

# Математические методы верификации схем и программ

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

## Блок 28

Символьный алгоритм проверки моделей для CTL  
(окончание)

Лектор:

**Подымов Владислав Васильевич**

E-mail:

**valdus@yandex.ru**

ВМК МГУ, 2024/2025, осенний семестр

## Преобразователь $\mathbf{EX}_M$

Каждой ctl-формуле  $\varphi$  для предзаданной модели Крипке  $M$  можно сопоставить предикат, задающий множество всех состояний  $M$ , в которых выполнена  $\varphi$ :  $Sat_M(\varphi) = Sat(M, \varphi)$

Этот предикат можно представить символьно:  $\Phi_\varphi^M = \Phi_{Sat_M(\varphi)}$

Для заданной модели Крипке комбинация  $\mathbf{EX}$  может расцениваться как преобразователь таких предикатов:

$$\mathbf{EX}_M(Sat_M(\varphi)) = Sat_M(\mathbf{EX}\varphi)$$

Согласно устройству процедуры  $\mathfrak{F}_{\mathbf{EX}}$ , преобразователь  $\mathbf{EX}_M$  можно задать так:

$$\mathbf{EX}_M(Z) = Pre(M, Z)$$

Преобразователь  $\mathfrak{f}$ , задающийся равенством  $\mathfrak{f}(Z) = E$  для произвольного предиката  $Z$  и выражения  $E$  (вообще говоря зависящего от  $Z$ ), можно представить записью  $\lambda Z.E$ : это запись функции, принимающей на вход значение  $Z$  и возвращающей значение выражения  $E$  для этого значения

Тогда, в частности,  $\mathbf{EX}_M = \lambda Z.Pre(M, Z)$ , и символьное представление этого преобразователя можно устроить так:  $\mathbf{EX}_{\mathfrak{M}} = \lambda Z.\mathfrak{F}_{pre}(\mathfrak{M}, Z)$

## Преобразователь $\mathbf{EX}_M$

**Лемма.** Для любых модели Крипке  $M$  и предиката  $C$  преобразователь  $\mathbb{f} = \lambda Z. C \cap \mathbf{EX}_M(Z)$  является монотонным

Доказательство.

Рассмотрим предикаты  $A$  и  $B$ , такие что  $A \subseteq B$ , и покажем, что  $\mathbb{f}(A) \subseteq \mathbb{f}(B)$ , то есть что для любого состояния  $s \in \mathbb{f}(A)$  верно  $s \in \mathbb{f}(B)$

Так как  $s \in \mathbb{f}(A)$ , верно  $s \in C$  и  $s \in \mathbf{EX}_M(A)$

$s \in \mathbf{EX}_M(A)$  означает, что существует состояние  $s'$ , такое что  $s' \in A$  и  $s \rightarrow s'$

Так как  $A \subseteq B$ , верно и  $s' \in B$

Значит,  $s \in \mathbf{EX}_M(B)$ , и следовательно,  $s \in C \cap \mathbf{EX}_M(B) = \mathbb{f}(B)$  ▼

# Преобразователь $EG_M$

**Лемма.** Для любых модели Крипке  $M$  и ctl-формулы  $\varphi$  предикат  $Sat_M(\mathbf{EG}\varphi)$  является неподвижной точкой преобразователя  $\lambda Z. Sat_M(\varphi) \cap \mathbf{EX}_M(Z)$

Доказательство.

По определению неподвижной точки, достаточно показать равенство

$$Sat_M(\mathbf{EG}\varphi) = Sat_M(\varphi) \cap \mathbf{EX}_M(Sat_M(\mathbf{EG}\varphi))$$

По определениям  $Sat_M$  и  $\mathbf{EX}_M$ , достаточно показать равносильность

$$M, s \models \mathbf{EG}\varphi \Leftrightarrow M, s \models \varphi \text{ и } M, s \models \mathbf{EX}\mathbf{EG}\varphi$$

По семантике ctl-формул,

- ▶ « $M, s \models \mathbf{EG}\varphi$ »  $\Leftrightarrow$  в  $M$  из  $s$  исходит хотя бы один бесконечный путь  $s_1, s_2, \dots$ , такой что  $M, s_1 \models \varphi, M, s_2 \models \varphi, \dots$
- ▶ « $M, s \models \varphi$  и  $M, s \models \mathbf{EX}\mathbf{EG}\varphi$ »  $\Leftrightarrow M, s \models \varphi$  и в  $M$  из  $s$  исходит хотя бы один бесконечный путь  $s_1, s_2, \dots$ , такой что  $M, s_2 \models \varphi, M, s_3 \models \varphi, \dots$

Легко видеть, что последние два пункта равносильны ▼

# Преобразователь $EG_M$

**Лемма.** Для любых конечной модели Крипке  $M$  и ctl-формулы  $\varphi$  предикат  $Sat_M(EG\varphi)$  является наибольшей неподвижной точкой преобразователя  $\lambda Z. Sat_M(\varphi) \cap EX_M(Z)$

Доказательство. Можете попробовать самостоятельно

Из последней леммы естественно вытекает альтернативный (по сравнению с базовым алгоритмом) вариант процедуры  $\mathfrak{P}_{EG}(M, \varphi)$ :

- ▶ Вычислить  $X = Sat(M, \varphi) = \mathfrak{P}'_{sat}(M, \varphi)$
- ▶ Вернуть предикат  $\mathfrak{P}_{gfp}(M, \lambda Z. X \cap EX_M(Z))$

Эту процедуру несложно представить символьно ( $\mathfrak{F}_{EG}(\mathfrak{M}, \varphi)$ ):

- ▶ Вычислить  $\Phi_X = \mathfrak{F}'_{sat}(\mathfrak{M}, \varphi)$
- ▶ Вернуть представление  $\mathfrak{F}_{gfp}(\mathfrak{M}, \lambda Z. \Phi_X \& EX_{\mathfrak{M}}(Z))$

## Преобразователь $EU_M$

**Лемма.** Для любых модели Крипке  $M$  и ctl-формул  $\varphi$  и  $\psi$  предикат  $Sat_M(\mathbf{E}(\varphi \mathbf{U} \psi))$  является неподвижной точкой преобразователя  $\lambda Z. Sat_M(\psi) \cup (Sat_M(\varphi) \cap \mathbf{EX}_M(Z))$

Доказательство.

По определению неподвижной точки, достаточно показать равенство  $Sat_M(\mathbf{E}(\varphi \mathbf{U} \psi)) = Sat_M(\psi) \cup (Sat_M(\varphi) \cap \mathbf{EX}_M(Sat_M(\mathbf{E}(\varphi \mathbf{U} \psi))))$

По определениям  $Sat_M$  и  $\mathbf{EX}_M$ , достаточно показать равносильность  $M, s \models \mathbf{E}(\varphi \mathbf{U} \psi) \Leftrightarrow M, s \models \psi$  или  $(M, s \models \varphi$  и  $M, s \models \mathbf{EXE}(\varphi \mathbf{U} \psi))$

Аналогично доказательству такой же леммы для  $\mathbf{EG}\varphi$ , легко видеть, что эта равносильность действительно справедлива ▼

**Лемма.** Для любых конечной модели Крипке  $M$  и ctl-формул  $\varphi$  и  $\psi$  предикат  $Sat_M(\mathbf{E}(\varphi \mathbf{U} \psi))$  является наименьшей неподвижной точкой преобразователя  $\lambda Z. Sat_M(\psi) \cup (Sat_M(\varphi) \cap \mathbf{EX}_M(Z))$

Доказательство. Можете попробовать самостоятельно

## Преобразователь $\mathbf{EU}_M$

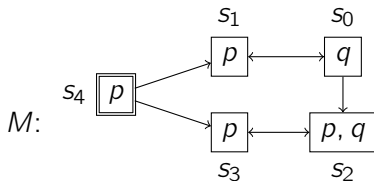
Из последней леммы естественно вытекает альтернативный (по сравнению с базовым алгоритмом) вариант процедуры  $\mathfrak{P}_{\mathbf{EU}}(M, \varphi, \psi)$ :

- ▶ Вычислить  $X = \text{Sat}(M, \varphi) = \mathfrak{P}'_{\text{sat}}(M, \varphi)$  и  $Y = \text{Sat}'(m, \psi) = \mathfrak{P}'_{\text{sat}}(M, \psi)$
- ▶ Вернуть предикат  $\mathfrak{P}_{\text{ifp}}(M, \lambda Z. Y \cup (X \cap \mathbf{EX}_M(Z)))$

Эту процедуру несложно представить символьно ( $\mathfrak{F}_{\mathbf{EU}}(\mathfrak{M}, \varphi, \psi)$ ):

- ▶ Вычислить  $\Phi_X = \mathfrak{F}'_{\text{sat}}(\mathfrak{M}, \varphi)$  и  $\Phi_Y = \mathfrak{F}'_{\text{sat}}(\mathfrak{M}, \psi)$
- ▶ Вернуть представление  $\mathfrak{F}_{\text{ifp}}(\mathfrak{M}, \lambda Z. \Phi_Y \vee (\Phi_X \& \mathbf{EX}_{\mathfrak{M}}(Z)))$

## Символьный алгоритм: пример



$$\varphi = \mathbf{EX}p \ \& \ \neg \mathbf{E}(q \mathbf{UEG} p)$$

Для начала проиллюстрируем модифицированный базовый алгоритм

Начало — такое же, как в исходном базовом алгоритме:

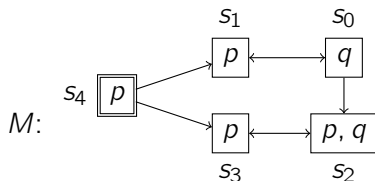
$$\text{Sat}_M(p) = \{s_1, s_2, s_3, s_4\}$$

$$\text{Sat}_M(\mathbf{EX}p) = \text{Pre}(\text{Sat}(M, p)) = \{s_0, s_2, s_3, s_4\}$$

$$\text{Sat}_M(q) = \{s_0, s_2\}$$



## Символьный алгоритм: пример



$$\varphi = \mathbf{EX}p \ \& \ \neg \mathbf{E}(q \mathbf{UEGP})$$

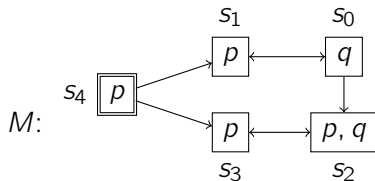
Преобразователь для  $\mathbf{EG}p$ :

$$f_1 = \lambda Z. \text{Sat}_M(p) \cap \mathbf{EX}_M(Z) = \lambda Z. \{s_1, s_2, s_3, s_4\} \cap \text{Pre}(M, Z)$$

Вычисление наибольшей неподвижной точки  $f_1$ :

- ▶  $X_0 = S = \{s_0, s_1, s_2, s_3, s_4\}$
- ▶  $X_1 = f_1(X_0) = \{s_1, s_2, s_3, s_4\} \cap \text{Pre}(M, S) = \{s_1, s_2, s_3, s_4\} \cap S = \{s_1, s_2, s_3, s_4\}$
- ▶  $X_2 = f_1(X_1) = \{s_1, s_2, s_3, s_4\} \cap \{s_0, s_2, s_3, s_4\} = \{s_2, s_3, s_4\}$
- ▶  $X_3 = f_1(X_2) = \{s_1, s_2, s_3, s_4\} \cap \{s_0, s_2, s_3, s_4\} = \{s_2, s_3, s_4\} = X_2$
- ▶  $\text{Sat}_M(\mathbf{EG}p) = \nu Z. f_1(Z) = X_3 = \{s_2, s_3, s_4\}$

# Символьный алгоритм: пример



$$\varphi = \mathbf{EX}p \ \& \ \neg \mathbf{E}(q \mathbf{UEGP})$$

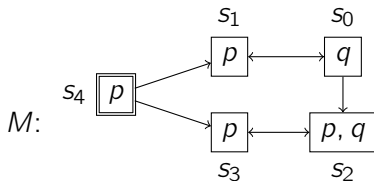
Преобразователь для  $\mathbf{E}(q \mathbf{UEGP})$ :

$$\begin{aligned} f_2 &= \lambda Z. \text{Sat}_M(\mathbf{EG}p) \cup (\text{Sat}_M(q) \cap \mathbf{EX}_M(Z)) = \\ & \lambda Z. \{s_2, s_3, s_4\} \cup (\{s_0, s_2\} \cap \mathbf{EX}_M(Z)) \end{aligned}$$

Вычисление наименьшей неподвижной точки  $f_2$ :

- ▶  $X_0 = \emptyset$
- ▶  $X_1 = f_2(X_0) = \{s_2, s_3, s_4\} \cup (\{s_0, s_2\} \cap \emptyset) = \{s_2, s_3, s_4\}$
- ▶  $X_2 = f_2(X_1) = \{s_2, s_3, s_4\} \cup (\{s_0, s_2\} \cap \{s_0, s_2, s_3, s_4\}) = \{s_0, s_2, s_3, s_4\}$
- ▶  $X_3 = f_2(X_1) = \{s_2, s_3, s_4\} \cup (\{s_0, s_2\} \cap \{s_0, s_1, s_2, s_3, s_4\}) = \{s_0, s_2, s_3, s_4\} = X_2$
- ▶  $\text{Sat}_M(\mathbf{E}(q \mathbf{UEGP})) = \mu Z. f_2(Z) = \{s_0, s_2, s_3, s_4\}$

## Символьный алгоритм: пример



$$\varphi = \mathbf{EX}p \ \& \ \neg \mathbf{E}(q \mathbf{UEG} p)$$

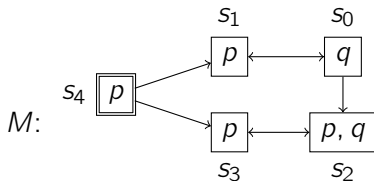
Конец — такой же, как в исходном базовом алгоритме

$$\text{Sat}_M(\neg \mathbf{E}(q \mathbf{UEG} p)) = S \setminus \text{Sat}_M(\mathbf{E}(q \mathbf{UEG} p)) = \{s_1\}$$

$$\text{Sat}_M(\varphi) = \text{Sat}_M(\mathbf{EX}p) \cap \text{Sat}_M(\neg \mathbf{E}(q \mathbf{UEG} p)) = \emptyset$$

Так как  $\{s_4\} \not\subseteq \emptyset$ , можно заключить, что  $M \not\models \varphi$

# Символьный алгоритм: пример



$$\varphi = \mathbf{EX}p \ \& \ \neg \mathbf{E}(q \mathbf{UEG} p)$$

Символьное представление модели  $M$ , основанное на формулах, для трёх разрядов, отвечающих переменным  $x_0, x_1, x_2$ , с естественным кодированием состояний согласно номерам выше:

- ▶  $\Phi_S = x_2 \rightarrow \neg x_1 \ \& \ \neg x_0$
- ▶  $\Phi_{S_0} = x_2 \ \& \ \neg x_1 \ \& \ \neg x_0$
- ▶  $\Phi_{\rightarrow} = \Phi_S \ \& \ \neg x'_2 \ \& \ ((x_0 \leftrightarrow x'_0) \ \& \ (x_1 \oplus x'_1)) \vee \neg x_1 \ \& \ \neg x_0 \ \& \ x'_1 \ \& \ \neg x'_0$
- ▶  $\Phi_p = \Phi_S \ \& \ (x_1 \vee x_0)$
- ▶  $\Phi_q = \neg x_2 \ \& \ \neg x_0$

А переписать результаты работы модифицированного базового алгоритма в символьном виде можете попробовать сами