# Математические методы верификации схем и программ

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

Блок 36

Бисимуляция состояний модели
Алгоритм проверки бисимуляционной эквивалентности
Фактор-модель

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

ВМК МГУ, 2024/2025, осенний семестр

# Вступление

Три отношения эквивалентности $\sim$ моделей Крипке с соответствующими фрагментами $\mathcal{L}$ языка CTL*:

1. Трассовая эквивалентность и LTL
2. Симуляционная эквивалентность и ACTL*
3. Бисимуляционная эквивалентность и CTL*

Если модель $M_1$ специфицирована в терминах фрагмента $\mathcal{L}$, то можно быть уверенным в том, что на любой модели $M_2$, такой что $M_1 \sim M_2$, выполняются в точности те же формулы, что и на $M_1$

А как проверить такую эквивалентность?

Про трассовую эквивалентность упоминалось, что её проверка — это трудная задача

Поэтому трассовую эквивалентность оставим в стороне

Симуляционная и бисимуляционная эквивалентности похожи, и алгоритмы проверки для них тоже похожи

Поэтому подробно рассмотрим только бисимуляционную эквивалентность

# Бисимуляция состояний модели

$M(s)$ — так будем обозначать модель Крипке, получающуюся из модели $M$ заменой множества начальных состояний на $\{s\}$

Состояния $s_1$ и $s_2$ модели Крипке $M$ бисимуляционно эквивалентны ($s_1 \sim_b^M s_2$), если $M(s_1) \sim_b M(s_2)$

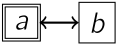
Проверку бисимуляционной эквивалентности конечных моделей $M_1$, $M_2$ можно свести к проверке бисимуляционной эквивалентности двух состояний одной конечной модели:

1. Добавим в каждую из моделей $M_i$ одно новое состояние $s_i$ с меткой $\emptyset$
2. Проведём из $s_i$ дуги во все начальные состояния
3. Переименуем состояния $M_1$ и $M_2$ так, чтобы их множества состояний не пересекались
4. Объединим все состояния и переходы моделей в модель $M$ с пустым множеством начальных состояний
5. $M_1 \sim_b M_2 \quad \Leftrightarrow \quad s_1' \sim_b^M s_2'$, где $s_1'$ и $s_2'$ — состояния, получающиеся из $s_1$ и $s_2$ после переименования

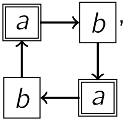
# Бисимуляция состояний модели

## Пример

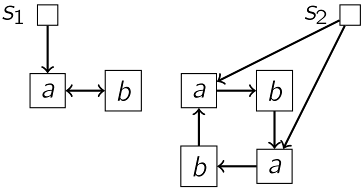
Чтобы проверить бисимуляционную эквивалентность моделей




и




достаточно проверить бисимуляционную эквивалентность состояний $s_1$ и $s_2$ в модели



# Бисимуляция состояний модели

Рассмотрим модель $M = (S, S_0, \to, L)$

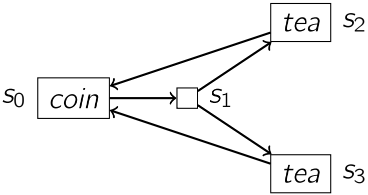
Отношение $\mathcal{R} \subseteq S \times S$ называется отношением бисимуляции на модели $M$, если для любой пары $(s, r) \in \mathcal{R}$ отношение $\mathcal{R}$ является отношением бисимуляции между $M(s)$ и $M(r)$

Это определение отличается от определения отношения бисимуляции для пары моделей только тем, что

- вместо двух моделей рассматривается одна, взятая два раза, и
- не требуется соответствие начальных состояний

# Бисимуляция состояний модели

## Пример




Примеры отношений бисимуляции на этой модели:

1. $\{(s_0, s_0), (s_1, s_1), (s_2, s_2), (s_3, s_3)\}$
2. $\{(s_0, s_0), (s_1, s_1), (s_2, s_2), (s_2, s_3), (s_3, s_2), (s_3, s_3)\}$
3. $\{(s_0, s_0), (s_1, s_1), (s_2, s_3), (s_3, s_2)\}$
4. $\emptyset$

**Утверждение.** **Если $\mathcal{R}_1$ и $\mathcal{R}_2$ — отношения бисимуляции на конечной модели Крипке $M$, то отношение $\mathcal{R}_1 \cup \mathcal{R}_2$ также является отношением бисимуляции на $M$**

Можете попробовать доказать это самостоятельно (это не сверхслож- но)

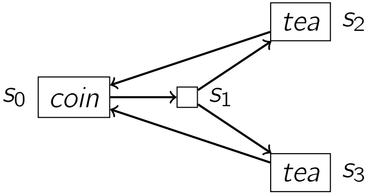
# Бисимуляция состояний модели

**Следствие.** **Если $\mathcal{R}_1, \dots, \mathcal{R}_n$ — все отношения бисимуляции на конечной модели Крипке $M$, то $\bigcup_{i=1}^{n} \mathcal{R}_i$ — отношение бисимуляции на $M$, наибольшее по теоретико-множественному включению**

$\approx_M$ — так будем обозначать отношение бисимуляции на конечной модели Крипке $M$, наибольшее по теоретико-множественному включению (*существующее согласно следствию выше, и очевидным образом единственное*)

**Пример**

$M$:




$$\approx_M = \{(s_0, s_0), (s_1, s_1), (s_2, s_2), (s_2, s_3), (s_3, s_2), (s_3, s_3)\}$$

# Бисимуляция состояний модели

**Утверждение.** **Для любой конечной модели Крипке $M$ отношение $\approx_M$ является отношением эквивалентности**

**Утверждение.** **Для любой конечной модели Крипке $M$ отношения $\sim_b^M$ и $\approx_M$ совпадают**

И это можете попробовать доказать самостоятельно (и это не очень сложно)

Следовательно, проверку соотношения $s_1 \sim_b^M s_2$ можно устроить так:

1. Вычислить все классы эквивалентности отношения $\approx_M$
2. Проверить, лежат ли $s_1$ и $s_2$ в одном классе эквивалентности

Осталось показать, как можно вычислить все классы эквивалентности отношения $\approx_M$

$S/\approx$ — так для отношения эквивалентности $\approx$ на множестве $S$ будем обозначать семейство всех классов эквивалентности отношения $\approx$

# Вычисление классов эквивалентности $\approx_M$

**Дано:** конечная модель Крипке $M = (S, S_0, \to, L)$

**Требуется:** вычислить семейство $S/{\approx_M}$

**Общая идея алгоритма** похожа на идею алгоритма минимизации детерминированного конечного автомата и на вычисление наибольшей неподвижной точки преобразователя предикатов:

- На каждом шаге имеем некоторое разбиение множества $S$ на предполагаемые классы эквивалентности
- Если можно «тривиально» заключить, что некоторые два состояния, предполагающиеся эквивалентными, на самом деле неэквивалентны, то соответственно разобъём предполагаемый класс эквивалентности на два
- Иначе полученное семейство множеств состояний выдаётся в ответ
- Начнём со «слабого» предположения: разбиения, из которого можно получить ответ такими подразбиениями классов

# Вычисление классов эквивалентности $\approx_M$

Разбиением множества $S$ будем называть любое конечное семейство $\{B_1, \dots, B_n\}$ попарно непересекающихся предикатов, такое что
$S = \bigcup\limits_{i=1}^{n} B_i$

$Post_M(s)$ — так будем обозначать множество всех состояний $s'$, таких что в $M$ содержится переход $s \to s'$

Предикат $C$ назовём разветвителем предиката $B$, если существует пара состояний $s_1, s_2 \in B$, такая что

- $Post_M(s_1) \cap C \neq \emptyset$ (*из $s_1$ можно перейти в $C$*) и
- $Post_M(s_2) \cap C = \emptyset$ (*из $s_2$ нельзя перейти в $C$*)

Содержательно, существование разветвителя — это «тривиальный» индикатор того, что состояния неэквивалентны

# Вычисление классов эквивалентности $\approx_M$

Уточнением предиката $B$ относительно предиката $C$ будем называть семейство предикатов $Ref(B|C)$, устроенное так:

- Если $C$ — разветвитель предиката $B$, то $Ref(B|C) = \{D, E\}$, где
  - $D = \{s \mid s \in B,\ Post_M(s) \cap C \neq \emptyset\}$
  - $E = \{s \mid s \in B,\ Post_M(s) \cap C = \emptyset\}$
- Иначе $Ref(B|C) = \{B\}$

Уточнением семейства предикатов $\mathfrak{B} = \{B_1, \dots, B_n\}$ относительно предиката $C$ будем называть семейство предикатов
$Ref(\mathfrak{B}|C) = \bigcup\limits_{i=1}^{n} Ref(B_i|C)$

Уточнением разбиения $\mathfrak{B} = \{B_1, \dots, B_n\}$ будем называть разбиение
$Ref(\mathfrak{B}) = Ref(\dots Ref(Ref(\mathfrak{B}|B_1)|B_2)\dots|B_n)$

# Вычисление классов эквивалентности $\approx_M$

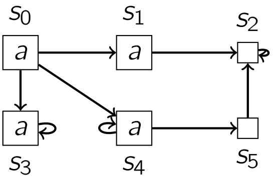
**Алгоритм** $\mathfrak{A}$ вычисления классов эквивалентности $\approx_M$ для $M = (S, S_0, \rightarrow, L)$ над AP:

1. Вычислить разбиение
   $\mathfrak{B}_0 = \{B_X | B_X = \{s \mid s \in S,\ L(s) = X\},\ B_X \neq \emptyset, X \subseteq \mathrm{AP}\}$
   - *То есть эквивалентными полагаются состояния с одинаковой разметкой атомарными высказываниями*

2. Последовательно для каждого $i \in \{1, 2, \dots\}$:
   2.1 Вычислить $\mathfrak{B}_i = \mathit{Ref}(\mathfrak{B}_{i-1})$
   2.2 Если $\mathfrak{B}_i = \mathfrak{B}_{i-1}$, то завершить алгоритм и выдать ответ $\mathfrak{B}_i$

# Вычисление классов эквивалентности $\approx_M$

## Пример




$\mathfrak{B}_0 = [\{s_0, s_1, s_3, s_4\}, \{s_2, s_5\}]$

$$
\begin{aligned}
\mathfrak{B}_1 &= Ref([\{s_0, s_1, s_3, s_4\}, \{s_2, s_5\}]) \\
&= Ref(Ref([\{s_0, s_1, s_3, s_4\}, \{s_2, s_5\}] | \{s_0, s_1, s_3, s_4\}) | \{s_2, s_5\}) \\
&= Ref([\{s_0, s_3, s_4\}, \{s_1\}, \{s_2, s_5\}] | \{s_2, s_5\}) \\
&= [\{s_0, s_3\}, \{s_4\}, \{s_1\}, \{s_2, s_5\}] \\
\mathfrak{B}_2 &= Ref([\{s_0, s_3\}, \{s_4\}, \{s_1\}, \{s_2, s_5\}]) \\
&= \dots \\
&= [\{s_0\}, \{s_3\}, \{s_4\}, \{s_1\}, \{s_2, s_5\}]
\end{aligned}
$$

$\mathfrak{B}_3 = Ref(\mathfrak{B}_2) = \dots = \mathfrak{B}_2$

Ответ: $[\{s_0\}, \{s_3\}, \{s_4\}, \{s_1\}, \{s_2, s_5\}]$

# Вычисление классов эквивалентности $\approx_M$

Уточнением отношения эквивалентности $\mathcal{R}$ на множестве $S$ назовём отношение эквивалентности $Ref(\mathcal{R})$, такое что $S/Ref(\mathcal{R}) = Ref(S/\mathcal{R})$

**Утверждение.** **Для любой конечной модели Крипке $M$ и любого отношения эквивалентности $\mathcal{R}$ на состояниях этой модели верно:**

1. $\mathcal{R}$ **— отношение бисимуляции** $\quad\Leftrightarrow\quad Ref(\mathcal{R}) = \mathcal{R}$
2. $Ref(\mathcal{R}) \subseteq \mathcal{R}$
3. **Если** $\approx_M \subseteq \mathcal{R}$**, то** $\approx_M \subseteq Ref(\mathcal{R})$

**Теорема.** **Для любой конечной модели Крипке $M = (S, S_0, \to, L)$ алгоритм $\mathfrak{A}$ завершается и выдаёт в ответ семейство $S/{\approx_M}$**

Можете доказать утверждение и теорему самостоятельно

Для самостоятельного размышления:

1. Какова сложность предложенного алгоритма по времени работы?
2. Можно ли предложить алгоритм с меньшим порядком сложности?
3. Попробуйте предложить (с обоснованием) аналогичный алгоритм для симуляционной эквивалентности

# Фактор-модель

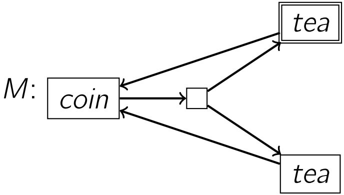
$[s]_\approx$ — так будем обозначать класс эквивалентности элемента $s$ по отношению $\approx$

Фактор-моделью модели Крипке $M = (S, S_0, \to, L)$ называется модель $M_\approx = (S', S'_0, \mapsto, L')$, устроенная так:

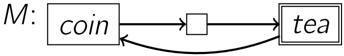
- $S' = S/{\approx_M}$
- $S'_0 = \{[s]_{\approx_M} \mid s \in S_0\}$
- $\mapsto = \{([s]_{\approx_M}, [r]_{\approx_M}) \mid s \to r\}$
- $L'([s]_{\approx_M}) = L(s)$

# Фактор-модель

## Пример




Фактор-модель $M_{\approx}$ устроена так:




**Утверждение.** **Для любой конечной модели Крипке $M$ верно** $M \sim_b M_{\approx}$

И это тоже можете попробовать доказать самостоятельно