УДК 51.681.3

С.Л. КРЫВЫЙ, А.Н. МАКСИМЕЦ

ВЕРИФИКАЦИЯ ПРОГРАММ: СОСТОЯНИЕ, ПРОБЛЕМЫ, РЕЗУЛЬТАТЫ. II[1]

Аннотация. Рассмотрены современные методы верификации программного обеспечения последовательных, функциональных, параллельных и распределенных систем. Основное внимание уделяется методам верификации на основе свойств абстрактных интерпретаций, транзиционных систем, сетей Петри.

Ключевые слова: верификация, абстрактные интерпретации, транзиционные системы, сети Петри, верификация на моделях.

Данная работа является второй частью обзора, начатого в [1–3]. В настоящей публикации рассматриваются методы и их приложения, ориентированные на верификацию реактивных и распределенных систем. В частности, анализируются такие модели программных систем, как транзиционные системы и их произведения, а также методы их верификации на моделях.

1. ТРАНЗИЦИОННЫЕ СИСТЕМЫ И ИХ ПРОИЗВЕДЕНИЯ

Транзиционные системы (ТС) — это одна из наиболее общих математических моделей программных систем. С ее помощью исследуются многие свойства реальных параллельных и распределенных систем.

Определение 1. ТС называется пятерка $\mathcal{A} = (S, T, \alpha, \beta, s_0)$, где S — множество состояний, T — множество переходов между состояниями, $\alpha : T \to S$ — функция начала перехода, $\beta : T \to S$ — функция конца перехода, $s_0 \in S$ — начальное состояние ТС.

ТС изображается в виде орграфа, вершины которого соответствуют состояниям, а дуги — переходам ТС. Рассмотрим примеры, взятые из [4].

Пример 1. Пусть $\mathcal{A} = (S = \{s_0, s_1, s_2, s_3\}, T = \{t_1, t_2, t_3, t_4, t_5\}, \alpha, \beta, s_0)$, где функции α и β задаются графом, изображенным на рис. 1. Здесь $\alpha(t_1) = s_0$, $\beta(t_1) = s_1, \ldots,$ $\alpha(t_5) = s_3$, $\beta(t_5) = s_0$.

Множество переходов T можно рассматривать как алфавит, а конечную или бесконечную последовательность переходов этого алфавита называть транзиционным словом или просто словом переходов. Множество всех слов в алфавите T будем обозначать $F(T)$.

Если $t \in T$, то тройка $(\alpha(t), t, \beta(t))$ является шагом вычислений в ТС $\mathcal{A} = (S, T, \alpha, \beta, s_0)$. Состояние $s \in S$ достижимо с помощью перехода $t \in T$, если существует $s' \in S$ такое, что (s, t, s') — шаг вычислений в ТС $\mathcal{A}$. Слово $t_1 t_2 \ldots t_k \in F(T)$ называют вычислением в $\mathcal{A} = (S, T, \alpha, \beta, s_0)$, если существует последовательность состояний $s_0, s_1, \ldots, s_k$ такая, что (s_{i-1}, t_i, s_i) — шаг вычислений для каждого $i \in \{1, 2, \ldots, k\}$. Добавим к множеству переходов T пустой переход ε, который обозначает отсутствие перехода из состояния $s \in T$. Если $t_1 t_2 \ldots t_k \in F(T)$ — вычисление в ТС, то говорят, что оно начинается в состоянии s_0 и ведет в состояние s_k. Вычисление называется историей, если оно начинается в начальном состоянии s_0. Слово $t_1 t_2 \ldots \in F(T)$ бесконечной длины представляет бесконечное вычисление в ТС, если существует бесконечная последовательность состояний $s_{i_1}, s_{i_2}, \ldots$ такая, что $(s_{i_{j-1}}, t_j, s_{i_j})$ — шаг вычислений в ТС для каждого $i_j \geq 1$, и бесконечной историей, если $s_{i_1} = s_0$.

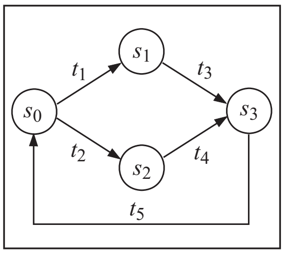

Рис. 1

Если h — история, ведущая в состояние s, а c — вычисление, начинающееся в состоянии s, то конкатенация hc тоже является историей. В этом случае hc — расширение истории h с помощью вычисления c.

[1] Начало см. в № 6, 2013.

Рассмотрим синхронное произведение ТС. Пусть $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_n$ — ТС, где $\mathcal{A}_i = (S_i, T_i, \alpha_i, \beta_i, s_0^i)$, $\mathcal{A}_i \cap \mathcal{A}_j = \varnothing$, если $i \neq j$, $i, j = 1, 2, \ldots, n$.

Определение 2. Ограничением синхронизации является подмножество $\mathbf{T}$ множества

$$(T_1 \cup \varepsilon) \times (T_2 \cup \varepsilon) \times \ldots \times (T_n \cup \varepsilon) \setminus (\varepsilon, \varepsilon, \ldots, \varepsilon),$$

где ε — пустой переход.

Элементы множества $\mathbf{T}$ называются глобальными переходами. Если $\mathbf{t} = (t_1, t_2, \ldots, t_n) \in \mathbf{T}$ и $t_i \neq \varepsilon$, то считается, что ТС $\mathcal{A}_i$ участвует в переходе $\mathbf{t}$.

Кортеж $\mathbf{A} = (\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_n, \mathbf{T})$ — произведение ТС $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_n$ над множеством $\mathbf{T}$, а ТС $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_n$ — компоненты $\mathbf{A}$.

Пример 2. На рис. 2 показано произведение ТС_1 и ТС_2.

В этой ТС выбирается такое множество глобальных переходов: $\mathbf{T} = \{(t_1, \varepsilon), (t_2, \varepsilon), (t_3, u_2), (t_4, u_2), (t_5, \varepsilon), (\varepsilon, u_1), (\varepsilon, u_3)\}$.

Глобальное состояние $\mathbf{A} = (\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_n, \mathbf{T})$ — n-ка $(s_1, s_2, \ldots, s_n)$, где $s_i \in S_i$, а состояние $(s_0^1, s_0^2, \ldots, s_0^n)$ — начальное состояние $\mathbf{A}$.

Шагом вычисления $\mathbf{A}$ является тройка $(\mathbf{s}, \mathbf{t}, \mathbf{s}')$, где $\mathbf{s} = (s_1, s_2, \ldots, s_n)$ и $\mathbf{s}' = (s_1', s_2', \ldots, s_n')$ — глобальные состояния, а $\mathbf{t} = (t_1, t_2, \ldots, t_n)$ — глобальный переход, который удовлетворяет следующим условиям $\forall i \in \{1, 2, \ldots, n\}$:

- если $t_i \neq \varepsilon$, то $s_i = \alpha(t_i)$ и $s_i' = \beta(t_i)$;
- если $t_i = \varepsilon$, то $s_i' = s_i$.

Глобальный переход $\mathbf{t}$ называется допустимым в глобальном состоянии $\mathbf{s}$, если существует глобальное состояние $\mathbf{s}'$ такое, что $(\mathbf{s}, \mathbf{t}, \mathbf{s}')$ является шагом вычисления.

Последовательность глобальных переходов $\mathbf{t}_1, \mathbf{t}_2, \ldots, \mathbf{t}_k, \ldots$ называют глобальным вычислением, если существует последовательность глобальных состояний $\mathbf{s}_0, \mathbf{s}_1, \ldots, \mathbf{s}_k$ такая, что $(\mathbf{s}_{i-1}, \mathbf{t}_i, \mathbf{s}_i)$ — шаг вычислений для каждого $i \in 1, 2, \ldots, k$. В этом случае глобальное вычисление начинается в глобальном состоянии s_0 и ведет в глобальное состояние $\mathbf{s}_k$. Глобальное вычисление, которое начинается в состоянии $\mathbf{s}_0$, представляет собой глобальную историю вычислений.

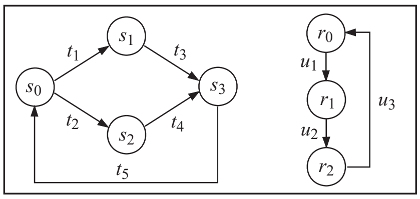

Рис. 2

Пример 3. Рассмотрим произведение ТС из рис. 2. Начальным глобальным состоянием является (s_0, r_0), глобальным вычислением — последовательность $(t_1, \varepsilon), (\varepsilon, u_1), (t_3, u_2)$, поскольку три шага вычислений:

$$((s_0, r_0)(t_1, \varepsilon),\ (s_1, r_0)),\ ((s_1, r_0)(\varepsilon, u_1), (s_1, r_1)),\ ((s_1, r_1)(t_3, u_2), (s_3, r_2)),$$

составляют вычисление, ведущее из состояния (s_0, r_0) в состояние (s_3, r_2).

Последовательность $(t_1, \varepsilon)(t_3, u_1)$ не будет глобальным вычислением, поскольку переход (t_3, u_1) не является глобальным переходом из $\mathbf{T}$.

Многие свойства произведения ТС можно исследовать с помощью его моделирования сетями Петри [4].

Сети Петри и произведения ТС. Сеть — это тройка (P, T, F), где P и T — непересекающиеся множества, элементы которых называются местами и переходами соответственно, а $F \subseteq (P \times T) \cup (T \times P)$ — отношение инцидентности. Элементы из F изображаются стрелками, а места — вершинами (в графическом представление сети). Если $(x, y) \in F$, то x называется входной вершиной y, а y — выходной вершиной x. Множества входных и выходных вершин для x обозначаются ${}^\bullet x$ и $x^\bullet$ соответственно.

Сеть (P, T, F) называется размеченной, если задана функция разметок $M : P \to N$, где N — множество натуральных чисел. Если $M(p) = m$, то это значит, что функция M ставит в вершину p ровно m фишек. Если $|P| = n$ и множество P упорядочено, то разметка сети представляется вектором $M = (m_1, m_2, \ldots, m_n)$, где $m_i = M(p_i)$, $p_i \in P$, $i = 1, 2, \ldots, n$.

Сетью Петри (СП) называется пятерка (P, T, F, W, M_0), где (P, T, F) — сеть, M_0 — начальная разметка ее мест, а $W : F \to N \setminus \{0\}$ — функция кратности дуг СП.

Необходимость введения функции кратности дуг объясняется тем, что место и переход или переход и место могут быть связаны не одной, а несколькими дугами. Если в СП все дуги имеют кратность 1, то такая СП называется ординарной. Заметим, что имеется алгоритм, с помощью которого произвольная СП может быть преобразована в ординарную СП [5], обозначим ее четверкой (P, T, F, M_0), и далее, если не оговорено противное, под СП будем понимать ординарную сеть.

Пример 4. На рис. 3 показана ординарная СП (P, T, F, M_0), где $P = \{p_1, p_2, p_3, p_4\}$, $T = \{t_1, t_2, t_3\}$, $F = \{(p_1, t_2), (p_2, t_2), (p_3, t_1), (p_4, t_3), (t_1, p_1), (t_2, p_3), (t_2, p_4), (t_3, p_2)\}$, $M_0 = \{1, 1, 0, 0\}$.

Переход $t \in T$ СП может сработать при разметке M, если она размечает каждое входное место этого перехода, т.е. ${}^\bullet t \subseteq M$. В этом случае разметка M называется допустимой для перехода t.

Если M допустима для t, то этот переход может сработать и привести к новой разметке: $M' = (M \setminus \{{}^\bullet t\}) \cup t^\bullet$. Разметка M' получается из разметки M удалением одной фишки из каждого входного места и добавлением одной фишки в каждое выходное место перехода t. Переход от M к M' обозначается $M \xrightarrow{t} M'$. Считается, что разметка M' достижима из разметки M, если существует последовательность переходов $t_1, t_2, \ldots, t_n$ из T таких, что $M \xrightarrow{t_1} M_1 \xrightarrow{t_2} M_2 \xrightarrow{t_3} \ldots \xrightarrow{t_n} M'$. Разметка M' считается достижимой, если она достижима из начальной разметки M_0 СП. Например, в СП из рис. 3 при разметке M_0 может сработать только переход t_2. После его срабатывания получаем разметку $M_1 = (0, 0, 1, 1)$. Из этой разметки достижимыми становятся разметки $M_2 = (1, 1, 0, 0)$, $M_3 = (1, 0, 0, 1)$, $M_4 = (0, 1, 1, 0)$.

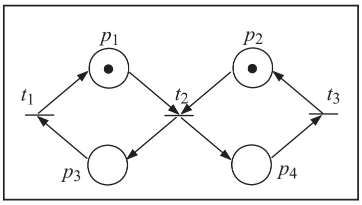

Рис. 3

СП, как математическая модель вычислений, достаточно изучена и поэтому принято моделировать ТС с помощью СП [6, 7].

Моделирование произведения ТС с помощью СП. Пусть СП (P, T, F, M_0) представляет произведение $\mathbf{A} = (\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_n, \mathbf{T})$ транзиционных систем $\mathcal{A}_i = (S_i, T_i, \alpha_i, \beta_i, s_0^i)$, где $\mathcal{A}_i \cap \mathcal{A}_j = \varnothing$ при $i \neq j$, $i, j = 1, 2, \ldots, n$, если:

- $P = S_1 \cup S_2 \cup \ldots \cup S_n$,
- $T = \mathbf{T}$,
- $F = \{(s, \mathbf{t}) \mid t_i \neq \varepsilon$ и $s = \alpha_i(t_i)\} \cup \{(\mathbf{t}, s) \mid t_i \neq \varepsilon$ и $s = \beta_i(t_i)\}$ для некоторого $i \in 1, 2, \ldots, n$, где t_i — i-я компонента $\mathbf{t} \in \mathbf{T}$,
- $M_0 = (s_0^1, s_0^2, \ldots, s_0^n)$.

Пример 5. СП для произведения двух ТС из рис. 2 показана на рис. 4. Здесь имеем ${}^\bullet(t_2, \varepsilon) = \{s_0\}, (t_2, \varepsilon)^\bullet = \{s_2\}, \ldots, {}^\bullet(t_4, u_2) = \{s_2, r_1\}$ и $(t_4, u_2)^\bullet = \{s_3, r_2\}$. Далее будем использовать обозначения ${}^\bullet t = \{\alpha_i(t_i) \mid t_i \neq \varepsilon\}$ и $t^\bullet = \{\beta_i(t_i) \mid t_i \neq \varepsilon\}$. Нетрудно заметить, что семантика произведения ТС и семантика СП, представляющая его, согласуются в том смысле, что последовательность глобальных переходов $\mathbf{t}_1, \mathbf{t}_2, \ldots, \mathbf{t}_k$ выступает глобальной историей произведения ТС $\mathbf{A}$ тогда и только тогда, когда она является допустимой последовательностью срабатываний переходов в СП.

Представление произведения ТС в виде СП позволяет исследовать свойства этого произведения методами анализа свойств СП, которые хорошо развиты (хотя бы для ТС малых размеров).

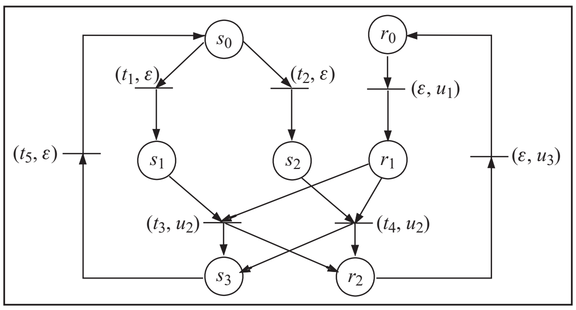

Рис. 4

Рассмотрим методы верификации свойств реактивных систем логическими средствами и средствами конечных автоматов.

2. ВЕРИФИКАЦИЯ РЕАКТИВНЫХ СИСТЕМ

Реактивной системой называется система, которая должна работать потенциально бесконечное время. Методы верификации таких систем основываются на проверке на модели и некоторых ее разновидностях [8, 9]. Неформально суть этого метода состоит в следующем. Ожидаемые свойства реальной системы описываются в виде формул некоторого формального логического языка, а реальная система моделируется соответствующей ТС или ее произведением. Верификация заключается в проверке выполнимости заданных формул на модели. Одним из популярных логических языков является язык линейной темпоральной логики (linear temporal logic — LTL).

Язык линейной темпоральной логики. Множество LTL-формул над заданным множеством атомарных формул AP определяется индуктивно следующим образом:

- каждая атомарная формула является LTL-формулой;
- если φ — LTL-формула, то $\neg\varphi$ и $\mathbf{X}\varphi$ — LTL-формулы;
- если φ, ψ — LTL-формулы, то $\varphi \vee \psi$ и $\varphi \mathbf{U} \psi$ — LTL-формулы.

LTL-формулы интерпретируются над бесконечными словами, символами которых есть множества атомарных формул, т.е. бесконечными словами в алфавите $B(AP)$, где $B(AP)$ — булеан множества атомарных формул AP. Интуитивно это означает, что некоторое множество атомарных формул, соответствующих исследуемому базисному утверждению, выполняется в i-й момент времени.

Пусть φ — LTL-формула и бесконечное слово $\pi = x_0 x_1 x_2 \ldots$, где $x_i \in B(AP)$ для каждого $i \geq 0$; $\pi \models \varphi$ означает, что слово π выполняет φ или удовлетворяет φ. Отношение выполнимости $\models$ определяется индуктивно следующим образом: пусть $p \in AP$ и $\pi^i = x_i x_{i+1} \ldots$ — суффикс слова π, тогда:

- $\pi \models p$, если $p \in x_0$,
- $\pi \models \neg\varphi$, если $\pi \not\models \varphi$,
- $\pi \models \neg\varphi \vee \psi$, если $\pi \models \varphi$ или $\pi \models \psi$,
- $\pi \models \mathbf{X}\varphi$, если $\pi^1 \models \varphi$,
- $\pi \models \varphi \mathbf{U} \psi$, если $\exists n \geq 0 \,|\, \pi^n \models \psi$ и $\forall i \; (0 \leq i < n) \pi^i \models \varphi$.

Формула $\mathbf{X}\varphi$ читается как «φ в следующий момент», а $\varphi\,\mathbf{U}\psi$ — как «φ пока не ψ». Другими словами, $\mathbf{X}\varphi$ выполняется в данный момент времени, если в следующий момент времени будет выполняться φ, а $\varphi\,\mathbf{U}\psi$ выполняется в данный момент времени, если формула ψ выполняется в данный момент или будет выполнена в следующий момент времени, а в каждый момент времени до этого момента выполняется формула φ.

Остальные логические связки вводятся обычным путем: $true = p \vee \neg p$ для любого $p \in AP$, $false = \neg true$, $\varphi \wedge \psi = \neg\varphi \vee \psi$, $\varphi \mathbf{R} \psi = \neg(\neg\varphi \mathbf{U} \neg\psi)$, $\mathbf{F}\varphi = true \mathbf{U} \varphi$ и $\mathbf{G}\varphi = false \mathbf{R} \varphi$. Часто операторы $\mathbf{X}\varphi, \mathbf{F}\varphi, \mathbf{G}\varphi$ обозначают $\bigcirc\varphi, \Diamond\varphi, \Box\varphi$ соответственно.

Пример 6. Пусть $AP = p$ и даны LTL-формулы $\mathbf{G}(p \to \mathbf{X}\neg p)$ и $\mathbf{F}(p \wedge \mathbf{X} p)$ над алфавитом $AP = p$ атомарных формул. Первая формула читается как «всегда, если p выполняется в данный момент времени, то в следующий момент времени она не выполняется», а вторая формула — «существует два последовательных момента времени, в которых формула p выполняется».

Пусть $(p0)^\omega$ и $00pp(0)^\omega$ — два бесконечных слова вида: $p0p0p0\ldots$ и $00pp000\ldots$ соответственно. Для этих слов получаем:

$$(p0)^\omega \models \mathbf{G}(p \to \mathbf{X}\neg p), \; 00pp(0)^\omega \not\models \mathbf{G}(p \to \mathbf{X}\neg p),$$

$$(p0)^\omega \not\models \mathbf{F}(p \wedge \mathbf{X} p), \; 00pp(0)^\omega \models \mathbf{F}(p \wedge \mathbf{X} p).$$

Интерпретация LTL-формул на произведении ТС. Пусть имеется произведение ТС $\mathbf{A} = (\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_n, \mathbf{T})$, где $\mathcal{A}_i = (S_i, T_i, \alpha_i, \beta_i, a_0^i)$, $i = 0, 1, \ldots, n$. Базисными утверждениями будут такие: «текущим локальным состоянием i-й компоненты является a_i». Следовательно, множеством атомарных формул выбирается множество $AP=\bigcup_{i=1}^{n} S_i$.

Пусть задана бесконечная глобальная история $\mathbf{h}=\mathbf{t}_1\mathbf{t}_2\mathbf{t}_3\ldots$ произведения **A**, тогда существует единственная последовательность глобальных состояний $\mathbf{a}_0\mathbf{a}_1\mathbf{a}_2\ldots$ такая, что $\mathbf{a}_0$ — начальное состояние, $(\mathbf{a}_i, \mathbf{t}_{i+1}, \mathbf{a}_{i+1})$ — шаг вычислений в **A** для каждого $i\geq 0$. Иными словами, $\mathbf{a}_0\mathbf{a}_1\mathbf{a}_2\ldots$ — последовательность состояний, которые проходятся во время выполнения **h**. Бесконечная последовательность $\pi(\mathbf{h})$ множеств атомарных формул определяется следующим образом: для каждого $i\geq 0$ i-й элемент $\pi(\mathbf{h})$ представляет собой множество локальных состояний глобального состояния $\mathbf{a}_i$ (т.е. множество локальных состояний компонент произведения ТС в i-й момент времени). Из определения шага вычисления следует, что если S_i и S_{i+1} — соответственно i-й и $(i+1)$-й элемент $\pi(\mathbf{h})$, то $S_{i+1}=(S_i \setminus {}^{\bullet}t_i)\bigcup t_i^{\bullet}$.

Пример 7. Рассмотрим произведение ТС (рис. 5) (пример заимствован из [4]). LTL-формулы строятся над алфавитом $AP=\{t_0, t_1, u_0, u_1\}$ и при этом $\mathbf{T}=\{\mathbf{a}=(\varepsilon, a), \mathbf{b}=(\varepsilon, b), \mathbf{c}=(c,\varepsilon)\}$.

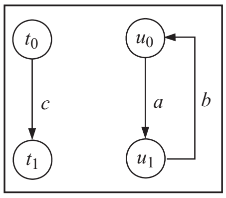

Рис. 5

Последовательность $\mathbf{h}=\mathbf{abc}(\mathbf{ab})^{\omega}$ является бесконечной историей. Запишем последовательность глобальных состояний:

$$(t_0, u_0)(t_0, u_1)(t_0, u_0)((t_1, u_0)(t_1, u_1))^{\omega},$$

т.е. $\pi(\mathbf{h})=(t_0, u_0)(t_0, u_1)(t_0, u_0)((t_1, u_0)(t_1, u_1))^{\omega}$.

Теперь можно определить интерпретацию LTL-формулы φ на $\pi(\mathbf{h})$. Будем считать, что произведение **A** выполняет формулу φ (обозначение $\mathbf{A}\vDash\varphi$), если каждая бесконечная история произведения **A** выполняет φ. Другими словами, произведение **A** выполняет формулу φ, если все ее бесконечные истории выполняют формулу φ.

Проблема проверки выполнимости на модели заключается в определении для заданных произведения **A** и LTL-формулы φ выполнимости формулы φ на **A**.

Пример 8. Рассмотрим произведение **A** из предыдущего примера и формулы $\mathbf{G}(u_0\to\mathbf{X}\neg u_0)$ и $\mathbf{F}(u_0\wedge\mathbf{X}u_0)$. Поскольку $\pi(\mathbf{h})$ содержит $(t_0, u_0)(t_1, u_0)$ как подслово, то

$$\pi(\mathbf{h})\nvDash\mathbf{G}(u_0\to\mathbf{X}\neg u_0) \text{ и } \pi(\mathbf{h})\vDash\mathbf{F}(u_0\wedge\mathbf{X}u_0).$$

Тогда согласно определению получаем $\mathbf{h}\nvDash\mathbf{G}(u_0\to\mathbf{X}\neg u_0)$ и $\mathbf{h}\vDash\mathbf{F}(u_0\wedge\mathbf{X}u_0)$.

Нетрудно убедиться, что история $\mathbf{h}=(\mathbf{ab})^{\omega}$ не выполняет формулу $\mathbf{F}(u_0\wedge\mathbf{X}u_0)$. Таким образом, существуют истории в **A**, которые не выполняют ни первую, ни вторую формулы, следовательно, $\mathbf{A}\nvDash\mathbf{G}(u_0\to\mathbf{X}\neg u_0)$ и $\mathbf{A}\nvDash\mathbf{F}(u_0\wedge\mathbf{X}u_0)$.

Проблема верификации свойств произведения **A** может быть распространена на проверку выполнимости LTL-формулы ψ и на ψ-истории.

Пусть AP_{ψ} — множество атомарных формул, входящих в формулу ψ; ψ-состоянием называется n-ка $\mathbf{r}=(r_1,\ldots,r_n)$ такая, что для каждого $i\in\{1,\ldots,n\}$ либо $r_i\in S_i\bigcap AP_{\psi}$, либо $a_i=\bot$, где $\bot$ — специальный символ. Данному глобальному состоянию $\mathbf{a}=(a_1,\ldots,a_n)$ сопоставим ψ-состояние $\mathbf{a}_{\psi}=(a_{1\psi},\ldots,a_{m\psi})$ следующим образом. Для каждого $i\in\{1,\ldots,n\}$ имеем

$$a_{i\psi}=\begin{cases} a_i, & \text{если } a_i\in AP_{\psi},\\ \bot & \text{в противном случае.}\end{cases}$$

Такое сопоставление означает, что в $\mathbf{a}_{\psi}$ имеется информация о глобальном состоянии, которая содержится в локальных состояниях из AP_{ψ}.

Тройка $(\mathbf{r}, \mathbf{t}, \mathbf{r}')$, где $\mathbf{r}, \mathbf{r}'$ — ψ-состояние, а $\mathbf{t}$ — глобальный переход, называется ψ-шагом, если существует шаг вычисления $(\mathbf{a}, \mathbf{t}, \mathbf{a}')$ такой, что $\mathbf{r}=\mathbf{a}_{\psi}$ и $\mathbf{r}'=\mathbf{a}'_{\psi}$. Определения ψ-вычисления и ψ-истории аналогичны вышеприведенным определениям вычисления и истории с заменой слова шаг на ψ-шаг.

Последовательность $\mathbf{t}_1\mathbf{t}_2\ldots\mathbf{t}_k$ глобальных переходов называется ψ-вычислением, если существует последовательность $\mathbf{r}_0, \mathbf{r}_1,\ldots,\mathbf{r}_k$ ψ-состояний такая, что

$(\mathbf{r}_{i-1}, \mathbf{t}_i, \mathbf{r}_i)$ — ψ-шаг для каждого $i \in \{1, 2, \ldots, k\}$; ψ-вычисление является ψ-историей, если можно выбрать последовательность $\mathbf{r}_0, \mathbf{r}_1, \ldots, \mathbf{r}_k$ такую, что $\mathbf{r}_0 = \mathbf{a}_{0\psi}$. Бесконечные вычисления и бесконечные истории определяются аналогично.

Пример 9. Рассмотрим произведение ТС **A** из предыдущего примера. Пусть $AP_\psi = \{u_0\}$, тройка $((t_0, u_0), \mathbf{c}, (t_1, u_0))$ является шагом вычислений, а $((\perp, u_0), \mathbf{c}, (\perp, u_0))$ — соответствующий ψ-шаг. Отсюда вытекает, что **cc** является ψ-историей, поскольку существует два ψ-шага:

$$((\perp, u_0), \mathbf{c}, (\perp, u_0))((\perp, u_0), \mathbf{c}, (\perp, u_0)),$$

однако **cc** не будет историей.

Последовательность **aa** не будет ψ-историей. Действительно, допустим, что существуют ψ-шаги $(\mathbf{r}_0, \mathbf{a}, \mathbf{r}_1)$ и $(\mathbf{r}_1, \mathbf{a}, \mathbf{r}_2)$ такие, что $\mathbf{r}_0$ — начальное состояние, т.е. $\mathbf{r}_0 = (\perp, u_0)$. Согласно определению ψ-шага получаем $r_1 = (\perp, \perp)$. Поскольку **a** может входить в глобальное состояние со второй компонентой, равной u_0, то не существует $\mathbf{r}_2$ такого, что $(\mathbf{r}_1, \mathbf{a}, \mathbf{r}_2)$ является ψ-шагом.

Как и в случае историй, нетрудно увидеть, что для данной бесконечной ψ-истории $\sigma = \mathbf{t}_1 \mathbf{t}_2 \ldots$ существует единственная последовательность $\mathbf{r}_0 \mathbf{r}_1 \ldots$ ψ-состояний такая, что $(\mathbf{r}_{i-1}, t_i, \mathbf{r}_i)$ является ψ-шагом произведения **A** для каждого $i \geq 1$.

Обозначим эту последовательность $\pi_\psi(\sigma)$ и будем называть ее ψ-последовательностью σ. В этом случае считается, что σ выполняет ψ и обозначается это $\sigma \models \psi$, если $\pi_\psi(\sigma) \models \psi$.

Проверка LTL-свойств. Проблема проверки LTL-свойств имеет несколько эквивалентных формулировок. Проверка того, что все бесконечные истории произведения **A** выполняют LTL-формулу ψ, эквивалентно существованию некоторой бесконечной истории, которая не выполняет ψ, а это, в свою очередь, эквивалентно тому, что существует некоторая история, выполняющая $\neg\psi$. Таким образом, рассматривая бесконечные истории, выполняющие некоторое свойство, как язык слов бесконечной длины в алфавите AP_ψ, проблема выполнимости сводится к проблеме проверки пустоты некоторых языков такого типа.

В данном случае тестер свойств произведения **A** воспринимает **A** как механизм, распознающий язык L слов бесконечной длины, соответствующих ψ-историям и бесконечным историям произведения **A**. Следовательно, получаем такую процедуру проверки выполнимости формулы ψ:

- построить тестер, распознающий язык L_1 всех ψ-историй, выполняющих $\neg\psi$;
- построить тестер, допускающий язык $L \bigcap L_1$, используя этот тестер и его произведение с тестером языка L всех ψ-историй;
- проверить равенство $L \bigcap L_1 = \varnothing$; если оно выполняется, то формула ψ выполняется на всех бесконечных ψ-историях, иначе на некоторой выполняется $\neg\psi$ (и эта история дает контрпример).

Такого типа тестеры известны — это автоматы Бюхи и обобщенные автоматы Бюхи, называемые также автоматами Мюлера [10, 11]. Тестер для LTL-формул называют Бюхи-тестером или просто тестером для произведения **A**. Формальное определение тестера имеет следующий вид: тестер — это тройка вида $\mathcal{BT} = (\mathcal{B}, \mathcal{T}, \lambda)$, где $\mathcal{B} = (S, T, \alpha, \beta, a_0)$ — транзитивная система, $F \subseteq S$ — множество заключительных состояний и $\lambda : T \to \mathbf{T}$ — функция отметок, сопоставляющая каждому переходу $\mathcal{B}$ некоторый глобальный переход из **T** произведения **A**. Тестер $\mathcal{BT}$ воспринимает бесконечные последовательности $\mathbf{t}_1 \mathbf{t}_2 \mathbf{t}_3 \ldots \in \mathbf{T}^\omega$, если существует бесконечная история $h = u_1 u_2 u_3 \ldots$ в $\mathcal{B}$ и заключительное состояние $a \in F$ такое, что $\mathbf{t}_i = \lambda(u_i)$ для каждого $i \geq 1$ и на истории h состояние a появляется бесконечно. Это значит, что последовательность $\pi(h)$ содержит бесконечное число вхождений состояния a. Язык, который воспринимается $\mathcal{BT}$, состоит из слов $\mathbf{T}^\omega$.

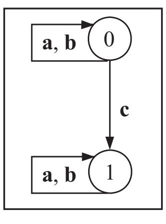

Рис. 6

Пример 10. На рис. 6 показан граф переходов Бюхи-тестера для произведения ТС **A** из предыдущего примера. Этот тестер воспринимает язык $(\mathbf{ab})^* \mathbf{c} (\mathbf{ab})^\omega$.

Пусть ψ — LTL-формула. Тестер $\mathcal{BT}$ проверяет выполнимость формулы ψ, является ли тестером свойства ψ, если он воспринимает все бесконечные ψ-истории **A**, которые выполняют ψ?

Существует множество публикаций по проблеме проверки на модели и большое число различных конструкций для такого типа проверки. Рассмотрим одну из самых простых конструкций.

Построение Бюхи-тестера часто выполняется в два этапа: сначала строится обобщенный Бюхи-тестер для заданной LTL-формулы ψ, а затем этот тестер преобразовывается в Бюхи-тестер для этой формулы.

Обобщенным Бюхи-тестером для **A** называется кортеж $\mathcal{BT} = (\mathcal{B}, \{F_0, F_1, \ldots$ $\ldots, F_{k-1}\}, \lambda)$, где $\mathcal{B}, \lambda$ такие же, как и в определении Бюхи-тестера, а $F_0, \ldots, F_{k-1}$ — множество подмножеств заключительных состояний. $\mathcal{B}$ воспринимает бесконечную последовательность $\mathbf{t}_1\mathbf{t}_2\mathbf{t}_3\ldots \in \mathbf{T}^{\omega}$, если существует бесконечная история $\mathbf{h} = a_1 a_2 a_3 \ldots$ и заключительные состояния $a_1 \in F_0, a_2 \in F_1, \ldots, a_k \in F_{k-1}$ такие, что $\mathbf{t}_i = \lambda(u_i)$ для каждого $i \geq 1$ и каждое состояние $a_1, \ldots, a_k$ входит в **h** бесконечное число раз. Язык называется распознаваемым или допускаемым тестером $\mathcal{BT}$, если каждое слово этого языка допускается этим тестером.

Последовательность Хинтикки. Построение тестера базируется на понятии последовательности Хинтикки для данной LTL-формулы.

Неформально последовательностью Хинтикки для LTL-формулы ψ называется бесконечная последовательность множеств подформул формулы ψ и их отрицаний.

Определение 3. Пусть ψ — LTL-формула. Замыканием $\mathrm{cl}(\psi)$ формулы ψ называется множество, содержащее все подформулы формулы ψ и их отрицания. Атомом a формулы ψ называется подмножество формул, которое удовлетворяет следующим условиям:

• для каждой подформулы $\neg\phi$ формулы ψ $\phi \in a$ тогда и только тогда, когда $\neg\phi \notin a$;

• для каждой подформулы $\phi_1 \vee \phi_2$ формулы ψ $\phi_1 \vee \phi_2 \in a$ тогда и только тогда, когда $\phi_1 \in a$ или $\phi_2 \in a$.

Заметим, что если подмножесто из замыкания имеет модель, то оно должно быть атомом.

Пример 11. Замыканием формулы $\psi = t_0 \mathbf{U}(\neg \mathbf{X} u_0)$ является множество

$$\mathrm{cl}(\psi) = \{t_0, \neg t_0, u_0, \neg u_0, \mathbf{X}u_0, \neg\mathbf{X}u_0, \psi, \neg\psi\}.$$

Множество $\{t_0, \neg u_0, \mathbf{X}u_0, \psi\}$ — атом, а подмножество $\{t_0, \neg u_0, \psi\}$ атомом не является, поскольку согласно определению атома либо $\mathbf{X}u_0$, либо $\neg\mathbf{X}u_0$ (но не обе формулы вместе) должны принадлежать атому.

Определение 4. Пусть $\sigma = \mathbf{t}_1\mathbf{t}_2\mathbf{t}_3\ldots$ — ψ-история и a_i для каждого $i \geq 0$ является таким множеством всех формул ϕ в замыкании формулы ψ, что $\mathbf{t}_{i+1}\mathbf{t}_{1+2}\mathbf{t}_{i+3}\ldots \vDash \phi$. Последовательностью Хинтикки для σ ($hin(\sigma)$) называется бесконечная последовательность $a_0 a_1 a_2 \ldots$

Таким образом, последовательность Хинтикки представляет собой последовательность атомов. Соотношение между $\pi_{\psi}(\sigma)$ и $hin(\sigma)$ проявляется в том, что i-й элемент $\pi_{\psi}(\sigma)$ содержит те элементы AP_{ψ}, которые выполняются после первых i переходов σ, а i-й элемент $hin(\sigma)$ содержит не только эти элементы, но и все формулы из замыкания формулы ψ, выполняющиеся в этой точке.

Пример 12. Пусть $\psi = t_0 \mathbf{U}(\neg\mathbf{X}u_0)$ и $\sigma = \mathbf{ab}(\mathbf{ba})^{\omega}$ — история произведения **A** из примера 7. Тогда $\pi_{\psi}(\sigma) = (t_0, u_0)(t_0, u_1)((t_1, u_1)(t_1, u_0))^{\omega}$. Для того чтобы получить последовательность Хинтикки, рассмотрим $\pi_{\psi}(\sigma)$ и преобразуем это в подмножества из множества AP_{ψ}. Игнорируя формальности, получаем такой результат:

$$\pi_{\psi}(\sigma) = (t_0, u_0)(t_0, \bot)((\bot, \bot)(\bot, u_0))^{\omega} = \{t_0, u_0\}\{t_0\}(\varnothing\{u_0\})^{\omega}.$$

Теперь к каждому из этих множеств атомарных формул добавим те формулы из $\mathrm{cl}(\psi)$, которые выполняются в этой точке. Тогда к множеству $\{t_0, u_0\}$ добавляются формулы ψ' такие, что $(t_0, u_0)(t_0, \bot)((\bot, \bot)(\bot, u_0))^{\omega} \vDash \psi'$, а к множеству $\{t_0\}$ — формулы ψ'' такие, что $(t_0, \bot)((\bot, \bot)(\bot, u_0))^{\omega} \vDash \psi''$. В первом случае это дает множество формул $\{t_0, u_0, \neg\mathbf{X}u_0, \psi\}$, а во втором — $\{t_0, \neg u_0, \neg\mathbf{X}u_0, \psi\}$ (потому что u_0 не выполняется в третьей точке $(\bot, \bot)$, а ψ выполняется в этой точке из-за выполнимости формулы $\neg\mathbf{X}u_0$).

Далее, в третьей точке не выполняется ни t_0, ни u_0, но выполняется $\mathbf{X}u_0$ (поскольку следующая точка имеет вид $(\bot, u_0)$, а ψ не выполняется, но тогда выполняется $\neg\psi$). Таким образом, получаем третье множество атомов $\{\neg t_0, \neg u_0, \mathbf{X}u_0, \neg\psi\}$. В четвертой точке $(\bot, u_0)$ выполняются формулы $\{\neg t_0, u_0, \neg\mathbf{X}u_0, \psi\}$ в силу тех же причин. В результате последовательность Хинтикки принимает вид

$$hin(\sigma) = \{t_0, u_0, \neg\mathbf{X}u_0, \psi\}\{t_0, \neg u_0, \neg\mathbf{X}u_0, \psi\}\{(\neg t_0, u_0, \mathbf{X}u_0, \neg\psi\}\{\neg t_0, u_0, \neg\mathbf{X}u_0, \psi\})^{\omega}.$$

Дадим более формальную характеристику последовательности Хинтикки. Пусть σ является ψ-историей такой, что $\sigma \vDash \psi$, и пусть $hin(\sigma) = a_0 a_1 a_2 \ldots$ Будем нумеровать свойства, выполняющиеся на $a_0 a_1 a_2 \ldots$, до тех пор, пока не достигнем точки, в которой конъюнкция всех этих свойств становится не только необходимым, но и достаточным условием. Под этим подразумевается, что каждая другая последовательность $a'_0 a'_1 a'_2 \ldots$, удовлетворяющая этим свойствам, должна быть последовательностью Хинтикки некоторой ψ-истории σ', которая выполняет формулу ψ.

Согласно определению последовательности Хинтикки атом a_0 должен содержать все подформулы ψ' формулы ψ такие, что $\sigma \vDash \psi'$, отсюда следуют условия 1–6.

Условие 1. Пусть a_0 содержит ψ.

Из того, что σ является ψ-историей, атом a_0 соответствует ψ-состояниям произведения **A** и тогда переходим к следующему условию.

Условие 2. Пусть $(a_0 \bigcap AP_{\psi}) = \mathbf{a}_{\psi}^{0} = (a_0 \bigcap P_{\psi})$.

Условие 3. Для каждой формулы $\mathbf{X}\psi_1$ из замыкания $\mathrm{cl}(\psi)$ состояние a_i содержит $\mathbf{X}\psi_1$ тогда и только тогда, когда a_{i+1} содержит ψ_1.

Следующие условия относятся к оператору $\psi_1 \mathbf{U} \psi_2$. Условие 4 базируется на LTL-тождестве $\psi_1 \mathbf{U} \psi_2 \Leftrightarrow \psi_2 \vee (\psi_1 \wedge \mathbf{X}(\psi_1 \mathbf{U} \psi_2))$.

Условие 4. Для каждой формулы $\psi_1 \mathbf{U} \psi_2$ из замыкания $\mathrm{cl}(\psi)$ состояние a_i содержит $\psi_1 \mathbf{U} \psi_2$ тогда и только тогда, когда или a_i содержит ψ_2, или a_i содержит ψ_1 и a_{i+1} содержит $\psi_1 \mathbf{U} \psi_2$.

Условия (1)–(4) недостаточны для того, чтобы быть последовательностью Хинтикки. Дело в том, что если атом последовательности Хинтикки содержит формулу $\psi_1 \mathbf{U} \psi_2$, то согласно семантике оператора *until* формула ψ_2 должна принадлежать некоторому атому в точке, которая встречается позже. Из этого вытекает следующее условие.

Условие 5. Для каждой формулы $\psi_1 \mathbf{U} \psi_2$ из замыкания $\mathrm{cl}(\psi)$ и каждого $i \geq 0$, если состояние a_i содержит $\psi_1 \mathbf{U} \psi_2$, существует точка $j \geq i$ такая, что a_j содержит ψ_2.

Пример 13. Рассмотрим произведение **A** из примера 7 и формулу $u_0 \mathbf{U} t_1$. Тогда последовательность $\{u_0, \neg t_1, u_0 \mathbf{U} t_1\}(\{\neg u_0, t_1, u_0 \mathbf{U} t_1\})^{\omega}$ является последовательностью атомов, которая удовлетворяет условиям (1)–(5). Однако не существует ψ-истории σ такой, что $\pi_{\psi}(\sigma)$ эквивалентна этой последовательности атомов. Дело в том, что в **A** нет глобального перехода, преобразующего первый атом во второй этой последовательности. Действительно, должен быть глобальный переход **t** такой, что $((\bot, u_0), t, (t_1, \bot))$ является ψ-шагом. Но такого перехода в **A** нет.

Этот пример показывает, что два последовательных атома (a_i и a_{i+1}) должны быть согласованы с некоторым ψ-шагом, т.е. должны предполагать существование ψ-шага $(\mathbf{r}_i, \mathbf{t}_i, \mathbf{r}_{i+1})$, согласованного с переходами в **A**. Это означает выполнение следующего условия.

Условие 6. Для каждого $i \geq 0$ существует глобальный переход $\mathbf{t}_i$ такой, что $(\mathbf{r}_i, t_i, \mathbf{r}_{i+1})$ является ψ-шагом, где $\mathbf{r}_i = a_i \bigcap AP_{\psi}$ и $\mathbf{r}_i = a_{i+1} \bigcap AP_{\psi}$.

Используя условия 1–6, перейдем к следующему предложению.

Предложение 1. Бесконечная последовательность атомов является последовательностью Хинтикки тогда и только тогда, когда она удовлетворяет условиям 1–6.

Построение обобщенного Бюхи-тестера. Опишем формальный способ построения по последовательности Хинтикки обобщенного-Бюхи тестера для произведения ТС **A**.

Для определения тестера $\mathcal{BT} = (\mathcal{B}_\psi, \{F_0, \ldots, F_{k-1}\}, \lambda_\psi)$ необходимо сначала определить транзиционную систему $\mathcal{B}_\psi$ и функцию отметок λ_ψ:

• состояниями $\mathcal{B}_\psi$ являются все атомы вместе с дополнительным состоянием a_ψ^0, которое будет начальным состоянием тестера;

• множество переходов $\mathcal{B}_\psi$ состоит из

— переходов для каждого глобального перехода $\mathbf{t}_i$ и каждой пары атомов a_i и a_{i+1}, удовлетворяющих условиям 3, 4 и 6, началом перехода является a_i, концом — a_{i+1}, а отметкой этого перехода — $\mathbf{t}_i$;

— для того чтобы соединить начальное состояние с остальными состояниями, выполним следующие шаги: определим переход для каждого глобального перехода $\mathbf{t}_i$ и каждой пары состояний a_i, a_{i+1}, удовлетворяющих условиям 3, 4, 6, а состояние a_i, кроме того, удовлетворяет условиям 1, 2. Началом перехода является a_ψ^0, концом — состояние a_{i+1}, а отметкой — $\mathbf{t}_i$;

• выбор множеств $F_0, \ldots, F_{k-1}$ заключительных состояний выполняется так, чтобы истории $\mathcal{B}_\psi$ включали эти множества бесконечное число раз, этими множествами будут те, которые удовлетворяют условию 5.

Пусть $\psi_0 \mathbf{U} \psi'_0, \ldots, \psi_{k-1} \mathbf{U} \psi'_{k-1}$ — *until*-подформулы формулы ψ. Для каждого $i \in \{0, \ldots, k-1\}$ множество F_i определяется следующим образом: F_i содержит состояния a такие, что $\psi_i \mathbf{U} \psi'_i \notin a$ или $\psi'_i \in a$.

Обоснованием такого построения является следующее предложение.

Предложение 2. Бесконечная история $\sigma = \mathbf{t}_1 \mathbf{t}_2 \mathbf{t}_3 \ldots$ произведения **A** удовлетворяет условиям 1–6 тогда и только тогда, когда она распознается $\mathcal{BT}_\psi$.

Из этого и предыдущего утверждений вытекает следствие.

Следствие 1. Бесконечная история $\sigma = \mathbf{t}_1 \mathbf{t}_2 \mathbf{t}_3 \ldots$ произведения **A** выполняет формулу ψ тогда и только тогда, когда $\mathcal{BT}_\psi$ распознает σ.

Пример 14. Построим обобщенный Бюхи-тестер для произведения ТС **A** из примера 7 и формулы $\psi = F(u_0 \wedge \mathbf{X} u_0)$. Используя известные тождества, преобразуем ψ к виду

$$F(u_0 \wedge \mathbf{X} u_0) \Leftrightarrow (u_0 \vee \neg u_0) \mathbf{U} (u_0 \wedge \mathbf{X} u_0).$$

Отсюда получаем, что замыкание $\mathrm{cl}(\psi)$ включает такие формулы:

$$\mathrm{cl}(\psi) = \{u_0, \neg u_0, u_0 \vee \neg u_0, \neg(u_0 \vee \neg u_0), \mathbf{X} u_0, \neg \mathbf{X} u_0, u_0 \wedge \mathbf{X} u_0,$$
$$\neg(u_0 \wedge \mathbf{X} u_0), (u_0 \vee \neg u_0) \mathbf{U} (u_0 \wedge \mathbf{X} u_0), \neg((u_0 \vee \neg u_0) \mathbf{U} (u_0 \wedge \mathbf{X} u_0))\}.$$

Дальнейший анализ показывает, что формула $u_0 \vee \neg u_0$ входит во все атомы, а вхождение формулы $u_0 \wedge \mathbf{X} u_0$ в некоторый атом зависит от того, будут ли входить формулы u_0 и $\mathbf{X} u_0$ в тот самый атом. Следовательно, содержимое каждого атома полностью определяется вхождением в атомы следующих трех формул: $\{u_0, \mathbf{X} u_0, \psi\}$.

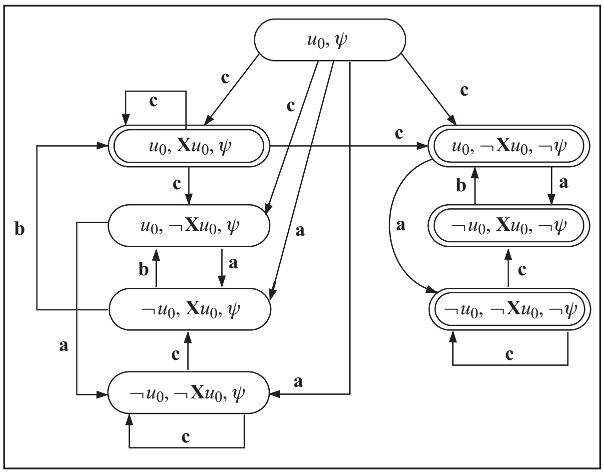

Рис. 7

Таким образом, получаем тестер (рис. 7), ограничиваясь только атомами, достижимыми из начального состояния с помощью определенных выше переходов. Множество заключительных состояний F_0 обозначено двойным начертанием.

Построение Бюхи-тестера по обобщенному тестеру выполняется с помощью известной процедуры [10, 11]. Оно сводится к построению k копий исходного тестера по одной для каждого заключительного множества $F_0, \ldots, F_k$. Переходы выбираются так, что Бюхи-тестер остается в в i-й копии до тех пор, пока не достигнет состояния из F_i. Если это случилось, то он переходит в $(i+1)$-ю копию по модулю k. Заключительными состояниями являются состояния из множества F_0. Очевидно, что такой тестер удовлетворяет свойству: между двумя попаданиями в состояния из F_0 он должен попасть в состояния из F_1, в состояния из F_2 и т.д.

В заключение отметим две основные проблемы, с которыми сталкиваются разработчики систем анализа программ. Основная проблема, которая препятствует широкому внедрению описанных методов, — проблема комбинаторного взрыва. Она состоит в том, что при моделировании реальной системы относительно небольших размеров ее математическая модель может иметь астрономическое число состояний и такой объект (СП или ТС) не может даже поместиться в память компьютера, что приводит к невозможности его дальнейшего анализа и обработки. На поиск решения этой проблемы направлены главные усилия специалистов в области разработки формальных методов анализа программного обеспечения.

Вторая проблема заключается в том, что имеющиеся алгоритмы анализа свойств обладают высокой временной и емкостной сложностью, что затрудняет их широкое использование в коммерческих системах анализа и верификации свойств формальных моделей реальных систем.

В общем случае ситуация выглядит так, что, с одной стороны, с каждым годом сложность программного обеспечения возрастает и необходимы автоматизированные средства их анализа, а с другой стороны, имеющиеся средства анализа свойств таких программных систем не могут обеспечить их надежную и качественную верификацию. В этом и заключаются, по нашему мнению, главные противоречия и трудности на текущий момент, связанные с разработкой надежного и высококачественного программного обеспечения.

СПИСОК ЛИТЕРАТУРЫ

1. Крывый С.Л., Максимец А.Н. Верификация программ: состояние, проблемы, результаты. I // Кибернетика и системный анализ. — 2013. — № 6. — С. 3–14.
2. Максимець О.М. Пошук програмних інваріантів у вигляді поліномів // Доп. НАН України. — 2013 — № 9. — С. 44–50.
3. Kryvyi S.L., Maksymets O.M. Program invariant generation over polynomial ring using iterative methods // Intern. J. «Information Theories & Applications». — 2013. — **20**, N 2. — P. 113–121.
4. Esparza J., Heljanko K. Unfoldings. A partial-order approach to model checking. — Berlin: Springer-Verlag, 2008. — 172 p.
5. Hack M.H.T. Decidability questions for Petri nets. — Ph.D. Thesis, M.I.T. — 1976. — 194 p.
6. Котов В.Е. Сети Петри. — М.: Наука, 1984. — 157 с.
7. Murata T. Petri nets: properties, analysis and applications // Proc. of the IEEE. — 1989. — **77**, N 4. — P. 541–580.
8. Карпов Ю.Г. Верификация параллельных и распределенных программных систем. — СПб: БХВ, 2010. — 551 с.
9. Кларк Е.М., Грумберг О., Пелед Д. Верификация моделей программ: Model Checking. — М.: Изд-во МЦНМО, 2002. — 416 с.
10. Трахтенброт Б.А., Барздинь Я.М. Конечные автоматы (Поведение и синтез). — М.: Наука, 1970. — 400 с.
11. Thomas W. Automata on infinite objects // Handbook on Theoretical Comput. Sci. — Elsiver, 1990. — Vol. B. — P. 135–191.

Поступила 15.04.2013