

Математические методы верификации схем и программ

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

Блок 12

Логика линейного времени (LTL)

Постановка задачи верификации
моделей Крипке относительно LTL

Лектор:

Подымов Владислав Васильевич

E-mail:

valdus@yandex.ru

ВМК МГУ, 2023/2024, осенний семестр

Напоминание



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

Но свойство трасс — это множество, состоящее из бесконечных последовательностей и являющееся в общем случае бесконечным

Для эффективного использования таких свойств необходимо иметь удобный язык их представления

Пара слов о логике высказываний

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

Иногда для языков предлагаются два варианта синтаксиса:

- ▶ **Полный** с широким спектром синтаксических конструкций «на все случаи жизни»
- ▶ **Краткий** с небольшим набором синтаксических конструкций и способом выражения остальных через него

Будем придерживаться «ленивого» способа изложения языков:

- ▶ Строго вводится краткий синтаксис с семантикой
- ▶ Остальные конструкции полного синтаксиса вводятся как сокращения
- ▶ Смысл всех конструкций содержательно поясняется
- ▶ В примерах, иллюстрациях, выкладках и т.п. используется полный синтаксис согласно содержательным пояснениям
- ▶ В обоснованиях по желанию используется краткий синтаксис

Пара слов о логике высказываний

БНФ, задающая краткий синтаксис **формул логики высказываний** над множеством **атомарных высказываний** AP:

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

где $p \in \text{AP}$ и φ — формула

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

Другие операции полного синтаксиса:

- ▶ $\text{f} = \neg \text{т}$
- ▶ $\psi_1 \vee \psi_2 = \neg((\neg \psi_1) \& (\neg \psi_2))$
 - ▶ Содержательный смысл: союз «или» в неисключающем смысле
- ▶ $\psi_1 \rightarrow \psi_2 = (\neg \psi_1) \vee \psi_2$
 - ▶ Содержательный смысл: «если-то»

Приоритеты операций по убыванию: \neg ; $\&$; \vee ; \rightarrow

Скобки в формулах нередко опускаются

согласно приоритетам и согласно ассоциативности операций $\&$ и \vee

Пара слов о логике высказываний

Правила, задающие **выполнимость** формулы φ в **интерпретации** $\mathcal{I} : AP \rightarrow \{\mathfrak{t}, \mathfrak{f}\}$ ($\mathcal{I} \models \varphi$):

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

Например,

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

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

Темпоральные логики

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

В **темпоральных логиках** учитывается изменение значений атомарных высказываний 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, как правило, делятся на

- ▶ операции ЛВ с тем же содержательным смыслом, что и в ЛВ, и
- ▶ **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 (LTL)

БНФ, задающая краткий синтаксис **ltl-формул** над множеством **атомарных высказываний** AP:

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

где $p \in AP$ и φ — ltl-формула

Моментами времени дальше будем называть натуральные числа (**\mathbb{N}**): 1, 2, 3, ...

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

X и **U** — это темпоральные операции со следующим содержательным смыслом:

- ▶ **X** φ : φ будет выполнено в следующий момент времени (*относительно рассматриваемого момента*)
- ▶ $\psi_1 \mathbf{U} \psi_2$: в будущем когда-нибудь выполнится ψ_2 , а до тех пор всегда будет выполняться ψ_1

Логика линейного времени (LTL)

Другие операции полного синтаксиса:

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

- ▶ Дословное прочтение: в будущем когда-нибудь выполнится φ , а до тех пор всегда будет выполняться \mathbf{t}
- ▶ Иными словами: в будущем когда-нибудь выполнится φ

▶ $\mathbf{G}\varphi = \neg(\mathbf{F}(\neg\varphi))$

- ▶ Дословное прочтение:
неверно то, что когда-нибудь в будущем выполнится формула не- φ
- ▶ Иными словами: в будущем всегда будет выполняться формула φ

Приоритеты операций по убыванию:

\neg , **F**, **G** и **X**;

затем **U**;

затем остальные операции с обычными приоритетами

Логика линейного времени (LTL)

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

$$cold \mathbf{U} summer$$

- ▶ Двух подряд плохих дней не бывает:

$$\mathbf{G}(bad_day \rightarrow \mathbf{X} \neg bad_day)$$

- ▶ 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

$$\mathbf{F}(\mathbf{G}heaven \vee \mathbf{G}hell)$$

Логика линейного времени (LTL)

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

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

- ▶ Соотношение $\tau \models \text{tt}$ верно всегда
- ▶ $\tau \models p$, где $p \in AP \iff p \in \tau[1]$
- ▶ $\tau \models (\psi_1 \& \psi_2) \iff \tau \models \psi_1 \text{ и } \tau \models \psi_2$
- ▶ $\tau \models (\neg\varphi) \iff \tau \not\models \varphi$
- ▶ $\tau \models (\mathbf{X}\varphi) \iff \tau^{\geq 2} \models \varphi$
- ▶ $\tau \models (\psi_1 \mathbf{U} \psi_2) \iff$ существует момент времени i , такой что
 - ▶ $\tau^{\geq i} \models \psi_2$ и
 - ▶ для любого момента времени j , такого что $j < i$, верно $\tau^{\geq j} \models \psi_1$

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

Логика линейного времени (LTL)

Утверждение (семантика F)

Для любых ltl-формулы φ и трассы τ верно:

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

Утверждение (семантика G)

Для любых ltl-формулы φ и трассы τ верно:

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

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

Логика линейного времени (LTL)

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

Доказательство. Перепишем это утверждение «негативно»:
 $\tau \not\models \mathbf{GF}\varphi \Leftrightarrow$ для не более чем конечного числа моментов времени i верно $\tau^{\geq i} \models \varphi$

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

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

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

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

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

Тогда для любого момента k' , такого что $k' \geq k + 1$, верно $\tau^{\geq k'} \not\models \varphi$

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

Логика линейного времени (LTL)

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 φ и трассы τ верно:
**формула φ почти всегда выполняется на $\tau \Leftrightarrow$
существует момент времени k , такой что
 φ выполняется на τ во все моменты, не меньшие k**

Доказательство.

(\Rightarrow) Пусть φ почти всегда выполняется на τ

Тогда множество $X = \{i \mid i \in \mathbb{N}, \tau^{\geq i} \not\models \varphi\}$ конечно

Пусть k — наибольший момент из X

Тогда φ выполняется на τ во все моменты, не меньшие $k + 1$

(\Leftarrow) Пусть существует момент k , такой что

для всех моментов k' , не меньших k , верно $\tau^{\geq k'} \models \varphi$

Тогда множество $X = \{i \mid i \in \mathbb{N}, \tau^{\geq i} \not\models \varphi\}$ включено в $\{1, 2, \dots, k - 1\}$

Следовательно, множество X конечно ▼

Логика линейного времени (LTL)

Утверждение. Для любых ltl-формулы φ и трассы τ верно:
 $\tau \models \mathbf{FG}\varphi \Leftrightarrow$ формула φ выполняется на τ почти всегда

Доказательство.

По предыдущему утверждению,
 φ выполняется на τ почти всегда \Leftrightarrow
существует момент k , такой что
для любого момента k' , не меньшего k , верно $\tau^{\geq k} \models \varphi$

По семантике **F** и **G**, последнее соотношение равносильно $\tau \models \mathbf{FG}\varphi$ ▼

Задача model checking относительно LTL

В блоке 11 для модели Крипке M и свойства трасс P было введено обозначение $M \models P$ того, что модель M удовлетворяет свойству P

Ltl-формула φ может восприниматься как

способ представления свойства трасс $\text{Tr}(\varphi) = \{\tau \mid \tau \in \text{Tr}, \tau \models \varphi\}$

Ltl-формула φ 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 $M \models \varphi$ 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 φ
проверить справедливость соотношения**

$$M \models \varphi$$