Верификация моделей программ

ЛЕКТОР:

Владимир Анатольевич Захаров
Владислав Васильевич Подымов

zakh@cs.msu.su

Лекция 8.

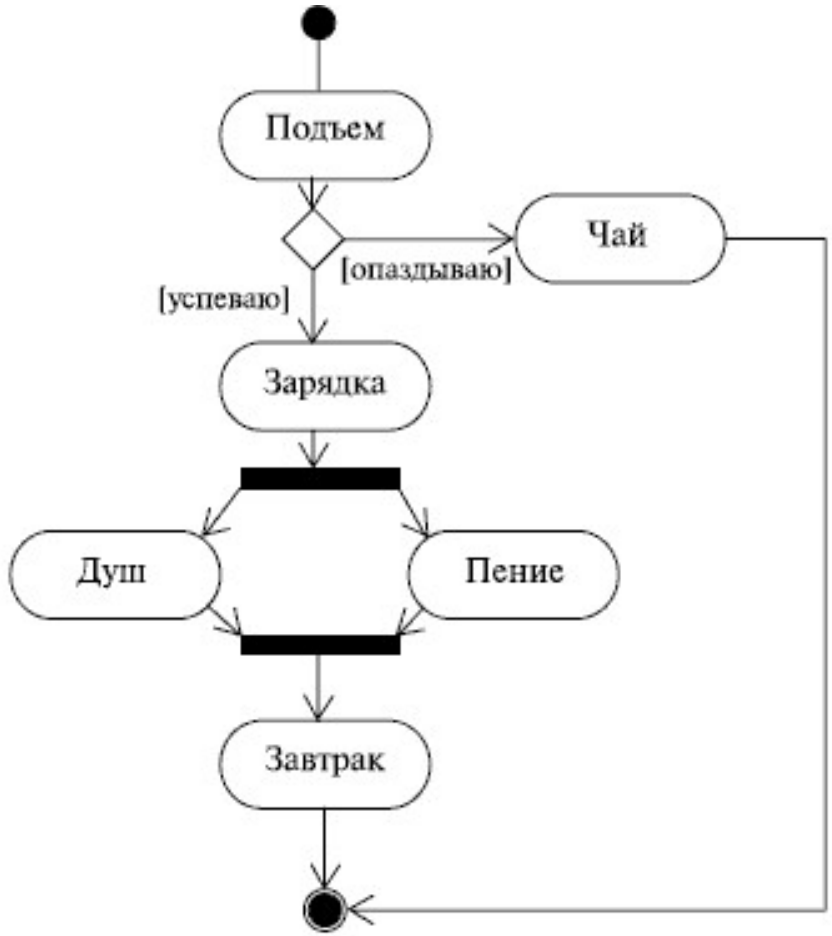
Бисимуляция, симуляция и абстракция моделей

1. Отношение бисимуляции и его свойства
2. Вычисление бисимуляционной эквивалентности
3. Отношения симуляции
4. Абстракция моделей
5. Редукция по конусу влияния
6. Абстракция данных

Модели простые и сложные

Модели информационных систем бывают разные.

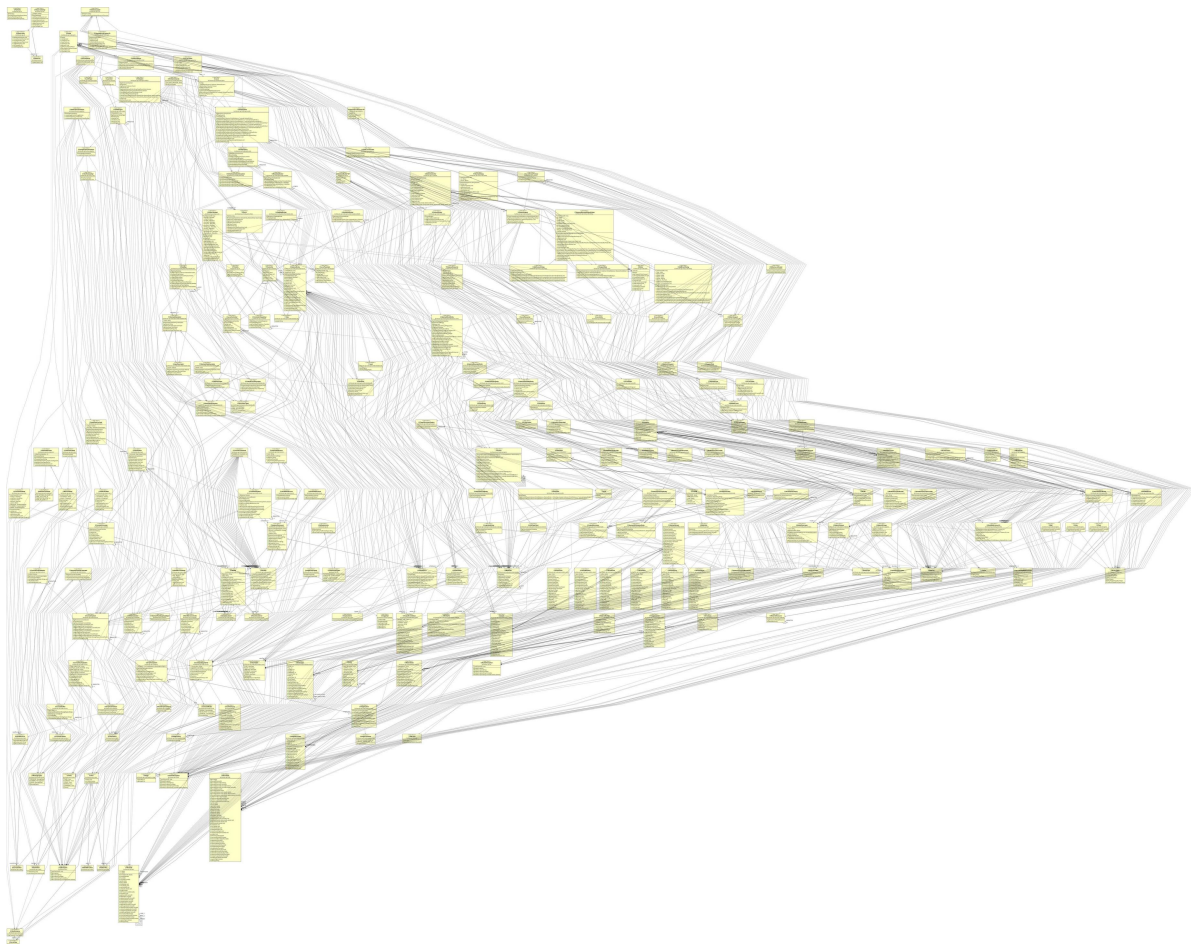
Бывают модели простые:



Модели простые и сложные

Модели информационных систем бывают разные.

И бывают сложные:



Модели простые и сложные

Сложные модели позволяют

- наиболее точно описывать устройство и поведение моделируемого объекта,
- наиболее подробно воспроизводить детали поведения («мелко гранулированные модели»),

но требуют значительных вычислительных ресурсов для их построения и анализа .

Модели простые и сложные

Сложные модели позволяют

- наиболее точно описывать устройство и поведение моделируемого объекта,
- наиболее подробно воспроизводить детали поведения («мелко гранулированные модели»),

но требуют значительных вычислительных ресурсов для их построения и анализа .

Простые модели не дают возможности увидеть подробности устройства моделируемого объекта и/или могут лишь весьма грубо (с небольшой точностью) описывать его поведение, но зато простые модели

- легко строить и
- легко анализировать .

Модели простые и сложные

Сложные модели позволяют

- наиболее точно описывать устройство и поведение моделируемого объекта,
- наиболее подробно воспроизводить детали поведения («мелко гранулированные модели»),

но требуют значительных вычислительных ресурсов для их построения и анализа .

Простые модели не дают возможности увидеть подробности устройства моделируемого объекта и/или могут лишь весьма грубо (с небольшой точностью) описывать его поведение, но зато простые модели

- легко строить и
- легко анализировать .

А нельзя ли воспользоваться достоинствами простых моделей для построения и анализа сложных моделей?

Модели простые и сложные

СЦЕНАРИЙ 1

Модель M была построена, и было проверено, что она удовлетворяет множеству спецификаций $\{\varphi_1, \ldots, \varphi_N\}$.

Однако позднее за счет улучшений, внедрения новых идей, изменений модель M была преобразована в модель M' .

Модели простые и сложные

СЦЕНАРИЙ 1

Модель M была построена, и было проверено, что она удовлетворяет множеству спецификаций $\{\varphi_1, \ldots, \varphi_N\}$.

Однако позднее за счет улучшений, внедрения новых идей, изменений модель M была преобразована в модель M' .

Можно ли, сравнив модели M и M' , убедиться в том, что в модели M' также выполняется множество спецификаций $\{\varphi_1, \ldots, \varphi_N\}$?

Модели простые и сложные

СЦЕНАРИЙ 1

Модель M была построена, и было проверено, что она удовлетворяет множеству спецификаций $\{\varphi_1, \ldots, \varphi_N\}$.

Однако позднее за счет улучшений, внедрения новых идей, изменений модель M была преобразована в модель M' .

Можно ли, сравнив модели M и M' , убедиться в том, что в модели M' также выполняется множество спецификаций $\{\varphi_1, \ldots, \varphi_N\}$?

Да, если удастся обнаружить такое отношение $\sim$ (отношение бисимуляции), для которого верно соотношение

$$M \sim M' \implies \forall\, \varphi\, (M \models \varphi \;\Leftrightarrow\; M' \models \varphi).$$

Модели простые и сложные

СЦЕНАРИЙ 2

Сложная информационная система строится инкрементально: на каждом i -ом этапе построения более простая модель M_i за счет уточнения некоторых ее компонентов преобразуется в более сложную модель M_{i+1} .

Чтобы проверять корректность уточнений, на каждом этапе проверяются некоторые требования к проектируемой системе.

Модели простые и сложные

СЦЕНАРИЙ 2

Сложная информационная система строится инкрементально: на каждом i -ом этапе построения более простая модель M_i за счет уточнения некоторых ее компонентов преобразуется в более сложную модель M_{i+1} .

Чтобы проверять корректность уточнений, на каждом этапе проверяются некоторые требования к проектируемой системе.

Можно ли, сравнив модели M_i и M_{i+1} , убедиться в том, что модель M_{i+1} удовлетворяет всем тем требованиям, которые были проверены для моделей $M_1, M_2, \ldots, M_i$?

Модели простые и сложные

СЦЕНАРИЙ 2

Сложная информационная система строится инкрементально: на каждом i -ом этапе построения более простая модель M_i за счет уточнения некоторых ее компонентов преобразуется в более сложную модель M_{i+1} .

Чтобы проверять корректность уточнений, на каждом этапе проверяются некоторые требования к проектируемой системе.

Можно ли, сравнив модели M_i и M_{i+1} , убедиться в том, что модель M_{i+1} удовлетворяет всем тем требованиям, которые были проверены для моделей $M_1, M_2, \ldots, M_i$?

Да, если удастся обнаружить такое отношение $\prec$ (отношение симуляции), для которого верно соотношение

$$M \prec M' \implies \forall\, \varphi\, (M \models \varphi \;\Rightarrow\; M' \models \varphi).$$

Модели простые и сложные

СЦЕНАРИЙ 3

Из-за недостатка вычислительных ресурсов невозможно проверить выполнимость спецификации φ для сложной модели M .

Модели простые и сложные

СЦЕНАРИЙ 3

Из-за недостатка вычислительных ресурсов невозможно проверить выполнимость спецификации φ для сложной модели M .

Можно ли для заданной модели M и спецификации φ построить такую модель M' (абстракцию модели M), для которой

- гораздо проще решать задачу верификации моделей программ, и
- верно соотношение $M' \models \varphi \implies M \models \varphi$.

Модели простые и сложные

Как известно, для любой LTL формулы φ и для любой модели M

$$M \models \varphi \Leftrightarrow \forall tr \in Trace(M) \;\; tr \models \varphi.$$

Почему бы тогда не сравнивать модели M_1 и M_2 , сопоставляя множества их трасс $Trace(M_1)$ и $Trace(M_2)$?
Например, объявляя $M_1 \approx M_2$ тогда и только тогда, когда $Trace(M_1) = Trace(M_2)$?

Модели простые и сложные

Как известно, для любой LTL формулы φ и для любой модели M

$$M \models \varphi \Leftrightarrow \forall tr \in Trace(M) \;\; tr \models \varphi.$$

Почему бы тогда не сравнивать модели M_1 и M_2 , сопоставляя множества их трасс $Trace(M_1)$ и $Trace(M_2)$?
Например, объявляя $M_1 \approx M_2$ тогда и только тогда, когда $Trace(M_1) = Trace(M_2)$?

Это нецелесообразно по двум причинам:

Модели простые и сложные

Как известно, для любой LTL формулы φ и для любой модели M

$$M \models \varphi \Leftrightarrow \forall tr \in Trace(M) \;\; tr \models \varphi.$$

Почему бы тогда не сравнивать модели M_1 и M_2 , сопоставляя множества их трасс $Trace(M_1)$ и $Trace(M_2)$?
Например, объявляя $M_1 \approx M_2$ тогда и только тогда, когда $Trace(M_1) = Trace(M_2)$?

Это нецелесообразно по двум причинам:

1. Равенство множества трасс не поддерживает равновыполнимость формул других логик, например, CTL.

Модели простые и сложные

Как известно, для любой LTL формулы φ и для любой модели M

$$M \models \varphi \;\Leftrightarrow\; \forall tr \in Trace(M)\;\; tr \models \varphi.$$

Почему бы тогда не сравнивать модели M_1 и M_2 , сопоставляя множества их трасс $Trace(M_1)$ и $Trace(M_2)$?
Например, объявляя $M_1 \approx M_2$ тогда и только тогда, когда $Trace(M_1) = Trace(M_2)$?

Это нецелесообразно по двум причинам:

1. Равенство множества трасс не поддерживает равновыполнимость формул других логик, например, CTL.
2. Проверка отношения равенства множеств трасс конечных моделей — это вычислительно сложная (PSPACE-полная) задача.

Поэтому нужны другие, более «простые» отношения сравнения моделей.

Отношение бисимуляции и его свойства

Будем заниматься сравнением моделей информационных систем, заданных в виде моделей Крипке (размеченных систем переходов, LTS) $M = (AP, S, R, S_0, L)$, где

- AP — множество атомарных высказываний;
- S — множество состояний модели;
- $R,\ R \subseteq S \times S$ — тотальное отношение переходов;
- $S_0,\ S_0 \subseteq S$ — множество начальных состояний;
- $L : S \to 2^{AP}$ — функция разметки.

Отношение бисимуляции и его свойства

Определение бисимуляции моделей

Пусть заданы две модели (LTS) с одним и тем же множеством атомарных высказываний AP :
$M = (AP, S, R, S_0, L)$ и $M' = (AP, S', R', S'_0, L')$

Отношение бисимуляции и его свойства

Определение бисимуляции моделей

Пусть заданы две модели (LTS) с одним и тем же множеством атомарных высказываний AP :
$M = (AP, S, R, S_0, L)$ и $M' = (AP, S', R', S'_0, L')$

Отношение $B \subseteq S \times S'$ называется **отношением бисимуляции** между M и M' , если для любой пары состояний s и s' , находящихся в отношении $B(s, s')$, выполняются следующие условия:

Отношение бисимуляции и его свойства

Определение бисимуляции моделей

Пусть заданы две модели (LTS) с одним и тем же множеством атомарных высказываний AP :
$M = (AP, S, R, S_0, L)$ и $M' = (AP, S', R', S'_0, L')$

Отношение $B \subseteq S \times S'$ называется **отношением бисимуляции** между M и M' , если для любой пары состояний s и s' , находящихся в отношении $B(s, s')$, выполняются следующие условия:

1) $L(s) = L'(s')$;

Отношение бисимуляции и его свойства

Определение бисимуляции моделей

Пусть заданы две модели (LTS) с одним и тем же множеством атомарных высказываний AP :
$M = (AP, S, R, S_0, L)$ и $M' = (AP, S', R', S'_0, L')$

Отношение $B \subseteq S \times S'$ называется **отношением бисимуляции** между M и M' , если для любой пары состояний s и s' , находящихся в отношении $B(s, s')$, выполняются следующие условия:

1) $L(s) = L'(s')$;
2) Для любого состояния s_1 , для которого выполняется отношение $R(s, s_1)$, найдется состояние s'_1 , для которого выполняются отношения $R'(s', s'_1)$ и $B(s_1, s'_1)$;

Отношение бисимуляции и его свойства

Определение бисимуляции моделей

Пусть заданы две модели (LTS) с одним и тем же множеством атомарных высказываний AP :
$M = (AP, S, R, S_0, L)$ и $M' = (AP, S', R', S'_0, L')$

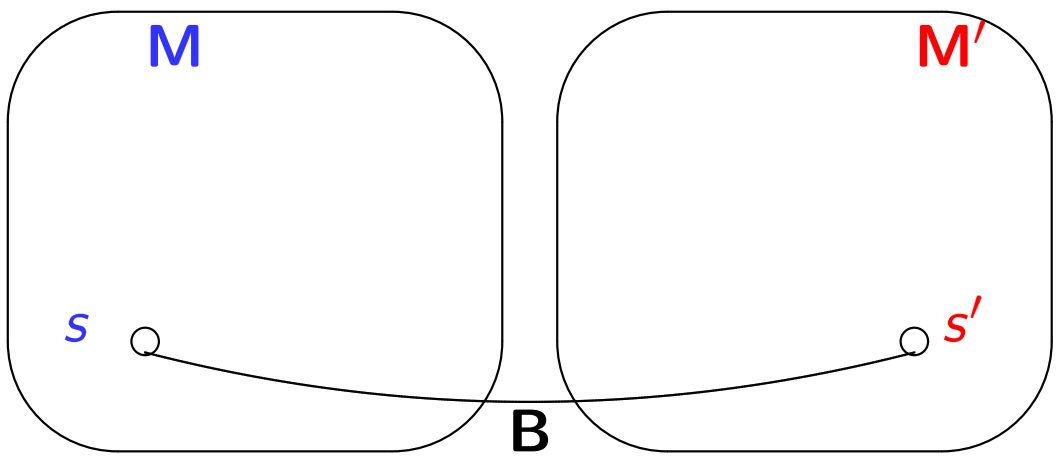
Отношение $B \subseteq S \times S'$ называется **отношением бисимуляции** между M и M' , если для любой пары состояний s и s' , находящихся в отношении $B(s, s')$, выполняются следующие условия:

1) $L(s) = L'(s')$;
2) Для любого состояния s_1 , для которого выполняется отношение $R(s, s_1)$, найдется состояние s'_1 , для которого выполняются отношения $R'(s', s'_1)$ и $B(s_1, s'_1)$;
3) Для любого состояния s'_1 , для которого выполняется отношение $R(s', s'_1)$, найдется состояние s_1 , для которого выполняются отношения $R(s, s_1)$ и $B(s_1, s'_1)$.

Отношение бисимуляции и его свойства

Иллюстрация определения бисимуляции

Для любой пары состояний s и s' , находящихся в отношении $B(s, s')$, выполняются следующие условия:

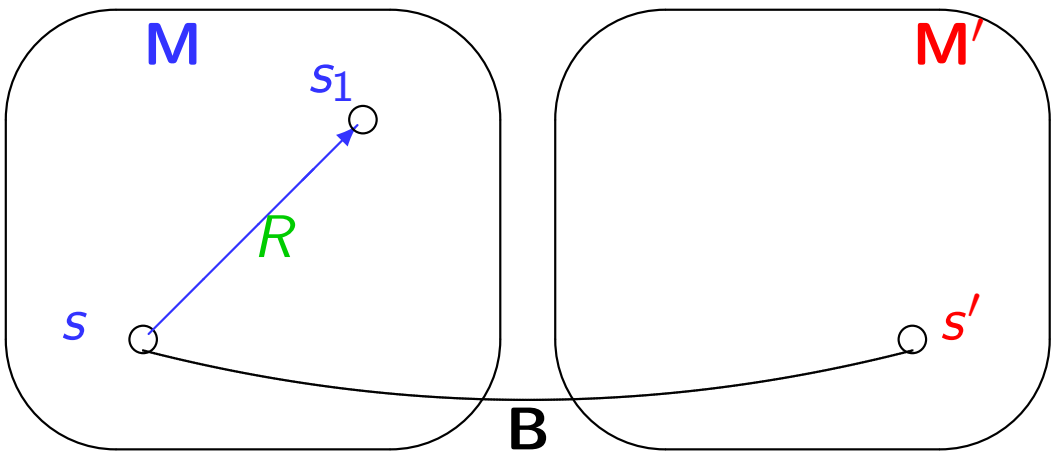


Отношение бисимуляции и его свойства

Иллюстрация определения бисимуляции

Для любой пары состояний s и s' , находящихся в отношении $B(s, s')$, выполняются следующие условия:

2) Для любого состояния s_1 , для которого выполняется отношение $R(s, s_1)$,

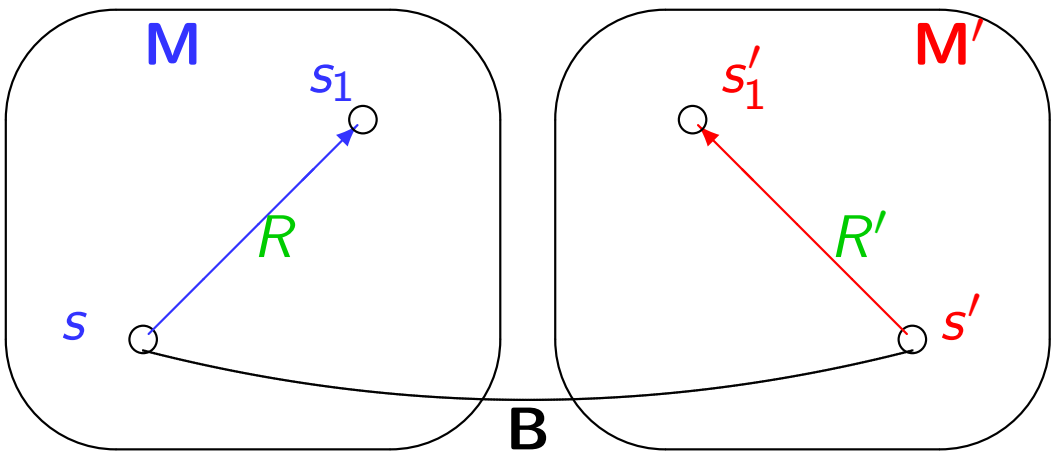


Отношение бисимуляции и его свойства

Иллюстрация определения бисимуляции

Для любой пары состояний s и s' , находящихся в отношении $B(s, s')$, выполняются следующие условия:

2) Для любого состояния s_1 , для которого выполняется отношение $R(s, s_1)$, найдется состояние s'_1 , для которого выполняются отношения $R'(s', s'_1)$

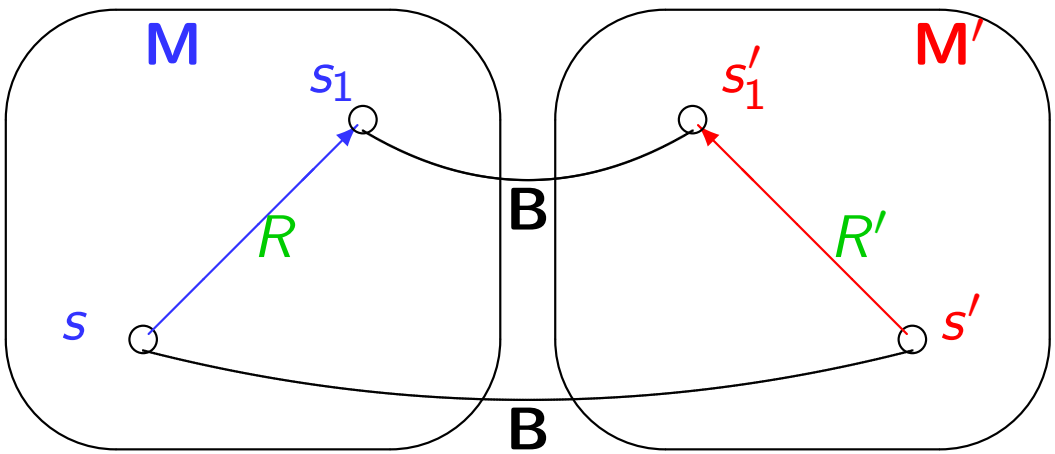


Отношение бисимуляции и его свойства

Иллюстрация определения бисимуляции

Для любой пары состояний s и s' , находящихся в отношении $B(s, s')$, выполняются следующие условия:

2) Для любого состояния s_1 , для которого выполняется отношение $R(s, s_1)$, найдется состояние s'_1 , для которого выполняются отношения $R'(s', s'_1)$ и $B(s_1, s'_1)$;

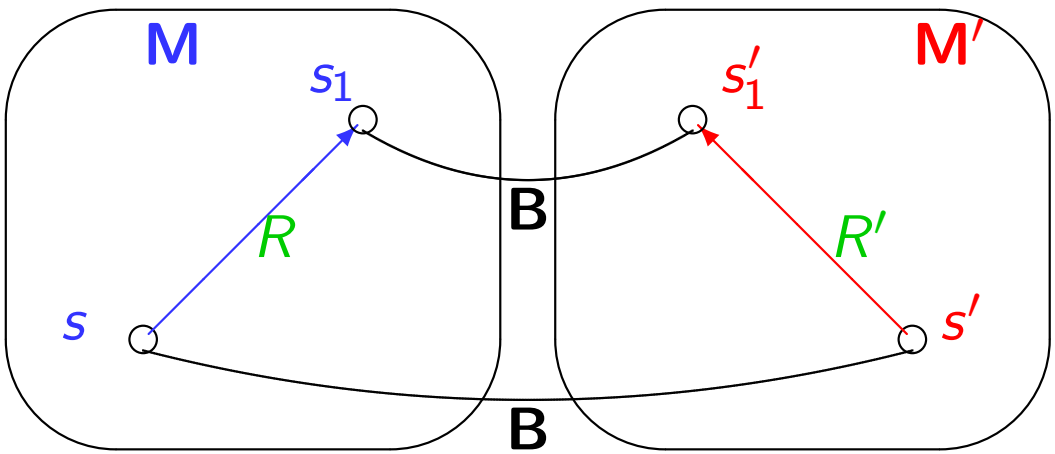


Отношение бисимуляции и его свойства

Иллюстрация определения бисимуляции

Для любой пары состояний s и s' , находящихся в отношении $B(s, s')$, выполняются следующие условия:

2) Для любого состояния s_1 , для которого выполняется отношение $R(s, s_1)$, найдется состояние s'_1 , для которого выполняются отношения $R'(s', s'_1)$ и $B(s_1, s'_1)$;



И НАОБОРОТ

Отношение бисимуляции и его свойства

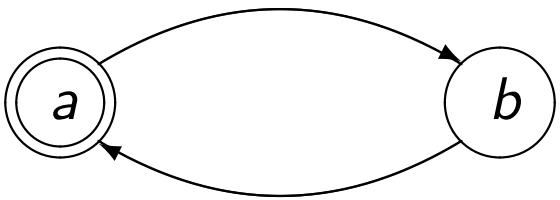
Определение бисимуляции

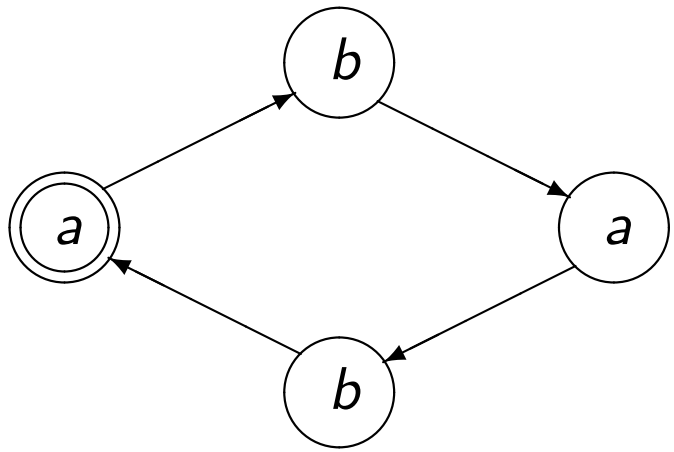
Модели M и M' считаются бисимуляционно эквивалентными (обозначается $M \sim M'$), если существует такое отношение бисимуляции B , что

- для всякого начального состояния s_0 из S_0 в модели M найдется начальное состояние s'_0 из S'_0 в модели M' , для которого выполняется отношение $B(s_0, s'_0)$,
- и для всякого начального состояния s'_0 из S'_0 в модели M' найдется начальное состояние s_0 из S_0 в модели M , для которого выполняется отношение $B(s_0, s'_0)$.

Отношение бисимуляции и его свойства

Примеры к определению бисимуляции





Отношение бисимуляции и его свойства

Примеры к определению бисимуляции

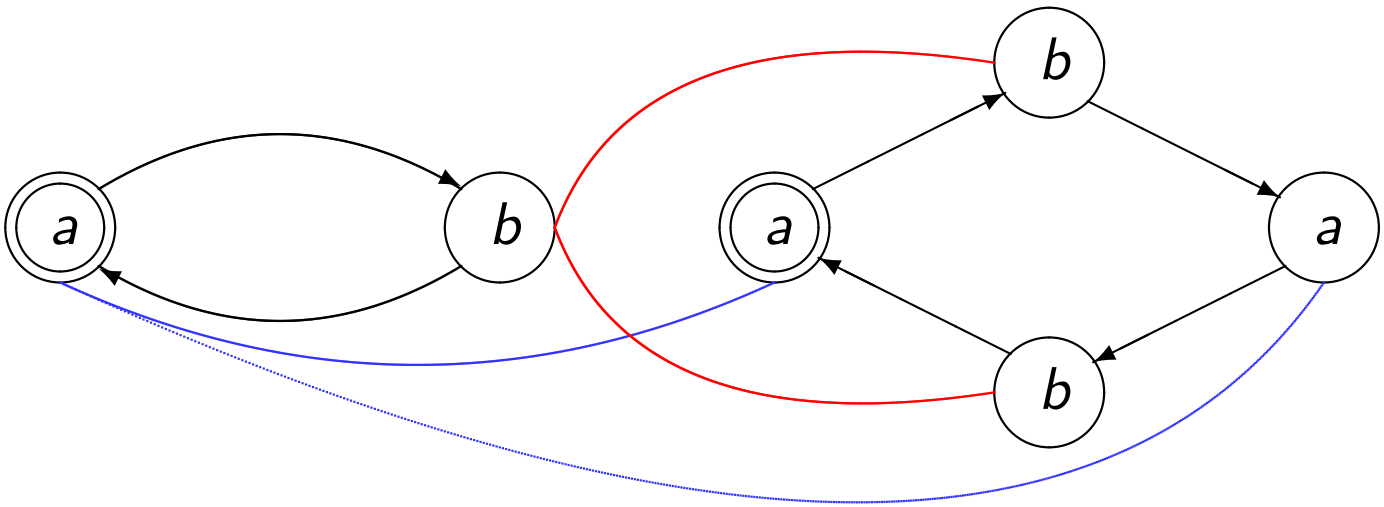


Рис.: Развертка сохраняет бисимуляцию

Отношение бисимуляции и его свойства

Примеры к определению бисимуляции

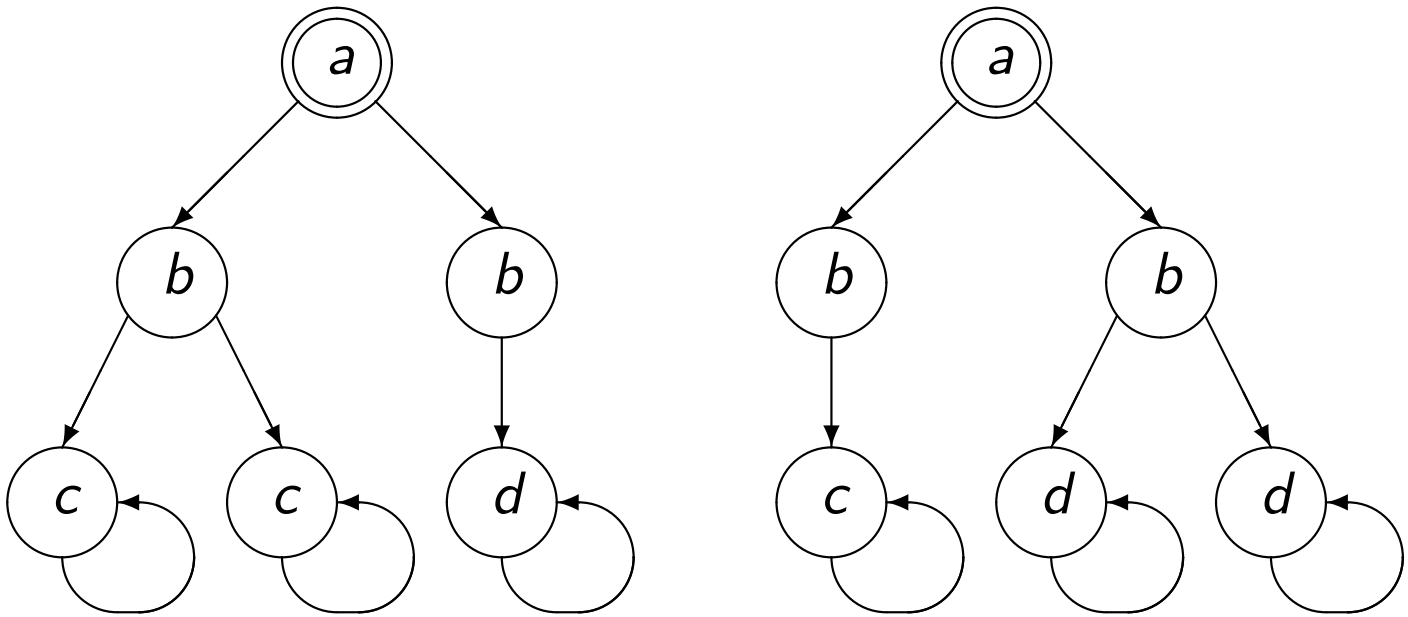


Рис.: Дублирование сохраняет бисимуляцию

Отношение бисимуляции и его свойства

Примеры к определению бисимуляции

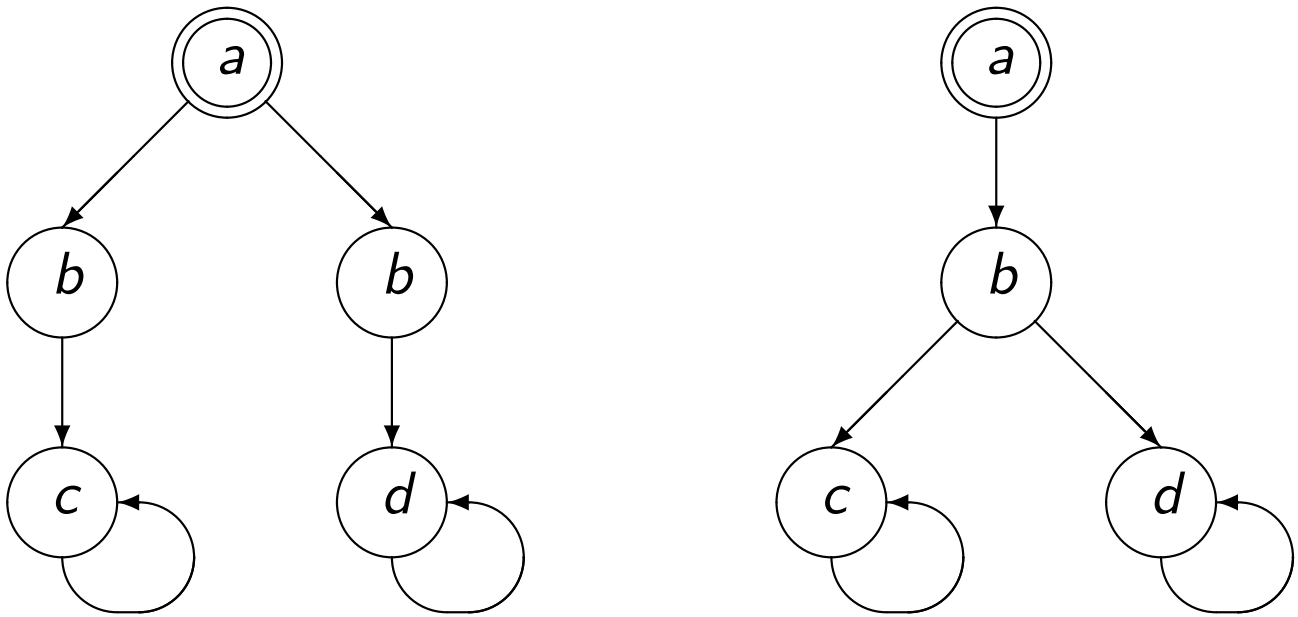


Рис.: Две бисимуляционно неэквивалентные модели

Отношение бисимуляции и его свойства

Утверждение 1.

Отношение бисимуляции $\sim$ — это отношение эквивалентности.

Отношение бисимуляции и его свойства

Утверждение 1.

Отношение бисимуляции $\sim$ — это отношение эквивалентности.

Будем говорить, что два пути $\pi = s_0, s_1, \ldots$ в модели M и $\pi' = s'_0, s'_1, \ldots$ в модели M' соответствуют друг другу , если для любого i, $i \geq 0$, справедливо отношение $B(s_i, s'_i)$.

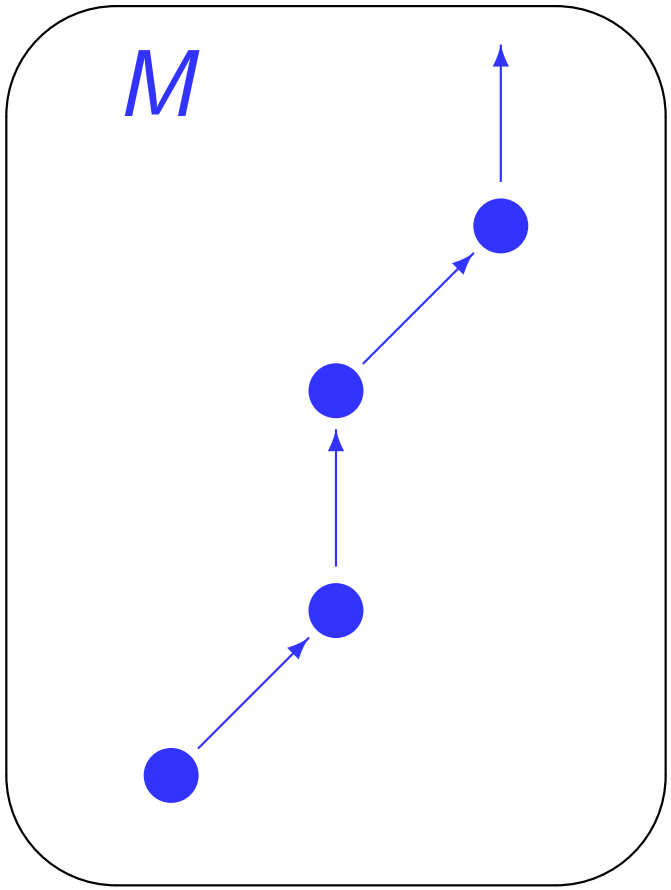
Утверждение 2.

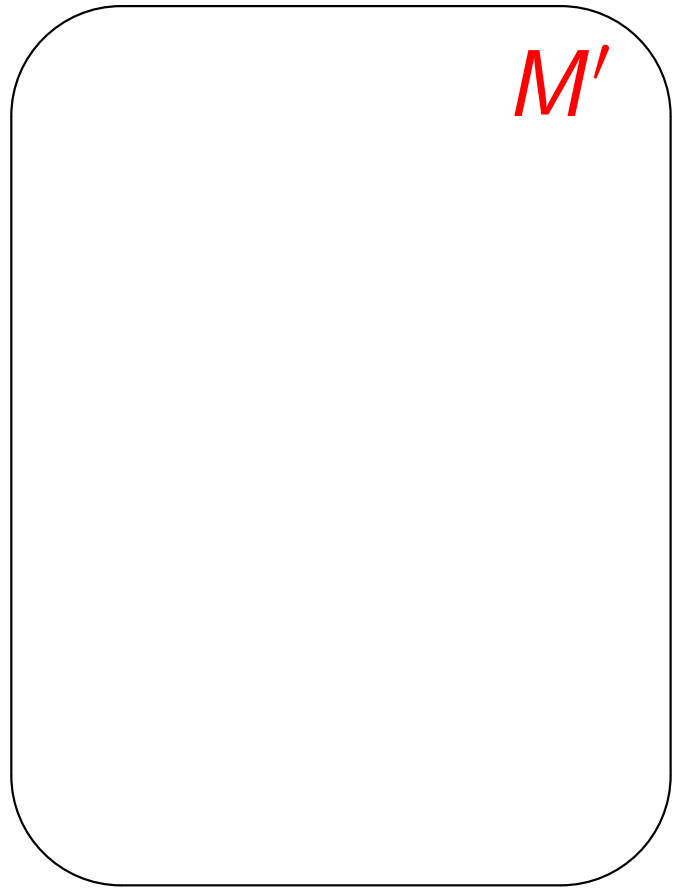
Пусть s и s' — два состояния, для которых выполняется $B(s, s')$. Тогда для всякого пути, начинающегося из s , найдется соответствующий ему путь, начинающийся из s' , и наоборот, для всякого пути, начинающегося из s' , найдется соответствующий ему путь, начинающийся из s .

Отношение бисимуляции и его свойства

Иллюстрация к Утверждению 2.

Для любого пути в одной модели

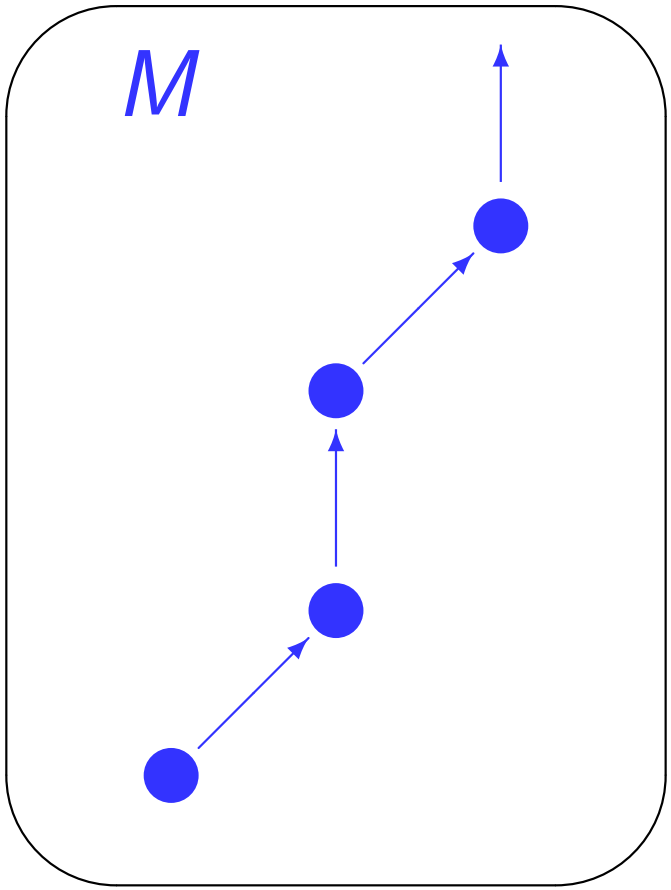


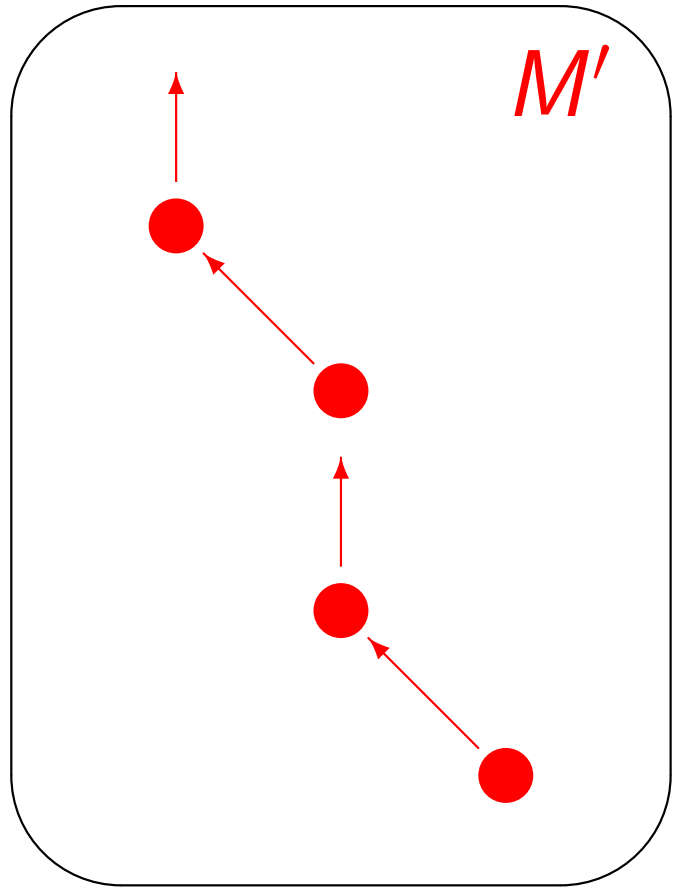


Отношение бисимуляции и его свойства

Иллюстрация к Утверждению 2.

Для любого пути в одной модели существует путь в другой модели,

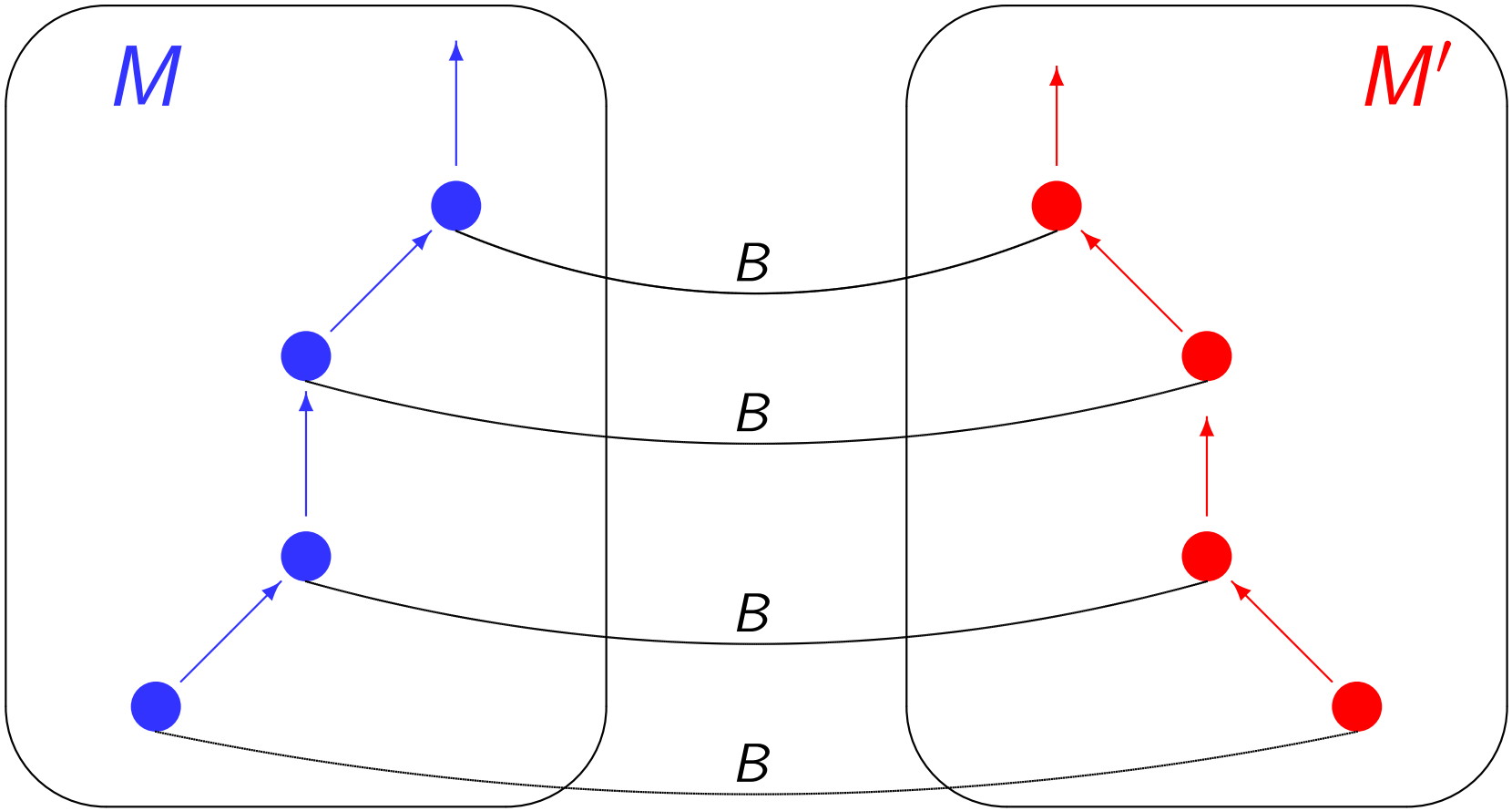




Отношение бисимуляции и его свойства

Иллюстрация к Утверждению 2.

Для любого пути в одной модели существует путь в другой модели, который соответствует первому пути.



Отношение бисимуляции и его свойства

Утверждение 3.

Пусть φ — это либо формула пути, либо формула состояния логики CTL*.
Предположим, что модели M и M' бисимуляционно эквивалентны, состояния s и s' таковы, что $(s, s') \in B$, а пути π и π' соответствуют друг другу.
Тогда

- если φ — это формула состояния, то $M, s \models \varphi \Leftrightarrow M', s' \models \varphi$;
- если φ — это формула пути, то $M, \pi \models \varphi \Leftrightarrow M', \pi' \models \varphi$.

Отношение бисимуляции и его свойства

Утверждение 3.

Пусть φ — это либо формула пути, либо формула состояния логики CTL*.
Предположим, что модели M и M' бисимуляционно эквивалентны, состояния s и s' таковы, что $(s, s') \in B$, а пути π и π' соответствуют друг другу.
Тогда

- если φ — это формула состояния, то $M, s \models \varphi \Leftrightarrow M', s' \models \varphi$;
- если φ — это формула пути, то $M, \pi \models \varphi \Leftrightarrow M', \pi' \models \varphi$.

Доказательство.

Индукцией по структуре формулы.

Отношение бисимуляции и его свойства

Теорема 1.

Если выполняется отношение $M \sim M'$, то для любой CTL* формулы φ мы имеем

$$M \models \varphi \Leftrightarrow M' \models \varphi.$$

Отношение бисимуляции и его свойства

Теорема 1.

Если выполняется отношение $M \sim M'$, то для любой CTL* формулы φ мы имеем

$$M \models \varphi \Leftrightarrow M' \models \varphi.$$

Обратная теорема также верна.

Если две модели удовлетворяют одному и тому же множеству CTL*-формул, то они бисимуляционно эквивалентны.

Отношение бисимуляции и его свойства

Теорема 1.

Если выполняется отношение $M \sim M'$, то для любой CTL* формулы φ мы имеем

$$M \models \varphi \Leftrightarrow M' \models \varphi.$$

Обратная теорема также верна.

Если две модели удовлетворяют одному и тому же множеству CTL*-формул, то они бисимуляционно эквивалентны.

Таким образом, если модель M' , образовалась в результате преобразования модели M , удовлетворяющей заданным CTL*-спецификациям, то для верификации модели M' достаточно проверить бисимуляционную эквивалентность $M' \sim M$.

Как это сделать?

Отношение бисимуляции и его свойства

Определение бисимуляции состояний

Пусть задана модель $M = (AP, S, R, S_0, L)$

Отношение $B \subseteq S \times S$ называется **отношением бисимуляции** на модели M , если для любой пары состояний s_1 и s_2 , находящихся в отношении $B(s_1, s_2)$, выполняются следующие условия:

Отношение бисимуляции и его свойства

Определение бисимуляции состояний

Пусть задана модель $M = (AP, S, R, S_0, L)$

Отношение $B \subseteq S \times S$ называется **отношением бисимуляции** на модели M , если для любой пары состояний s_1 и s_2 , находящихся в отношении $B(s_1, s_2)$, выполняются следующие условия:

1) $L(s_1) = L(s_2)$;

Отношение бисимуляции и его свойства

Определение бисимуляции состояний

Пусть задана модель $M = (AP, S, R, S_0, L)$

Отношение $B \subseteq S \times S$ называется **отношением бисимуляции** на модели M , если для любой пары состояний s_1 и s_2 , находящихся в отношении $B(s_1, s_2)$, выполняются следующие условия:

1) $L(s_1) = L(s_2)$;
2) Для любого состояния t_1 , для которого выполняется отношение $R(s_1, t_1)$, найдется состояние t_2 , для которого выполняются отношения $R(s_2, t_2)$ и $B(t_1, t_2)$;

Отношение бисимуляции и его свойства

Определение бисимуляции состояний

Пусть задана модель $M = (AP, S, R, S_0, L)$

Отношение $B \subseteq S \times S$ называется **отношением бисимуляции** на модели M , если для любой пары состояний s_1 и s_2 , находящихся в отношении $B(s_1, s_2)$, выполняются следующие условия:

1) $L(s_1) = L(s_2)$;
2) Для любого состояния t_1 , для которого выполняется отношение $R(s_1, t_1)$, найдется состояние t_2 , для которого выполняются отношения $R(s_2, t_2)$ и $B(t_1, t_2)$;
3) Для любого состояния t_2 , для которого выполняется отношение $R(s_2, t_2)$, найдется состояние t_1 , для которого выполняются отношения $R(s_1, t_1)$ и $B(t_1, t_2)$.

Отношение бисимуляции и его свойства

Определение бисимуляционной эквивалентности состояний

Два состояния s_1 и s_2 модели $M = (AP, S, R, S_0, L)$ называются бисимуляционно эквивалентными (обозначается $s_1 \approx s_2$), если существует такое отношение бисимуляции B на модели M , для которого выполняется соотношение $B(s_1, s_2)$.

Отношение бисимуляции и его свойства

Определение бисимуляционной эквивалентности состояний

Два состояния s_1 и s_2 модели $M = (AP, S, R, S_0, L)$ называются бисимуляционно эквивалентными (обозначается $s_1 \approx s_2$), если существует такое отношение бисимуляции B на модели M , для которого выполняется соотношение $B(s_1, s_2)$.

Утверждение 4.

Отношение бисимуляционной эквивалентности $\approx$ состояний модели $M = (AP, S, R, S_0, L)$ является

- отношением эквивалентности,
- отношением бисимуляции на модели M ,
- наибольшим отношением бисимуляции на модели M

Отношение бисимуляции и его свойства

Определение фактор-модели

Фактор-моделью модели $M = (AP, S, R, S_0, L)$ называется модель $M/_{\approx} = (AP, S/_{\approx}, R/_{\approx}, S_0/_{\approx}, L/_{\approx})$ для которой

- $S/_{\approx} = \{[s]_{\approx} : s \in S\}$ — множество классов бисимуляционной эквивалентности состояний;
- $R/_{\approx} = \{([s']_{\approx}, [s'']_{\approx}) : s', s'' \in S, (s', s'') \in R\}$;
- $S_0/_{\approx} = \{[s]_{\approx} : s \in S_0\}$;
- $L/_{\approx}([s]_{\approx}) = L(s)$.

Отношение бисимуляции и его свойства

Упражнение 1.

Докажите, что для любой модели M верно соотношение $M \sim M/\approx$

Упражнение 2.

Какова взаимосвязь отношения бисимуляционной эквивалентности моделей $\sim$ и отношения бисимуляционной эквивалентости состояний модели $\approx$?

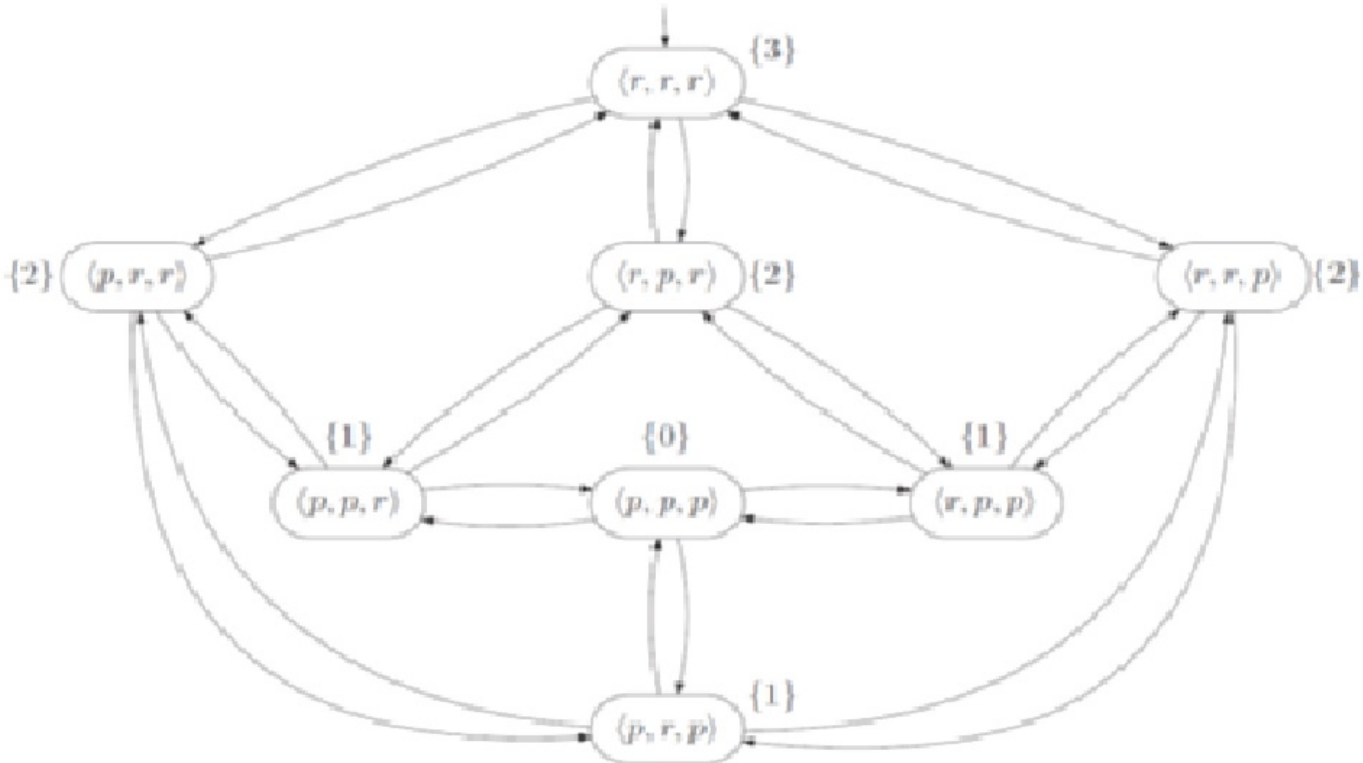
Упражнение 3. [трудное]

Докажите, что для любой модели M если B_1 и B_2 — отношения бисимуляции состояний модели M , то и отношение $B_1 \cup B_2$ также является отношением бисимуляции состояний модели M .

Отношение бисимуляции и его свойства

Модель информационной системы из 3-х принтеров.

M



Отношение бисимуляции и его свойства

И ее фактор-модель.

$M/\sim$

Вычисление бисимуляционной эквивалентности

Алгоритм вычисления бисимуляционной эквивалентности состояний $\approx$ для конечных моделей Крипке похож на алгоритм минимизации детерминированных конечных автоматов.

Для каждой модели $M = (AP, S, R, S_0, L)$ он вычисляет множество $S_{\approx}$ и, таким образом, может быть использован для построения фактор-модели $M/_{\approx}$.

Вычисление бисимуляционной эквивалентности

Алгоритм вычисления бисимуляционной эквивалентности состояний $\approx$ для конечных моделей Крипке похож на алгоритм минимизации детерминированных конечных автоматов.

Для каждой модели $M = (AP, S, R, S_0, L)$ он вычисляет множество $S_{\approx}$ и, таким образом, может быть использован для построения фактор-модели $M/_{\approx}$.

Основной принцип алгоритма — приближение сверху множества $S/_{\approx}$, представляющего собой разбиение пространства состояний S по отношению бисимуляционной эквиавлентности $\approx$.

Вычисление бисимуляционной эквивалентности

Пусть задана модель Крипке модели $M = (AP, S, R, S_0, L)$.

Блоком называется всякое непустое подмножество состояний D, $D \subseteq S$.

Вычисление бисимуляционной эквивалентности

Пусть задана модель Крипке модели $M = (AP, S, R, S_0, L)$.

Блоком называется всякое непустое подмножество состояний D, $D \subseteq S$.

Разбиением множества состояний S называется всякое такое конечное семейство $\Pi = \{D_1, \ldots, D_k\}$ попарно непересекающихся блоков, которое удовлетворяет равенству $S = \bigcup_{i=1}^{k} D_i$.

Вычисление бисимуляционной эквивалентности

Пусть задана модель Крипке модели $M = (AP, S, R, S_0, L)$.

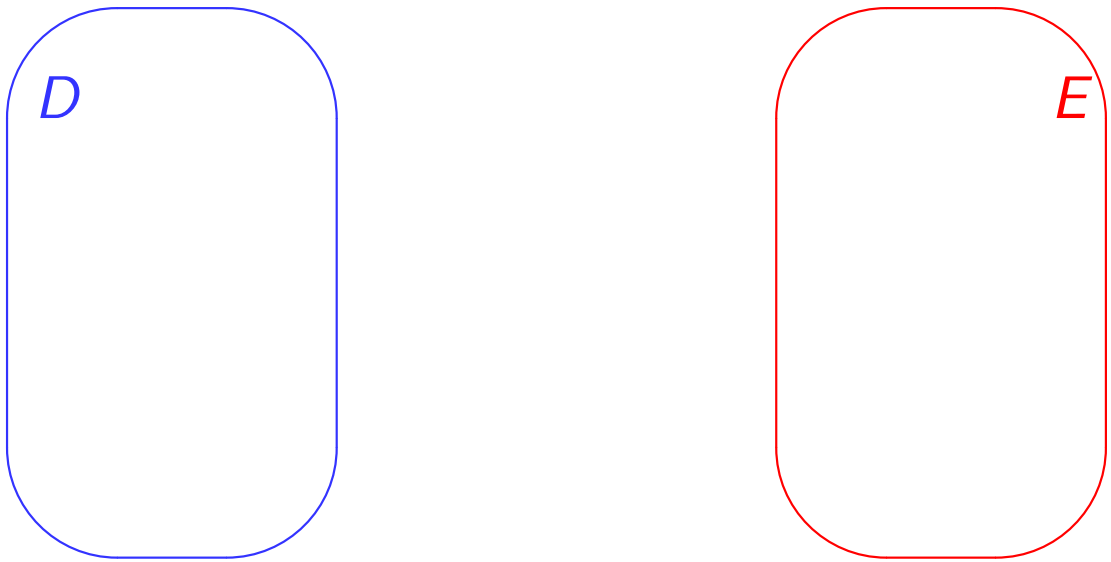
Блоком называется всякое непустое подмножество состояний D, $D \subseteq S$.

Разбиением множества состояний S называется всякое такое конечное семейство $\Pi = \{D_1, \ldots, D_k\}$ попарно непересекающихся блоков, которое удовлетворяет равенству $S = \bigcup_{i=1}^{k} D_i$.

Блок E называется разветвителем блока D , если существует такая пара состояний $s', s'' \in D$, для которой верны соотношения
$(\{s'\} \times E) \cap R \neq \emptyset$
и
$(\{s''\} \times E) \cap R = \emptyset$,

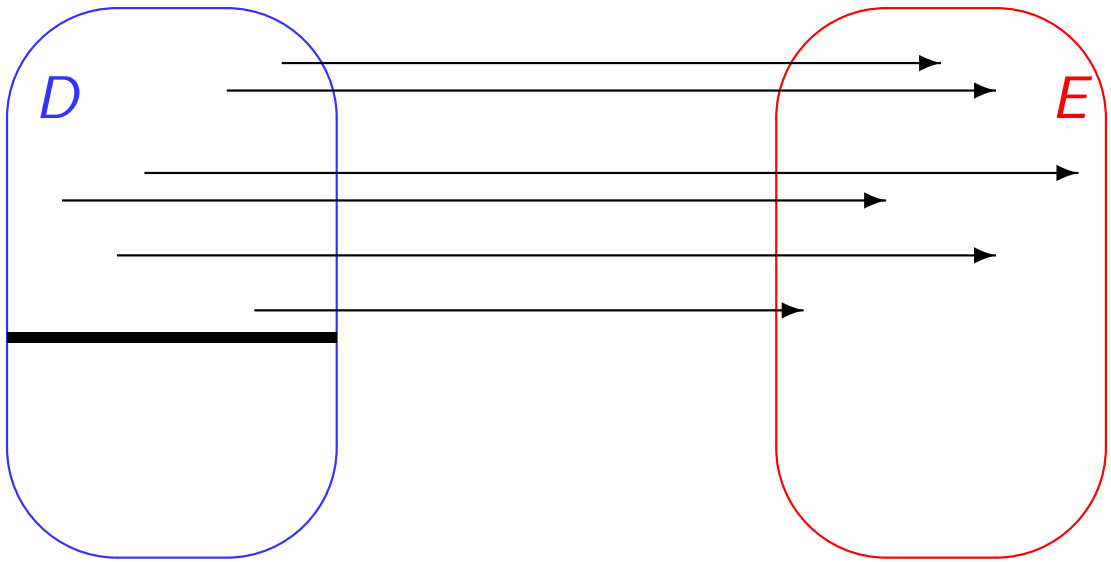
Вычисление бисимуляционной эквивалентности

т.е. из одних состояний блока D есть переходы в состояния блока E ,



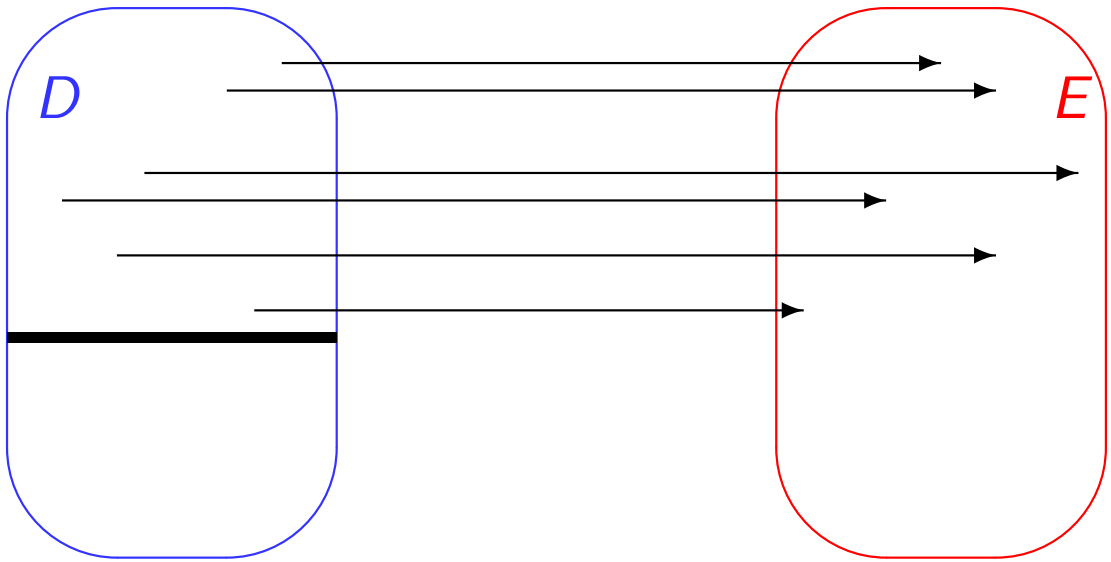
Вычисление бисимуляционной эквивалентности

т.е. из одних состояний блока D есть переходы в состояния блока E ,



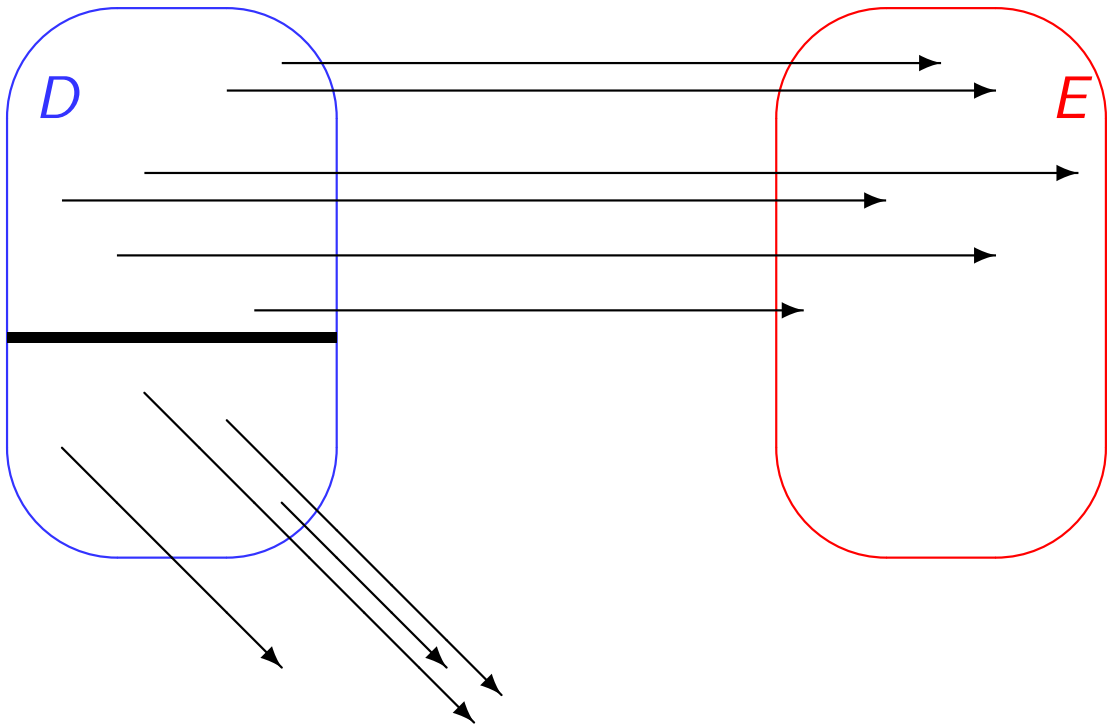
Вычисление бисимуляционной эквивалентности

т.е. из одних состояний блока D есть переходы в состояния блока E , а из других — нет.



Вычисление бисимуляционной эквивалентности

т.е. из одних состояний блока D есть переходы в состояния блока E , а из других — нет.



Вычисление бисимуляционной эквивалентности

Уточнением блока D относительно блока E называется семейство блоков $Ref(D|E)$, состоящее из

- пары блоков D', D'' , где
  $D' = \{s' : s' \in D,\ (\{s'\} \times E) \cap R \neq \emptyset\}$,
  $D'' = \{s'' : s'' \in D,\ (\{s''\} \times E) \cap R = \emptyset\}$,
  если блок E — разветвитель блока D ,
- единственного блока D в противном случае.

Вычисление бисимуляционной эквивалентности

Уточнением блока D относительно блока E называется семейство блоков $Ref(D|E)$, состоящее из

- пары блоков D', D'' , где
  $D' = \{s' : s' \in D,\ (\{s'\} \times E) \cap R \neq \emptyset\}$,
  $D'' = \{s'' : s'' \in D,\ (\{s''\} \times E) \cap R = \emptyset\}$,
  если блок E — разветвитель блока D ,
- единственного блока D в противном случае.

Уточнением семейства блоков $\Pi = \{D_1, \ldots, D_k\}$ относительно блока E называется семейство блоков
$Ref(\Pi|E) = \bigcup_{i=1}^{n} Ref(D_i|E)$.

Вычисление бисимуляционной эквивалентности

Уточнением блока D относительно блока E называется семейство блоков $Ref(D|E)$, состоящее из

- пары блоков D', D'' , где
  $D' = \{s' : s' \in D,\ (\{s'\} \times E) \cap R \neq \emptyset\}$,
  $D'' = \{s'' : s'' \in D,\ (\{s''\} \times E) \cap R = \emptyset\}$,
  если блок E — разветвитель блока D ,
- единственного блока D в противном случае.

Уточнением семейства блоков $\Pi = \{D_1, \ldots, D_k\}$ относительно блока E называется семейство блоков
$Ref(\Pi|E) = \bigcup_{i=1}^{n} Ref(D_i|E)$.

Уточнением разбиения $\Pi = \{D_1, \ldots, D_k\}$ называется разбиение

$$Ref(\Pi) = Ref(\ldots Ref(Ref(\Pi|D_1)|D_2)|\ldots|D_k).$$

Вычисление бисимуляционной эквивалентности

Алгоритм вычисления разбиения $S/_{\approx}$.

1. Вычисление начального разбиения Π_0 .

Введем отношение эквивалентности $\mathcal{R}_L$ на множестве состояний S :

$$(s', s'') \in \mathcal{R}_L \Leftrightarrow L(s') = L(s'').$$

и положим $\Pi_0 = S/_{\mathcal{R}_L}$.

Вычисление бисимуляционной эквивалентности

Алгоритм вычисления разбиения $S/_{\approx}$.

1. Вычисление начального разбиения Π_0 .

Введем отношение эквивалентности $\mathcal{R}_L$ на множестве состояний S :

$$(s', s'') \in \mathcal{R}_L \Leftrightarrow L(s') = L(s'').$$

и положим $\Pi_0 = S/_{\mathcal{R}_L}$.

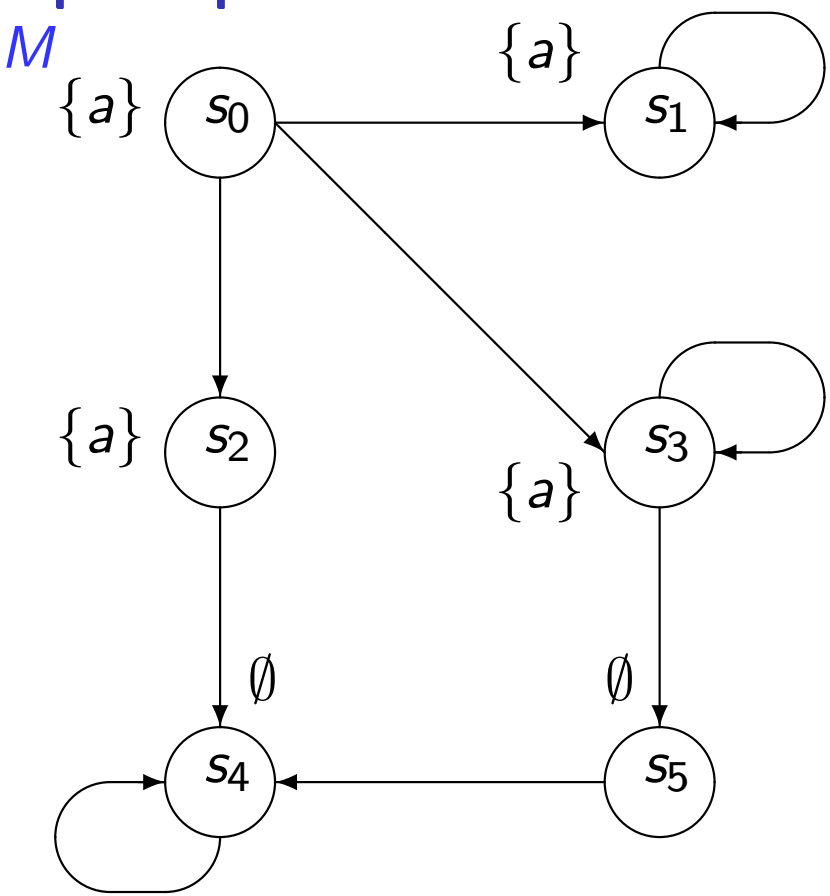
2. Итеративное вычисление $S/_{\approx}$.

do $\Pi_{i+1} := Ref(\Pi_i)$ **until** $\Pi_i = \Pi_{i+1}$

Вычисление бисимуляционной эквивалентности

Алгоритм вычисления разбиения $S/\approx$.

Пример.

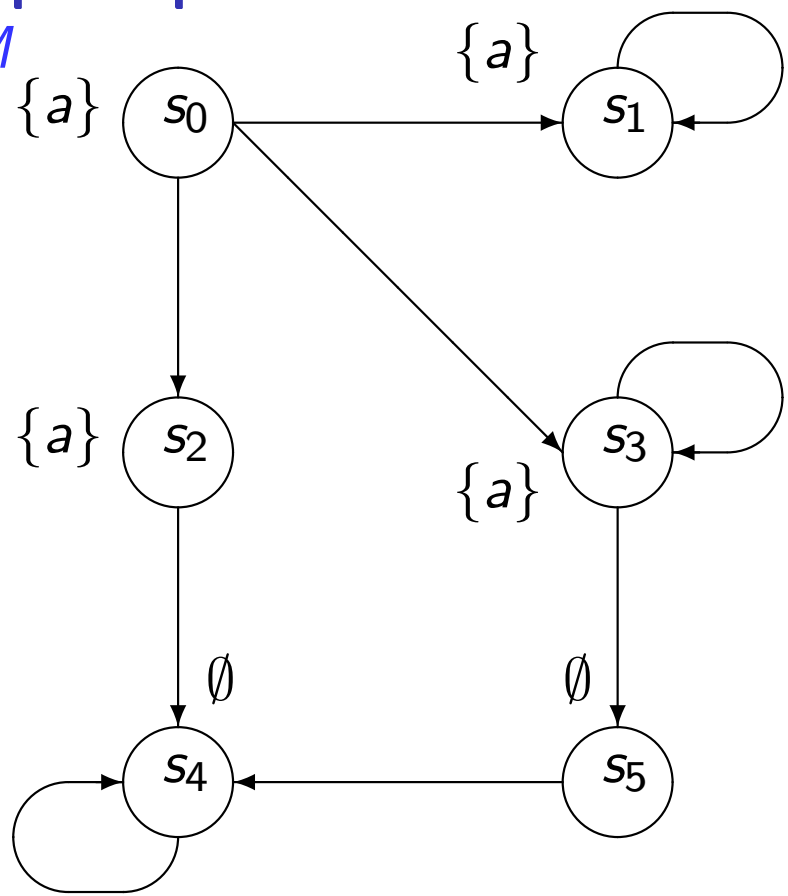


Вычисление бисимуляционной эквивалентности

Алгоритм вычисления разбиения $S/\approx$.

Пример.

M



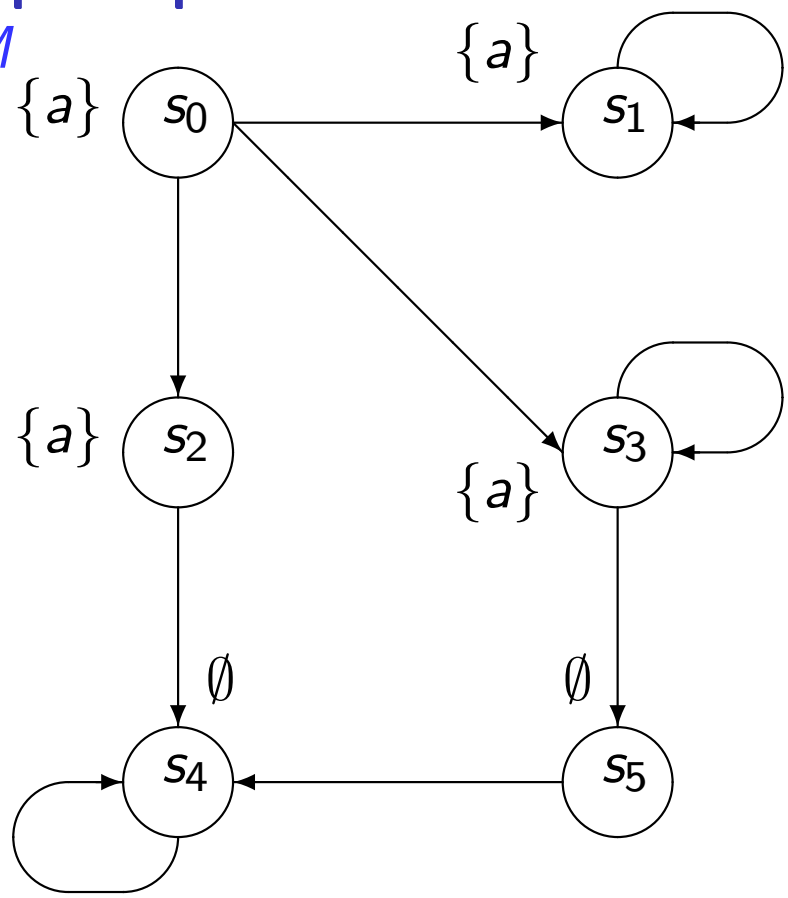
$$\Pi_0 = [\underbrace{\{s_0, s_1, s_2, s_3\}}_{D_1}; \underbrace{\{s_4, s_5\}}_{D_2}]$$

Вычисление бисимуляционной эквивалентности

Алгоритм вычисления разбиения $S/\approx$.

Пример.

M



$$\Pi_0 = [\underbrace{\{s_0, s_1, s_2, s_3\}}_{D_1}; \underbrace{\{s_4, s_5\}}_{D_2}]$$

$$\Pi_1 = Ref(\Pi_0) =$$

$$= Ref(Ref(\Pi_0|D_1)|D_2)$$

$$= Ref([\underbrace{\{s_0, s_1, s_3\}}_{D_{11}}; \underbrace{\{s_2\}}_{D_{12}}; \underbrace{\{s_4, s_5\}}_{D_2}]|D_2)$$

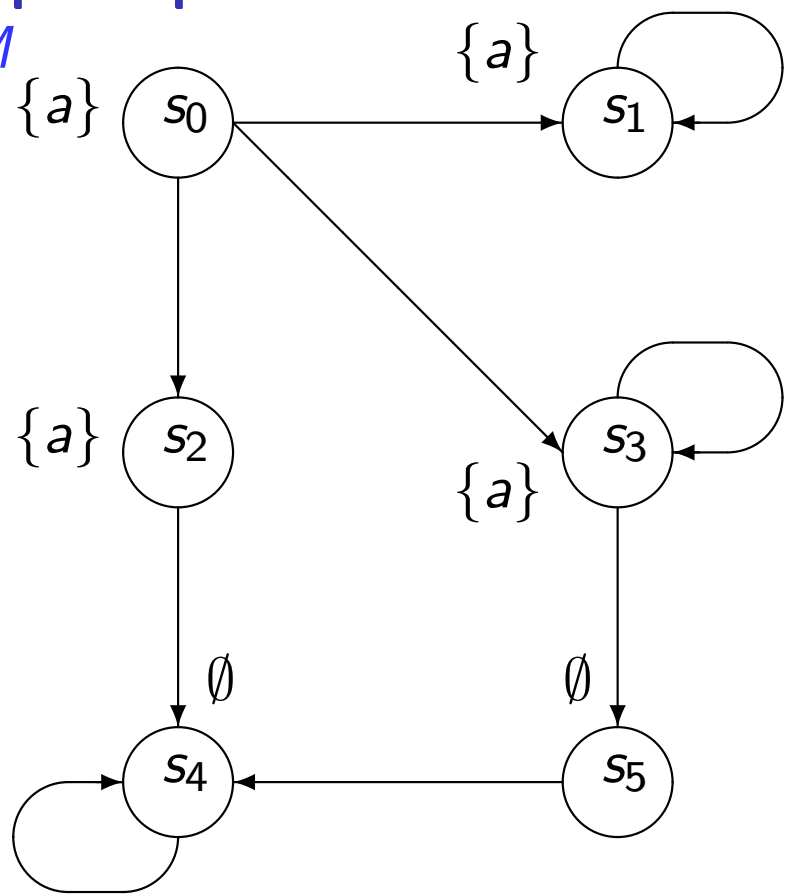
$$= [\underbrace{\{s_0, s_1\}}_{D_{111}}; \underbrace{\{s_3\}}_{D_{112}}; \underbrace{\{s_2\}}_{D_{12}}; \underbrace{\{s_4, s_5\}}_{D_2}]$$

Вычисление бисимуляционной эквивалентности

Алгоритм вычисления разбиения $S/\approx$.

Пример.

M



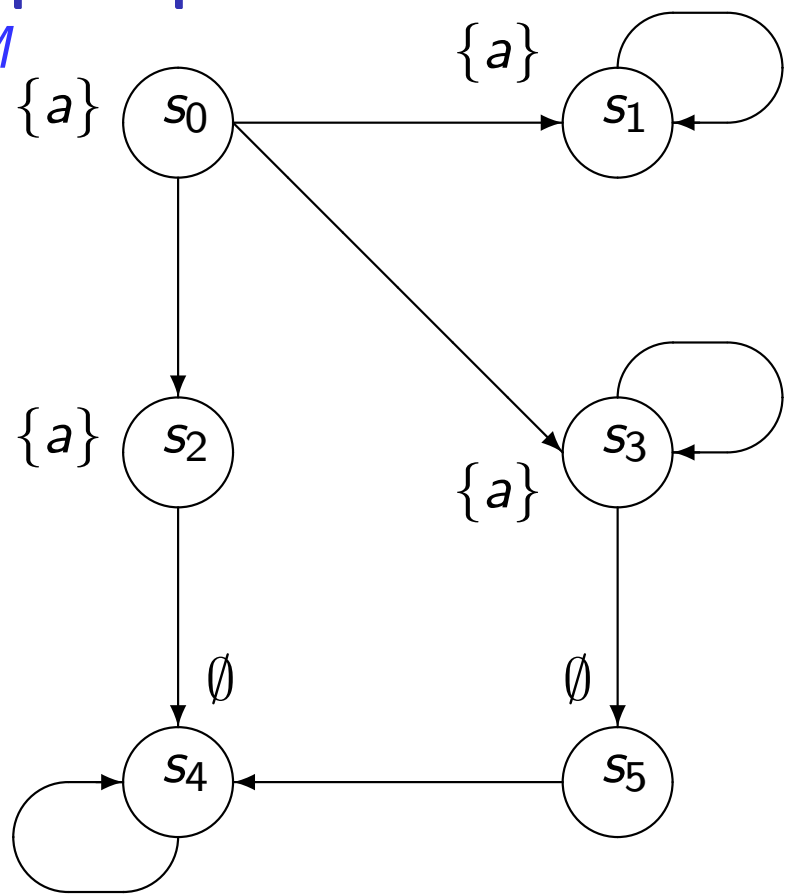
$$\Pi_2 = Ref(\Pi_1) =$$

$$= [\underbrace{\{s_0\}}_{D_{1111}}; \underbrace{\{s_1\}}_{D_{1112}}; \underbrace{\{s_3\}}_{D_{112}}; \underbrace{\{s_2\}}_{D_{12}}; \underbrace{\{s_4, s_5\}}_{D_2}]$$

Вычисление бисимуляционной эквивалентности

Алгоритм вычисления разбиения $S/\approx$.

Пример.



$$\Pi_2 = Ref(\Pi_1) =$$

$$= [\underbrace{\{s_0\}}_{D_{1111}}; \underbrace{\{s_1\}}_{D_{1112}}; \underbrace{\{s_3\}}_{D_{112}}; \underbrace{\{s_2\}}_{D_{12}}; \underbrace{\{s_4, s_5\}}_{D_2}]$$

$$\Pi_3 = Ref(\Pi_2) = \Pi_2$$

Конец вычислениям

Вычисление бисимуляционной эквивалентности

Уточнением отношения эквивалентности B на множестве состояний S назовем такое отношение эквивалентности Ref(B) , которое удовлетворяет равнеству $S/_{Ref(B)} = Ref(S/_B)$.

Вычисление бисимуляционной эквивалентности

Уточнением отношения эквивалентности B на множестве состояний S назовем такое отношение эквивалентности Ref(B) , которое удовлетворяет равнеству $S/_{Ref(B)} = Ref(S/_B)$.

Утверждение 5.

Отношение эквивалентности B на множестве состояний S является отношением бисимуляции на S тогда и только тогда, когда $Ref(B) = B$.

Вычисление бисимуляционной эквивалентности

Уточнением отношения эквивалентности B на множестве состояний S назовем такое отношение эквивалентности Ref(B) , которое удовлетворяет равнеству $S/_{Ref(B)} = Ref(S/_B)$.

Утверждение 5.

Отношение эквивалентности B на множестве состояний S является отношением бисимуляции на S тогда и только тогда, когда $Ref(B) = B$.

Утверждение 6.

Для любого отношения эквивалентности B на множестве состояний S верно

- $Ref(B) \subseteq B$,
- $\approx \subseteq B \implies \approx \subseteq Ref(B)$

Вычисление бисимуляционной эквивалентности

Теорема 2.

Алгоритм вычисления бисимуляционной эквивалентности для любой модели M

1. завершает вычисление;
2. вычисляет наибольшее отношение бисимуляции $\approx$ на S .

Вычисление бисимуляционной эквивалентности

Упражнение 4.

Докажите утверждения 5 и 6.

Упражнение 5.

Какова сложность предложенного алгоритма вычисления бисимуляционной эквивалентности?

Упражнение 6 [трудное].

Разработайте алгоритм вычисления бисимуляционной эквивалентности, имеющий сложность $O(|S||AP| + |R| \log |S|)$.

Отношение симуляции

Иногда бисимуляционная эквивалентность не приводит значительному сокращению числа состояний. Ослабляя требование того, чтобы на моделях выполнялось одно и то же множество формул, можно добиться большего сокращения.

Определение симуляции

Если для заданных моделей M и M' выполняется включение $AP \supseteq AP'$, то отношение $H \subseteq S \times S'$ называется отношением симуляции между M и M' в том и только том случае, когда

- для всякого начального состояния s_0 из S_0 в модели M найдется начальное состояние s_0' из S_0' в модели M' , для которого выполняется отношение $H(s_0, s_0')$,
- для любой пары состояний s и s' , находящихся в отношении $H(s, s')$, выполняются следующие условия:
  1) $L(s) \cap AP' = L'(s')$;
  2) для любого состояния s_1 , для которого выполняется отношение $R(s, s_1)$, найдется состояние s_1' , для которого выполняются отношения $R'(s', s_1')$ и $H(s_1, s_1')$.

Отношения симуляции

Будем говорить, что M' симулирует M (обозначим это отношение записью $M \preceq M'$), если существует отношение симуляции между M и M' .

Отношения симуляции

Будем говорить, что M' симулирует M (обозначим это отношение записью $M \preceq M'$), если существует отношение симуляции между M и M' .

Примеры к определению бисимуляции

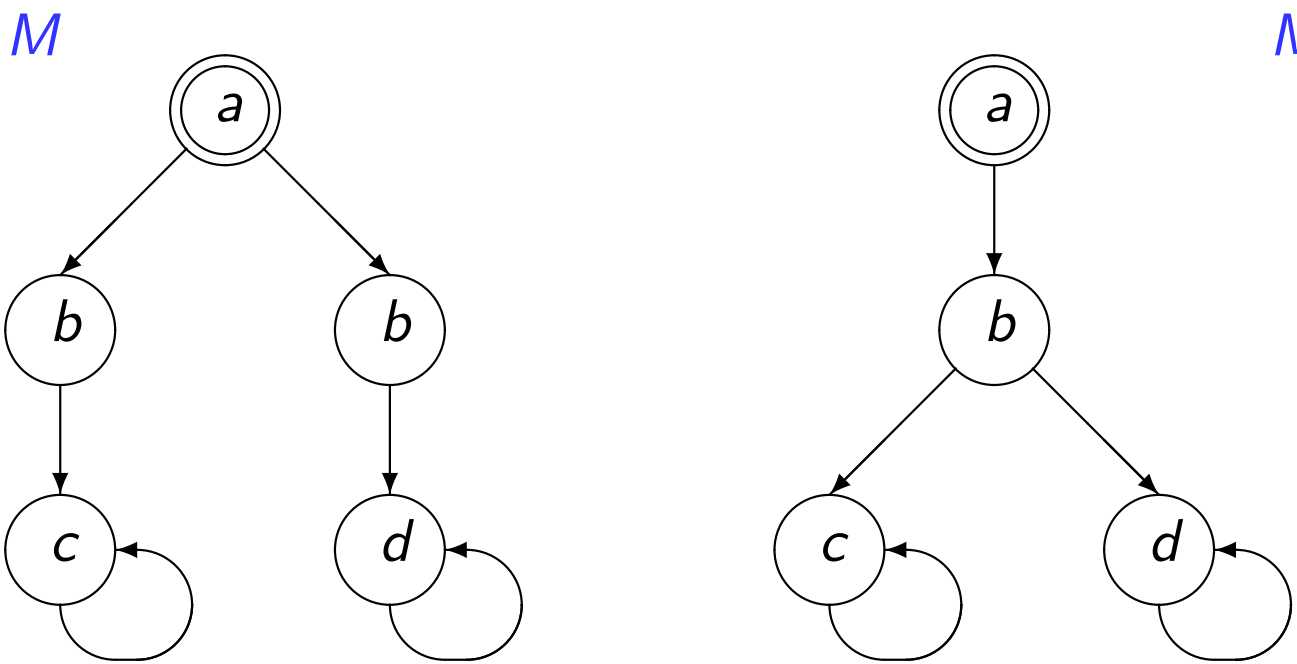


Рис.: Модель M' симулирует модель M : $M \preceq M'$

Отношение симуляции

Утверждение 7.

Отношение $\preceq$ является квазипорядком на множестве моделей.

Отношение симуляции

Утверждение 7.

Отношение $\preceq$ является квазипорядком на множестве моделей.

Будем говорить, что пути $\pi = s_0 s_1, \ldots$ в модели M и $\pi' = s'_0 s'_1, \ldots$ в модели M' соответствуют друг другу , если для любого i , $i \geq 0$, выполняется отношение $H(s_i, s'_i)$.

Утверждение 8.

Предположим, что для состояний s и s' выполняется отношение $H(s, s')$. Тогда для каждого пути π , выходящего из s , имеется соответствующий ему путь π' , выходящий из s' .

Отношение симуляции

Формула CTL в позитивной нормальной, содержащая только темпоральные операторы с квантором всеобщности, т.е. операторы $\mathbf{AX}, \mathbf{AF}, \mathbf{AG}, \mathbf{AU}, \mathbf{AR}$, называется ACTL-формулой.

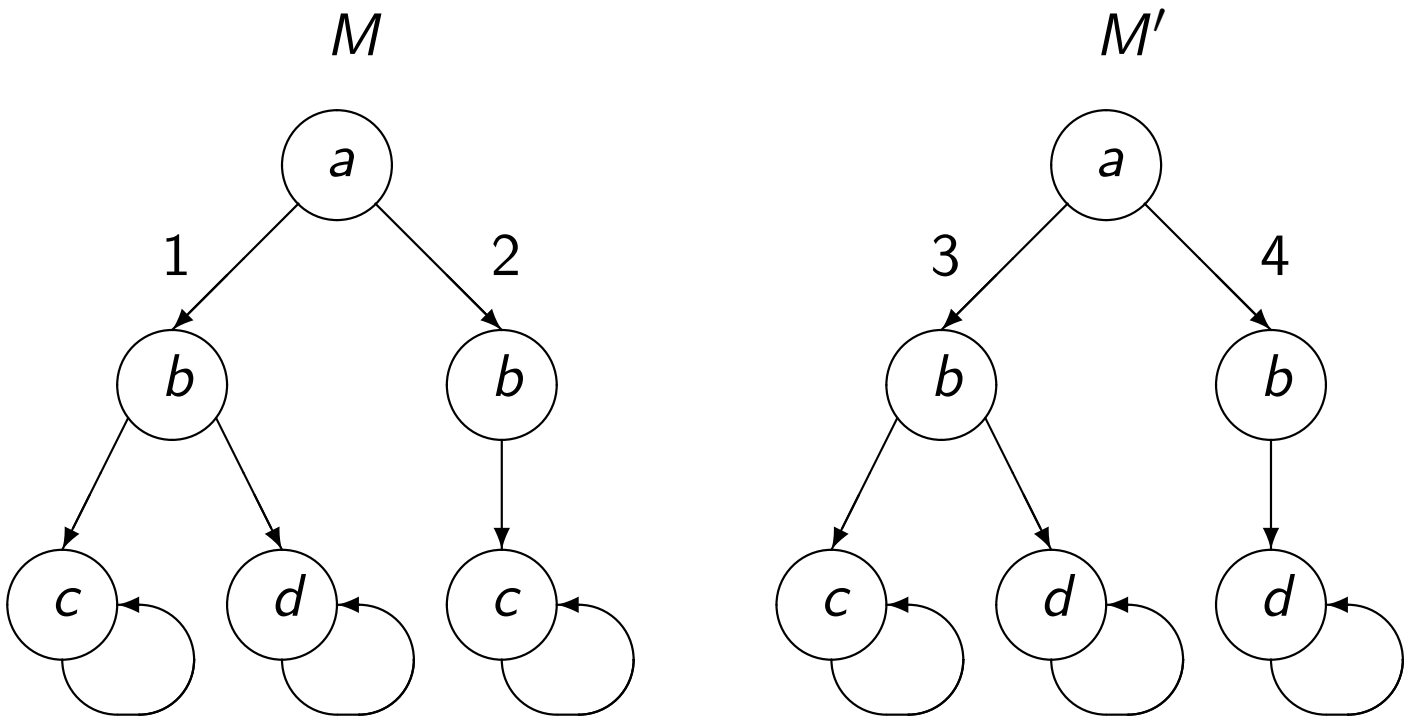
Теорема 3.

Допустим, что $M \preceq M'$. Тогда для всякой ACTL-формулы φ (с атомарными высказываниями из AP') из соотношения $M' \models \varphi$ следует, что $M \models \varphi$.

Доказательство Индукцией по структуре формулы с применением Утверждения 8.

Отношение симуляции

В чем состоит различие между симуляцией и бисимуляцией?



Модели, представленные на рисунке, не являются бисимуляционно эквивалентными, хотя каждая из них симулирует другую.

Отношение симуляции

Будем говорить, что модели M' и M'' симуляционно эквивалентны , если $M' \preceq M''$ и $M'' \preceq M'$.

Отношение симуляции

Будем говорить, что модели M' и M'' симуляционно эквивалентны , если $M' \preceq M''$ и $M'' \preceq M'$.

Теорема 5.

Если модели M' и M'' симуляционно эквивалентны, то для любой ACTL формулы φ мы имеем

$$M' \models \varphi \Leftrightarrow M'' \models \varphi.$$

Отношение симуляции

Будем говорить, что модели M' и M'' симуляционно эквивалентны , если $M' \preceq M''$ и $M'' \preceq M'$.

Теорема 5.

Если модели M' и M'' симуляционно эквивалентны, то для любой ACTL формулы φ мы имеем

$$M' \models \varphi \Leftrightarrow M'' \models \varphi.$$

Обратная теорема также верна.

Если две модели удовлетворяют одному и тому же множеству ACTL-формул, то они симуляционно эквивалентны.

Отношение симуляции

Упражнение 7. [трудное]

Руководствуясь идеями, предложенными при создании алгоритма вычисления бисимуляционной эквивалентности, разработайте алгоритм вычисления наибольшего отношения симуляции между состояниями заданной модели.

Абстракция моделей

Абстракция — это самый действенный метод решения проблемы «комбинаторного взрыва». Мы рассмотрим два различных метода абстракции: редукцию по конусу влияния и абстракцию данных .
Они применяются к описаниям системы на высшем уровне, еще до того как построена ее модель, и позволяют избежать построения нередуцированной модели, которая может оказаться слишком большой, чтобы поместиться в память.

Абстракция моделей

Метод редукции по конусу влияния состоит в том, чтобы сократить размер графа переходов, рассматривая только те переменные системы, которые задействованы в спецификации.
Сокращение достигается за счет удаления переменных, которые не оказывают никакого влияния на переменные, фигурирующие в спецификации.
Таким образом, проверяемые свойства сохраняются, но размер модели, которую нужно верифицировать, становится меньше.

Абстракция моделей

Метод редукции по конусу влияния состоит в том, чтобы сократить размер графа переходов, рассматривая только те переменные системы, которые задействованы в спецификации. Сокращение достигается за счет удаления переменных, которые не оказывают никакого влияния на переменные, фигурирующие в спецификации.
Таким образом, проверяемые свойства сохраняются, но размер модели, которую нужно верифицировать, становится меньше.

Абстракция данных предусматривает поиск отображения реальных значений данных, используемых в системе, в небольшое множество абстрактных значений данных. Распространив это отображение на состояния и переходы, можно построить абстрактную систему, которая симулирует исходную, но обычно имеет гораздо меньший размер.
Из-за такого сокращения размера абстрактную систему подчас удается верифицировать гораздо легче, нежели исходную.

Редукция по конусу влияния

Посмотрим, как редукция по конусу влияния может быть применена к синхронным схемам.

Пусть V — множество переменных заданной логической схемы. Эта схема может быть описана системой уравнений вида

$$v_i' = f_i(V)$$

для каждой переменной $v_i \in V$, где f_i — булева формула.

Редукция по конусу влияния

Посмотрим, как редукция по конусу влияния может быть применена к синхронным схемам.

Пусть V — множество переменных заданной логической схемы. Эта схема может быть описана системой уравнений вида

$$v_i' = f_i(V)$$

для каждой переменной $v_i \in V$, где f_i — булева формула.

Предположим, что задано множество переменных $V' \subseteq V$, представляющих интерес в свете предъявленной спецификации. Нам хотелось бы упростить описание системы, сохранив в нем только эти переменные, но они могут зависеть от значений переменных, не входящих в V'.

Поэтому мы определяем конус влияния C для V' и используем C для сокращения описания системы.

Редукция по конусу влияния

Определение конуса влияния

Конусом влияния C для множества переменных V' назовем такое наименьшее множество переменных, что

- $V' \subseteq C$,
- если для некоторой переменной $v_\ell \in C$ ее функция f_ℓ зависит от переменной v_j , то $v_j \in C$.

Чтобы построить новую (упрощенную) систему, нужно удалить все те уравнения, у которых переменные в левой части не входят в C .

Редукция по конусу влияния

Пример конуса влияния

Обратимся к примеру счетчика по модулю 8. Его система уравнений такова:

$v_0' = \neg v_0$;
$v_1' = v_0 \oplus v_1$;
$v_2' = (v_0 \wedge v_1) \oplus v_2$.

Ясно, что если $V' = \{v_0\}$, то $C = \{v_0\}$, поскольку f_0 не зависит ни от какой другой переменной, кроме v_0 .

Если же $V' = \{v_1\}$, то $C = \{v_0, v_1\}$, поскольку f_1 зависит от обеих переменных, но при этом $v_2 \notin C$, ибо никакая переменная из C не зависит от v_2 .

И если, наконец, $V' = \{v_2\}$, то C — это множество всех переменных.

Редукция по конусу влияния

Покажем, что редукция по конусу влияния сохраняет корректность спецификаций в логике CTL, если они определены над переменными (атомарными высказываниями) из C .

Рассмотрим множество булевых переменных $V = \{v_1, \ldots, v_n\}$ и модель синхронной схемы $M = (S, R, S_0, L)$ над множеством переменных V , где

- $S = \{0, 1\}^n$ — множество всех возможных значений переменных из V ;
- $R = \bigwedge_{i=1}^{n} [v_i' = f_i(V)]$;
- $L(s) = \{v_i \mid s(v_i) = 1,\ 1 \leq i \leq n\}$;
- $S_0 \subseteq S$.

Редукция по конусу влияния

Предположим, что мы редуцируем схему относительно конуса влияния $C = \{v_1, \ldots, v_k\}$ для некоторого $k \leq n$.

Упрощенная модель имеет вид $red(M, C) = (S', R', S'_0, L')$, где

- $S' = \{0, 1\}^k$ — множество всех возможных значений переменных из C ;
- $R' = \bigwedge_{i=1}^{k} [v'_i = f_i(V)]$;
- $L'(s') = \{v_i \mid s'(v_i) = 1,\ 1 \leq i \leq k\}$;
- $S'_0 = \{(d'_1, \ldots, d'_k) \mid$ существуют такие биты $(d_{k+1}, \ldots, d_n)$, что $(d'_1, \ldots, d'_k, d_{k+1}, \ldots, d_n) \in S_0\}$.

Редукция по конусу влияния

Обозначим записью $M|_C$ проекцию модели M на конус влияния C , т.е. $M|_C = (S, R, S_0, L|_C)$, где $L|_C(s) = L(s) \cap C$ для любого состояния $s, s \in S$.

Редукция по конусу влияния

Обозначим записью $M|_C$ проекцию модели M на конус влияния C , т.е. $M|_C = (S, R, S_0, L|_C)$, где $L|_C(s) = L(s) \cap C$ для любого состояния $s, s \in S$.

Утверждение 9.

Для любой CTL*-формулы φ , зависящей только от атомарных высказываний из множества C , верно соотношение

$$M \models \varphi \iff M|_C \models \varphi.$$

Редукция по конусу влияния

Обозначим записью $M|_C$ проекцию модели M на конус влияния C , т.е. $M|_C = (S, R, S_0, L|_C)$, где $L|_C(s) = L(s) \cap C$ для любого состояния $s, s \in S$.

Утверждение 9.

Для любой CTL*-формулы φ , зависящей только от атомарных высказываний из множества C , верно соотношение

$$M \models \varphi \iff M|_C \models \varphi.$$

Утверждение 10.

Модели $M|_C$ и $red(M, C)$ бисимуляционно эквивалентны.

Редукция по конусу влияния

Обозначим записью $M|_C$ проекцию модели M на конус влияния C , т.е. $M|_C = (S, R, S_0, L|_C)$, где $L|_C(s) = L(s) \cap C$ для любого состояния $s, s \in S$.

Утверждение 9.

Для любой CTL*-формулы φ , зависящей только от атомарных высказываний из множества C , верно соотношение

$$M \models \varphi \iff M|_C \models \varphi.$$

Утверждение 10.

Модели $M|_C$ и $red(M, C)$ бисимуляционно эквивалентны.

Доказательство. Покажите, что отношение $B \subseteq S \times S'$, такое что $((d_1, \ldots, d_n), (d'_1, \ldots, d'_k)) \in B \iff d_1 = d'_1, \ldots, d_k = d'_k$. является отношением бисимуляции между $M|_C$ и $red(M, C)$.

Редукция по конусу влияния

Теорема 6.

Для любой модели M , конуса влияния C и произвольной CTL*-формулы φ , зависящей только от атомарных высказываний из множества C , верно соотношение

$$M \models \varphi \iff red(M, C) \models \varphi.$$

Абстракция данных

Абстракция данных определяется отображением фактических значений данных системы в небольшое множество абстрактных значений данных. Распространив это отображение на состояния и переходы, можно построить абстрактный вариант анализируемой системы.

Абстрактная система оказывается гораздо меньше реальной системы, и поэтому на абстрактном уровне проверять свойства поведения модели значительно проще. Корректность проверки обеспечивает отношение симуляции, поддерживаемое между исходной моделью и ее абстракцией.

Абстракция данных

Пусть задана некоторая модель $M = (AP, S, R, S_0, L)$ и разбиение $H = (D_1, D_2, \ldots, D_k)$ пространства ее состояний S , согласованное с функцией разметки L , т.е. удовлетворяющее условию равенства $L(s') = L(s'')$ для любой пары состояний s', s'' из любого блока $B_j, 1 \leq j \leq k$.

Абстракция данных

Пусть задана некоторая модель $M = (AP, S, R, S_0, L)$ и разбиение $H = (D_1, D_2, \ldots, D_k)$ пространства ее состояний S, согласованное с функцией разметки L, т.е. удовлетворяющее условию равенства $L(s') = L(s'')$ для любой пары состояний s', s'' из любого блока $B_j, 1 \leq j \leq k$.

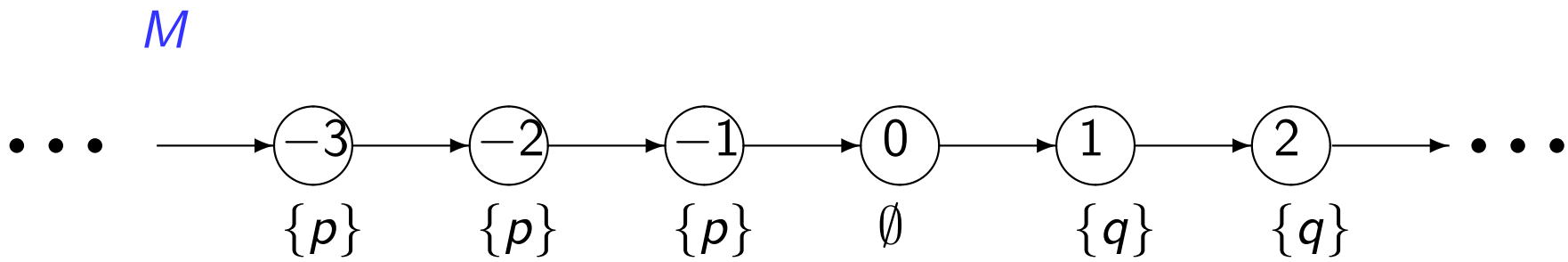
Абстракция, порожденная разбиением

Абстракцией модели M, порожденной разбиением H называется модель $abstr(M, H) = (AP, S', R', S'_0, L')$, в которой

- $S = H$,
- $R' = \{(D_i, D_j) \ : \ (s_i, s_j) \in R$ для некоторой пары состояний $s_i \in D_i, s_j \in D_j\}$,
- $S'_0 = \{D_i \ : D_i \cap S_0 \neq \emptyset\}$,
- $L'(D_i) = L(s_i)$, где s_i — произвольное состояние из блока D_i.

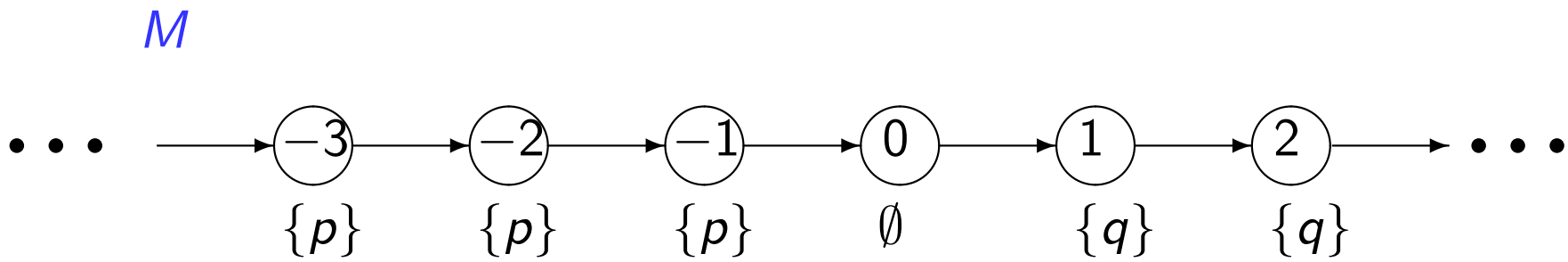
Абстракция данных

Пример абстракции, порожденной разбиением



Абстракция данных

Пример абстракции, порожденной разбиением

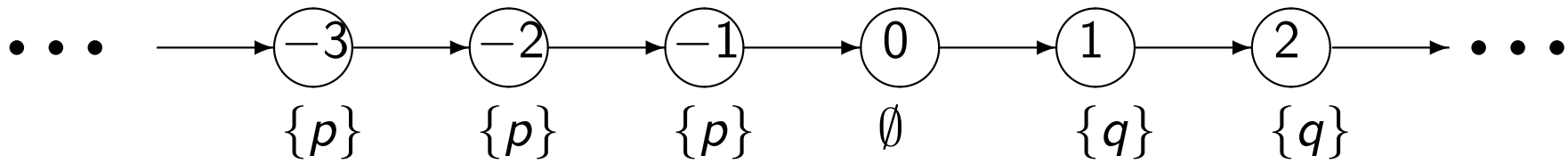


Разбиение H : $D_1 = \{\ldots, -3, -2, -1\}, D_2 = \{0\}, D_3 = \{1, 2, \ldots\}$

Абстракция данных

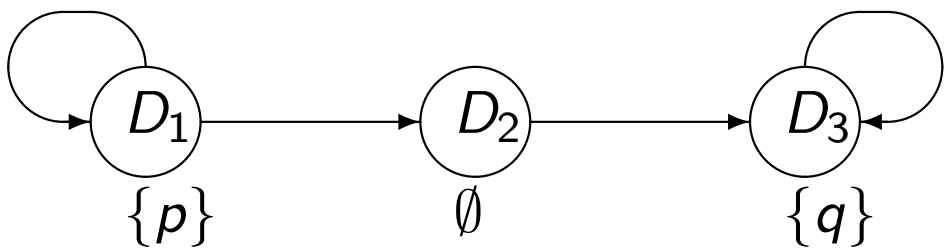
Пример абстракции, порожденной разбиением

M



Разбиение H : $D_1 = \{\ldots, -3, -2, -1\}, D_2 = \{0\}, D_3 = \{1, 2, \ldots\}$

$abstr(M, H)$



Абстракция данных

Утверждение 11.

Для любой модели M и разбиения H пространства ее состояний, согласованного с ее функцией разметки, выполняется отношение $M \preceq abstr(M, H)$.

Абстракция данных

Утверждение 11.

Для любой модели M и разбиения H пространства ее состояний, согласованного с ее функцией разметки, выполняется отношение $M \preceq abstr(M, H)$.

Теорема 7.

Для любой модели M , разбиения H пространства ее состояний, согласованного с ее функцией разметки, и произвольной ACTL-формулы φ верно соотношение

$$abstr(M, H) \models \varphi \implies M \models \varphi.$$

КОНЕЦ ЛЕКЦИИ 8.