Математические методы верификации схем и программ

Лекторы:

Захаров Владимир Анатольевич

Подымов Владислав Васильевич

e-mail рассказчика:

valdus@yandex.ru

Осень 2018

Лекция 10

Алгоритм верификации временны́х автоматов относительно TCTL

Временны́е регионы

Системы регионов

Сети временны́х автоматов

Вступление

Задача model checking для CTL (MC-CTL)
Для заданной модели Крипке M и заданной CTL-формулы φ проверить справедливость соотношения $M \models \varphi$

Задача model checking для TCTL (MC-TCTL)
Для заданного корректного временнóго автомата A и заданной TCTL-формулы φ проверить справедливость соотношения

$$A \models \varphi$$

Выполнимость TCTL-формул для наглядности будет обозначаться знаком $\models_t$

AP — множество атомарных высказываний, над которыми описываются автоматы, модели Крипке и формулы

Схема алгоритма model checking для TCTL

Дано: временной автомат A, TCTL-формула φ
Требуется: проверить справедливость соотношения $A \models_t \varphi$

Схема проверки:

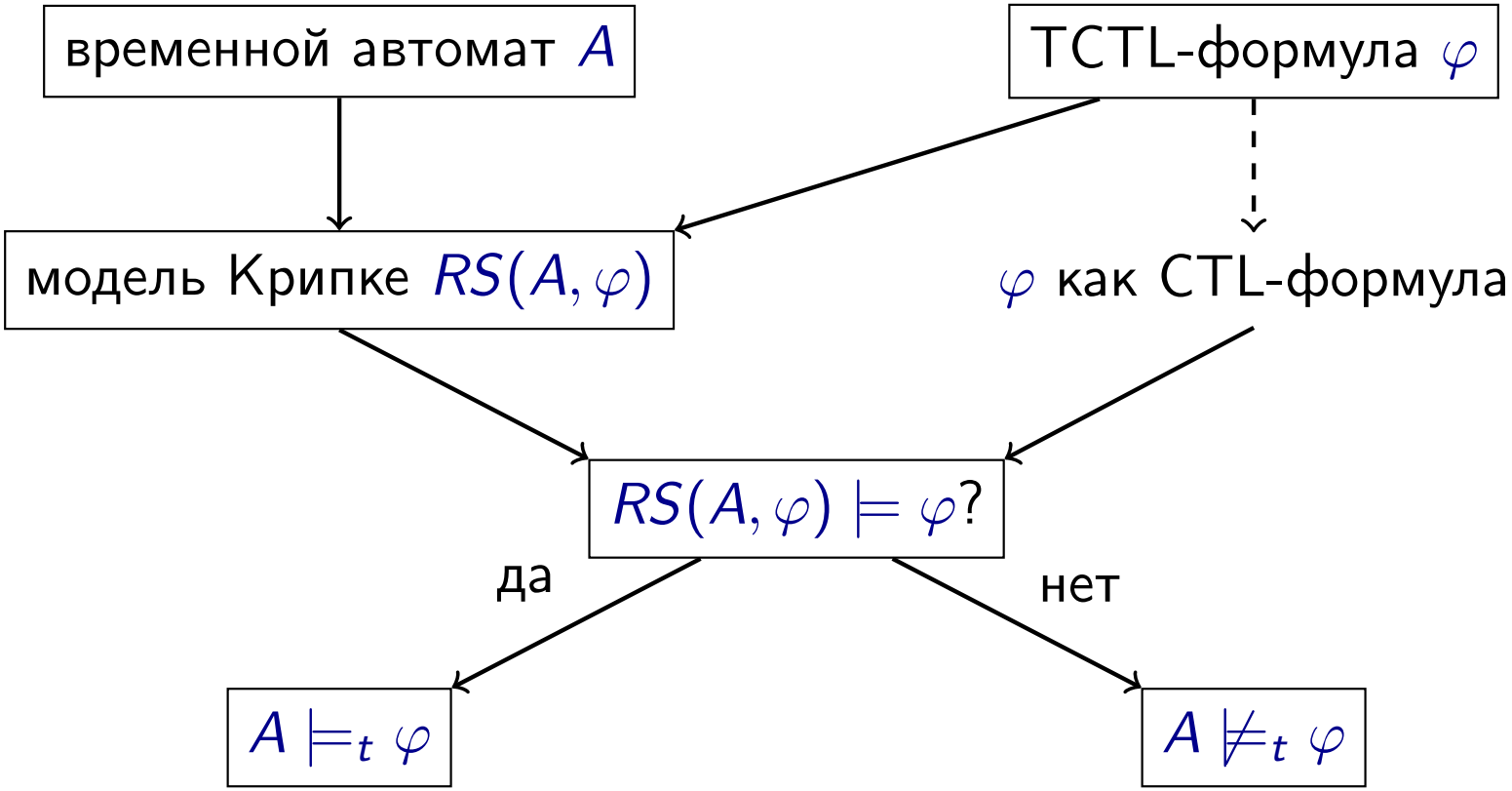


Схема алгоритма model checking для TCTL

ETC_A и ETC_φ — все элементарные временны́е ограничения, содержащиеся в автомате A и формуле φ соответственно

Модель Крипке $RS(A, \varphi)$ может быть устроена так:

- атомарные высказывания модели: $AP \cup ETC_\varphi$
- каждое состояние s модели имеет вид (ℓ, r), где ℓ — состояние автомата и r — множество оценок часов, и отвечает множеству конфигураций автомата $\Sigma_s = \{(\ell, \nu) \mid \nu \in r\}$
- начальное состояние модели отвечает множеству из одного элемента: начальной конфигурации автомата
- множества оценок r подбираются так, чтобы оценки одного множества были неотличимы выражениями e, $e \in ETC_A \cup ETC_\varphi$: если $\nu_1, \nu_2 \in r$, то $\nu_1 \models e \Leftrightarrow \nu_2 \models e$

Схема алгоритма model checking для TCTL

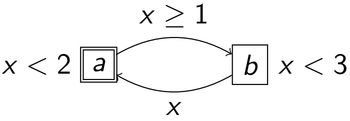
ETC_A и ETC_φ — все элементарные временны́е ограничения, содержащиеся в автомате A и формуле φ соответственно

Модель Крипке $RS(A, \varphi)$ может быть устроена так:

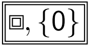
- состояние s модели размечается выражениями e множества $AP \cup ETC_\varphi$, выполненными в каждой конфигурации множества Σ_s
- переход $(\ell_1, r_1) \to (\ell_2, r_2)$ модели трактуется так:
  для любой оценки часов ν_1 из r_1
  существует оценка часов ν_2 из r_2,
  такая что $(\ell_1, \nu_1) \to (\ell_2, \nu_2)$
- состояния модели подбираются так, чтобы переходами модели "охватывались" в точности все шаги вычисления автомата

Схема алгоритма model checking для TCTL

Пример: попробуем построить такую модель $RS(A, \varphi)$ “методом пристального взгляда” для таких A и φ:



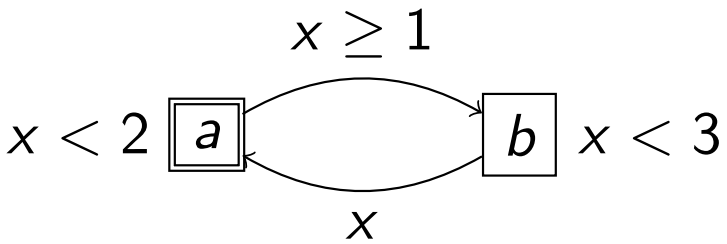
$\mathbf{AGAF}(x = 1)$



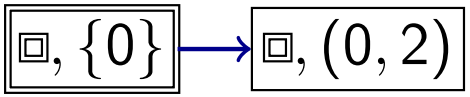
Начальное состояние модели = состояние ⧈ + оценка 0 часов x

Схема алгоритма model checking для TCTL

Пример: попробуем построить такую модель $RS(A, \varphi)$ "методом пристального взгляда" для таких A и φ:



$\mathbf{AGAF}(x = 1)$

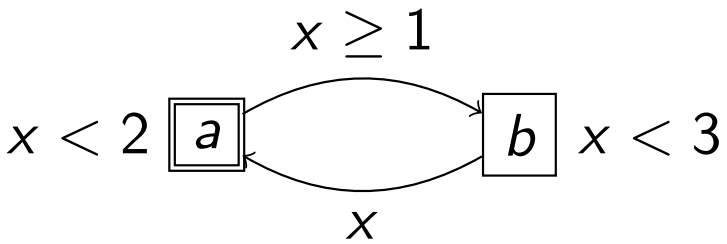


Первый шаг вычисления автомата обязательно выглядит так: $(\boxdot, 0) \overset{d}{\mapsto} (\boxdot, d)$, где $0 < d < 2$

Добавим в модель состояние, отвечающее всем таким конфигурациям $(\boxdot, d)$, и переход, "охватывающий" все первые шаги вычисления

Схема алгоритма model checking для TCTL

Пример: попробуем построить такую модель $RS(A, \varphi)$ "методом пристального взгляда" для таких A и φ:



$\mathbf{AGAF}(x = 1)$

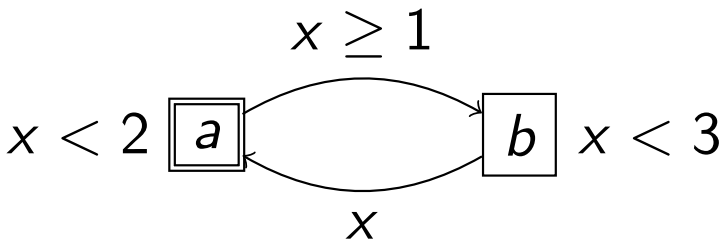
$\boxed{\boxed{\boxdot, \{0\}}}$ $\boxed{\boxdot, (0, 1)}$ $\boxed{\boxdot, [1, 2)}$

Условие $x \geq 1$ выполнено для значений часов x из интервала $[1, 2)$ и не выполнено для значений из интервала $(0, 1)$

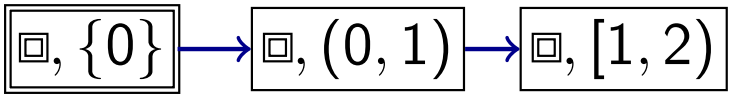
"Разобьём" состояние $(\boxdot, (0, 2))$ на два относительно условия $x \geq 1$

Схема алгоритма model checking для TCTL

Пример: попробуем построить такую модель $RS(A, \varphi)$ "методом пристального взгляда" для таких A и φ:



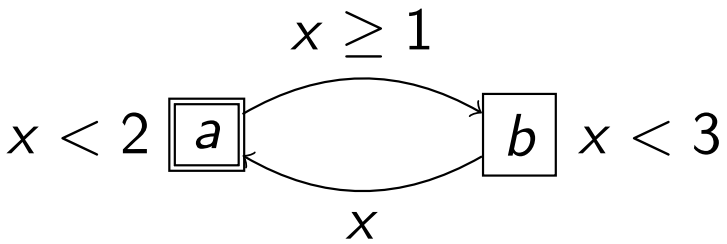
AGAF$(x = 1)$



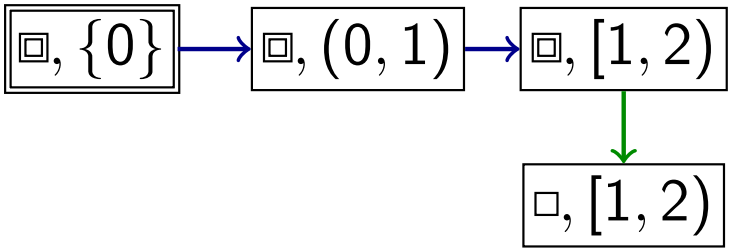
При **непрерывном** увеличении время принимает сначала значение 0, затем все значения интервала $(0, 1)$, и затем все значения интервала $[1, 2)$ — соединим состояния в эту последовательность

Схема алгоритма model checking для TCTL

Пример: попробуем построить такую модель $RS(A, \varphi)$ "методом пристального взгляда" для таких A и φ:



$\mathbf{AGAF}(x = 1)$

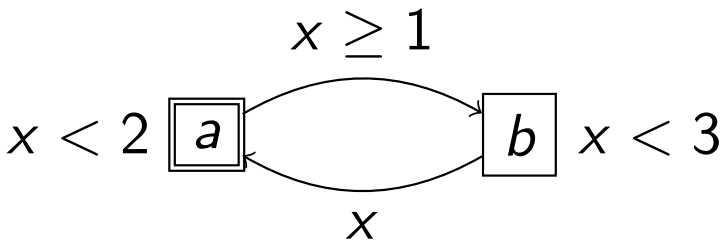


Для **любой** конфигурации $(\boxdot, d)$, где $1 \leq d < 2$, справедливо соотношение $(\boxdot, d) \xhookrightarrow{\boxdot \xrightarrow{x \geq 1} \square} (\square, d)$

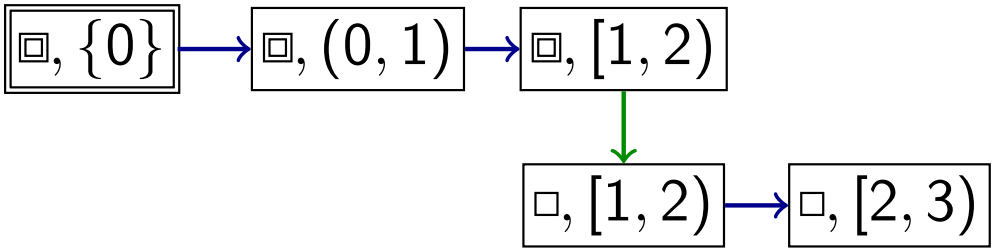
Добавим в модель состояние и переход, "охватывающие" все такие шаги вычисления автомата

Схема алгоритма model checking для TCTL

Пример: попробуем построить такую модель $RS(A, \varphi)$ "методом пристального взгляда" для таких A и φ:



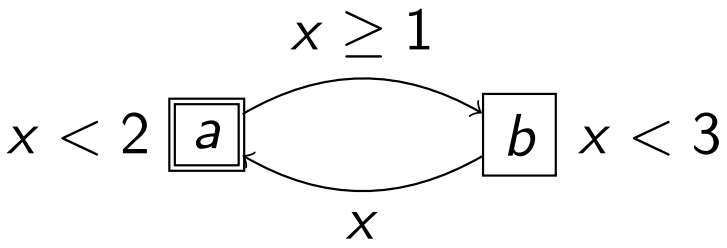
$\mathbf{AGAF}(x = 1)$



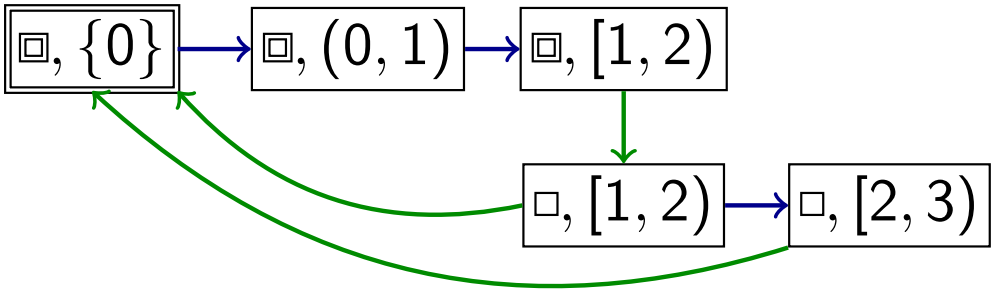
При **непрерывном** продвижении времени из конфигурации $(\square, d)$, где $1 \leq d < 2$, значение часов x либо принадлежит имеющемуся интервалу $[1, 2)$, либо выходит за пределы интервала и лежит в интервале $[2, 3)$ — добавим в модель соответствующие состояние и переход

Схема алгоритма model checking для TCTL

Пример: попробуем построить такую модель $RS(A, \varphi)$ "методом пристального взгляда" для таких A и φ:



AGAF$(x = 1)$

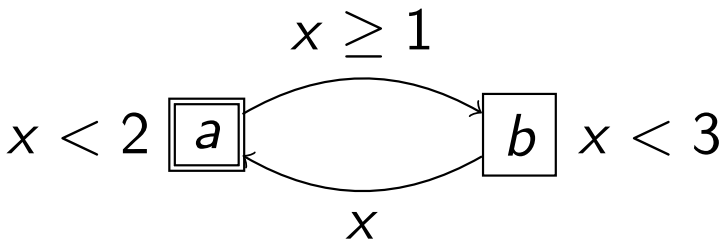


Для каждой конфигурации $(\square, d)$, где $1 \leq d < 3$, справедливо соотношение $(\square, d) \xhookrightarrow{\square \xrightarrow{x} \boxdot} (\boxdot, 0)$

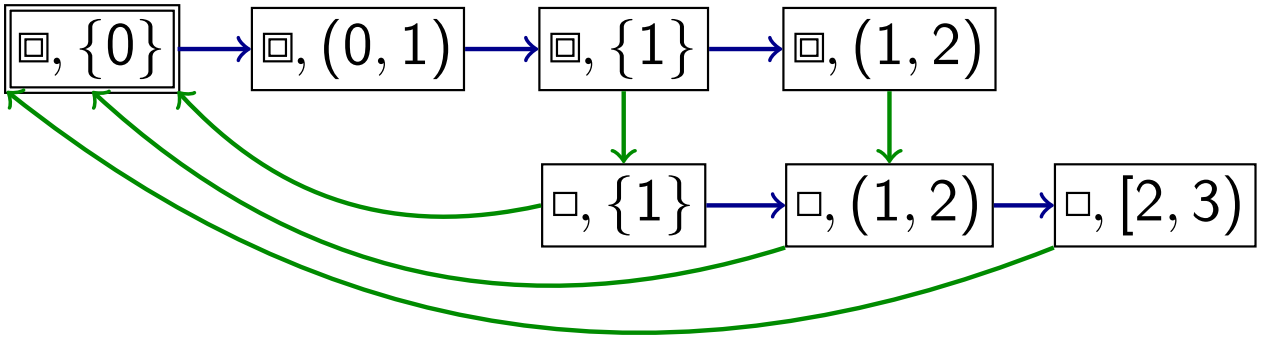
Добавим в модель соответствующие переходы

Схема алгоритма model checking для TCTL

Пример: попробуем построить такую модель $RS(A, \varphi)$ "методом пристального взгляда" для таких A и φ:



AGAF$(x = 1)$



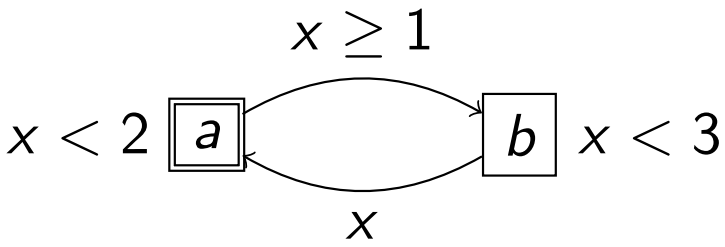
В формуле φ содержатся ограничения $x \leq 1$ и $x < 1$:

$$(x = 1) \equiv (x \leq 1 \,\&\, \neg(x < 1))$$

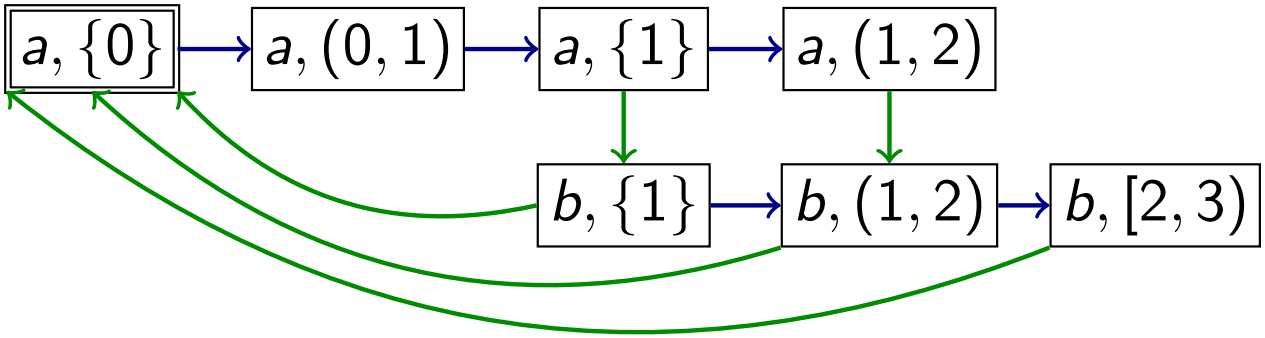
Чтобы однозначно разметить модель этими ограничениями, достаточно "разбить" интервал $[1, 2)$ в каждом имеющемся состоянии на два: $\{1\}$ и $(1, 2)$

Схема алгоритма model checking для TCTL

Пример: попробуем построить такую модель $RS(A, \varphi)$ "методом пристального взгляда" для таких A и φ:



AGAF$(x = 1)$

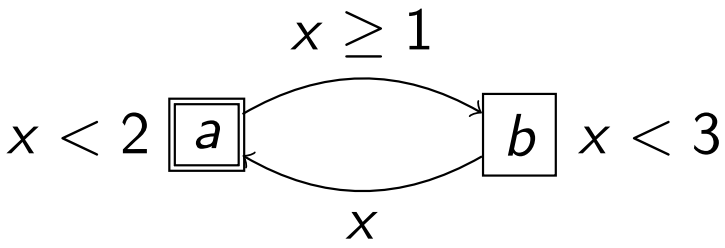


В результате получена модель Крипке, переходами которой описываются всевозможные дивергентные вычисления автомата A и неявно порождаемые ими конфигруации

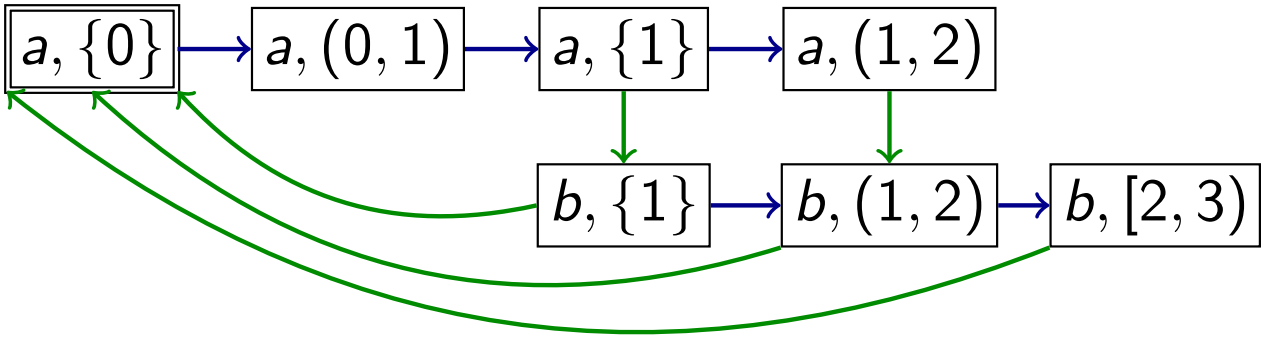
Можно легко убедиться, что $A \models_t \varphi$ и $M \models \varphi$

Схема алгоритма model checking для TCTL

Пример: попробуем построить такую модель $RS(A, \varphi)$ “методом пристального взгляда” для таких A и φ:



AGAF$(x = 1)$



Осталось показать, как построить аналогичную модель Крипке для **произвольных** временно́го автомата и TCTL-формулы, и доказать, что равновыполнимость формулы на автомате и модели не случайна

Временны́е регионы

Множества оценок часов, которые разрешено включать
в состояния модели $RS(A, \varphi)$,
называются временны́ми регионами

Временной регион можно определить как класс регионального отношения эквивалентности $\sim$ на множестве всех оценок часов

$\mathfrak{R}$ — множество всех временны́х регионов

Для технической простоты
во всех дальнейших рассуждениях об отношении $\sim$,
о множестве $\mathfrak{R}$ и о модели $RS(A, \varphi)$ полагается,
что автомат A и формула φ
не содержат ограничений вида $x - y < k$ **и** $x - y \leq k$

Временны́е регионы

Чтобы корректно определить состояния и переходы модели $RS(A, \varphi)$, следует выбрать отношение $\sim$ с (*как минимум*) такими свойствами:

- Конечность: $\mathfrak{R}$ — **конечное** множество
  - (*число состояний модели конечно*)
- Неотличимость эквивалентных оценок: если $\nu_1 \sim \nu_2$ и $e \in ETC_A \cup ETC_\varphi$, то $\nu_1 \models e \Leftrightarrow \nu_2 \models e$
  - (*метки состояний модели однозначны, а переходы безусловны*)
- Корректность сброса: если r — регион и X — множество часов, то $r[X] = \{\nu[X] \mid \nu \in r\}$ — также регион
  - (*при выполнении переходов автомата могут произвольно сбрасываться часы*)
- Однозначность продвижения времени: для каждого региона r однозначно определён регион r^+, следующий за r *при непрерывном продвижении времени*
  - (*в модели требуется явно и однозначно учесть все конфигурации, порождаемые при продвижении времени автоматом*)

Временны́е регионы

Первая попытка определить $\sim$ (неуспешная)

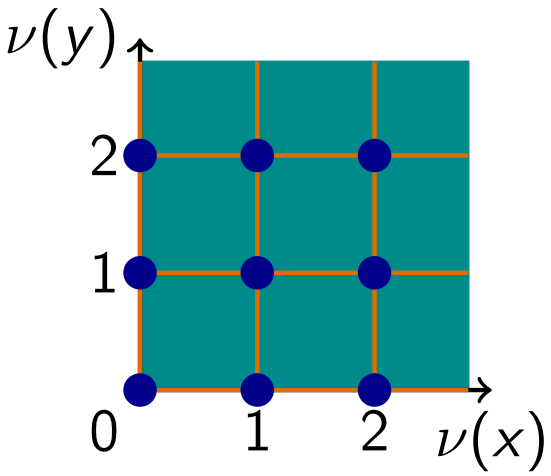
$\lfloor t \rfloor$ — целая часть числа t

$frac(t)$ — дробная часть числа t

$\nu_1 \sim_1 \nu_2 \quad \Leftrightarrow \quad$ для любых часов x верны два условия:

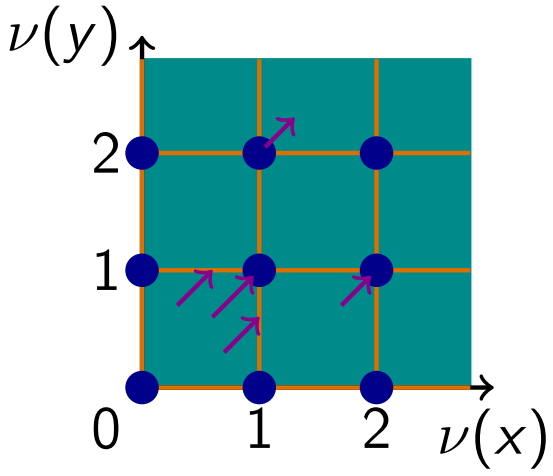
1. $\lfloor \nu_1(x) \rfloor = \lfloor \nu_2(x) \rfloor$
2. $frac(\nu_1(x)) = 0 \Leftrightarrow frac(\nu_2(x)) = 0$

Пример: $\sim_1$-регионы для часов x, y изображены связными областями одного цвета на картинке



Временны́е регионы

Первая попытка определить $\sim$ (неуспешная)



Хорошие свойства $\sim_1$*:*

- неотличимость эквивалентных оценок
- корректность сброса

Оставшиеся проблемы:

- $|\mathfrak{R}| = \infty$
- существует (*и далеко не единственен*) регион r, для которого неоднозначно определён регион r^+
  - примеры переходов от r к r^+ изображены стрелками

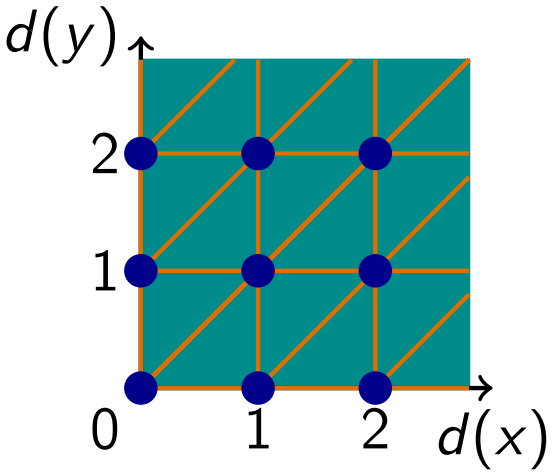
Временны́е регионы

Вторая попытка определить $\sim$ (неуспешная)

$\nu_1 \sim_2 \nu_2 \quad \Leftrightarrow \quad$ для любой пары часов x, y верны три условия:

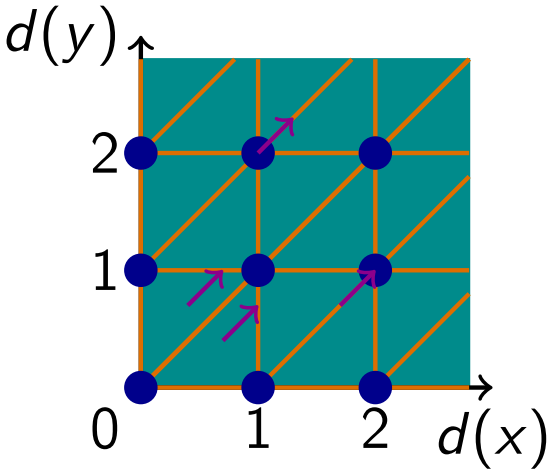
1. $\lfloor \nu_1(x) \rfloor = \lfloor \nu_2(x) \rfloor$
2. $frac(\nu_1(x)) = 0 \Leftrightarrow frac(\nu_2(x)) = 0$
3. $frac(\nu_1(x)) \leq frac(\nu_1(y)) \Leftrightarrow frac(\nu_2(x)) \leq frac(\nu_2(y))$

Пример: $\sim_2$-регионы для часов x, y изображены связными областями одного цвета на картинке



Временны́е регионы

Вторая попытка определить $\sim$ (неуспешная)



Хорошие свойства $\sim_2$*:*

- неотличимость эквивалентных оценок
- корректность сброса
- однозначность продвижения времени

Оставшиеся проблемы:

- $|\mathfrak{R}| = \infty$

Временны́е регионы

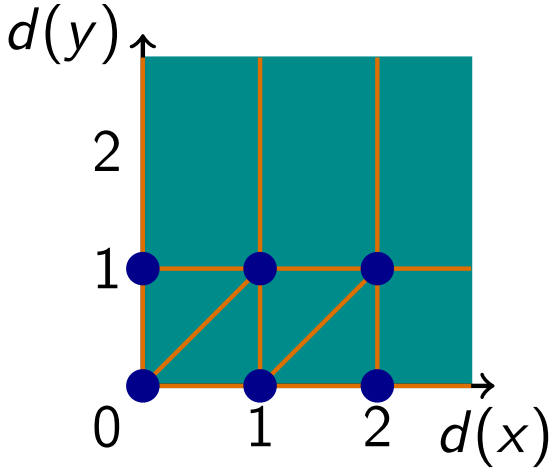
Третья попытка определить $\sim$ (успешная)

k_x — это наибольшая константа k, встречающаяся в выражениях вида $x < k$ и $x \leq k$ множества $ETC_A \cup ETC_\varphi$

$\nu_1 \sim \nu_2 \quad \Leftrightarrow \quad$ для любой пары часов x, y верно следующее:

1. $\nu_1(x) > k_x \Leftrightarrow \nu_2(x) > k_x$
2. если $\nu_1(x) \leq k_x$ и $\nu_1(y) \leq k_y$, то
   - $\lfloor \nu_1(x) \rfloor = \lfloor \nu_2(x) \rfloor$
   - $frac(\nu_1(x)) = 0 \Leftrightarrow frac(\nu_2(x)) = 0$
   - $frac(\nu_1(x)) \leq frac(\nu_1(y)) \Leftrightarrow frac(\nu_2(x)) \leq frac(\nu_2(y))$

Пример: регионы для часов x, y и констант $k_x = 2$, $k_y = 1$ изображены связными областями одного цвета на картинке



Оценка числа временны́х регионов

Утверждение

Пусть $\mathfrak{R}$ — множество всех регионов отношения $\sim$, построенного для конечного множества часов $\mathcal{C}$ и заданных констант k_x, $x \in \mathcal{C}$. Тогда

$$|\mathcal{C}|! \cdot \prod_{x \in \mathcal{C}} k_x \leq |\mathfrak{R}| \leq |\mathcal{C}|! \cdot 2^{|\mathcal{C}|-1} \cdot \prod_{x \in \mathcal{C}} (2k_x + 2)$$

Доказательство.

Откуда в оценках взялось

- $\prod_{x \in C} k_x$: отношение эквивалентности содержит столько единичных кубов размерности $|C|$, покрывающих диапазоны $[0, k_x]$ для всех часов x
- $|C|!$: столькими способами можно определить порядок ($\leq$) дробных частей часов региона

Оценка числа временны́х регионов

Утверждение

Пусть $\mathfrak{R}$ — множество всех регионов отношения $\sim$, построенного для конечного множества часов $\mathcal{C}$ и заданных констант k_x, $x \in \mathcal{C}$. Тогда

$$|\mathcal{C}|! \cdot \prod_{x \in \mathcal{C}} k_x \le |\mathfrak{R}| \le |\mathcal{C}|! \cdot 2^{|\mathcal{C}|-1} \cdot \prod_{x \in \mathcal{C}} (2k_x + 2)$$

Доказательство.

Откуда в оценках взялось

- $2k_x + 2$: столькими способами можно выбрать диапазон допустимых значений часов x в регионе
- $2^{|C|-1}$: столькими способами для каждого порядка дробных частей можно выбрать, какие из неравенств $\le$ строгие ▼

Следствие

Множество $\mathfrak{R}$ конечно

Свойства временны́х регионов

Утверждение

Если $\nu_1 \sim \nu_2$, x **— часы и** $k \in \{0, 1, \ldots, k_x\}$, **то**

$$\nu_1 \models x < k \quad \Leftrightarrow \quad \nu_2 \models x < k \quad \text{и}$$
$$\nu_1 \models x \leq k \quad \Leftrightarrow \quad \nu_2 \models x \leq k$$

Временно́е граничение g, построенное над элементарными ограничениями множества $ETC_A \cup ETC_\varphi$, выполнено в регионе r ($r \models g$), если для любой оценки ν региона r верно соотношение $\nu \models g$

Утверждение

Для любого региона r **и любого множества часов** X **множество оценок** $r[X]$ **является регионом**

Свойства временны́х регионов

Регион открыт для часов x,
если он содержит оценку ν, такую что $\nu(x) > k_x$

Регион, открытый для всех часов, называется открытым,
а все остальные — закрытыми

Продвижение региона r — это регион r^+, определяющийся так:

- если r — открытый регион, то r^+ — открытый регион
- если r — закрытый регион, то r^+ — регион, удовлетворяющий следующим свойствам:
  - $r^+ \neq r$
  - если $\nu \in r$ и $(\nu + d) \in r^+$, где $d > 0$, то для любого числа d', такого что $0 \leq d' \leq d$, верно соотношение $(\nu + d') \in r \cup r^+$

Утверждение

Для любого региона r
существует единственное продвижение r^+

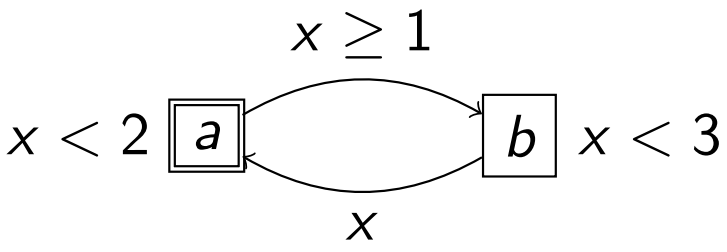
Системы регионов

Система регионов $RS(A, \varphi)$ для автомата $A = (L, \ell_0, \mathcal{C}, \xi, I, T)$ и TCTL-формулы φ — это модель Крипке, являющаяся наибольшим тотальным подграфом следующего графа G:

- $L \times \mathfrak{R}$ — множество вершин графа G
- вершина $(\ell_0, \{(0, \ldots, 0)\})$ является начальной
- каждая вершина (ℓ, r) помечена множеством
$$\xi(\ell) \cup \{e | e \in ETC_\varphi,\ r \models e\}$$
- $(\ell, r) \to (\ell', r')$ в том и только том случае, если верно хотя бы одно из двух:
  - $r' = r^+$, $\ell' = \ell$ и $r^+ \models I(\ell)$
  - в множестве T переходов автомата содержится переход $\ell \xrightarrow{g,X} \ell'$, такой что $r \models g$, $r' = r[X]$ и $r' \models I(\ell')$

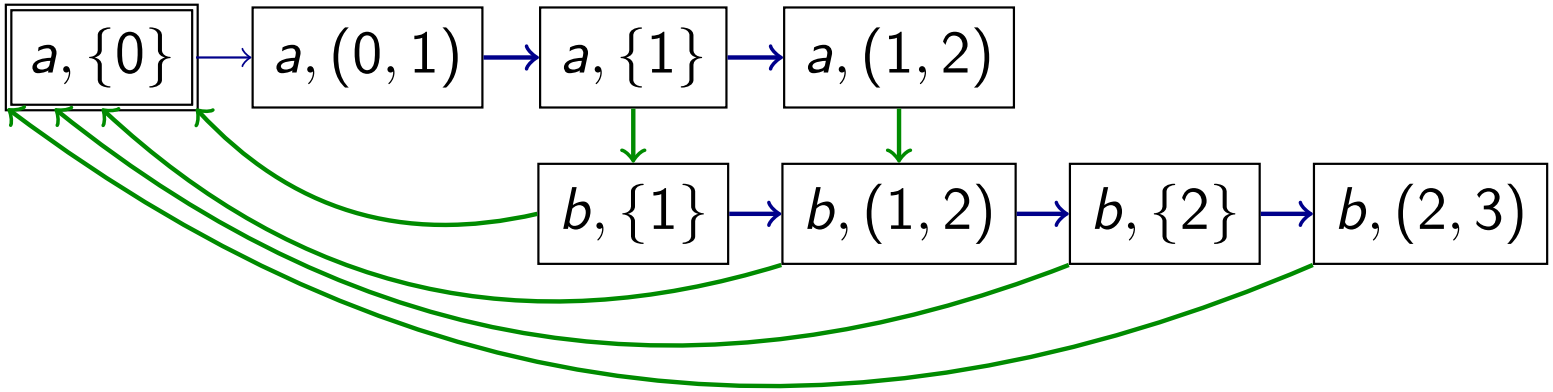
Системы регионов

Пример:



$\mathbf{AGAF}(x = 1)$

Система регионов для этих автомата и формулы выглядит так:



Системы регионов

Теорема

Для любого корректного временнóго автомата A и любой TCTL-формулы φ справедлива равносильность

$$A \models_t \varphi \quad \Leftrightarrow \quad RS(A, \varphi) \models \varphi$$

Доказательство.

Если ν — оценка часов и ℓ — состояние автомата A, то:

- $[\nu]$ — регион, содержащий оценку ν
- $[(\ell, \nu)] = (\ell, [\nu])$

Достаточно доказать индукцией по построению формулы, что для любой конфигурации σ, порождаемой любым дивергентным вычислением автомата A, и для любой подформулы ψ формулы φ справедлива равносильность

$$A, \sigma \models_t \psi \quad \Leftrightarrow \quad RS(A, \varphi), [\sigma] \models \psi$$

Для определённости считаем, что $A = (L, \ell_0, \mathcal{C}, \xi, I, T)$ и $RS(A, \varphi) = (S, s_0, \Rightarrow, \mathcal{L})$

Системы регионов

Доказательство. $(A, \sigma \models_t \psi \quad \Leftrightarrow \quad RS(A, \varphi), [\sigma] \models \psi)$

База индукции (1): $\psi = a$, где $a \in AP$

$A, (\ell, \nu) \models_t a \Leftrightarrow a \in \xi(\ell) \Leftrightarrow a \in \mathcal{L}(\ell, [\nu]) \Leftrightarrow RS(A, \varphi), (\ell, [\nu]) \models a$

База индукции (2): $\psi = e$, где $e \in ETC_\varphi$

$A, (\ell, \nu) \models_t e \Leftrightarrow \nu \models_t e \Leftrightarrow [\nu] \models_t e$

$\Leftrightarrow e \in \mathcal{L}(\ell, [\nu]) \Leftrightarrow RS(A, \varphi), (\ell, [\nu]) \models e$

Индуктивный переход (1): $\psi = \neg\chi$

$A, \sigma \models_t \neg\chi \Leftrightarrow A, \sigma \not\models_t \chi$

$\Leftrightarrow RS(A, \varphi), [\sigma] \not\models \chi \Leftrightarrow RS(A, \varphi), [\sigma] \models \neg\chi$

Индуктивный переход (2): $\psi = \chi_1 \,\&\, \chi_2$

$A, \sigma \models_t \chi_1 \,\&\, \chi_2 \Leftrightarrow A, \sigma \models_t \chi_1$ и $A, \sigma \models_t \chi_2$

$\Leftrightarrow RS(A, \varphi), [\sigma] \models \chi_1$ и $RS(A, \varphi), [\sigma] \models \chi_2$

$\Leftrightarrow RS(A, \varphi), [\sigma] \models \chi_1 \,\&\, \chi_2$

Системы регионов

Доказательство. $(A, \sigma \models_t \psi \quad \Leftrightarrow \quad RS(A, \varphi), [\sigma] \models \psi)$

Индуктивный переход (3): $\psi = \mathbf{E}(\chi_1 \mathbf{U} \chi_2)$

($\Leftarrow$):

Пусть $RS(A, \varphi), [\sigma] \models \mathbf{E}(\chi_1 \mathbf{U} \chi_2)$

Тогда существуют путь $(\gamma_1 \Rightarrow \gamma_2 \Rightarrow \dots)$ из состояния $[\sigma]$ в модели $RS(A, \varphi)$ и индекс k, такие что:

- $RS(A, \varphi), \gamma_k \models \chi_2$
- для любого состояния γ_i, $i < k$, верно $RS(A, \varphi), \gamma_i \models \chi_1$

По определению $RS(A, \varphi)$, существует дивергентная σ—трасса $(\sigma_1 \to \sigma_2 \to \dots)$ автомата A, такая что $[\sigma_i] = \gamma_i$, $i \geq 2$

По индуктивному предположению и определению $RS(A, \varphi)$:

- $A, \sigma_k \models_t \chi_2$
- для любой конфигурации δ, порождаемой трассой $\sigma_1 \to \dots \to \sigma_k$, верно $[\delta] \in \{\gamma_1, \dots, \gamma_k\}$, а значит, $A, \delta \models_t \chi_1$ или $A, \delta \models_t \chi_2$

Системы регионов

Доказательство. $(A, \sigma \models_t \psi \quad \Leftrightarrow \quad RS(A, \varphi), [\sigma] \models \psi)$

Индуктивный переход (3): $\psi = \mathbf{E}(\chi_1 \mathbf{U} \chi_2)$

($\Rightarrow$):

Пусть $A, \sigma \models_t \mathbf{E}(\chi_1 \mathbf{U} \chi_2)$

Тогда существуют дивергентная σ-трасса

$$(\ell_1, \nu_1) \to (\ell_2, \nu_2) \to \dots$$

автомата A и индекс k, такие что:

- $A, (\ell_k, \nu_k) \models_t \chi_2$
- для любой конфигурации δ, порождаемой трассой

  $$(\ell_1, \nu_1) \to \dots \to (\ell_k, \nu_k),$$

  верно $A, \delta \models_t \chi_1$ или $A, \delta \models_t \chi_2$

Системы регионов

Доказательство. $(A, \sigma \models_t \psi \quad \Leftrightarrow \quad RS(A, \varphi), [\sigma] \models \psi)$

Индуктивный переход (3): $\psi = \mathbf{E}(\chi_1 \mathbf{U} \chi_2)$

($\Rightarrow$):

Рассмотрим путь

$$\gamma_1 \Rightarrow \gamma_2 \Rightarrow \dots$$

в модели $RS(A, \varphi)$ следующего вида:

- $\gamma_1 = [(\ell_1, \nu_1)] = (\ell_1, [\nu_1])$
- шагу $(\ell_i, \nu_i) \mapsto (\ell_{i+1}, \nu_{i+1})$, где $[\nu_i]$ — **закрытый** регион, соответствует подпуть
  $$(\ell_i, [\nu_i]) \Rightarrow (\ell_i, [\nu_i]^+) \Rightarrow (\ell_i, [\nu_i]^{++}) \Rightarrow \dots \Rightarrow (\ell_i, [\nu_{i+1}])$$
- шагам $(\ell_i, \nu_i) \mapsto (\ell_{i+1}, \nu_{i+1})$, где $[\nu_i]$ — **открытый** регион, и $(\ell_i, \nu_i) \hookrightarrow (\ell_{i+1}, \nu_{i+1})$
  соответствует подпуть $(\ell_i, [\nu_i]) \Rightarrow (\ell_{i+1}, [\nu_{i+1}])$

Системы регионов

Доказательство. $(A, \sigma \models_t \psi \quad \Leftrightarrow \quad RS(A, \varphi), [\sigma] \models \psi)$

Индуктивный переход (3): $\psi = \mathbf{E}(\chi_1 \mathbf{U} \chi_2)$

($\Rightarrow$):

По определению $RS(A, \varphi)$ и индуктивному предположению, существует индекс m, такой что:

- $RS(A, \varphi), \gamma_m \models \chi_2$
- для каждого состояния γ_i, $i < m$, существует конфигурация δ, порождаемая трассой $(\ell_1, \nu_1) \to \cdots \to (\ell_k, \nu_k)$ и такая что $[\delta] = \gamma_i$, а значит, $RS(A, \varphi), \gamma_i \models \chi_1$ или $RS(A, \varphi), \gamma_i \models \chi_2$

Следовательно, $RS(A, \varphi), \gamma_1 \models \mathbf{E}(\chi_1 \mathbf{U} \chi_2)$

Индуктивный переход (4): $\psi = \mathbf{A}(\chi_1 \mathbf{U} \chi_2)$

Рассуждения в этом случае аналогичны рассуждениям *индуктивного перехода (3)* ▼

Системы регионов

Теорема

Для любого корректного временно́го автомата A и любой TCTL-формулы φ справедлива равносильность

$$A \models_t \varphi \quad \Leftrightarrow \quad RS(A, \varphi) \models \varphi$$

Упражнение.

Определить региональное отношение
и доказать аналогичную теорему для **общего случая**:
автомат A и формула φ могут содержать
ограничения вида $x - y < k$ и $x - y \leq k$

Сети временны́х автоматов

Система реального времени (СРВ), как правило, состоит из нескольких взаимодействующих компонентов, работающих **параллельно**

Временной автомат — это **последовательная** модель системы

Попытки вручную описать последовательное выполнение параллельной (*распределённой*) системы в большинстве случаев приводят к нетривиальным ошибкам, из-за которых верификация системы теряет смысл

Модель, более естественная для формализации СРВ, представляет собой **совокупность** взаимодействующих временны́х автоматов

Сети временны́х автоматов

Синхронизируемый временной автомат
определяется над конечными множествами
атомарных высказываний AP и каналов синхронизации CH

Единственное синтаксическое отличие такого автомата
от *обычного* временного автомата:
каждый переход дополнительно помечен синхронизацией:
выражением $c!$ или $c?$, где $c \in CH$
(посылка в канал приём из канала соответственно),
либо специальным символом λ (отсутствие синхронизации)

$$Sync(CH) = \{c! \mid c \in CH\} \cup \{c? \mid c \in CH\} \cup \{\lambda\}$$

Множество всевозможных переходов синхронизируемого
автомата $A = (L, \ell_0, \mathcal{C}, \xi, I, T)$ над AP и CH имеет вид

$$L \times Guard(\mathcal{C}) \times Sync(CH) \times 2^{\mathcal{C}} \times L$$

$\ell \xrightarrow{g,s,X} \ell'$ — наглядная запись перехода (ℓ, g, s, X, ℓ')

Сети временны́х автоматов

Сеть временны́х автоматов над атомарными высказываниями AP — это система $(\mathcal{C}, CH, (A_1, \ldots, A_k))$, где

- $\mathcal{C}$ и CH — конечные множества **часов** и **каналов** соответственно
- $A_i = (L^i, \ell_0^i, \mathcal{C}, \xi^i, I^i, T^i)$, $1 \leq i \leq k$, — синхронизируемый временной автомат над высказываниями AP_i и каналами CH
- $L^i \cap L^j = \emptyset$, если $1 \leq i < j \leq k$
- $AP_i \cap AP_j = \emptyset$, если $1 \leq i < j \leq k$
- $AP_1 \cup \cdots \cup AP_k = AP$

Сети временны́х автоматов

Конфигурация сети $(\mathcal{C}, CH, (A_1, \ldots, A_k))$, где $A_i = (L^i, \ell_0^i, \mathcal{C}, \xi^i, I^i, T^i)$ — это пара $(\vec{\ell}, \nu)$, где

- $\vec{\ell} \in L^1 \times L^2 \times \cdots \times L^k$
- ν — оценка часов C

Начальная конфигурация сети имеет вид $(\ell_0^1, \ldots, \ell_0^k, 0, \ldots, 0)$

Все обозначения для преобразования конфигураций автомата ($\sigma + d$, $\sigma[X]$, $\sigma[\ell/\ell']$) напрямую переносятся на случай конфигураций сети

Конфигурации (*дискретно*) преобразуются сетью в процессе вычисления тремя способами:

- Продвижение времени ($\sigma \mapsto \sigma'$)
- Выполнение перехода ($\sigma \hookrightarrow \sigma'$)
- Рандеву-синхронизация ($\sigma \Rightarrow \sigma'$)

Отношение шага вычисления $\rightarrow$ сети — это объединение отношений $\mapsto$, $\hookrightarrow$ и $\Rightarrow$

Сети временны́х автоматов

Рассмотрим сеть $(\mathcal{C}, CH, (A_1, \ldots, A_k))$, где $A_i = (L^i, \ell_0^i, \mathcal{C}, \xi^i, I^i, T^i)$, и конфигурацию $\sigma = (\ell_1, \ldots, \ell_k, \nu)$ сети

Продвижение времени

$\sigma \overset{d}{\mapsto} \sigma'$, где $d \in \mathbb{R}_{>0}$,
если $\sigma' = \sigma + d$ и $\nu + d \models I^1(\ell_1) \,\&\, \ldots \,\&\, I^k(\ell_k)$

$\sigma \mapsto \sigma'$, если существует число d, $d \in \mathbb{R}_{>0}$, такое что $\sigma \overset{d}{\mapsto} \sigma'$

Выполнение перехода

$\sigma \xhookrightarrow{\ell_i \xrightarrow{g,\lambda,X} \ell_i'} \sigma'$, где $\ell_i \xrightarrow{g,\lambda,X} \ell_i' \in T^i$, если:

- $\sigma' = \sigma[X][\ell_i/\ell_i']$
- $\nu \models g$
- $\nu[X] \models I^i(\ell_i')$

$\sigma \hookrightarrow \sigma'$, если существуют автомат A_i сети N и переход t этого автомата, такие что $\sigma \overset{t}{\hookrightarrow} \sigma'$

Сети временны́х автоматов

Рассмотрим сеть $N = (\mathcal{C}, CH, (A_1, \ldots, A_k))$, где $A_i = (L^i, \ell_0^i, \mathcal{C}, \xi^i, I^i, T^i)$, и конфигурацию $\sigma = (\ell_1, \ldots, \ell_k, \nu)$ сети

Рандеву

$\sigma \xRightarrow{t_1, t_2} \sigma'$, где $t_1 = (\ell_i \xrightarrow{g_1, c!, X_1} \ell_i') \in T^i$, $t_2 = (\ell_j \xrightarrow{g_2, c?, X_2} \ell_j') \in T^j$ и $i \neq j$, если:

- $\sigma' = \sigma[X_1][X_2][\ell_i/\ell_i'][\ell_j/\ell_j']$
- $\nu \models g_1 \,\&\, g_2$
- $\nu[X_1][X_2] \models I^i(\ell_i') \,\&\, I^j(\ell_j')$

$\sigma \Rightarrow \sigma'$, если существуют автоматы A_i, A_j, $i \neq j$, и переходы t_1, t_2 этих автоматов, такие что $\sigma \xRightarrow{t_1, t_2} \sigma'$

Трансляция сетей во временны́е автоматы

Сеть N эквивалентна временно́му автомату A, если отношения шага вычисления для N и A совпадают

Теорема

Для любой сети временны́х автоматов N существует эквивалентный временной автомат A

Доказательство.

Пусть $N = (\mathcal{C}, CH, (A_1, \ldots, A_k))$, где $A_i = (L^i, \ell_0^i, \mathcal{C}, \xi^i, I^i, T^i)$

Требуемый автомат $A = (L, \ell_0, \mathcal{C}, \xi, I, T)$ можно определить следующим образом:

- $L = L^1 \times \cdots \times L^k$
- $\ell_0 = (\ell_0^1, \ldots, \ell_0^k)$
- $\xi(\ell_1, \ldots, \ell_k) = \xi^1(\ell_1) \cup \cdots \cup \xi^k(\ell_k)$
- $I(\ell_1, \ldots, \ell_k) = I^1(\ell_1) \,\&\, \ldots \,\&\, I^k(\ell_k)$

Трансляция сетей во временны́е автоматы

Сеть N эквивалентна временно́му автомату A, если отношения шага вычисления для N и A совпадают

Теорема

Для любой сети временны́х автоматов N существует эквивалентный временной автомат A

Доказательство.

Пусть $N = (\mathcal{C}, CH, (A_1, \ldots, A_k))$, где $A_i = (L^i, \ell_0^i, \mathcal{C}, \xi^i, I^i, T^i)$

Требуемый автомат $A = (L, \ell_0, \mathcal{C}, \xi, I, T)$ можно определить следующим образом:

- Отношение T содержит в точности следующие переходы:
  - $(\ell_1, \ldots, \ell_m) \xrightarrow{g, X} (\ell_1, \ldots, \ell_{i-1}, \ell_i', \ell_{i+1}, \ldots, \ell_m)$, если $\ell_i \xrightarrow{g, \lambda, X} \ell_i'$
  - $(\ell_1, \ldots, \ell_m) \xrightarrow{g_1 \,\&\, g_2, X_1 \cup X_2} (\ell_1, \ldots, \ell_{i-1}, \ell_i', \ell_{i+1}, \ldots, \ell_{j-1}, \ell_j', \ell_{j+1}, \ldots, \ell_m)$, если
    - $\ell_i \xrightarrow{g_1, c!, X_1} \ell_i'$ и $\ell_j \xrightarrow{g_2, c?, X_2} \ell_j'$ или
    - $\ell_i \xrightarrow{g_1, c?, X_1} \ell_i'$ и $\ell_j \xrightarrow{g_2, c!, X_2} \ell_j'$ ▼