# Математическая логика и логическое программирование

mk.cs.msu.ru → Лекционные курсы
→ Математическая логика и логическое программирование (3-й поток)

Блок 58

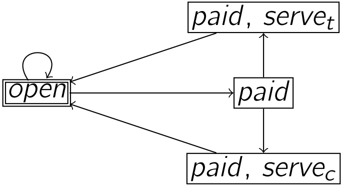
Алгоритм model checking для CTL

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

ВМК МГУ, 2022/2023, осенний семестр

# Напоминание

Система переходов $M$ над множеством атомарных высказываний AP:




Примеры CTL-формул $\varphi$ над тем же множеством AP:

$$open \,\&\, \neg paid \,\&\, \neg serve_t \,\&\, \neg serve_c$$
$$\neg \mathbf{EF}(\neg paid \,\&(serve_c \vee serve_t))$$
$$\mathbf{AG}(paid \to \mathbf{AF}(serve_c \vee serve_t))$$
$$\mathbf{EF}(paid \,\&\, \mathbf{EG}\neg serve_t)$$
$$\mathbf{AG}(\neg paid \to \mathbf{AX}(paid \to \mathbf{EF} serve_t))$$

$M \models \varphi \Leftrightarrow$

формула $\varphi$ выполняется в каждом начальном состоянии системы $M$

# Алгоритм model checking для CTL

Алгоритм проверки соотношения $M \models \varphi$ для СП $M$ и CTL-формулы $\varphi$ будет излагаться «сверху вниз»: от общей схемы (главной процедуры) к деталям реализации этой схемы (остальным процедурам)

По ходу изложения будет приводиться
обоснование корректности (правильности) каждой процедуры

«Описание алгоритма
\+ обоснование корректности
\+ оценка сложности» —
типичное сочетание в «умном» изложении алгоритмов, позволяющее

- понять, как это реализовать,
- убедиться, что это действительно работает правильно, и
- оценить, достаточно ли эффективно решение для желаемых целей

Но оценку сложности приводить не будем,
чтобы не перегружать рассказ излишними деталями

# Алгоритм model checking для CTL

$Sat(M, \psi)$ — так будем обозначать множество состояний СП $M$, в которых выполняется формула $\psi$: $Sat(M, \psi) = \{s \mid s \in S,\ M, s \models \psi\}$

**Лемма. Для любых СП $M = (S, S_0, \mapsto, L)$ и CTL-формулы $\varphi$ верно:**

$$M \models \varphi \quad \Leftrightarrow \quad S_0 \subseteq Sat(M, \varphi)$$

Доказательство. Напрямую следует из определений соотношения $M \models \varphi$ и множества $Sat(M, \varphi)$ ▼

**Главная процедура**

*Дано:* конечная СП $M$; CTL-формула $\varphi$

*Результат:* ответ на вопрос «$M \models \varphi$?»

*Тело процедуры:*

1. Вычислить множество $X = \Pi_{sat}(M, \varphi) = Sat(M, \varphi)$
2. Проверить соотношение $S_0 \subseteq X$
3. Вернуть результат проверки пункта 2

# Алгоритм model checking для CTL

CTL-формулы $\psi_1$ и $\psi_2$ назовём равносильными ($\psi_1 \sim \psi_2$), если для любой СП $M$ верно $Sat(M, \psi_1) = Sat(M, \psi_2)$

CTL-формулу $\varphi$ назовём упрощённой, если она задаётся БНФ

$$\varphi \ ::= \ \mathbb{t} \ \mid \ p \ \mid \ (\varphi \,\&\, \varphi) \ \mid \ (\neg\varphi) \ \mid \ (\mathbf{EX}\varphi) \ \mid \ (\mathbf{EG}\varphi) \ \mid \ (\mathbf{E}(\varphi \mathbf{U} \varphi))$$

**Процедура** $\Pi_{sat}(M, \varphi)$

*Дано:* конечная СП $M$; CTL-формула $\varphi$

*Результат:* $Sat(M, \varphi)$

*Тело процедуры:*

1. Построить упрощённую формулу $\psi$, равносильную исходной:
$$\psi = Simplify(\varphi)$$
2. Вернуть множество $Sat(M, \psi)$ для упрощённой формулы:
$$\Pi^s_{sat}(M, \psi)$$

# Алгоритм model checking для CTL

**Лемма (о равносильностях в CTL).** **Для любых CTL-формул $\varphi$ и $\psi$ справедливы следующие равносильности:**

- $\varphi \to \psi \sim \neg\varphi \vee \psi$
- $\varphi \vee \psi \sim \neg(\neg\varphi \,\&\, \neg\psi)$
- $\mathbf{AX}\varphi \sim \neg\mathbf{EX}\neg\varphi$
- $\mathbf{AF}\varphi \sim \neg\mathbf{EG}\neg\varphi$
- $\mathbf{AG}\varphi \sim \neg\mathbf{EF}\neg\varphi$
- $\mathbf{EF}\varphi \sim \mathbf{E}(\mathbb{t}\mathbf{U}\varphi)$
- $\mathbf{A}(\varphi\mathbf{U}\psi) \sim \neg\mathbf{E}(\neg\psi\mathbf{U}(\neg\varphi \,\&\, \neg\psi)) \,\&\, \neg\mathbf{EG}\neg\psi$

# Лемма о равносильностях в CTL

Доказательство. $\varphi \ ::= \ \mathbb{t} \ | \ p \ | \ \varphi \,\&\, \varphi \ | \ \neg\varphi \ | \ \mathbf{EX}\varphi \ | \ \mathbf{EG}\varphi \ | \ \mathbf{E}(\varphi\mathbf{U}\varphi)$

$\varphi \to \psi \sim \neg\varphi \vee \psi$ и $\varphi \vee \psi \sim \neg(\neg\varphi \,\&\, \neg\psi)$ — так же как и в логиках высказываний и предикатов

$\mathbf{AX}\varphi \sim \neg\mathbf{EX}\neg\varphi$: покажем, что для любых СП $M = (S, S_0, \mapsto, L)$ и её состояния $s$ верно $M, s \models \mathbf{AX}\varphi \quad \Leftrightarrow \quad M, s \models \neg\mathbf{EX}\neg\varphi$

Верно $M, s \models \mathbf{AX}\varphi$

$\Leftrightarrow$ (по семантике комбинации **AX**)

Для любого состояния $s'$, такого что $s \mapsto s'$, верно $M, s' \models \varphi$

$\Leftrightarrow$ (т.к. $\forall \mathrm{x}\ (A \to B) \sim \neg\exists \mathrm{x}\ (A \,\&\, \neg B)$)

Не существует состояние $s''$, такое что $s \mapsto s''$ и неверно $M, s' \models \varphi$

$\Leftrightarrow$ (по семантике $\neg$)

Не существует состояние $s''$, такое что $s \mapsto s''$ и верно $M, s'' \models \neg\varphi$

$\Leftrightarrow$ (по семантике комбинации **EX**)

Неверно $M, s \models \mathbf{EX}\neg\varphi$

$\Leftrightarrow$ (по семантике $\neg$)

Верно $M, s \models \neg\mathbf{EX}\neg\varphi$

# Лемма о равносильностях в CTL

Доказательство. $\varphi ::= \mathbb{t} \mid p \mid \varphi \,\&\, \varphi \mid \neg\varphi \mid \mathbf{EX}\varphi \mid \mathbf{EG}\varphi \mid \mathbf{E}(\varphi\mathbf{U}\varphi)$

$\mathbf{AF}\varphi \sim \neg\mathbf{EG}\neg\varphi$ и $\mathbf{AG}\varphi \sim \neg\mathbf{EF}\neg\varphi$ — аналогично

$\mathbf{EF}\varphi \sim \mathbf{E}(\mathbb{t}\mathbf{U}\varphi)$ — очевидно следует
из семантики комбинаций **EF** и **EU** и формулы $\mathbb{t}$

$\mathbf{A}(\varphi\mathbf{U}\psi) \sim \neg\mathbf{E}(\neg\psi\mathbf{U}(\neg\varphi \,\&\, \neg\psi)) \,\&\, \neg\mathbf{EG}\neg\psi$:

$M, s \models \mathbf{A}(\varphi\mathbf{U}\psi)$

$\Leftrightarrow$ (по семантике комбинации **AU**)

$\forall$ пути $\pi$ из $s$ в $M$ $\exists i$: $M, \pi[i] \models \psi$ и $\forall j < i$ верно $M, \pi[j] \models \varphi$

$\Leftrightarrow$ (по двойственности $\forall$-$\exists$ и $\&$-$\vee$)

Не $\exists$ путь $\pi$ из $s$ в $M$: $\forall i$ верно $(M, \pi[i] \not\models \psi$ или $\exists j < i$: $M, \pi[j] \not\models \varphi)$

$\Leftrightarrow$ (*применяем метод пристального взгляда*)

1. Не $\exists$ путь $\pi$ из $s$ в $M$ и номер $i$:
   $M, \pi[i] \not\models \varphi$, $M, \pi[i] \not\models \psi$ и $\forall j < i$ верно $M, \pi[j] \not\models \psi$
   и
2. не $\exists$ путь $\pi$ из $s$ в $M$: $\forall i$ верно $M, \pi[i] \not\models \psi$

$\Leftrightarrow$ (по семантике **E**, **U**, **G**, $\neg$ и $\&$)

$M, s \models \neg\mathbf{E}(\neg\psi\mathbf{U}(\neg\varphi \,\&\, \neg\psi)) \,\&\, \neg\mathbf{EG}\neg\psi$ ▼

# Алгоритм model checking для CTL

**Процедура** *Simplify*$(\varphi)$

*Дано:* CTL-формула $\varphi$

*Результат:* упрощённая CTL-формула $\psi$, такая что $\varphi \sim \psi$

*Тело процедуры:*

1. Пока это возможно, преобразовывать формулу $\varphi$ согласно равносильностям из последней леммы, заменяя подформулу, отвечающую левой части равносильности, на правую часть
2. Вернуть формулу, получившуюся после всех преобразований

Корректность процедуры *Simplify* обеспечивается тем, что

- наряду с последней леммой для CTL справедлива такая же теорема о равносильной замене, как и для логики предикатов, и
- цикл упрощающих преобразований обязательно завершается: если в исходной формуле содержится $n$ подформул, отвечающих левым частям равносильностей, то после не более чем $2n$ преобразований формула обязательно станет упрощённой, и цикл завершится

# Алгоритм model checking для CTL

**Процедура** $\Pi^{s}_{sat}(M, \varphi)$

*Дано:* конечная СП $M = (S, S_0, \mapsto, L)$; упрощённая CTL-формула $\varphi$

*Результат:* $Sat(M, \varphi)$

*Тело процедуры:*

1. Если $\varphi = \mathbb{t}$, то вернуть $S$
2. Если $\varphi = p \in \mathrm{AP}$, то вернуть $\{s \mid s \in S,\ p \in L(s)\}$
3. Если $\varphi = \psi_1 \,\&\, \psi_2$, то вернуть $\Pi^{s}_{sat}(M, \psi_1) \cap \Pi^{s}_{sat}(M, \psi_2)$
4. Если $\varphi = \neg\psi$, то вернуть $S \setminus \Pi^{s}_{sat}(M, \varphi)$
5. Если $\varphi = \mathbf{EX}\psi$, то вернуть $\Pi^{\mathbf{EX}}_{sat}(M, \psi)$
6. Если $\varphi = \mathbf{EG}\psi$, то вернуть $\Pi^{\mathbf{EG}}_{sat}(M, \psi)$
7. Если $\varphi = \mathbf{E}(\psi_1 \mathbf{U} \psi_2)$, то вернуть $\Pi^{\mathbf{EU}}_{sat}(M, \psi_1, \psi_2)$

Корректность этой процедуры для пунктов 1–4 очевидна (обеспечивается семантикой формул)

Осталось предложить подходящие процедуры $\Pi^{\mathbf{EX}}_{sat}$, $\Pi^{\mathbf{EG}}_{sat}$ и $\Pi^{\mathbf{EU}}_{sat}$

# Алгоритм model checking для CTL

$Pre(\Gamma, v)$ — так для графа $\Gamma$ и его вершины $v$ обозначим множество вершин, из которых $v$ достижима по одной дуге:

$$Pre(v) = \{v' \mid (v \mapsto v') \in \Gamma\}$$

$Pre(\Gamma, X)$ — так для графа $\Gamma$ и множества $X$ его вершин обозначим множество вершин, из которых по одной дуге достижима хотя бы одна вершина из $X$: $Pre(\Gamma, V) = \bigcup\limits_{v \in V} Pre(\Gamma, v)$

**Лемма.** **Для любой СП $M$ и любой CTL-формулы $\varphi$ справедливо равенство $Sat(M, \mathbf{EX}\varphi) = Pre(M, Sat(M, \varphi))$**

Доказательство

$s \in Sat(M, \mathbf{EX}\varphi) \quad \Leftrightarrow$ (по определению $Sat$)

$M, s \models \mathbf{EX}\varphi \quad \Leftrightarrow$ (по семантике **E** и **X**)

$\exists$ состояние $s'$: $s \to s'$ и $M, s' \models \varphi \quad \Leftrightarrow$ (по определению $Sat$)

$\exists$ состояние множества $Sat(M, \varphi)$, достижимое из $s$ по одной дуге

$\Leftrightarrow$ (по определению $Pre$)

$s \in Pre(M, Sat(M, \varphi))$ ▼

# Алгоритм model checking для CTL

**Процедура** $\Pi_{sat}^{\mathbf{EX}}(M, \varphi)$

*Дано:* конечная СП $M$; упрощённая CTL-формула $\varphi$

*Результат:* $Sat(M, \mathbf{EX}\varphi)$

*Тело процедуры:*

1. Вычислить $X = \Pi_{sat}^{s}(M, \varphi)$
2. Вернуть множество $Pre(M, X)$

# Алгоритм model checking для CTL

**Лемма.** **Для любой конечной СП $M$ и любых CTL-формул $\varphi_1$, $\varphi_2$ верно следующее:** $s \in Sat(M, \mathbf{E}(\varphi_1 \mathbf{U} \varphi_2)) \Leftrightarrow$
**в $M$ существует путь $s_0 \to \cdots \to s_k$,**
**такой что $s_0 = s$, $s_k \in Sat(M, \varphi_2)$ и $\{s_0, \ldots, s_{k-1}\} \subseteq Sat(M, \varphi_1)$**

Доказательство.

$s \in Sat(M, \mathbf{E}(\varphi_1 \mathbf{U} \varphi_2))$

$\Leftrightarrow$ (по определению $Sat$)

$M, s \models \mathbf{E}(\varphi_1 \mathbf{U} \varphi_2)$

$\Leftrightarrow$ (по определению $\mathbf{E}$ и $\mathbf{U}$)

$\exists$ бесконечный путь $\pi$ из $s$ в $M$ и номер $k$:
$M, \pi[k] \models \varphi_2$ и $\forall i < k$ верно $M, \pi[i] \models \varphi_1$

$\Leftrightarrow$ (переформулировка)

$\exists$ путь $s_0 \mapsto \cdots \mapsto s_k$ в $M$ (префикс пути $\pi$):
$s_0 = s$, $M, s_k \models \varphi_2$ и $\forall i \in \{0, \ldots, k-1\}$ верно $M, s_i \models \varphi_1$

$\Leftrightarrow$ (по определению $Sat$)

$\exists$ путь $s_0 \mapsto \cdots \mapsto s_k$ в $M$:
$s_0 = s$, $s_k \in Sat(M, \varphi_2)$ и $\{s_0, \ldots, s_{k-1}\} \subseteq Sat(M, \varphi_1)$ ▼

# Алгоритм model checking для CTL

**Процедура** $\Pi^{\mathbf{EU}}_{sat}(M, \varphi_1, \varphi_2)$

*Дано:* конечная СП $M$; упрощённые CTL-формулы $\varphi_1$, $\varphi_2$

*Результат:* $Sat(M, \mathbf{E}(\varphi_1 \mathbf{U} \varphi_2))$

*Тело процедуры:*

1. Вычислить $X_0 = \Pi^s_{sat}(M, \varphi_2)$ и $Z = \Pi^s_{sat}(M, \varphi_1)$
2. Последовательно вычислять множества $X_1, X_2, \dots$ по схеме $X_i = X_{i-1} \cup (Pre(M, X_{i-1}) \cap Z)$, пока для очередного $X_i$ не окажется верно $X_i = X_{i-1}$
3. Вернуть последнее вычисленное множество $X_i$

Корректность этой процедуры обосновывается

- последней леммой,
- наблюдением «на грани очевидного» о том, что в множество $X_i$ входят все вершины всех путей вида $s_0 \to \dots \to s_i$, где $s_i \in Sat(M, \varphi_2)$ и $\{s_0, \dots, s_{i-1}\} \subseteq Sat(M, \varphi_1)$, и
- гарантированным равенством $X_i = X_{i-1}$ хотя бы для одного $i$ в связи с конечностью $M$

# Алгоритм model checking для CTL

Вершина $u$ достижима из вершины $v$ в ориентированном графе $\Gamma$, если в $\Gamma$ существует путь из $v$ в $u$ (быть может, тривиальный, если $u = v$)

Ориентированный граф сильно связен,
если любые его две вершины достижимы друг из друга

Компонента сильной связности ориентированного графа — это максимальный по включению вершин и дуг сильно связный подграф этого графа

Компонента сильной связности нетривиальна,
если в ней содержится хотя бы одна дуга

# Алгоритм model checking для CTL

**Лемма.** **В конечном ориентированном графе $\Gamma$ из вершины $s$ исходит хотя бы один бесконечный путь $\Leftrightarrow$ в $\Gamma$ из $s$ достижима хотя бы одна нетривиальная компонента сильной связности**

Доказательство.

($\Leftarrow$) Пусть $\pi$ — путь из $s$, оканчивающийся в вершине $v$ нетривиальной компоненты сильной связности

По выбору $v$, существует путь из $v$ в $v$, содержащий хотя бы две вершины

Пусть $\pi'$ — указанный путь из $v$ в $v$ без первой вершины $v$

Тогда в $\Gamma$ содержится и бесконечный путь, исходящий из $s$:

$$\pi\pi'\pi'\ldots\pi'\ldots$$

($\Rightarrow$) Рассмотрим бесконечный путь $\pi$ в $\Gamma$, исходящий из $s$

Так как граф $\Gamma$ конечен, то в $\pi$ содержится хотя бы одна вершина $v$, встречающаяся хотя бы два раза: $\pi[i] = \pi[i+k] = v$, $k > 0$

Тогда все вершины множества $\{\pi[i+1], \ldots, \pi[i+k]\}$ достижимы друг из друга, то есть входят в некоторую компоненту сильной связности, и эта компонента достижима из $s$ по пути $\pi[0] \to \cdots \to \pi[i]$ ▼

# Алгоритм model checking для CTL

Для ориентированного графа $\Gamma$ и подмножества $V$ его вершин записью $\Gamma|_V$ обозначим подграф графа $\Gamma$, порождённый множеством $V$:

- Множество вершин $\Gamma|_V$ — это $V$
- $(s_1, s_2) \in \Gamma|_V \Leftrightarrow \{s_1, s_2\} \subseteq V$ и $(s_1, s_2) \in \Gamma$
- Если граф $\Gamma$ размечен, то все метки переносятся из $\Gamma$ в $\Gamma|_V$

**Лемма.** **Для любой конечной модели Крипке $M$ и любой ctl-формулы $\varphi$ верно следующее: $s \in Sat(M, \mathbf{EG}\varphi) \Leftrightarrow$ в графе $M|_{Sat(M,\varphi)}$ содержится вершина $s$ и из неё достижима хотя бы одна нетривиальная компонента сильной связности**

Доказательство.

$s \in Sat(M, \mathbf{EG}\varphi) \Leftrightarrow M, s \models \mathbf{EG}\varphi \Leftrightarrow$

в $M$ существует бесконечный путь $\pi$, исходящий из $s$

и такой что $M, \pi[i] \models \varphi$ для каждого момента времени $i \Leftrightarrow$

в $\Gamma = M|_{Sat(M,\varphi)}$ существует бесконечный путь, исходящий из $s \Leftrightarrow$

в $\Gamma$ содержится $s$ и из неё достижима хотя бы одна

нетривиальная компонента сильной связности ▼

# Алгоритм model checking для CTL

**Процедура** $Sat_{\mathbf{EG}}(M, \varphi)$

*Дано:* конечная СП $M$; упрощённая CTL-формула $\varphi$

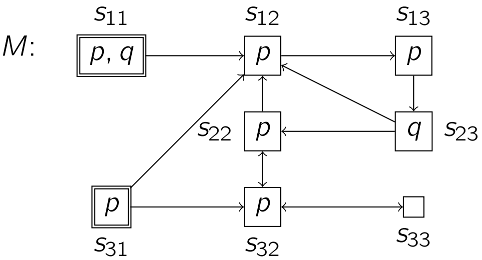
*Результат:* $Sat(M, \mathbf{EG}\varphi)$

*Тело процедуры:*

- Вычислить множество $Z = Sat(M, \varphi)$
- Вычислить граф $\Gamma = M|_Z$
- Каким-либо известным эффективным алгоритмом вычислить множество $X_0$ всех вершин, входящих в какие-либо нетривиальные компоненты сильной связности графа $\Gamma$
- Последовательно вычислять множества $X_1, X_2, \ldots$ по схеме $X_i = X_{i-1} \cup Pre(\Gamma, X_{i-1})$, пока для очередного $X_i$ не окажется верно $X_i = X_{i-1}$
- Вернуть последнее вычисленное множество $X_i$

Корректность этой процедуры обосновывается аналогично корректности $Sat_{\mathbf{EU}}$

# Алгоритм model checking для CTL (пример)




$\varphi = \mathbf{AXA}(p\mathbf{U}q)$

$M \models \varphi?$

$\psi = \mathit{Simplify}(\varphi) = \neg\mathbf{EX}\neg(\neg\mathbf{E}(\neg q\mathbf{U}(\neg q \,\&\, \neg p))\,\&\,\neg\mathbf{EG}\neg q)$

$\Pi^s_{sat}(M, q) = \{s_{11}, s_{23}\}$

$S = \{s_{11}, s_{12}, s_{13}, s_{22}, s_{23}, s_{31}, s_{32}, s_{33}\}$

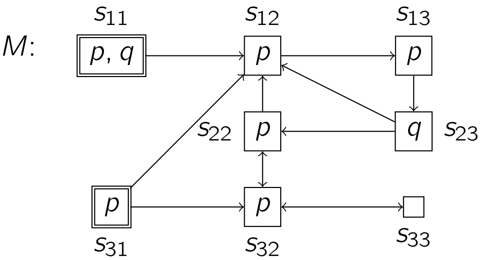
$\Pi^s_{sat}(M, \neg q) = S \setminus \Pi^s_{sat}(M, q) = \{s_{12}, s_{13}, s_{22}, s_{31}, s_{32}, s_{33}\}$

$\Pi^s_{sat}(M, p) = \{s_{11}, s_{12}, s_{13}, s_{22}, s_{31}, s_{32}\}$

$\Pi^s_{sat}(M, \neg p) = S \setminus \Pi^s_{sat}(M, p) = \{s_{23}, s_{33}\}$

$\Pi^s_{sat}(M, \neg q \,\&\, \neg p) = \Pi^s_{sat}(M, \neg q) \cap \Pi^s_{sat}(M, \neg p) = \{s_{33}\}$

# Алгоритм model checking для CTL (пример)




$\varphi = \mathbf{AXA}(p\mathbf{U}q)$

$M \models \varphi?$

$$\psi = Simplify(\varphi) = \neg\mathbf{EX}\neg(\neg\mathbf{E}(\underbrace{\neg q}_{\chi_1}\ \mathbf{U}\ \underbrace{(\neg q \,\&\, \neg p)}_{\chi_2})\,\&\,\neg\mathbf{EG}\neg q)$$

$\Pi^s_{sat}(M, \chi_1) = \{s_{12}, s_{13}, s_{22}, s_{31}, s_{32}, s_{33}\}$

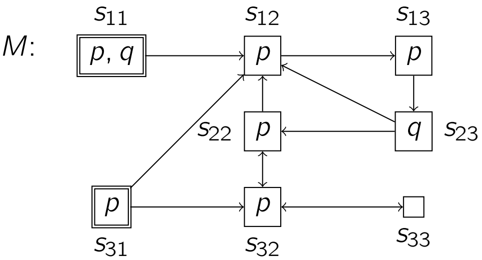
$\Pi^s_{sat}(M, \chi_2) = \{s_{33}\}$

$\Pi^s_{sat}(M, \mathbf{E}(\chi_1\mathbf{U}\chi_2)) = ?$

- $X_0 = \Pi^s_{sat}(M, \psi_2)$, $Z = \Pi^s_{sat}(M, \psi_1)$
- $X_1 = X_0 \cup (Pre(M, X_0) \cap Z) = \{s_{32}, s_{33}\}$
- $X_2 = X_1 \cup (Pre(M, X_1) \cap Z) = \{s_{22}, s_{31}, s_{32}, s_{33}\}$
- $X_3 = X_2 \cup (Pre(M, X_2) \cap Z) = \{s_{22}, s_{31}, s_{32}, s_{33}\} = X_2$

$\Pi^s_{sat}(M, \mathbf{E}(\chi_1\mathbf{U}\chi_2)) = X_3 = \{s_{22}, s_{31}, s_{32}, s_{33}\}$

# Алгоритм model checking для CTL (пример)




$\varphi = \mathbf{AXA}(p\mathbf{U}q)$

$M \models \varphi?$

$\psi = Simplify(\varphi) = \neg\mathbf{EX}\neg(\neg\mathbf{E}(\neg q\mathbf{U}(\neg q \,\&\, \neg p)) \,\&\, \neg\mathbf{EG}\underbrace{\neg q}_{\chi})$

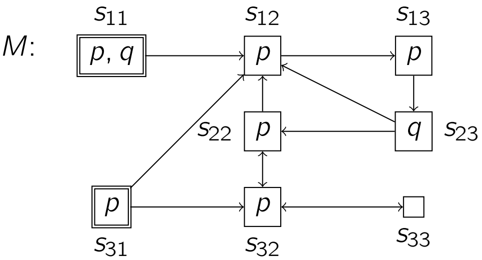
$\Pi^s_{sat}(M, \chi) = \{s_{12}, s_{13}, s_{22}, s_{31}, s_{32}, s_{33}\}$

$\Pi^s_{sat}(M, \mathbf{EG}\chi) = ?$

- $Z = \Pi^s_{sat}(M, \chi)$
- В графе $M|_Z$ содержится ровно одна нетривиальная компонента сильной связности, и её вершины: $X_0 = \{s_{22}, s_{32}, s_{33}\}$
- $X_1 = X_0 \cup Pre(M|_Z, X_0) = \{s_{22}, s_{31}, s_{32}, s_{33}\}$
- $X_2 = X_1 \cup Pre(M|_Z, X_1) = \{s_{22}, s_{31}, s_{32}, s_{33}\} = X_1$

$\Pi^s_{sat}(M, \mathbf{EG}\chi) = X_2 = \{s_{22}, s_{31}, s_{32}, s_{33}\}$

# Алгоритм model checking для CTL (пример)




$\varphi = \mathbf{AXA}(p\mathbf{U}q)$

$M \models \varphi?$

$$\psi = Simplify(\varphi) = \neg\mathbf{EX}\neg(\neg\underbrace{\mathbf{E}(\neg q\mathbf{U}(\neg q \,\&\, \neg p))}_{\chi_1} \,\&\, \neg\underbrace{\mathbf{EG}\neg q}_{\chi_2})$$

$$S = \{s_{11}, s_{12}, s_{13}, s_{22}, s_{23}, s_{31}, s_{32}, s_{33}\}$$

$$\Pi^s_{sat}(M, \chi_1) = \{s_{22}, s_{31}, s_{32}, s_{33}\}$$

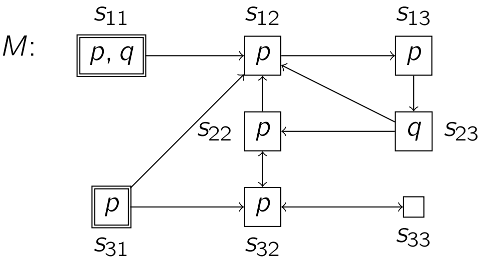
$$\Pi^s_{sat}(M, \chi_2) = \{s_{22}, s_{31}, s_{32}, s_{33}\}$$

$$\Pi^s_{sat}(M, \neg\chi_1) = S \setminus \Pi^s_{sat}(M, \chi_1) = \{s_{11}, s_{12}, s_{13}, s_{23}\}$$

$$\Pi^s_{sat}(M, \neg\chi_2) = S \setminus \Pi^s_{sat}(M, \chi_1) = \{s_{11}, s_{12}, s_{13}, s_{23}\}$$

$$\Pi^s_{sat}(M, \neg\chi_1 \,\&\, \neg\chi_2) = \Pi^s_{sat}(M, \chi_1) \cap \Pi^s_{sat}(M, \chi_2) = \{s_{11}, s_{12}, s_{13}, s_{23}\}$$

# Алгоритм model checking для CTL (пример)




$\varphi = \mathbf{AXA}(p\mathbf{U}q)$

$M \models \varphi$?

$$\psi = Simplify(\varphi) = \neg\mathbf{EX}\neg\underbrace{(\neg\mathbf{E}(\neg q\mathbf{U}(\neg q \,\&\, \neg p))\,\&\,\neg\mathbf{EG}\neg q)}_{\chi}$$

$S = \{s_{11}, s_{12}, s_{13}, s_{22}, s_{23}, s_{31}, s_{32}, s_{33}\}$

$\Pi^s_{sat}(M, \chi) = \{s_{11}, s_{12}, s_{13}, s_{23}\}$

$\Pi^s_{sat}(M, \neg\chi) = S \setminus \Pi^s_{sat}(M, \chi) = \{s_{22}, s_{31}, s_{32}, s_{33}\}$

$\Pi^s_{sat}(M, \mathbf{EX}\neg\chi) = Pre(M, \Pi^s_{sat}(M, \neg\chi)) = \{s_{22}, s_{23}, s_{31}, s_{32}, s_{33}\}$

$\Pi^s_{sat}(M, \psi) = S \setminus \Pi^s_{sat}(M, \mathbf{EX}\neg\chi) = \{s_{11}, s_{12}, s_{13}\}$

$S_0 = \{s_{11}, s_{31}\} \not\subseteq \Pi^s_{sat}(M, \psi)$

Следовательно, $M \not\models \varphi$