

# Математические методы верификации схем и программ

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

## Блок 29

CTL\*  
CTL и LTL как фрагменты CTL\*  
Сравнение выразительности CTL и LTL

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

ВМК МГУ, 2023/2024, осенний семестр

## Вступление

БНФ для ctl-формул ( $\Phi$ ) и ltl-формул ( $\varphi$ ) устроены так:

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

$$\chi ::= (\mathbf{X}\Phi) \mid (\Phi \mathbf{U}\Phi)$$

$$\varphi ::= \top \mid p \mid (\varphi \& \varphi) \mid (\neg \varphi) \mid (\mathbf{X}\varphi) \mid (\varphi \mathbf{U}\varphi)$$

В языке CTL использование темпоральных операторов ограничивается так, чтобы каждый оператор ( $\mathbf{U}$ ,  $\mathbf{X}$ ) обязательно был предварён квантором пути ( $\mathbf{A}$ ,  $\mathbf{E}$ )

В LTL можно произвольно комбинировать темпоральные операторы, но использование кванторов пути крайне ограничено:

- ▶ В синтаксисе этих кванторов нет
- ▶ В задаче model checking неявно предполагается квантор  $\mathbf{A}$  в качестве внешней операции формулы:

$$M \models \varphi \Leftrightarrow \text{любое вычисление } M \text{ удовлетворяет формуле } \varphi$$

**А насколько сильно отличаются выразительные возможности этих двух языков?**

## CTL\*

$$\begin{aligned}\Phi & ::= \top \mid p \mid (\Phi \& \Phi) \mid (\neg\Phi) \mid (\mathbf{A}\chi) \mid (\mathbf{E}\chi), \\ \chi & ::= (\mathbf{X}\Phi) \mid (\Phi\mathbf{U}\Phi)\end{aligned}$$

$$\varphi ::= \top \mid p \mid (\varphi \& \varphi) \mid (\neg\varphi) \mid (\mathbf{X}\varphi) \mid (\varphi\mathbf{U}\varphi)$$

Язык CTL\* — это расширение языка CTL, в котором в качестве формул пути ( $\chi$ ) разрешены произвольные ltl-формулы

Синтаксис ctl\*-формул задаётся следующей БНФ:

$$\begin{aligned}\Phi & ::= \top \mid p \mid (\Phi \& \Phi) \mid (\neg\Phi) \mid (\mathbf{A}\varphi) \mid (\mathbf{E}\varphi), \\ \varphi & ::= \Phi \mid \varphi \& \varphi \mid \neg\varphi \mid (\mathbf{X}\varphi) \mid (\varphi\mathbf{U}\varphi),\end{aligned}$$

где  $\Phi$  — формула состояния (она же ctl\*-формула) и  $\varphi$  — формула пути

Для ctl\*-формул и их подформул, как и для ctl-формул, определяются два вида выполнимости:

- ▶ Выполнимость ctl\*-формулы  $\Phi$  в состоянии  $s$  модели Крипке  $M$  ( $M, s \models \Phi$ )
  - ▶ Эта часть семантики дословно переносится из языка CTL
- ▶ Выполнимость формулы пути  $\varphi$  на бесконечном пути  $\pi$  модели Крипке  $M$  ( $M, \pi \models \varphi$ )

# CTL\*

Выполнимость формулы пути на бесконечном пути  $\pi$  модели Крипке  $M$  в CTL\* задаётся почти так же, как и для LTL:

- ▶  $M, \pi \models \Phi$  для ctl\*-формулы  $\Phi \Leftrightarrow M, \pi[1] \models \Phi$
- ▶  $M, \pi \models \varphi_1 \& \varphi_2 \Leftrightarrow M, \pi \models \varphi_1$  и  $M, \pi \models \varphi_2$
- ▶  $M, \pi \models \neg\varphi \Leftrightarrow M, \pi \not\models \varphi$
- ▶  $M, \pi \models \mathbf{X}\varphi \Leftrightarrow M, \pi^{\geq 2} \models \varphi$
- ▶  $M, \pi \models \varphi_1 \mathbf{U}\varphi_2 \Leftrightarrow$  существует момент времени  $k$ , такой что
  - ▶  $M, \pi^{\geq k} \models \varphi_2$  и
  - ▶ для любого момента времени  $i, i < k$ , верно  $M, \pi^{\geq i} \models \varphi_1$

CTL\*-формула  $\varphi$  выполняется на модели  $M$  ( $M \models \varphi$ ), если она выполняется в каждом начальном состоянии этой модели

Задача model checking для CTL\* (MC-CTL\*) формулируется так:

**Для заданной модели Крипке  $M$  и заданной ctl\*-формулы  $\varphi$  проверить справедливость соотношения  $M \models \varphi$**

## CTL и LTL как фрагменты CTL\*

Из устройства семантических правил в языке CTL и для ctl-формулы как фрагмента языка CTL\* немедленно вытекают следующие утверждения

**Утверждение.** Для любых модели Крипке  $M$ , её состояния  $s$  и ctl-формулы  $\varphi$  верно:

$$M, s \models \varphi \text{ в языке CTL} \quad \Leftrightarrow \quad M, s \models \varphi \text{ в языке CTL}^*$$

**Утверждение.** Для любой модели Крипке  $M$  и любой ctl-формулы  $\varphi$  верно:

$$M \models \varphi \text{ в языке CTL} \quad \Leftrightarrow \quad M \models \varphi \text{ в языке CTL}^*$$

Таким образом, любая ctl-формула может расцениваться как ctl\*-формула частного вида

## CTL и LTL как фрагменты CTL\*

Из устройства семантических правил в языках LTL и CTL\* немедленно вытекают следующие утверждения

**Утверждение.** Для любых модели Крипке  $M$  и её пути  $\pi$ , трассы  $\tau$  этого пути и любой ltl-формулы  $\varphi$  верно:

$$\tau \models \varphi \text{ в языке LTL} \quad \Leftrightarrow \quad M, \pi \models \varphi \text{ в языке CTL}^*$$

**Утверждение.** Для любых модели крипке  $M$  и ltl-формулы  $\varphi$  верно:

$$M \models \varphi \text{ в языке LTL} \quad \Leftrightarrow \quad M \models \mathbf{A}\varphi \text{ в языке CTL}^*$$

Таким образом, любая ltl-формула  $\varphi$  может расцениваться как формула  $\mathbf{A}\varphi$  языка CTL\* с тем же смыслом

# Сравнение выразительности CTL и LTL

Теперь CTL и LTL можно полноценно рассматривать как фрагменты «объемлющего» языка CTL\*, а значит, можно сравнивать широту возможностей выражения тех или иных свойств моделей на этих языках

CTL\*-формулы  $\varphi$  и  $\psi$  будем называть **эквивалентными** ( $\varphi \sim \psi$ ), если для любой модели Крипке  $M$  и любого состояния  $s$  справедлива равносильность

$$M, s \models \varphi \quad \Leftrightarrow \quad M, s \models \psi$$

Для фрагментов  $\mathcal{L}_1, \mathcal{L}_2$  языка CTL\* будем говорить, что

- ▶  $\mathcal{L}_1$  **не менее выразителен**, чем  $\mathcal{L}_2$  ( $\mathcal{L}_1 \preceq \mathcal{L}_2$ ), если для любой формулы из  $\mathcal{L}_1$  существует эквивалентная формула из  $\mathcal{L}_2$
- ▶  $\mathcal{L}_1$  и  $\mathcal{L}_2$  **эквивалентны** ( $\mathcal{L}_1 \sim \mathcal{L}_2$ ), если  $\mathcal{L}_1 \preceq \mathcal{L}_2$  и  $\mathcal{L}_2 \preceq \mathcal{L}_1$
- ▶  $\mathcal{L}_1$  **строго менее выразителен**, чем  $\mathcal{L}_2$  ( $\mathcal{L}_1 \prec \mathcal{L}_2$ ), если  $\mathcal{L}_1 \preceq \mathcal{L}_2$  и  $\mathcal{L}_1 \not\sim \mathcal{L}_2$
- ▶  $\mathcal{L}_1$  и  $\mathcal{L}_2$  **несравнимы** ( $\mathcal{L}_1 \perp \mathcal{L}_2$ ), если  $\mathcal{L}_1 \not\preceq \mathcal{L}_2$  и  $\mathcal{L}_2 \not\preceq \mathcal{L}_1$

# Сравнение выразительности CTL и LTL

**Утверждение.** Не существует ctl-формулы, эквивалентной формуле  $AFGp$ , где  $p$  — атомарное высказывание

**Утверждение.** Не существует ltl-формулы  $\varphi$ , такой что формула  $A\varphi$  эквивалентна формуле  $AGEFp$ , где  $p$  — атомарное высказывание

**Утверждение.** Не существует ни ctl-формулы, ни формулы вида  $A\varphi$ , где  $\varphi$  — ltl-формула, эквивалентной формуле  $AFGp \vee AGEFp$ , где  $p$  — атомарное высказывание

Доказать эти утверждения можете попробовать самостоятельно (и каждое из этих утверждений трудно)

**Следствие.** Справедливы следующие соотношения:

- ▶  $CTL \perp LTL$
- ▶  $CTL \cup LTL \prec CTL^*$