Математическая логика и логическое программирование

Лектор:

Подымов Владислав Васильевич

e-mail:
valdus@yandex.ru

2015, весенний семестр

Лекция 19

Задача model checking для LTL

Подформулы Фишера-Ладнера

Табличный метод model checking

Система Хинтикки

Алгоритм model checking

Задача model checking для LTL

для заданных LTL-формулы φ и LTS M
проверить условие $M \models \varphi$

Задача model checking непроста, потому что

- выполнимость формул LTL проверяется на бесконечных интерпретациях
- в LTS M имеется бесконечно много интерпретаций (трасс)

Задача model checking имеет эффективное решение, потому что

- всё это бесконечное множество бесконечных интерпретаций "упаковано" в **конечную** структуру — LTS M

Как же выглядит это решение? (табличный метод)

Задача model checking для LTL

Основная идея табличного метода

1. Попытаемся найти **контрмодель**: подходящую интерпретацию $I(tr)$, в которой формула φ не выполняется
2. Проверку (не)выполнимости φ сведём к проверке (не)выполнимости её подформул Ф: значение φ полностью определяется значениями Ф
3. Расширим задачу: вычислим множество $\overline{S}$ всех состояний s LTS M, для которых формула φ не выполняется хотя бы для одной трассы, начинающейся в s
4. В процессе проверки будем "путешествовать" по состояниям LTS M, получать новые формулы и проверять их выполнимость
5. Проверим, содержится ли в множестве $\overline{S}$ хотя бы одно начальное состояние

Задача model checking для LTL

Немного обозначений

Пусть

$$tr = s_1 \to s_2 \to s_3 \to \dots$$ —

трасса LTS M, и φ — формула LTL

Тогда:

- $tr \models \varphi$ сокращение для записи $l(tr), 1 \models \varphi$
- $tr[j]$ — j-е состояние трассы tr: s_j
- $tr|_j$ — суффикс трассы tr, начинающийся с состояния $tr[j]$:

$$s_j \to s_{j+1} \to s_{j+2} \to \dots$$

Задача model checking для LTL

Утверждение 1

Пусть M — LTS и φ — формула LTL. Тогда

$M \not\models \varphi \quad \Leftrightarrow$ **существует начальная трасса tr LTS M, такая что t $\not\models \varphi$**

Доказательство.

Самостоятельно

Теперь от задачи "$M \models \varphi$?" можно перейти к такой:

найти начальную трассу tr LTS M, для которой верно $tr \not\models \varphi$

Если такой трассы найти не удастся, то верно $M \models \varphi$

Задача model checking для LTL

Формула φ находится в позитивной форме, если в ней:

1. используются только связки $\vee$, $\&$, $\neg$ и операторы **X**, **U**, **R**
2. связка $\neg$ применяется только к атомарным высказываниям

Утверждение 2

Для любой LTL-формулы φ существует равносильная ей формула φ' в позитивной нормальной форме

Задача model checking для LTL

Доказательство.

Не просто докажем существование формулы φ', но **явно построим** её

Этап 1: удалим из формулы φ связку $\to$ и операторы **F**, **G**

Для этого достаточно использовать законы

$$\psi \to \chi \approx \neg\psi \vee \chi$$
$$\mathbf{F}\psi \approx \mathbf{true}\ \mathbf{U}\psi \qquad \mathbf{G}\psi \approx \mathbf{false}\ \mathbf{R}\psi,$$

Этап 2: продвинем отрицание вглубь

Для этого достаточно использовать законы

$$\neg(\psi\&\chi) \approx \neg\psi \vee \neg\chi \qquad \neg(\psi \vee \chi) \approx \neg\psi\&\neg\chi$$
$$\neg\neg\psi \approx \psi \qquad \neg\mathbf{X}\psi \approx \mathbf{X}\neg\psi$$
$$\neg(\psi\mathbf{U}\chi) \approx \neg\psi\mathbf{R}\neg\chi \qquad \neg(\psi\mathbf{R}\chi) \approx \neg\psi\mathbf{U}\neg\chi$$

конец доказательства

Задача model checking для LTL

Пример

$\mathbf{G}(\mathit{free} \& \mathbf{X}\mathit{busy} \to \mathbf{XF}(\mathit{pr}_1 \vee \mathit{pr}_2))$.

Этап 1: удаление $\to$, $\mathbf{F}$, $\mathbf{G}$

$$\ldots$$

$$\mathbf{false}\ \mathbf{R}(\neg(\mathit{free} \& \mathbf{X}\mathit{busy}) \vee \mathbf{X}(\mathbf{true}\ \mathbf{U}(\mathit{pr}_1 \vee \mathit{pr}_2)))$$

Этап 2: продвижение отрицания

$$\ldots$$

$$\mathbf{false}\ \mathbf{R}(\neg\mathit{free} \vee \mathbf{X}\neg\mathit{busy} \vee \mathbf{X}(\mathbf{true}\ \mathbf{U}(\mathit{pr}_1 \vee \mathit{pr}_2)))$$

Подформулы Фишера-Ладнера

Проверка выполнимости формулы φ **в позитивной форме** будет состоять в разметке состояний LTS множествами формул, определяемыми на основе семейств подформул Фишера-Ладнера $FLSub_\varphi$ для φ

Неформально: это формулы, максимально близкие к подформулам φ, влияющие на её значение в текущем состоянии (s) и всех соседних состояниях (s': $s \to s'$)

Формально: это наименьшее множество формул, содержащее φ и такое что:

- если $p \in FLSub_\varphi$, то $\neg p \in FLSub_\varphi$ $\quad (p \in \mathcal{AP})$
- если $\psi \& \chi \in FLSub_\varphi$, то $\{\psi, \chi\} \subseteq FLSub_\varphi$,
- если $\psi \vee \chi \in FLSub_\varphi$, то $\{\psi, \chi\} \subseteq FLSub_\varphi$,
- если $\neg\psi \in FLSub_\varphi$, то $\psi \in FLSub_\varphi$,
- если $\mathbf{X}\psi \in FLSub_\varphi$, то $\psi \in FLSub_\varphi$,
- если $\psi \mathbf{U} \chi \in FLSub_\varphi$, то $\{\psi, \chi, \mathbf{X}(\psi \mathbf{U} \chi)\} \subseteq FLSub_\varphi$,
- если $\psi \mathbf{R} \chi \in FLSub_\varphi$, то $\{\psi, \chi, \mathbf{X}(\psi \mathbf{R} \chi)\} \subseteq FLSub_\varphi$.

Подформулы Фишера-Ладнера

Пример

Пусть $\varphi = \mathbf{false}\ \mathbf{R}(\neg free \vee \mathbf{X}\neg busy \vee \mathbf{X}(\mathbf{true}\ \mathbf{U}(pr_1 \vee pr_2)))$

Тогда

$$FLSub_\varphi =$$

$$\left\{ \begin{array}{l} \varphi, \\ \mathbf{false}, \neg free \vee \mathbf{X}\neg busy \vee \mathbf{X}(\mathbf{true}\ \mathbf{U}(pr_1 \vee pr_2)), \mathbf{X}\varphi, \\ \neg free, \mathbf{X}\neg busy, \mathbf{X}(\mathbf{true}\ \mathbf{U}(pr_1 \vee pr_2)), \\ free, \neg busy, \mathbf{true}\ \mathbf{U}(pr_1 \vee pr_2), \\ busy, \mathbf{true}, pr_1 \vee pr_2, \\ pr_1, pr_2, \neg pr_1, \neg pr_2 \end{array} \right\}$$

Утверждение 3

Если φ содержит n связок и темпоральных операторов, то $|FLSub_\varphi| \leq 3n$

Доказательство.Очевидно

Подформулы Фишера-Ладнера

Особую роль будут играть формулы множества $FLSub_\varphi$, представимые в виде $\mathbf{X}\psi$ и $\psi\mathbf{U}\chi$, $\psi\mathbf{R}\chi$

Для простоты работы с такими подмножествами введём для них специальные обозначения

$XSub_\varphi$ — множество всех формул, содержащихся в $FLSub_\varphi$ и представимых в виде $\mathbf{X}\psi$:

$URSub_\varphi$ — множество всех формул, содержащихся в $FLSub_\varphi$ и представимых в виде $\psi\mathbf{U}\chi$ либо $\psi\mathbf{R}\chi$

Пример: пусть
$\varphi = \mathbf{false}\ \mathbf{R}(\neg free \vee \mathbf{X}\neg busy \vee \mathbf{X}(\mathbf{true}\ \mathbf{U}(pr_1 \vee pr_2)))$; тогда

$$XSub_\varphi = \{\mathbf{X}\varphi, \mathbf{X}\neg busy, \mathbf{X}(\mathbf{true}\ \mathbf{U}(pr_1 \vee pr_2))\}$$

$$URSub_\varphi = \{\varphi, \mathbf{true}\ \mathbf{U}(pr_1 \vee pr_2)\}$$

Подформулы Фишера-Ладнера

Семейства формул, которыми будут размечаться состояния, представляют собой **предположения** о том, какие подформулы выполняются в текущем состоянии

В некоторых предположениях может содержаться (явное или неявное) противоречие

Явных противоречий можно избежать, оставляя только согласованные семейства $B \subseteq FLSub_\varphi$:

- $\mathbf{false} \notin B$
- хотя бы одна из формул p, $\neg p$ **не содержится** в B $(p \in \mathcal{AP})$
- $\psi \vee \chi \in B \iff \psi \in B$ или $\chi \in B$ $\qquad (\psi \vee \chi \in FLSub_\varphi)$
- $\psi \& \chi \in B \iff \psi \in B$ и $\chi \in B$ $\qquad (\psi \& \chi \in FLSub_\varphi)$
- $\psi \mathbf{U} \chi \in B \iff \chi \in B$ или $\{\psi, \mathbf{X}(\psi \mathbf{U} \chi)\} \subseteq B$ $\qquad (\psi \mathbf{U} \chi \in FLSub_\varphi)$
- $\psi \mathbf{R} \chi \in B \iff \chi \in B$ и либо $\psi \in B$, либо $\mathbf{X}(\psi \mathbf{R} \chi) \in B$ $\qquad (\psi \mathbf{R} \chi \in FLSub_\varphi)$

Подформулы Фишера-Ладнера

А как выглядят неявные противоречия в согласованных семействах формул?

Например, две такие формулы:

$\mathbf{X}p$: “я завтра брошу пить”

$\mathbf{X}\neg p$: “завтра всё как обычно” —

хотя и содержат противоречие, но могут содержаться в согласованном множестве: моему образу жизни сегодня ни одна из них не противоречит

Согласованное множество формул — это аналог **семантической таблицы**: оно выражает наше пожелание сделать все утверждения, содержащиеся в этом множестве, истинными, а все утверждения, не содержащиеся в нем, — ложными

Подформулы Фишера-Ладнера

Пример

Пусть $\varphi = \mathbf{false}\ \mathbf{R}(\neg free \vee \mathbf{X}\neg busy \vee \mathbf{X}(\mathbf{true}\ \mathbf{U}(pr_1 \vee pr_2)))$, то есть

$$FLSub_\varphi = \left\{ \begin{array}{l} free, busy, pr_1, pr_2, \neg free, \neg busy, \neg pr_1, \neg pr_2, \\ pr_1 \vee pr_2, \\ \mathbf{true}\ \mathbf{U}(pr_1 \vee pr_2), \\ \mathbf{X}\neg busy, \mathbf{X}(\mathbf{true}\ \mathbf{U}(pr_1 \vee pr_2)), \\ \neg free \vee \mathbf{X}\neg busy \vee \mathbf{X}(\mathbf{true}\ \mathbf{U}(pr_1 \vee pr_2)), \\ \varphi, \mathbf{X}\varphi \end{array} \right\}$$

Тогда согласованным будет, например, такое семейство $B \subseteq FLSub_\varphi$:

$$B = \left\{ \begin{array}{l} \mathbf{true}, pr_1, \neg pr_2, \neg free, busy, \mathbf{X}\neg busy, \\ \mathbf{true}\ \mathbf{U}(pr_1 \vee pr_2), \mathbf{X}(\mathbf{true}\ \mathbf{U}(pr_1 \vee pr_2)), \varphi \} \end{array} \right\}$$

Подформулы Фишера-Ладнера

Утверждение 4

Пусть I — произвольная темпоральная интерпретация, и φ — произвольная формула в позитивной форме. Тогда для любого момента времени n множество формул

$$B_n = \{\psi \mid \psi \in FLSub_\varphi \text{ и } I, n \models \psi\}$$

является согласованным

Доказательство.

Самостоятельно (достаточно использовать только определение согласованного семейства)

А верно ли обратное утверждение: “каждое согласованное семейство формул выполнимо в некоторой интерпретации в начальный момент времени”?

Подформулы Фишера-Ладнера

Утверждение 5

Пусть φ — LTL-формула в позитивной форме. Тогда

1. **для любой пары множеств $B_{\mathcal{AP}} \subseteq \mathcal{AP} \cap FLSub_\varphi$, $B_X \subseteq XSub_\varphi$ существует согласованное семейство подформул $B \subseteq FLSub_\varphi$, такое что $B \cap \mathcal{AP} = B_{\mathcal{AP}}$ и $B \cap XSub_\varphi = B_X$**
2. **для любой пары согласованных семейств $B_1, B_2 \subseteq FLSub_\varphi$ верно:**

$$B_1 = B_2 \quad \Leftrightarrow \quad B_1 \cap \mathcal{AP} = B_2 \cap \mathcal{AP} \text{ и } B_1 \cap XSub_\varphi = B_2 \cap XSub_\varphi$$

Доказательство.Самостоятельно

Утверждение 6

Если LTL-формула φ содержит n связок и темпоральных операторов, то число различных согласованных семейств $B \subseteq FLSub_\varphi$ не превосходит величины 2^{3n}

Табличный метод model checking

Какую задачу мы решаем?

Даны LTL-формула φ и **конечная** LTS $M = (S, S_0, \to, \rho)$

Проверить справедливость соотношения $M \models \varphi$

Как мы собираемся решать эту задачу?

1. приведём φ к позитивной форме ψ
2. построим
   - 2.1 множество $FLSub_\psi$
   - 2.2 множество $XSub_\psi$
   - 2.3 множество $URSub_\psi$
   - 2.4 все согласованные семейства $B \subseteq FLSub_\psi$: Con_ψ
   - 2.5 систему Хинтикки
   - 2.6 ...

Табличный метод model checking

Система Хинтикки[1] для LTL-формулы φ в позитивной форме и LTS $M = (S, S_0, \to, \rho)$ — это раскрашенный ориентированный граф $G_{\varphi,M} = (V, E)$ следующего вида:

- вершины — это всевозможные пары (состояние M, согласованное семейство формул), такие что текущая разметка подтверждает истинность и ложность всех атомарных высказываний семейства:
$$V = \{(s, B) \mid s \in S,\ B \in Con_\varphi,\ \rho(s) = B \cap \mathcal{AP}\}$$
- дуги — это всевозможные переходы в M с подтверждением предположений вида $\mathbf{X}\psi$:
$$E = \{\langle (s', B'), (s'', B'') \rangle : s' \longrightarrow s'' \text{ и для любой формулы } \mathbf{X}\psi \in XSub_\varphi \text{ верно соотношение } \mathbf{X}\psi \in B' \iff \psi \in B''\}$$

[1] Каарло Яакко Юхани Хинтикка

Табличный метод model checking

Раскрасим граф $G_{\varphi,M}$
Каждой формуле φ_i из множества $URSub_\varphi$ сопоставим уникальный цвет i
Раскрасим в цвет i все вершины (s, B), для которых выполнено **хотя бы одно** из двух условий

в случае, когда $\varphi_i = \psi_i \mathbf{U} \chi_i$:	в случае, когда $\varphi_i = \psi_i \mathbf{R} \chi_i$:
1) $\chi_i \in B$ 2) $\mathbf{X}(\psi_i \mathbf{U} \chi_i) \notin B$	1) $\chi_i \notin B$ 2) $\mathbf{X}(\psi_i \mathbf{R} \chi_i) \in B$

Бесконечный маршрут

$$(s_1, B_1), (s_2, B_2), \ldots, (s_n, B_n), \ldots$$

в графе $G_{\varphi,M}$ назовем радужным, если в нем бесконечно часто встречаются вершины каждого цвета $1, 2, \ldots, |URSub_\varphi|$

Табличный метод model checking

Основная теорема

Для любой LTL-формулы φ в позитивной форме и LTS $M = (S, S_0, \to, \rho)$

$$M \not\models \varphi$$

$$\Updownarrow$$

в графе $G_{\varphi,M}$ существует хотя бы один радужный маршрут, исходящий из вершины (s, B), в которой $s \in S_0$ и $\varphi \notin B$

Табличный метод model checking

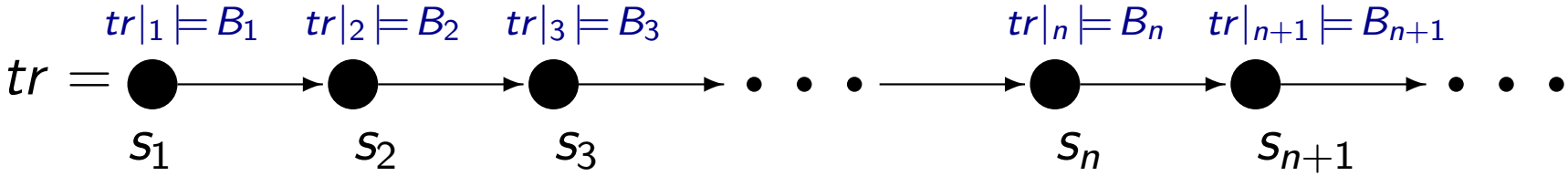
Доказательство.

($\Uparrow$) Предположим, что в графе $G_{\varphi,M}$ есть радужный маршрут

$$(s_1, B_1), (s_2, B_2), \ldots, (s_n, B_n), (s_{n+1}, B_{n+1}), \ldots \ ,$$

в котором $\varphi \notin B_1$

Тогда по определению системы Хинтикки $G_{\varphi,M}$ в LTS M есть начальная трасса



Покажем, что для любой формулы $\psi \in FLSub_\varphi$, и для любого $n \geq 1$, верно

$$tr|_n \models \psi \iff \psi \in B_n$$

Табличный метод model checking

Доказательство.

Если удастся показать, что

$$tr|_n \models \psi \iff \psi \in B_n \qquad (*)$$

то, учитывая $\varphi \notin B_1$, придем к заключению $tr \not\models \varphi$

Для доказательства соотношения $(*)$ воспользуемся индукцией по числу связок в формуле ψ

Базис индукции: $p \in \mathcal{AP}$

$p \in B_n \iff p \in \xi(s_n) \iff tr|_n \models p$

$\neg p \in B_n \iff p \notin B_n \iff p \notin \xi(s_n) \iff tr|_n \not\models p \iff tr|_n \models \neg p$

Табличный метод model checking

Доказательство.

Индуктивный переход

1. Логические связки & и $\vee$

$\psi_1 \& \psi_2 \in B_n$

Табличный метод model checking

Доказательство.
Индуктивный переход

1. Логические связки & и $\vee$

$\psi_1 \& \psi_2 \in B_n \iff \psi_1 \in B_n$ и $\psi_2 \in B_n$

по определению согласованного множества

Табличный метод model checking

Доказательство.
Индуктивный переход

1. Логические связки & и $\vee$

$$\psi_1 \& \psi_2 \in B_n \iff \psi_1 \in B_n \text{ и } \psi_2 \in B_n \iff tr|_n \models \psi_1 \text{ и } tr|_n \models \psi_2$$

по индуктивному предположению

Табличный метод model checking

Доказательство.

Индуктивный переход

1. Логические связки & и $\vee$

$\psi_1 \& \psi_2 \in B_n \iff \psi_1 \in B_n$ и $\psi_2 \in B_n \iff tr|_n \models \psi_1$ и $tr|_n \models \psi_2$
$\iff tr|_n \models \psi_1 \& \psi_2$

Табличный метод model checking

Доказательство.
Индуктивный переход

1. Логические связки & и $\vee$

$\psi_1 \& \psi_2 \in B_n \iff \psi_1 \in B_n$ и $\psi_2 \in B_n \iff tr|_n \models \psi_1$ и $tr|_n \models \psi_2$
$\iff tr|_n \models \psi_1 \& \psi_2$

Для формул вида $\psi_1 \vee \psi_2$ применяются аналогичные рассуждения

Табличный метод model checking

Доказательство.
Индуктивный переход

1. Логические связки & и $\vee$

$\psi_1 \& \psi_2 \in B_n \iff \psi_1 \in B_n$ и $\psi_2 \in B_n \iff tr|_n \models \psi_1$ и $tr|_n \models \psi_2$
$\iff tr|_n \models \psi_1 \& \psi_2$

Для формул вида $\psi_1 \vee \psi_2$ применяются аналогичные рассуждения

2. Темпоральный оператор **X**

$\mathbf{X}\psi \in B_n$

Табличный метод model checking

Доказательство.
Индуктивный переход

1. Логические связки & и $\vee$

$\psi_1 \& \psi_2 \in B_n \iff \psi_1 \in B_n$ и $\psi_2 \in B_n \iff tr|_n \models \psi_1$ и $tr|_n \models \psi_2$
$\iff tr|_n \models \psi_1 \& \psi_2$

Для формул вида $\psi_1 \vee \psi_2$ применяются аналогичные рассуждения

2. Темпоральный оператор **X**

$\mathbf{X}\psi \in B_n \iff \psi \in B_{n+1}$

т. к. $(s_n, B_n) \longrightarrow (s_{n+1}, B_{n+1})$ тогда и только тогда, когда для любой формулы $\mathbf{X}\chi$ верно $\mathbf{X}\chi \in B_n \iff \chi \in B_{n+1}$

Табличный метод model checking

Доказательство.

Индуктивный переход

1. Логические связки & и $\vee$

$\psi_1 \& \psi_2 \in B_n \iff \psi_1 \in B_n$ и $\psi_2 \in B_n \iff tr|_n \models \psi_1$ и $tr|_n \models \psi_2$
$\iff tr|_n \models \psi_1 \& \psi_2$

Для формул вида $\psi_1 \vee \psi_2$ применяются аналогичные рассуждения

2. Темпоральный оператор **X**

$\mathbf{X}\psi \in B_n \iff \psi \in B_{n+1} \iff tr|_{n+1} \models \psi \in B_{n+1}$

по индуктивному предположению

Табличный метод model checking

Доказательство.
Индуктивный переход

1. Логические связки & и $\vee$

$\psi_1 \& \psi_2 \in B_n \iff \psi_1 \in B_n$ и $\psi_2 \in B_n \iff tr|_n \models \psi_1$ и $tr|_n \models \psi_2$
$\iff tr|_n \models \psi_1 \& \psi_2$

Для формул вида $\psi_1 \vee \psi_2$ применяются аналогичные рассуждения

2. Темпоральный оператор $\mathbf{X}$

$\mathbf{X}\psi \in B_n \iff \psi \in B_{n+1} \iff tr|_{n+1} \models \psi \in B_{n+1} \iff tr|_n \models \mathbf{X}\psi$

по определению выполнимости формул $\mathbf{X}\chi$

Табличный метод model checking

Индуктивный переход.

3. Темпоральный оператор **R**

3.1. Покажем $\psi_1 \mathbf{R} \psi_2 \in B_n \Longrightarrow tr|_n \models \psi_1 \mathbf{R} \psi_2$

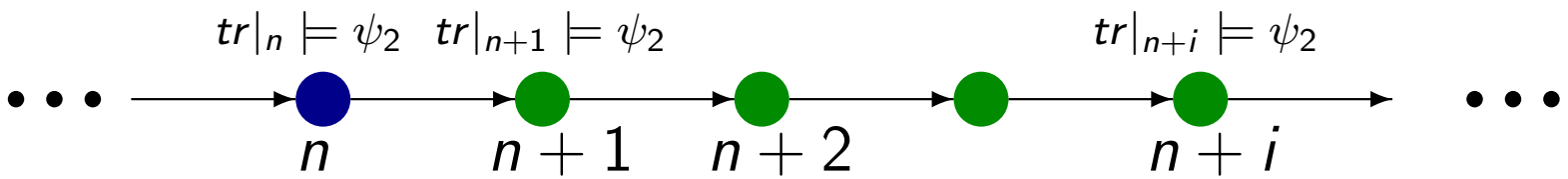
Заметим, что согласно определению согласованного семейства $\psi_1 \mathbf{R} \psi_2 \in B \iff \psi_2 \in B$ и при этом $\psi_1 \in B$ или $\mathbf{X}(\psi_1 \mathbf{R} \psi_2) \in B$

Пусть $\psi_1 \mathbf{R} \psi_2 \in B_n$. Тогда возможны 2 случая

Вариант 1: $\mathbf{X}(\psi_1 \mathbf{R} \psi_2) \in B_{n+i}$ для любого $i, i \geq 0$

Тогда по определению $G_{\varphi_1, M}$ в каждом множестве B_{n+i}, $i \geq 0$, содержится формула $\psi_1 \mathbf{R} \psi_2$ и, следовательно, $\psi_2 \in B_{n+i}$

Тогда по индуктивному предположению $tr|_{n+i} \models \psi_2$ для любого $i, i \geq 0$. Следовательно, $tr|_n \models \psi_1 \mathbf{R} \psi_2$



Табличный метод model checking

Индуктивный переход

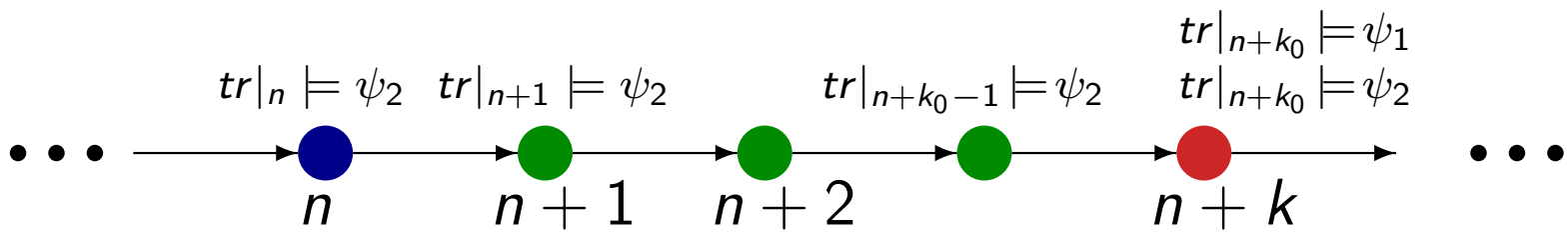
Вариант 2: $\mathbf{X}(\psi_1 \mathbf{R} \psi_2) \notin B_{n+k}$ для некоторого $k, k \geq 0$

Тогда существует такое k_0, что $\mathbf{X}(\psi_1 \mathbf{R} \psi_2) \notin B_{n+k_0}$, но $\mathbf{X}(\psi_1 \mathbf{R} \psi_2) \in B_{n+i}$ для любого $i, 0 \leq i < k_0$

Тогда по определению графа $G_{\varphi_1, M}$ в каждом множестве B_{n+i}, $0 \leq i \leq k_0$, содержится формула $\psi_1 \mathbf{R} \psi_2$

Тогда по определению согласованных семейств подформул $\psi_2 \in B_{n+i}$ для любого $i, 0 \leq i \leq k_0$, и, кроме того, $\psi_1 \in B_{n+k_0}$

Тогда по индуктивному предположению $tr|_{n+i} \models \psi_2$ для любого $0 \leq i \leq k_0$ и $tr|_{n+k_0} \models \psi_1$. Значит, $tr|_n \models \psi_1 \mathbf{R} \psi_2$



Итак, в обоих случаях $\psi_1 \mathbf{R} \psi_2 \in B_n \Longrightarrow tr|_n \models \psi_1 \mathbf{R} \psi_2$

Табличный метод model checking

Индуктивный переход

3.2. Покажем $\psi_1 \mathbf{R} \psi_2 \notin B_n \Longrightarrow tr|_n \not\models \psi_1 \mathbf{R} \psi_2$

Пусть $\psi_1 \mathbf{R} \psi_2 \notin B_n$. Т. к. $\psi_1 \mathbf{R} \psi_2 \in URSub_{\varphi_1}$ этой формуле соответствует некоторый цвет j

Поскольку рассматриваемый маршрут

$$(s_1, B_1), (s_2, B_2), \ldots, (s_n, B_n), (s_{n+1}, B_{n+1}), \ldots$$

является радужным, то вершины, окрашенные в цвет j, встречаются в этом маршруте бесконечно часто

Значит, существует такое $k \geq 0$, что вершина (s_{n+k}, B_{n+k}) — первая, окрашенная в цвет j вершина, следующая в этом радужном маршруте вслед за вершиной (s_n, B_n)

Имеются две причины, по которым вершина (s_{n+k}, B_{n+k}) оказалась окрашенной в цвет j: $\psi_2 \notin B_{n+k}$ и $\mathbf{X}(\psi_1 \mathbf{R} \psi_2) \in B_{n+k}$

Рассмотрим каждый из этих случаев

Табличный метод model checking

Индуктивный переход

Случай 1: $\psi_2 \notin B_{n+k}$

Т. к. все вершины (s_{n+i}, B_{n+i}), $0 \leq i < k$ не окрашены в цвет j, для каждого из множеств B_{n+i}, $0 \leq i < k$, верны соотношения

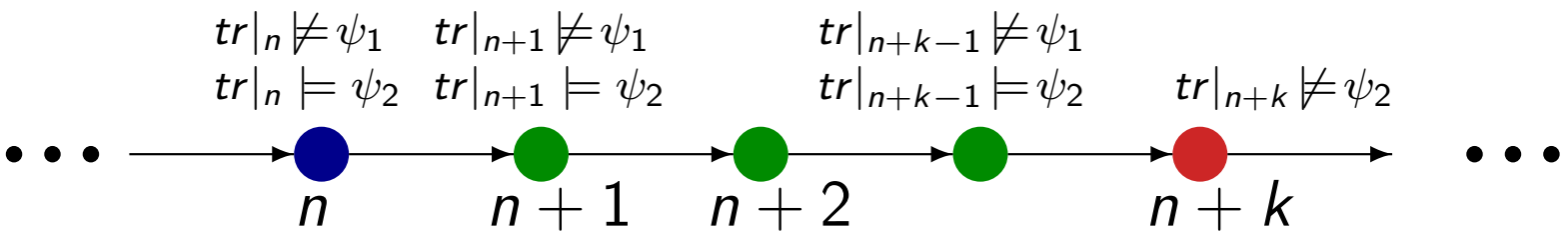
$$\psi_2 \in B_{n+i} \qquad \text{и} \qquad \mathbf{X}(\psi_1 \mathbf{R} \psi_2) \notin B_{n+i}$$

Тогда по определению графа $G_{\varphi_1, M}$ для каждого множества B_{n+i}, $0 \leq i < k$, верно соотношение $\psi_1 \mathbf{R} \psi_2 \notin B_{n+i}$. А отсюда следует, что $\psi_1 \notin B_{n+i}$ для любого $i, 0 \leq i < k$

Тогда по индуктивному предположению

$tr|_{n+i} \models \psi_2$ и $tr|_{n+i} \not\models \psi_1$ для любого $i, 0 \leq i < k$,

$tr|_{n+k} \not\models \psi_2$



А это означает, что $tr|_n \not\models \psi_1 \mathbf{R} \psi_2$

Табличный метод model checking

Индуктивный переход

Случай 2: $\mathbf{X}(\psi_1 \mathbf{R} \psi_2) \in B_{n+k}$

Т. к. все вершины (s_{n+i}, B_{n+i}), $0 \leq i < k$ не окрашены в цвет j, для каждого из множеств B_{n+i}, $0 \leq i < k$, верны соотношения

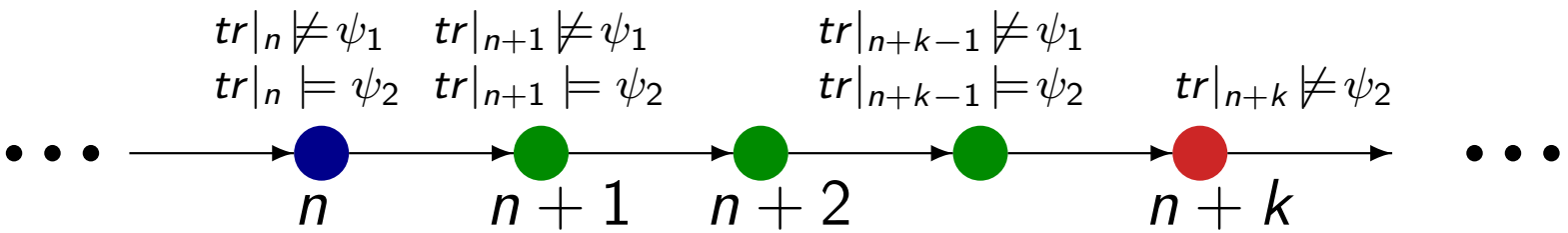
$$\psi_2 \in B_{n+i} \qquad \text{и} \qquad \mathbf{X}(\psi_1 \mathbf{R} \psi_2) \notin B_{n+i}$$

Тогда по определению графа $G_{\varphi_1, M}$ для каждого множества B_{n+i}, $0 \leq i \leq k$, верно соотношение $\psi_1 \mathbf{R} \psi_2 \notin B_{n+i}$. А отсюда следует, что $\psi_1 \notin B_{n+i}$ для любого $i, 0 \leq i < k$ и $\psi_2 \notin B_{n+k}$

Тогда по индуктивному предположению

$tr|_{n+i} \models \psi_2$ и $tr|_{n+i} \not\models \psi_1$ для любого $i, 0 \leq i < k$,

$tr|_{n+k} \not\models \psi_2$



И во втором случае $tr|_n \not\models \psi_1 \mathbf{R} \psi_2$

Табличный метод model checking

Индуктивный переход

Таким образом, если $\psi_1 \mathbf{R} \psi_2 \notin B_n$, то $tr|_n \not\models \psi_1 \mathbf{R} \psi_2$

В итоге, для любой формулы вида $\psi_1 \mathbf{R} \psi_2$ и для любой вершины (s_n, B_n) нашего радужного маршрута верно соотношение

$$\psi_1 \mathbf{R} \psi_2 \in B_n \iff tr|_n \models \psi_1 \mathbf{R} \psi_2$$

4. Темпоральный оператор **U**

Для доказательства соотношения

$$\psi_1 \mathbf{U} \psi_2 \in B_n \iff tr|_n \models \psi_1 \mathbf{U} \psi_2$$

применяются рассуждения, аналогичные тем, которые были использованы для исследования оператора **R**

Самостоятельно

Табличный метод model checking

Завершив обоснование индуктивного перехода, мы тем самым завершили доказательство первой части теоремы:

$$M \not\models \varphi$$

$$\Uparrow$$

в графе $G_{\varphi,M}$ существует хотя бы один радужный маршрут, исходящий из вершины (s, B), в которой $s \in S_0$ и $\varphi \notin B$

Покажем, что в том случае, когда имеет место $M \not\models \varphi$, в графе $G_{\varphi,M}$ из некоторой вершины (s, B), в которой $s \in S_0$ и $\varphi \notin B$, исходит хотя бы один радужный маршрут

Табличный метод model checking

Пусть $M \not\models \varphi$. Тогда в LTS M существует такая начальная трасса tr, для которой $tr \not\models \varphi$. Рассмотрим эту трассу tr

Для каждого $i, i \geq 1$, положим

$$B_i = \{\psi : \psi \in FLSub_\varphi, tr|_i \models \psi\}$$

По утверждению 4 все построенные множества B_i являются согласованными

Покажем, что последовательность пар

$(tr[1], B_1), (tr[2], B_2), (tr[3], B_3), \ldots, (tr[n], B_n), (tr[n+1], B_{n+1}), \ldots$

образует радужный маршрут в графе G_φ

Табличный метод model checking

Действительно,

1. Для любого $n, n \geq 1$, верно $tr[n] \longrightarrow tr[n+1]$, поскольку tr — маршрут в LTS M.

2. Для любого $n, n \geq 1$ и для любой формулы $\mathbf{X}\psi \in XSub_{\varphi}$, верно

$$\mathbf{X}\psi \in B_n \iff \psi \in B_{n+1}$$

поскольку

$$\mathbf{X}\psi \in B_n \iff tr|_n \models \mathbf{X}\psi \iff tr|_{n+1} \models \psi \iff \psi \in B_{n+1}$$

3. $tr[1] \in S_0$ (т. к. tr — начальная трасса в M) и $\varphi \notin B_1$ (т. к. $tr|_1 \not\models \varphi$)

Значит, последовательность

$$(tr[1], B_1), (tr[2], B_2), (tr[3], B_3), \ldots, (tr[n], B_n), (tr[n+1], B_{n+1}), \ldots$$

является маршрутом в графе $G_{\varphi,M}$, исходящим из нужной вершины

Табличный метод model checking

4. Осталось показать, что маршрут

$$(tr[1], B_1), (tr[2], B_2), (tr[3], B_3), \ldots, (tr[n], B_n), (tr[n+1], B_{n+1}), \ldots$$

является радужным

Рассмотрим произвольное число n, $n \geq 1$ и произвольную формулу $\psi_i \in URSub_\varphi$. Покажем, что существует такое k, $k \geq 0$, что вершина $(tr[n+k], B_{n+k})$ окрашена в цвет i

Табличный метод model checking

Ограничимся рассмотрением формулы вида $\psi_i = \chi_1 \mathbf{U} \chi_2$.
(Для формул вида $\psi_i = \chi_1 \mathbf{R} \chi_2$ — самостоятельно)

1. Если $tr|_n \not\models \mathbf{X}(\chi_1 \mathbf{U} \chi_2)$, то $\mathbf{X}(\chi_1 \mathbf{U} \chi_2) \notin B_n$, и, следовательно, вершина $(tr[n], B_n)$ окрашена в цвет i
2. А если $tr|_n \models \mathbf{X}(\chi_1 \mathbf{U} \chi_2)$, то $tr|_{n+1} \models \chi_1 \mathbf{U} \chi_2$. Тогда существует такое $k, k \geq 1$, что $tr|_{n+k} \models \chi_2$. Поэтому $\chi_2 \in B_{n+k}$, и вершина $(tr[n+k], B_{n+k})$ окрашена в цвет i

Таким образом, вершины цвета i встречаются в нашем маршруте бесконечно часто. Поскольку ψ_i была произвольной (Until-Release)-формулой, это означает, что наш маршрут в графе $G_{\varphi,M}$ является радужным

конец доказательства

Алгоритм model checking

Но как проверить, что из заданной вершины в графе $G_{\varphi,M}$ не исходит ни одного радужного маршрута?

Ориентированный граф G называется сильно связным, если для любой пары вершин v и u в графе G существует маршрут из v в u и маршрут из u в v

Всякий максимальный сильно связный подграф графа G называется компонентой сильной связности

Компоненту сильной связности графа (системы Хинтикки) $G_{\varphi,M}$ будем называть радужной, если в ней содержатся вершины **всех** цветов

Алгоритм model checking

Теорема

Из вершины v в графе $G_{\varphi,M}$ исходит радужный маршрут тогда и только тогда, когда существует маршрут , ведущий из вершины v хотя бы в одну из вершин хотя бы одной радужной компоненты сильной связности

Доказательство.

Очевидно (самостоятельно)

Алгоритм model checking

Исходные данные: LTL-формула φ и LTS $M = (S, S_0, \to, \rho)$

1. Построить равносильную позитивную форму ψ
2. Построить систему Хинтикки $G_{\psi,M}$
3. Выделить множество подформул $URSub_\psi$ и раскрасить вершины графа $G_{\psi,M}$
4. Выделить радужные компоненты сильной связности в графе $G_{\psi,M}$
5. Выделить множество V' всех вершин графа $G_{\psi,M}$, из которых достижимы радужные компоненты сильной связности
6. Выделить множество V'' всех вершин (s, B), для которых выполняется $s \in S_0$, $\psi \notin B$
7. Вычислить $V = V' \cap V''$

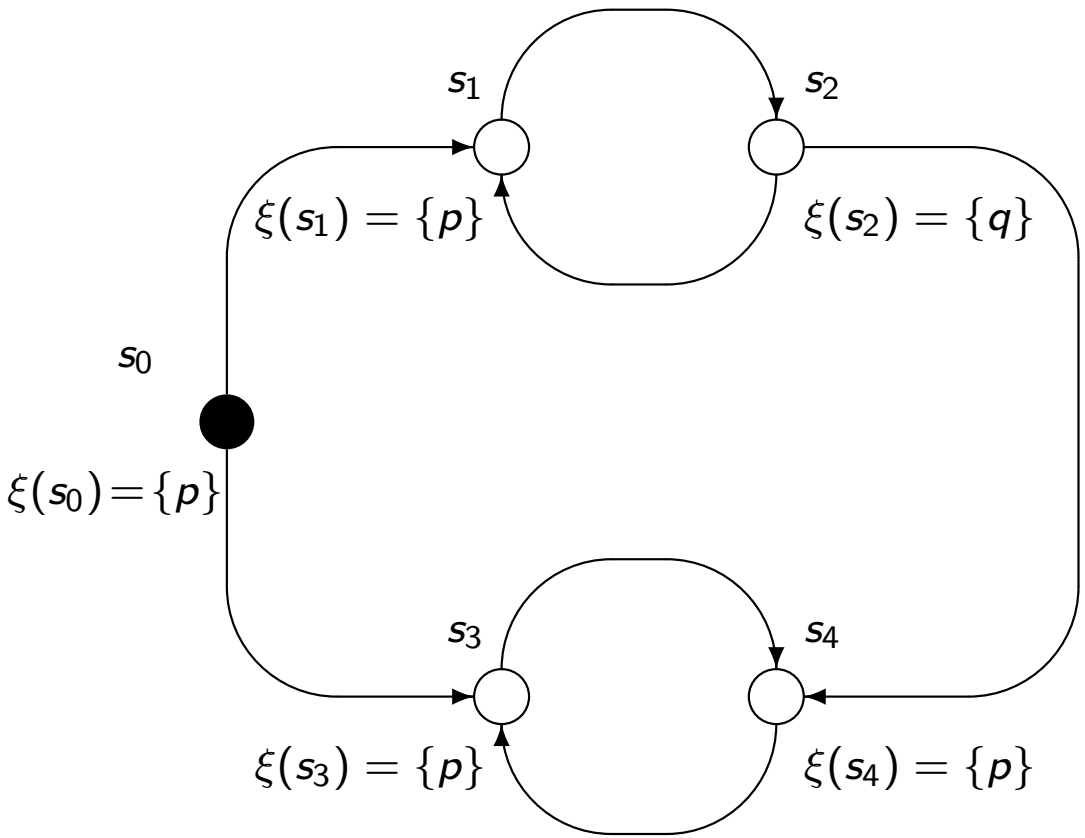
Результат: $M \models \varphi \iff V = \emptyset$

Алгоритм model checking

Пример

$$\varphi = p\mathbf{U}q$$

LTS M:



Алгоритм model checking

Пример

$\varphi = p\mathbf{U}q$

1. Позитивная форма $\varphi_1 = p\mathbf{U}q$

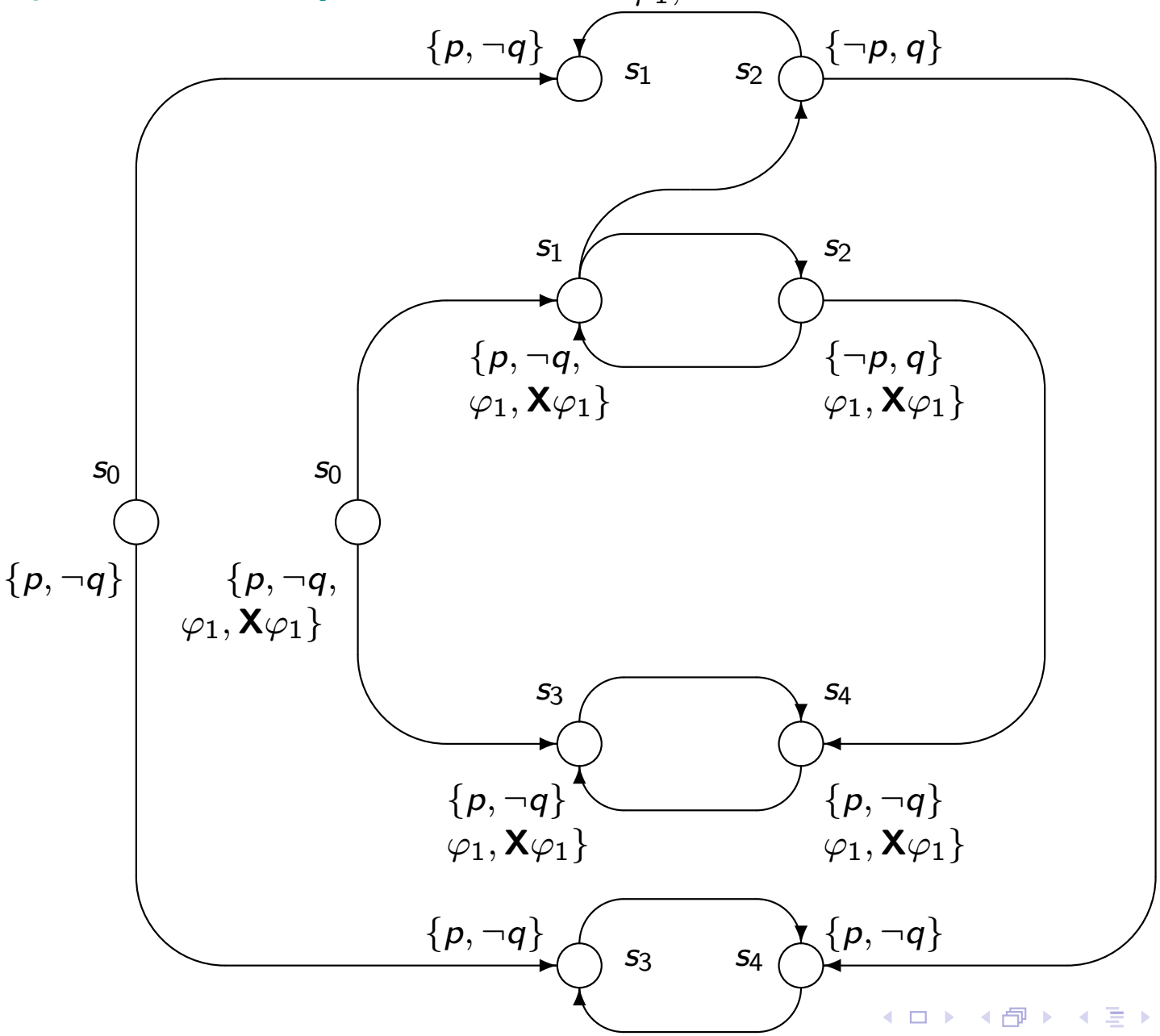
$FLSub_{\varphi_1} = \{p, \neg p, q, \neg q, p\mathbf{U}q, \mathbf{X}(p\mathbf{U}q)\}$

$XSub_{\varphi_1} = \{\mathbf{X}(p\mathbf{U}q)\}$

$URSub_{\varphi_1} = \{p\mathbf{U}q\}$

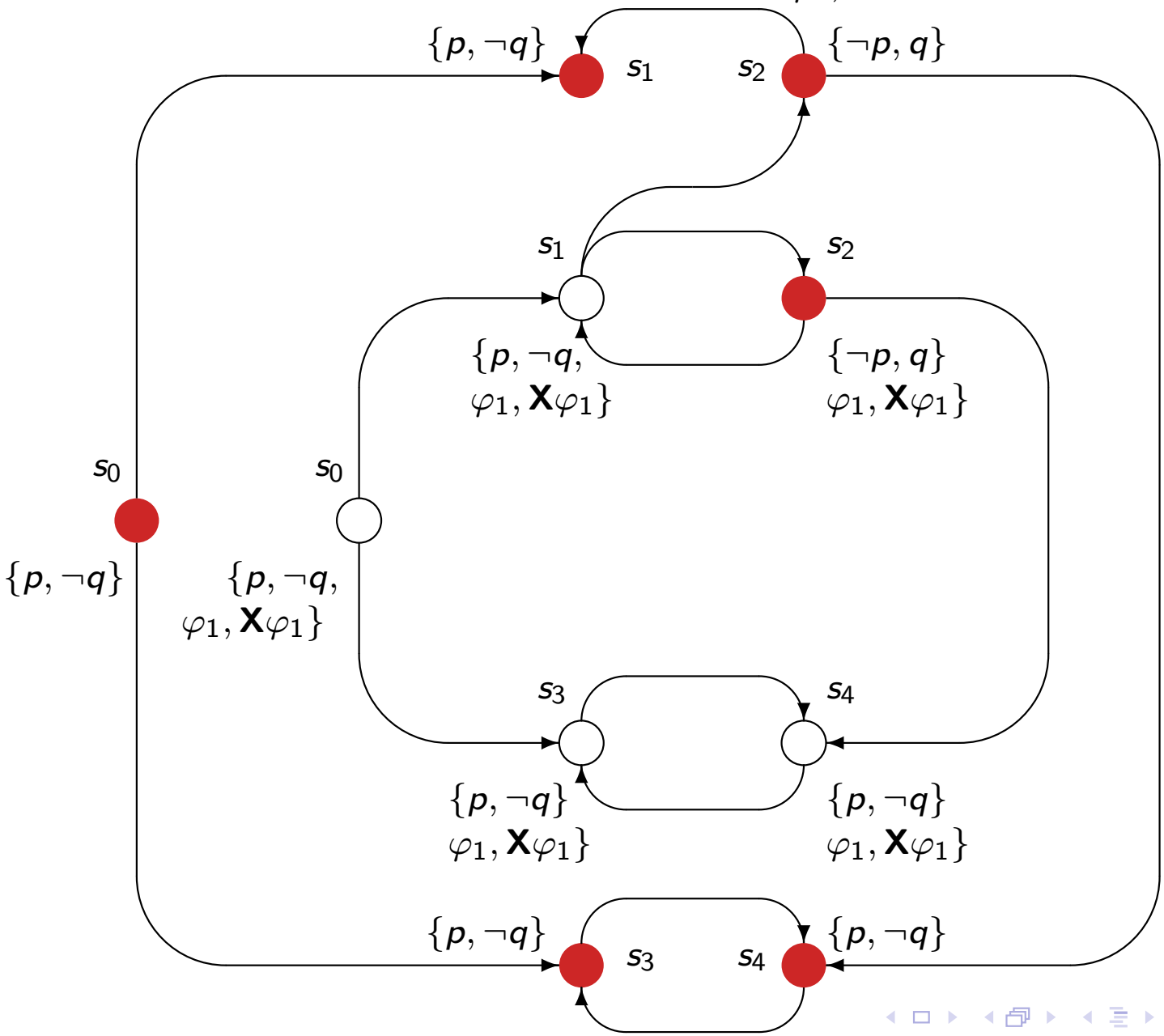
Алгоритм model checking

2. Строим систему Хинтикки $G_{\varphi_1, M}$



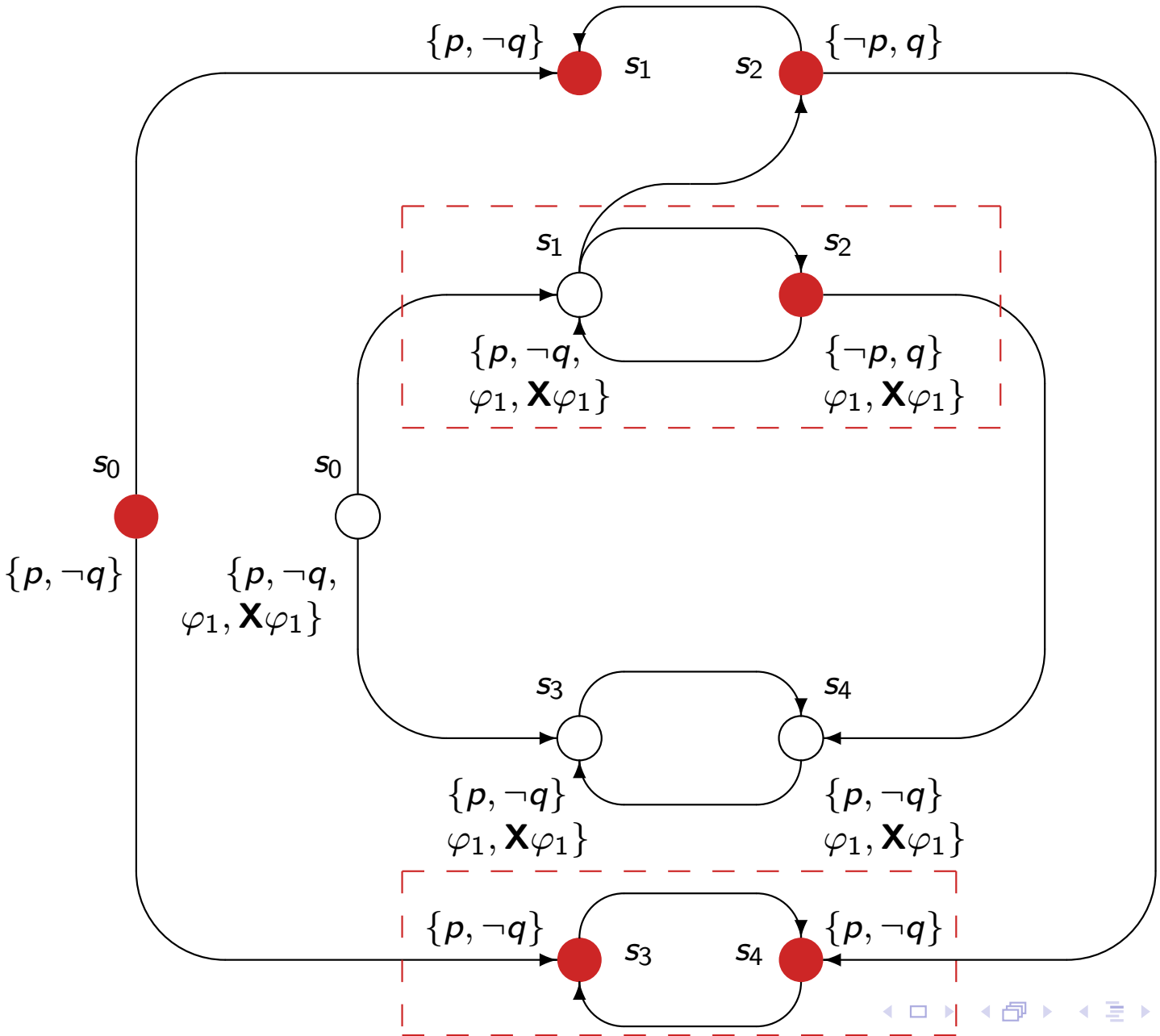
Алгоритм model checking

3. Раскрашиваем вершины системы $G_{\varphi_1, M}$



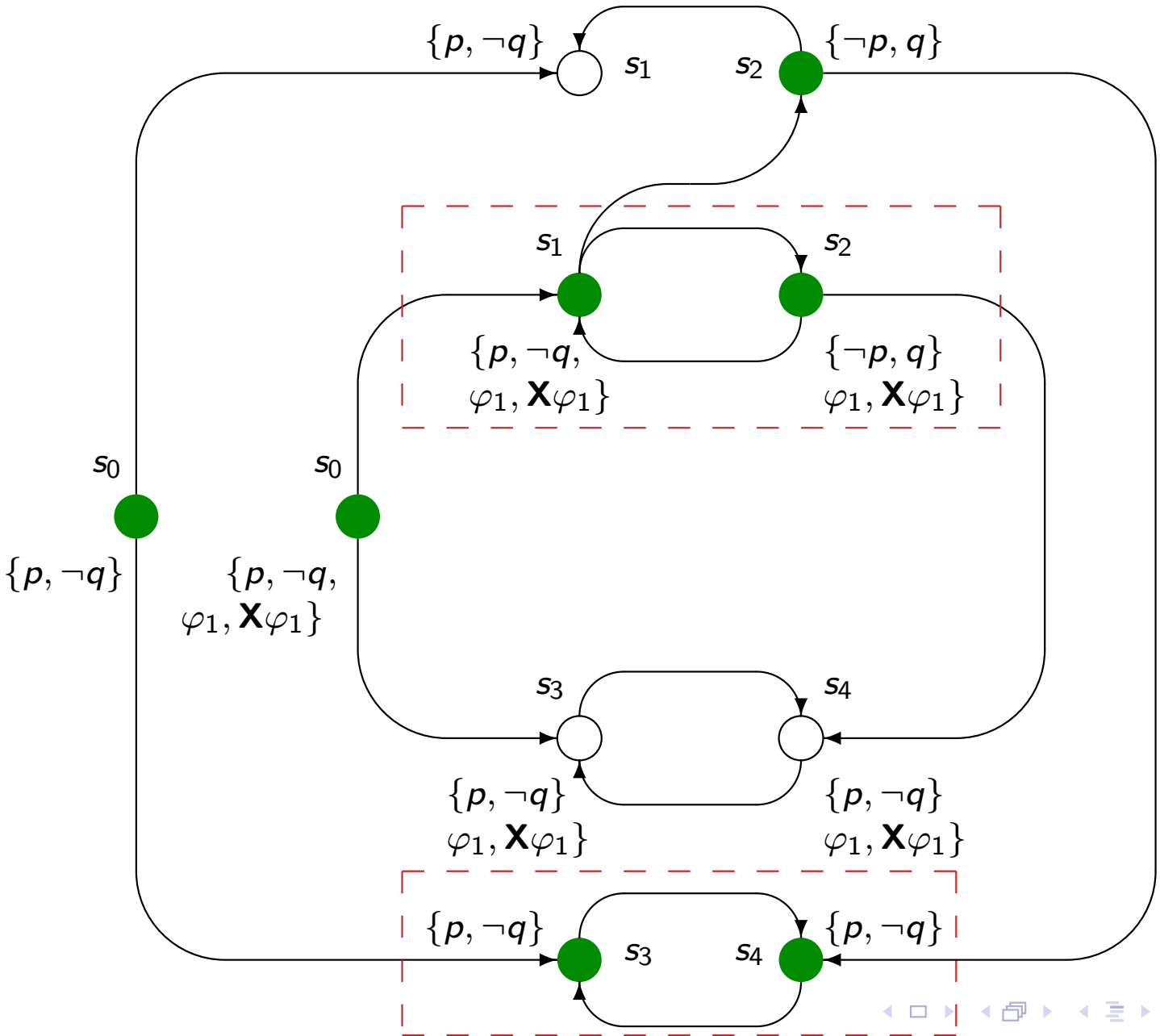
Алгоритм model checking

4. Выделяем радужные компоненты сильной связности



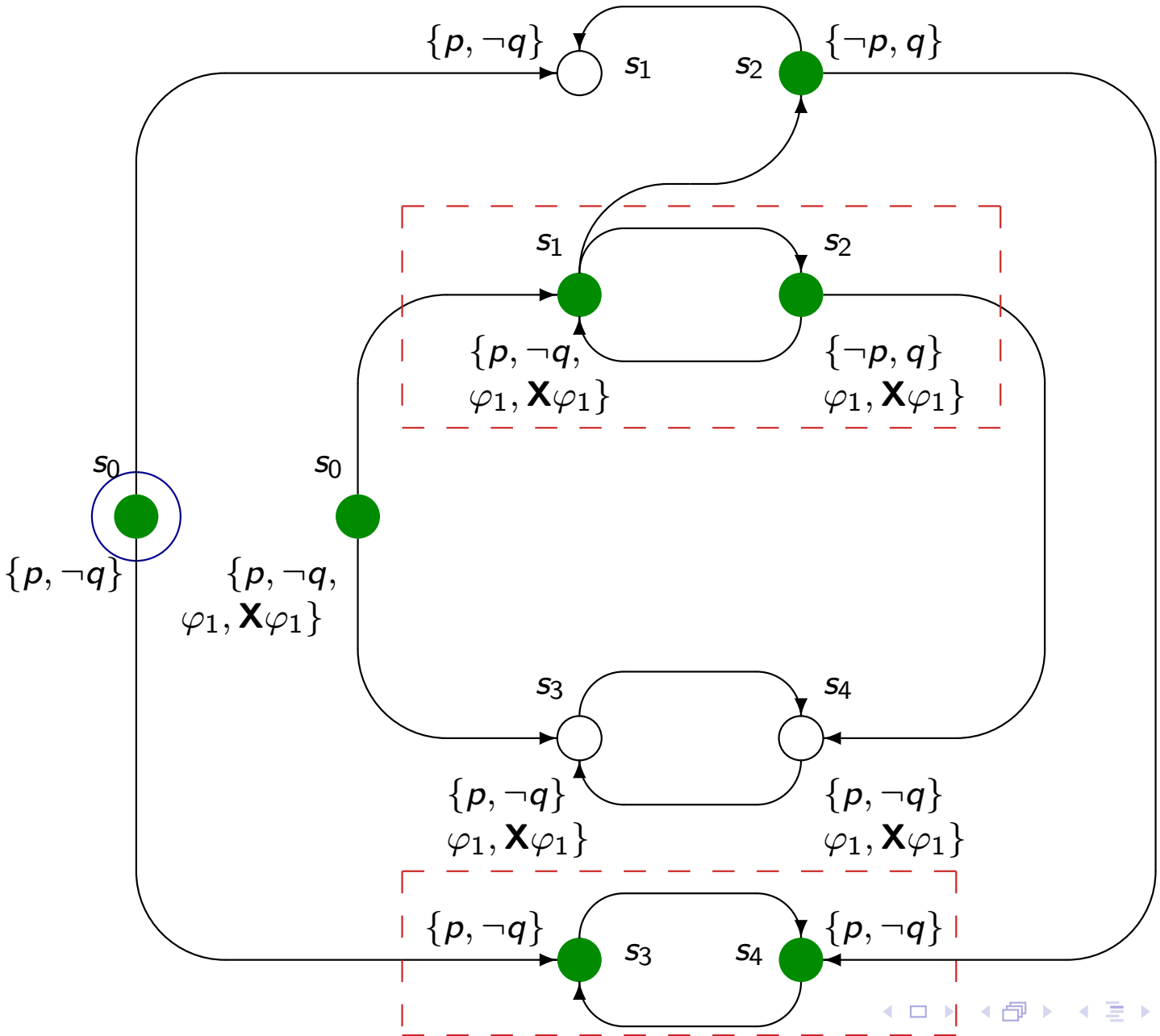
Алгоритм model checking

5. Выделяем вершины из которых достижимы радужные компонент



Алгоритм model checking

6. Ищем вершину (s_0, B) на которой опровергается φ_1



Алгоритм model checking

И в заключение несколько вопросов

1. Какова сложность описанного алгоритма model checking в зависимости от размеров формулы и LTS?
2. Можно ли видоизменить описанный алгоритм model checking так, чтобы при раскраске вершин системы Хинтикки можно было ограничиться только одним цветом?
3. Можно ли видоизменить описанный алгоритм model checking так, чтобы не строить всю систему Хинтикки целиком?

Если вы смогли ответить на эти вопросы, то вы поняли, как устроена проверка LTL-формул с помощью табличного метода

А ещё это реализовано и применяется в: SPIN, NuSMV, ...

Конец лекции 19