

Математические методы верификации схем и программ

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

Блок 27

Преобразователи предикатов
и их неподвижные точки

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

ВМК МГУ, 2024/2025, осенний семестр

Преобразователи предикатов

В базовом алгоритме вычисление множеств $Sat(M, \mathbf{EX}\varphi)$, $Sat(M, \mathbf{EG}\varphi)$ и $Sat(M, \mathbf{E}(\varphi_1 \mathbf{U} \varphi_2))$ при помощи процедур $\mathfrak{P}_{\mathbf{EX}}$, $\mathfrak{P}_{\mathbf{EU}}$, $\mathfrak{P}_{\mathbf{EG}}$ основывалось на преобразовании множеств состояний — или, по-другому, одноместных предикатов на множестве S

Способ преобразования предиката на S можно представить как преобразователь предикатов на S : функцию вида $\mathbb{f} : 2^S \rightarrow 2^S$

В частности, темпоральную комбинацию \mathbf{EX} в контексте заданной модели M можно расценивать как преобразователь предикатов:

$$Sat(M, \mathbf{EX}\varphi) = \{s \mid \exists s' : s \rightarrow s', s' \in Sat(M, \varphi)\}$$

$$Sat_M(\mathbf{EX}\varphi) = \{s \mid \exists s' : s \rightarrow s', s' \in Sat_M(\varphi)\}$$

$$\mathbf{EX}_M(Sat_M(\varphi)) = \{s \mid \exists s' : s \rightarrow s', s' \in Sat_M(\varphi)\}$$

$$\mathbf{EX}_M(A) = \{s \mid \exists s' : s \rightarrow s', s' \in A\}$$

Преобразователи предикатов

Совокупность $(2^S, \subseteq)$ — это **решётка**, в которой:

- ▶ Точная верхняя грань $\sup(A, B)$ множеств A и B — это их объединение
- ▶ Точная нижняя грань $\inf(A, B)$ множеств A и B — это их пересечение
- ▶ Наибольший элемент — это множество S
- ▶ Наименьший элемент — это \emptyset

Таким образом, преобразователь предикатов может расцениваться как функция преобразования элементов решётки, и из этого далее будут вытекать терминология и свойства преобразователей

\subseteq в такой решётке — это отношение нестрогого частичного порядка, и для него будем применять соответствующую терминологию:

- ▶ $A \subseteq B \Leftrightarrow A$ не больше B и B не меньше A
- ▶ $A \subset B \Leftrightarrow A$ меньше B и B больше A
- ▶ ...

Преобразователи предикатов

Преобразователь предикатов $f : 2^S \rightarrow 2^S$ называется

- ▶ **монотонным**, если для любых предикатов A, B справедлива импликация

$$A \subseteq B \Rightarrow f(A) \subseteq f(B)$$

- ▶ **\cup -непрерывным**, если для любой бесконечной монотонно неубывающей последовательности предикатов

$$A_1 \subseteq A_2 \subseteq \dots$$

$$\text{верно } f\left(\bigcup_{i=1}^{\infty} A_i\right) = \bigcup_{i=1}^{\infty} f(A_i)$$

- ▶ **\cap -непрерывным**, если для любой бесконечной монотонно невозрастающей последовательности предикатов

$$A_1 \supseteq A_2 \supseteq \dots$$

$$\text{верно } f\left(\bigcap_{i=1}^{\infty} A_i\right) = \bigcap_{i=1}^{\infty} f(A_i)$$

Преобразователи предикатов

Лемма. Любой монотонный преобразователь предикатов \mathbb{f} на конечном множестве S \cup -непрерывен и \cap -непрерывен

Доказательство.

Рассмотрим бесконечную последовательность предикатов $A_1 \subseteq A_2 \subseteq \dots$

Так как множество S конечно, для некоторого k верно

$$A_k = A_{k+1} = A_{k+2} = \dots$$

Так как $A_1 \subseteq \dots \subseteq A_k$, то верно и $\bigcup_{i=1}^k A_i = A_k$

Значит, $\bigcup_{i=1}^{\infty} A_i = A_k$

Так как \mathbb{f} монотонен, верно $\mathbb{f}(A_1) \subseteq \dots \subseteq \mathbb{f}(A_k) = \mathbb{f}(A_{k+1}) = \dots$, и аналогично верно $\bigcup_{i=1}^{\infty} \mathbb{f}(A_i) = \mathbb{f}(A_k)$

Следовательно, $\mathbb{f}(\bigcup_{i=1}^{\infty} A_i) = \mathbb{f}(A_k) = \bigcup_{i=1}^{\infty} \mathbb{f}(A_i)$, то есть \mathbb{f} \cup -непрерывен

\cap -непрерывность обосновывается аналогично ▼

Неподвижные точки

Неподвижной точкой преобразователя $f : 2^S \rightarrow 2^S$ называется предикат A , такой что $f(A) = A$

Неподвижная точка A преобразователя f называется **наименьшей** ($A = \mu Z.f(Z)$), если она наименьшая по включению среди всех неподвижных точек f , и **наибольшей** ($A = \nu Z.f(Z)$), если она наибольшая по включению среди всех неподвижных точек

$f^i(A)$ — так обозначим i -кратное применение преобразователя f к предикату A :

- ▶ $f^0(A) = A$
- ▶ $f^i(A) = f(f^{i-1}(A))$, если $i > 0$

Неподвижные точки

Лемма. Для любого монотонного \cup -непрерывного

преобразователя \mathbb{f} верно $\mu Z. \mathbb{f}(Z) = \bigcup_{i=0}^{\infty} \mathbb{f}^i(\emptyset)$

Доказательство. Пусть $A = \bigcup_{i=0}^{\infty} \mathbb{f}^i(\emptyset)$

По определению наименьшей неподвижной точки, достаточно обосновать два факта:

1. $\mathbb{f}(A) = A$
2. Если $\mathbb{f}(B) = B$, то $A \subseteq B$

1. По \cup -непрерывности \mathbb{f} : $\mathbb{f}(A) = \bigcup_{i=1}^{\infty} \mathbb{f}^i(\emptyset) = \mathbb{f}^0(\emptyset) \cup \bigcup_{i=1}^{\infty} \mathbb{f}^i(\emptyset) = A$

2. Верно $\mathbb{f}^0(\emptyset) = \emptyset \subseteq B$

По монотонности \mathbb{f} , для любого $i \in \{0, 1, 2, \dots\}$ верно следующее: если $\mathbb{f}^i(\emptyset) \subseteq B$, то верно и $\mathbb{f}^{i+1}(\emptyset) = \mathbb{f}(\mathbb{f}^i(\emptyset)) \subseteq \mathbb{f}(B) = B$

Значит, для любого $i \in \{0, 1, 2, \dots\}$ верно $\mathbb{f}^i(\emptyset) \subseteq B$, и следовательно,

$$\bigcup_{i=0}^{\infty} \mathbb{f}^i(\emptyset) \subseteq B \quad \blacktriangledown$$

Неподвижные точки

Лемма. Для любого монотонного \sqcap -непрерывного преобразователя f на S верно $\nu Z.f(Z) = \bigcap_{i=0}^{\infty} f^i(S)$

Доказательство. Аналогично доказательству предыдущей леммы

Лемма. Для любого монотонного преобразователя и любого i , $i \in \mathbb{N}_0$, верно $f^i(\emptyset) \subseteq f^{i+1}(\emptyset)$

Доказательство.

$$f^0(\emptyset) = \emptyset \subseteq f^1(\emptyset)$$

Если $f^{i-1}(\emptyset) \subseteq f^i(\emptyset)$ ($i \geq 1$), то $f^i(\emptyset) = f(f^{i-1}(\emptyset)) \subseteq f(f^i(\emptyset)) = f^{i+1}(\emptyset)$

Значит, согласно принципу математической индукции, для любого $i \in \{0, 1, 2, \dots\}$ верно $f^i(\emptyset) \subseteq f^{i+1}(\emptyset)$ ▼

Лемма. Для любого монотонного преобразователя на S и любого i , $i \in \mathbb{N}_0$, верно $f^i(S) \supseteq f^{i+1}(S)$

Доказательство. Аналогично доказательству предыдущей леммы

Неподвижные точки

Лемма. Для любого монотонного преобразователя f на конечном множестве S существует k , $k \in \mathbb{N}_0$, такое что $f^k(\emptyset) = f^{k+1}(\emptyset)$

Доказательство. Предположим от противного, что это не так

По доказанной ранее лемме, для любого $i \in \{0, 1, \dots\}$ верно $f^i(\emptyset) \subseteq f^{i+1}(\emptyset)$

По предположению, $f^i(\emptyset) \neq f^{i+1}(\emptyset)$, а значит, $f^i(\emptyset) \subset f^{i+1}(\emptyset)$

Следовательно, $|f^0(\emptyset)| < |f^1(\emptyset)| < |f^2(\emptyset)| < \dots$

Но тогда существует m , такое что $|f^m(\emptyset)| > |S|$, что *противоречит* включению $f^m(\emptyset) \subseteq S$ ▼

Лемма. Для любого монотонного преобразователя f на конечном множестве S существует k , $k \in \mathbb{N}_0$, такое что $f^k(S) = f^{k+1}(S)$

Доказательство. Аналогично доказательству предыдущей леммы

Неподвижные точки

Лемма. Для любого преобразователя \mathbb{f} , любого k , $k \in \mathbb{N}_0$, и любого предиката A верно следующее: если $\mathbb{f}^k(A) = \mathbb{f}^{k+1}(A)$, то для любого m , $m \in \mathbb{N}$, верно $\mathbb{f}^k(A) = \mathbb{f}^{k+m}(A)$

Доказательство (индукцией по m).

База ($m = 1$): верно по условию леммы

Индуктивный переход: если $\mathbb{f}^k(A) = \mathbb{f}^{k+(m-1)}(A)$, то
 $\mathbb{f}^{k+m}(A) = \mathbb{f}^{k+1}(\mathbb{f}^{m-1}(A)) = \mathbb{f}^k(\mathbb{f}^{m-1}(A)) = \mathbb{f}^{k+m-1}(A) = \mathbb{f}^k(A) \blacktriangledown$

Неподвижные точки

Объединив результаты всех предложенных лемм, можно легко получить следующие теорему и процедуру вычисления наименьшей неподвижной точки (\mathfrak{P}_{lfp}) для преобразователя предикатов на конечном множестве S

Теорема (о поиске наименьшей неподвижной точки). Для любого монотонного преобразователя \mathbb{f} на конечном множестве S существует k , $k \in \mathbb{N}_0$, такое что

$$\mathbb{f}^0(\emptyset) \subset \mathbb{f}^1(\emptyset) \subset \dots \subset \mathbb{f}^k(\emptyset) = \mathbb{f}^{k+1}(\emptyset),$$

и верно $\mu Z. \mathbb{f}(Z) = \mathbb{f}^k(\emptyset)$

Процедура $\mathfrak{P}_{lfp}(M, \mathbb{f})$:

- ▶ Положить $X_0 = \emptyset$
- ▶ Последовательно для $i \in \{1, 2, \dots\}$:
 - ▶ Вычислить $X_i = \mathbb{f}(X_{i-1})$
 - ▶ Если $X_i = X_{i-1}$, то завершить процедуру и вернуть X_i

Для использования преобразователей в качестве аргументов процедур требуется подходящее представление — оно будет введено чуть позже

Неподвижные точки

Символьным представлением преобразователя \mathbb{f} назовём отображение \mathbb{f}_s множества символьных представлений предикатов в него же, такое что $\mathbb{f}_s(\Phi_A) = \Phi_{\mathbb{f}(A)}$

Процедура вычисления наименьшей неподвижной точки очевидным образом переформулируется в терминах символьных представлений

Процедура $\mathfrak{F}_{lfp}(\mathcal{M}, \mathbb{f}_s)$:

- ▶ Положить $\Phi^0 = \Phi_\emptyset$
- ▶ Последовательно для $i \in \{1, 2, \dots\}$:
 - ▶ Вычислить $\Phi^i = \mathbb{f}_s(\Phi^{i-1})$
 - ▶ Если $\Phi^i \sim \Phi^{i-1}$, то завершить процедуру и вернуть Φ^i

Неподвижные точки

Аналогичные теорема и алгоритмы получаются и для наибольшей неподвижной точки

Теорема (о поиске наибольшей неподвижной точки). Для любого монотонного преобразователя \mathbb{f} на конечном множестве S существует k , $k \in \mathbb{N}_0$, такое что

$$\mathbb{f}^0(S) \supset \mathbb{f}^1(S) \supset \dots \supset \mathbb{f}^k(S) = \mathbb{f}^{k+1}(S),$$

и верно $\nu Z. \mathbb{f}(Z) = \mathbb{f}^k(S)$

Процедура $\mathfrak{P}_{gfp}(M, \mathbb{f})$:

- ▶ Положить $X_0 = S$
- ▶ Последовательно для $i \in \{1, 2, \dots\}$:
 - ▶ Вычислить $X_i = \mathbb{f}(X_{i-1})$
 - ▶ Если $X_i = X_{i-1}$, то завершить процедуру и вернуть X_i

Процедура $\mathfrak{F}_{gfp}(\mathfrak{M}, \mathbb{f}_s)$:

- ▶ Положить $\Phi^0 = \Phi_S$
- ▶ Последовательно для $i \in \{1, 2, \dots\}$:
 - ▶ Вычислить $\Phi^i = \mathbb{f}_s(\Phi^{i-1})$
 - ▶ Если $\Phi^i \sim \Phi^{i-1}$, то завершить процедуру и вернуть Φ^i