

Математические методы верификации схем и программ

mk.cs.msu.ru → Лекционные курсы
→ Математические методы верификации схем и программ

Блок 33

Сети временных автоматов

Лектор:

Подымов Владислав Васильевич

E-mail:

valdus@yandex.ru

ВМК МГУ, 2023/2024, осенний семестр

Вступление

Для **моделей Крипке** существуют способы автоматического построения параллельной композиции (**синхронной**, **асинхронной** и смешанной)

Такое построение позволяет избежать незаметных, но при этом критичных ошибок, которые пользователь может внести в модель, пытаясь описать такую композицию вручную, и тем самым упрощает разработку модели и повышает уверенность в её правильности

CPV, как и другие системы, как правило тоже состоят из параллельно выполняющихся компонентов

Ручное построение параллельной композиции временных автоматов, моделирующих компоненты CPV — это процесс даже более подверженный ошибкам, чем то же для моделей Крипке

Поэтому критичными оказываются и средства автоматического построения параллельной композиции временных автоматов

Автомат с синхронизацией

Временной автомат с синхронизацией $(S, s_0, \mathcal{I}, T, L)$ над множествами атомарных высказываний AP, часов \mathcal{C} и каналов синхронизации \mathcal{E} отличается от «обычного» временного автомата только тем, как устроены его переходы:

- ▶ $T \subseteq S \times CC(\mathcal{C}) \times 2^{\mathcal{C}} \times \text{Sync}(\mathcal{E}) \times S$, где $\text{Sync}(\mathcal{E})$ — множество действий синхронизации, устроенное так:

$$\text{Sync}(\mathcal{E}) = \{c! \mid c \in \mathcal{E}\} \cup \{c? \mid c \in \mathcal{E}\} \cup \{\lambda\}$$

Действие λ означает, что переход автомата выполняется так же, как и в обычном временном автомате, асинхронно относительно остальных автоматов сети

Переход (s, g, X, α, s') будем изображать так: $s \xrightarrow{g, X, \alpha} s'$

Если переход не помечен действием синхронизации, то это означает действие λ

Автомат с синхронизацией

$$T \subseteq S \times CC(\mathcal{C}) \times 2^{\mathcal{C}} \times \text{Sync}(\mathcal{C}) \times S$$
$$\text{Sync}(\mathcal{C}) = \{c! \mid c \in \mathcal{C}\} \cup \{c? \mid c \in \mathcal{C}\} \cup \{\lambda\}$$

Переход с действием $c!$ обязан выполняться одновременно с переходом с парным действием $c?$, то есть два автомата с выбранными переходами выполняются **синхронно**, но при этом асинхронно относительно остальных автоматов сети

Такой тип синхронизации принято называть **рандеву** (синонимы: **точка-точка**, **рукопожатие**, handshake, peer-to-peer)

Действия $c!$ и $c?$ будут «симметричны» с точки зрения семантики, но тем не менее в связи с тем, как на практике разрабатываются автоматы с синхронизацией, будем называть действие $c!$ **посылкой** сигнала в канал c , а действие $c?$ — **приёмом** сигнала из канала c

Сеть временных автоматов: синтаксис

Сеть временных автоматов (далее для краткости просто **сеть**) над множествами атомарных высказываний AP , часов \mathcal{C} и каналов синхронизации \mathcal{C} — это набор $\mathcal{N} = (\mathcal{A}_1, \dots, \mathcal{A}_n)$, где:

- ▶ $\mathcal{A}_i = (S^i, s_0^i, \mathcal{I}^i, T^i, L^i)$, $1 \leq i \leq n$, — временной автомат с синхронизацией над теми же часами \mathcal{C} и каналами \mathcal{C} и над множеством атомарных высказываний AP_i , где $AP_i \subseteq AP$
- ▶ $AP_i \cap AP_j = \emptyset$ для любых номеров i, j , таких что $1 \leq i < j \leq n$
- ▶ $AP_1 \cup \dots \cup AP_n = AP$
- ▶ $S_i \cap S_j = \emptyset$ для любых номеров i, j , таких что $1 \leq i < j \leq n$

Сеть временных автоматов: синтаксис

Пример

Смоделируем в виде сети автоматов такую систему:

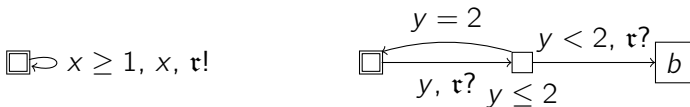
- ▶ Пользователь может посылать запросы на сервер
- ▶ *Из физических соображений* полагаем, что запросы посылаются не чаще чем раз в секунду
- ▶ Если сервер получил два запроса с интервалом строго менее двух секунд, то он ломается

Заведём в сети два автомата: один для пользователя, и один для сервера

Запрос смоделируем как сигнал в канале τ

То, что сервер сломан, смоделируем как атомарное высказывание b

Тогда сеть может быть устроена так:



Сеть временных автоматов: семантика

Рассмотрим сеть $\mathcal{N} = (\mathcal{A}_1, \dots, \mathcal{A}_n)$ над множеством часов \mathcal{C} , где $\mathcal{A}_i = (S^i, s_0^i, \mathcal{I}^i, T^i, L^i)$

Конфигурация сети \mathcal{N} — это пара (\vec{s}, ν) , где $\vec{s} \in S^1 \times \dots \times S^n$ и ν — оценка часов множества \mathcal{C}

Начальная конфигурация сети \mathcal{N} — это $((s_0^1, \dots, s_0^n), (0, 0, \dots, 0))$

Шаг вычисления $\rightarrow_{\mathcal{N}}$ сети \mathcal{N} — это двуместное отношение на множестве конфигураций, являющееся объединением трёх:

- ▶ **Продвижение времени:** $\sigma \mapsto_{\mathcal{N}} \sigma'$
- ▶ **Выполнение перехода:** $\sigma \hookrightarrow_{\mathcal{N}} \sigma'$
- ▶ **Шаг рандеву:** $\sigma \Rightarrow_{\mathcal{N}} \sigma'$

Сеть временных автоматов: семантика

Рассмотрим сеть $\mathcal{N} = (\mathcal{A}_1, \dots, \mathcal{A}_n)$ над множеством часов \mathcal{C} , где $\mathcal{A}_i = (S^i, s_0^i, \mathcal{I}^i, T^i, L^i)$

Для оценки часов ν , константы $d, d \in \mathbb{R}_{\geq 0}$, множества часов X , конфигурации σ и перехода t ряд обозначений дословно переносится с модели автомата на модель сети:

- ▶ $\nu + d$
- ▶ $\sigma + d$
- ▶ $\sigma \xrightarrow{d} \sigma'$
- ▶ $\nu[X]$
- ▶ $\sigma[X]$

$\sigma[s/s']$ — так будем обозначать конфигурацию, получающуюся из σ заменой состояния s одного из автоматов сети на s'

$\sigma \xrightarrow{s_i \xrightarrow{g, X, \alpha} s'_i} \sigma'$ означает, что $\sigma' = \sigma[X][s_i/s'_i]$

Сеть временных автоматов: семантика

Рассмотрим сеть $\mathcal{N} = (\mathcal{A}_1, \dots, \mathcal{A}_n)$ над множеством часов \mathcal{C} , где $\mathcal{A}_i = (S^i, s_0^i, \mathcal{I}^i, T^i, L^i)$, и конфигурации $\sigma = ((s_1, \dots, s_n), \nu)$ и σ'

Продвижение времени

$\sigma \mapsto_{\mathcal{N}} \sigma'$, если существует константа $d \in \mathbb{R}_{>0}$, такая что:

1. $\sigma \xrightarrow{d} \sigma'$
2. $\nu + d \models \mathcal{I}^1(s_1) \& \dots \& \mathcal{I}^n(s_n)$

Выполнение перехода

$\sigma \hookrightarrow_{\mathcal{N}} \sigma'$, если в сети \mathcal{N} есть переход $t = (s_k \xrightarrow{g, X, \lambda} s'_k)$, такой что:

1. $\nu \models g$
2. $\sigma \xrightarrow{t} \sigma'$
3. $\nu[X] \models \mathcal{I}^k(s'_k)$

Сеть временных автоматов: семантика

Рассмотрим сеть $\mathcal{N} = (\mathcal{A}_1, \dots, \mathcal{A}_n)$ над множеством часов \mathcal{C} , где $\mathcal{A}_i = (S^i, s_0^i, \mathcal{I}^i, T^i, L^i)$, и конфигурации $\sigma = ((s_1, \dots, s_n), \nu)$ и σ'

Шаг рандеву

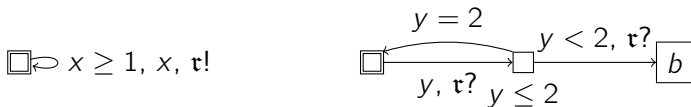
$\sigma \Rightarrow_{\mathcal{N}} \sigma'$, если в сети \mathcal{N} есть канал c и переходы $t_1 = (s_k \xrightarrow{g_k, X_k, c!} s'_k)$ и $t_2 = (s_m \xrightarrow{g_m, X_m, c?} s'_m)$, такие что:

- ▶ $k \neq m$
- ▶ $\nu \models g_k \ \& \ g_m$
- ▶ Для некоторой конфигурации σ'' верно $\sigma \xrightarrow{t_1} \sigma'' \xrightarrow{t_2} \sigma'$
- ▶ $\nu[X_k][X_m] \models \mathcal{I}^k(s'_k) \ \& \ \mathcal{I}^m(s'_m)$

Понятия, основанные на отношении $\rightarrow_{\mathcal{N}}$, дословно переносятся с модели временного автомата на модель сети: **трасса** (в том числе начальная, тупиковая, конвергентная, дивергентная, зеноновская), **вычисление**, **корректность**

Сеть временных автоматов: семантика

Пример



Это корректная сеть над часами $\{x, y\}$, и вот пример её вычисления для порядка часов (x, y) и для имён состояний (слева направо) n, ℓ, c, r :

$$\begin{aligned} & ((n, \ell), (0, 0)) \\ \mapsto & ((n, \ell), (\sqrt{2}, \sqrt{2})) \\ \Rightarrow & ((n, c), (0, 0)) \\ \mapsto & ((n, c), (2, 2)) \\ \hookrightarrow & ((n, \ell), (2, 2)) \\ \Rightarrow & ((n, c), (0, 0)) \\ \mapsto & ((n, c), (1, 1)) \\ \Rightarrow & ((n, r), (0, 1)) \\ \mapsto & ((n, r), (1, 2)) \\ \mapsto & ((n, r), (2, 3)) \\ & \mapsto \dots \end{aligned}$$

Трансляция сети в автомат

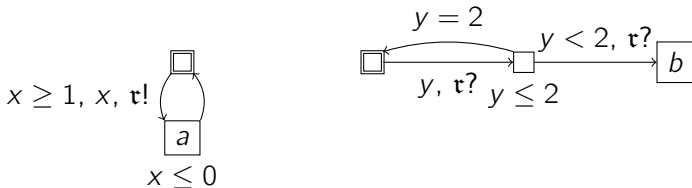
Рассмотрим произвольную сеть $\mathcal{N} = (\mathcal{A}_1, \dots, \mathcal{A}_n)$, где $\mathcal{A}_i = (S^i, s_0^i, \mathcal{I}^i, T^i, L^i)$

Записью $\otimes \mathcal{N}$ обозначим временной автомат $(S, s_0, \mathcal{I}, T, L)$ над теми же атомарными высказываниями и часами, устроенный так:

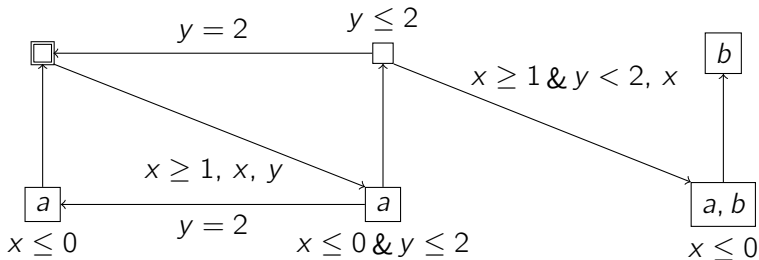
- ▶ $S = S^1 \times \dots \times S^n$
- ▶ $s_0 = (s_0^1, \dots, s_0^n)$
- ▶ $\mathcal{I}(s^1, \dots, s^n) = \mathcal{I}^1(s^1) \& \dots \& \mathcal{I}^n(s^n)$
- ▶ $L(s^1, \dots, s^n) = L(s^1) \cup \dots \cup L(s^n)$
- ▶ В T входят следующие переходы и только они:
 - ▶ $(s^1, \dots, s^n) \xrightarrow{g, X} (s^1, \dots, s^{i-1}, q^i, s^{i+1}, \dots, s^n)$, если $(s^i \xrightarrow{g, X, \lambda} q^i) \in T^i$
 - ▶ $(s^1, \dots, s^n) \xrightarrow{g_1 \& g_2, X_1 \cup X_2} (s^1, \dots, s^{i-1}, q^i, s^{i+1}, \dots, s^{j-1}, q^j, s^{j+1}, \dots, s^n)$, если $i < j$ и существует канал c , такой что $(s^i \xrightarrow{g_1, X_1, \alpha_1} q^i) \in T^i$ и $(s^j \xrightarrow{g_2, X_2, \alpha_2} q^j) \in T^j$ и $\{\alpha_1, \alpha_2\} = \{c!, c?\}$

Трансляция сети в автомат

Пример



Автомат $\otimes \mathcal{N}$ для сети \mathcal{N} из двух автоматов, изображённой выше:



Трансляция сети в автомат

Сеть \mathcal{N} и временной автомат \mathcal{A} будем называть **эквивалентными** ($\mathcal{N} \sim \mathcal{A}$), если

- ▶ они определены над одинаковыми множествами атомарных высказываний и часов и
- ▶ отношения $\rightarrow_{\mathcal{N}}$ и $\rightarrow_{\mathcal{A}}$ совпадают

Теорема. Для любой сети \mathcal{N} верно: $\mathcal{N} \sim \otimes \mathcal{N}$

Доказательство этой теоремы можно считать нетрудным упражнением