

Математические методы верификации схем и программ

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

Блок 29

Абстракция моделей
Редукция по конусу влияния
Абстракция данных

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

Абстракция моделей

Абстракция модели — это устранение из неё деталей, которые по тем или иным причинам считаются излишними (избыточными, несущественными) и не влияют на результаты анализа интересующих свойств

Абстракция — это самый действенный способ решения проблемы **комбинаторного взрыва числа состояний**

Для примера рассмотрим два метода абстракции:

1. Редукция по конусу влияния
2. Абстракция данных

Эти методы применяются к описанию модели, более «высокоуровневому» по сравнению с моделью Крипке, и потому позволяют избежать построения чрезмерно большой модели Крипке за счёт её упрощения до построения

Абстракция моделей

Редукция по конусу влияния применяется к системам, состояния которых задаются как наборы значений переменных системы

Основная идея метода состоит в том, чтобы устранить из системы те переменные, которые не содержатся в спецификации и не оказывают на спецификацию никакого *влияния*

То есть удаляются переменные, которые с точки зрения спецификации являются *фиктивными*

Абстракция данных состоит в отображении «реальных» значений переменных (которых может быть очень много) в небольшое число *абстрактных* значений данных с сохранением интересующих свойств исходной системы

Например, если абстрактная система *симулирует* исходную, то можно гарантировать сохранение выполнимости спецификаций из *достаточно широкого фрагмента языка ACTL**

Редукция по конусу влияния

Рассмотрим систему, состояния которой определяются как всевозможные наборы значений переменных множества $V = \{v_1, \dots, v_n\}$, а переходы определяются согласно рассказанному для **символьных представлений** относительно **двух комплектов переменных** как система уравнений вида

$$v'_i = f_i(v_1, \dots, v_n)$$

Пусть в спецификации системы используются только переменные множества W , $W \subseteq V$

Для упрощения системы можно было бы попробовать удалить из неё все переменные, которые не входят в W

Но увы, так сделать «в лоб» нельзя: значение переменной v из множества $V \setminus W$ может прямо или косвенно зависеть от значения переменной из V

Редукция по конусу влияния

Системой при обсуждения конусов влияния будем называть четвёрку $\mathfrak{S} = (V, X, \vec{f}, W)$ такого вида:

- ▶ $V = (v_1, \dots, v_n)$ — конечный набор булевых переменных, $n \geq 1$
- ▶ $X \subseteq \{0, 1\}^n$ — множество начальных оценок переменных
- ▶ $\vec{f} = (f_1, \dots, f_n)$ — набор n -местных булевых функций, задающих уравнения системы
- ▶ W — множество наблюдаемых переменных, $W \subseteq V$

Для такой системы \mathfrak{S} модель Крипке $M_{\mathfrak{S}} = (S, S_0, \rightarrow, L)$ устроим так:

- ▶ $S = \{0, 1\}^n$
- ▶ $S_0 = X$
- ▶ \rightarrow — множество переходов, символьное представление которого имеет вид $\bigwedge_{i=1}^n (v_i' \leftrightarrow f_i(v_1, \dots, v_n))$
- ▶ $L(s) = \{v_i \mid s[i-1] = 1, v_i \in W\}$

Редукция по конусу влияния

Конусом влияния $C_{\mathfrak{S}}(W)$ множества переменных W в системе \mathfrak{S} будем называть наименьшее множество переменных, для которого верно следующее:

- ▶ $W \subseteq C$
- ▶ Если для переменной v_i из C функция f_i системы \mathfrak{S} **существенно** зависит от переменной v_m , то $v_m \in C$

Метод редукции по конусу влияния состоит в удалении всех переменных системы, не входящих в конус влияния переменных, значения которых используются в спецификации системы

Редукция по конусу влияния

Пример (счётчик по модулю 8)

Рассмотрим систему над переменными $V = (v_0, v_1, v_2)$, принимающими значения $\{0, 1\}$ и задаваемую системой

$$\begin{cases} v'_0 &= \neg v_0 \\ v'_1 &= v_0 \oplus v_1 \\ v'_2 &= (v_0 \& v_1) \oplus v_2 \end{cases}$$

Для множества $\{v_0\}$ конусом влияния является $\{v_0\}$

Для множеств $\{v_1\}$ и $\{v_0, v_1\}$ конусом влияния является $\{v_0, v_1\}$

Для множеств переменных, содержащих v_2 , конус влияния — это множество всех переменных

Таким образом, если в спецификации существенным является только значение переменной v_0 , то систему можно упростить, оставив только первое уравнение, и если в спецификации не используется значение v_2 , то из системы можно удалить третье уравнение

Редукция по конусу влияния

Записью $M|_W$ для модели Крипке $M = (S, S_0, \rightarrow, L)$ и подмножества W атомарных высказываний обозначим модель, получающуюся из M заменой каждой метки $L(s)$ на $L(s) \cap W$

Утверждение. Для любой модели Крипке M и любой ctl^* -формулы φ над атомарными высказываниями W верна равносильность

$$M \models \varphi \quad \Leftrightarrow \quad M|_W \models \varphi$$

Систему $\text{red}(\mathfrak{G}, W)$, получающуюся из $\mathfrak{G} = (V, X, \vec{f}, U)$ редукцией по множеству переменных W , зададим как четвёрку $(C, Y, \vec{g}, U \cap W)$, где:

- ▶ C — множество $C_{\mathfrak{G}}(W)$ с таким же порядком переменных, как в V
- ▶ Y получается из X удалением разрядов всех наборов, отвечающих расположению переменных из $V \setminus C_{\mathfrak{G}}(W)$ в V
- ▶ \vec{g} — функции из \vec{f} , отвечающие переменным из C

Редукция по конусу влияния

Утверждение. Для любой системы \mathfrak{S} и любого подмножества переменных W верно соотношение

$$M_{\mathfrak{S}}|_W \sim_b M_{red(\mathfrak{S}, W)}$$

Доказательство. Можете доказать самостоятельно, основываясь на отношении бисимуляции, состоящий из всех пар $(x, y) \in \{0, 1\}^n \times \{0, 1\}^{|\mathcal{C}_{\mathfrak{S}}(W)|}$, в которых y получается из x вычёркиванием разрядов, отвечающих переменным не из конуса влияния

Следствие. Для любых системы \mathfrak{S} , подмножества её переменных W и ctl^* -формулы φ над атомарными высказываниями W верно

$$M_{\mathfrak{S}}|_W \models \varphi \quad \Leftrightarrow \quad M_{red(\mathfrak{S}, W)} \models \varphi$$

Абстракция данных

Редукция системы основывалась на том, что редуцированная система бисимуляционно эквивалентна исходной: системы до и после имеют одинаковую степень детализации и отличаются только удалением несущественных переменных

Абстракция данных обычно приводит к существенному снижению детальности модели, и бисимуляцию для таких целей использовать нецелесообразно

Но для метода абстракции хорошо подходит симуляция, предоставляющая гарантии выполнимости пускай и не всех возможных свойств, но достаточно широкого фрагмента

Абстракция данных

Рассмотрим модель Крипке $M = (S, S_0, \rightarrow, L)$ и разбиение множества S : $\mathfrak{B} = [B_1, \dots, B_n]$, согласованное с функцией разметки модели M : для любой пары состояний s, r из одного блока разбиения верно $L(s) = L(r)$

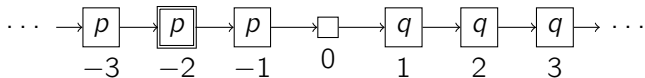
Абстракцией модели M , порождённой разбиением \mathfrak{B} , согласованным с функцией разметки, называется модель $\text{abstr}(M, \mathfrak{B}) = (S', S'_0, \mapsto, L')$, где:

- ▶ $S' = \mathfrak{B}$
- ▶ $S'_0 = \{B_i \mid B_i \in \mathfrak{B}, B_i \cap S_0 \neq \emptyset\}$
- ▶ $B_i \mapsto B_j \iff$ существуют состояния $s_i \in B_i$ и $s_j \in B_j$, такие что $s_i \rightarrow s_j$
- ▶ $L'(B_i) = L(s)$, где $s \in B_i$

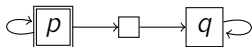
Абстракция данных

Пример

Абстракцией (бесконечной) модели M



для разбиения $\mathfrak{B} = [\{i \mid i \in \mathbb{Z}, i \leq -1\}, \{0\}, \{j \mid j \in \mathbb{Z}, j \geq 1\}]$
($abstr(M, \mathfrak{B})$) является модель



Утверждение. Для любой модели Крипке M и любого разбиения \mathfrak{B} её множества состояний, согласованного с функцией разметки, верно:

$$M \preceq abstr(M, \mathfrak{B})$$

Доказательство. И это тоже можете попробовать доказать самостоятельно, если хотите

Следствие. Для любых модели Крипке M , разбиения \mathfrak{B} её множества состояний, согласованного с функцией разметки, и act1*-формулы φ верно: если $abstr(M, \mathfrak{B}) \models \varphi$, то $M \models \varphi$