

# Математические методы верификации схем и программ

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

## Блок 9

Логика линейного времени (LTL)

Постановка задачи верификации  
моделей Крипке относительно LTL

Лектор:

Подымов Владислав Васильевич

E-mail:

**valdus@yandex.ru**

# Напоминание



Для **моделей Крипке** обсудили «лобовой» теоретико-множественный способ задания спецификаций в виде **свойств трасс**

А на каком языке можно было бы удобно записывать такие свойства?

# Пара слов о логике высказываний

Самый простой логический язык записи спецификаций, в сравнении с которым можно объяснять устройство других языков — это язык **логики высказываний**

Синтаксис **формул логики высказываний** над множеством **атомарных высказываний** AP можно задать следующей БНФ:

$$\varphi ::= \text{т} \mid p \mid (\varphi \& \varphi) \mid (\neg \varphi),$$

где  $p \in AP$  и  $\varphi$  — формула

**Приоритеты операций**, согласно которым можно опускать скобки, по убыванию:  $\neg$ ;  $\&$

Операции  $\&$  и  $\neg$  имеют естественный содержательный смысл: связки «и» и «не» в предложениях

# Пара слов о логике высказываний

Другие «обычные» операции могут быть выражены через  $\&$  и  $\neg$  — например,

- ▶  $\psi_1 \vee \psi_2 = \neg(\neg\psi_1 \& \psi_2)$ 
  - ▶ Содержательный смысл: союз «или» в неисключающем смысле
  - ▶ Приоритет операции  $\vee$  ниже, чем у  $\&$
  
- ▶  $\psi_1 \rightarrow \psi_2 = \neg\psi_1 \vee \psi_2$ 
  - ▶ Содержательный смысл: «если-то»
  - ▶ Приоритет операции  $\rightarrow$  ниже, чем у  $\vee$

В «ленивом» способе повествования, которого будем придерживаться и в этом курсе, в синтаксисе, семантике и обоснованиях вводится и анализируется «укороченный» синтаксис, но при этом в рассуждениях и примерах в качестве сокращений используется «расширенный» набор операций

## Пара слов о логике высказываний

Формула  $\varphi$  выполняется в интерпретации  $\mathcal{I} : AP \rightarrow \{\mathfrak{t}, \mathfrak{f}\}$  ( $\mathcal{I} \models \varphi$ ) в следующих случаях:

- ▶ Соотношение  $\mathcal{I} \models \mathfrak{t}$  выполняется всегда
- ▶  $\mathcal{I} \models p \Leftrightarrow \mathcal{I}(p) = \mathfrak{t}$
- ▶  $\mathcal{I} \models (\psi_1 \& \psi_2) \Leftrightarrow \mathcal{I} \models \psi_1$  и  $\mathcal{I} \models \psi_2$
- ▶  $\mathcal{I} \models (\neg\varphi) \Leftrightarrow \mathcal{I} \not\models \varphi$

**Например**, для интерпретации  $\mathcal{I}$ , такой что  $\mathcal{I}(x) = \mathfrak{t}$  и  $\mathcal{I}(y) = \mathfrak{f}$ , верно следующее:

- ▶  $\mathcal{I} \models x$
- ▶  $\mathcal{I} \not\models y$
- ▶  $\mathcal{I} \not\models y$
- ▶  $\mathcal{I} \models (\neg y)$
- ▶  $\mathcal{I} \models (x \& \neg y)$
- ▶  $\mathcal{I} \not\models (x \& y)$

# Темпоральные логики

В **логике высказываний** выполнимость формулы зависит от и определяется для истинностных значений атомарных высказываний

В **темпоральных логиках** значения атомарных высказываний могут меняться с течением **времени**, и выполнимость формулы зависит от выбора рассматриваемого момента времени и от взаимосвязи значений атомарных высказываний в различные моменты времени

Операции темпоральной логики — это, как правило, операции логики высказываний с тем же содержательным смыслом, к которым добавлены специальные **темпоральные операции**, позволяющие рассуждать о взаимосвязи значений высказываний в различные моменты времени

Прежде всего обсудим наиболее известную и популярную логику, предназначенную для записи **свойств трасс**: **логику линейного времени** (LTL)

# Логика линейного времени

«Укороченный» синтаксис **ltl-формул** над множеством **атомарных высказываний** AP задаётся следующей БНФ:

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

где  $p \in AP$  и  $\varphi$  — ltl-формула

Набор операций LTL — то **операции логики высказываний**, к которым добавлены **темпоральные операции**

**Приоритеты операций** по убыванию:  $\neg$  и **X**; затем **U**; затем остальные операции логики с обычными приоритетами

**Моментами времени** дальше будем называть неотрицательные целые числа:  $0, 1, 2, \dots$

Понятие выполнимости формул в LTL уточняется так: формула выполняется или не выполняется (*истинна или ложна*) не «абсолютно», а в те или иные моменты времени

Содержательный смысл операций логики высказываний остаётся тем же

# Логика линейного времени

Темпоральные операции имеют следующий смысл:

- ▶  $X\varphi$ : формула  $\varphi$  выполняется в следующий (относительно рассматриваемого) момент времени
- ▶  $\psi_1 U \psi_2$ : в будущем когда-нибудь выполнится формула  $\psi_2$ , а до тех пор всегда будет выполняться формула  $\psi_1$

В «расширенный» набор операций будем включать также следующие две темпоральные операции:

- ▶  $F\varphi = \top U \varphi$ 
  - ▶ Дословное прочтение: в будущем когда-нибудь выполнится формула  $\varphi$ , а до тех пор всегда будет выполняться  $\top$
  - ▶ Иными словами: в будущем когда-нибудь выполнится  $\varphi$
  - ▶ Приоритет **F** такой же, как и  $\neg$
- ▶  $G\varphi = \neg F \neg \varphi$ 
  - ▶ Дословное прочтение: неверно то, что когда-нибудь в будущем выполнится формула не- $\varphi$
  - ▶ Иными словами: в будущем всегда будет выполняться формула  $\varphi$
  - ▶ Приоритет **G** такой же, как и  $\neg$



# Логика линейного времени

**Примеры** формул, выражающих требования правильности вычислительных систем:

- ▶ Никогда светофоры  $\updownarrow$  и  $\leftrightarrow$  не будут  $\bullet$  одновременно  
$$\neg \mathbf{F}(g_{\updownarrow} \ \& \ g_{\leftrightarrow})$$
- ▶ Когда-нибудь наступит лето, а до тех пор будет холодно  
$$\mathit{cold} \mathbf{U} \mathit{summer}$$
- ▶ Двух подряд плохих дней не бывает:  
$$\mathbf{G}(\mathit{bad\_day} \rightarrow \mathbf{X} \neg \mathit{bad\_day})$$
- ▶ После  $\bullet$  светофор  $\updownarrow$  рано или поздно станет  $\bullet$   
$$\mathbf{G}(r_{\updownarrow} \rightarrow \mathbf{F} g_{\updownarrow})$$
- ▶ Светофор  $\updownarrow$  бесконечно часто бывает  $\bullet$   
$$\mathbf{GF} g_{\updownarrow}$$
- ▶ Мне уготована вечность в раю или в аду  
$$\mathbf{F}(\mathbf{G} \mathit{heaven} \vee \mathbf{G} \mathit{hell})$$

# Логика линейного времени

Роль интерпретаций для ltl-формул выполняют **трассы**: событием  $\tau[i]$  трассы  $\tau$  задаются истинностные значения всех атомарных высказываний в момент времени  $i$

Семантика ltl-формул задаётся **отношением выполнимости** ltl-формулы  $\varphi$  на трассе  $\tau$  ( $\tau \models \varphi$ ):

- ▶ Соотношение  $\tau \models \mathbb{t}$  верно всегда
- ▶  $\tau \models p$ , где  $p \in AP \Leftrightarrow p \in \tau[0]$
- ▶  $\tau \models (\psi_1 \& \psi_2) \Leftrightarrow \tau \models \psi_1$  и  $\tau \models \psi_2$
- ▶  $\tau \models (\neg\varphi) \Leftrightarrow \tau \not\models \varphi$
- ▶  $\tau \models (\mathbf{X}\varphi) \Leftrightarrow \tau^1 \models \varphi$
- ▶  $\tau \models (\psi_1 \mathbf{U} \psi_2) \Leftrightarrow$  существует момент времени  $i$ , такой что
  - ▶  $\tau^i \models \psi_2$  и
  - ▶ для любого момента времени  $j$ , такого что  $j < i$ , верно  $\tau^j \models \psi_1$

Запись  $\tau^m \models \varphi$  можно содержательно трактовать как выполнимость формулы  $\varphi$  на трассе  $\tau$  **в момент времени  $m$**

# Логика линейного времени

**Утверждение (семантика F).** Для любых ltl-формулы  $\varphi$  и трассы  $\tau$  верно:

$$\tau \models \mathbf{F}\varphi \Leftrightarrow \text{существует момент времени } i, \text{ такой что } \tau^i \models \varphi$$

**Утверждение (семантика G).** Для любых ltl-формулы  $\varphi$  и трассы  $\tau$  верно:

$$\tau \models \mathbf{G}\varphi \Leftrightarrow \text{для любого момента времени } i \text{ верно } \tau^i \models \varphi$$

**Доказательство.** Очевидным образом следует из определений **F** и **G** и семантики ltl-формул

# Логика линейного времени

**Утверждение.** Для любых ltl-формулы  $\varphi$  и трассы  $\tau$  верно:  
 $\tau \models \mathbf{GF}\varphi \Leftrightarrow$  для бесконечного числа попарно различных моментов времени  $i$  верно  $\tau^i \models \varphi$

**Доказательство.** Перепишем это утверждение «негативно»:

$\tau \not\models \mathbf{GF}\varphi \Leftrightarrow$  для не более чем конечного числа моментов времени  $i$  верно  $\tau^i \models \varphi$

( $\Rightarrow$ ) Пусть  $\tau \not\models \mathbf{GF}\varphi$

По семантике **F** и **G**, верно следующее: существует момент времени  $k$ , такой что для любого момента времени  $m$  верно  $\tau^{k+m} \not\models \varphi$

Значит, соотношение  $\tau^i \models \varphi$  выполняется только для  $i < k$ , то есть для не более чем  $k$  моментов времени

( $\Leftarrow$ ) Пусть соотношение  $\tau^i \models \varphi$  выполняется для не более чем конечного числа моментов времени  $i$

Рассмотрим наибольший момент времени  $k$ , такой что  $\tau^k \models \varphi$

Тогда для момента  $k' = k + 1$  верно следующее: для любого момента  $m$  верно  $\tau^{k'+m} \not\models \varphi$

По семантике **F** и **G**, это означает, что  $\tau \not\models \mathbf{GF}\varphi \blacktriangledown$

# Логика линейного времени

Будем говорить, что формула выполняется **почти всегда** (более широко — нечто справедливо почти всегда), если она выполняется во все моменты времени, кроме, быть может, некоторого конечного числа моментов

**Утверждение.** Для любых **ltl**-формулы  $\varphi$  и трассы  $\tau$  верно:

$\tau \models \mathbf{FG}\varphi \Leftrightarrow$  формула  $\varphi$  выполняется на  $\tau$  почти всегда

**Доказательство.**

( $\Rightarrow$ ) Пусть  $\tau \models \mathbf{FG}\varphi$

По семантике **F** и **G**, существует момент времени  $k$ , такой что для любого момента времени  $m$  верно  $\tau^{k+m} \models \varphi$

Следовательно,  $\varphi$  выполняется на  $\tau$  во все моменты времени, кроме, быть может,  $\{0, 1, \dots, k-1\}$

( $\Leftarrow$ ) Пусть формула  $\varphi$  выполняется на  $\tau$  почти всегда

Рассмотрим наибольший момент времени  $k$ , такой что  $\tau^k \not\models \varphi$

Тогда для момента времени  $k' = k + 1$  и любого момента времени  $m$  верно  $\tau^{k'+m} \models \varphi$

По семантике **F** и **G**, это означает, что  $\tau \models \mathbf{FG}\varphi \blacktriangledown$

## Задача model checking относительно LTL

В блоке 8 для модели Крипке  $M$  и свойства трасс  $P$  было введено обозначение  $M \models P$  того, что модель  $M$  удовлетворяет свойству  $P$

Ltl-формула  $\varphi$  может восприниматься как способ представления свойства трасс  $\text{Tr}(\varphi) = \{\tau \mid \tau \in \text{Tr}, \tau \models \varphi\}$

Ltl-формула  $\varphi$  выполняется на модели  $M$  ( $M \models \varphi$ ), если справедливо включение  $\text{Tr}(M) \subseteq \text{Tr}(\varphi)$

*Небольшое пояснение:*

- ▶ Ltl-формула делит все трассы на хорошие (на которых формула выполняется) и плохие (на которых формула не выполняется)
- ▶ Соотношение  $M \models P$  означает, что все трассы модели  $M$  хорошие (т.е. что в модели  $M$  нет ни одной плохой трассы)

Задача model checking для LTL (MC-LTL) формулируется так:

Для заданной модели Крипке  $M$  и заданной ltl-формулы  $\varphi$   
проверить справедливость соотношения

$$M \models \varphi$$