Раздел I.
Дискретные модели информационных систем

В. В. Подымов[1]

АЛГОРИТМ УПЛОЩЕНИЯ ИЕРАРХИЧЕСКИХ ВРЕМЕННЫХ АВТОМАТОВ*

Введение

Модели сетей временных автоматов (СВА) [1] и иерархических временных автоматов (ИВА) [2] нередко используются для формальной верификации распределённых систем реального времени (СРВ) [3], то есть систем параллельно работающих взаимодействующих компонентов, выполнение которых существенно зависит не только от порядка возникновения событий в системе, но и от реального времени возникновения этих событий. Модель СВА проста для понимания и выразительна, и потому популярна в сфере верификации СРВ. Основным недостатоком модели СВА является отсутствие средств описания иерархии компонентов СРВ: СВА представляет собой совокупность взаимодействующих конечных автоматов, функционирующих в реальном времени, и если одни компоненты СРВ являются составными частями других компонентов, то описание таких компонентов в модели СВА неестественно и подвержено труднообнаружимым ошибкам на стадии разработки модели. Основное отличие модели ИВА от модели СВА состоит в наличии средств описания иерархии компонентов СРВ: одни автоматы ИВА могут содержаться в других автоматах в качестве состояний. Типичная схема верификации ИВА H имеет следующий вид: производится *уплощение* (flattening) H, то есть преобразование H в СВА $\mathfrak{A}(H)$ со схожим (эквивалентным) поведением; выбирается требование заранее заданного вида, предъявляемое к поведению H и переформулируемое в равносильное требование к поведению СВА $\mathfrak{A}(H)$; проверка выполнимости требования для H сводится к проверке выполнимости равносильного требования для $\mathfrak{A}(H)$.

Вариации понятия ИВА, используемые в работах, посвящённых уплощению [2,4–6], несравнимы по выразительным возможностям и являются избыточно громоздкими ввиду привязки синтаксиса к устройству графического представления ИВА UML-диаграммами. В данной работе приводится более компактное определение ИВА, в рамках

[1]М.н.с. факультета ВМК МГУ имени М. В. Ломоносова, e-mail: valdus@yandex.ru.

*Исследование выполнено при финансовой поддержке РФФИ в рамках проекта № 18-01-00854.

которого можно переформулировать произвольные ИВА в смыслах, используемых в [2,4–6].

Понятия эквивалентности ИВА и СВА, используемые в [2,4–6], также различаются, и от точного вида рассматриваемой эквивалентности зависит общий вид требований, доказанно равновыполнимых на ИВА H и СВА $\mathfrak{A}(H)$. В [2,4] требования имеют вид достижимости заданной конфигурации при выполнении ИВА и СВА. В [5,6] используется понятие *эквивалентности по прореживанию*, позволяющее обосновать утверждение о равновыполнимости формул фрагмента логики ветвящегося действительного времени (TCTL), используемого в программном средстве верификации UPPAAL [1]. Понятие эквивалентности, предлагаемое в данной работе, является частным случаем отношения *бисимуляционной эквивалентности* с прореживанием, чувствительной к расхождению трасс (divergence-sensitive stutter bisimulation equivalence, [3]), адаптированной к особенностям поведения ИВА и СВА. Из эквивалентности ИВА и СВА, в частности, следует их эквивалентность по прореживанию. Выбор более строгого понятия эквивалентности продиктован желанием обосновать равновыполнимость всех TCTL-формул на произвольном ИВА H и СВА $\mathfrak{A}(H)$ в рамках дальнейшего исследования.

Основным результатом данной работы является описание алгоритма уплощения, строящего по произвольному ИВА эквивалентную СВА, и теорема 1 о корректности предложенного алгоритма. Вторичным результатом является теорема 2: утверждение о размерах компонентов СВА, получаемой в результате уплощения произвольного ИВА, показывающее меньший (полиномиальный) порядок числа состояний СВА $\mathfrak{A}(H)$ по сравнению с заявленным в [6] (экспоненциальным).

Общие черты иерархических временных автоматов и сетей временных автоматов

В данном разделе описываются общие структурные и поведенческие элементы моделей ИВА и СВА. Как ИВА, так и СВА в данном разделе называются просто автоматами.

Автомат строится над четырьмя конечными множествами: действительных *часов*, целочисленных *переменных*, *рандеву-каналов* и *широковещательных каналов* связи (по умолчанию — $\mathscr{C}$, $\mathscr{V}$, $\mathscr{P}$ и $\mathscr{B}$ соответственно). *Конфигурацией*, последовательно преобразуемой автоматом в процессе выполнения, задаются, в числе прочего, целочисленные значения переменных и неотрицательные действительные значения всех часов: *оценка переменных* $\mu : \mathscr{V} \to \mathbb{Z}$ и *оценка часов* $\nu : \mathscr{C} \to \mathbb{R}^{\geq 0}$, где $\mathbb{Z}$ и $\mathbb{R}^{\geq 0}$ — множества целых чисел и неотрицательных действительных чисел соответственно.

В описании автомата используются (целочисленные)

арифметические выражения в обычном понимании: переменные и целочисленные константы, соединённые арифметическими операциями. Точные синтаксис и семантика выражений в рамках данной работы несущественны и приводятся, например, в [1]. Далее используется только только следующая особенность арифметических выражений: для каждого выражения E и каждой оценки переменных μ определено целое число $\mu(E)$, являющееся *значением* выражения E на оценке μ.

Пусть $\sim$ — любое из отношений $<$, $\leq$, $>$, $\geq$, $=$, $\neq$. *Ограничение данных* — это выражение вида $E_1 \sim E_2$, где E_1 и E_2 — арифметические выражения. *Ограничение часов* — это выражение вида $c_1 \sim n$ или $c_1 - c_2 \sim n$, где $c_1, c_2 \in \mathscr{C}$ и n — неотрицательное целое число. *Предусловие* — это множество ограничений часов и данных. *Инвариант* — это предусловие, в котором используются только оценки часов вида $c_1 < n$ и $c_1 \leq n$.

Выполнимость ограничения данных $E_1 \sim E_2$, ограничений часов $c_1 \sim n$ и $c_1 - c_2 \sim n$ и предусловия g в конфигурации σ, содержащей оценку переменных μ и оценку часов ν, обозначается символом $\models$ и определяется следующим образом: $\sigma \models E_1 \sim E_2$, если верно соотношение $\mu(E_1) \sim \mu(E_2)$; $\sigma \models c_1 \sim n$, если верно соотношение $\nu(c_1) \sim n$; $\sigma \models c_1 - c_2 \sim n$, если верно соотношение $\nu(c_1) - \nu(c_2) \sim n$; $\sigma \models g$, если $\sigma \models e$ для каждого ограничения e, $e \in g$.

Присваивание арифметического выражения E переменной x — это выражение $(x \leftarrow E)$. Множество присваиваний *совместно*, если переменные в левых частях присваиваний этого множества попарно различны.

Записью $\mathbb{R}^{>0}$ обозначается множество положительных действительных чисел. При преобразовании конфигурации автоматом оценка переменных μ и оценка часов ν могут изменяться следующим образом. *Продвижение времени* на константу d, $d \in \mathbb{R}^{>0}$: оценка ν заменяется на оценку ν^{+d}, такую что $\nu^{+d}(c) = \nu(c) + d$ для каждых часов c. *Сброс часов* множества C: оценка ν заменяется на оценку $\nu[C]$, такую что $\nu[C](c) = 0$, если $c \in C$, и $\nu[C](c) = \nu(c)$ иначе. *Выполнение совместного множества присваиваний* $u = \{x_1 \leftarrow E_1, \ldots, x_k \leftarrow E_k\}$: оценка μ заменяется на оценку $\mu[u]$, такую что $\mu[u](x_i) = \mu(E_i)$, $1 \leq i \leq k$, и $\mu[u](y) = \mu(y)$, если $y \notin \{x_1, \ldots, x_k\}$.

Составные части автомата взаимодействуют (синхронизируются) посредством мгновенной передачи сигналов через каналы связи. Для описания передачи сигнала через канал ch, $ch \in \mathscr{P} \cup \mathscr{B}$, используются два выражения: *посылка* в канал ($ch!$) и *приём* из канала ($ch?$). Посылки и приёмы, а также специальный символ λ, обозначающий отсутствие посылок и приёмов, называются *синхронизациями*.

Символами $\mathfrak{G}$, $\mathfrak{I}$, $\mathfrak{U}$ и $\mathfrak{S}$ обозначаются множество всех предусловий, множество всех инвариантов, семейство всех совместных множеств

присваиваний и множество всех синхронизаций соответственно.

Иерархические временные автоматы

ИВА — это система $H = (L, \mathfrak{T}, L_s, I, EN, EX, en_0, \varphi, \psi, \mathscr{T})$, где:

- L — конечное множество *состояний*, содержащее хотя бы 2 элемента.
- $\mathfrak{T}$ — *дерево вложенности*: ориентированное корневое дерево с множеством вершин L и направлением дуг от корня к листьям. Внутренние вершины дерева вложенности называются *метасостояниями*, листья — *базовыми состояниями*. Множества всех метасостояний и базовых состояний обозначаются записями L_m и L_b соответственно. Корень дерева обозначается записью ℓ_{root}. Вершина, достижимая из ℓ по одной дуге, называется *вложенной* в ℓ. Множество всех вершин, вложенных в вершину ℓ, обозначается записью $nest(\ell)$. Множество всех вершин, достижимых из вершины ℓ, включая и саму вершину ℓ, обозначается записью $nest^*(\ell)$.
- L_s — множество *последовательных* метасостояний, $L_s \subseteq L_m$. Метасостояния, не являющиеся последовательными, называются *параллельными*. Множество всех параллельных метасостояний обозначается записью L_p.
- $I : L \to \mathfrak{I}$ — разметка состояний инвариантами.
- EN и EX — конечные множества *входов* и *выходов* соответственно.
- en_0 — *главный вход*, $en_0 \in EN$.
- $\varphi : L \to 2^{EN}$ — *входная разметка*, удовлетворяющая следующим свойствам. $\varphi(\ell_{root}) = \{en_0\}$. Если $\ell \in L_p$ и $\ell^+ \in nest(\ell)$, то $\varphi(\ell) = \varphi(\ell^+)$. Если $\ell \in L_s$, то $\varphi(\ell) \subseteq \cup_{\ell^+ \in nest(\ell)} \varphi(\ell^+)$. Если $\ell \in L_s$, $\{\ell_1^+, \ell_2^+\} \subseteq nest(\ell)$ и $\ell_1^+ \neq \ell_2^+$, то $\varphi(\ell_1^+) \cap \varphi(\ell_2^+) = \emptyset$.
- $\psi : L_b \to 2^{EX}$ — *выходная разметка*.
- $\mathscr{T}$ — *разметка переходами*, отображающая каждое последовательное метасостояние ℓ в множество *переходов* $\mathscr{T}(\ell)$: $\mathscr{T}(\ell) \subseteq nest(\ell) \times (EX \cup \{\perp\}) \times \mathfrak{G} \times \mathfrak{S} \times \mathfrak{U} \times 2^{\mathscr{C}} \times (EN \cup \{\perp\}) \times nest(\ell)$, где $\perp$ — специальный символ, отличный от всех входов и выходов. Переход $(\ell^s, ex, g, s, u, C, en, \ell^d)$, ведущий из состояния ℓ^s в состояние ℓ^d и помеченный компонентами ex, g, s, u, C, en, изображается следующим образом: $\ell^s \xrightarrow{ex,g,s,u,C,en} \ell^d$.

Для корректного функционирования ИВА на разметку $\mathscr{T}$ накладываются следующие ограничения. Если $(\ell^s \xrightarrow{ex,g,s,u,C,en} \ell^d) \in \mathscr{T}(\ell)$, то: $ex = \perp$ тогда и только тогда, когда $\ell^s \in L_b$; если $\ell^d \in L_b$, то $en = \perp$; если $\ell^d \in L_m$, то $en \in \varphi(\ell^d)$; если s — приём, то $u = \emptyset$. Если переходы с синхронизациями

через канал ch содержатся в множествах $\mathscr{T}(\ell_1)$ и $\mathscr{T}(\ell_2)$, где $\ell_1 \neq \ell_2$, то $\ell_1 \notin nest^*(\ell_2)$ и $\ell_2 \notin nest^*(\ell_1)$.

Деревом активности состояния ℓ ИВА H называется поддерево дерева $\mathfrak{T}$, содержащее корень ℓ, все вершины множества $nest(\ell')$ для каждого содержащегося параллельного метасостояния ℓ' и ровно одну вершину множества $nest(\ell'')$ для каждого содержащегося последовательного метасостояния ℓ''. *Деревом активности ИВА* H называется дерево активности состояния ℓ_{root}. Записью $\mathfrak{T}(\ell, en)$, где $\ell \in L$ и $en \in \varphi(\ell)$, обозначается наибольшее поддерево дерева $\mathfrak{T}$, содержащее только вершины множества $nest^*(\ell)$, помеченные входом en. *Начальным деревом активности* является дерево $\mathfrak{T}(\ell_{root}, en_0)$.

Конфигурацией ИВА H называется система (T, μ, ν), где T — дерево активности ИВА H, μ — оценка переменных и ν — оценка часов. Множество всех конфигураций ИВА H обозначается записью Σ_H. *Начальная конфигурация* ИВА H обозначается записью σ_H^0 и состоит из начального дерева активности ИВА H и оценок, отображающих все переменные и часы в число 0.

Метасостояние ℓ *завершаемо* через выход ex в конфигурации (T, μ, ν), если для каждого базового состояния, достижимого из ℓ в дереве T, верно соотношение $ex \in \psi(\ell)$. Для единообразия также полагаем, что базовое состояние завершаемо через $\perp$ в любой конфигурации. Переход $\ell^s \xrightarrow{ex,g,s,u,C,en} \ell^d$ *активен* в конфигурации σ, если выполнены три условия: $\ell^s \in T$; $\sigma \models g$; состояние ℓ^s завершаемо через ex в σ.

Рассмотрим конфигурацию $\sigma = (T, \mu, \nu)$ и множество переходов $\mathscr{X} = \{t_1, \ldots, t_k\}$, где $t_i = (\ell_i^s \xrightarrow{ex_i,g_i,s_i,u_i,C_i,en_i} \ell_i^d) \in \mathscr{T}(\ell_i)$, $1 \leq i \leq k$. Множество $\mathscr{X}$ *независимо*, если состояния ℓ_i попарно различны. Множество $\mathscr{X}$ *допустимо* в конфигурации σ, если оно независимо, каждый переход этого множества активен и, кроме того, выполнен один из следующих наборов условий:

1. $k = 1$; $s_1 = \lambda$.
2. $k = 2$; существует рандеву-канал ch, такой что $s_1 = ch!$ и $s_2 = ch?$.
3. Существует широковещательный канал ch, такой что $s_1 = ch!$ и $s_i = ch?$ для каждого i, $2 \leq i \leq k$; не существует активного перехода t, помеченного синхронизацией $ch?$ и такого что множество $\mathscr{X} \cup \{t\}$ независимо.

Записью $\sigma[\mathscr{X}]$ обозначается конфигурация $(T', \mu[u_1], \nu[C_1 \cup \cdots \cup C_k])$, где T' — дерево активности, получающееся из T заменой каждого поддерева с корнем в вершине ℓ_i^s, $1 \leq i \leq k$, на вершину ℓ_i^d, если $\ell_i^d \in L_b$, или на дерево $\mathfrak{T}(\ell_i^d, en_i)$, если $\ell_i^d \in L_m$. Конфигурация σ *допустима*, если верно соотношение $\sigma \models \cup_{\ell \in T} I(\ell)$. Записью σ^{+d}, где $d \in \mathbb{R}^{>0}$, обозначается конфигурация (T, μ, ν^{+d}).

Один шаг выполнения ИВА H задаётся отношениями $\rightarrow_H$ и $\mapsto_H$ на множестве $\Sigma_H \times \Sigma_H$: $\sigma' \rightarrow_H \sigma''$, если существует множество переходов $\mathscr{X}$, допустимое в конфигурации σ' и такое что $\sigma'' = \sigma'[\mathscr{X}]$, и конфигурация σ'' допустима; $\sigma' \mapsto_H \sigma''$, если существует число d, $d \in \mathbb{R}^{>0}$, такое что $\sigma'' = \sigma'^{+d}$, и конфигурация σ'' допустима.

Сети временных автоматов

Временной автомат — это система (L, en, L_c, I, T), где: L — непустое множество *состояний*; en — *начальное состояние*, $en \in L$; L_c — множество *срочных* состояний, $L_c \subseteq L$; $I : L \to \mathfrak{I}$ — разметка состояний инвариантами; $T \subseteq L \times \mathfrak{G} \times \mathfrak{S} \times \mathfrak{U} \times 2^{\mathscr{C}} \times L$ — множество *переходов*. Переход $t = (\ell^s, g, s, u, C, \ell^d)$, ведущий из состояния ℓ^s в состояние ℓ^d и помеченный компонентами g, s, u, C, изображается следующим образом: $\ell^s \xrightarrow{g,s,u,C} \ell^d$. Для корректного функционирования СВА на множество T налагается следующее ограничение: если $t \in T$ и s — приём, то $u = \emptyset$.

СВА — это непустое множество временных автоматов со взаимно непересекающимися множествами состояний. Далее полагается заданной СВА $N = \{A_1, \ldots, A_m\}$, где $A_i = (L^i, en^i, L^i_c, I^i, T^i)$, $1 \leq i \leq m$.

Конфигурацией СВА N называется система $(\mathscr{L}, \mu, \nu)$, где: $\mathscr{L}$ — множество, содержащее ровно одно состояние каждого автомата A_i, $1 \leq i \leq k$; μ — оценка переменных; ν — оценка часов. Множество всех конфигураций СВА N обозначается записью Σ_N. *Начальная конфигурация* СВА N обозначается записью σ^0_N и состоит из множества $\{en^1, \ldots, en^m\}$ и оценок, отображающих все переменные и часы в число 0.

Переход $\ell^s \xrightarrow{g,s,u} \ell^d$ *активен* в конфигурации $\sigma = (\mathscr{L}, \mu, \nu)$, если выполнены два условия: $\ell^s \in \mathscr{L}$; $\sigma \models g$.

Рассмотрим конфигурацию $\sigma = (\mathscr{L}, \mu, \nu)$ и непустое множество переходов $\mathscr{X} = \{t_1, \ldots, t_k\}$, где $t_i = (\ell^s_i \xrightarrow{g_i, s_i, u_i} \ell^d_i)$, $1 \leq i \leq k$. Множество $\mathscr{X}$ *независимо*, если содержит не более одного перехода каждого автомата A_i, $1 \leq i \leq m$. Множество $\mathscr{X}$ *приоритетно* в конфигурации σ, если верно хотя бы одно из двух: одно из состояний ℓ^s_i, $1 \leq i \leq m$, является срочным; в $\mathscr{L}$ не содержится срочных состояний. Множество $\mathscr{X}$ *допустимо* в конфигурации σ, если оно независимо и приоритетно в σ, каждый переход этого множества активен и, кроме того, выполнен один из следующих наборов условий:

1. $k = 1$; $s_i = \lambda$.
2. $k = 2$; существует рандеву-канал ch, такой что $s_1 = ch!$ и $s_2 = ch?$.
3. Существует широковещательный канал ch, такой что $s_1 = ch!$ и $s_i = ch?$ для каждого i, $2 \leq i \leq k$; не существует активного перехода t с синхронизацией $ch?$, такого что множество $X \cup \{t\}$ независимо.

Записью $\sigma[\mathscr{X}]$ обозначается конфигурация $(\mathscr{L}', \mu[u_1], \nu[C_1 \cup \cdots \cup C_k])$, где

$\mathscr{L}' = (\mathscr{L} \setminus \{\ell_1^s, \ldots, \ell_k^s\}) \cup \{\ell_1^d, \ldots, \ell_k^d\}$. Конфигурация σ *допустима*, если верно соотношение $\sigma \models \cup_{\ell \in \mathscr{L}} I(\ell)$. Записью σ^{+d}, где $d \in \mathbb{R}^{>0}$, обозначается конфигурация $(\mathscr{L}, \mu, \nu^{+d})$.

Один шаг выполнения СВА N задаётся отношениями $\to_N$ и $\mapsto_N$ на множестве $\Sigma_N \times \Sigma_N$: $\sigma' \to_N \sigma''$, если существует множество переходов $\mathscr{X}$, допустимое в конфигурации σ' и такое что $\sigma'' = \sigma'[\mathscr{X}]$, и конфигурация σ'' допустима; $\sigma' \mapsto_H \sigma''$, если существует число d, $d \in \mathbb{R}^{>0}$, такое что $\sigma'' = \sigma'^{+d}$, конфигурация σ'' допустима и конфигурация σ' не содержит срочных состояний.

Уплощение иерархических временных автоматов

Далее считаем заданными ИВА H над множествами часов и переменных $\mathscr{C}_H$, $\mathscr{V}_H$, СВА N над множествами часов и переменных $\mathscr{C}_N$, $\mathscr{V}_N$, где $\mathscr{C}_H \subseteq \mathscr{C}_N$ и $\mathscr{V}_H \subseteq \mathscr{V}_N$, и множество $\mathscr{E}$ всех ограничений часов и данных над $\mathscr{C}_H$, $\mathscr{V}_H$.

Рассмотрим функцию $\xi : (\Sigma_H \cup \Sigma_N) \to \mathscr{E}$ следующего вида: $\xi(\sigma)$ — множество всех ограничений e из $\mathscr{E}$, таких что $\sigma \models e$. ИВА H и СВА N *эквивалентны*, если существует отношение R, $R \subseteq \Sigma_H \times \Sigma_N$, такое что $(\sigma_H^0, \sigma_N^0) \in R$ и для каждой пары конфигураций (σ_1, σ_2), входящей в R, верно следующее:

1. $\xi(\sigma_1) = \xi(\sigma_2)$.
2. Если $\sigma_1 \mapsto_H \sigma_1'$, то существует конфигурация σ_2', такая что $\sigma_2 \mapsto_N \sigma_2'$ и $(\sigma_1', \sigma_2') \in R$.
3. Если $\sigma_2 \mapsto_N \sigma_2'$, то существует конфигурация σ_1', такая что $\sigma_1 \mapsto_H \sigma_1'$ и $(\sigma_1', \sigma_2') \in R$.
4. Если $\sigma_1 \to_H \sigma_1'$, то существует последовательность конфигураций $\sigma_2 \to_N \delta_1 \to_N \cdots \to_N \delta_k$, $k \geq 1$, такая что $\xi(\delta_1) = \cdots = \xi(\delta_k)$ и $(\sigma_1', \delta_k) \in R$.
5. Если $\sigma_2 \to_N \delta_1$, то существуют конфигурации σ_1', σ_2', такие что $\sigma_1 \to_H \sigma_1'$, $(\sigma_1', \sigma_2') \in R$ и для любой последовательности конфигураций $\delta_1 \to_N \delta_2 \to_N \ldots$ существует индекс k, такой что $\xi(\delta_1) = \cdots = \xi(\delta_k)$ и $\delta_k = \sigma_2'$.

Уплощением ИВА H называется построение СВА N, эквивалентной H.

Алгоритм уплощения

Предлагаемый *алгоритм уплощения* ИВА $H = (L, \mathfrak{T}, L_s, I, EN, EX, en_0, \varphi, \psi, \mathscr{T})$ над множествами $\mathscr{C}$, $\mathscr{V}$, $\mathscr{P}$, $\mathscr{B}$ состоит из трёх этапов: на первом этапе ИВА упрощается; на втором этапе по компонентам ИВА строится СВА N^2 над множествами $\mathscr{C}$, $\mathscr{V}$, $\mathscr{P}$, $\mathscr{B}$; на третьем этапе СВА N^2 изменяется с добавлением, в числе прочего,

новых переменных и каналов. СВА, построенная по итогам работы алгоритма для автомата H, обозначается записью $\mathfrak{A}(H)$. В описании алгоритма используются переменные, каналы и состояния со скобками «[]» в названии: полагается, что эти компоненты не содержатся в ИВА H.

Первый этап. Операция *спуска инварианта* с метасостояния ℓ устроена следующим образом: к инварианту каждого состояния множества $nest(\ell)$ добавляется множество $I(\ell)$; инвариант $I(\ell)$ заменяется на $\emptyset$. Инвариант спускается с корня ИВА, и затем, пока это возможно, с каждого метасостояния ℓ, вложенного в какое-либо параллельное метасостояние и такого что $I(\ell) \neq \emptyset$.

Разметка инвариантами, получающаяся после первого этапа, обозначается записью I^1. Очевидно, любая конфигурация допустима для ИВА с исходной разметкой I тогда и только тогда, когда она допустима для ИВА с изменённой разметкой I^1.

Второй этап. На этом этапе строится СВА $\{A[\ell] \mid \ell \in L_s\}$, где каждый автомат $A[\ell] = (L^\ell, en^\ell, L_c^\ell, I^\ell, T^\ell)$ задаётся следующим образом: $L^\ell = nest(\ell) \cup \{idle[\ell]\}$; если $\ell \in \mathfrak{T}(\ell_{root}, en_0)$, то en^ℓ — состояние множества $nest(\ell)$, помеченное входом en_0, иначе $en^\ell = idle[\ell]$; $L_c^\ell = \emptyset$; значения функции I^ℓ совпадают со значениями функции I^1 на множестве $nest(\ell)$, и $I^\ell(idle[\ell]) = \emptyset$; множество T^ℓ получается из множества $\mathscr{T}(\ell)$ удалением всех входов, выходов и символов $\perp$, помечающих переходы.

Третий этап. Для наглядности в записи переходов ИВА и СВА будут опускаться пустые множества, синхронизация λ и символ $\perp$, если это не приводит к неоднозначности определения перехода.

Для каждого перехода $\ell^s \xrightarrow{ex,g,s,u,C,en} \ell^d$ каждого множества $\mathscr{T}(\ell)$, такого что $en \neq \perp$, делается следующее. В СВА добавляется широковещательный канал $enter[\ell^d, en]$. В $A[\ell]$ добавляется срочное состояние $pre[\ell^d, en]$. Из $A[\ell]$ удаляется переход $\ell^s \xrightarrow{g,s,u,C} \ell^d$ (если не удалён ранее). В $A[\ell]$ добавляются два перехода: $\ell^s \xrightarrow{g,s,u,C} pre[\ell^d, en] \xrightarrow{enter[\ell^d,en]!} \ell^d$. Состояние $pre[\ell^d, en]$ помечается инвариантом $\cup_{\ell^* \in \mathfrak{T}(\ell^d, en)} I^1(\ell^*)$. Для каждого последовательного метасостояния ℓ^*, $\ell^* \in \mathfrak{T}(\ell^d, en)$, в $A[\ell^*]$ добавляется переход $idle_{\ell^*} \xrightarrow{pre[\ell^d,en]?} \ell^+$, где $\ell^+ \in nest(\ell^*)$ и $en \in \varphi(\ell^+)$.

Для каждого перехода $t = (\ell^s \xrightarrow{ex,g,s,u,C,en} \ell^d)$ каждого множества $\mathscr{T}(\ell)$, такого что $ex \neq \perp$, производятся следующие преобразования. В СВА добавляется широковещательный канал $exit[\ell^s, ex]$. В $A[\ell]$ добавляется срочное состояние $post[t]$. Переход $\ell^s \xrightarrow{g,s,u,C} \ell'$, где $\ell' = \ell^d$, если $en = \perp$, и $\ell' = pre[\ell^d, en]$ иначе, удаляется из $A[\ell]$, в $A[\ell]$ добавляются переходы $\ell^s \xrightarrow{g,s,u,C} post[t] \xrightarrow{exit[\ell^s,ex]!} \ell'$. Состояние $post[t]$ помечается инвариантом $I^\ell(\ell')$. Для каждого последовательного метасостояния ℓ^*,

$\ell^* \in nest^*(\ell^s)$, и каждого состояния ℓ^+, $\ell^+ \in nest(\ell^*)$, такого что хотя бы одно базовое состояние множества $nest^*(\ell^+)$ помечено выходом ex, в $A[\ell^*]$ добавляется переход $\ell^+ \xrightarrow{exit[\ell^s,ex]?} idle[\ell^*]$.

Записями $on(\ell,ex)$ и $off(\ell,ex)$, где ℓ — последовательное метасостояние и ex — выход, далее обозначаются соответственно числа 0 и 1, если состояние начального дерева активности ИВА H, вложенное в ℓ, помечено выходом ex, и числа 1 и 0 иначе.

Для каждых последовательного метасостояния ℓ, базового состояния ℓ^+, $\ell^+ \in nest(\ell)$, и выхода ex, $ex \in \psi(\ell^+)$, производятся следующие действия. В СВА добавляется переменная $inexit[\ell,ex]$. К метке u каждого перехода $\ell^+ \xrightarrow{g,s,u,C} \ell^t$ автомата $A[\ell]$, такого что $\ell^t \notin L_b$ или $ex \notin \psi(\ell^t)$, добавляется присваивание $(inexit[\ell,ex] \leftarrow off(\ell,ex))$. К метке u каждого перехода $\ell^s \xrightarrow{g,s,u,C} \ell^+$ автомата $A[\ell]$, такого что $\ell^s \notin L_b$ или $ex \notin \psi(\ell^s)$, добавляется присваивание $(inexit[\ell,ex] \leftarrow on(\ell,ex))$.

На последнем шаге третьего этапа алгоритма каждый переход $\ell \xrightarrow{g,s,u,C} post[t]$ каждого автомата строящейся СВА, где t — переход, помеченный выходом ex, заменяется на множество переходов вида $\ell \xrightarrow{g \cup g_i,s,u,C} post[t]$, $1 \le i \le k$, где число k и предусловия g_i определяются следующим образом. k — число попарно различных деревьев, получаемых удалением базовых состояний из всевозможных деревьев активности состояния ℓ ИВА H, все листья которых помечены выходом ex. Эти деревья произвольно пронумерованы от 1 до k. g_i — множество всех ограничений данных вида $(inexit[\ell',ex] = on(\ell',ex))$, где ℓ' — последовательное метасостояние i-го пронумерованного дерева активности, $1 \le i \le k$. Этим шагом завершается построение СВА $\mathfrak{A}(H)$.

Теорема 1. *Любой иерархический временной автомат H эквивалентен сети временных автоматов $\mathfrak{A}(H)$.*

Доказательство. Достаточно явно описать отношение R, определяющее эквивалентность, и обосновать справедливость свойств этого отношения. Подходящее отношение R задаётся следующим образом: $((\mu,\nu,T),(\mu',\nu',\mathscr{L})) \in R$ тогда и только тогда, когда $\mu = \mu'$, $\nu = \nu'$ и множество $\mathscr{L}$ состоит из всех состояний дерева T, вложенных в последовательные метасостояния ИВА H, и состояний $idle[\ell]$ для всех последовательных метасостояний ИВА H, не содержащихся в дереве T.

Соотношение $(\sigma_H^0,\sigma_N^0) \in R$ очевидным образом следует из определений начальной конфигурации ИВА и СВА и описания второго этапа алгоритма уплощения. Рассмотрим конфигурации $\sigma_H = (\mu,\nu,T)$ и $\sigma_N = (\mu,\nu,\mathscr{L})$, такие что $(\sigma_H,\sigma_N) \in R$. Первый пункт списка свойств отношения R очевидным образом следует из равенства оценок переменных и оценок часов конфигураций σ_H, σ_N. Справедливость второго и третьего пунктов обосновывается следующим образом. Без

ограничения общности можно полагать, что все состояния ИВА H с непустыми инвариантами вложены в последовательные метасостояния (первый этап уплощения). Все состояния, вложенные в последовательные метасостояния, добавляются в СВА $\mathfrak{A}(H)$ с теми же инвариантами, и инварианты всех состояний вида $idle[\ell]$ пусты (второй этап уплощения). Множество состояний дерева T, вложенных в последовательные метасостояния, совпадает с множеством, получаемым из $\mathscr{L}$ удалением всех состояний вида $idle[\ell]$ (по выбору отношения R), а значит, объединения всех инвариантов состояний дерева T и множества $\mathscr{L}$ совпадают. Справедливость четвёртого и пятого пунктов обосновывается следующим образом. Завершаемость метасостояния ℓ ИВА H через выход ex в σ_H равносильна выполнимости в σ_N одного из условий g_i, добавляемых на последнем шаге третьего этапа алгоритма уплощения для перехода, исходящего из ℓ и помеченного выходом ex. Следовательно, активность в σ_H перехода ИВА, исходящего из ℓ и помеченного предусловием g, равносильна активности перехода СВА, исходящего из ℓ и помеченного предусловием $g \cup g_i$. Значит, допустимость множества переходов $\mathscr{X}_H$ ИВА равносильна допустимости множества переходов $\mathscr{X}_N$ СВА, получающихся из переходов $\mathscr{X}_H$ в результате всех замен (на третьем этапе алгоритма) и исходящих несрочных состояний. По построению СВА, объединения всех присваиваний переменным $\mathscr{V}$ и объединения всех часов переходов $\mathscr{X}_H$ и $\mathscr{X}_N$ совпадают. Значит, оценки конфигураций σ_H и σ_N после применения этих присваиваний и сброса этих часов совпадают, и по заданию инвариантов *pre*- и *post*-состояний, конфигурации $\sigma_H[\mathscr{X}_H]$ и $\sigma_N[\mathscr{X}_N]$ одинаково допустимы. Если в конфигурации $\sigma_N[\mathscr{X}_N]$ не содержится срочных состояний, то по построению СВА верно $(\sigma_H[\mathscr{X}_H], \sigma_N[\mathscr{X}_N]) \in R$, в противном случае последующее преобразование конфигурации $\sigma_N[\mathscr{X}_N]$ состоит в обязательном выполнении переходов с синхронизациями по каналам *exit* и *enter* без изменения значений переменных и часов, и для первой полученной конфигурации σ'_N без срочных состояний верно соотношение $(\sigma_H[\mathscr{X}_H], \sigma'_N) \in R$.

Теорема 2. *Если ИВА H содержит n_c часов, n_v переменных, n_{ch} каналов, n_{en} входов, n_{ex} выходов, n_b базовых состояний, n_s последовательных метасостояний и n_t переходов, то СВА $\mathfrak{A}(H)$ содержит n_c часов, не более $(n_v + n_b)$ переменных, не более $(n_{ch} + n_s \cdot (n_{en} + n_{ex}))$ каналов, не более $(n_b + n_s \cdot (n_{en} + 2) + n_t \cdot n_{ex})$ состояний и не более $O(n_s \cdot n_{en} + n_t \cdot 2^{n_s})$ переходов.*

Справедливость теоремы 2 очевидна: можно легко посчитать количество компонентов СВА, добавление которых явно упомянуто в описании алгоритма уплощения. Экспонента в оценке числа переходов следует из дублирования переходов на последнем шаге третьего этапа

алгоритма уплощения — более точно, из экспоненциальности числа деревьев, которым соответствуют предусловия g_i.

Литература

1. *Behrmann G., David A., Larsen K.G.* A Tutorial on Uppaal // Formal Methods for the Design of Real-Time Systems: 4th International School on Formal Methods for the Design of Computer, Communication, and Software Systems, SFM-RT 2004. In series: LNCS. 2004. V. 3185. P. 200–236.
2. *David A., Möller M.O., Yi W.* Formal Verification of UML Statecharts with Real-Time Extensions // Fundamental Approaches to Software Engineering. 2002. P. 218–232.
3. *Baier C., Katoen J.-P.* Principles of Model Checking. The MIT Press, 2008.
4. *David A., Moller M.O.* From HUppaal to Uppaal: a translation from hierarchical timed automata to flat timed automata // Research Series RS-01-11, BRICS. Department of Computer Science, University of Aarhus. March 2001.
5. *Волканов Д.Ю., Захаров В.А., Зорин Д.А., Коннов И.В., Подымов В.В.* Как разработать простое средство верификации систем реального времени // Моделирование и анализ информационных систем. 2012. Т. 19. № 6. С. 45–56.
6. *Волканов Д.Ю., Захаров В.А., Зорин Д.А., Подымов В.В, Коннов И.В.* Комбинированное средство верификации распределенных вычислительных систем реального времени // Программирование. 2015. № 6. С. 72–86.