Российская академия наук
Сибирское отделение
Институт систем информатики
им. А. П. Ершова

Е. А. Покозий

МЕТОД ВЕРИФИКАЦИИ СВОЙСТВ ПАРАЛЛЕЛИЗМА ВРЕМЕННЫХ СЕТЕЙ ПЕТРИ

Препринт
61

Новосибирск 1999

В работе предложен метод верификации количественных свойств параллелизма в системах реального времени. Для этой цели вводится новая темпоральная логика реального времени TCCTL, которая является расширением языка ветвящегося времени CCTL, предложенного Пенчеком, за счет добавления временных ограничений на его операторы. Предложенная логика позволяет как различать точки параллельного ветвления и точки недетерминированного выбора, так и выражать временные аспекты поведения системы. Таким образом, TCCTL позволяет адекватно описывать системы, представленные моделями с семантикой "истинного параллелизма". В качестве модели параллельных систем реального времени используются временные сети Петри. Предлагается алгоритм анализа поведенческих свойств временных сетей Петри, основанный на темпоральной логике TCCTL. Алгоритм линеен по размеру формулы и экспоненциален по размеру сети.

Siberian Division of the Russian Academy of Sciences
A. P. Ershov Institute of Informatics Systems

E. A. Pokozy

TOWARD VERIFICATION OF CONCURRENT PROPERTIES OF TIME PETRI NETS

Preprint
61

Novosibirsk 1999

The intention of the paper is to develop an algorithm for verification of quantitative concurrent properties of real-time systems. For this purpose we introduce a new real-time temporal logic TCCTL which is similar extension of TCTL as CCTL is an extension of CTL. The proposed logic allows to distinguish concurrency from non-determinism. On the other hand, it is able to express quantitative aspects of the system behaviour using explicit time restrictions as a subscripts in temporal operators. So, TCCTL is a natural formalism for specification of concurrent real-time systems. In this paper we use time Petri nets for modelling of real-time systems. Note, that concurrency can be expressed in this model in a natural way. The TCCTL-based verification algorithm for time Petri nets is proposed. The algorithm of checking if the given time Petri net satisfies to the given TCCTL-formula is linear in the size of the formula and exponential in the size of the time Petri net.

1. ВВЕДЕНИЕ

Последние годы ведутся интенсивные исследования по применению аппарата темпоральных логик для спецификации и верификации распределенных систем реального времени. Известно, что логики линейного времени не различают точек ветвления, в то время как логики ветвящегося времени, распознавая точки ветвления, не различают истинного параллелизма и недетерминированного выбора. Например, для таких логик процессы $a \parallel b$ и $ab + ba$ имеют одно и то же множество путей — $\{ab, ba\}$, и, следовательно, неразличимы. Для спецификации существенно параллельных систем на основе логики ветвящегося времени CTL была разработана логика CCTL [5]. CCTL явно различает точки параллельного ветвления и ветвления по недетерминированному выбору, вводя в дерево путей структуру поддеревьев, представляющую множества путей, ведущих в одновременно достижимые состояния. В частности, CCTL различает процессы $a \parallel b$ и $ab + ba$, полагая в первом случае множеством поддеревьев $\{\{ab, ba\}\}$, во втором — $\{\{ab\}, \{ba\}\}$. С другой стороны, темпоральные логики дискретного времени позволяют выразить только качественные временные характеристики, а следовательно, не пригодны для анализа корректности систем реального времени, поведение которых в значительной степени зависит от количественных временных характеристик. В качестве модели систем реального времени рассматриваются временные сети модели Мерлина [4], где с каждым переходом связаны нижняя и верхняя границы его срабатывания. Далее приводится алгоритм верификации свойств временной сети Петри, выраженных в терминах TCCTL.

Материал статьи разбит на части следующим образом. Основные определения, касающиеся временной сети и ее поведения, даны в п. 2. Синтаксис и семантика темпоральной логики реального времени TCCTL рассматриваются в п. 3. В п. 4 строится конечное представление поведения временной сети, приводится алгоритм пометки на модели, дается оценка его сложности и доказывается его корректность.

2. ВРЕМЕННЫЕ СЕТИ

Введем ряд понятий, связанных с временной сетью модели Мерлина [4] и ее поведением. Под временной сетью понимается сеть Петри, где с

[0]Данная работа частично финансируется РФФИ-ИНТАС (грант № 95-0378)

каждым переходом связаны нижняя и верхняя временные границы его срабатывания.

Пусть $\mathbf{N}$ — множество натуральных чисел, $\mathbf{R}^+$ — множество неотрицательных вещественных чисел.

Определение 2.1. *Временная сеть* — это кортеж

$$\mathcal{N} = (P, T, F, Eft, Lft, m_0),$$

где

- $P = \{p_1, p_2, \ldots, p_m\}$ — конечное множество мест;
- $T = \{t_1, t_2, \ldots, t_n\}$ — конечное множество переходов ($P \cap T = \emptyset$);
- $F \subseteq (P \times T) \cup (T \times P)$ — отношение инцидентности;
- $Eft, Lft : T \to \mathbf{N}$ — функции, сопоставляющие каждому переходу $t \in T$ нижнюю (Eft) и верхнюю (Lft) временные границы, которые удовлетворяют следующему ограничению: $Eft(t) \leq Lft(t)$;
- $m_0 \subseteq P$ — начальная разметка.

Для перехода $t \in T$ определим ${}^\bullet t = \{p \in P \mid (p, t) \in F\}$ (множество входных мест) и $t^\bullet = \{p \in P \mid (t, p) \in F\}$ (множество выходных мест). Для упрощения представления полагаем, что ${}^\bullet t \cap t^\bullet = \emptyset$ для каждого перехода $t \in T$.

Пример временной сети приведен на рис. 1, где пара чисел, сопоставленная каждому переходу, представляет его нижнюю и верхнюю временные границы.

В дальнейшем временную сеть будем обозначать шестеркой

$$\mathcal{N} = (P, T, F, Eft, Lft, m_0).$$

Разметкой в $\mathcal{N}$ назовем произвольное подмножество m множества P мест, содержащих фишки. Переход t *готов к срабатыванию* при разметке m, если ${}^\bullet t \subseteq m$ (все входные места перехода t имеют фишки). Обозначим через $enable(m)$ множество переходов, готовых к срабатыванию при разметке m.

Пусть $\mathcal{V} = [T \to \mathbf{R}^+]$ — множество *значений счетчиков*, связанных с переходами из T. Для заданных $\nu \in \mathcal{V}$ и $\delta \in \mathbf{R}^+$ обозначим через $\nu + \delta$ значение счетчиков, равное $\nu(t) + \delta$ для каждого перехода t из T.

Состоянием в $\mathcal{N}$ будем называть пару $q = <m, \nu>$, где m — разметка в $\mathcal{N}$ и $\nu \in \mathcal{V}$. Тогда *начальное состояние* в $\mathcal{N}$ — это пара $q_0 = <m_0, \nu_0>$ такая, что $\nu_0(t) = 0$ для всех $t \in T$. Через S обозначим множество состояний в $\mathcal{N}$.

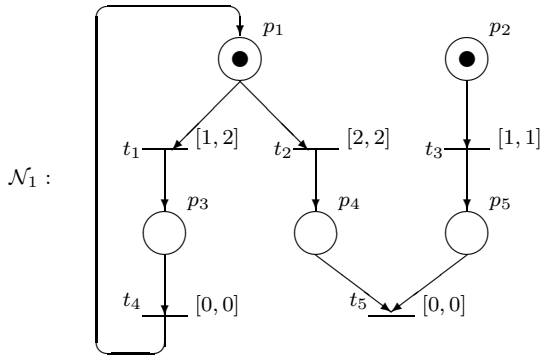

Рис. 1. Временная сеть $\mathcal{N}_1$

Во временной сети смена одного состояния другим осуществляется либо при истечении некоторого времени, либо при срабатывании некоторого перехода сети.

Будем говорить, что в состоянии $q = <m, \nu>$ переход $t \in T$ *может сработать* (обозначаем $t \in fireable(q)$), если $t \in enable(m)$ и $\nu(t) \geq Eft(t)$. Тогда состояние $q' = <m', \nu'>$ получается *при срабатывании перехода* t из состояния q (обозначаем $q \stackrel{0}{\Rightarrow} q'$), если

- $m' = (m \setminus^\bullet t) \cup t^\bullet$,
- $\forall t' \in T : \nu'(t') = \begin{cases} 0, \text{ если } t' \in enable(m') \setminus enable(m), \\ \nu(t') \text{ иначе.} \end{cases}$

Будем говорить, что в состоянии $q = <m, \nu>$ *может пройти время* $\delta \in \mathbf{R}^+$, если для всех $t \in enable(m)$ верно $\nu(t) + \delta \leq Lft(t)$. Тогда состояние $q' = <m', \nu'>$ получается *при истечении времени* δ из состояния q (обозначаем $q \stackrel{\delta}{\Rightarrow} q'$), если

- $m' = m$,
- $\nu'(t) = \nu(t) + \delta$ для всех $t \in T$.

Традиционно для описания поведения временных сетей используют последовательности состояний, называемые путями. Однако такое представление теряет информацию о параллелизме системы. Для сохранения этой информации введем понятие поддеревьев. Будем говорить,

что поддерево представляет одно из возможных альтернативных (конфликтных) поведений системы. Как и в п. 1 через S обозначаем множество состояний временной сети. Чтобы определить понятие поддерева, введем отношение $R \subseteq S \times 2^{\mathbf{R}^+ \times S}$. Неформально R сопоставляет состоянию q из S множество состояний, получающихся из q при истечении времени или при срабатывании переходов, которые могут выполняться параллельно.

Определим $TS(q)$ как множество максимальных подмножеств параллельных переходов, которые могут сработать в состоянии q. Формально

$$TS(q) = \{T' \subseteq fireable(q) \mid \begin{array}{l} \forall t, t' \in T'\ {}^\bullet t \cap {}^\bullet t' = \emptyset \wedge \\ \forall T'' \supset T'\ \exists t, t' \in T''.\ {}^\bullet t \cap {}^\bullet t' \neq \emptyset\}. \end{array}$$

Пусть $q \in S$ и $T' \in TS(q)$. Назовем *T'-потомком* состояния q (обозначим T'-$Succ(q)$) множество, состоящее из пар вида $(0, q)$, где $q \stackrel{t}{\Rightarrow} q'$ для некоторого $t \in T'$. Тогда

$$R = \{(q, T'\text{-}Succ(q)) \mid T' \in TS(q)\} \cup \{(q, (\delta, q')) \mid \exists \delta \in \mathbf{R}^+ . q \stackrel{\delta}{\Rightarrow} q'\}$$

Введем вспомогательное отношение $R_1 \subseteq S \times (\mathbf{R}^+ \times S)$ следующим образом: $(q, (\delta, q')) \in R_1$ тогда и только тогда, когда существует $(q, Q) \in R$ такое, что $(\delta, q') \in Q$.

Назовем *q-путем* r в $\mathcal{N}$ бесконечную последовательность состояний $q_i \in S$ и моментов времени $\delta_i \in \mathbf{R}^+$ вида $q_1 \stackrel{\delta_1}{\Rightarrow} \ldots q_n \stackrel{\delta_n}{\Rightarrow} \ldots$ таких, что $q = q_1$ и $(q_i, (\delta_i, q_{i+1})) \in R_1$, если q_{i+1} существует. Обозначим через r_n n-е состояние q-пути r. *Временной длительностью* q-пути r до n-го состояния назовем величину $time(r, n) = \sum_{1 \leq i < n} \delta_i$. *$q$-Поддеревом* tr в $\mathcal{N}$ назовем множество q-путей таких, что для любого r из tr и для любого $i \in \mathbf{N}$ пара $(r_i, \{(\delta'_i, r'_{i+1}) \mid r' \in tr \ \wedge\ r'_i \stackrel{\delta'_i}{\Rightarrow} r'_{i+1} \ \wedge\ r_j = r'_j\ \forall j \leq i\})$ принадлежит R. Множество всех q-поддеревьев обозначим через $Tr(q)$.

Проиллюстрируем введенные понятия на временной сети $\mathcal{N}_1$ (см. рис. 1). Для состояния $q_1 = \langle \{p_1, p_2\}, \nu \equiv 1 \rangle$ имеем $TS(q_1) = \{\{t_2, t_3\}\}$. Тогда

$$\{t_2, t_3\}\text{-}Succ(q_1) = \{(0, \langle \{p_2, p_4\}, \nu \equiv 1 \rangle), (0, \langle \{p_1, p_5\}, \nu \equiv 1 \rangle)\}$$

и

$$(q_1, \{t_2, t_3\}\text{-}Succ(q_1)) \in R.$$

Графическое представление q_1-поддерева tr в $\mathcal{N}_1$ показано на рис. 2.

q	m	$\nu(t_1)$	$\nu(t_2)$	$\nu(t_3)$	$\nu(t_4)$	$\nu(t_5)$
q_1	$\{p_1, p_2\}$	1	1	1	1	1
q_2	$\{p_2, p_3\}$	1	1	1	0	1
q_3	$\{p_3, p_5\}$	1	1	1	0	1
q_4	$\{p_1, p_5\}$	0	0	1	0	1
q_5	$\{p_1, p_2\}$	0	0	1	0	1
q_6	$\{p_1, p_5\}$	1	1	1	1	1
q_7	$\{p_1, p_5\}$	1.3	1.3	2.3	1.3	2.3

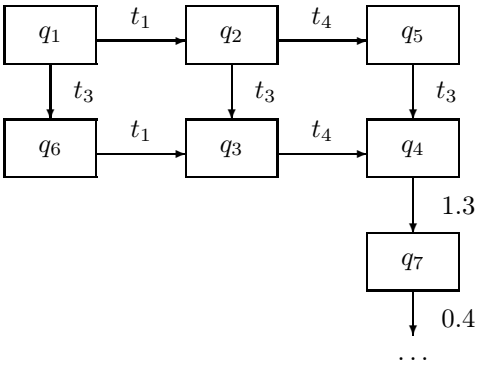

Рис. 2. q_1-Поддерево tr временной сети $\mathcal{N}_1$

Рассмотрим один из путей в tr:

$$r : q_1 \stackrel{\delta_1=0}{\Longrightarrow} q_2 \stackrel{\delta_2=0}{\Longrightarrow} q_3 \stackrel{\delta_3=0}{\Longrightarrow} q_4 \stackrel{\delta_4=1.3}{\Longrightarrow} q_7 \stackrel{\delta_5=0.4}{\Longrightarrow} \dots .$$

Тогда $time(r, 6) = \sum_{1 \le i < 6} \delta_i = 1.7$.

Состояние q *достижимо* в $\mathcal{N}$, если оно принадлежит некоторому q_0-пути. Обозначим через RS множество всех достижимых состояний в $\mathcal{N}$.

Будем говорить, что $\mathcal{N}$ *безопасна*, если для любого достижимого состояния $< m, \nu > \in RS$ и для любого перехода $t \in enable(m)$ верно $t^\bullet \cap m = \emptyset$. Для того чтобы исключить ситуацию, когда на некотором q-пути в $\mathcal{N}$ может сработать бесконечное число переходов за конечный отрезок времени, рассмотрим следующее условие (назовем его прогресс-условием): для всякого множества переходов $\{t_1, t_2, \dots, t_n\}$ таких, что $\forall\, 1 \le i < n$ $t_i^\bullet \cap^\bullet t_{i+1} \neq \emptyset$ и $t_n^\bullet \cap^\bullet t_1 \neq \emptyset$, верно

$$\sum_{1 \le i \le n} Eft(t_i) > 0.$$

Временная сеть $\mathcal{N}_1$ (см. рис. 1) удовлетворяет прогресс-условию, так как имеем $Eft(t_1) + Eft(t_4) = 1$.

Далее ограничимся рассмотрением безопасных временных сетей, удовлетворяющих прогресс-условию, и будем обозначать их через $\mathcal{N}$ с нижним индексом или без него.

3. TCCTL: СИНТАКСИС И СЕМАНТИКА

В данном пункте вводится темпоральная логика реального времени TCCTL (Timed Concurrent Computation Tree Logic), которая является расширением языка ветвящегося времени CCTL, предложенного Пенчеком [5], за счет добавления временных ограничений на его операторы.

Чтобы выражать свойства, связанные с параллелизмом, удобно иметь темпоральный оператор, позволяющий рассмотреть ситуацию после срабатывания некоторого перехода и дающий информацию о моменте времени, в который этот переход сработал. Такой оператор является аналогом оператора $Next$ в логиках дискретного времени для логик реального времени.

Опишем формально синтаксис и семантику языка TCCTL. Пусть AP — множество элементарных формул. Для наших целей удобно взять $AP = P$.

Определение 3.1. Пусть $c \in \mathbf{N}$ и $\sim$ — одно из бинарных отношений $<$, $\leq$, $=$, $\geq$, $>$. Определим множество $\mathcal{F}^s$ *state-формул* и множество $\mathcal{F}^{tr}$ *tree-формул* взаимно-индуктивно следующим образом:

1. $p \in AP$ — state-формула;
2. если ϕ_1 и ϕ_2 — state-формулы, то $\neg\phi_1$ и $\phi_1 \wedge \phi_2$ — state-формулы;
3. если ϕ_1 и ϕ_2 — state-формулы, то $\mathbf{A}X_{\sim c}\phi_1$,$\mathbf{E}X_{\sim c}\phi_1$, $\mathbf{A}\phi_1\mathcal{U}_{\sim c}\phi_2$, $\mathbf{E}\phi_1\mathcal{U}_{\sim c}\phi_2$ — tree-формулы;
4. если ϕ_1 и ϕ_2 — tree-формулы, то $\neg\phi_1$ и $\phi_1 \wedge \phi_2$ — tree-формулы;
5. если ϕ_1 — tree-формула, то $\forall\phi_1$ и $\exists\phi_1$ — state-формулы.

State-формулы интерпретируются на состояниях временной сети, в то время как tree-формулы интерпретируются на поддеревьях. Интуитивно state-формула $\forall\mathbf{E}\phi_1\mathcal{U}_{<c}\phi_2$ в данном состоянии q означает, что во всяком q-поддереве для некоторого вычисления системы существует префикс с временной длительностью, меньшей, чем c такой, что формула ϕ_2 истинна на его последнем состоянии, а формула ϕ_1 истинна на всех предыдущих состояниях. Tree-формула $\mathbf{E}X_{\leq c}\phi$ на поддереве tr означает, что в данном поддереве формула ϕ истинна на состоянии, получающемся при срабатывании некоторого перехода не позже, чем в момент времени c.

Приведем ряд используемых сокращений:

- $\mathbf{A}\Diamond_{\sim c}\phi \equiv \mathbf{A}true\ \mathcal{U}_{\sim c}\phi$,
- $\mathbf{E}\Diamond_{\sim c}\phi \equiv \mathbf{E}true\ \mathcal{U}_{\sim c}\phi$,
- $\mathbf{A}\Box_{\sim c}\phi \equiv \neg\mathbf{E}\Diamond_{\sim c}\neg\phi$,
- $\mathbf{E}\Box_{\sim c}\phi \equiv \neg\mathbf{A}\Diamond_{\sim c}\neg\phi$.

Определение 3.2. Для заданных состояния $q = <m, \nu> \in RS(\mathcal{N})$, поддерева $tr \in Tr(q)$ и формулы $\phi \in \mathcal{F}^s \cup \mathcal{F}^{tr}$ отношение *выводимости*

($\models$) определяется индуктивно следующим образом:

$$
\begin{array}{lll}
q \models p & <=> & p \in m; \\
q \models \neg\phi_1 & <=> & q \not\models \phi_1; \\
q \models \phi_1 \wedge \phi_2 & <=> & q \models \phi_1 \text{ и } q \models \phi_2; \\
q \models \forall\phi_1 & <=> & \forall tr \in Tr(q).\ tr \models \phi_1; \\
q \models \exists\phi_1 & <=> & \exists tr \in Tr(q).\ tr \models \phi_1;
\end{array}
$$

$$
\begin{array}{lll}
tr \models \neg\phi_1 & <=> & tr \not\models \phi_1; \\
tr \models \phi_1 \wedge \phi_2 & <=> & tr \models \phi_1 \text{ и } tr \models \phi_2; \\
tr \models \mathbf{A}\phi_1\mathcal{U}_{\sim c}\phi_2 & <=> & \forall r \in tr.\ r \models \phi_1\mathcal{U}_{\sim c}\phi_2; \\
tr \models \mathbf{E}\phi_1\mathcal{U}_{\sim c}\phi_2 & <=> & \exists r \in tr.\ r \models \phi_1\mathcal{U}_{\sim c}\phi_2; \\
tr \models \mathbf{A}X_{\sim c}\phi_1 & <=> & \forall r \in tr.\ r \models X_{\sim c}\phi_1; \\
tr \models \mathbf{E}X_{\sim c}\phi_1 & <=> & \exists r \in tr.\ r \models X_{\sim c}\phi_1.
\end{array}
$$

Для q-пути $r : <m_1, \nu_1> \stackrel{\delta_1}{\Rightarrow} <m_2, \nu_2> \stackrel{\delta_2}{\Rightarrow} \ldots$ в $\mathcal{N}$ верно $r \models \phi_1\mathcal{U}_{\sim c}\phi_2$ тогда и только тогда, когда существуют k и $\delta \leq \delta_k$ такие, что:

1. $(\delta + time(r, k)) \sim c$;
2. $<m_k, \nu_k + \delta> \models \phi_2$;
3. $\forall\, 1 \leq i < k\ .\ (<m_i, \nu_i> \models \phi_1 \wedge \forall\ 0 < \delta' < \delta_i\ .\ <m_i, \nu_i + \delta'> \models \phi_1)$;
4. $\forall\ 0 \leq \delta' < \delta\ .\ <m_k, \nu_k + \delta'> \models \phi_1$.

Для q-пути $r : <m_1, \nu_1> \stackrel{\delta_1}{\Rightarrow} <m_2, \nu_2> \stackrel{\delta_2}{\Rightarrow} \ldots$ в $\mathcal{N}$ верно $r \models X_{\sim c}\phi_1$ тогда и только тогда, когда существуют k и $\delta \leq \delta_k$ такие, что:

1. $(\delta + time(r, k)) \sim c$;
2. $<m_k, \nu_k + \delta> \models \phi_1$;
3. $\forall\, 1 < i < k\ .\ m_{i-1} = m_i\ \wedge\ m_{k-1} \neq m_k$.

Будем говорить, что $\mathcal{N}$ *удовлетворяет* формуле ϕ (обозначаем $\mathcal{N} \models \phi$), если $q_0 \models \phi$.

Рассмотрим временную сеть $\mathcal{N}_1$ (см. рис. 1) и state-формулу

$$\phi_1 = p_1 \wedge p_2 \wedge \forall\mathbf{E}X_{<2}p_3 \wedge \forall\mathbf{E}X_{<2}p_5,$$

выражающую для $\mathcal{N}_1$ свойство: "переходы t_1 и t_3 в момент времени, меньший 2, параллельны". Заметим, что $\mathcal{N}_1 \models \phi_1$, так как в $\mathcal{N}_1$ при любом параллельном исполнении в момент времени 1 относительно q_0 могут сработать переходы t_1 (появляется фишка в месте p_3) и t_3 (появляется фишка в месте p_5).

Теорема 3.1. Проблема TCCTL-выводимости Σ_1^1-сложна.

Доказательство. Следует из определения 3.2 и теоремы о неразрешимости TCTL [1]. □

4. ВЕРИФИКАЦИОННЫЙ АЛГОРИТМ

Цель данного пункта — разработать алгоритм, проверяющий, удовлетворяет ли временная сеть своим спецификациям, заданным в виде TCCTL-формулы.

Поскольку понятие временной сети базируется на модели непрерывного времени, то число состояний любой временной сети бесконечно. Чтобы получить конечное представление сетевого поведения, введем понятие обобщенного состояния, которое является аналогом региона [1]. Два состояния временной сети принадлежат одному и тому же обобщенному состоянию, если они в некотором смысле эквивалентны, т. е. их разметки совпадают и значения соответствующих счетчиков согласованы по целым частям и порядку дробных частей.

Для некоторого числа $\delta \in \mathbf{R}^+$ обозначим через $\lfloor \delta \rfloor$ его целую часть, а через $\{\delta\}$ — дробную.

Определение 4.1. Пусть $\nu, \nu' \in \mathcal{V}$. Тогда $\nu \simeq \nu'$, если и только если выполнены следующие условия:

- для любого $t \in T$ верно:

$$(\lfloor \nu(t) \rfloor = \lfloor \nu'(t) \rfloor) \ \vee \ (\nu(t) > Lft(t) \ \& \ \nu'(t) > Lft(t));$$

- для любых $t, t' \in T$ таких, что $\nu(t) \leq Lft(t)$ и $\nu(t') \leq Lft(t')$, верно:

$$\{\nu(t)\} \leq \{\nu(t')\} \Leftrightarrow \{\nu'(t)\} \leq \{\nu'(t')\};$$
$$\{\nu(t)\} = 0 \Leftrightarrow \{\nu'(t)\} = 0.$$

В качестве примера рассмотрим временную сеть $\mathcal{N}_2$ (см. рис. 2) и следующие значения счетчиков ее переходов: $\nu_1 = (1.99, 1.99, 0.13)$, $\nu_2 = (1.1, 1.1, 0.05)$, $\nu_3 = (1.1, 1.1, 0.8)$. Имеем $\nu_1 \simeq \nu_2$, однако $\nu_1 \not\simeq \nu_3$, так как $(\{\nu_1(t_3)\} < \{\nu_1(t_1)\}$ и $\{\nu_3(t_3)\} > \{\nu_3(t_1)\})$.

Лемма 4.1. Пусть $<m, \nu>, <m, \nu'> \in RS(\mathcal{N})$ такие, что $\nu \simeq \nu'$. Тогда для всякой state-формулы ϕ верно $<m, \nu> \models \phi \Leftrightarrow <m, \nu'> \models \phi$.

Доказательство. Прежде чем доказывать лемму, покажем, что в $\mathcal{N}$ существуют $<m, \nu>$-поддерево tr и $<m, \nu'>$-поддерево tr', эквивалентные в определенном ниже смысле. Для всякого $<m, \nu>$-пути

$$r : <m, \nu> = <m_1, \nu_1> \stackrel{\delta_1}{\Rightarrow} <m_2, \nu_2> \stackrel{\delta_2}{\Rightarrow} \ldots <m_i, \nu_i> \stackrel{\delta_i}{\Rightarrow} <m_{i+1}, \nu_{i+1}> \ldots$$

из tr существует $<m,\nu'>$-путь

$$r' : <m,\nu'> = <m_1,\nu'_1> \overset{\delta'_1}{\Rightarrow} <m_2,\nu'_2> \overset{\delta'_2}{\Rightarrow} ... <m_i,\nu'_i> \overset{\delta'_i}{\Rightarrow} <m_{i+1},\nu'_{i+1}> ...$$

из tr' такой, что для каждого $i \geq 1$ выполнены следующие условия эквивалентности между $(\nu_i, time(r,i))$ и $(\nu'_i, time(r',i))$ (обозначаем $(\nu_i,\ time(r,i)) \simeq (\nu'_i, time(r',i))$):

- $\nu_i \simeq \nu'_i$;
- значения $time(r,i)$ и $time(r',i)$ согласованы по целым частям, т. е.
  $\lfloor time(r,i) \rfloor = \lfloor time(r',i) \rfloor$,
  $\{time(r,i)\} = 0 \Leftrightarrow \{time(r',i)\} = 0$;
- дробные части значений $time(r,i)$ и $time(r',i)$ находятся в одном и том же отношении с дробными частями значений ν_i и ν'_i соответственно, т. е. для всякого перехода $t \in T$ верно:
  $\{\nu_i(t)\} < \{time(r,i)\} \Leftrightarrow \{\nu'_i(t)\} < \{time(r',i)\}$,
  $\{\nu_i(t)\} > \{time(r,i)\} \Leftrightarrow \{\nu'_i(t)\} > \{time(r',i)\}$.

Будем строить tr' пошагово по заданному tr. Пусть $<m,\nu'> \in tr'$, что не нарушает условий эквивалентности, так как $\nu \simeq \nu'$ и

$$time(r,1) = time(r',1) = 0$$

для всякого $<m,\nu>$-пути r из tr и для всякого $<m,\nu'>$-пути r' из tr'. Пусть все $<m,\nu'>$-пути из tr построены до i-го состояния. Рассмотрим некоторый $<m,\nu>$-путь r. Тогда существует $<m,\nu'>$-путь r', соответствующий r и построенный до i-го состояния.

По определению поддерева пара (r_i, Q) принадлежит R, где

$$Q = \{(\widetilde{\delta}_i, \widetilde{r}_{i+1}) \mid \widetilde{r} \in tr \wedge \widetilde{r}_i \overset{\widetilde{\delta}_i}{\Rightarrow} \widetilde{r}_{i+1} \wedge \forall j \leq i\ r_j = \widetilde{r}_j\}.$$

Рассмотрим произвольный путь $\widetilde{r}$ такой, что $(\widetilde{\delta}_i, \widetilde{r}_{i+1}) \in Q$. Теперь покажем, что по заданному $\widetilde{\delta}_i$ можно найти $\widetilde{\delta}'_i$ такое, что $\widetilde{r}'$ может быть продолжен до состояния $\widetilde{r}'_{i+1}$ без нарушения приведенных выше условий эквивалентности.

Определим множество Δ для пути $\widetilde{r}$ следующим образом:

$$\Delta = \{time(\widetilde{r}, i)\} \cup \{\nu_i(t) \mid t \in T\}.$$

Множество Δ' для пути $\widetilde{r}'$ определяется аналогично. Так как до i-го состояния путь $\widetilde{r}'$ построен корректно, то необходимое и достаточное

требование к значению $\widetilde{\delta}'_i$ заключается в том, чтобы значение каждого элемента множества Δ' пересекало некоторую целочисленную границу, если и только если эту границу пересекает значение соответствующего элемента множества Δ. Очевидно, что выбор $\widetilde{\delta}'_i$ зависит только от порядка дробных частей значений элементов в Δ', который совпадает с порядком дробных частей значений элементов в Δ. Следовательно, существование $\widetilde{\delta}_i$ гарантирует существование $\widetilde{\delta}'_i$. Таким образом, любой путь, совпадающий с r' до i-го состояния и соответствующий пути из tr, может быть продолжен до $(i+1)$-го состояния без нарушения условий эквивалентности. Заметим, что условие поддерева сохраняется и построенное таким образом множество путей является поддеревом.

Теперь докажем справедливость леммы индукцией по структуре формулы ϕ. Для базиса индукции (атомарных формул) и логических связок справедливость леммы очевидна. Рассмотрим случай $\phi = \exists\psi$ (случай $\psi = \forall\psi$ доказывается аналогично). Предположим, что $<m, \nu> \models \phi$. Тогда по определению 3.2 в $\mathcal{N}$ существует $<m, \nu>$-поддерево tr такое, что $tr \models \psi$. Для заданного tr существует $<m, \nu'>$-поддерево tr', построенное так, как показано выше. Покажем, что $tr' \models \psi$. Будем доказывать индукцией по структуре формулы ψ. Пусть $\widetilde{\psi}$ — tree-подформула формулы ψ.

- $\widetilde{\psi} = \neg\phi_1$.
  По определению 3.2 $tr \not\models \phi_1$. По предположению индукции имеем $tr' \not\models \phi_1$, следовательно, $tr' \models \widetilde{\psi}$.

- $\widetilde{\psi} = \phi_1 \wedge \phi_2$.
  По определению 3.2 $tr \models \phi_1$ и $tr \models \phi_2$. По предположению индукции имеем $tr' \models \phi_1$ и $tr \models \phi_2$, следовательно, $tr' \models \widetilde{\psi}$.

- $\widetilde{\psi} = \mathbf{E}\phi_1\mathcal{U}_{\sim c}\phi_2$ (случай $\widetilde{\psi} = \mathbf{A}\phi_1\mathcal{U}_{\sim c}\phi_2$ доказывается аналогично). По определению 3.2 в tr существует $<m, \nu>$-путь r такой, что $r \models \phi_1\mathcal{U}_{\sim c}\phi_2$, т. е. существует k и $\delta \leq \delta_k$ такие, что:
  1. $(\delta + time(r, k)) \sim c$;
  2. $<m_k, \nu_k + \delta> \models \phi_2$;
  3. $\forall\, 1 \leq i < k\, .\, (<m_i, \nu_i> \models \phi_1 \wedge \forall\, 0 < \delta' < \delta_i\, .\, <m_i, \nu_i + \delta'> \models \phi_1)$;
  4. $\forall\, 0 \leq \delta' < \delta\, .\, <m_k, \nu_k + \delta'> \models \phi_1$.

  По построению tr' существует $<m, \nu'>$-путь r' из tr', эквивалентный r. Покажем, что $r' \models \phi_1\mathcal{U}_{\sim c}\phi_2$. Необходимо рассмотреть четыре случая:

1) так как $(\nu_k, time(r,k)) \simeq (\nu'_k, time(r',k))$, то согласно построению r' по заданному δ можно найти δ' такое, что $(\nu_k + \delta, time(r,k)+\delta) \simeq (\nu'_k + \delta', time(r',k)+\delta')$. Тогда, исходя из того, что $(\delta' + time(r',k)) \sim c$, имеем $(\delta + time(r,k)) \sim c$;

2) так как $<m_k, \nu_k + \delta> \models \phi_2$, то по предположению индукции верно $<m_k, \nu'_k + \delta'> \models \phi_2$;

3) пусть $1 \leq i < k$ и $0 < \delta' < \delta'_i$. Так как $(\nu_i, time(r,i)) \simeq (\nu'_i, time(r',i))$, то согласно построению r' существует $0 < \delta < \delta_i$ такое, что $(\nu_i+\delta, time(r,i)+\delta) \simeq (\nu'_i+\delta', time(r',i)+\delta')$. Исходя из того, что $<m_i, \nu_i> \models \phi_1$ и $<m_i, \nu_i + \delta> \models \phi_1$, по предположению индукции имеем $<m_i, \nu'_i> \models \phi_1$ и $<m_i, \nu'_i + \delta'> \models \phi_1$;

4) аналогично пункту 3.

Таким образом, $r' \models \phi_1 \mathcal{U}_{\sim c} \phi_2$. Следовательно, $tr' \models \widetilde{\psi}$.

- $\widetilde{\psi} = \mathbf{E} X_{\sim c} \phi_1$ (случай $\widetilde{\psi} = \mathbf{A} X_{\sim c} \phi_1$ доказывается аналогично). По определению 3.2 в tr существует $<m, \nu>$-путь

$$r : <m_1, \nu_1> \stackrel{\delta_1}{\Rightarrow} <m_2, \nu_2> \stackrel{\delta_2}{\Rightarrow} \ldots$$

такой, что $r \models X_{\sim c} \phi_1$, т. е. существуют k и $\delta \leq \delta_k$ такие, что:
1. $(\delta + time(r,k)) \sim c$;
2. $<m_k, \nu_k + \delta> \models \phi_1$;
3. $\forall\, 1 < i < k \;.\; m_{i-1} = m_i \;\wedge\; m_{k-1} \neq m_k$.

По построению tr' существует $<m, \nu'>$-путь

$$r' : <m_1, \nu'_1> \stackrel{\delta'_1}{\Rightarrow} <m_2, \nu'_2> \stackrel{\delta'_2}{\Rightarrow} \ldots$$

из tr', эквивалентный r. Покажем, что $r' \models X_{\sim c} \phi_1$. Пункты 1) и 2) доказываются аналогично случаю $\widetilde{\psi} = \mathbf{E} \phi_1 \mathcal{U}_{\sim c} \phi_2$. Рассмотрим пункт 3). По построению r' имеем $m_i = m'_i$ $(i \in \mathbf{N})$. Тогда

$$\forall\, 1 < i < k \;.\; m_{i-1} = m_i \;\wedge\; m_{k-1} \neq m_k.$$

Таким образом, $r' \models X_{\sim c} \phi_1$. Следовательно, $tr' \models \widetilde{\psi}$.

Таким образом, $tr' \models \psi$ и, следовательно, по определению 3.2 $<m, \nu'> \models \phi$. □

Для того чтобы проверить истинность временных ограничений формулы ϕ, необходимо ввести дополнительный переход $t^* \notin T$, который не

готов к срабатыванию ни при одной разметке в $\mathcal{N}$, и поэтому его счетчик будет хранить значение времени, прошедшего с некоторого фиксированного начального момента. Рассмотрим формулу $\phi \in \mathcal{F}^s \cup \mathcal{F}^{tr}$, обозначим через c_ϕ максимальную константу, встречающуюся в ϕ. Пусть $T^* = T \cup \{t^*\}$ и $\mathcal{V}^* = [T^* \to \mathbf{R}^+]$. Определим отношение $\simeq^*_\phi$ как расширение отношения $\simeq$ на переход t^*, полагая $Lft(t^*)$ равным c_ϕ. Будем использовать $[\nu]^*_\phi$ для обозначения класса эквивалентности по $\mathcal{V}^*$, к которому принадлежит ν. Для $\nu \in \mathcal{V}$ и $x \in \mathbf{R}^+$ обозначим через $[x]\nu$ множество значений счетчиков из $\mathcal{V}^*$, в котором счетчику, соответствующему переходу t^*, сопоставлено значение x, а значения остальных счетчиков согласуются с ν. Для произвольного $t \in T^*$ введем следующее обозначение: $[\nu(t)]^*_\phi = \{\nu(t) \mid \nu \in [\nu]^*_\phi\}$.

Пусть $\phi \in \mathcal{F}^s \cup \mathcal{F}^{tr}$. *Обобщенным состоянием* в $\mathcal{N}$, существенным для ϕ, назовем пару $v = <m, [\nu]^*_\phi>$, где $<m, \nu> \in RS(\mathcal{N})$. Тогда *начальное* обобщенное состояние в $\mathcal{N}$, существенное для ϕ, — это пара $v_0 = <m_0, [[0]\nu_0]^*_\phi>$. Обозначим через $GS(\mathcal{N}, \phi)$ множество всех обобщенных состояний в $\mathcal{N}$, существенных для ϕ.

Обобщенные состояния во временной сети $\mathcal{N}_1$ (см. рис. 1), существенные для state-формулы

$$p_1 \wedge p_2 \wedge \forall\mathbf{E}X_{<2}p_3 \wedge \forall\mathbf{E}X_{<2}p_5,$$

показаны на рис. 3.

Пусть $<m, [\nu]^*_\phi>$, $<m', [\nu']^*_\phi>$ — различные обобщенные состояния из $GS(\mathcal{N}, \phi)$. Будем говорить, что $<m', [\nu']^*_\phi> = succ(<m, [\nu]^*_\phi>)$, если $m = m'$ и для некоторого положительного $\delta \in \mathbf{R}^+$ верно $\nu + \delta \in [\nu']^*_\phi$ и $\{\nu + \delta' \mid 0 \le \delta' \le \delta\} \subseteq [\nu]^*_\phi \cup [\nu']^*_\phi$.

Чтобы проиллюстрировать данное определение, рассмотрим временную сеть $\mathcal{N}_2$ (см. рис. 2) и некоторые ее обобщенные состояния, существенные для формулы $\forall\mathbf{A}\Diamond_{\ge 2}p_4$. Имеем

$$\begin{aligned}
v_1 &= \langle\{p_2, p_3\}, \{\nu' \mid \nu'(t_1) = \nu'(t_2) = \nu'(t^*) \in (0,1),\ \nu'(t_3) \in [0,0]\}\rangle,\\
v_2 &= succ(v_1) = \langle\{p_2, p_3\}, \{\nu' \mid \nu'(t_1) = \nu'(t_2) = \nu'(t^*) \in (0,1),\\
&\quad \nu'(t_3) \in (0,1), \{\nu'(t_3)\} < \{\nu'(t_1)\}\}\rangle,\\
v_3 &= succ(v_2) = \langle\{p_2, p_3\}, \{\nu' \mid \nu'(t_1) = \nu'(t_2) = \nu'(t^*) \in [1,1],\\
&\quad \nu'(t_3) \in (0,1)\}\rangle
\end{aligned}$$

и т.д.

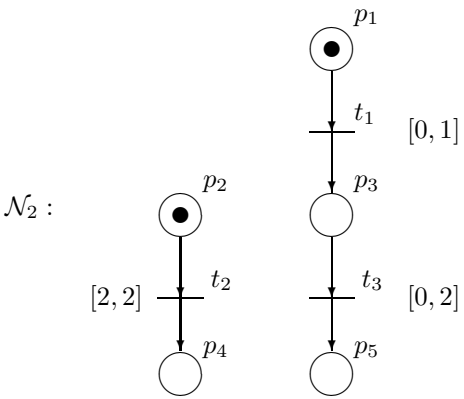

Рис. 3. Временная сеть $\mathcal{N}_2$

Структурой обобщенных состояний над $\mathcal{N}$ и $\phi \in \mathcal{F}^s$ назовем пару $\mathcal{M}(\mathcal{N}, \phi) = (V, E)$, где V — множество обобщенных состояний в $\mathcal{N}$, $E \subseteq V \times 2^V$ определяется следующим образом: $([q]^*_\phi, [Q]) \in E$, если $(q, Q) \in R$ и

$$[Q] = \{[q']^*_\phi \mid (0, q') \in Q \vee ([q']^*_\phi = succ([q]^*_\phi) \ \wedge \ \exists \delta > 0.\ (\delta, q') \in Q)\}.$$

Структура обобщенных состояний над временной сетью Петри $\mathcal{N}_1$ (см. рис. 1) и state-формулой

$$\phi_1 = p_1 \wedge p_2 \wedge \forall \mathbf{E} X_{<2} p_3 \wedge \forall \mathbf{E} X_{<2} p_5$$

показана на рис. 4, где дуга $(v, \widetilde{V})$ из E представляется множеством стрелок, объединенных чертой, или одиночной стрелкой в случае $\mid \widetilde{V} \mid = 1$. Обобщенные состояния временной сети $\mathcal{N}_1$ приведены в табл. 1.

Таблица 1

Обобщенные состояния временной сети $\mathcal{N}_1$

v	m	$[\nu]$						
		t_1	t_2	t_3	t_4	t_5	t^*	Порядок
v_0	11000	[0,0]	[0,0]	[0,0]	[0,0]	[0,0]	[0,0]	
v_1	11000	(0,1)	(0,1)	(0,1)	>0	>0	(0,1)	
v_2	11000	[1,1]	[1,1]	[1,1]	>0	>0	[1,1]	
v_3	01100	[1,1]	[1,1]	[1,1]	[0,0]	>0	[1,1]	
v_4	00101	[1,1]	[1,1]	[1,1]	[0,0]	>0	[1,1]	
v_5	10001	[0,0]	[0,0]	[1,1]	[0,0]	>0	[1,1]	
v_6	10001	(0,1)	(0,1)	>1	>0	>0	(1,2)	
v_7	10001	[1,1]	[1,1]	>1	>0	>0	[2,2]	
v_8	00101	[1,1]	[1,1]	>1	[0,0]	>0	[2,2]	
v_9	10001	[0,0]	[0,0]	>1	[0,0]	>0	[2,2]	
v_{10}	10001	(0,1)	(0,1)	>1	>0	>0	>2	
v_{11}	10001	[1,1]	[1,1]	>1	>0	>0	>2	
v_{12}	00101	[1,1]	[1,1]	>1	[0,0]	>0	>2	
v_{13}	10001	[0,0]	[0,0]	>1	[0,0]	>0	>2	
v_{14}	10001	(1,2)	(1,2)	>1	>0	>0	>2	
v_{15}	00101	(1,2)	(1,2)	>1	[0,0]	>0	>2	
v_{16}	10001	[2,2]	[2,2]	>1	>0	>0	>2	
v_{17}	00101	[2,2]	[2,2]	>1	[0,0]	>0	>2	
v_{18}	00011	[2,2]	[2,2]	>1	>0	[0,0]	>2	
v_{19}	00000	[2,2]	[2,2]	>1	>0	[0,0]	>2	
v_{20}	00000	>2	>2	>1	>0	>0	>2	
v_{21}	11000	[0,0]	[0,0]	[1,1]	[0,0]	>0	[1,1]	
v_{22}	10001	[1,1]	[1,1]	[1,1]	>0	>0	[1,1]	
v_{23}	10001	(1,2)	(1,2)	>1	>0	>0	(1,2)	
v_{24}	00101	(1,2)	(1,2)	>1	[0,0]	>0	(1,2)	
v_{25}	10001	[0,0]	[0,0]	>1	[0,0]	>0	(1,2)	
v_{26}	10001	(0,1)	(0,1)	>1	>0	>0	(1,2)	$fract(\nu(t^*)) > fract(\nu(t_1))$
v_{27}	10001	(0,1)	(0,1)	>1	>0	>0	[2,2]	
v_{28}	10001	[2,2]	[2,2]	>1	>0	>0	[2,2]	
v_{29}	00101	[2,2]	[2,2]	>1	[0,0]	>0	[2,2]	
v_{30}	00011	[2,2]	[2,2]	>1	>0	[0,0]	[2,2]	
v_{31}	00000	[2,2]	[2,2]	>1	>0	[0,0]	[2,2]	

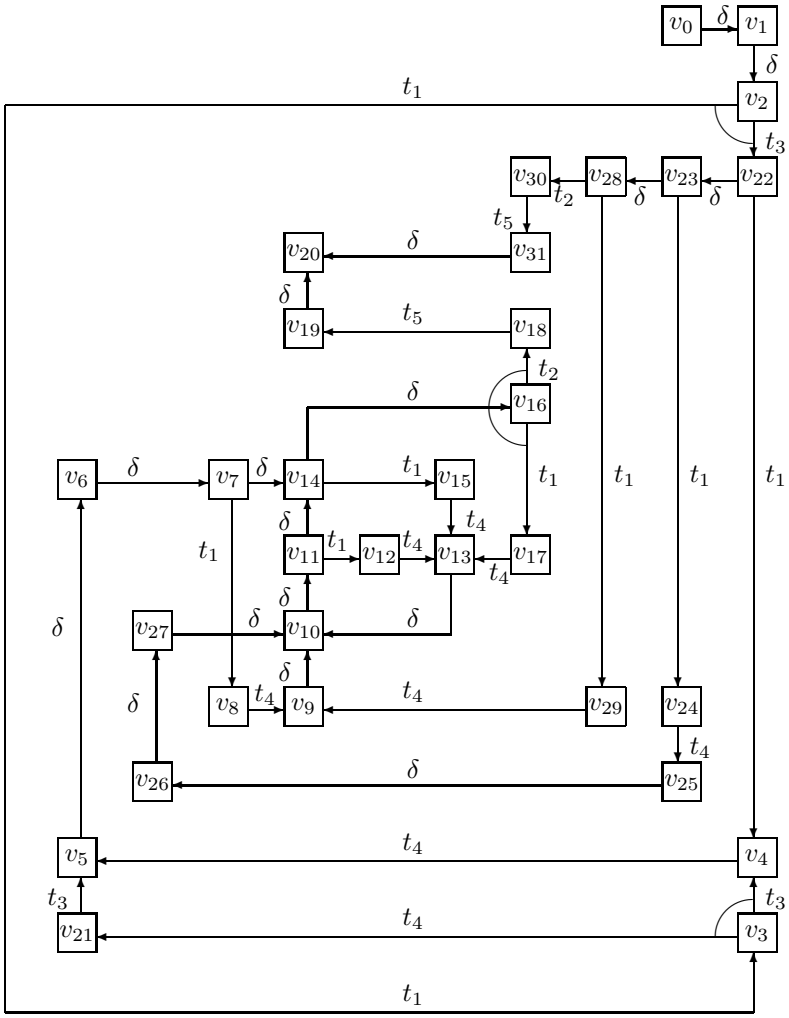

Рис. 4. Структура обобщенных состояний $\mathcal{M}(\mathcal{N}_1, \phi_5)$

Пусть $v, v' \in V$. Будем называть v-*путем* в структуре обобщенных состояний $\mathcal{M}(\mathcal{N}, \phi)$ последовательность $\Gamma = \langle v_1 v_2 \ldots \rangle$ вершин из V таких, что $v_1 = v$, и для любого $i \geq 1$ существует $[Q]$ такое, что $(v_i, [Q]) \in E$ и $v_{i+1} \in [Q]$, если v_{i+1} существует. Обозначим через Γ_n n-е состояние пути Γ.

v-Поддеревом Δ в структуре обобщенных состояний $\mathcal{M}(\mathcal{N},\phi)$ назовем множество v-путей структуры $\mathcal{M}(\mathcal{N},\phi)$ таких, что для любого Γ из Δ и для любого $i \in \mathbf{N}$ пара

$$(\Gamma_i, \{\Gamma'_{i+1} \mid \Gamma' \in \Delta \wedge \forall j \leq i \ \Gamma_j = \Gamma'_j\})$$

принадлежит E.

Пусть $(\widetilde{v},\widetilde{V}) \in E$. Будем говорить, что путь $\Gamma = \langle v_1 v_2 \ldots\rangle$ *принадлежит тому же v-поддереву, что и дуга* $(\widetilde{v},\widetilde{V})$, если существует путь $\widetilde{\Gamma} = \langle \widetilde{v}_1 \widetilde{v}_2 \ldots\rangle$, содержащий вершины $\widetilde{v},\widetilde{v}'$ (для некоторой $\widetilde{v}' \in \widetilde{V}$), совпадающий с Γ до вершины v_k $(k \geq 1)$, и существует дуга $(v_k, V_k) \in E$ такая, что $v_{k+1}, \widetilde{v}_{k+1} \in V_k$.

Теперь рассмотрим *алгоритм пометки* структуры $\mathcal{M}(\mathcal{N},\phi)$.

Будем помечать вершины из $\mathcal{M}(\mathcal{N},\phi)$ state-подформулами формулы ϕ или их отрицанием, начиная с подформул длины 1, затем длины 2 и т. д. Дополнительно помечаем дуги из $\mathcal{M}(\mathcal{N},\phi)$ tree-подформулами формулы ϕ или их отрицанием.

Для каждого индекса $' \sim c'$, встречающегося в ϕ, введем новую элементарную формулу $p_{\sim c}$. Помечаем вершину $<m, [\nu]^*_\phi>$ формулой $p_{\sim c}$, если $<m,\nu> \models \nu(t^*) \sim c$, иначе — формулой $\neg p_{\sim c}$.

Пусть v — вершина из $\mathcal{M}(\mathcal{N},\phi)$ и ψ — state-подформула формулы ϕ. Предположим, что все вершины из $\mathcal{M}(\mathcal{N},\phi)$ уже помечены state-подформулами формулы ψ или их отрицанием. Рассмотрим структуру формулы ψ.

- $\psi \in AP$. Если $\psi \in m$, то помечаем v формулой ψ, иначе — формулой $\neg\psi$.
- $\psi = \neg\phi_1$. Если v помечена формулой ϕ_1, то помечаем v формулой $\neg\psi$, иначе — формулой ψ.
- $\psi = \phi_1 \wedge \phi_2$. Если v помечена формулами ϕ_1 и ϕ_2, то помечаем v формулой ψ, иначе — формулой $\neg\psi$.
- $\psi = Q^1\phi_1$, где $Q^1 \in \{\forall, \exists\}$.
  Чтобы пометить вершину v формулой ψ, рассмотрим значение tree-формулы ϕ_1 на v-поддеревьях. Для этого помечаем дуги из $\mathcal{M}(\mathcal{N},\phi)$ tree-подформулами формулы ϕ_1. Пусть $\widetilde{\psi}$ — tree-подформула формулы ϕ_1. Предположим, что все дуги из $\mathcal{M}(\mathcal{N},\phi)$ уже помечены tree-подформулами формулы $\widetilde{\psi}$ или их отрицанием.

  Рассмотрим структуру формулы $\widetilde{\psi}$.

• $\widetilde{\psi} = \neg\phi_1$.

Если дуга $(\widetilde{v}, \widetilde{V})$ помечена формулой ϕ_1, то помечаем ее формулой $\widetilde{\psi}$, иначе — формулой $\neg\widetilde{\psi}$.

• $\widetilde{\psi} = \phi_1 \wedge \phi_2$.

Если дуга $(\widetilde{v}, \widetilde{V})$ помечена формулами ϕ_1 и ϕ_2, то помечаем ее формулой $\widetilde{\psi}$, иначе — формулой $\neg\widetilde{\psi}$.

• $\widetilde{\psi} = \mathbf{E}\phi_1\mathcal{U}_{\sim c}\phi_2$.

Дуга $(\widetilde{v}, \widetilde{V})$ помечается формулой $\widetilde{\psi}$, если существует v-путь $\Gamma = \langle v_1 v_2 \ldots\rangle$ в $\mathcal{M}(\mathcal{N}, \phi)$, который принадлежит тому же v-поддереву, что и дуга $(\widetilde{v}, \widetilde{V})$, и такой, что для некоторого $n \in \mathbf{N}$ v_i помечена формулой ϕ_1 для любого $1 \leq i < n$, а v_n помечена формулами ϕ_2 и $p_{\sim c}$.

• $\widetilde{\psi} = \mathbf{A}\phi_1\mathcal{U}_{\sim c}\phi_2$.

Дуга $(\widetilde{v}, \widetilde{V})$ помечается формулой $\widetilde{\psi}$, если для всякой вершины $\widetilde{v}' \in \widetilde{V}$ и для всякого v-пути $\Gamma = \langle v_1 v_2 \ldots\rangle$ в $\mathcal{M}(\mathcal{N}, \phi)$, для которого $\widetilde{v}, \widetilde{v}' \in \Gamma$, существует $n \in \mathbf{N}$ такой, что v_i помечена формулой ϕ_1 для любого $1 \leq i < n$; v_n помечена формулами ϕ_2 и $p_{\sim c}$.

• $\widetilde{\psi} = \mathbf{E}X_{\sim c}\phi_1$.

Дуга $(\widetilde{v}, \widetilde{V})$ помечается формулой $\widetilde{\psi}$, если существует v-путь $\Gamma = \langle v_1 v_2 \ldots\rangle$ в $\mathcal{M}(\mathcal{N}, \phi)$ $(v_i = <m_i, [\nu_i]^*_\phi> \forall i \in \mathbf{N})$, который принадлежит тому же v-поддереву, что и дуга $(\widetilde{v}, \widetilde{V})$ и такой, что для некоторого $n \in \mathbf{N}$ выполнено следующее: $m_1 = m_2 = \ldots = m_{n-1}$ и v_n помечена формулами ϕ_1 и $p_{\sim c}$.

• $\widetilde{\psi} = \mathbf{A}X_{\sim c}\phi_1$.

Дуга $(\widetilde{v}, \widetilde{V})$ помечается формулой $\widetilde{\psi}$, если для всякой вершины $\widetilde{v}' \in \widetilde{V}$ и для всякого v-пути $\Gamma = \langle v_1 v_2 \ldots\rangle$ в $\mathcal{M}(\mathcal{N}, \phi)$ $(v_i = <m_i, [\nu_i]^*_\phi> \forall i \in \mathbf{N})$, для которого $\widetilde{v}, \widetilde{v}' \in \Gamma$, существует $n \in \mathbf{N}$ такой, что $m_1 = m_2 = \ldots = m_{n-1}$ и v_n помечена формулами ϕ_1 и $p_{\sim c}$.

Вершина v помечается формулой ψ, если не существует дуги e из $\mathcal{M}(\mathcal{N}, \phi)$, помеченной формулой $\neg\phi_1$ (существует дуга $e = (v, \widetilde{V})$, помеченная формулой ϕ_1, в зависимости от квантора Q^1).

Алгоритм проверки, что $\mathcal{N} \models \phi$, состоит в следующем: строится структура обобщенных состояний $\mathcal{M}(\mathcal{N}, \phi)$, затем выполняется алго-

ритм ее пометки; $\mathcal{N}$ удовлетворяет ϕ, если и только если $\langle m_0, [[0]v_0]^*_\phi\rangle$ помечена ϕ.

Результат применения алгоритма пометки к структуре обобщенных состояний $\mathcal{M}(\mathcal{N}_1, \phi_1)$, где $\phi_1 = p_1 \wedge p_2 \wedge \forall\mathbf{E}X_{<2}p_3 \wedge \forall\mathbf{E}X_{<2}p_5$, приведен в табл. 2. Таким образом, получаем $\mathcal{N}_1 \models \phi_1$.

Следующая теорема устанавливает корректность алгоритма пометки.

Теорема 4.1. Пусть $<m, \nu> \in RS(\mathcal{N})$ и ψ — state-подформула формулы ϕ или ее отрицание. Приведенный выше алгоритм помечает вершину $<m, [\rhd\nu^*_\phi]$ из структуры обобщенных состояний $\mathcal{M}(\mathcal{N}, \phi)$ формулой ψ тогда и только тогда, когда $<m, \nu> \models \psi$.

Доказательство. Будем доказывать справедливость леммы индукцией по структуре state-формулы ψ. Случаи $\psi \in AP$, $\psi = \neg\phi_1$ и $\psi = \phi_1 \to \phi_2$ очевидны. Докажем, что алгоритм помечает $<m, [\nu]^*_\phi>$ формулой $\psi = \exists\psi_1$ тогда и только тогда, когда $<m, \nu> \models \psi$. Случай $\psi = \forall\psi_1$ доказывается аналогично.

($\Leftarrow$) Предположим, что $<m, \nu> \models \psi$. Тогда по определению 3.2 в $\mathcal{N}$ существует поддерево $tr \in Tr(<m, \nu>)$ такое, что $tr \models \psi_1$.

Для заданного поддерева tr в $\mathcal{N}$ будем строить пошагово соответствующее ему $<m, [\nu]^*_\phi>$-поддерево Δ в $\mathcal{M}(\mathcal{N}, \phi)$. Очевидно, что $<m, [\nu]^*_\phi> \in \Delta$. Пусть до i-го состояния каждого $<m, \nu>$-пути из tr построен соответствующий конечный $<m, [\nu]^*_\phi>$-путь в $\mathcal{M}(\mathcal{N}, \phi)$. Рассмотрим некоторый $<m, \nu>$-путь r из tr, и соответствующий ему конечный путь Γ из Δ.

По определению поддерева $(r_i, Q) \in R$, где

$$Q = \{(\widetilde{\delta}_i, \widetilde{r}_{i+1}) \mid \widetilde{r} \in tr \wedge \widetilde{r}_i \overset{\widetilde{\delta}_i}{\Rightarrow} \widetilde{r}_{i+1} \wedge \forall j \le i \; r_j = \widetilde{r}_j\}.$$

Рассмотрим произвольный путь $\widetilde{r}$ такой, что $(\widetilde{\delta}_i, \widetilde{r}_{i+1}) \in Q$. Строим конечный путь Γ^i в Δ следующим образом:

$$\Gamma^i = \{[\widetilde{r}_i]^*_\phi = <m^0_i, [\nu^0_i]^*_\phi>, \; <m^1_i, [\nu^1_i]^*_\phi>, \ldots, \; <m^{j_i}_i, [\nu^{j_i}_i]^*_\phi> = [\widetilde{r}_{i+1}]^*_\phi\}$$

где для всех $0 \le l < j_i$ верно $<m^{l+1}_i, [\nu^{l+1}_i]^*_\phi> = succ_\delta(<m^l_i, [\nu^l_i]^*_\phi>)$, если $<m_{i+1}, \nu_{i+1}>$ получается по истечении времени δ_i из $<m_i, \nu_i>$, иначе $j_i = 1$ и $(<m^0_i, [\nu^0_i]^*_\phi>, <m^1_i, [\nu^1_i]^*_\phi>) \in E$.

Таким образом, Γ может быть продолжен конечным путем Γ^i, не нарушая соответствия пути $\widetilde{r}$. Такое построение не нарушает и условия поддерева для Δ.

Таблица 2

Пометка вершин $\mathcal{M}(\mathcal{N}_1, \phi_1)$ state-подформулами ϕ_1 $(i = 3, 5)$

v	m	$[\nu(t^*)]$	$p_{\leq 2}$	p_1	p_2	p_3	p_5	$p_1 \wedge p_2$	$\forall \mathbf{E} X_{\leq 2} p_i$	ϕ_1
v_0	11000	[0,0]	1	1	1	0	0	1	1	1
v_1	11000	(0,1)	1	1	1	0	0	1	-	-
v_2	11000	[1,1]	1	1	1	0	0	1	-	-
v_3	01100	[1,1]	1	0	1	1	0	0	-	-
v_4	00101	[1,1]	1	0	0	1	1	0	-	-
v_5	10001	[1,1]	1	1	0	0	1	0	-	-
v_6	10001	(1,2)	1	1	0	0	1	0	-	-
v_7	10001	[2,2]	1	1	0	0	1	0	-	-
v_8	00101	[2,2]	1	0	0	1	1	0	-	-
v_9	10001	[2,2]	1	1	0	0	1	0	-	-
v_{10}	10001	> 2	0	1	0	0	1	0	-	-
v_{11}	10001	> 2	0	1	0	0	1	0	-	-
v_{12}	00101	> 2	0	0	0	1	1	0	-	-
v_{13}	10001	> 2	0	1	0	0	1	0	-	-
v_{14}	10001	> 2	0	1	0	0	1	0	-	-
v_{15}	00101	> 2	0	0	0	1	1	0	-	-
v_{16}	10001	> 2	0	1	0	0	1	0	-	-
v_{17}	00101	> 2	0	0	0	1	1	0	-	-
v_{18}	00011	> 2	0	0	0	0	1	0	-	-
v_{19}	00000	> 2	0	0	0	0	0	0	-	-
v_{20}	00000	> 2	0	0	0	0	0	0	-	-
v_{21}	11000	[1,1]	1	1	1	0	0	1	-	-
v_{22}	10001	[1,1]	1	1	0	0	1	0	-	-
v_{23}	10001	(1,2)	1	1	0	0	1	0	-	-
v_{24}	00101	(1,2)	1	0	0	1	1	0	-	-
v_{25}	10001	(1,2)	1	1	0	0	1	0	-	-
v_{26}	10001	(1,2)	1	1	0	0	1	0	-	-
v_{27}	10001	[2,2]	1	1	0	0	1	0	-	-
v_{28}	10001	[2,2]	1	1	0	0	1	0	-	-
v_{29}	00101	[2,2]	1	0	0	1	1	0	-	-
v_{30}	00011	[2,2]	1	0	0	0	1	0	-	-
v_{31}	00000	[2,2]	1	0	0	0	0	0	-	-

Покажем, что если $tr \models \psi_1$, то все дуги из Δ помечены ψ_1. Будем доказывать этот факт индукцией по структуре ψ_1. Пусть $\widetilde{\psi}$ — tree-подформула формулы ψ_1.

- Случаи $\widetilde{\psi} = \phi_1 \wedge \phi_2$ и $\widetilde{\psi} = \neg\phi_1$ очевидны.
- $\widetilde{\psi} = \mathbf{E}\phi_1\mathcal{U}_{\sim c}\phi_2$. Покажем, что если $tr \models \widetilde{\psi}$, то для всякой дуги e из Δ существует v-путь $\Gamma = \langle v_1 \dots v_n \dots \rangle$, который принадлежит тому же v-поддереву, что и e такой, что v_i помечена формулой ϕ_1 для любого $1 \le i < n$ и v_n помечена формулами ϕ_2 и $p_{\sim c}$. По определению 3.2 в $\mathcal{N}$ существует путь $r \in tr$ такой, что $r \models \phi_1\mathcal{U}_{\sim c}\phi_2$, т. е. существует k и $\delta \le \delta_k$ такие, что:
  1. $(\delta + time(r,k)) \sim c$;
  2. $< m_k, \nu_k + \delta > \models \phi_2$;
  3. $\forall\, 1 \le i < k\, .\, (< m_i, \nu_i > \models \phi_1 \wedge \forall\, 0 < \delta' < \delta_i\, .\, < m_i, \nu_i + \delta' > \models \phi_1)$;
  4. $\forall\, 0 \le \delta' < \delta\, .\, < m_k, \nu_k + \delta' > \models \phi_1$.

  Покажем, что для Γ, построенного так, как показано выше, существуют k и $l < j_k$ такие, что:

  а) $< m_k^l, [\nu_k^l]_\phi^* >$ помечено формулой $p_{\sim c}$;

  б) $< m_k^l, [\nu_k^l]_\phi^* >$ помечено формулой ϕ_2;

  в) любое $< m_{k'}^{l'}, [\nu_{k'}^{l'}]_\phi^* >$, стоящее в Γ раньше, чем $< m_k^l, [\nu_k^l]_\phi^* >$, помечено формулой ϕ_1.

  По построению Γ_k имеем $\exists 0 \le l \le j_k\, .\, \nu_k + \delta \simeq_\phi^* \nu_k^l$.

  а) Так как $time(r,k) = \nu_k(t^*)$, то $\delta + \nu_k(t^*) \sim c$. Следовательно, $\nu_k^l \sim c$, т. е. $< m_k^l, [\nu_k^l]_\phi^* >$ помечено формулой $p_{\sim c}$.

  б) Так как $< m_k, \nu_k + \delta > \models \phi_2$, то $< m_k^l, \nu_k^l > \models \phi_2$. Тогда по предположению индукции $< m_k^l, [\nu_k^l]_\phi^* >$ помечено формулой ϕ_2.

  в) Рассмотрим $< m_{k'}^{l'}, [\nu_{k'}^{l'}]_\phi^* >$, стоящее в Γ раньше $< m_k^l, [\nu_k^l]_\phi^* >$ (т. е. либо $k' < k$, либо $k' = k$ и $l' < l$). По построению $\Gamma_{k'}$ существует $0 \le \delta' \le \delta_{k'}$ такое, что $\nu_{k'} + \delta' \simeq_\phi^* \nu_{k'}^{l'}$. Так как $< m_{k'}, \nu_{k'} + \delta' > \models \phi_1$, то $< m_{k'}^{l'}, \nu_{k'}^{l'} > \models \phi_1$. Следовательно, по предположению индукции $< m_{k'}^{l'}, [\nu_{k'}^{l'}]_\phi^* >$ помечено формулой ϕ_1.

  Тогда согласно алгоритму все дуги из Δ помечены $\widetilde{\psi}$.
- Случаи $\widetilde{\psi} = \mathbf{A}\phi_1\mathcal{U}_{\sim c}\phi_2$, $\mathbf{A}X_{\sim c}\phi_1$, $\mathbf{E}X_{\sim c}\phi_1$ доказываются аналогично предыдущему.

Таким образом, все дуги из Δ помечены ψ_1. Следовательно, существует дуга $e = (v, \widetilde{V})$, помеченная формулой ψ_1, и, согласно алгоритму

пометки v помечена $\psi = \exists\psi_1$.

($\Rightarrow$) Обозначим вершину $<m, [\nu]^*_\phi>$ через v. Предположим, что вершина v помечена формулой $\psi = \exists\phi_1$ и существует дуга $e = (v, \widetilde{V})$, помеченная формулой ψ_1. Покажем, что тогда существует $<m, \nu>$-поддерево tr такое, что $tr \models \psi_1$. Будем доказывать этот факт индукцией по структуре ψ_1. Пусть $\widetilde{\psi}$ — tree-подформула формулы ψ_1.

- Случаи $\widetilde{\psi} = \neg\phi_1$ и $\widetilde{\psi} = \phi_1 \wedge \phi_2$ — очевидны.
- $\widetilde{\psi} = \mathbf{E}\phi_1\mathcal{U}_{\sim c}\phi_2$. Согласно алгоритму пометки существует v-путь

$$\Gamma = \langle v_1 = <m_n, [\nu_n]^*_\phi> \ldots v_n = <m_n, [\nu_n]^*_\phi> \ldots \rangle$$

в $\mathcal{M}(\mathcal{N}, \phi)$, который принадлежит тому же v-поддереву, что и e, и такой, что v_i помечена формулой ϕ_1 для любого $1 \leq i < n$; v_n помечена формулами ϕ_2 и $p_{\sim c}$. Построим соответствующий $\widetilde{\Gamma}$ $<m, \nu>$-путь

$$r : <m_1, \nu_1> \stackrel{\delta_1}{\Rightarrow} <m_2, \nu_2> \stackrel{\delta_2}{\Rightarrow} \ldots$$

в $\mathcal{N}$ такой, что для каждого $i \geq 1$ существует $\delta_i \in \mathbf{R}^+$ такое, что $<m_i, \nu_i> \stackrel{\delta_i}{\Rightarrow} <m_{i+1}, \nu_i + \delta_i>$ и $\nu_i + \delta_i \in [\nu_{i+1}]^*_\phi$. Далее, рассуждая, как в первой части доказательства, можно показать, что $r \models \mathbf{E}\phi_1\mathcal{U}_{\sim c}\phi_2$. Заметим, что существует поддерево $tr \in Tr(<m, \nu>)$ такое, что $r \in tr$. Тогда по определению 3.2 $tr \models \widetilde{\psi}$.

- Случаи $\widetilde{\psi} = \mathbf{A}\phi_1\mathcal{U}_{\sim c}\phi_2$, $\widetilde{\psi} = \mathbf{E}X_{\sim c}\phi_1$ и $\widetilde{\psi} = \mathbf{A}X_{\sim c}\phi_1$ доказываются аналогично предыдущему.

Таким образом, существует $<m, \nu>$-поддерево tr такое, что $tr \models \psi_1$. Следовательно, $<m, \nu> \models \psi$. □

Лемма 4.2. Число обобщенных состояний в $\mathcal{N}$, существенных для ϕ, ограничено величиной

$$|T^*|! \cdot 2^{2|T^*|+|P|} \cdot \prod_{t \in |T^*|} (Lft(t) + 1).$$

Доказательство. Класс эквивалентности $[\nu]^*_\phi$ по $\mathcal{V}^*$ относительно $\simeq^*_\phi$ можно представить тройкой массивов $<\alpha, \beta, \gamma>$, определенных ниже.

Массив α — T^*-индексированный массив, в котором каждому переходу $t \in T^*$ сопоставлен один из интервалов $[0,0]$, $(0,1)$, $[1,1]$, $\cdots$, $[Lft(t^*), Lft(t^*)]$, $(Lft(t^*), \infty)$. Таким образом, массив α представляет набор значений счетчиков ν, если и только если $\nu(t) \in \alpha(t)$ для любого $t \in T^*$.

Пусть T^*_α — множество переходов таких, что $\alpha(t)$ имеет вид $(i, i+1)$ для некоторого $i \leq Lft(t)$. Таким образом T^*_α — множество переходов с ненулевыми дробными частями значений счетчиков.

Массив $\beta : T^*_\alpha \to \{1 \cdots | T^*_\alpha |\}$ является перестановкой множества T^*_α, задающей порядок по отношению $\leq$ дробных частей значений счетчиков, связанных с переходами из T^*_α. Таким образом, массив β представляет набор значений счетчиков ν, если и только если для любой пары $t_1, t_2 \in T^*_\alpha$ верно $\{\nu(t_1)\} \leq \{\nu(t_2)\}$ при $\beta(t_1) \leq \beta(t_2)$.

Массив γ — булевозначный T^*_α-индексированный массив, определяющий переходы из T^*_α с одинаковыми дробными частями. Для перехода $t \in T^*_\alpha$ $\gamma(t)$ определяет, равна ли дробная часть значения его счетчика дробной части значения счетчика перехода, расположенного справа от t в массиве β. Таким образом, массив γ представляет набор значений счетчиков ν, если и только если для любого $t_1 \in T^*_\alpha$ верно $\gamma(t_1) = 0$, если существует $t_2 \in T^*_\alpha$ такой, что $\beta(t_2) = \beta(t_1) + 1$ и $\{\nu(t_1)\} = \{\nu(t_2)\}$.

Легко видеть, что число классов эквивалентности по $\mathcal{V}^*$ относительно $\simeq^*_\phi$ ограничено числом троек $< \alpha, \beta, \gamma >$ описанной выше формы. Число способов выбора α оценивается как

$$\prod_{t \in T^*} (2Lft(t) + 2).$$

Для заданного α число способов выбора β ограничено числом перестановок над T^*_α, которое равно $| T^* |!$, а число способов выбора γ ограничено числом булевозначных массивов над T^*_α, оцениваемым как $2^{|T^*|}$.

Пусть $< m, [\nu]^*_\phi >$ — обобщенное состояние в $\mathcal{N}$, существенное для ϕ. Так как m — массив длины $| P |$, состоящий из '0' и '1', то число различных разметок в $\mathcal{N}$ равно $2^{|P|}$. Как показано выше, число классов эквивалентности по $\mathcal{V}^*$, порожденных отношением $\simeq^*_\phi$, ограничено величиной

$$| T^* |! \cdot 2^{2^{|T^*|}} \cdot \prod_{t \in |T^*|} (Lft(t) + 1).$$

Таким образом, число обобщенных состояний в $\mathcal{N}$, существенных для

ϕ, ограничено величиной

$$|T^*|! \cdot 2^{2|T^*|+|P|} \cdot \prod_{t \in |T^*|} (Lft(t) + 1).$$

□

Теорема 4.2. Пусть ϕ — state-формула. Существует алгоритм проверки, что $\mathcal{N} \models \phi$, который удовлетворяет следующей оценке:

$$O[|\phi| \cdot c_\phi^2 \cdot |T|!^3 \cdot 2^{2(|P|+2|T|)} \cdot \prod_{t \in T} Lft(t)^2].$$

Доказательство. Из леммы 4.2. следует, что

$$|V| = O[c_\phi \cdot |T|! \cdot 2^{|P|+2|T|} \cdot \prod_{t \in T} Lft(t)].$$

Для вершины v в структуре обобщенных состояний $\mathcal{M}(\mathcal{N}, \phi)$ существует не более $|T|!$ различных множеств переходов и соответствующих им пар из E. Отсюда

$$|E| = O[c_\phi \cdot |T|!^2 \cdot 2^{|P|+2|T|} \cdot \prod_{t \in T} Lft(t)].$$

Далее $\mathcal{M}(\mathcal{N}, \phi)$ может быть построена за время

$$g = O[|V| + |E|] = O[|T|!^2 \cdot 2^{|P|+2|T|} \cdot \prod_{t \in T} Lft(t)].$$

Сложность пометки вершины пропозициональной state-формулой линейна. Рассмотрим state-формулу вида $Q\phi$, где $Q \in \{\forall, \exists\}$. Заметим, что пометка дуги некоторой tree-формулой может быть выполнена за один просмотр структуры обобщенных состояний. Пусть все дуги помечены tree-подформулами формулы $Q\phi$. Тогда сложность пометки вершины v формулой $Q\phi$ равна $O[|E|]$.

Таким образом, алгоритм проверки имеет сложность

$$O[|\phi| \cdot |E| \cdot |V|] = O[|\phi| \cdot c_\phi^2 \cdot |T|!^3 \cdot 2^{2(|P|+2|T|)} \cdot \prod_{t \in T} Lft(t)^2].$$

□

СПИСОК ЛИТЕРАТУРЫ

1. **Alur R., Dill D.** The theory of timed automata // Lect. Notes Comput. Sci. — 1991. — Vol. 600. — P. 45–73.
2. **Alur R., Henziger T.A.** Logics and models of real time: a survey // Ibid. — P. 74–106.
3. **Henzinger T.A., Manna Z., Pnueli A.** Timed transition systems // Ibid. — P. 226–251.
4. **Merlin P., Faber D.J.** Recoverability of communication protocols // IEEE Trans. Commun. — 1976. — Vol. 24, N 9.
5. **Penczek W.** A concurrent branching time temporal logic // Lect. Notes Comput. Sci. — 1990. — Vol. 440. — P. 337–354.
6. **Schneider S., a. o.** Timed CSP: theory and practice // Lect. Notes Comput. Sci. — 1991. — Vol. 600. — P. 640–675.
7. **Yoneda T., Shibayama A., Schlingloff B.H., Clarke E.M.** Efficient verification of parallel real-time systems // Lect. Notes Comput. Sci. — 1993. — Vol. 697. — P. 321–333.
8. **Вирбицкайте И.Б., Покозий Е.А.** Использование техники частичных порядков для верификации временных сетей Петри // Программирование. — 1999. — № 1.

Е. А. Покозий

МЕТОД ВЕРИФИКАЦИИ СВОЙСТВ ПАРАЛЛЕЛИЗМА ВРЕМЕННЫХ СЕТЕЙ ПЕТРИ

Препринт
61

Рукопись поступила в редакцию 23.04.1999
Рецензент А. В. Вотинцева
Редактор Л. А. Карева

Подписано в печать 28.04.1999
Формат бумаги 60×84 1/16 Объем 1,6 уч.-изд.л., 1,7 п.л.
Тираж 50 экз.

Отпечатано на ризографе “AL Group”
630090, г. Новосибирск, пр. Акад. Лаврентьева, 6