Математические методы верификации схем и программ

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

Блок 34

Отношения симуляции и бисимуляции
Симуляционная и бисимуляционная эквивалентности

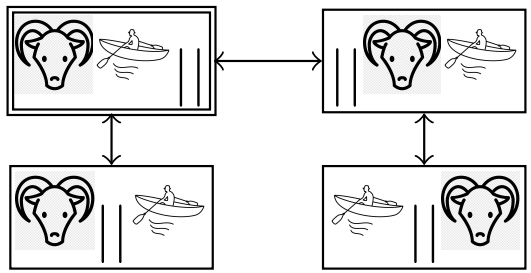
Лектор:
Подымов Владислав Васильевич
E-mail:
valdus@yandex.ru

ВМК МГУ, 2025, сентябрь–декабрь

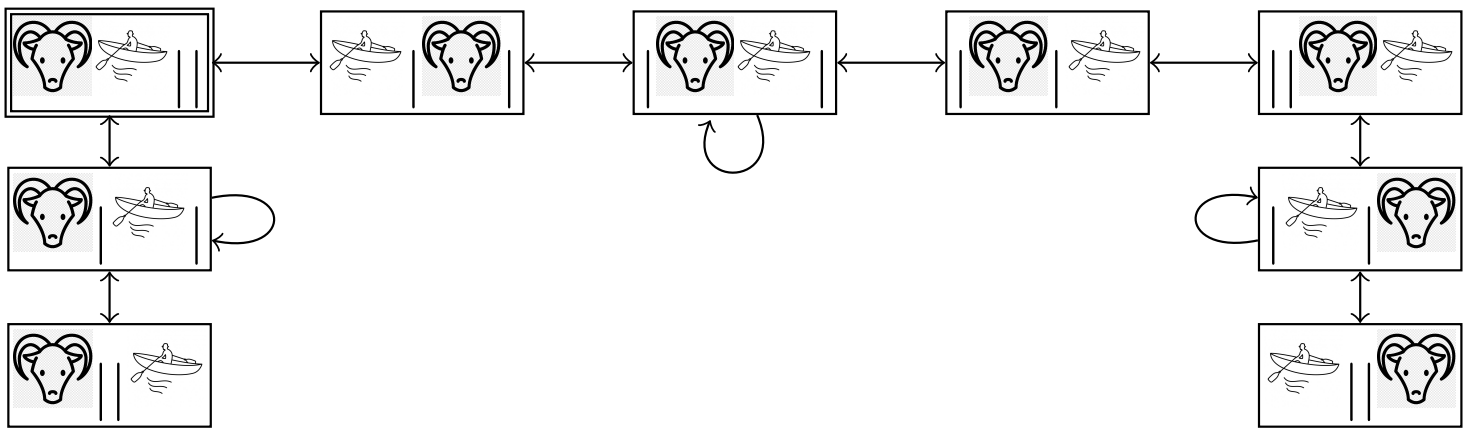
Вступление

Пример/наблюдение 1

Модели Крипке бывают простые



А бывают и сложные



Вступление

Пример/наблюдение 1

Сложные модели придумываются для

- точного соответствия поведению исходной системы и
- детального воспроизведения шагов выполнения системы

Но такие модели трудно строить (вычислять) и трудно анализировать

С другой стороны, простые модели

- легко строятся и
- легко анализируются

Но простой моделью лишь приблизительно (неточно) описывается поведение исходной системы и предоставляется лишь поверхностная информация о шагах выполнения системы

Вступление

Пример/наблюдение 1

Хотелось бы иметь возможность «переключать» степень простоты модели, чтобы использовать преимущества, отвечающие текущим целям исследования системы

Например, было бы неплохо уметь разрабатывать точную детальную модель так, чтобы она затем не слишком трудно перестраивалась в простую для достаточно эффективной верификации

Но для этого требуются гарантии того, что две заданные модели настолько схожи, что обладают одинаковыми спектрами свойств относительно поставленной задачи верификации

Вступление

Пример/наблюдение 2

Представим себе, что

- для системы $\mathfrak{S}$ была построена модель M,
- для этой модели было показано соответствие набору спецификаций $\varphi_1, \ldots, \varphi_k$,
- но после этого в модель были внесены изменения (исправления, улучшения, оптимизации), и в результате получена модель M'

Хотелось бы иметь возможность переносить результаты о правильности модели с M на M', избегая трудоёмкого процесса проверки соответствия модели спецификациям и ограничившись только анализом различий моделей M и M'

Но тогда требуется придумать отношение схожести между двумя моделями, гарантирующее одинаковое соответствие или несоответствие спецификациям $\varphi_1, \ldots, \varphi_k$ для схожих моделей

Трассовая эквивалентность моделей

Если в качестве языка спецификаций выбрать язык LTL, то нетрудно заметить (вспомнить), что:

- Каждая ltl-формула φ является формой записи множества «хороших» трасс $\mathrm{Tr}(\varphi)$
- Верификация модели M состоит в том, чтобы проверить, что все трассы модели являются «хорошими»: $\mathrm{Tr}(M) \subseteq \mathrm{Tr}(\varphi)$

Тогда можно схожесть моделей определить так

Модели M_1 и M_2 трассово эквивалентны, если $\mathrm{Tr}(M_1) = \mathrm{Tr}(M_2)$

Трассовая эквивалентность моделей

Утверждение. **Для любых трассово эквивалентных моделей M_1, M_2 и любой ltl-формулы φ верно:**

$$M_1 \models \varphi \quad \Leftrightarrow \quad M_2 \models \varphi$$

Но иметь одну только трассовую эквивалентность в качестве меры схожести моделей недостаточно:

- Аналогичное утверждение для многих других языков спецификаций оказывается неверным
  - Например, для CTL
- Проверка трассовой эквивалентности конечных моделей Крипке — это очень трудная задача
  - Более точно — PSPACE-полная, но не хочется тратить время на разъяснение этого факта

Необходимо иметь и такие определения схожести моделей, которые были бы более «простыми» и подходили для других языков спецификаций

Отношение симуляции

Рассмотрим две модели Крипке над общим множеством атомарных высказываний AP (в этом блоке множество AP считается всегда заданным по умолчанию):

$$M' = (S', S'_0, \to, L'), \quad M'' = (S'', S''_0, \mapsto, L'')$$

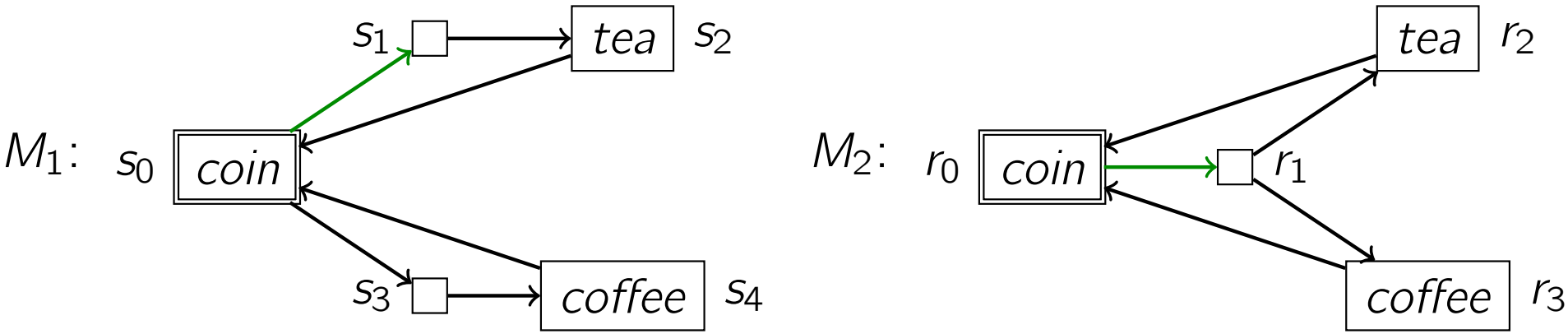
Отношение $\mathcal{R} \subseteq S' \times S''$ называется отношением симуляции между M' и M'', если для него выполнены два условия:

1. Для любого состояния s'_0 из S'_0 существует состояние s''_0 из S''_0, такое что $(s'_0, s''_0) \in \mathcal{R}$
2. Для любой пары s', s'', такой что $\mathcal{R}(s', s'')$, верно следующее:
   - 2.1 $L'(s') = L''(s'')$
   - 2.2 Для любого состояния r', такого что $s' \to r'$, существует состояние r'', такое что $s'' \mapsto r''$ и $\mathcal{R}(r', r'')$

Будем говорить, что модель M' симулируется моделью M'' ($M' \preceq M''$), если существует отношение симуляции между M' и M''

Отношение симуляции

Пример



Пример отношения симуляции между M_1 и M_2:

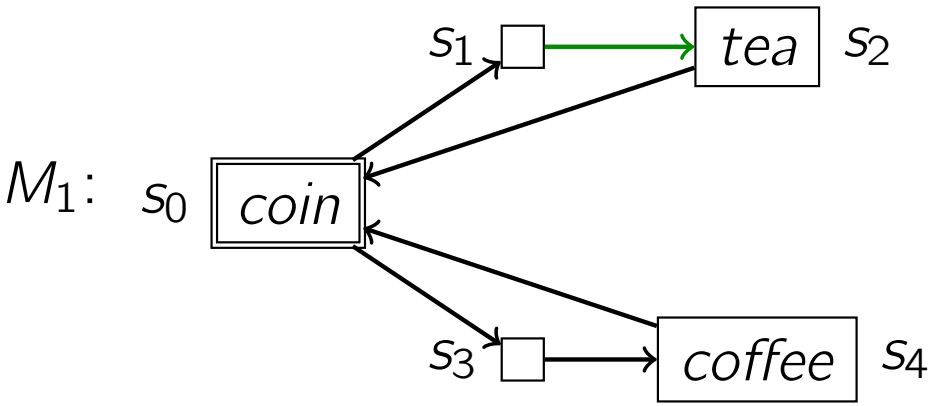
$$\{(s_0, r_0), (s_1, r_1), (s_2, r_2), (s_3, r_1), (s_4, r_3)\}$$

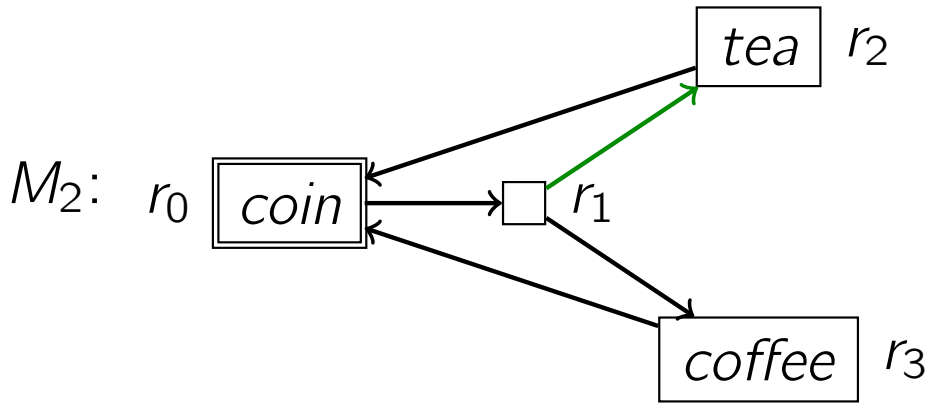
Это несложно проверить:

- Для s_0 в отношении существует пара
- Состояния каждой пары одинаково размечены атомарными высказываниями
- Каждой паре и каждому переходу в первой модели отвечает подходящий переход из парного состояния во второй модели (такой что пара концов переходов входит в отношение)

Отношение симуляции

Пример





Пример отношения симуляции между M_1 и M_2:

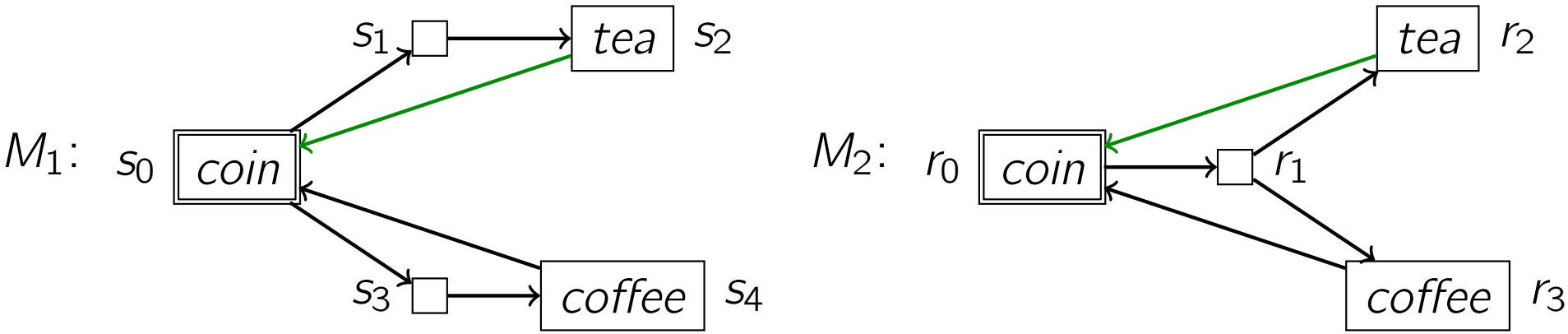
$$\{(s_0, r_0), (s_1, r_1), (s_2, r_2), (s_3, r_1), (s_4, r_3)\}$$

Это несложно проверить:

- Для s_0 в отношении существует пара
- Состояния каждой пары одинаково размечены атомарными высказываниями
- Каждой паре и каждому переходу в первой модели отвечает подходящий переход из парного состояния во второй модели (такой что пара концов переходов входит в отношение)

Отношение симуляции

Пример



Пример отношения симуляции между M_1 и M_2:

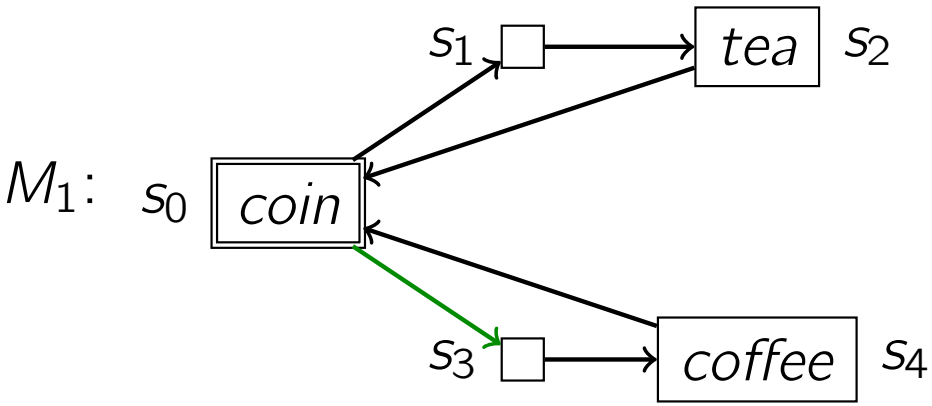
$$\{(s_0, r_0), (s_1, r_1), (s_2, r_2), (s_3, r_1), (s_4, r_3)\}$$

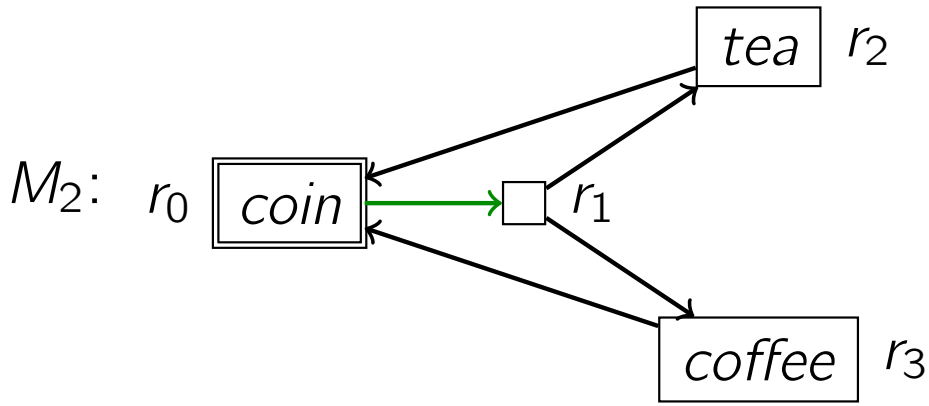
Это несложно проверить:

- Для s_0 в отношении существует пара
- Состояния каждой пары одинаково размечены атомарными высказываниями
- Каждой паре и каждому переходу в первой модели отвечает подходящий переход из парного состояния во второй модели (такой что пара концов переходов входит в отношение)

Отношение симуляции

Пример





Пример отношения симуляции между M_1 и M_2:

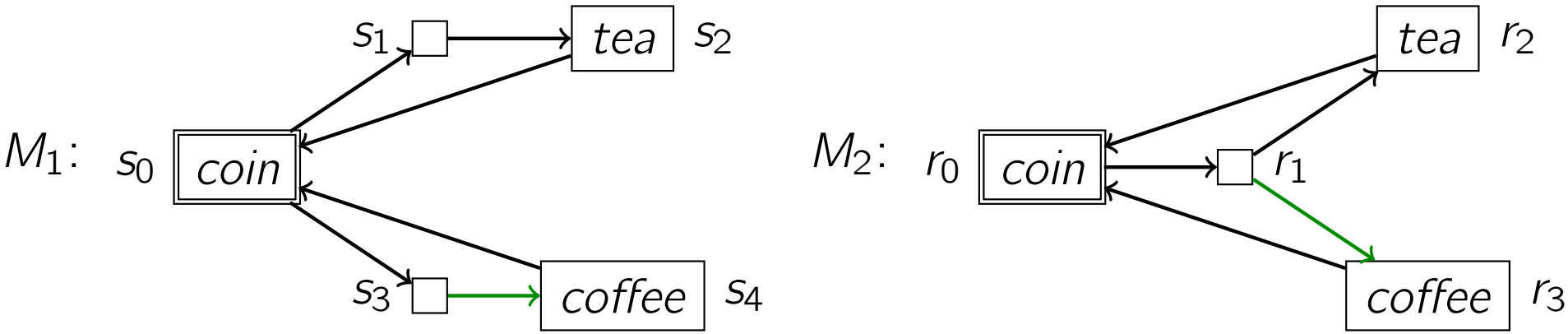
$$\{(s_0, r_0), (s_1, r_1), (s_2, r_2), (s_3, r_1), (s_4, r_3)\}$$

Это несложно проверить:

- Для s_0 в отношении существует пара
- Состояния каждой пары одинаково размечены атомарными высказываниями
- Каждой паре и каждому переходу в первой модели отвечает подходящий переход из парного состояния во второй модели (такой что пара концов переходов входит в отношение)

Отношение симуляции

Пример



Пример отношения симуляции между M_1 и M_2:

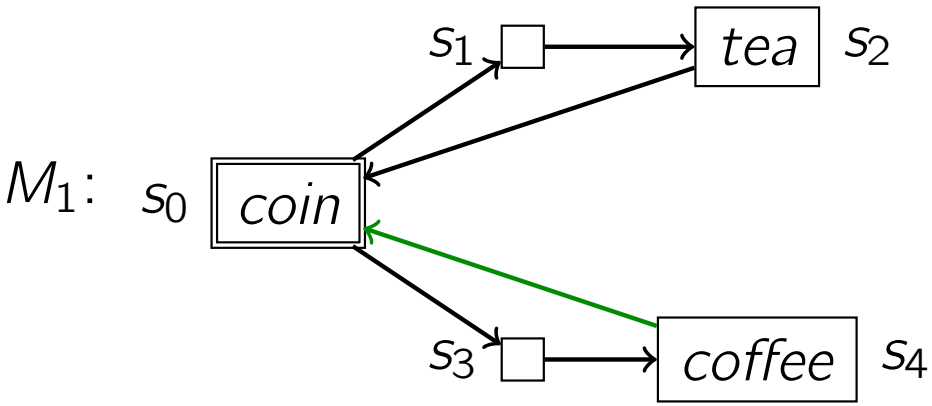
$$\{(s_0, r_0), (s_1, r_1), (s_2, r_2), (s_3, r_1), (s_4, r_3)\}$$

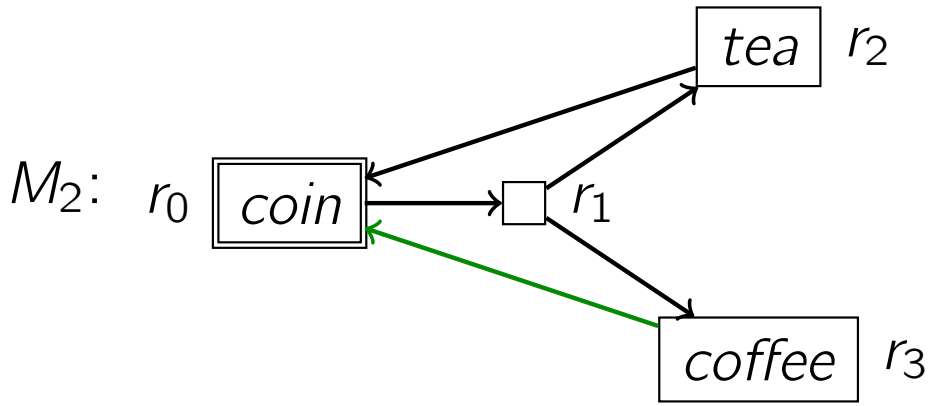
Это несложно проверить:

- Для s_0 в отношении существует пара
- Состояния каждой пары одинаково размечены атомарными высказываниями
- Каждой паре и каждому переходу в первой модели отвечает подходящий переход из парного состояния во второй модели (такой что пара концов переходов входит в отношение)

Отношение симуляции

Пример





Пример отношения симуляции между M_1 и M_2:

$$\{(s_0, r_0), (s_1, r_1), (s_2, r_2), (s_3, r_1), (s_4, r_3)\}$$

Это несложно проверить:

- Для s_0 в отношении существует пара
- Состояния каждой пары одинаково размечены атомарными высказываниями
- Каждой паре и каждому переходу в первой модели отвечает подходящий переход из парного состояния во второй модели (такой что пара концов переходов входит в отношение)

Отношение симуляции

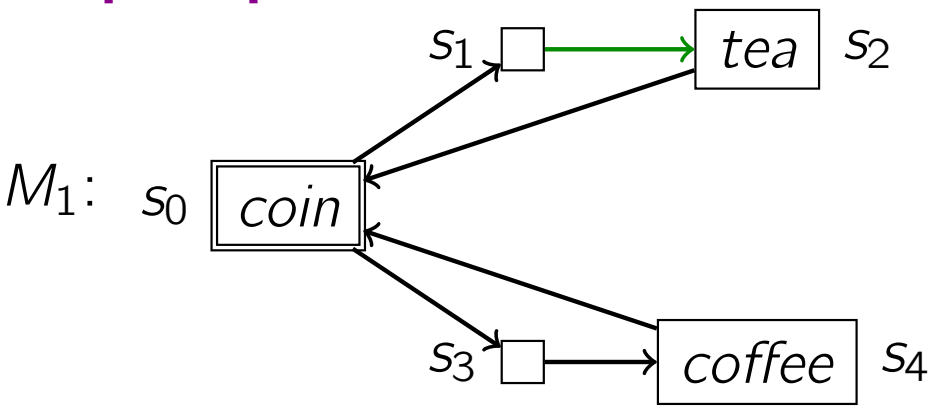
Симуляцию можно представить себе как *игру* между моделями M_1, M_2:

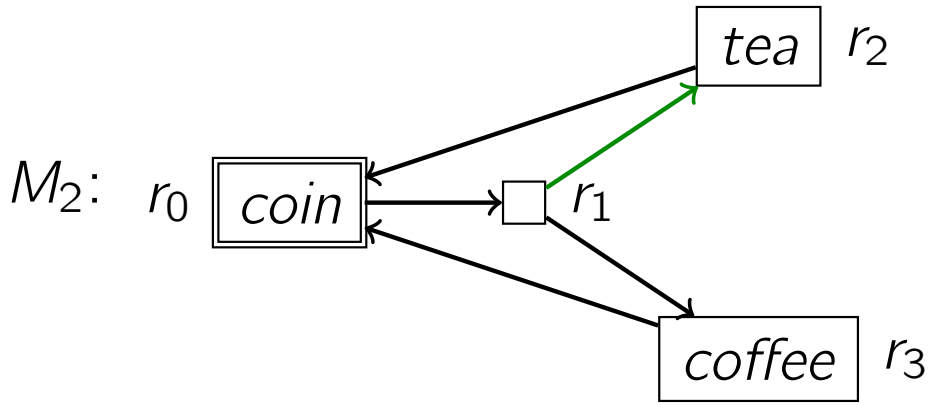
- M_1 выбирает своё начальное состояние
- M_2 выбирает начальное состояние с такой же разметкой
- Затем пошагово происходит следующее:
  - Каждая модель M_i находится в некотором состоянии s_i (на первом шаге — в выбранных начальных состояниях)
  - M_1 выбирает переход из s_1 и выполняет его, изменяя своё текущее состояние
  - M_2 выбирает переход из s_2 так, чтобы перейти в состояние с такой же разметкой
- M_2 проигрывает партию игры, если не может выбрать подходящее начальное состояние или подходящий очередной переход, и выигрывает, если партия бесконечна

Тогда $M_1 \preceq M_2$ означает, что существует *выигрышная стратегия* M_2, то есть способ выбора начального состояния и переходов в ответ на любые действия M_1 так, чтобы выиграть

Отношение симуляции

Например:





Тогда

- пары переходов, которые ранее подсвечивались зелёным для обоснования того, что отношение
$$\{(s_0, r_0), (s_1, r_1), (s_2, r_2), (s_3, r_1), (s_4, r_3)\},$$
является отношением симуляции между M_1 и M_2, и
- пары состояний, входящие в это отношение,

представляют собой соответственно

- выигрышный способ ответного выбора переходов для M_2 и
- всевозможные расклады партии, возникающие при таком способе игры

Отношение симуляции

Утверждение. Отношение $\preceq$ рефлексивно и транзитивно

Доказательство.

Рефлексивность ($M \preceq M$) подтверждается отношением $\{(s, s) \mid s \in S\}$, где S — множество состояний модели M

Транзитивность: если $M_1 \preceq M_2$ и $M_2 \preceq M_3$, то $M_1 \preceq M_3$

Пусть $M_i = (S^i, S^i_0, \rightarrow^i, L^i)$

Рассмотрим отношения $\mathcal{R}_1$ и $\mathcal{R}_2$ симуляции для (M_1, M_2) и для (M_2, M_3) соответственно

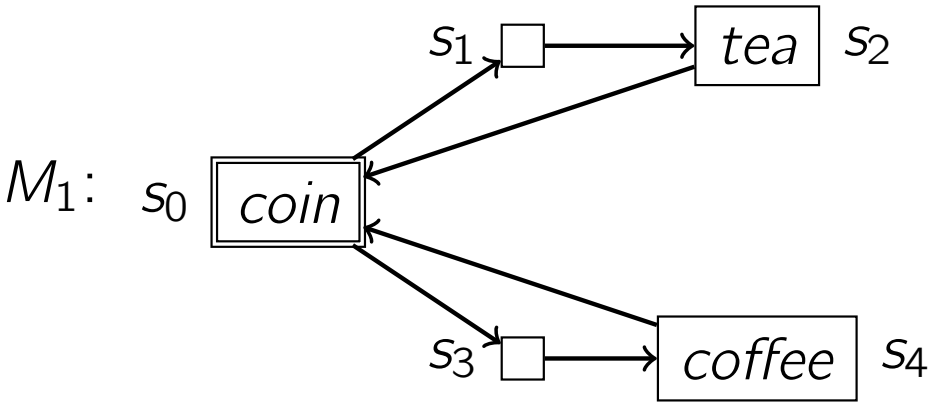
Тогда отношение симуляции $\mathcal{R}$ для M_1 и M_3 может быть устроено так: $\mathcal{R} = \{(s_1, s_3) \mid \exists s_2 : (s_1, s_2) \in \mathcal{R}_1,\ (s_2, s_3) \in \mathcal{R}_2\}$

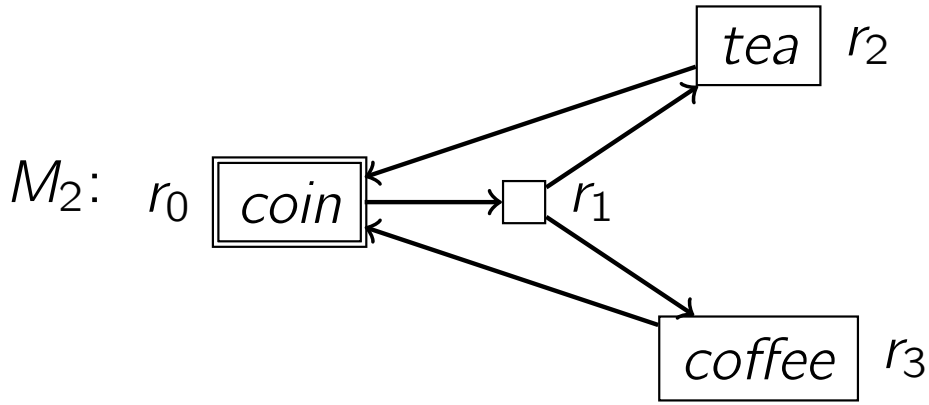
Несложно убедиться, что для этого отношения выполнены все пункты определения симуляции ▼

Симуляционная эквивалентность

Модели M_1 и M_2 симуляционно эквивалентны ($M_1 \sim_s M_2$), если $M_1 \preceq M_2$ и $M_2 \preceq M_1$

Пример



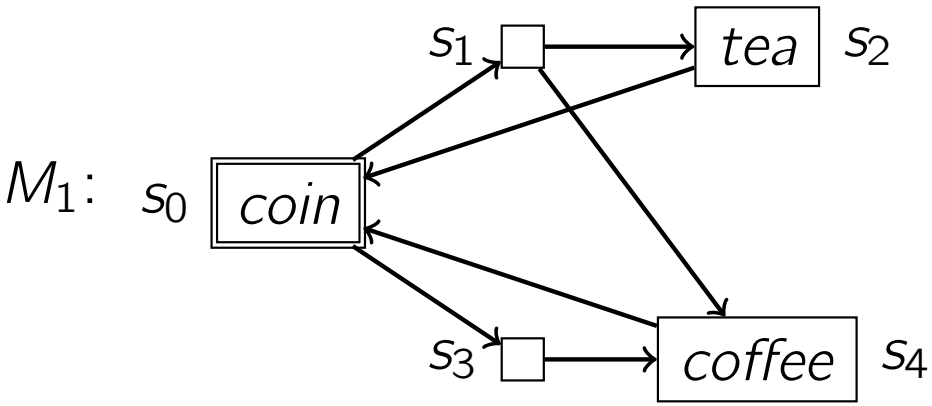


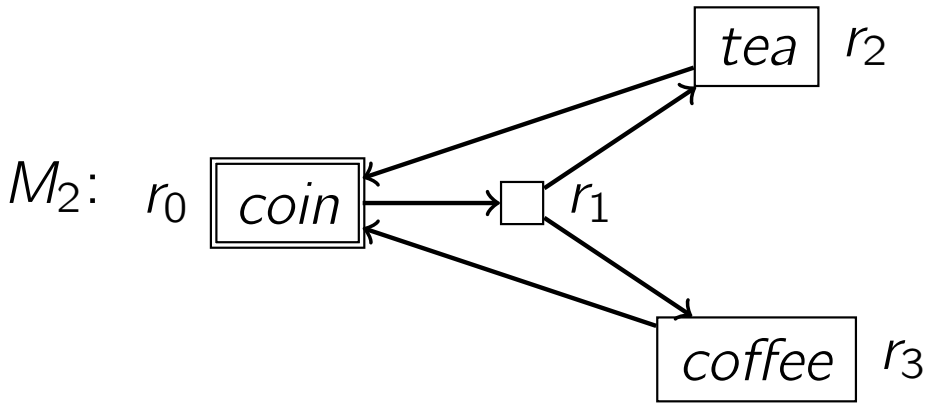
Эти модели не являются симуляционно эквивалентными, т.к. $M_2 \not\preceq M_1$:

- В отношение симуляции $\mathcal{R}$, если оно существует, должна входить хотя бы одна пара вида $(r_1, \_)$
- Согласно функции разметки, для $\mathcal{R}$ могут подойти только пары (r_1, s_1) и (r_1, s_3)
- Ни одна из этих пар не подходит:
  - (r_1, s_1) — т.к. из s_1 не исходит переход, отвечающий $r_1 \to r_3$
  - (r_1, s_3) — т.к. из s_1 не исходит переход, отвечающий $r_1 \to r_2$

Симуляционная эквивалентность

Другой пример





Эти модели симуляционно эквивалентны, что подтверждается такими двумя отношениями симуляции:

- $M_1 \preceq M_2$: $\{(s_0, r_0), (s_1, r_1), (s_2, r_2), (s_3, r_1), (s_4, r_3)\}$
- $M_2 \preceq M_1$: $\{(r_0, s_0), (r_1, s_1), (r_2, s_2), (r_3, s_4)\}$

Утверждение. $\sim_s$ **— отношение эквивалентности**

Доказательство.

Рефлексивность и транзитивность следуют из рефлексивности и транзитивности отношения $\preceq$

Симметричность очевидна: $M_1 \sim_s M_2 \Leftrightarrow M_1 \preceq M_2$ и $M_2 \preceq M_1 \Leftrightarrow M_2 \preceq M_1$ и $M_1 \preceq M_2 \Leftrightarrow M_2 \sim M_1$ ▼

Свойства симуляционной эквивалентности

Будем говорить, что пути π_1, π_2 в моделях Крипке $M_1 = (S^1, S_0^1, \to^1, L^1)$, $M_2 = (S^2, S_0^2, \to^2, L^2)$ $\mathcal{R}$-соответствуют друг другу для отношения $\mathcal{R} \subseteq S^1 \times S^2$, если для любого момента времени k верно $(\pi_1[k], \pi_2[k]) \in \mathcal{R}$

Утверждение. **Для любых**

- **моделей Крипке** $M_1 = (S^1, S_0^1, \to^1, L^1)$, $M_2 = (S^2, S_0^2, \to^2, L^2)$,
- **отношения симуляции** $\mathcal{R}$ **для** M_1 **и** M_2,
- **состояний** $s_1 \in S^1$ **и** $s_2 \in S^2$, **таких что** $(s_1, s_2) \in \mathcal{R}$, **и**
- **пути** π_1 **в** M_1, **исходящего из** s_1

существует $\mathcal{R}$**-соответствующий путь** π_2 **в** M_2, **исходящий из** s_2

Это утверждение несложно доказывается индукцией по длине пути

Следствие. **Если** $M_1 \preceq M_2$, **то** $\mathrm{Tr}(M_1) \subseteq \mathrm{Tr}(M_2)$

Следствие. **Если** $M_1 \sim_s M_2$, **то модели** M_1 **и** M_2 **трассово эквивалентны**

Свойства симуляционной эквивалентности

Actl∗-формулой будем называть ctl*-формулу частного вида, подходящего под БНФ

$$\Phi \quad ::= \quad \mathbb{t} \mid p \mid \neg p \mid (\Phi \,\&\, \Phi) \mid (\Phi \vee \Phi) \mid (\mathbf{A}\varphi),$$
$$\varphi \quad ::= \quad \Phi \mid \varphi \,\&\, \varphi \mid \varphi \vee \varphi \mid (\mathbf{X}\varphi) \mid (\varphi \mathbf{U} \varphi) \mid (\varphi \mathbf{R} \psi),$$

где

- $p \in \mathrm{AP}$ и
- $\varphi \mathbf{R} \psi = \neg(\neg\varphi \mathbf{U} \neg\psi)$

Теорема. **Для любых моделей M_1, M_2, таких что $M_1 \preceq M_2$, и любой actl*-формулы φ, верно:** **если $M_1 \models \varphi$, то $M_2 \models \varphi$**

Можете попробовать сами доказать это индукцией по структуре формулы с использованием последнего утверждения о соответствующих путях (это не очень трудно)

Следствие. **Для любых моделей M_1, M_2, таких что $M_1 \sim_s M_2$, и любой actl*-формулы φ верно:** $M_1 \models \varphi \quad \Leftrightarrow \quad M_2 \models \varphi$

Хотя ACTL* — это достаточно широкий фрагмент CTL* (*шире LTL*), но хотелось бы иметь аналогичное утверждение и про весь язык CTL*

Бисимуляция (отношение, эквивалентность)

Отношение $\mathcal{R}^{-} = \{(y, x) \mid (x, y) \in R\}$ называется обратным к отношению $\mathcal{R} \subseteq X \times Y$

Рассмотрим модели Крипке $M' = (S', S'_0, \to, L')$ и $M'' = (S'', S''_0, \mapsto, L'')$

Отношение $\mathcal{R} \subseteq S' \times S''$ называется отношением бисимуляции между M' и M'', если $\mathcal{R}$ и $\mathcal{R}^{-}$ — отношения симуляции между M' и M'' и между M'' и M' соответственно

Модели M_1 и M_2 бисимуляционно эквивалентны ($M_1 \sim_b M_2$), если существует отношение бисимуляции между этими моделями

Пример

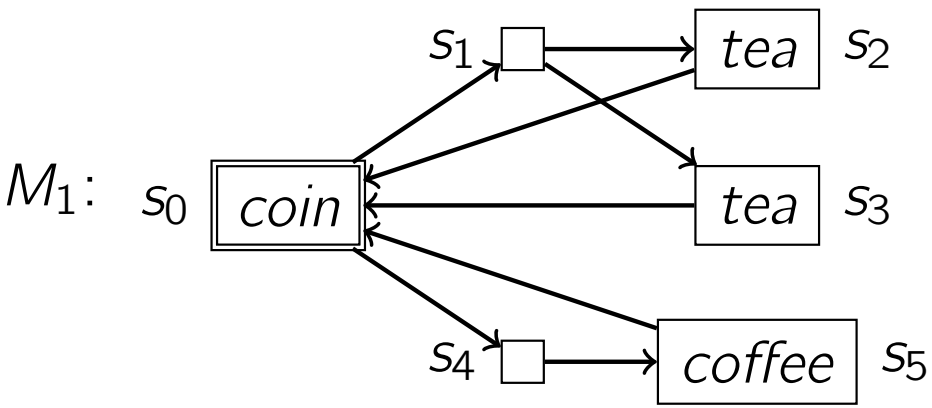
Эти две модели бисимуляционно эквивалентны, что подтверждается таким отношением бисимуляции:

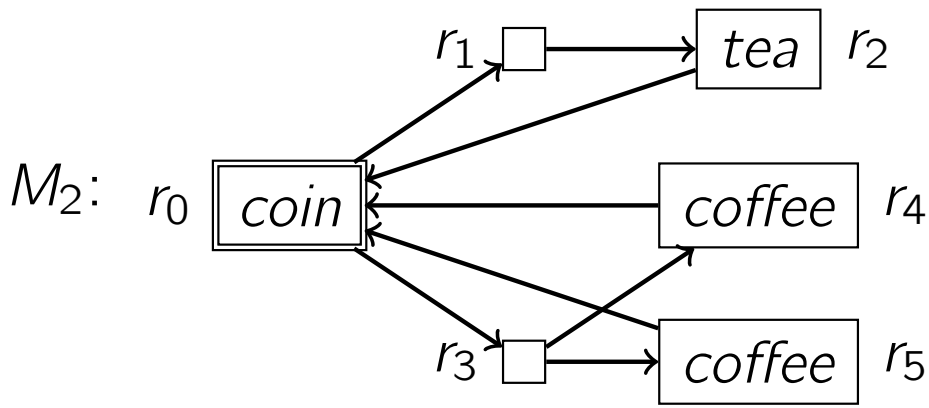
$$\{(s_0, r_0), (s_0, r_2), (s_1, r_1), (s_1, r_3)\}$$

Бисимуляционная эквивалентность похожа на изоморфизм графов, но допускает, в числе прочего, «частичную развёртку» модели

Бисимуляция (отношение, эквивалентность)

Другой пример





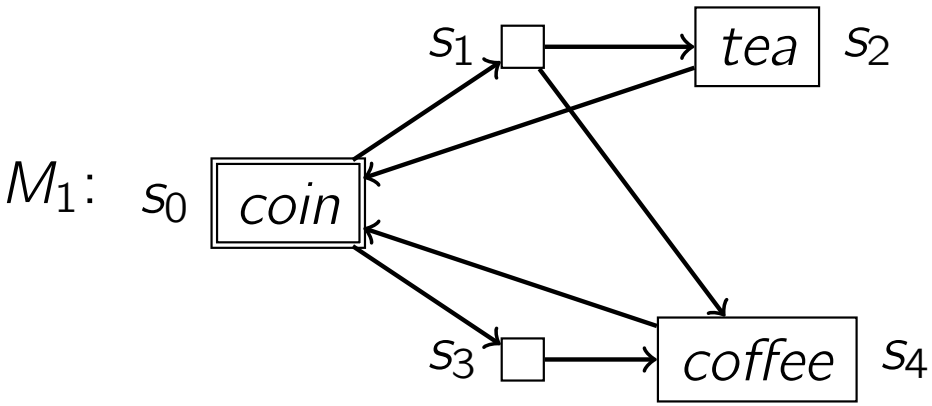
Эти модели бисимуляционно эквивалентны, что подтверждается отношением бисимуляции

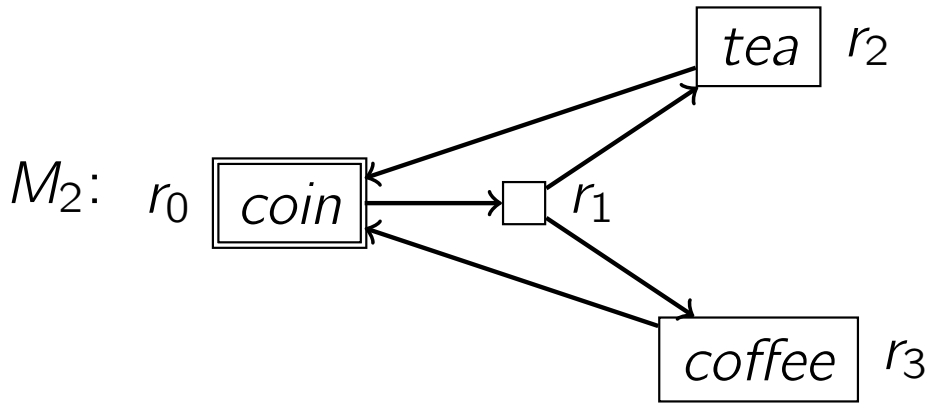
$$\{(s_0, r_0), (s_1, r_1), (s_2, r_2), (s_3, r_2), (s_4, r_3), (s_5, r_4), (s_5, r_5)\}$$

Бисимуляция допускает и «дублирование» состояний в модели

Бисимуляция (отношение, эквивалентность)

И ещё один пример





Ранее было показано, что эти модели симуляционно эквивалентны

Но они не являются бисимуляционно эквивалентными, так как если существует отношение бисимуляции $\mathcal{R}$ между M_1 и M_2, то:

- Так как $\mathcal{R}$ — отношение симуляции между M_1 и M_2, то в нём должна содержаться хотя бы одна пара вида $(s_3, \_)$
- Согласно функции разметки, такой парой может быть только (s_3, r_1)
- Так как $\mathcal{R}^-$ — отношение симуляции между M_2 и M_1 и переходу $r_1 \to r_2$ не соответствует ни один переход из s_3, то пара (s_3, r_1) не может содержаться в $\mathcal{R}$ (*противоречие*)

Бисимуляционная эквивалентность и её свойства

Утверждение. $\sim_b$ **— отношение эквивалентности**

Доказательство. Рефлексивность и транзитивность следуют из того, что

- отношение бисимуляции между двумя моделями является и отношением симуляции между этими моделями
- отношение $\preceq$ рефлексивно и транзитивно

Симметричность очевидна: если $\mathcal{R}$ — отношение бисимуляции между M_1 и M_2, то $\mathcal{R}^-$ — отношение бисимуляции между M_2 и M_1 ▼

Утверждение. Любые две бисимуляционно эквивалентные модели симуляционно эквивалентны

Доказательство. Достаточно заметить, что (по определению) если $\mathcal{R}$ — отношение бисимуляции между M_1 и M_2, то $\mathcal{R}$ и $\mathcal{R}^-$ — отношения симуляции между M_1 и M_2 и между M_2 и M_1 соответственно ▼

Бисимуляционная эквивалентность и её свойства

Утверждение. **Для любых**

- **моделей Крипке** $M_1 = (S^1, S_0^1, \to^1, L^1)$, $M_2 = (S^2, S_0^2, \to^2, L^2)$,
- **отношения бисимуляции** $\mathcal{R}$ **для** M_1 **и** M_2,
- **состояний** $s_1 \in S^1$ **и** $s_2 \in S^2$, **таких что** $(s_1, s_2) \in \mathcal{R}$,
- **номера** i, $i \in \{1, 2\}$ **и**
- **пути** π_i **из** s_i **в** M_i

существует путь π_{3-i} **из** s_{3-i} **в** M_{3-i}, $\mathcal{R}$**-соответствующий** π_i

Это утверждение несложно доказывается индукцией по длине пути

Бисимуляционная эквивалентность и её свойства

Утверждение. **Для любых**

- **бисимуляционно эквивалентных моделей M_1, M_2,**
- **отношения бисимуляции $\mathcal{R}$ между этими моделями,**
- **состояний s_1, s_2 этих моделей, таких что $(s_1, s_2) \in \mathcal{R}$,**
- **$\mathcal{R}$-соответсвующих путей π_1, π_2 в этих моделях,**
- **формулы состояния Φ CTL* и**
- **формулы пути φ CTL***

верны равносильности

$$M_1, s_1 \models \Phi \quad \Leftrightarrow \quad M_2, s_2 \models \Phi$$
$$M_1, \pi_1 \models \varphi \quad \Leftrightarrow \quad M_2, \pi_2 \models \varphi$$

Можете попробовать сами доказать это индукцией по структуре формулы с привлечением предыдущего утверждения

Бисимуляционная эквивалентность и её свойства

Теорема. **Для любых бисимуляционно эквивалентных моделей M_1, M_2 и любой ctl*-формулы φ верно:**

$$M_1 \models \varphi \quad \Leftrightarrow \quad M_2 \models \varphi$$

Итого определено 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 для спецификации модели M_1 используется фрагмент $\mathcal{L}$, то можно быть уверенным в том, что на любой модель M_2, такая что $M_1 \sim M_2$ для соответствующего $\sim$, настолько же удовлетворяет всем спецификациям, насколько и M_1