

Математические методы верификации схем и программ

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

Блок 24

Логика ветвящегося реального времени
(TCTL)

Задача model checking для TCTL

Лектор:

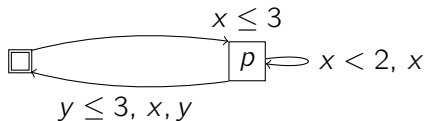
Подымов Владислав Васильевич

E-mail:

valdus@yandex.ru

Напоминание

Временной автомат над множеством часов $\{x, y\}$ и множеством атомарных высказываний $\{p\}$:



Дивергентное вычисление (для порядка часов (x, y)):

$$(\square, 0, 0) \mapsto (\square, 1, 1) \mapsto (\square, 2, 2) \mapsto \dots \mapsto (\square, n, n) \mapsto \dots$$

Вычисление Зенона (конвергентное и с бесконечным числом \leftrightarrow):

$$(\square, 0, 0) \mapsto (\square, 1.2, 1.2) \leftrightarrow (\square, 1.2, 1.2) \leftrightarrow (\square, 0, 0) \mapsto (\square, 1.2, 1.2) \leftrightarrow \dots$$

Тупиковое (конвергентное) вычисление:

$$(\square, 0, 0) \leftrightarrow (\square, 0, 0) \mapsto (\square, 1, 1) \mapsto (\square, \sqrt{2}, \sqrt{2}) \leftrightarrow (\square, 0, \sqrt{2}) \mapsto (\square, 3, \sqrt{2} + 3)$$

Автомат **корректен**, если не имеет зеноновских вычислений и любая его начальная трасса может быть продолжена до дивергентной

TCTL: синтаксис

Логика ветвящегося реального времени (Timed CTL; TCTL) — это аналог CTL, предназначенный для записи требований, предъявляемых к CPB

Будем использовать такой укороченный синтаксис tctl-формул над конечным множеством часов \mathcal{C} и конечным множеством атомарных высказываний AP:

$$\Phi ::= \top \mid p \mid ag \mid (\Phi \& \Phi) \mid (\neg \Phi) \mid (\mathbf{A}\varphi) \mid (\mathbf{E}\varphi),$$

$$\varphi ::= (\Phi \mathbf{U} \Phi),$$

где Φ — формула состояния (она же tctl-формула), φ — формула пути, $p \in AP$ и $ag \in AC(\mathcal{C})$

Отличия от синтаксиса ctl-формул:

1. Наряду с атомарными высказываниями (p) можно записывать и атомарные временные ограничения (ag)
2. Для реального времени понятие «следующий момент времени» бессмысленно, поэтому в синтаксисе нет оператора **X**

TCTL: семантика

Содержательная трактовка кванторов пути (**A**, **E**) и темпорального оператора (**U**) — это их трактовка в CTL, адаптированная к особенностям поведения CPB:

- ▶ **Eφ**: существует **дивергентная** трасса, для которой верно Φ
- ▶ **Aφ**: для любой **дивергентной** трассы верно Φ
- ▶ **φUψ**: в **реальном** будущем станет верным Ψ , а до тех пор будет верно Φ

Чтобы адекватно учесть реальное время в операторе **U**, следует «реально» переосмыслить дискретные (пошаговые) трассы автоматов

TCTL: семантика

Например, трассу

$$(\ell, 0) \mapsto (\ell, 1) \leftrightarrow (r, 0)$$

следует понимать так:

- ▶ Автомат начинает выполнение в состоянии ℓ и значением часов 0
- ▶ Затем автомат ожидает единицу времени, и во время ожидания значение часов **непрерывно** возрастает от 0 до 1, проходя через **все** значения интервала $[0, 1]$
- ▶ После этого автомат мгновенно переходит в состояние r , и значение часов сбрасывается

Таким образом, между конфигурациями $(\ell, 0)$ и $(\ell, 1)$ в этой трассе *неявно подразумевается* континуум промежуточных конфигураций для всех значений часов интервала $(0, 1)$

TCTL: семантика

Будем говорить, что конфигурация σ

- ▶ порождается парой конфигураций σ_1, σ_2 , если верно хотя бы одно из двух:

- ▶ $\sigma = \sigma_2$

- ▶ $\sigma_1 \xrightarrow{d} \sigma_2$ и $\sigma_1 \xrightarrow{d'} \sigma$, где $d' \in (0, d)$

- ▶ порождается на k -м шаге трассы

$$\sigma_0 \rightarrow \sigma_1 \rightarrow \dots,$$

где $k \geq 1$, если она порождается парой конфигураций σ_{k-1}, σ_k

- ▶ порождается на 0-м шаге трассы

$$\sigma_0 \rightarrow \sigma_1 \rightarrow \dots,$$

если $\sigma = \sigma_0$

- ▶ порождается трассой, если она порождается на каком-либо шаге этой трассы

TCTL: семантика

Как и для CTL, для TCTL задаются два вида выполнимости:

- ▶ **Выполнимость tctl-формулы Φ** в конфигурации σ автомата \mathcal{A} :
 $\mathcal{A}, \sigma \models \Phi$
- ▶ **Выполнимость формулы пути φ** на дивергентной трассе τ автомата \mathcal{A} : $\mathcal{A}, \tau \models \varphi$

Эти отношения для автомата $\mathcal{A} = (S, s_0, \mathcal{I}, T, L)$ над атомарными высказываниями AP и часами \mathcal{C} и формул над AP и \mathcal{C} задаются так:

- ▶ Всегда верно $\mathcal{A}, \sigma \models \mathfrak{t}$
- ▶ $\mathcal{A}, (s, \nu) \models p$, где $p \in AP \iff p \in L(s)$
- ▶ $\mathcal{A}, (s, \nu) \models ag$, где $ag \in AC(\mathcal{C}) \iff \nu \models ag$
- ▶ $\mathcal{A}, \sigma \models \Phi_1 \& \Phi_2 \iff \mathcal{A}, \sigma \models \Phi_1$ и $\mathcal{A}, \sigma \models \Phi_2$
- ▶ $\mathcal{A}, \sigma \models \neg\Phi \iff \mathcal{A}, \sigma \not\models \Phi$

TCTL: семантика

Как и для CTL, для TCTL задаются два вида выполнимости:

- ▶ **Выполнимость tctl-формулы** Φ в конфигурации σ автомата \mathcal{A} :
 $\mathcal{A}, \sigma \models \Phi$
- ▶ **Выполнимость формулы пути** φ на дивергентной трассе τ автомата \mathcal{A} : $\mathcal{A}, \tau \models \varphi$

Эти отношения для автомата $\mathcal{A} = (S, s_0, \mathcal{I}, T, L)$ над атомарными высказываниями AP и часами \mathcal{C} и формул над AP и \mathcal{C} задаются так:

- ▶ $\mathcal{A}, \sigma \models \mathbf{A}\varphi \Leftrightarrow$ для любой дивергентной σ -трассы τ автомата \mathcal{A} верно $\mathcal{A}, \tau \models \varphi$
- ▶ $\mathcal{A}, \sigma \models \mathbf{E}\varphi \Leftrightarrow$ существует дивергентная σ -трасса τ автомата \mathcal{A} , такая что верно $\mathcal{A}, \tau \models \varphi$

TCTL: семантика

Как и для CTL, для TCTL задаются два вида выполнимости:

- ▶ **Выполнимость tctl-формулы Φ** в конфигурации σ автомата \mathcal{A} :
 $\mathcal{A}, \sigma \models \Phi$
- ▶ **Выполнимость формулы пути φ** на дивергентной трассе τ автомата \mathcal{A} : $\mathcal{A}, \tau \models \varphi$

Эти отношения для автомата $\mathcal{A} = (S, s_0, \mathcal{I}, T, L)$ над атомарными высказываниями AP и часами \mathcal{C} и формул над AP и \mathcal{C} задаются так:

- ▶ $\mathcal{A}, \tau \models \Phi \mathbf{U} \Psi$, где $\tau = (\sigma_0 \rightarrow \sigma_1 \rightarrow \dots)$ \Leftrightarrow существуют номер k , $k \in \mathbb{N}_0$, и конфигурация σ , порождаемая на k -м шаге трассы τ , такие что
 - ▶ $\mathcal{A}, \sigma \models \Psi$
 - ▶ Если $k > 0$, то для любой конфигурации σ' , порождаемой трассой
 $\sigma_0 \rightarrow \sigma_1 \rightarrow \dots \rightarrow \sigma_{k-1} \rightarrow \sigma$,
верно $\mathcal{A}, \sigma' \models \Phi \vee \Psi$

Tctl-формула φ **выполняется на автомате \mathcal{A}** ($\mathcal{A} \models \varphi$), если она выполняется в начальной конфигурации этого автомата

TCTL: семантика, особенность **U**

«Если $k > 0$, то для любой конфигурации σ' ... верно $\mathcal{A}, \sigma' \models \Phi \vee \Psi$ »

В CTL в соответствующем месте семантики **U** вместо $\Phi \vee \Psi$ записывалось просто Φ

В содержательной трактовке **U** в TCTL говорится «а до тех пор верно Φ » (а не $\Phi \vee \Psi$)

Откуда же взялось « $\Phi \vee \Psi$ », и почему бы не написать просто Φ ?

Можно легко убедиться в том, что если в CTL написать в соответствующем месте $\Phi \vee \Psi$, то семантика **U** останется прежней

При этом для реального времени различие существенно, и в этом можно убедиться на таком примере

TCTL: семантика, особенность U

«Если $k > 0$, то для любой конфигурации σ' ... верно $\mathcal{A}, \sigma' \models \Phi \vee \Psi$ »

Пример автомата \mathcal{A} и tctl-формулы φ :

$$\square \quad \mathbf{A}((x \leq 1)\mathbf{U}(x > 1))$$

Все дивергентные вычисления этого автомата имеют вид

$$(\square, 0) \mapsto (\square, d_1) \mapsto (\square, d_2) \mapsto \dots$$

для неограниченно возрастающей последовательности чисел d_1, d_2, \dots

Содержательное прочтение формулы: «в любом вычислении автомата становится верным $x > 1$, и до тех пор верно $x \leq 1$ »

Согласно прочтению формулы и согласно семантике **U**, верно $\mathcal{A} \models \varphi$

Если в семантике **U** записать « Φ » вместо « $\Phi \vee \Psi$ », то формула не будет выполняться на \mathcal{A} :

- ▶ «становится верным $x > 1$ »: выберем какую-либо конфигурацию со значением d часов x , где $d > 1$
- ▶ этой конфигурации в вычислении предшествуют порождённые конфигурации со значениями x из $(1, d)$, и для этих значений не выполняется неравенство $x \leq 1$

TCTL

В *расширенном* синтаксисе tctl-формул могут встречаться и другие привычные логические связки и темпоральные операторы:

▶ $\varphi \vee \psi = \neg(\neg\varphi \& \neg\psi)$

▶ $\varphi \rightarrow \psi = \neg\varphi \vee \psi$

▶ $\mathbf{F}\varphi = \mathbf{t}\mathbf{U}\varphi$

▶ $\mathbf{AG}\varphi = \neg\mathbf{EF}\neg\varphi$

▶ $\mathbf{EG}\varphi = \neg\mathbf{AF}\neg\varphi$

Содержательная трактовка операторов **F** и **G** тоже привычна с поправкой на реальное время:

▶ **F** φ : в **реальном** будущем рано или поздно станет верным φ

▶ **G** φ : всегда в **реально** будущем будет верно φ

TCTL

Примеры tctl-формул напоследок:

- ▶ Как бы ни работал компьютер (*в реальном времени*), если он включен, то есть возможность его выключить

$$\mathbf{AG}(on \rightarrow \mathbf{EF}\neg on)$$

- ▶ Задача не может выполняться больше минуты (x — часы, в которых отмеряется реальное время выполнения задачи в минутах)

$$\mathbf{AG}(executing \rightarrow (x \leq 1))$$

- ▶ Если послан запрос, то неотвратимо не более чем за 5 минут на него будет получен отклик (x — часы, в которых отмеряется реальное время с отсылки запроса в минутах)

$$\mathbf{AG}(request \rightarrow \mathbf{AF}(response \ \&(x \leq 5)))$$

- ▶ Существует вычисление СРВ, в котором действия, выполнение которых сопровождается сбросом часов x , выполняются не реже чем раз в 5 единиц времени

$$\mathbf{EG}(x \leq 5)$$

Задача model checking для TCTL (MC-TCTL)

Для заданного корректного временного автомата \mathcal{A}
и заданной tctl-формулы
над теми же множествами атомарных высказываний и часов
проверить справедливость соотношения

$$\mathcal{A} \models \varphi$$