow{w_0/s'_0} q' \xrightarrow{w/s'_1} p'_1$ и $q'_0 \xrightarrow{w_0/s'_0} q' \xrightarrow{w/s'_2} p'_2$, а преобразователь π имеет полное вычисление $q_0 \xrightarrow{w_0/s_0} q \xrightarrow{w/s} q_1$. Принимая во внимание, что преобразователь π является 2-значным, то, что $s'_0 s'_1 \neq s'_0 s'_2$, а также то, что $Lab(\pi') \subseteq Lab(\pi)$, мы можем быть уверены, что справедливо хотя бы одно из равенств $s_0 s = s'_0 s'_1$ или $s_0 s = s'_0 s'_2$. Следовательно, либо $g = s'_1 s^-$, либо $g = s'_2 s^-$. Таким образом, утверждение леммы следует из того факта, что оба возможных значений g зависят только от типа (q', B) и рассматриваемого состояния q. QED

Лемма 13. Предположим, что $Lab(\pi') \subseteq Lab(\pi)$ и пара (q', B) является B-типом. Тогда из стартовой вершины LTS $\Gamma^3_{\pi,\pi'}$ достижимо не более $3^{|B|}$ вершин типа (q', B).

Доказательство. Рассмотрим язык L типа (q', B) и произвольную вершину $v = (q', X)$ типа (q', B), для которой имеется путь $v_{src} \overset{w_0}{\Rightarrow} v$. Пусть (q, g) – произвольная пара из множества X, для которой есть такое слово w из L, что финальные вычисления $q \xrightarrow{w/s_1} p_1$ и $q \xrightarrow{w/s_2} p_2$ преобразователя π дают разные образы слова w. Выберем произвольную пару (p, h) из множества X. Так как $w \in L$, есть хотя бы одно финальное вычисление $p \xrightarrow{w/s} p_3$ и $q' \xrightarrow{w/s'} p'$ у каждого из преобразователей π и π'. Но тогда в силу утверждения 2 мы приходим к следующим выводам. Ввиду включения $Lab(\pi') \subseteq Lab(\pi)$, справедливо в точности одно из равенств $s' = g s_1$ или $s' = g s_2$. Поскольку преобразователь π является 2-значным, справедливо в точности одно из равенств $g s_1 = h s$ или $g s_2 = h s$. Значит, возможен лишь один из трех вариантов равенства: $h = s' s^-$, $h = s' (s_1)^- s_2 s^-$, или $h = s' (s_1)^- s_2 s^-$.

Тогда утверждение леммы следует из того факта, что во всех трех случаях значение h зависит только от типа (q', B) и выбранных состояний q и p. QED

Предположим, что пара (q', B) относится к С-типу, и $B = \{q_1, \dots, q_m\}$, а L – язык этого типа. Будем ассоциировать с типом (q', B) произвольное слово w_0 из множества L. Рассмотрим финальное вычисление $q' \xrightarrow{w_0/s'} p'$ преобразователя π', а также финальные вычисления $q_i \xrightarrow{w_0/s_i} p_i$ преобразователя π для каждого i, $1 \le i \le m$. Набор $(s', s_1, \dots, s_m)$ элементов полугруппы S будем называть w_0-*характеристикой* типа (q', B). Она будет использована для сокращения поиска опровергающих вершин. Допустим, что вершина $u = (q', \{(q_1, g_1), \dots, (q_m, g_m)\})$ является достижимой вершиной С-типа (q', B). Если соотношение $s' \neq g_i s_i$ соблюдается для каждого $i, 1 \le i \le m$, то, по определению LTS $\Gamma^3_{\pi,\pi'}$, опровергающая вершина достижима из вершины u. Тогда мы будем говорить, что вершина u является предопровергающей вершиной типа (q', B). В противном случае множество X можно разбить на два подмножества $X_0 = \{(q_i, g_i) : s' = g_i s_i, 1 \le i \le m\}$ и $X_1 = \{(q_j, g_j) : s' \neq g_j s_j, 1 \le j \le m\}$ и использовать обозначение $(q', X_0 \oplus X_1)$ для такой вершины u. Заметим, что в силу 2-значности преобразователя π, для любых двух пар (q_i, g_i), (q_j, g_j) из X_1 верно равенство $g_i s_i = g_j s_j$.

Лемма 14. Пусть пара (q', B) относится к С-типу, $B = \{q_1, \dots, q_m\}$, и $k = 2m$. Предположим, что из стартовой вершины LTS $\Gamma^3_{\pi,\pi'}$ достижимы $k+1$ вершин $u_1 = (q', X_0 \oplus X_{11}), \dots, u_{k+1} = (q', X_0 \oplus X_{1k+1})$ типа (q', B). Тогда опровергающая вершина достижима из одной из вершин списка $u_1, \dots, u_{k+1}$ в том и только том случае, если опровергающая вершина достижима из какой-либо вершины списка $u_1, \dots, u_k$.

Доказательство. Пусть $(s', s_1, \dots, s_m)$ – характеристика типа (q', B). Предположим, что $X_0 = \{(q_1, g_1), \dots, (q_\ell, g_\ell)\}$ и $X_{1j} = \{(q_{\ell+1}, g_{\ell+1j}), \dots, (q_m, g_{mj})\}$ для каждого j, $1 \le j \le k+1$.

Допустим, что путь $u_{k+1} \overset{w}{\Rightarrow} v$ позволяет достичь опровергающей вершины v для некоторого слова w. Тогда, по определению LTS $\Gamma^3_{\pi,\pi'}$, преобразователь π' имеет финальное вычисление $q' \xrightarrow{w/s'} p'$, и для каждого $i, 1 \le i \le m$, преобразователь π либо не имеет финальных вычислений на слове w из состояния q_i, либо в каждом финальном вычислении $q_i \xrightarrow{w/t_i} p_i$ образ t_i слова w удовлетворяет соотношению $s' \neq g_{ik+1} t_i$ (на самом деле, одно и то же слово может иметь не более двух разных образов t_{i1} и t_{i2} в силу 2-значности преобразователя π). Не умаляя общности мы можем предполагать, что вторая альтернатива осуществляется для каждого состояния $q_i, 1 \le i \le m$. Таким образом, мы располагаем не более чем $2(m-1)$ элементами $t_{i\sigma}$, $\sigma \in \{1,2\}$, полугруппы S, которые являются образами одного и того же слова w для всех возможных финальных вычислений преобразователя π из состояний $q_{\ell+1}, \dots, q_m$.

Если опровергающая вершина недостижима из вершины u_1, то для некоторой пары (q_i, g_{i1}) из X_{11} и для некоторого образа t слова w верно равенство $s' = g_{i1}t$, т.е. $g_{i1} = s't^-$. Заметим, что для всякой другой пары (q_j, g_{j1}) имеет место равенство $g_{i1}s_i = g_{j1}s_j$, т.е. $g_{j1} = s't^-s_is_j^-$. Это означает, что образ t полностью определяет все элементы g_{j1}, $\ell + 1 \le j \le m$, из X_{11}. Ясно, что разные образы слова w определяют разные элементы в различных множествах X_{1i}. Так как число разных образов слова w не превосходит величины $2(m-1) < k$, существует такая вершина u_i, $1 \le i \le k$, для которой соотношение $s' \ne g_{ji}t_{j\sigma}$ соблюдается для каждой компоненты (q_j, g_{ji}) множества X_{1i} и образов $t_{j\sigma}$ слова w. Последнее означает, что опровергающая вершина достижима из этой вершины u_i. QED

Теорема 5. Если полугруппа S может быть вложена в конечно порожденную разрешимую группу G, то проблема включения $Lab(\pi') \subseteq Lab(\pi)$ для 2-значных преобразователей над полугруппой S разрешима.

Доказательство. Поиск опровергающей вершины в LTS $\Gamma^3_{\pi,\pi'}$ представляет собой обход этой системы переходов, начинающийся в стартовой вершине v_{src}. Предположим, что на некотором шаге этот обход достиг ранее не пройденной вершины $u = (q', X)$ типа (q', B). Тогда возможны шесть следующих альтернатив продолжения этого обхода.

1) Если $u \in \mathrm{R}^3_{\pi,\pi'}$, то обход прекращается, и объявляется о том, что преобразователь π не включает преобразователь π' (отношение $Lab(\pi') \subseteq Lab(\pi)$ не выполняется).

2) В противном случае, если тип (q', B) относится к A-типу и ранее были пройдены $2^{|B|}$ вершин того же типа, то обход прекращается и объявляется о том, что преобразователь π не включает преобразователь π'.

3) В противном случае, если тип (q', B) относится к B-типу и ранее были пройдены $3^{|B|}$ вершин того же типа, то обход прекращается и объявляется о том, что преобразователь π не включает преобразователь π'.

4) В противном случае, если тип (q', B) относится к C-типу и вершина u является пред-опровергающей вершиной этого типа, то обход прекращается и объявляется о том, что преобразователь π не включает преобразователь π'.

5) В противном случае, если тип (q', B) относится к C-типу, $u = (q', X_0 \oplus X_1)$, и $2|B|$ вершин вида $u_i = (q', X_0 \oplus X_{1i})$ уже были пройдены ранее, то из вершины u совершается откат к ее предшественнику в этом обходе.

6) В противном случае обход в глубину LTS Γ^2_π продолжается регулярным образом.

Если при обходе происходит окончательный откат в стартовую вершину, то объявляется о том, что справедливо включение $Lab(\pi') \subseteq Lab(\pi)$.

Завершаемость, корректность и полнота описанной процедуры проверки отношения включения для преобразователей вытекает из лемм 11-14. Из описания процедуры обхода видно, что для проверки включения $Lab(\pi') \subseteq$

$Lab(\pi)$ достаточно проанализировать не более $|Q'|8^{|Q|}$ вершин LTS $\Gamma^3_{\pi,\pi'}$. QED

Следствие.

Если полугруппа S может быть вложена в конечно порожденную разрешимую группу G, то проблема эквивалентности для 2-значных преобразователей над полугруппой S разрешима.

7. Сложность разрешающих алгоритмов

Сложность разрешающих алгоритмов существенно зависит от свойств группы G, и, в частности, от сложности разрешения проблемы равенства слов в группе G. Мы ограничимся рассмотрением двух случаев, когда S является свободной полугруппой и свободной коммутативной полугруппой. Сложность предложенных алгоритмов оценивается относительно следующих параметров, характеризующих размер анализируемых преобразователей π' и π'': n – максимальное число состояний преобразователей π' и π'', m – максимальное число переходов в преобразователях π' и π'', ℓ – максимальная длина полугруппового выражения s в переходах $q \xrightarrow{a/s} q'$ преобразователей π' и π''.

Всякая конечно порожденная свободная полугруппа S может быть вложена в свободную группу G с тем же множеством образующих. Каждое выражение g составленное из порождающих элементов свободной группы может быть задано двоичной строкой длины $O(|g|)$.

Всякая конечно порожденная свободная коммутативная полугруппа S может быть вложена в абелеву группу G с тем же множеством образующих. Каждое выражение g составленное из порождающих элементов свободной группы может быть задано двоичной строкой длины $O(\log|g|)$.

Верхние оценки сложности разрешающих алгоритмов будем вычислять, руководствуясь следующей схемой.

1) Оцениваем максимальное число N вершин, которые могут быть пройдены при обходе размеченной системы переходов для проверки анализируемого свойства преобразователей. Это число явно указано в соответствующих разделах 2-5 данной статьи. Вершинами каждой такой LTS являются различные структуры данных, которые включают в себя состояния q преобразователей и элементы g группы G. Очевидно, что все групповые элементы g, встречающиеся в пройденных вершинах LTS, могут быть заданы двоичными строками размера $N_1 = O(\ell N)$ (в том случае, если S – свободная полугруппа) или $N_1 = O(\log \ell N)$ (в том случае, если S – свободная коммутативная полугруппа).
2) Оцениваем максимальное число N_2 переходов из тех вершин LTS, которые должны быть пройдены при ее обходе. Это число зависит от

структур данных, используемых для представления этих вершин. Если a) такая структура данных включает не более r_1 состояний преобразователей, и b) при обходе LTS может быть пройдено не более r_2 вершин с одним и тем же ансамблем состояний $(q_1, \dots, q_{r_1})$, то $N_2 = r_2\, m^{r_1}$.

3) Оцениваем сложность $\varphi(N_1)$ построения отдельного перехода $u \overset{a}{\Rightarrow} v$. Она зависит от a) структур данных, используемых для представления вершин LTS u и v, и b) размера N_1 двоичного представления групповых элементов g, содержащихся в этих структурах данных.

Проведя вычисление указанных параметров, мы можем получить верхнюю оценку $N_2\varphi(N_1)$ сложности по времени верификации свойств ограниченной недетерминированности и эквивалентности конечных преобразователей над полугруппами.

Утверждение 3. Пусть π' и π'' – пара преобразователей над свободной полугруппой S. Предположим, что из стартовой вершины LTS $\Gamma^0_{\pi',\pi''}$ достижима вершина $v = (q', q'', s)$, где $s \notin S$ и $s^- \notin S$. Тогда $\mathrm{V}^0_{\pi',\pi''} \cap R^0_{\pi',\pi''} \neq \emptyset$.

Доказательство. Нетрудно заметить, что если G – свободная группа и $s \notin S$ и $s^- \notin S$, то для любой пары слов h, g из множества A^* верно $h^- sg \neq e$. Поэтому любая вершина $(p', p'', \hat{s})$, достижимая из вершины v, является опровергающей, если хотя бы одно из состояний p', p'' является финальным.

QED

Утверждение 4. Пусть π' и π'' – пара преобразователей над свободной полугруппой S. Предположим, что из стартовой вершины LTS $\Gamma^0_{\pi',\pi''}$ достижима вершина (q', q'', s), где $s \in S$ или $s^- \in S$, и длина выражения s превосходит величину ℓn. Тогда $\mathrm{V}^0_{\pi',\pi''} \cap R^0_{\pi',\pi''} \neq \emptyset$.

Доказательство. Рассмотрим лишь случай $s \in S$. Пусть w – кратчайшее слово, для которого преобразователь π' имеет финальное вычисление $q' \xrightarrow{w/s'} p'$. Очевидно, что длина выражения s не превосходит величины ℓn. Если преобразователь π'' также имеет финальное вычисление $q'' \xrightarrow{w/s''} p''$, то в LTS $\Gamma^0_{\pi',\pi''}$ из вершины (q', q'', s) достижима вершина $u = (q', q'', (s')^- s s'')$. Нетрудно видеть, что $ss'' \in S$, и при этом длина выражения ss'' превосходит величины ℓn. Тогда, как следует из свойств свободной группы G, справедливо соотношение $(s')^- s s'' \neq$ e. Значит, $u \in \mathrm{V}^0_{\pi',\pi''} \cap R^0_{\pi',\pi''}$.

QED

Из этих утверждений и теоремы 1 вытекает

Теорема 6. Проблема эквивалентности детерминированных преобразователей над свободной полугруппой разрешима за время $O(\ell n^3)$.

Доказательство. Из утверждения 3 и 4 следует, что $N_1 = O(\ell n)$. Для детерминированных преобразователей верно $m = O(n)$. Потому $N_2 = O(n^2)$. Каждый переход в LTS $\Gamma^0_{\pi,\pi'}$ можно построить за время $\varphi(N_1) = 2\log n + N_1 = O(n)$. Таким образом, описанная выше схема вычислений дает указанную в теореме оценку сложности. QED

Аналогичным образом может быть доказана

Теорема 7. Проблема эквивалентности детерминированных преобразователей над свободной коммутативной полугруппой разрешима за время $O(n^2\ log\ \ell n)$.

Теорема 8. Свойство функциональности конечных преобразователей над свободной полугруппой можно проверить за время $O(\ell m^2 n^2)$.

Доказательство. Как следует из лемм 3 и 4, для проверки свойства функциональности (однозначности) недетерминированного преобразователя нужно рассмотреть не более $n^2 + 1$ вершин $v = (q_1, q_1', g)$ в LTS $\Gamma^1_{\pi,\pi}$. Поэтому $N = n^2 + 1$ и $N_1 = O(\ell n^2)$. Каждый переход $(q_1, q_1', g_1) \overset{a}{\Rightarrow} (q_1, q_2', g_2)$ в LTS $\Gamma^1_{\pi,\pi}$ можно построить за время $\varphi(N_1) = \log n + N_1 + \ell = O(n^2)$. Нужно отметить, что при построении этих переходов нет необходимости всякий раз проверять условие $L(A_\pi[q_2]) \cap L(A_{\pi'}[q_2']) \neq \emptyset$: верификация проводится «налету» по ходу поиска опровергающей вершины. Таким образом, получается указанная в теореме верхняя оценка сложности $O(\ell\ n^2 m^2)$. QED

Теорема 9. Свойство функциональности конечных преобразователей над свободной коммутативной полугруппой можно проверить за время $O(m^2 \log \ell n)$.

Теорема 10. Свойство k-значности конечных преобразователей над свободной полугруппой можно проверить за время $O((k+1)^{2(k+1)^2}\ell\ m^{k+1} n^{k+1})$.

Доказательство. Хотя в теореме 4 был описан только метод проверки 2-значности конечных преобразователей, его можно применить и для проверки свойства k-значности преобразователей при любом k. Вершинами LTS Γ^2_π являются наборы $v = (q_0, (q_1, h_1), \dots, (q_k, h_k))$, и задача проверки k-значности преобразователей сводится к проверке достижимости опровергающих вершин в LTS Γ^2_π. Для этого достаточно проверить не более $\binom{k+1}{2}^{\binom{k+1}{2}} |Q|^{k+1} + 1$ значимых вершин. Значит, $\mathrm{N}_1 = \ell \binom{k+1}{2}^{\binom{k+1}{2}} n^{k+1}$, $\mathrm{N}_2 = \binom{k+1}{2}^{\binom{k+1}{2}} \mathrm{m}^{\mathrm{k+1}}$, $\varphi(N_1) = O(kN_1)$. Таким образом, мы приходим к указанной и теореме оценке сложности. QED

Оценка сложности в теореме 10 показывает, что предложенный нами алгоритм существенно эффективнее процедуры проверки свойства k-значности конечных преобразователей, описанной в статье [18], которая решает эту задачу за время $O(2^{(k+1)^4}\ell\ m^{k+1} n^{k+1})$.

Теорема 11. Проверку эквивалентности функциональных преобразователей над свободной полугруппой можно провести за время $\ell 2^{O(n)}$.

Доказательство. Отличительная особенность проверки эквивалентности функциональных преобразователей π и π' состоит в том, что вначале нужно проверить равенство $L(A_\pi[q_0]) = L(A_{\pi'}[q_0'])$. Этот предварительный анализ можно провести за время $2^{O(n)}$. Все остальные операции в алгоритме проверки эквивалентности, описанном в теореме 3, можно выполнить за время $O(\ell\, m^2\, n^2)$. QED

Теорема 12. Проблема эквивалентности для 2-значных конечных преобразователей над свободными полугруппами может быть решена за время $\ell\, 2^{O(n \log n)}$.

Доказательство. 1. По теореме 5 для проверки эквивалентности $\pi \sim \pi'$ нужно проверить не более $N = 2^{O(n)}$ вершин в LTS $\Gamma^3_{\pi,\pi'}$. Поэтому $N_1 = \ell\, 2^{O(n)}$.

2. Рассмотрим произвольную тройку вершин v_1, v_2, v_3, являющихся последователями вершины u в LTS $\Gamma^3_{\pi,\pi'}$. Поскольку π и π' являются 2-значными преобразователями, из определения $\Gamma^3_{\pi,\pi'}$ следует, что вершины v_1, v_2, v_3 не могут иметь один и тот же тип. Но поскольку в LTS $\Gamma^3_{\pi,\pi'}$ существует не более $n3^n$ различных типов вершин, приходим к выводу о том, что $N_2 = 2^{O(n)}$.

3. Выделить все возможные блоки состояний можно за время $2^n n^n = 2^{O(n \log n)}$. Как только это сделано, каждый переход в LTS $\Gamma^3_{\pi,\pi'}$ можно построить за время $\varphi(N_1) = O(mN_1)$.

Так мы приходим к оценке сложности, объявленной в теореме. QED

Полученная оценка сложности показывает, что предложенный нами алгоритм существенно эффективнее процедуры проверки эквивалентности 2-значных конечных преобразователей, описанной в статье [20], которая решает эту задачу за время $O(2^{n^6})$.

8. Заключение

В данной статье предложен универсальный подход к решению некоторых задач анализа поведения конечных преобразователей над полугруппами; преобразователи такого вида можно рассматривать как простую модель последовательных реагирующих программ. Предложенный метод основывается на сведении рассматриваемых проблем – задачи проверки k-значности и задачи проверки эквивалентности преобразователей – к хорошо известной задача проверки достижимости заданного класса вершин в конечном ориентированном графе. Фактически, сложность алгоритмов, которые могут быть построены при помощи нашего метода, определяется размером того графа (размеченной системы переходов), который сопоставляется анализируемым преобразователям. Построенные нами алгоритмы имеют более простое устройство и меньшую вычислительную сложность, чем ранее известные алгоритмы решения тех же самых задач.

Есть основания полагать, что полученные в данной статье результаты можно применить и для решения задач минимизации конечных преобразователей над полугруппами и обобщить тем самым ранее известные результаты исследования этой задачи, представленные в статье [15]. Также представляет интерес задача детерминизации конечных преобразователей над полугруппами. В этом случае использование алгебраических особенностей полугрупп, над которыми определяются вычисления преобразователей, может существенно расширить класс однозначных преобразователей, допускающих детерминизацию.

Наконец, как видно из приведенных оценок сложности решения задач проверки свойства -значности преобразователей, предложенный нами метод позволяет решать эту задачу за время, полиномиально зависящее относительно размера проверяемого преобразователя, но при этом экспоненциально зависящее от параметра k. Такой же эффект наблюдается и для разрешающих алгоритмов, описанных в работе [17]. Поэтому при больших значениях параметра k все известные алгоритмы практически непригодны для проверки свойства -значности преобразователей. Поэтому желательно выяснить, какова нижняя оценка того вклада, который привносит параметр k в сложность решения указанной задачи.

Список литературы

[1]. Aho A.V., Hopcroft J.E., Ullman J.D. The design and analysis of computer algorithms. Addison-Wesley, Reading, MA, 1974.

[2]. Aho A.V., Sethi R., Ullman J.D. Compilers: principles, techniques, and tools. Addison-Wesley, Reading, MA, 1986.

[3]. Alur R., Cerny P. Streaming transducers for algorithmic verification of single-pass list-processing programs. Proceedings of 38th ACM SIGACT-SIGPLAN Symposium on Principles of Programming Languages, 2011, p. 599-610.

[4]. Blattner M, Head T. Single-valued a-transducers. Journal of Computer and System Sciences, 1977, v. 15, p. 310-327.

[5]. Blattner M, Head T. The decidability of equivalence for deterministic finite transducers. Journal of Computer and System Sciences, 1979, v. 19, p. 45-49.

[6]. Beal M.-P., Carton O., Prieur C., Sakarovitch J. Squaring transducers: an efficient procedure for deciding functionality and sequentiality. Theoretical Computer Science, 2003, v. 292.

[7]. Culik K., Karhumaki J. The equivalence of finite-valued transducers (on HDTOL languages) is decidable. Theoretical Computer Science, 1986, v. 47, p. 71-84.

[8]. Fischer P.C., Rosenberg A.L. Multi-tape one-way nonwriting automata. Journal of Computer and System Sciences, 1968, v. 2, p. 88-101.

[9]. Griffiths T. The unsolvability of the equivalence problem for ε-free nondeterministic generalized machines. Journal of the ACM, 1968, v. 15, p.409-413.

[10]. Gurari, E., Ibarra, O. A note on finite-valued and finitely ambiguous transducers. Mathematical Systems Theory, 1983, v. 16, p. 61–66.

[11]. Ibarra O. The unsolvability of the equivalence problem for Efree NGSM's with unary input (output) alphabet and applications. SIAM Journal on Computing, 1978, v. 4.

[12]. Malcev, A. I. Uber die Einbettung von assoziativen Systemen. Gruppen, Rec. Math. (Mat. Sbornik) N.S., 1939, v. 6, p. 331–336.
[13]. Malcev, A. I. Uber die Einbettung von assoziativen Systemen. Gruppen. II, Rec. Math. (Mat. Sbornik) N.S., 1940, v. 8, p. 251–264.
[14]. Mohri M. Finite state transducers in language and speech processing. Computer Linguistics, 1997, v. 23, N 2.
[15]. Mohri M. Minimization algorithms for sequential transducers. Theoretical Computer Science, 2000, v. 234, p. 177-201.
[16]. Nerode A., Kohn W. Models for hybrid systems: automata, topology, controllability, observability. Cornell University, Technical Report 93-28, 1993, MIT Press, Cambridge.
[17]. Sakarovitch J., de Souza R. On the decomposition of k-valued rational relations. Proceedings of 25th International Symposium on Theoretical Aspects of Computer Science, 2008, p.621-632.
[18]. Sakarovitch J., de Souza R. On the decidability of bounded valuedness for transducers. Proceedings of the 33rd International Symposium on Mathematical Foundations of Computer Science, 2008, p. 588-600.
[19]. Schutzenberger M. P. Sur les relations rationnelles. Proceedings of Conference on Automata Theory and Formal Languages, 1975, p. 209-213.
[20]. de Souza R. On the decidability of the equivalence for k-valued transducers. Proceedings of 12th International Conference on Developments in Language Theory, 2008, p. 252-263.
[21]. Veanes M., Hooimeijer P., Livshits B., et al. Symbolic finite state transducers: algorithms and applications. Proceedings of the 39th ACM SIGACT-SIGPLAN Symposium on Principles of Programming Languages, 2012.
[22]. Weber A. On the valuedness of finite transducers. Acta Informatica, 1989, v. 27, p. 749–780.
[23]. Weber A. Decomposing finite-valued transducers and deciding their equivalence. SIAM Journal on Computing, 1993, v. 22, p. 175-202.
[24]. Zakharov V.A. An efficient and unified approach to the decidability of equivalence of propositional program schemes. Proceedings of the 25th International Colloquium "Automata, Languages and Programming", 1998, p. 247-258.

Modeling and Analysis of the Behavior of Successive Reactive Programs

V.A. Zakharov <zakh@cs.msu.su>
Institute for System Programming Russian Academy of Science,
109004, A. Solzhenitsina, 25, Moscow, Russia;
Higher School of Economics National Research University,
101000, Myasnitskaya, 20, Moscow, Russia

Annotation. Finite state transducers extend the finite state automata to model functions on strings or lists. They may be used also as simple models of sequential reactive programs. These programs operate in the interaction with the environment permanently receiving data (requests) from it. At receiving a piece of data such program performs a sequence of actions.

When certain control points are achieved a program outputs the current results of computation as a response. It is significant that different sequences of actions may yield the same result. Therefore, the basic actions of a program may be viewed as generating elements of some appropriate semigroup, and the result of computation may be regarded as the composition of actions performed by the program. This paper offers an alternative technique for the analysis of finite state transducers over semigroups. To check the equivalence of transducers $\boldsymbol{\pi_1}$ and $\boldsymbol{\pi_2}$ we associate with them a Labeled Transition Systems $\boldsymbol{\Gamma_{\pi_1,\pi_2}}$. Each path in this LTS represents all possible runs of $\boldsymbol{\pi_1}$ and $\boldsymbol{\pi_2}$ on the same input word. Every node of $\boldsymbol{\Gamma_{\pi_1,\pi_2}}$ keeps track of the states of $\boldsymbol{\pi_1}$ and $\boldsymbol{\pi_2}$ achieved at reading some input word and the deficiency of the output words computed so far. If both transducers reach their final states and the deficiency of their outputs is nonzero then this indicates that $\boldsymbol{\pi_1}$ and $\boldsymbol{\pi_2}$ produce different images for the same word, and, hence, they are not equivalent. The nodes of $\boldsymbol{\Gamma_{\pi_1,\pi_2}}$ that capture this effect are called rejecting nodes. Thus, the equivalence checking of $\boldsymbol{\pi_1}$ and $\boldsymbol{\pi_2}$ is reduced to checking the reachability of rejecting nodes in LTS $\boldsymbol{\Gamma_{\pi_1,\pi_2}}$. We show that one needs to analyze only a bounded fragment of $\boldsymbol{\Gamma_{\pi_1,\pi_2}}$ to certify (un)reachability of rejecting nodes. The size of this fragment is polynomial of the size of $\boldsymbol{\pi_1}$ and $\boldsymbol{\pi_2}$ if both transducers are deterministic, and single-exponential if they are k-bounded. The same approach is applicable for checking k-valuedness of transducers over semigroups.

Keywords: reactive program; finite state transducer; semigroup; Labelled Transition System; equivalence checking; k-valuedness; decision procedure; complexity.

DOI: 10.15514/ISPRAS-2015-27(2)-13

For citation: Zakharov V.A. Modeling and Analysis of the Behavior of Successive Reactive Programs. *Trudy ISP RAN/Proc. ISP RAS*, vol. 27, issue 2, 2015, pp. 221-250 (in Russian). DOI: 10.15514/ISPRAS-2015-27(2)-13.

References

[1]. Aho A.V., Hopcroft J.E., Ullman J.D. The design and analysis of computer algorithms. Addison-Wesley, Reading, MA, 1974.

[2]. Aho A.V., Sethi R., Ullman J.D. Compilers: principles, techniques, and tools. Addison-Wesley, Reading, MA, 1986.

[3]. Alur R., Cerny P. Streaming transducers for algorithmic verification of single-pass list-processing programs. Proceedings of 38th ACM SIGACT-SIGPLAN Symposium on Principles of Programming Languages, 2011, p. 599-610.

[4]. Blattner M, Head T. Single-valued a-transducers. Journal of Computer and System Sciences, 1977, v. 15, p. 310-327.

[5]. Blattner M, Head T. The decidability of equivalence for deterministic finite transducers. Journal of Computer and System Sciences, 1979, v. 19, p. 45-49.

[6]. Beal M.-P., Carton O., Prieur C., Sakarovitch J. Squaring transducers: an efficient procedure for deciding functionality and sequentiality. Theoretical Computer Science, 2003, v. 292.

[7]. Culik K., Karhumaki J. The equivalence of finite-valued transducers (on HDTOL languages) is decidable. Theoretical Computer Science, 1986, v. 47, p. 71-84.

[8]. Fischer P.C., Rosenberg A.L. Multi-tape one-way nonwriting automata. Journal of Computer and System Sciences, 1968, v. 2, p. 88-101.

[9]. Griffiths T. The unsolvability of the equivalence problem for ε-free nondeterministic generalized machines. Journal of the ACM, 1968, v. 15, p.409-413.
[10]. Gurari, E., Ibarra, O. A note on finite-valued and finitely ambiguous transducers. Mathematical Systems Theory, 1983, v. 16, p. 61–66.
[11]. Ibarra O. The unsolvability of the equivalence problem for Efree NGSM's with unary input (output) alphabet and applications. SIAM Journal on Computing, 1978, v. 4.
[12]. Malcev, A. I. Uber die Einbettung von assoziativen Systemen. Gruppen, Rec. Math. (Mat. Sbornik) N.S., 1939, v. 6, p. 331–336.
[13]. Malcev, A. I. Uber die Einbettung von assoziativen Systemen. Gruppen. II, Rec. Math. (Mat. Sbornik) N.S., 1940, v. 8, p. 251–264.
[14]. Mohri M. Finite state transducers in language and speech processing. Computer Linguistics, 1997, v. 23, N 2.
[15]. Mohri M. Minimization algorithms for sequential transducers. Theoretical Computer Science, 2000, v. 234, p. 177-201.
[16]. Nerode A., Kohn W. Models for hybrid systems: automata, topology, controllability, observability. Cornell University, Technical Report 93-28, 1993, MIT Press, Cambridge.
[17]. Sakarovitch J., de Souza R. On the decomposition of k-valued rational relations. Proceedings of 25th International Symposium on Theoretical Aspects of Computer Science, 2008, p.621-632.
[18]. Sakarovitch J., de Souza R. On the decidability of bounded valuedness for transducers. Proceedings of the 33rd International Symposium on Mathematical Foundations of Computer Science, 2008, p. 588-600.
[19]. Schutzenberger M. P. Sur les relations rationnelles. Proceedings of Conference on Automata Theory and Formal Languages, 1975, p. 209-213.
[20]. de Souza R. On the decidability of the equivalence for k-valued transducers. Proceedings of 12th International Conference on Developments in Language Theory, 2008, p. 252-263.
[21]. Veanes M., Hooimeijer P., Livshits B., et al. Symbolic finite state transducers: algorithms and applications. Proceedings of the 39th ACM SIGACT-SIGPLAN Symposium on Principles of Programming Languages, 2012.
[22]. Weber A. On the valuedness of finite transducers. Acta Informatica, 1989, v. 27, p. 749–780.
[23]. Weber A. Decomposing finite-valued transducers and deciding their equivalence. SIAM Journal on Computing, 1993, v. 22, p. 175-202.
[24]. Zakharov V.A. An efficient and unified approach to the decidability of equivalence of propositional program schemes. Proceedings of the 25th International Colloquium "Automata, Languages and Programming", 1998, p. 247-258.