Модел. и анализ информ. систем. Т. **17**, № **3** (2010) 29–37

УДК 681.3+519.68

Составные редукции моделей Крипке и автоморфизмы

Белов Ю.А.[1]

Ярославский государственный университет им. П.Г. Демидова

e-mail: belov45@yandex.ru

получена 22 марта 2010

Ключевые слова: Модель Крипке, фактор-модель, автоморфизмы модели Крипке

Показано, что с помощью понятия фактор-модели, предложенного в [1], произвольные модели Крипке могут быть представлены в виде композиции моделей с простыми группами автоморфизмов. Доказано также, что любая конечная группа изоморфна группе автоморфизмов некоторой подходящей модели Крипке.

Определения

Модель Крипке (МК) можно считать специализированной системой переходов, являющейся инструментом верификации распределённых программных систем. При этом актуальной является проблема редукции получающейся модели. В качестве одного из способов редукции можно использовать группу автоморфизмов МК для построения фактор-модели. При этом получающаяся фактор-модель имеет меньшее количество состояний, чем исходная модель, но бисимулярна ей. Такой подход изложен, например, в [1].

В данной работе приводятся некоторые замечания по возможному развитию этого подхода на составные редукции и даются соображения, касающиеся сложности возникающих задач. Сначала напомним исходные определения, в основном опираясь на [1], вводя далее по необходимости дополнительные конструкции и отмечая промежуточные факты.

Моделью Крипке над конечным множеством атомарных высказываний AP называется четвёрка $M = (S, S_0, R, f)$, в которой:

S – конечное множество состояний системы;

$S_0 \subseteq S$ – подмножество начальных состояний;

[1]Работа проводилась при финансовой поддержке госконтракта 02.740.11.0207, ФЦП "Научные и научно-педагогические кадры инновационной России на 2009 – 2013 годы".

$R \subseteq S \times S$ – отношение переходов, которое должно быть тотальным, то есть для любого $s \in S$ должно существовать такое $s' \in S$, что $(s, s') \in R$;

$f : S \to 2^{AP}$ – функция, отмечающая все атомарные высказывания, истинные в данном состоянии.

Принадлежность $(s, s') \in R$ часто записывается более наглядно: $s \to s'$ или $s \xrightarrow{R} s'$, если требуется явно указать отношение R.

Иногда множество S_0 не участвует в каких-то рассмотрениях, тогда оно пропускается и в определении МК.

Автоморфизмом модели Крипке M называется биективное отображение $g : S \to S$, если из того, что $s_1, s_2 \in S$ и $(s_1, s_2) \in R$ следует, что $(g(s_1), g(s_2)) \in R$.

Другими словами, автоморфизм модели есть подстановка g на множестве S состояний МК, такая что индуцированная подстановка на множестве S^2 пар элементов из S оставляет инвариантным подмножество R, то есть $g(R) \subseteq R$. В силу биективности g и конечности S и S^2 тогда, очевидно, получается, что $g(R) = R$.

Свойства, требуемые в определении автоморфизма, называются ещё прямым и обратным свойствами переноса: а именно – говорят, что отображение $g : S \to S$ обладает прямым свойством переноса, если из того, что $s \to s'$, следует, что $g(s) \to g(s')$; говорят, что отображение g обладает обратным свойством переноса, если из того, что $g(s) \to g(s')$, следует, что $s \to s'$.

Конечно, можно аналогично определить отображение со свойствами переноса и в более общем случае, когда состояния одной модели однозначно отображаются на состояния другой модели. Некоторые усложнения возникают при этом лишь из-за неоднозначности прообразов. Далее соответствующее определение будет приведено.

Отметим ещё, что для модели Крипке, если отображение $g : S \to S$ является сюръекцией с прямым свойством переноса, то, в силу конечности S, отображение g будет биекцией, обладать обратным свойством переноса и являться, таким образом, автоморфизмом.

Условимся записывать действие произведения автоморфизмов следующим образом: $(g_1 \circ g_2)(s) = g_2(g_1(s))$; это не вполне логично, но соответствует стандарту функциональных обозначений.

В исходном определении автоморфизма не упоминается функция разметки f, учёт которой будет необходим для построения фактор-модели. В связи с этим напомним ещё определение. Атомарное высказывание $p_0 \in AP$ называется инвариантным (является инвариантом) относительно автоморфизма g, если $\forall s \in S$ $(f(s) = f(g(s)))$.

Несколько переформулируем данное определение. Хотя f задаётся как отображение из S в 2^{AP}, нам потребуется также представлять данную информацию как отображение из множества AP в множество 2^S. Тогда каждому атомарному высказыванию сопоставляется его область истинности: $I(p) = \{s \in S : p \in f(s)\}$, то есть множество тех состояний, в которых p истинно. С использованием этого понятия можно сказать, что высказывание $p_0 \in AP$ является **инвариантом** автоморфизма g, если $g(I(p_0)) \subseteq I(p_0)$ (а тогда, в силу биективности g и конечности S, получаем $g(I(p_0)) = I(p_0)$).

Для данного $p_0 \in AP$ можно рассмотреть группу автоморфизмов G, для всех элементов которой p_0 является инвариантом. Тогда группа G называется группой

инвариантности высказывания p_0. Это понятие потребуется нам для построения корректной фактор-модели МК.

Сначала напомним понятие орбиты (см.[10]). Если имеется группа перестановок G на множестве S, то на S определяется отношение эквивалентности ϵ: $(s, s') \in \epsilon \Longleftrightarrow \exists g \in G : g(s) = s'$. То есть два элемента из S считаются эквивалентными (симметричными) относительно G, если существует подстановка из G, отображающая один элемент в другой. В силу того, что G является группой, легко проверяется, что ϵ действительно является отношением эквивалентности на S и потому генерируется фактор-множество S/ϵ, элементами которого являются классы эквивалентных элементов из S, называемые орбитами (относительно группы G). Таким образом, орбита есть объединение всех симметричных элементов.

Орбита, содержащая данное состояние $s \in S$, есть множество всех состояний, ему симметричных: $G(s) = \{g(s) | \ g \in G\}$. Ясно, что количество элементов в фактор-множестве $S_G = S/\epsilon$, то есть количество орбит, вообще говоря, меньше, чем количество элементов в исходном множестве S. При этом, чем больше группа автоморфизмов, тем больше элементов в каждой орбите и тем меньше общее количество орбит, то есть количество элементов в фактор-множестве $S_G = \bar{S}$.

Имеется так называемое **естественное** отображение – сюръекция $\pi : S \to S_G$, сопоставляющая каждому элементу из S ту орбиту, которой он принадлежит. Другими словами, $\pi(s) = G(s), \forall s \in S$. Иногда придётся уточнять, что естественное отображение построено с использованием группы G, и это будет записываться так: $\pi_G(s)$; когда возможно, будет использоваться краткая запись: $\pi(s) = \bar{s}$. Если имелась исходная модель Крипке с множестовм состояний S и если возможно построить МК на основе S_G, бисимулярную исходной, то это и будет корректная редукция исходной модели.

Дадим соответствующее определение.

Пусть имеется модель Крипке $M = (S, R, f)$ над множеством атомарных высказываний AP. G – группа автоморфизмов M, для которой все высказывания из AP являются инвариантами. Тогда, в силу инвариантности $I(p)$ относительно всех автоморфизмов из группы G, справедливо замечание.

Предложение 1. Пусть для модели Крипке M имеется группа автоморфизмов G, для которой все высказывания из данного множества AP являются инвариантами. Тогда для любого $p \in AP$ область истинности $I(p)$ есть объединение нескольких орбит группы G. ■

То есть можно сказать, что область истинности высказывания состоит из нескольких элементов фактор-множества S_G, и, значит, в этом случае высказывания из AP можно рассматривать и на множестве S_G

Тогда определим понятие **фактор-модели** M_G следующим образом.

$M_G = (S_G, R_G, f_G)$ – МК с множеством состояний S_G, определённым ранее. Множество R_G есть образ R при естественном отображении: $R_G = \pi(R) = \{(\pi(s), \pi(s')) : (s, s') \in R\}$.

Разметка определяется «по представителям» следующим образом: $f_G(\pi(s)) = f(s)$. Легко проверить, что если $\pi(s) = \pi(s')$, то $f(s) = f(s')$. Это означает, что данное определение однозначно, то есть не зависит от выбора представителя из класса $\pi(s)$.

Конечно, совершенно аналогично можно определить понятие фактор-модели на основе любого отношения эквивалентности, определённого на множестве состояний S. Единственное условие корректности определения состоит в том, чтобы для $\forall p \in AP$ область истинности $I(p)$ состояла ровно из нескольких классов эквивалентности (что в нашем случае обеспечивается предложением 1).

Далее требуется определение бисимулярности двух моделей Крипке. Пусть имеется две МК: $M = (S, R, f)$ и $L = (V, W, h)$ с одним и тем же множеством атомарных высказываний AP.

$B \subseteq S \times V$ называется **соответствием (отношением) бисимуляции** между M и L, если для любой пары состояний $(s, v) \in B$ выполнены условия:

1. $f(s) = h(v)$;

2. Если $s_1 \xrightarrow{R} s_2$, и $(s_1, v_1) \in B$, то найдётся такое состояние $v_2 \in V$, что $(s_2, v_2) \in B$ и $v_1 \xrightarrow{W} v_2$.

3. С другой стороны, аналогично, если $v_1 \xrightarrow{W} v_2$ и $(s_1, v_1) \in B$, то найдётся такое состояние $s_2 \in S$, что $s_1 \xrightarrow{R} s_2$ и $(s_2, v_2) \in B$.

Таким боразом, в определении бисимуляции рассматриваются те же ранее упомянутые свойства переноса, только для соответствий, а не для отображений.

Понятие корректного (то есть сохраняющего бисимулярность) слияния позиций для сетей Петри было определено и изучено в [3] с помощью языка бинарных соответствий.

В работе [5] было дано общее определение корректной редукции и корректного отображения для произвольных систем переходов. В этой же заметке были указаны достаточные условия для корректности отображения одной системы на другую. Понятие корректного отображения представляется более наглядным (чем бинарные соответствия), оно соответствует классическому понятию гомоморфизма конечных автоматов (см. [8]) и облегчает использование алгебраических методов (см. [2]).

Напомним соответствующие определения.

Система помеченных переходов (labeled transitions systems LTS) – это тройка $D = \langle S, L, T \rangle$, где S – произвольное абстрактное множество, называемое множеством состояний. L – множество меток (имен) переходов, $T \subseteq S \times L \times S$ – множество переходов. Элементы из T записываются в следующем виде: $s \xrightarrow{l} s'$, если $(s, l, s') \subseteq T$ и читаются так: система D из состояния s под действием перехода с именем l перешла в состояние s'.

Для модели Крипке $M = (S, R, f)$ также имеются состояния и переходы. Отличие от LTS только в том, что для МК каждое состояние s сопровождается множеством высказываний $f(s)$, истинных в данном состоянии, и необходимо отслеживать инвариантность этого множества при автоморфизмах.

Понятие бисимуляции LTS определяется точно так же, как и для МК. Пусть имеются две системы $D = \langle S_1, L, T_1 \rangle$ и $H = \langle S_2, L, T_2 \rangle$ с одинаковым множеством L имен переходов. Бинарное отношение $R \subseteq S_1 \times S_2$ является **отношением бисимуляции**, если для любой пары $(s, q) \in R$ из того, что $s \xrightarrow{l} s'$ в D следует, что в H существует переход с той же меткой l вида $q \xrightarrow{l} q'$, при котором $(s', q') \in R$. Аналогично, если $q \xrightarrow{l} q'$ в H, то в D найдется переход $s \xrightarrow{l} s'$ с той же меткой l,

при котором $(s', q') \in R$.

Упоминавшиеся ранее свойства переноса для отображений в общем виде определяются следующим образом. Пусть заданы две системы переходов - $D = \langle S_1, L, T_1 \rangle$ и $H = \langle S_2, L, T_2 \rangle$ и пусть f – отображение S_1 на S_2. Говорим, что f имеет **прямое свойство переноса**, если из того, что в D существует переход $s \xrightarrow{l} s'$ следует, что в H существует переход $f(s) \xrightarrow{l} f(s')$ с той же меткой l. Говорим, что f имеет **обратное свойство переноса**, если из того, что в H имеется переход $f(s) \xrightarrow{l} f(s')$ для некоторых $s, s' \in S_1$, следует, что существуют такие состояния $\tilde{s}, \tilde{s}'$, что: $f(\tilde{s}) = f(s)$, $f(\tilde{s}') = f(s')$ и переход $\tilde{s} \xrightarrow{l} \tilde{s}'$ в D.

Естественно предположить, что если f имеет прямое и обратное свойство переноса, то множество пар $\{(s, f(s))|\ s \in S\}$ задаёт отношение бисимуляции (такие отображения называются корректными). Для биекций это действительно справедливо, для произвольных отображений требуется подправить пары, участвующие в обратном отношении переноса. Точные формулировки следующие.

Пусть даны две LTS: D и H. Сюръекция $f : S_1 \to S_2$ называется **корректным** отображением, если для любого $s \in S_1$ имеется соотношение: $(D, s) \cong (H, f(s))$. Напомним, что частный случай корректного отображения – корректное слияние для сетей Петри, было предложено в [3].

Имеется следующий критерий корректности:([5]):

Пусть D и H – две системы помеченных переходов. Пусть f – отображение S_1 на S_2. Тогда, если f имеет оба свойства переноса и прообразы f состоят из бисимулярных состояний, то f – корректно.

Две системы $D = \langle S_1, L, T_1 \rangle$ и $H = \langle S_2, L, T_2 \rangle$ D и H называются **бисимулярными при начальных состояниях** $s_{01} \in S_1$ и $s_{02} \in S_2$ (обозначение: $(D, s_{01}) \cong (H, s_{02})$), если существует такое отношение бисимуляции R, что $(s_{01}, s_{02}) \in R$. Если $D = H$ и из контекста ясно, какая система рассматривается, можно употреблять запись вида $s \cong s'$ и говорить, что состояния s и s' бисимулярны. Например:

Предложение 2. Пусть M – модель Крипке, g_0 – некоторый автоморфизм, для которого все высказывания из AP являются инвариантами. Тогда для любого $s \in S$ выполнено соотношение $s \cong g_0(s)$. ■

По поводу приведённого предложения можно уточнить, что для каждого $g_0 \in G$ множество $B_{g_0} = \{(s, g_0(s))|s \in S\}$ задаёт отношение бисимуляции на M, то есть все пары лежат даже в одном бисимуляционном отношении.

Если корректное отображение f является биекцией, то тогда системы D и H являются **изоморфными** (см. [2, 8]). Конечно, одна система может быть бисимулярна другой, но не изоморфной. Корректная фактор-система как раз и даёт пример системы, бисимулярной исходной, но меньшей размерности.

Отметим, что, как легко проверить, корректная биекция системы на себя является автоморфизмом и обратно.

Результаты

Используя определения и обозначения, введённые ранее, можно формулировать и доказывать следующие утверждения.

Предложение 3 [1]. Пусть имеется модель Крипке $M = (S, R, f)$ над множеством атомарных высказываний AP. G – группа автоморфизмов M, для которой все высказывания из AP являются инвариантами, M_G – соответствующая фактор-модель. Тогда естественное отображение $\pi : S \to S_G$ является корректным, то есть для любого $s \in S$ выполнено соотношение бисимулярности: $(M, s) \cong (M_G, \pi(s))$.

Доказательство. Легко проверить, что естественное отображение $\pi : S \to S_G$ удовлетворяет и условиям переноса и бисимулярности прообразов.

Например, проверим свойство бисимулярности прообразов. Пусть $\pi(s_1) = \pi(s_2)$. Тогда, согласно определению ϵ, существует такой автоморфизм $g_0 \in G$, что $s_2 = g_0(s_1)$. Тогда, согласно предложению 2, получаем $s_1 \cong g_0(s_1) = s_2$, что и требовалось.

Таким образом, выполнены все условия применимости критерия корректности и предложение 3 доказано. ■

Конечно, для моделей Крипке это можно проверить непосредственно, как в [1]. Для систем с бесконечным числом состояний ситуация сложнее.

Теорема 1. Пусть M – модель Крипке, имеющая группу автоморфизмов G, для которой все высказывания из множества AP являются инвариантами и пусть $H \lhd G$ – нормальный делитель группы G (см.[10]). Тогда

- фактор-группа G/H является группой автоморфизмов фактор-модели M_H с действием $\bar{g}(\bar{s}) = \overline{g(s)}$, где $\bar{g} \in G/H$, $\bar{s} \in S_H$, при этом все высказывания из AP являются инвариантами для элементов группы G/H;

- фактор-модель $(M_H)_{G/H}$ фактор-модели M_H изоморфна фактор-модели M_G с изоморфизмом, определяемым правилом $\forall s \in S\ G(s) \to (\pi_H \circ \pi_{G/H})(s) = \pi_{G/H}(\pi_H(s))$.

Доказательство. Сначала проверим, что указанное в теореме действие фактор-группы G/H на элементы фактор-множества S_H определено однозначно, то есть не зависит от выбора элементов из смежного класса $\bar{g}$ и элементов из класса эквивалентности $\bar{s}$. Действительно, пусть $\bar{g} = \bar{g}_1$ и $\bar{s} = \bar{s}_1$. Тогда, по определению смежного класса по подгруппе H, можно сказать, что g отличается от g_1 на множитель из H, то есть $g_1 = g \circ h$, и, по определению орбиты, $s_1 = h'(s)$, где $h, h' \in H$. Тогда $g_1(s_1) = (g \circ h)(h'(s)) = (h' \circ g \circ h)(s)$. Тогда, учитывая, что H является в G нормальным делителем, можно записать $h' \circ g \circ h = g \circ g^{-1} \circ h' \circ g \circ h = g \circ \tilde{h}$. Поэтому $g_1(s_1) = (g \circ \tilde{h})(s) = \tilde{h}(g(s))$; это означает, что $g_1(s_1)$ и $g(s)$ принадлежат одной орбите и, следовательно, действие фактор-группы на фактор-множестве однозначно.

Свойства переноса (то есть автоморфности) для элементов группы G/H проверяются также непосредственно. Например, проверим прямое свойство переноса. Пусть $\bar{s} \to \bar{s}'$, и $\bar{g} \in G/H$. Тогда, по определению отношения переходов в фактор-модели, можно утверждать, что существуют такие $s_1, s_2 \in S$, что $\bar{s}_1 = \bar{s}$, $\bar{s}_2 = \bar{s}'$ и $s_1 \to s_2$. Тогда, по определению орбит по подгруппе H, можно отметить, что $s_1 = h_1(s)$, $s_2 = h_2(s')$, а по свойству переноса в исходной модели получим $h_1^{-1}(s_1) = s \to h_1^{-1}(s_2) = h_1^{-1}(h_2(s'))$. Далее, применив автоморфизм g, получим: $g(s) \to g(h_1^{-1}(s_2)) = \tilde{h}(g(s'))$. Последнее равенство справедливо в силу того, что H является нормальным делителем в G. Теперь, заметив, что $\overline{\tilde{h}(g(s'))} = \overline{g(s')}$ и

что естественное отображение имеет оба свойства переноса, получаем окончательно $\overline{g(s)} \to \overline{g(s')}$. Свойство обратного переноса проверяется аналогично.

Проверим, что все высказывания из AP являются инвариантами для автоморфизмов из G/H. Итак, пусть $\bar{g} \in G/H$, $\bar{s} \in S_H = \overline{S}$. Докажем,что $f_H(\bar{s}) = f_H(\bar{g}(\bar{s}))$. По определению f_H имеем $f_H(\bar{s}) = f(s)$ и это определение не зависит от выбора представителя из орбиты $\bar{s}$, как отмечалось в определении фактор-модели. Аналогично, а также используя уже доказанный пункт теоремы, получаем $f_H(\bar{g}(\bar{s})) = f_H(\overline{g(s)}) = f(g(s))$. В силу инвариантности высказываний из AP относительно элементов из G, имеем $f(s) = f(g(s))$ и, таким образом, первое утверждение теоремы установлено.

Доказательство второго утверждения можно было бы провести непосредственно, проверив, что указанное в формулировке теоремы отображение действительно является изоморфизмом, но для упрощения этого процесса используем стандартную теорему об эпиморфизме, доказанную для систем переходов в [7]:

Пусть $D = \langle S_1, L, T_1 \rangle$ и $H = \langle S_2, L, T_2 \rangle$ – две системы переходов, $f : S_1 \to S_2$ – сюръекция. Тогда, если f имеет прямое и обратное свойства переноса, то D/f и H изоморфны и f является суперпозицией естественного отображения D на D/f и изоморфизма между D/f и H.

Для применения этой теоремы рассмотрим такое отображение α модели M на $(M_H)_{G/H}$: $\forall s \in S\ s \to (\pi_H \circ \pi_{G/H})(s) = \pi_{G/H}(\pi_H(s))$. Данное отображение является суперпозицией двух естественных отображений. Согласно предложению 3 естественное отображение удовлетворяет обоим свойствам переноса и бисимулярности прообразов. Тогда и суперпозиция α также будет обладать всеми этими свойствами. Тогда, согласно указанной теореме об эпиморфизме, фактор-модель M/α изоморфна модели $(M_H)_{G/H}$. Остаётся только доказать, что фактор-модель M/α есть, в действительности, фактор-модель M_G. Для этого достаточно доказать, что прообраз каждого элемента $s \in S$ при отображении α (то есть состояние из M/α) есть орбита этого элемента относительно группы G: $\alpha^{-1}(s) = G(s)$. Другими словами, требуется доказать, что $\alpha(s_1) = \alpha(s_2) \Longleftrightarrow \exists g \in G :\ s_1 = g(s_2)$. Пусть, например, $\alpha(s_1) = \alpha(s_2)$. Тогда, по определению α, имеются равенства $\pi_{G/H}(\pi_H(s_1)) = \pi_{G/H}(\pi_H(s_2))$, или $\pi_{G/H}(\overline{s_1}) = \pi_{G/H}(\overline{s_2})$. Это, в свою очередь, означает, что $\bar{s_1} = \bar{g}(\bar{s_2})$ для некоторого $\bar{g} \in G/H$. Но $\bar{g}(\bar{s_2}) = \overline{g(s)}$, согласно первому пункту теоремы. Последнее равенство означает, что $s_1 = h(g(s_2))$, то есть элементы s_1 и s_2 принадлежат одной орбите относительно группы G. Аналогично проводится доказательство в обратную сторону. ■

Из полученной теоремы можно получить следствие, возможно, представляющее определённый интерес.

Следствие. Фактор-модель M_G, построенная с помощью произвольной группы автоморфизмов G, изоморфна суперпозиции фактор-моделей, группы автоморфизмов которых простые, то есть не содержат нетривиальных нормальных делителей.

Доказательство. Как известно [10], всякая конечная группа G обладает композиционным рядом, то есть такой последовательностью подгрупп $E = H_0 \lhd H_1 \lhd H_2 \lhd \cdots \lhd H_k = G$, что все фактор-группы H_{l+1}/H_l – простые. Далее применима теорема 1 ■

В связи с полученным следствием приведём цитату из [10]: «подобно тому, как

натуральные числа получаются из простых чисел посредством умножения, так и любую конечную группу можно построить из простых конечных групп посредством расширений». И далее: «классификация простых конечных групп ... пожалуй главная проблема в теории конечных групп».

Можно отметить, что к настоящему времени классификация завершена и является исключительно сложным результатом работы десятков математиков в течение десятков лет, так что практическое применение её в полном объёме весьма проблематично. Однако использование ограниченных подклассов простых групп, не включающих «спорадических монстров» огромных порядков, более реально.

Установим факт, некоторые аналоги которого для сетей Петри доказаны в [6].

Теорема 2. Произвольная конечная группа G изоморфна группе всех автоморфизмов некоторой модели Крипке.

Доказательство. Будем рассматривать автоморфизмы без учёта свойств инвариантности. В силу известной теоремы Фрухта (см. [11]), для всякой группы G можно построить неориентированный граф $N(S, E)$, группа автоморфизмов которого изоморфна G. На основе графа построим модель Крипке $M(S, R)$, множество состояний которой совпадает с множеством S вершин графа N, а пары (s_i, S_j) и (s_j, S_i) принадлежат отношению R тогда и только тогда, когда две вершины s_i, S_j составляют ребро. Автоморфизмы модели есть, по определению, подстановки на множестве S, отображающие на себя множество R. По выбору графа и построению модели это, очевидно, элементы группы G и только они. ■

Как видим, для моделей Крипке данная теорема фактически является следствием теоремы Фрухта. Её роль только в указании, что при рассмотрении произвольных моделей нельзя ограничиться каким-то подклассом групп. Это значит, что для успешной работы с моделями Крипке желательно иметь какое-то дополнительное, но не слишком обременительное структурное ограничение, которое отсекало бы патологические случаи. Это важно и в связи со следующим замечанием.

При построении фактор-модели первым шагом является задача построения орбит, то есть состояний фактор-системы. По этому вопросу в [1] имеется утверждение, что проблема орбит столь же вычислительно трудна, как и проблема изоморфизма графов. Однако в [4] доказано, что проблема изоморфизма графов полиномиально разрешима, откуда следует, что и проблема орбит из [1] принадлежит этому же классу. Это означает, что имеет смысл задача разработки практически приемлемых алгоритмов построения фактор-моделей, хотя бы для каких-то разумных подклассов моделей.

Список литературы

1. Кларк Э.М., мл., Грамберг О., Пелед Д. Верификация моделей программ: Model Checking М.: МЦНМО, 2002.

2. Тарасюк И.В. Эквивалентности для поведенческого анализа параллельных и распределённых вычислительных систем. Новосибирск: ГЕО, 2007.

3. Schnoeblin Ph., Sidorova N. Bisimulation and reduction of Petri nets. Proc. 21^{th} Int. Conf. Appl. and Theory of Petri Nets. Aarhus, Denmark, June 2000.

4. (ArXiv.org) ArXiv:0711.2010v4[cs.CC]23 Jan 2008

5. Белов Ю.А. Корректные отображения систем с переходами // Моделирование и анализ информационных систем. 2001. Том 8, №1. С. 47-49.

6. Белов Ю.А. Конечные группы автоморфизмов сетей Петри // Моделирование и анализ информационных систем. 2008. Том 14, №4. С. 3-9.

7. Белов Ю.А. Теорема об эпиморфизме для систем переходов // Моделирование и анализ информационных систем. 2004. Том 11, №2. С. 42-43.

8. Алгебраическая теория автоматов, языков и полугрупп: Сб. статей / Под ред. М. Арбиба. М.: Статистика, 1975.

9. Емеличев В.А., Мельников О.И., Сарванов В.И., Тышкевич В.И. Лекции по теории графов. М.: Наука, 1990.

10. Каргаполов М.И., Мерзляков Ю.И. Основы теории групп. М.: Наука,1972.

11. Емеличев В.А., Мельников О.И., Сарванов В.И., Тышкевич В.И. Лекции по теории графов. М.: Наука, 1990. 383 с.

Composite reductions for Kripke models

Belov. Y.A.

Keywords: Kripke model, factor-model, automorphisms of a Kripke model

Kripke factor-model concept is investigated. It is shown, that every factor-model is represented as a decomposition of several special factor-models, which groups of automorphisms are primes. Moreover, we show, that every finite group is isomorphic for a group of automorphisms of a certain Kripke model.

Сведения об авторе:
Белов Юрий Анатольевич,
Ярославский государственный университет им. П.Г. Демидова,
кандидат физико-математических наук, доцент