Математические методы верификации схем и программ

Лекторы:

Захаров Владимир Анатольевич

Подымов Владислав Васильевич

e-mail рассказчика:

valdus@yandex.ru

Осень 2017

Лекция 10

Сведение верификации TCTL к верификации CTL

Временные регионы

Системы регионов

Сети временных автоматов

Вступление

Задача верификации временных автоматов относительно TCTL (MC-TCTL): для временного автомата A и TCTL-формулы φ проверить соотношение

$$A \models_T \varphi$$

Задача верификации моделей Крипке относительно CTL (MC-CTL): для заданных модели Крипке M и CTL-формулы φ проверить соотношение

$$M \models \varphi$$

Вступление

Задачу MC-TCTL невозможно *напрямую* переформулировать как задачу MC-CTL:

- модель Крипке **конечна**, а модель временного автомата **континуально-бесконечна**
- разнообразие меток состояний модели Крипке **конечно**, а моделей временных автоматов — **счётно-бесконечно**
- для проверки выполнимости CTL-формулы $\varphi \mathbf{U} \psi$ на трассе достаточно проанализировать только элементы этой трассы, а для проверки TCTL-формулы — континуально много неявно подразумеваемых *промежуточных* элементов

Сведение MC-TCTL к MC-CTL

Рассмотрим временной автомат A и TCTL-формулу φ над атомарными высказываниями AP

AC_A и AC_φ — записи, обозначающие **конечные** множества элементарных ограничений, используемых в описаниях A и φ соответственно

Опишем алгоритм построения системы регионов: модели Крипке $RS(A, \varphi)$ над **конечным** множеством высказываний $AP \cup AC_\varphi$, такой что

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

Если получится описать алгоритм построения системы регионов, то немедленно будет получен такой алгоритм решения задачи MC-TCTL:

1. построить $RS(A, \varphi)$
2. при помощи любого известного алгоритма проверить соотношение $RS(A, \varphi) \models \varphi$

Сведение MC-TCTL к MC-CTL

Состояние системы $RS(A, \varphi)$ — это пара (ℓ, r), где ℓ — состояние автомата A, и r — множество оценок часов

Переход $(\ell, r) \to (\ell', r')$ в $RS(A, \varphi)$, будет трактоваться так: **для любой оценки ν из r существует оценка ν' из r', такая что $(\ell, \nu) \mapsto (\ell', \nu')$ или $(\ell, \nu) \hookrightarrow (\ell', \nu')$**

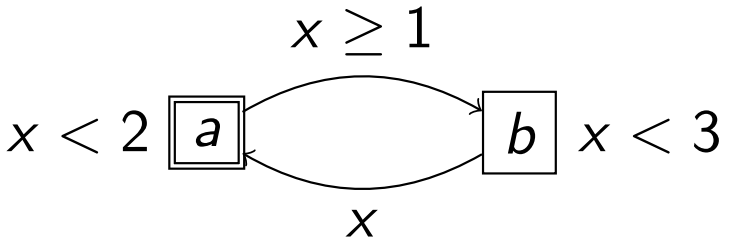
В состояниях системы $RS(A, \varphi)$ будут использоваться специальные множества оценок — временнЫе регионы: классы эквивалентности регионального отношения эквивалентности $\sim$

Отношение $\sim$ будет подобрано так, чтобы в числе прочего были выполнены следующие свойства:

- множество $\mathfrak{R}$ всевозможных регионов конечно
- для **каждого** ограничения e, $e \in AC_A \cup AC_\varphi$, и **каждой** пары оценок часов ν_1, ν_2 из одного региона верно $\nu_1 \models e \Leftrightarrow \nu_2 \models e$
  - $r \models g$ — отношение выполнимости временного ограничения g **хотя бы на одной** оценке ν региона r (а значит, и **на всех** оценках региона)

Сведение MC-TCTL к MC-CTL на примере

Рассмотрим такие временной автомат A и формулу φ:

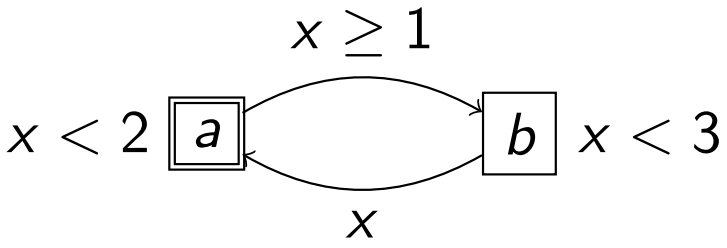


$$\mathbf{AGAF}(x = 1)$$

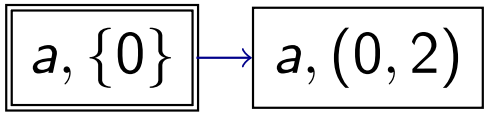
Попробуем построить систему регионов
“методом пристального взгляда”

Для наглядности синим цветом будут раскрашены переходы,
отвечающие продвижению времени ($\mapsto$),
а зелёным — отвечающие изменению состояния ($\hookrightarrow$)

Сведение MC-TCTL к MC-CTL на примере



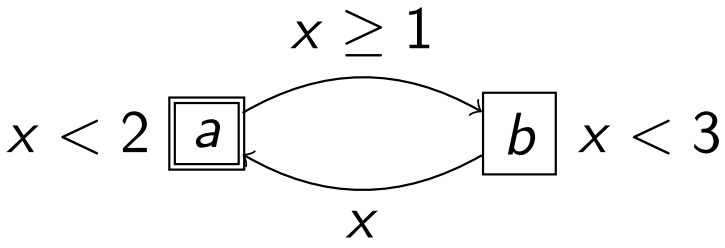
$\mathbf{AGAF}(x = 1)$



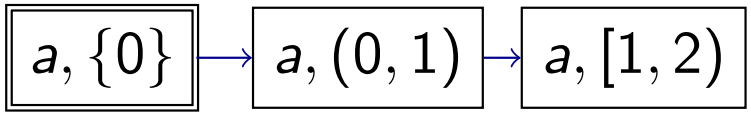
Модель содержит одно начальное состояние: $(\boxed{\square}, 0)$

Продвижением времени в левом состоянии автомата можно получить любое значение часов x в диапазоне $(0, 2)$

Сведение MC-TCTL к MC-CTL на примере



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

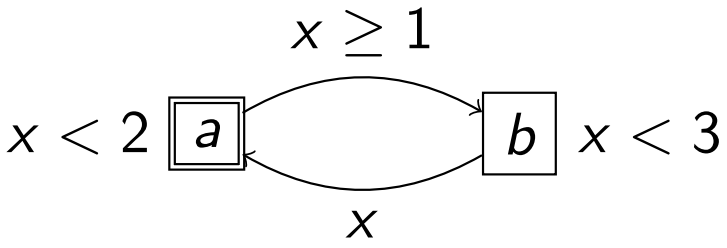


Переход $\xrightarrow{x \geq 1}$ из состояния с инвариантом $x < 2$ в состояние с инвариантом $x < 3$ можно выполнить только при значении часов x из интервала $[1, 2)$

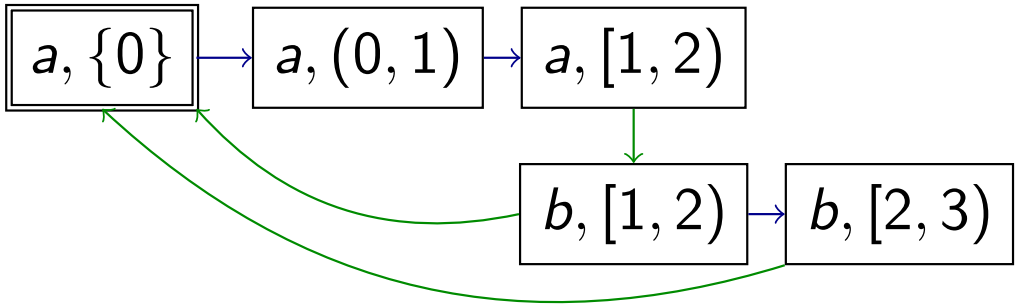
Разобьём интервал $(0, 2)$ на два: $(0, 1)$ и $[1, 2)$

При *непрерывном* увеличении времени из начального состояния значение x будет последовательно проходить через интервалы $\{0\}$, $(0, 1)$, $[1, 2)$

Сведение MC-TCTL к MC-CTL на примере



AGAF$(x = 1)$

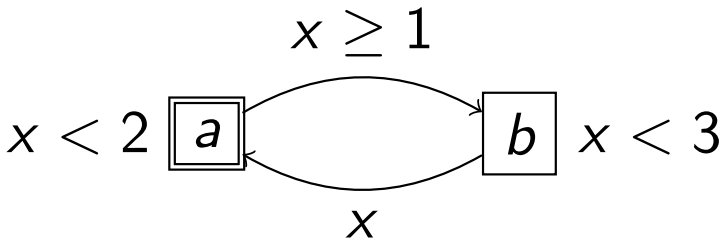


Из левого состояния автомата при значении часов в диапазоне $[1, 2)$ можно перейти в правое состояние с сохранением показания часов

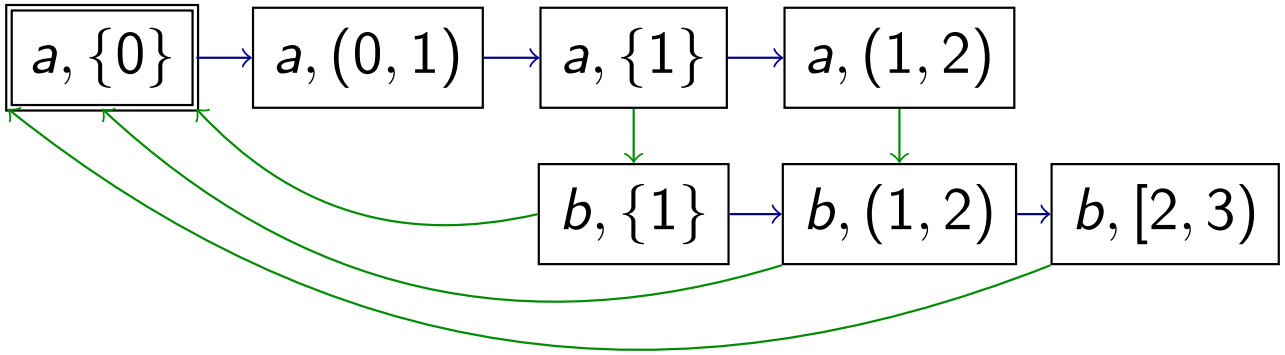
В правом состоянии значение часов можно поднять до любого, меньшего 3

Из правого состояния автомата всегда можно перейти в левое, сбросив часы

Сведение MC-TCTL к MC-CTL на примере



AGAF$(x = 1)$

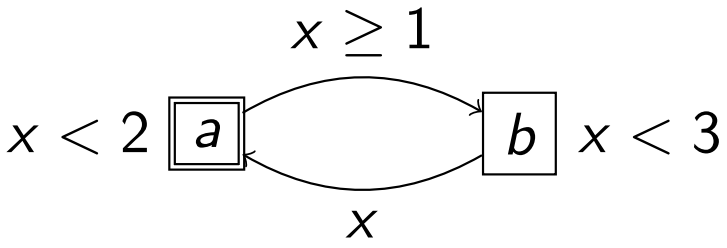


Формула φ содержит элементарные ограничения $x \leq 1$ и $x < 1$

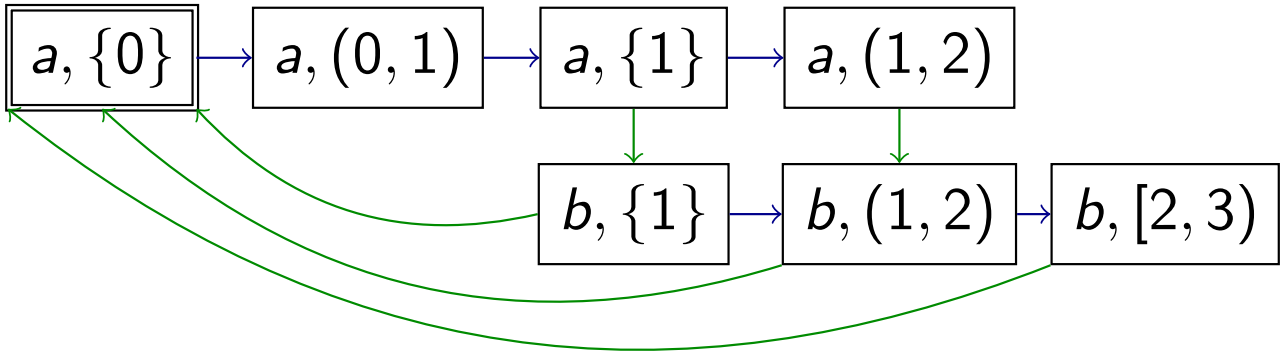
$$((x = 1) \equiv (x \leq 1 \,\&\, \neg(x < 1)))$$

Чтобы **однозначно** разметить состояния модели этими ограничениями, следует разбить интервал $[1, 2)$ на $\{1\}$ и $(1, 2)$

Сведение MC-TCTL к MC-CTL на примере



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



В результате получена модель Крипке M, которой описываются в точности все прогрессивные вычисления автомата A, включая все промежуточные конфигурации вычислений

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

Осталось показать, как построить аналогичную модель Крипке в общем случае, и доказать, что равновыполнимость формулы φ на A и M не случайна

Временные регионы

Попытаемся определить региональное отношение $\sim$, используя как можно меньше информации об устройстве автомата A и формулы φ

Для упрощения технических выкладок и пояснений будем считать, что ни автомат, ни формула не содержат разностных ограничений ($c_1 - c_2 < k$, $c_1 - c_2 \leq k$)

Для описания системы регионов потребуются две операции:

(r — регион, X — множество часов)

- r^+ — регион, следующий за r при *непрерывном* продвижении времени
  - синие переходы будут иметь вид $(\ell, r) \rightarrow (\ell, r^+)$
  - для каждого r должно существовать не более одного региона r^+
- $r[X] = \{\nu[X] \mid \nu \in r\}$
  - зелёные переходы будут иметь вид $(\ell, r) \rightarrow (\ell', r[X])$
  - для каждых r и X должен существовать единственный регион $r[X]$

Временные регионы

Первая попытка определить $\sim$ (неуспешная)

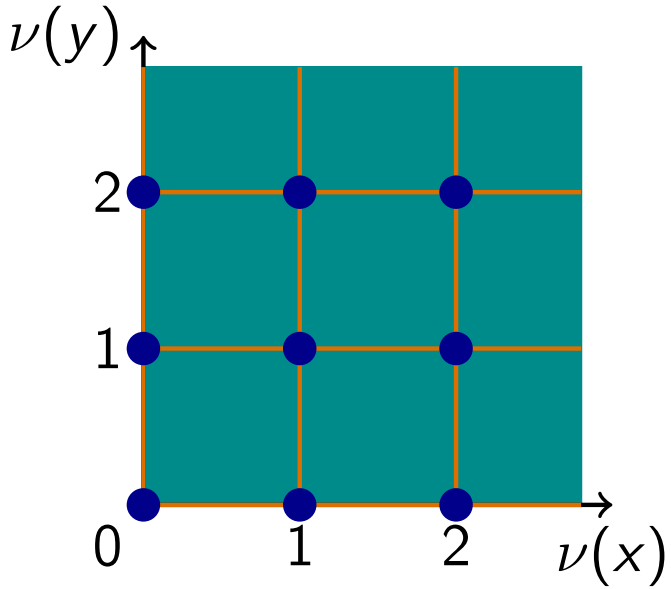
$\lfloor t \rfloor$ — это целая часть числа t

$frac(t)$ — это дробная часть числа t

$\nu_1 \sim \nu_2$ в том и только том случае, если для любых часов x верны два условия:

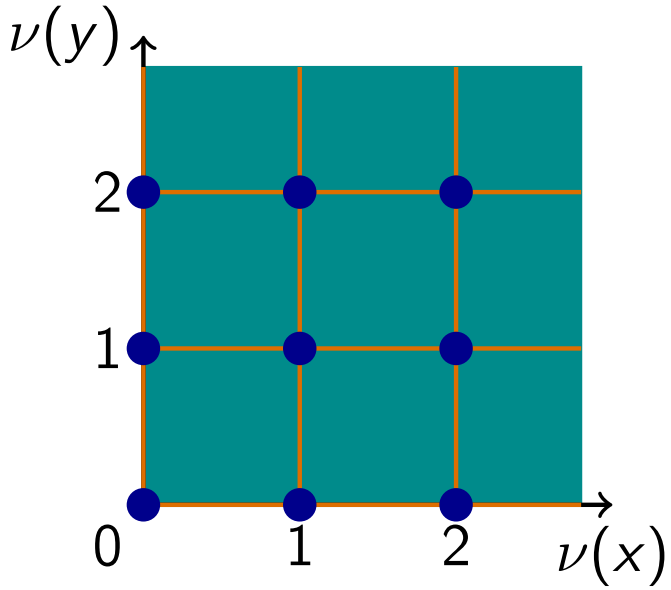
1. $\lfloor \nu_1(x) \rfloor = \lfloor \nu_2(x) \rfloor$
2. $frac(\nu_1(x)) = 0 \Leftrightarrow frac(\nu_2(x)) = 0$

Пример: временные регионы для двух часов x, y — это связные области одного цвета на картинке



Временные регионы

Первая попытка определить $\sim$ (неуспешная)



Хорошие свойства $\sim$:

- если $\nu_1 \sim \nu_2$, то для любого ограничения g верно $\nu_1 \models g \Leftrightarrow \nu_2 \models g$
- для любого региона r и любого множества часов X множество $r[X]$ является регионом

Оставшиеся проблемы:

- $|\mathfrak{R}| = \infty$
- как определить операцию r^+?

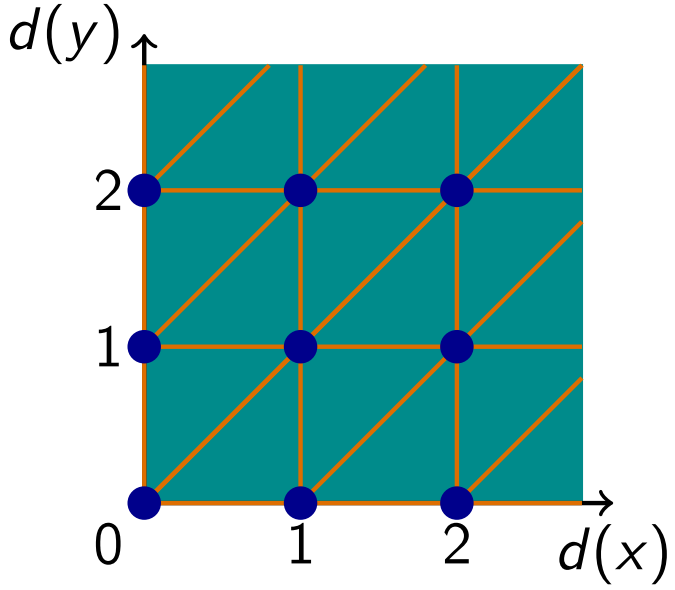
Временные регионы

Вторая попытка определить $\sim$ (неуспешная)

$\nu_1 \sim \nu_2$ в том и только том случае, если для любой пары часов x, y верны три условия:

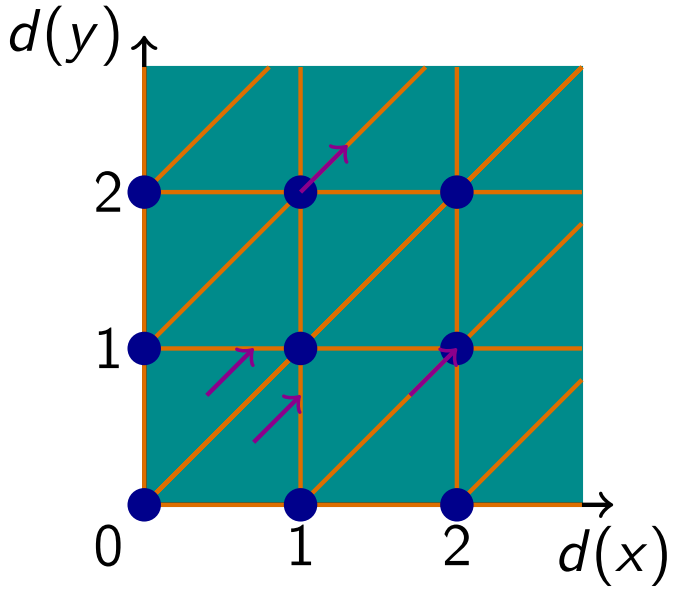
1. $\lfloor \nu_1(x) \rfloor = \lfloor \nu_2(x) \rfloor$
2. $frac(\nu_1(x)) = 0 \Leftrightarrow frac(\nu_2(x)) = 0$
3. $frac(\nu_1(x)) \leq frac(\nu_1(y)) \Leftrightarrow frac(\nu_2(x)) \leq frac(\nu_2(y))$

Пример: временные регионы для двух часов x, y — это связные области одного цвета на картинке



Временные регионы

Вторая попытка определить $\sim$ (неуспешная)

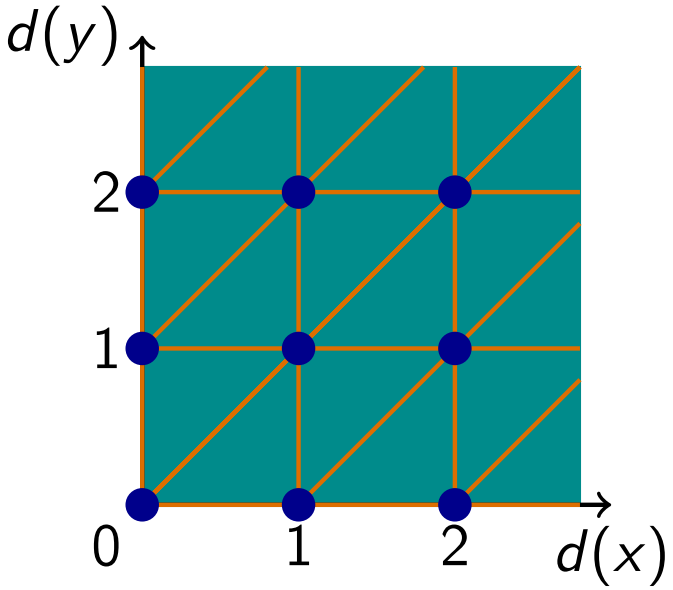


Хорошие свойства $\sim$:

- если $\nu_1 \sim \nu_2$, то для любого ограничения g верно $\nu_1 \models g \Leftrightarrow \nu_2 \models g$
- для любого региона r и любого множества часов X множество $r[X]$ является регионом
- можно корректно определить операцию r^+
  - примеры переходов от r к r^+ изображены стрелками

Временные регионы

Вторая попытка определить $\sim$ (неуспешная)



Оставшиеся проблемы:

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

Временные регионы

Третья попытка определить $\sim$ (успешная)

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

Очевидное утверждение: если $\nu_1(x) > k_x$ и $k \leq k_x$, то $\nu_1 \not\models (x < k)$ и $\nu_1 \not\models (x \leq k)$

Это означает, что все регионы *во второй попытке определить* $\sim$, различающиеся только *очень большими* значениями таймеров, с точки зрения проверки свойств и (не)возможности выполнения переходов автомата *абсолютно одинаковы*

Объединим каждое семейство *абсолютно одинаковых* регионов в один

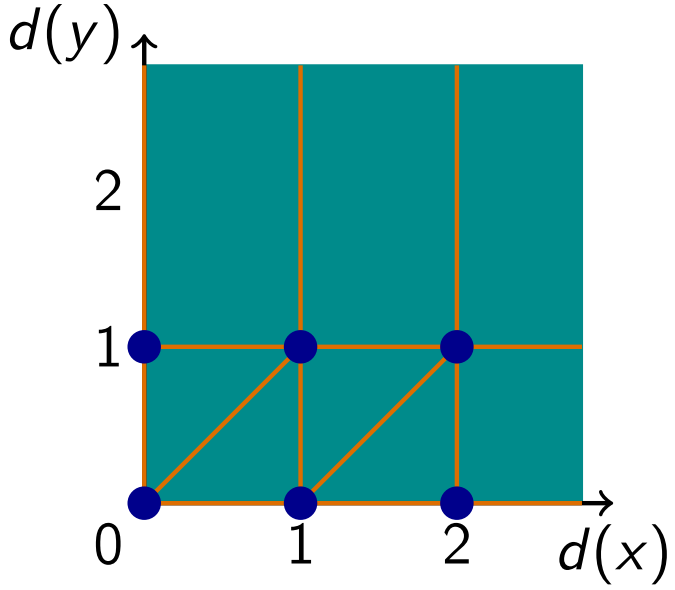
Временные регионы

Третья попытка определить $\sim$ (успешная)

$\nu_1 \sim \nu_2$ в том и только том случае, если для любой пары часов x, y верно следующее:

1. $\nu_1(x) > k_x \Leftrightarrow \nu_2(x) > k_x$
2. если $\nu_1(x) \leq k_x$, $\nu_1(y) \leq k_y$, 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: временные регионы для двух часов x, y и констант $k_x = 2$, $k_y = 1$ — это связные области одного цвета на картинке



Оценка числа временных регионов

Утверждение

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

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

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 таймеров региона

Оценка числа временных регионов

Утверждение

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

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

Доказательство.

Откуда в оценках взялось

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

Следствие

$|\mathfrak{R}| < \infty$

Продвижение регионов

Последняя деталь, которая потребуется в определении системы регионов $RS(A, \varphi)$ — это определение операции r^+ над регионами r

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

Открытый регион — это регион, открытый для всех часов

Продвижение региона r, где r — любой регион, кроме открытого, — это регион r^+, 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 $(\nu + d') \in r \cup r^+$

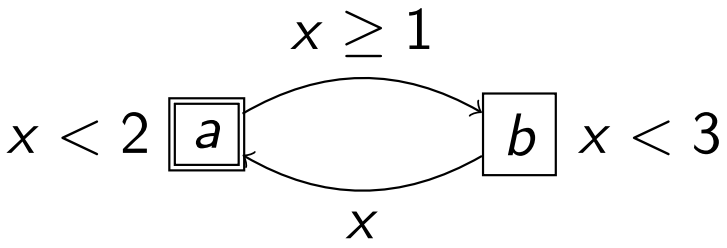
Системы регионов

Система регионов $RS(A, \varphi)$ для автомата $A = (L, \ell_0, C, \xi, I, T)$ и TCTL-формулы φ — это наибольший тотальный подграф размеченного графа G, определяемого так:

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

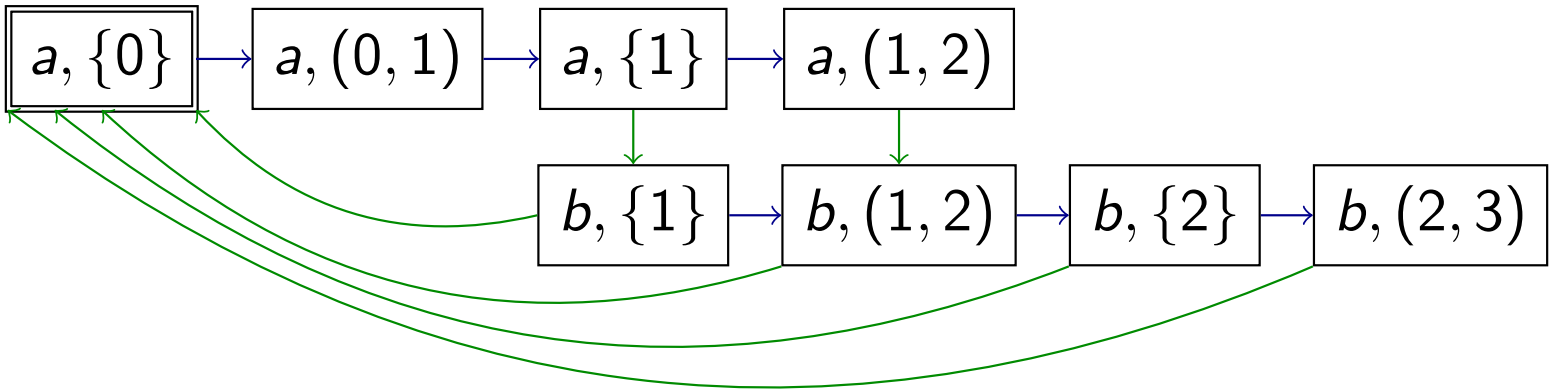
Системы регионов

Пример:



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

Система регионов для автомата A и TCTL-формулы φ, рассмотренных в качестве примера в начале лекции, выглядит так:



Сведение MC-TCTL к MC-CTL

Теорема

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

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

Доказательство.

Записью $[\nu]$, где ν — оценка часов, обозначим регион r, такой что $\nu \in r$

Записью $[s]$, где $s = (\ell, \nu)$ — состояние модели $M(A)$ автомата A, обозначим состояние $(\ell, [\nu])$ системы регионов $RS(A, \varphi)$

Записью $[s]^-$, где $s = (\ell, r)$ — состояние системы регионов $RS(A, \varphi)$, обозначим множество $\{(\ell, \nu) \mid [\nu] = r\}$

Сведение MC-TCTL к MC-CTL

Доказательство.

Записью $[path]$, где $path = s_1 \to s_2 \to \dots$ — путь в модели $M(A)$, обозначим путь в $RS(A, \varphi)$ следующего вида:

- переход $s_i \hookrightarrow s_{i+1}$ соответствует переходу $[s_i] \to [s_{i+1}]$
- переход $s_1 \mapsto s_{i+1}$ соответствует подпути $[s_i] \to [s_i^+] \to [s_i^{++}] \to \dots \to [s_{i+1}]$

Записью $[comp]^-$, где $comp = s_1 \to s_2 \to \dots$ — путь в $RS(A, \varphi)$, обозначим множество путей в модели $M(A)$, таких что

- переход $s_i \to s_{i+1}$ соответствует переходу $q_m \hookrightarrow q_{m+1}$, где $q_m \in [s_i]^-$ и $q_{m+1} \in [s_{i+1}]^-$
- каждый максимальный подпуть $s_i \to s_{i+1} \to \dots \to s_{i+k}$ соответствует переходу $q_m \mapsto q_{m+1}$, где $q_m \in [s_i]^-$ и $q_{m+1} \in [s_{i+k}]^-$

Сведение MC-TCTL к MC-CTL

Доказательство.

Докажем индукцией по построению формулы, что для любой промежуточной конфигурации s любого прогрессивного вычисления автомата A верна равносильность

$$M(A), s \models_T \varphi \quad \Leftrightarrow \quad RS(A, \varphi), [s] \models \varphi$$

База индукции: $\varphi = a$, $a \in AP \cup AC_\varphi$
Очевидно: s и $[s]$ помечены одинаковыми атомарными высказываниями, и $\nu \models e \Leftrightarrow [\nu] \models e$

Индуктивный переход, булевы связки: $\varphi = \neg\psi_1$ или $\varphi = \psi_2 \,\&\, \psi_3$ или $\varphi = \psi_4 \vee \psi_5$ или $\varphi = \psi_6 \to \psi_7$
Очевидно: семантики булевых связок в TCTL и CTL дословно совпадают

Индуктивный переход, темпоральные операции
Подробно рассмотрим только один случай: $\varphi = \mathbf{E}(\psi \mathbf{U} \chi)$

Сведение MC-TCTL к MC-CTL

Доказательство.

$$M(A), s \models_T \varphi \quad \Leftrightarrow \quad RS(A, \varphi), [s] \models \varphi$$
$$\varphi = \mathbf{E}(\psi \mathbf{U} \chi)$$

Необходимость: пусть $M(A), s_0 \models_T \varphi$

Тогда существует путь $path : s_0 \to s_1 \to \cdots \to s_k$ в $M(A)$, являющийся подпоследовательностью прогрессивного вычисления, такой что

- $M(A), s_k \models_T \chi$
- для любой промежуточной конфигурации s для пары (s_{i-1}, s_i), $1 \leq i \leq k$, верно $M(A), s \models_T \psi \vee \chi$

По построению системы $RS(A, \varphi)$, в ней содержится путь $[path] : q_1 \to \cdots \to q_k$

По индуктивному предположению, $RS(A, \varphi), q_k \models \chi$ и $RS(A, \varphi), q_j \models \psi \vee \chi$ для $j < k$, а значит, $RS(A, \varphi) \models \psi \mathbf{U} \chi$

Сведение MC-TCTL к MC-CTL

Доказательство.

$$M(A), s \models_T \varphi \quad \Leftrightarrow \quad RS(A, \varphi), [s] \models \varphi$$
$$\varphi = \mathbf{E}(\psi \mathbf{U} \chi)$$

Достаточность: пусть $RS(A, \varphi), s_0 \models_T \varphi$

Тогда существует путь $path : s_0 \to s_1 \to \cdots \to s_k$ в $RS(A, \varphi)$, такой что

- $RS(A, \varphi), s_k \models \chi$
- $RS(A, \varphi), s_i \models \psi$ для $i < k$

По построению системы $RS(A, \varphi)$, для любой конфигурации q_0, $q_0 \in [s_0]^-$, в $M(A)$ содержится путь $path' : q_0 \to q_1 \to \cdots \to q_m$, $path' \in [path]^-$

По индуктивному предположению,

- $M(A), q_m \models \chi$, так как $[q_m] = s_k$
- для любой промежуточной конфигурации q для пары q_{i-1}, q_i, $1 \leq i \leq m$, верно хотя бы одно из двух:
  - $M(A), q \models \chi$, если $[q] = s_k$
  - $M(A), q \models \psi$, в остальных случаях ▼

Сведение MC-TCTL к MC-CTL

Теорема

Для любого корректного временного 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**: и автомат, и формула могут содержать **разностные ограничения**

Сети временных 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 временных автоматов

Сети временных автоматов

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

Единственное синтаксическое отличие такого автомата от *обычного* временного автомата состоит в том, что каждый переход, помимо предусловия и множества сбрасываемых часов, помечен также синхронизацией: выражением $c!$ или $c?$, где $c \in CH$ (посылка в канал и 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 $A = (L, \ell_0, C, \xi, I, T)$ над AP и CH имеет вид $L \times Guard(C) \times Sync(CH) \times 2^C \times L$

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

Сети временных автоматов

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

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

Семантика сетей временных автоматов

Конфигурация сети $(C, CH, (A_1, \ldots, A_k))$, где
$A_i = (L^i, \ell_0^i, C, \xi^i, I^i, T^i)$ — это пара $((\ell_1, \ldots, \ell_k), \nu)$, где

- $\ell_i \in L^i$
- ν — оценка часов C

Для удобочитаемости иногда скобки вокруг набора состояний автоматов в конфигурации будут опускаться

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

Вычисление сети — это бесконечная последовательность конфигураций, такая что

- первая конфигурация последовательности — начальная
- каждая следующая конфигурация c_{i+1} получается из предыдущей c_i (сокращённо: $c_i \to c_{i+1}$) одним из трёх способов:
  - продвижение времени: $c_i \mapsto c_{i+1}$
  - изменение состояния: $c_i \hookrightarrow c_{i+1}$
  - рандеву: $c_i \rightsquigarrow c_{i+1}$

Семантика сетей временных автоматов

Продвижение времени

$((\ell_1, \ldots, \ell_k), \nu) \mapsto_d ((\ell_1, \ldots, \ell_k), \nu + d)$, если
$\nu + d \models I^1(\ell_1) \,\&\, \ldots \,\&\, I^k(\ell_k)$

$(\vec{\ell}, \nu) \mapsto (\vec{\ell'}, \nu')$, если существует положительное действительное число d, такое что $(\vec{\ell}, \nu) \mapsto_d (\vec{\ell'}, \nu')$

Изменение состояния

$((\ell_1, \ldots, \ell_k), \nu) \hookrightarrow ((\ell_1, \ldots, \ell_{i-1}, \ell'_i, \ell_{i+1}, \ldots, \ell_k), \nu')$, где
$1 \leq i \leq k$, если существуют предусловие g и множество часов X, такие что

- $\ell_i \xrightarrow{g,\lambda,X} \ell'_i \in T^i$
- $\nu \models g$
- $\nu' = \nu[X]$
- $\nu' \models I^i(\ell'_i)$

Семантика сетей временных автоматов

Рандеву

$((\ell_1, \ldots, \ell_k), \nu) \rightsquigarrow$
$((\ell_1, \ldots, \ell_{i-1}, \ell'_i, \ell_{i+1}, \ldots, \ell_{j-1}, \ell'_j, \ell_{j+1}, \ldots, \ell_k), \nu')$, где
$1 \leq i < j \leq k$, если существуют предусловия g_1, g_2, множества часов X_1, X_2 и канал ch, такие что

- либо $\ell_i \xrightarrow{g_1, ch!, X_1} \ell'_i \in T^i$ и $\ell_j \xrightarrow{g_2, ch?, X_2} \ell'_j \in T^j$,
  либо $\ell_i \xrightarrow{g_1, ch?, X_1} \ell'_i \in T^i$ и $\ell_j \xrightarrow{g_2, ch!, X_2} \ell'_j \in T^j$
- $\nu \models g_1 \,\&\, g_2$
- $\nu' = \nu[X_1 \cup X_2]$
- $\nu' \models I^i(\ell'_i) \,\&\, I^j(\ell'_j)$

Семантика сетей временных автоматов

Модель $M(N)$ сети N определяется так же, как и модель временного автомата, с двумя добавлениями:

- вместо дуг $\rightsquigarrow$ в модели проводятся дуги $\hookrightarrow$
- состояние $(\ell_1, \ldots, \ell_k, \nu)$ помечается множеством $\xi^1(\ell_1) \cup \cdots \cup \xi^k(\ell_k) \cup \{e \mid e \in AC(C),\ \nu \models e\}$, где $\xi^1, \ldots, \xi^k$ — функции разметки состояний соответствующих автоматов сети высказываниями, и C — множество часов сети

$N \models_T \varphi$ — это синоним записи $M(N) \models_T \varphi$

Задача model checking для сетей временных автоматов (MCN-TCTL):

Для заданной корректной сети N и заданной TCTL-формулы φ проверить справедливость соотношения

$$N \models_T \varphi$$

Трансляция сетей во временные автоматы

Теорема

Для любой сети временных автоматов N существует временной автомат A, такой что $M(N) = M(A)$

Доказательство.

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

Требуемый автомат $A = (L, \ell_0, C, \xi, I, T)$ устроен так:

- $L = L^1 \times \cdots \times L^m$
- $\ell_0 = (\ell_0^1, \ldots, \ell_0^m)$
- $I(\ell_1, \ldots, \ell_m) = I^1(\ell_1) \,\&\, \ldots \,\&\, I^m(\ell_m)$
- $(\ell_1, \ldots, \ell_m) \xrightarrow{g,X} (\ell'_1, \ldots, \ell'_m)) \in T$ тогда и только тогда, когда верно одно из условий:
  - существует i, такое что: $\ell_i \xrightarrow{g,\lambda,X} \ell'_i \in T^i$; $\ell_p = \ell'_p$ при $p \neq i$
  - существуют различные i и j, такие что: $\ell_i \xrightarrow{g_1,c!,X_1} \ell'_i \in T^i$ и $\ell_j \xrightarrow{g_2,c?,X_2} \ell'_j \in T_j$; $\ell_p = \ell'_p$ при $p \notin \{i, j\}$; $g = g_1 \,\&\, g_2$; $X = X_1 \cup X_2$

▼

Трансляция сетей во временные автоматы

Теорема

Для любой сети временных автоматов N существует временной автомат A, такой что $M(N) = M(A)$

На основании этой теоремы можно

- утверждать, что выразительные возможностей **сетей** временных автоматов в точности совпадают с выразительными возможностями *обычных* временных автоматов
- сформулировать простой алгоритм решения задачи MCN-TCTL ($N \overset{?}{\models}_T \varphi$):
  - построить временной автомат $A(N)$, такой что $M(A(N)) = M(N)$
  - применить алгоритм решения задачи $A(N) \overset{?}{\models}_T \varphi$

Конец лекции 10