

Математические методы верификации схем и программ

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

Блок 34

Алгоритм проверки моделей для TCTL
Временные регионы
Системы регионов

Лектор:
Подымов Владислав Васильевич
E-mail:
valdus@yandex.ru

ВМК МГУ, 2024/2025, осенний семестр

Вступление

Задача MC-TCTL: для заданного корректного временного автомата \mathcal{A} и заданной tctl-формулы φ проверить соотношение $\mathcal{A} \models \varphi$

Задача MC-CTL: для заданной модели Крипке M и заданной ctl-формулы φ проверить соотношение $M \models \varphi$

Синтаксис CTL строго шире синтаксиса TCTL

Семантика CTL похожа на семантику TCTL, но существенно различается из-за особенностей отсчёта времени

Эти две логики настолько похожи друг на друга, что можно попробовать *свести* решение MC-TCTL к решению MC-CTL

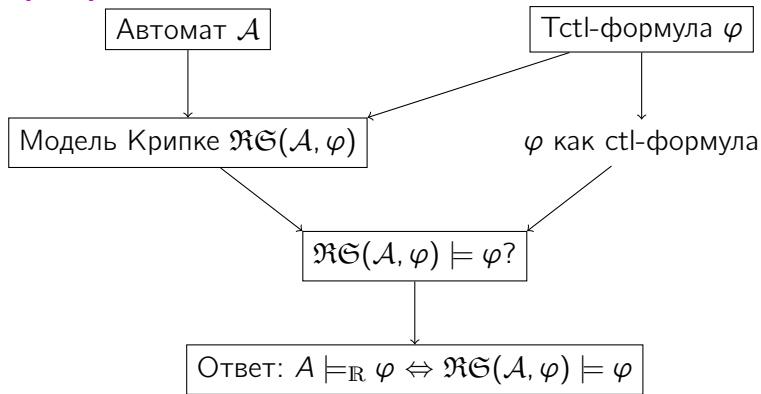
Чтобы нагляднее различать отношения выполнимости в смысле CTL и в смысле TCTL, будем отношение выполнимости для TCTL записывать так: $\models_{\mathbb{R}}$

Общая схема MC-TCTL

Дано: временной автомат \mathcal{A} , tctl-формула φ над множествами атомарных высказываний AP и часов \mathcal{C}

Требуется проверить справедливость соотношения $\mathcal{A} \models_{\mathbb{R}} \varphi$

Схема проверки:



Модель $\mathcal{RG}(\mathcal{A}, \varphi)$ будет называться **системой регионов** для автомата \mathcal{A} и формулы φ

Общая схема MC-TCTL

$AC(\mathcal{A})$ и $AC(\varphi)$ — так будем обозначать все атомарные временные ограничения, содержащиеся соответственно в \mathcal{A} и в φ

Система $\mathfrak{RG}(\mathcal{A}, \varphi)$ будет строиться над множеством $AP \cup AC(\varphi)$
(и тогда можно считать φ *ctl*-формулой)

Каждая конфигурация автомата будет отвечать некоторому состоянию системы $\mathfrak{RG}(\mathcal{A}, \varphi)$:

- ▶ Множество всех оценок часов будет разбито на классы эквивалентности (регионы)
- ▶ Оценка ν будет отвечать её региону $[\nu]$
- ▶ Конфигурация (s, ν) будет отвечать состоянию $(s, [\nu])$
- ▶ $[(0, 0, \dots, 0)] = \{(0, 0, \dots, 0)\}$

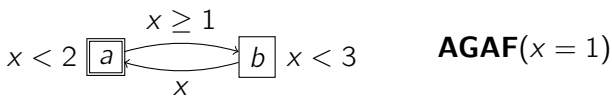
Шаг вычисления $(s_1, \nu_1) \rightarrow (s_2, \nu_2)$ автомата будет отвечать пути $(s_1, [\nu_1]) \rightarrow \dots \rightarrow (s_2, [\nu_2])$ в системе регионов

(и, в частности, все покрывающиеся конфигурации станут явными)

Состояние $(s, [\nu])$ будет размечаться высказываниями из AP согласно s и ограничениями из $AC(\varphi)$ согласно ν

Общая схема MC-TCTL

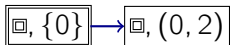
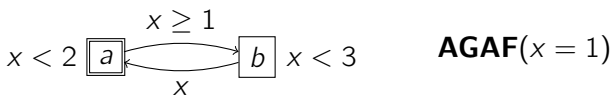
Пример: попробуем при помощи «пристального взгляда» построить подходящую модель Крипке (хотя и не в точности $\mathfrak{R}\mathfrak{G}(\mathcal{A}, \varphi)$) для таких автомата \mathcal{A} и tctl-формулы φ :



Единственное начальное состояние модели — это $\boxed{\square}$ со значением 0 часов x

Общая схема MC-TCTL

Пример: попробуем при помощи «пристального взгляда» построить подходящую модель Крипке (хотя и не в точности $\mathfrak{R}\mathfrak{G}(\mathcal{A}, \varphi)$) для таких автомата \mathcal{A} и tctl-формулы φ :

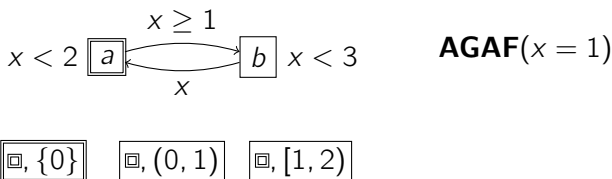


Начав вычисление в $([a], 0)$, \mathcal{A} обязан продвинуть время, и может продвинуть часы до любого значения интервала $(0, 2)$

Для начала запишем все такие продвижения времени как один переход в модели

Общая схема MC-TCTL

Пример: попробуем при помощи «пристального взгляда» построить подходящую модель Крипке (хотя и не в точности $\mathfrak{R}\mathfrak{G}(\mathcal{A}, \varphi)$) для таких автомата \mathcal{A} и tctl-формулы φ :

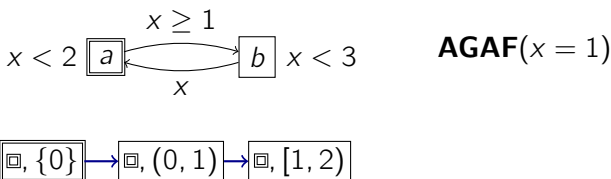


Для значений часов из $[1, 2)$ открыт верхний переход автомата, а для значений из $(0, 1)$ этот переход закрыт

Чтобы **детерминированно** воспроизвести шаги вычисления автомата, следует разбить состояние $(\boxed{a}, (0, 2))$ на два: $(\boxed{a}, (0, 1))$ и $(\boxed{a}, [1, 2))$

Общая схема MC-TCTL

Пример: попробуем при помощи «пристального взгляда» построить подходящую модель Крипке (хотя и не в точности $\mathfrak{R}\mathfrak{G}(\mathcal{A}, \varphi)$) для таких автомата \mathcal{A} и tctl-формулы φ :

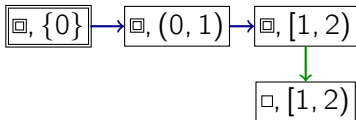
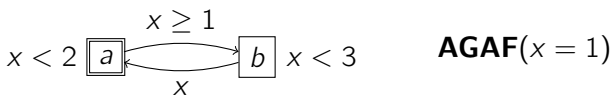


Когда автомат **непрерывно** ожидает (продвигает время), начав в $(\boxed{a}, 0)$, значение часов последовательно проходит через интервалы $\{0\}$, $(0, 1)$ и $[1, 2)$

Чтобы воспроизвести все варианты такого ожидания, соединим соответствующие состояния по порядку

Общая схема MS-TCTL

Пример: попробуем при помощи «пристального взгляда» построить подходящую модель Крипке (хотя и не в точности $\mathfrak{R}\mathfrak{G}(\mathcal{A}, \varphi)$) для таких автомата \mathcal{A} и tctl-формулы φ :



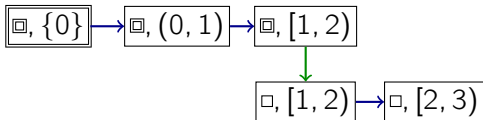
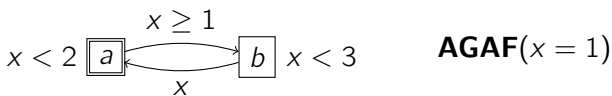
Для каждой конфигурации вида (\square, d) , где $1 \leq d < 2$,

верно соотношение $(\square, d) \xrightarrow{x \geq 1} (\square, d)$

Добавим в модель переход, воспроизводящий все такие шаги вычисления автомата

Общая схема MC-TCTL

Пример: попробуем при помощи «пристального взгляда» построить подходящую модель Крипке (хотя и не в точности $\mathfrak{R}\mathfrak{G}(\mathcal{A}, \varphi)$) для таких автомата \mathcal{A} и tctl-формулы φ :

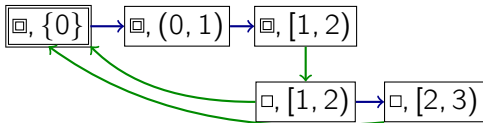
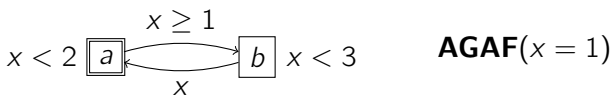


Когда автомат ожидает, начав в (\square, d) , где $1 \leq d < 2$, значение часов может пройти через остаток интервала $[1, 2)$ и через часть интервала $[2, 3)$

Добавим в модель переход, воспроизводящий такое ожидание

Общая схема MC-TCTL

Пример: попробуем при помощи «пристального взгляда» построить подходящую модель Крипке (хотя и не в точности $\mathfrak{R}\mathfrak{G}(\mathcal{A}, \varphi)$) для таких автомата \mathcal{A} и tctl-формулы φ :



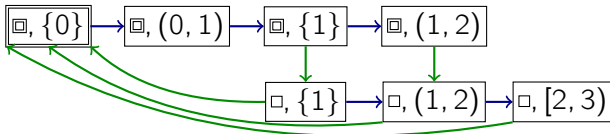
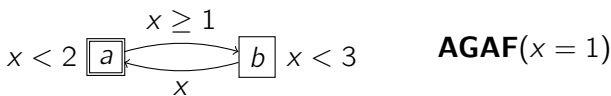
Для каждой конфигурации (\square, d) , где $1 \leq d < 3$,

верно соотношение $(\square, d) \xrightarrow{x} (\square, 0)$

Добавим в модель переходы, отвечающие всем таким шагам вычисления автомата

Общая схема MC-TCTL

Пример: попробуем при помощи «пристального взгляда» построить подходящую модель Крипке (хотя и не в точности $\mathcal{R}\mathcal{G}(\mathcal{A}, \varphi)$) для таких автомата \mathcal{A} и tctl-формулы φ :



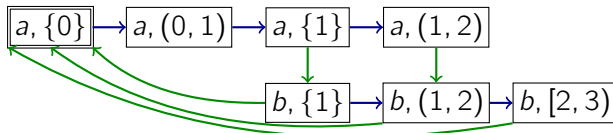
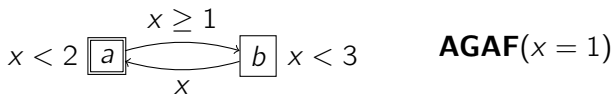
$(x = 1) \equiv (x \leq 1 \ \& \ \neg(x < 1))$:

в формуле φ содержатся ограничения $x \leq 1$ и $x < 1$

Чтобы **детерминированно** разметить состояния модели этими ограничениями, следует разбить в каждом состоянии модели интервал $[1, 2)$ на два: $\{1\}$ и $(1, 2)$

Общая схема MC-TCTL

Пример: попробуем при помощи «пристального взгляда» построить подходящую модель Крипке (хотя и не в точности $\mathfrak{R}\mathfrak{G}(\mathcal{A}, \varphi)$) для таких автомата \mathcal{A} и tctl-формулы φ :

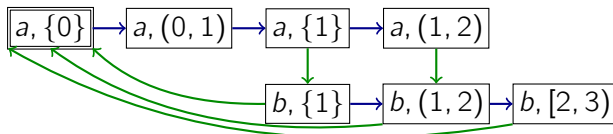
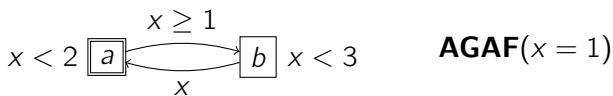


Получилась модель Крипке M , содержащая в точности все шаги вычисления автомата \mathcal{A} и все неявно покрытые конфигурации таких шагов

Нетрудно видеть, что $\mathcal{A} \models_{\mathbb{R}} \varphi$ и $M \models \varphi$

Общая схема MC-TCTL

Пример: попробуем при помощи «пристального взгляда» построить подходящую модель Крипке (хотя и не в точности $\mathfrak{R}\mathfrak{G}(\mathcal{A}, \varphi)$) для таких автомата \mathcal{A} и tctl-формулы φ :



Теперь перейдём к трудной части: **в общем случае ...**

- ▶ как устроить множества оценок (регионы), чтобы обеспечить требуемое соответствие, детерминированность и конечность?
- ▶ как совместить состояния автомата, регионы и переходы, чтобы чудесным образом превратить « $\models_{\mathbb{R}}$ » в « \models »?

Временные регионы

Разбиение оценок часов на классы основывается на **региональном отношении эквивалентности** оценок часов (\approx)

Полное подробное определение этого отношения будет приведено далее, и оно будет описываться постепенно (поэтапно)

Временной регион — это класс эквивалентности отношения \approx

Временные регионы — это множества оценок часов, использующиеся в качестве второго компонента состояния системы регионов

\mathfrak{R} — так будем обозначать семейство всех временных регионов

Временные регионы

Особенности устройства отношения \approx , которые необходимы для соответствия содержательному краткому описанию системы регионов и для всех технических тонкостей, возникших в примере, строго можно определить так:

- ▶ **Конечность**: общее число классов эквивалентности отношения \approx конечно
 - ▶ \Rightarrow множество состояний системы регионов конечно, и можно к ней применять известные алгоритмы анализа конечных моделей Крипке
- ▶ **Неразличимость временными ограничениями**: если $\nu_1 \approx \nu_2$ и $ag \in AC(\mathcal{A}) \cup AC(\varphi)$, то $\nu_1 \models ag \Leftrightarrow \nu_2 \models ag$
 - ▶ \Rightarrow детерминированность относительно предусловий и разметки состояний
- ▶ **Корректный сброс**: если ρ — регион и X — множество часов, то $\rho[X] = \{\nu[X] \mid \nu \in \rho\}$ — тоже регион
 - ▶ \Rightarrow детерминированность относительно сброса часов при выполнении переходов автомата
- ▶ **Корректное ожидание**: для любого региона ρ существует единственный регион ρ^+ , следующий за ρ при непрерывном ожидании автомата
 - ▶ \Rightarrow детерминированность относительно продвижения времени автоматом

Временные регионы

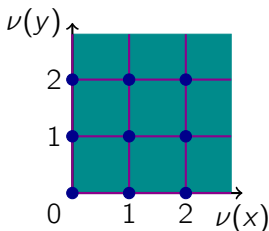
Первая (неудачная) попытка определить \approx

$\lfloor t \rfloor$ и $\text{frac}(t)$ — так будем обозначать соответственно целую и дробную часть числа действительного числа t

$\nu_1 \approx_1 \nu_2 \Leftrightarrow$ для любых часов x верно следующее:

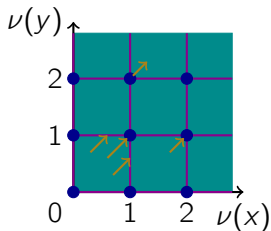
1. $\lfloor \nu_1(x) \rfloor = \lfloor \nu_2(x) \rfloor$
2. $\text{frac}(\nu_1(x)) = 0 \Leftrightarrow \text{frac}(\nu_2(x)) = 0$

Пример: регионы отношения \approx_1 для пары часов x, y изображены ниже как связанные одноцветные области числовой плоскости



Временные регионы

Первая (неудачная) попытка определить \approx



Хорошие свойства \approx_1 :

- ▶ Неразличимость временными ограничениями
- ▶ Корректный сброс

Плохие свойства \approx_1 :

- ▶ $|\mathfrak{R}| = \infty$
- ▶ Невозможно однозначно определить ρ^+
 - ▶ примеры пар (ρ, ρ^+) изображены выше стрелками

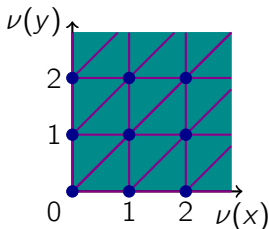
Временные регионы

Вторая (неудачная) попытка определить \approx

$\nu_1 \approx_2 \nu_2 \Leftrightarrow$ для любых часов x, y верно следующее:

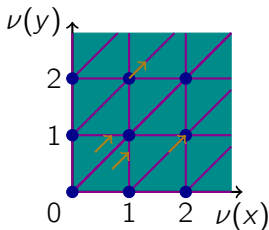
1. $\lfloor \nu_1(x) \rfloor = \lfloor \nu_2(x) \rfloor$
2. $\text{frac}(\nu_1(x)) = 0 \Leftrightarrow \text{frac}(\nu_2(x)) = 0$
3. $\text{frac}(\nu_1(x)) \leq \text{frac}(\nu_1(y)) \Leftrightarrow \text{frac}(\nu_2(x)) \leq \text{frac}(\nu_2(y))$

Пример: регионы отношения \approx_2 для пары часов x, y изображены ниже как связанные одноцветные области числовой плоскости



Временные регионы

Вторая (неудачная) попытка определить \approx



Хорошие свойства \approx_2 :

- ▶ Неразличимость временными ограничениями
- ▶ Корректный сброс
- ▶ Корректное ожидание

Плохие свойства \approx_2 :

- ▶ $|\mathfrak{R}| = \infty$

Временные регионы

Определение \approx

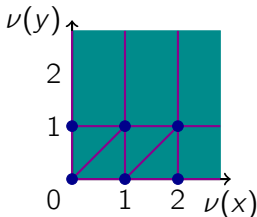
(третья попытка, удачная)

k_x — так будем обозначать максимальное целое число, встречающееся в правых частях ограничений из $AC(\mathcal{A}) \cup AC(\varphi)$

$\nu_1 \approx \nu_2 \Leftrightarrow$ для любых 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
 - ▶ $\lfloor \nu_1(x) \rfloor = \lfloor \nu_2(x) \rfloor$,
 - ▶ $\text{frac}(\nu_1(x)) = 0 \Leftrightarrow \text{frac}(\nu_2(x)) = 0$ и
 - ▶ $\text{frac}(\nu_1(x)) \leq \text{frac}(\nu_1(y)) \Leftrightarrow \text{frac}(\nu_2(x)) \leq \text{frac}(\nu_2(y))$

Пример: регионы для пары часов x, y и констант $k_x = 2, k_y = 1$ изображены ниже как связанные одноцветные области числовой плоскости



Оценка числа регионов

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

Доказательство. Ограничимся пояснениями всех множителей в оценках:

- ▶ $\prod_{x \in C} k_x$ — это количество единичных $|C|$ -мерных кубов, которыми можно покрыть декартово произведение всех интервалов $[0, k_x]$
- ▶ $|C|!$ — столькими способами можно упорядочить дробные части значений часов
 - ▶ В оценке снизу: по крайней мере столько регионов содержится во внутренности одного единичного куба
- ▶ $2k_x + 2$ — это общее число попарно различных интервалов значений часов x в регионах: $\{0\}$; $(0, 1)$; $\{1\}$; $(1, 2)$; $\{2\}$; ...
- ▶ $2^{|C|-1}$ — столькими способами можно для заданного порядка дробных частей объявить, какие из этих дробных частей равны ▼

Следствие (конечность отношения \approx). $|\mathfrak{R}| < \infty$

Другие свойства регионов

Утверждение (неразличимость временными ограничениями)

Для любых часов x , оценок ν_1 и ν_2 , таких что $\nu_1 \approx \nu_2$, и числа $k \in \mathbb{N}_0$ верно:

$$\begin{aligned}\nu_1 \models x < k &\Leftrightarrow \nu_2 \models x < k \quad \text{и} \\ \nu_1 \models x \leq k &\Leftrightarrow \nu_2 \models x \leq k\end{aligned}$$

Временное ограничение g над атомарными ограничениями $\text{ACC}_A \cup \text{ACC}_\varphi$ выполняется в регионе ρ ($\rho \models g$), если для любой оценки часов ν из ρ верно $\nu \models g$

Утверждение (корректный сброс). Для любого региона ρ и любого множества часов X множество $\rho[X]$ является регионом

Другие свойства регионов

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

Регион называется **открытым**, если он открыт для всех часов, а иначе — **закрытым**

ρ^+ — это регион, **следующий** за регионом ρ :

- ▶ Если ρ открыт, то $\rho^+ = \rho$
- ▶ Иначе ρ^+ — регион, для которого верно следующее:
 - ▶ $\rho^+ \neq \rho$
 - ▶ Если $\nu \in \rho$ и $(\nu + d) \in \rho^+$, где $d \in \mathbb{R}_{>0}$, то для любого d' из $\mathbb{R}_{>0}$, такого что $d' < d$, верно $(\nu + d') \in \rho \cup \rho^+$

Утверждение (корректное ожидание)

За любым регионом ρ следует ровно один регион

Для лучшего понимания регионов можете попробовать строго доказать последние три утверждения

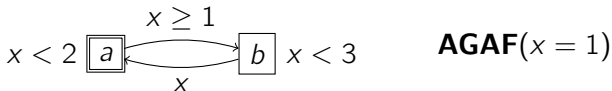
Системы регионов

Для временного автомата $\mathcal{A} = (S, s_0, \mathcal{I}, T, L)$ и tctl-формулы φ ...

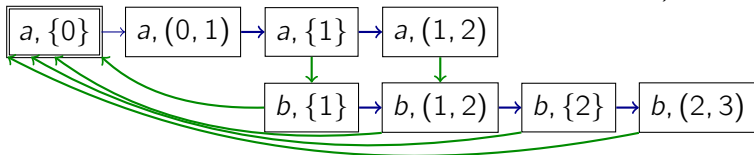
- ▶ **региональным состоянием** будем называть пару $(s, \rho) \in S \times \mathfrak{R}$
- ▶ **системой регионов** будем называть модель Крипке $\mathfrak{RS}(\mathcal{A}, \varphi)$, задающуюся как подграф следующего графа Γ , порождённый множеством всех вершин, достижимых из начальной:
 - ▶ Вершины Γ — это всевозможные региональные состояния
 - ▶ Вершина $(s_0, \{(0, 0, \dots, 0)\})$ — начальная
 - ▶ Каждая вершина (s, ρ) помечена множеством $L(s) \cup \{ag \mid ag \in AC(\varphi), \rho \models ag\}$
 - ▶ Дуга $(s, \rho) \rightarrow (s', \rho')$ входит в $\Gamma \iff$ верно хотя бы одно из двух:
 1. $\rho' = \rho^+, s' = s$ и $\rho^+ \models \mathcal{I}(s)$
 2. В \mathcal{A} существует переход $s \xrightarrow{g, X} s'$, такой что $\rho \models g$, $\rho' = \rho[X]$, and $\rho' \models \mathcal{I}(s')$

Системы регионов

Пример



Система регионов для изображённых автомата и формулы устроена так (атомарные временные ограничения, помечающие состояние, изображены как подходящие интервалы значений часов x):



Теорема. Для любого корректного временного автомата \mathcal{A} и любой tctl-формулы φ верно:

$$\mathcal{A} \models_{\mathbb{R}} \varphi \Leftrightarrow \mathcal{RG}(\mathcal{A}, \varphi) \models \varphi$$

Доказательство опустим: его объём и трудность намного превосходят пользу включения его в рассказ