Основы математической логики и логического программирования

ЛЕКТОР: В.А. Захаров

Лекция 23.

Задача верификации моделей программ. Подформулы Фишера-Ладнера. Табличный метод верификации моделей программ. Алгоритм верификации моделей программ.

ЗАДАЧА ВЕРИФИКАЦИИ МОДЕЛЕЙ ПРОГРАММ

Задача model checking для PLTL

Для заданной формулы PLTL φ и конечной LTS M проверить $M \models \varphi$.

Почему задача model checking непроста? Потому что

- выполнимость формул PLTL проверяется на бесконечных интерпретациях,
- В LTS M имеется бесконечно много интерпретаций (трасс).

Почему задача model checking имеет эффективное решение? Потому что

- все это бесконечное множество бесконечных интерпретаций «упаковано» в **конечную** структуру — LTS M.

ЗАДАЧА ВЕРИФИКАЦИИ МОДЕЛЕЙ ПРОГРАММ

Замысел табличного метода

1. Вместо проверки выполнимости φ во всех интерпретациях лучше заняться поиском контрмодели — интерпретации I, в которой не выполняется φ.
2. Выполнимость всякой формулы φ полностью определяется выполнимостью ее подформул. Поэтому (не)выполнимость формул можно проверять индуктивно.
3. (Не)выполнимость формулы на одной из трасс LTS M, начинающейся в состоянии s, — это свойство состояния s. Значит, проверяя (не)выполнимость всех подформул формулы φ для всех состояний LTS M, можно вычислить множество $\overline{S}_\varphi$ всех тех состояний, в которых не выполняется формула φ. Если $S_0 \cap \overline{S}_\varphi \neq \varnothing$, то $M \not\models \varphi$.

ЗАДАЧА ВЕРИФИКАЦИИ МОДЕЛЕЙ ПРОГРАММ

Вспомогательные определения и обозначения

Для заданной LTS $M = \langle \mathcal{AP}, S, S_0, \longrightarrow, \rho \rangle$, трассы $tr = s_{i_0}, s_{i_1}, \ldots, s_{i_n}, s_{i_{n+1}}, \ldots$ в LTS M и формулы PLTL φ будем использовать запись

- $tr \models \varphi$ для обозначения отношения выполнимости $I(tr), 0 \models \varphi$;
- $tr[j]$ для обозначения j-го состояния s_{i_j} в трассе tr;
- $tr|_j$ для обозначения трассы $tr' = s_{i_j}, s_{i_{j+1}}, \ldots,$ являющейся суффиксом трассы tr, начинающейся состоянием s_{i_j}.

ЗАДАЧА ВЕРИФИКАЦИИ МОДЕЛЕЙ ПРОГРАММ

Утверждение 1.

Для любой LTS M и формула PLTL φ верно

$M \not\models \varphi \iff$ существует такая начальная трасса tr, $tr \in Tr_0(M)$, для которой $tr \not\models \varphi$.

Доказательство.

Самостоятельно.

Таким образом, вместо задачи $M \models \varphi$ мы будем рассматривать другую задачу:

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

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

ЗАДАЧА ВЕРИФИКАЦИИ МОДЕЛЕЙ ПРОГРАММ

Приведение формулы к позитивной форме

Применяя равносильные преобразования, упростим формулу φ.

Этап 1. Удаление импликации $\to$ и темпоральных операторов $\mathbf{G}, \mathbf{F}$ на основании законов взаимной зависимости

$$\models\ \psi \to \psi \equiv \neg\psi \vee \chi;$$

$$\models\ \mathbf{F}\psi \equiv \mathbf{true}\ \mathbf{U}\psi; \qquad \models\ \mathbf{G}\psi \equiv \mathbf{false}\ \mathbf{R}\psi.$$

Этап 2. Продвижение $\neg$ вглубь формулы на основании законов двойственности

$$\models\ \neg(\psi \& \chi) \equiv \neg\psi \vee \neg\chi; \qquad \models\ \neg(\psi \vee \chi) \equiv \neg\psi \& \neg\chi;$$

$$\models \neg\neg\psi \equiv \psi; \qquad \models\ \neg\mathbf{X}\psi \equiv \mathbf{X}\neg\psi;$$

$$\models\ \neg(\psi\mathbf{U}\chi) \equiv \neg\psi\mathbf{R}\neg\chi; \qquad \models\ \neg(\psi\mathbf{R}\chi) \equiv \neg\psi\mathbf{U}\neg\chi.$$

ЗАДАЧА ВЕРИФИКАЦИИ МОДЕЛЕЙ ПРОГРАММ

Утверждение 2.

В результате применения равносильных преобразований этапов 1 и 2 любая формула PLTL φ приводится к равносильной формуле φ', представленной в позитивной форме, в которой

- используются только логические связки $\vee, \&, \neg$ и темпоральные операторы $\mathbf{X}, \mathbf{U}, \mathbf{R}$,
- связка $\neg$ применяется только к атомарным высказываниям $p, \;\; p \in \mathcal{AP}$.

Доказательство.

Самостоятельно.

ЗАДАЧА ВЕРИФИКАЦИИ МОДЕЛЕЙ ПРОГРАММ

Приведение формулы к позитивной форме

Пример.

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

Этап 1.

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

Этап 2.

$\varphi_1 = \mathbf{false}\ \mathbf{R}\ (\neg\mathit{free} \ \vee\ \mathbf{X}\neg\mathit{busy} \ \vee\ \mathbf{X}(\mathbf{true}\ \mathbf{U}(\mathit{pr}_1 \ \vee\ \mathit{pr}_2))).$

ПОДФОРМУЛЫ ФИШЕРА–ЛАДНЕРА

Пусть φ_1 — формула PLTL в позитивной форме. Тогда множеством подформул Фишера–Ладнера называется наименьшее множество формул PLTL $FLSub_{\varphi_1}$, содержащее формулу φ_1 и удовлетворяющее следующим условиям:

- если $p \in FLSub_{\varphi_1}$ и $p \in \mathcal{AP}$, то $\neg p \in FLSub_{\varphi_1}$,
- если $\psi \& \chi \in FLSub_{\varphi_1}$, то $\{\psi, \chi\} \subseteq FLSub_{\varphi_1}$,
- если $\psi \vee \chi \in FLSub_{\varphi_1}$, то $\{\psi, \chi\} \subseteq FLSub_{\varphi_1}$,
- если $\neg\psi \in FLSub_{\varphi_1}$, то $\psi \in FLSub_{\varphi_1}$,
- если $\mathbf{X}\psi \in FLSub_{\varphi_1}$, то $\psi \in FLSub_{\varphi_1}$,
- если $\psi \mathbf{U} \chi \in FLSub_{\varphi_1}$, то $\{\psi, \chi, \mathbf{X}(\psi \mathbf{U} \chi)\} \subseteq FLSub_{\varphi_1}$,
- если $\psi \mathbf{R} \chi \in FLSub_{\varphi_1}$, то $\{\psi, \chi, \mathbf{X}(\psi \mathbf{R} \chi)\} \subseteq FLSub_{\varphi_1}$.

Утверждение 3.

Если φ_1 содержит n логических связок и темпоральных операторов, то $|FLSub_{\varphi_1}| \leq 3n$.

ПОДФОРМУЛЫ ФИШЕРА–ЛАДНЕРА

Пример.

Пусть

$\varphi_1 = \mathbf{false}\ \mathbf{R}\ (\neg \mathit{free} \ \vee\ \mathbf{X}\neg \mathit{busy} \ \vee\ \mathbf{X}(\mathbf{true}\ \mathbf{U}(\mathit{pr}_1 \ \vee\ \mathit{pr}_2)))$.

Тогда

$$\begin{aligned}
\mathit{FLSub}_{\varphi_1} \quad = \quad & \{\varphi_1, \\
& \mathbf{false}, {\color{red}\mathbf{X}\varphi_1}, \ \neg \mathit{free} \ \vee\ \mathbf{X}\neg \mathit{busy} \ \vee\ \mathbf{X}(\mathbf{true}\ \mathbf{U}(\mathit{pr}_1 \ \vee\ \mathit{pr}_2)), \\
& \neg \mathit{free}, \ \mathbf{X}\neg \mathit{busy}, \ \mathbf{X}(\mathbf{true}\ \mathbf{U}(\mathit{pr}_1 \ \vee\ \mathit{pr}_2)), \\
& \mathit{free}, \neg \mathit{busy}, \ \mathbf{true}\ \mathbf{U}(\mathit{pr}_1 \ \vee\ \mathit{pr}_2), \\
& \mathit{busy}, \mathbf{true}, \mathit{pr}_1 \ \vee\ \mathit{pr}_2, \\
& \mathit{pr}_1, \ \mathit{pr}_2, \ \neg \mathit{pr}_1, \ \neg \mathit{pr}_2\}.
\end{aligned}$$

Подформулы Фишера–Ладнера

Next-подформулы

Пусть φ_1 — формула PLTL в позитивной форме и $FLSub_{\varphi_1}$ — множеством подформул Фишера–Ладнера формулы φ_1.

Тогда запись $XSub_{\varphi_1}$ будет обозначать множество всех тех подформул Фишера–Ладнера, которые начинаются оператором **X** (neXttime), т. е.

$$XSub_{\varphi_1} = \{\psi \;:\; \psi = \mathbf{X}\chi,\; \psi \in FLSub_{\varphi_1}\}.$$

Пример.

Пусть

$\varphi_1 = \mathbf{false}\ \mathbf{R}\ (\neg free \ \vee\ \mathbf{X}\neg busy \ \vee\ \mathbf{X}(\mathbf{true}\ \mathbf{U}(pr_1 \ \vee\ pr_2)))$.

Тогда

$$\begin{aligned} XSub_{\varphi_1} \;=\; & \{\mathbf{X}\varphi_1,\ \mathbf{X}\neg busy, \\ & \mathbf{X}(\mathbf{true}\ \mathbf{U}(pr_1 \ \vee\ pr_2))\}. \end{aligned}$$

ПОДФОРМУЛЫ ФИШЕРА–ЛАДНЕРА

(Until-Release)-подформулы

Пусть φ_1 — формула PLTL в позитивной форме и $FLSub_{\varphi_1}$ — множеством подформул Фишера–Ладнера формулы φ_1.

Тогда запись $URSub_{\varphi_1}$ будет обозначать множество всех тех подформул Фишера–Ладнера, которые начинаются оператором **U** (Until) или **R** (Release), т. е.

$$\begin{array}{rcl} USub_{\varphi_1} & = & \{\psi \;:\; \psi = \chi_1 \mathbf{U} \chi_2,\ \psi \in FLSub_{\varphi_1}\} \cup \\ & & \{\psi \;:\; \psi = \chi_1 \mathbf{R} \chi_2,\ \psi \in FLSub_{\varphi_1}\}. \end{array}$$

Пример.

Пусть

$\varphi_1 = \mathbf{false}\ \mathbf{R}\ (\neg free \ \vee\ \mathbf{X}\neg busy \ \vee\ \mathbf{X}(\mathbf{true}\ \mathbf{U}(pr_1 \ \vee\ pr_2)))$.

Тогда

$$USub_{\varphi_1} = \{\varphi_1, \mathbf{true}\ \mathbf{U}(pr_1 \ \vee\ pr_2)\}.$$

ПОДФОРМУЛЫ ФИШЕРА–ЛАДНЕРА

Согласованные множества подформул

Пусть φ_1 — формула PLTL в позитивной форме, и $FLSub_{\varphi_1}$ — множество подформул Фишера–Ладнера для φ_1.
Тогда согласованным семейством подформул формулы φ_1 называется всякое подмножество B, $B \subseteq FLSub_{\varphi_1}$, удовлетворяющее следующим условиям:

1. $\mathbf{true} \in B$, $\mathbf{false} \notin B$,
2. для любого атомарного высказывания p, $p \in \mathcal{AP} \cap FLSub_{\varphi_1}$, выполняется **в точности одно из двух** включений: либо $p \in B$, либо $\neg p \in B$;
3. $\psi \vee \chi \in B \iff \psi \in B$ или $\chi \in B$,
4. $\psi \& \chi \in B \iff \psi \in B$ и $\chi \in B$,
5. $\psi \mathbf{U} \chi \in B \iff \chi \in B$ или $\{\psi, \mathbf{X}(\psi \mathbf{U} \chi)\} \subseteq B$,
6. $\psi \mathbf{R} \chi \in B \iff \chi \in B$ и при этом $\psi \in B$ или $\mathbf{X}(\psi \mathbf{R} \chi) \in B$.

ПОДФОРМУЛЫ ФИШЕРА–ЛАДНЕРА

Согласованные множества подформул

Согласованные семейства подформул — это максимальные множества формул, которые не содержат «явных» противоречий, т. е. таких противоречий, которые можно обнаружить в текущий момент времени.

Например, множество, состоящее из двух формул

$\mathbf{X}p$ — завтра я пойду на лекцию,

$\mathbf{X}\neg p$ — завтра я не пойду на лекцию,

может быть согласованным (хотя и противоречивым), поскольку сегодня возможное противоречие, содержащееся в этих высказываниях, не проявляется.

Согласованное семейство подформул является аналогом 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

Согласованные семейства подформул

Пример.

Пусть

$$\begin{aligned} FLSub_{\varphi_1} \;=\; & \{free,\ busy,\ pr_1,\ pr_2,\ \neg free,\ \neg busy,\ \neg pr_1,\ \neg pr_2, \\ & pr_1 \ \vee \ pr_2, \\ & \mathbf{true}\ \mathbf{U}(pr_1 \ \vee \ pr_2), \\ & \mathbf{X}\neg busy, \mathbf{X}(\mathbf{true}\ \mathbf{U}(pr_1 \ \vee \ pr_2)), \\ & \neg free \ \vee \ \mathbf{X}\neg busy \ \vee \ \mathbf{X}(\mathbf{true}\ \mathbf{U}(pr_1 \ \vee \ pr_2)), \\ & \varphi_1, \mathbf{X}\varphi_1\}. \end{aligned}$$

Тогда одним из согласованных семейств подформул формулы φ_1 является множество

$$\begin{aligned} B \;=\; & \{\mathbf{true}, pr_1,\ \neg pr_2, \neg free,\ busy, \mathbf{X}\neg busy, \\ & \mathbf{true}\ \mathbf{U}(pr_1 \ \vee \ pr_2),\ \mathbf{X}(\mathbf{true}\ \mathbf{U}(pr_1 \ \vee \ pr_2)), \varphi_1\}. \end{aligned}$$

ПОДФОРМУЛЫ ФИШЕРА–ЛАДНЕРА

Утверждение 4.

Пусть I — произвольная темпоральная интерпретация, и φ_1 — произвольная формула в позитивной форме.
Тогда для любого момента времени n множество формул

$$B_n = \{\psi \ : \ \psi \in FLSub_{\varphi_1} \text{ и } I, n \models \psi\}$$

является согласованным.

Доказательство.

Самостоятельно. Непосредственно из определения 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_1 — формула PLTL в позитивной форме. Тогда

1. для любой пары $B' \subseteq \mathcal{AP} \cap FLSub_{\varphi_1}$, $B'' \subseteq XSub_{\varphi_1}$, существует такое согласованное семейство подформул B, для которого верно $B \cap \mathcal{AP} = B'$, $B \cap XSub_{\varphi_1} = B''$;
2. для любой пары B_1 и B_2 согласованных семейств подформул Фишера-Ладнера φ_1 верны соотношения
$$B_1 = B_2 \iff B_1 \cap \mathcal{AP} = B_2 \cap \mathcal{AP} \text{ и } B_1 \cap XSub_{\varphi_1} = B_1 \cap XSub_{\varphi_1}.$$

Доказательство.

Самостоятельно.

Утверждение 6.

Если φ_1 содержит n логических связок и темпоральных операторов, то число различных согласованных семейств подформул Фишера-Ладнера не превосходит величины 2^{3n}.

ТАБЛИЧНЫЙ МЕТОД ВЕРИФИКАЦИИ МОДЕЛЕЙ ПРОГРАММ

Пусть задана формулы PLTL φ и конечная LTS
$M = \langle \mathcal{AP}, S, S_0, \longrightarrow, \rho \rangle$.
Нужно проверить выполнимость $M \models \varphi$.

Для этого

ТАБЛИЧНЫЙ МЕТОД ВЕРИФИКАЦИИ МОДЕЛЕЙ ПРОГРАММ

Пусть задана формулы PLTL φ и конечная LTS $M = \langle \mathcal{AP}, S, S_0, \longrightarrow, \rho \rangle$.
Нужно проверить выполнимость $M \models \varphi$.

Для этого

1. формула φ приводится к позитивной форме φ_1,
2. для формулы φ_1 строятся
   - множество подформул Фишера–Ладнера $FLSub_{\varphi_1}$,
   - множество Next-подформул $XSub_{\varphi_1}$,
   - множество UR-подформул $URSub_{\varphi_1}$,
   - совокупность Con_{φ_1} всех возможных согласованных семейств подформул Фишера–Ладнера.

ТАБЛИЧНЫЙ МЕТОД ВЕРИФИКАЦИИ МОДЕЛЕЙ ПРОГРАММ

Системой Хинтикки для формулы PLTL φ_1 и LTS M называется раскрашенный ориентированный граф $G_{\varphi_1,M} = (V, E)$ с множеством вершин V и множеством дуг E, которые устроены так:

$$V = \{(s, B) \ : \ s \in S,\ B \in Con_{\varphi_1},\ \rho(s) = B \cap \mathcal{AP}\},$$

т. е. вершинами графа являются всевозможные пары (состояние s, согласованное семейство B), для которых разметка $\rho(s)$ состояния s подтверждает истинность всех атомарных высказываний множества B;

$$\begin{aligned} E \ = \ \{\langle (s', B'), (s'', B'')\rangle \ &: \ s' \longrightarrow s'' \\ &\text{и для любой Next-подформулы } \mathbf{X}\psi, \mathbf{X}\psi \in XSub_{\varphi_1}, \\ &\text{верно соотношение } \ \mathbf{X}\psi \in B' \iff \psi \in B''\}, \end{aligned}$$

т. е. дугами графа являются все такие переходы LTS M, которые позволяют подтвердить все обещания $\mathbf{X}\psi$ выполнить ψ в следующий момент времени.

ТАБЛИЧНЫЙ МЕТОД ВЕРИФИКАЦИИ

Теперь проведем раскраску вершин графа $\Gamma_{\varphi_1,M} = (V, E)$.
Рассмотрим множество (Until-Release)-подформул
$URSub_{\varphi_1} = \{\chi'_1 \mathbf{U} \chi''_1, \dots, \chi'_k \mathbf{U} \chi''_k, \chi'_{k+1} \mathbf{R} \chi''_{k+1}, \dots, \chi'_{k+m} \mathbf{R} \chi''_{k+m}\}$.
Каждой формуле ψ_i из множества $URSub_{\varphi_1}$ сопоставим индивидуальный цвет i.
Раскрасим в цвет i все вершины (s, B), для которых выполнено **хотя бы одно** из двух условий

в случае, когда $\psi_i = \chi'_i \mathbf{U} \chi''_i$:	в случае, когда $\psi_i = \chi'_i \mathbf{R} \chi''_i$:
1) $\chi''_i \in B$, 2) $\mathbf{X}(\chi'_i \mathbf{U} \chi''_i) \notin B$.	1) $\chi''_i \notin B$, 2) $\mathbf{X}(\chi'_i \mathbf{R} \chi''_i) \in B$.

ТАБЛИЧНЫЙ МЕТОД ВЕРИФИКАЦИИ

Теперь проведем раскраску вершин графа $\Gamma_{\varphi_1,M} = (V, E)$.
Рассмотрим множество (Until-Release)-подформул
$URSub_{\varphi_1} = \{\chi'_1 \mathbf{U} \chi''_1, \dots, \chi'_k \mathbf{U} \chi''_k, \chi'_{k+1} \mathbf{R} \chi''_{k+1}, \dots, \chi'_{k+m} \mathbf{R} \chi''_{k+m}\}$.
Каждой формуле ψ_i из множества $URSub_{\varphi_1}$ сопоставим индивидуальный цвет i.
Раскрасим в цвет i все вершины (s, B), для которых выполнено **хотя бы одно** из двух условий

в случае, когда $\psi_i = \chi'_i \mathbf{U} \chi''_i$:	в случае, когда $\psi_i = \chi'_i \mathbf{R} \chi''_i$:
1) $\chi''_i \in B$, 2) $\mathbf{X}(\chi'_i \mathbf{U} \chi''_i) \notin B$.	1) $\chi''_i \notin B$, 2) $\mathbf{X}(\chi'_i \mathbf{R} \chi''_i) \in B$.

Бесконечный маршрут

$$(s_{i_1}, B_{i_1}), (s_{i_2}, B_{i_2}), \dots, (s_{i_n}, B_{i_n}), \dots$$

в графе $\Gamma_{\varphi_1,M}$ назовем радужным, если в нем бесконечно часто встречаются вершины каждого цвета $1, 2, \dots, k$.

ТАБЛИЧНЫЙ МЕТОД ВЕРИФИКАЦИИ

Основная теорема

Для любой формулы PLTL φ_1 в позитивной форме и LTS $M = \langle \mathcal{AP}, S, S_0, \longrightarrow, \rho \rangle$

$$M \not\models \varphi_1$$

$$\Updownarrow$$

в графе $\Gamma_{\varphi_1, M}$ существует хотя бы один радужный маршрут, исходящий из вершины $v_0 = (s_0, B_0)$, в которой $s_0 \in S_0$ и $\varphi_1 \notin B_0$.

ТАБЛИЧНЫЙ МЕТОД ВЕРИФИКАЦИИ

Доказательство.

($\Uparrow$) Предположим, что в графе $\Gamma_{\varphi_1,M}$ есть радужный маршрут

$$(s_0, B_0), (s_1, B_1), \dots, (s_n, B_n), (s_{n+1}, B_{n+1}), \dots$$

указанного вида, в котором $\varphi_1 \notin B_0$.

ТАБЛИЧНЫЙ МЕТОД ВЕРИФИКАЦИИ

Доказательство.

(⇑) Предположим, что в графе $\Gamma_{\varphi_1,M}$ есть радужный маршрут

$$(s_0, B_0), (s_1, B_1), \dots, (s_n, B_n), (s_{n+1}, B_{n+1}), \dots$$

указанного вида, в котором $\varphi_1 \notin B_0$.
Тогда согласно определению системы Хинтикки $\Gamma_{\varphi_1,M}$ в LTS M есть начальная трасса

$$tr = \underset{s_0}{\bullet} \longrightarrow \underset{s_1}{\bullet} \longrightarrow \underset{s_2}{\bullet} \longrightarrow \bullet\ \bullet\ \bullet \longrightarrow \underset{s_n}{\bullet} \longrightarrow \underset{s_{n+1}}{\bullet} \longrightarrow \bullet\ \bullet\ \bullet$$

ТАБЛИЧНЫЙ МЕТОД ВЕРИФИКАЦИИ

Доказательство.

($\Uparrow$) Предположим, что в графе $\Gamma_{\varphi_1,M}$ есть радужный маршрут

$$(s_0, B_0), (s_1, B_1), \dots, (s_n, B_n), (s_{n+1}, B_{n+1}), \dots$$

указанного вида, в котором $\varphi_1 \notin B_0$.
Тогда согласно определению системы Хинтикки $\Gamma_{\varphi_1,M}$ в LTS M есть начальная трасса

$$tr = \underset{s_0}{\overset{tr|_0 \models B_0}{\bullet}} \longrightarrow \underset{s_1}{\overset{tr|_1 \models B_1}{\bullet}} \longrightarrow \underset{s_2}{\overset{tr|_2 \models B_2}{\bullet}} \longrightarrow \bullet\ \bullet\ \bullet \longrightarrow \underset{s_n}{\overset{tr|_n \models B_n}{\bullet}} \longrightarrow \underset{s_{n+1}}{\overset{tr|_{n+1} \models B_{n+1}}{\bullet}} \longrightarrow \bullet\ \bullet\ \bullet$$

Покажем, что для любой формулы ψ, $\psi \in FLSub_{\varphi_1}$, и для любого n, $n \geq 0$, верно

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

ТАБЛИЧНЫЙ МЕТОД ВЕРИФИКАЦИИ

Доказательство.

Если удастся показать, что

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

то, учитывая $\varphi_1 \notin B_0$, придем к заключению $tr \not\models \varphi_1$.
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 ВЕРИФИКАЦИИ

Доказательство.

Индуктивный переход.

ТАБЛИЧНЫЙ МЕТОД ВЕРИФИКАЦИИ

Доказательство.

Индуктивный переход.

1. Логические связки & и $\vee$.

$\psi_1 \& \psi_2 \in B_n$

ТАБЛИЧНЫЙ МЕТОД ВЕРИФИКАЦИИ

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 ВЕРИФИКАЦИИ

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 $tr|_n \models \psi_2$

по индуктивному предположению

ТАБЛИЧНЫЙ МЕТОД ВЕРИФИКАЦИИ

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 ВЕРИФИКАЦИИ

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 ВЕРИФИКАЦИИ

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 ВЕРИФИКАЦИИ

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 $\mathbf{X}$.

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

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

ТАБЛИЧНЫЙ МЕТОД ВЕРИФИКАЦИИ

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 $\mathbf{X}$.

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

по индуктивному предположению

ТАБЛИЧНЫЙ МЕТОД ВЕРИФИКАЦИИ

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 ВЕРИФИКАЦИИ

Индуктивный переход.

3. Темпоральный оператор **R**.

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

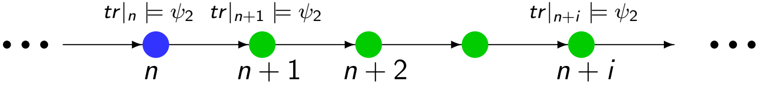
Заметим, что согласно определению согласованного семейства $\psi_1 \mathbf{R} \psi_2 \in B \iff \psi_2 \in B$ и при этом $\psi_1 \in B$ или $\mathbf{X}(\psi_1 \mathbf{R} \psi_2) \in B$.

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 $\Gamma_{\varphi_1, M}$ 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 ВЕРИФИКАЦИИ

Индуктивный переход.

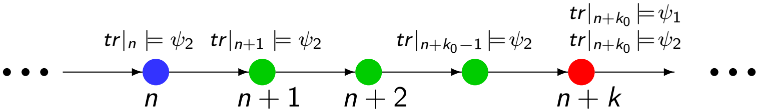
Вариант 2. $\mathbf{X}(\psi_1 \mathbf{R} \psi_2) \notin B_{n+k}$ для некоторого k, $k \geq 0$.

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 $\Gamma_{\varphi_1, M}$ 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 ВЕРИФИКАЦИИ

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

$$(s_0, B_0), (s_1, B_1), \dots, (s_n, B_n), (s_{n+1}, B_{n+1}), \dots$$

является радужным, то вершины, окрашенные в цвет j, встречаются в этом маршруте бесконечно часто.
Значит, существует такое k, $k \geq 0$, 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:

- $\psi_2 \notin B_{n+k}$,
- $\mathbf{X}(\psi_1 \mathbf{R} \psi_2) \in B_{n+k}$,

Рассмотрим каждый из этих случаев по отдельности.

ТАБЛИЧНЫЙ МЕТОД ВЕРИФИКАЦИИ

Индуктивный переход.

Вариант 1. $\psi_2 \notin B_{n+k}$.

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

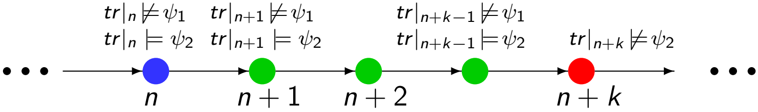
$$\psi_2 \in B_{n+i} \qquad \text{и} \qquad \mathbf{X}(\psi_1 \mathbf{R} \psi_2) \notin B_{n+i}.$$

Тогда по определению графа $\Gamma_{\varphi_1,M}$ для каждого множества B_{n+i}, $0 \le i < k$, 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, $0 \le i < k$.

Тогда по индуктивному предположению

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

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



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

ТАБЛИЧНЫЙ МЕТОД ВЕРИФИКАЦИИ

Индуктивный переход.

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

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

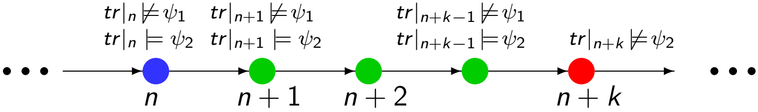
$$\psi_2 \in B_{n+i} \qquad \text{и} \qquad \mathbf{X}(\psi_1 \mathbf{R} \psi_2) \notin B_{n+i}.$$

Тогда по определению графа $\Gamma_{\varphi_1, M}$ для каждого множества B_{n+i}, $0 \le i \le k$, 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, $0 \le i < k$ 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, $0 \le i < k$,

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



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

ТАБЛИЧНЫЙ МЕТОД ВЕРИФИКАЦИИ

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

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

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

Самостоятельно.

ТАБЛИЧНЫЙ МЕТОД ВЕРИФИКАЦИИ

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

$$M \not\models \varphi_1$$

$$\Uparrow$$

в графе $\Gamma_{\varphi_1,M}$ существует хотя бы один радужный маршрут, исходящий из вершины $v_0 = (s_0, B_0)$, в которой $s_0 \in S_0$ и $\varphi_1 \notin B_0$.

Покажем, что в том случае, когда имеет место $M \not\models \varphi_1$, в графе $\Gamma_{\varphi_1,M}$ из некоторой вершины $v_0 = (s_0, B_0)$, в которой $s_0 \in S_0$ и $\varphi_1 \notin B_0$, исходит хотя бы один радужный маршрут.

ТАБЛИЧНЫЙ МЕТОД ВЕРИФИКАЦИИ

Пусть $M \not\models \varphi_1$. Тогда в LTS M существует такая начальная трасса tr, для которой $tr \not\models \varphi_1$. Рассмотрим эту трассу tr.

Для каждого i, $i \geq 0$, положим

$$B_i = \{\psi \ : \ \psi \in FLSub_{\varphi_1}, tr|_i \models \psi \ .\}$$

Согласно утверждению 4, все построенные множества B_i являются согласованными.

Покажем, что последовательность пар

$$(tr[0], B_0), (tr[1], B_1), (tr[2], B_2), \dots, (tr[n], B_n), (tr[n+1], B_{n+1}), \dots$$

образует искомый радужный маршрут в графе Γ_{φ_1}.

ТАБЛИЧНЫЙ МЕТОД ВЕРИФИКАЦИИ

Действительно,

1. Для любого n, $n \geq 0$, верно $tr[n] \longrightarrow tr[n+1]$, поскольку tr — маршрут в LTS M.

2. Для любого n, $n \geq 0$ и для любой формулы $\mathbf{X}\psi \in XSub_{\varphi_1}$, 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. $tr[0] \in S_0$ (т. к. tr — начальная трасса в M) и $\varphi_1 \notin B_0$ (т. к. $tr|_0 \not\models \varphi_1$).

Значит, последовательность

$$(tr[0], B_0), (tr[1], B_1), (tr[2], B_2), \ldots, (tr[n], B_n), (tr[n+1], B_{n+1}), \ldots$$

является маршрутом в графе $\Gamma_{\varphi_1, M}$, исходящим из нужной вершины.

ТАБЛИЧНЫЙ МЕТОД ВЕРИФИКАЦИИ

4. Осталось показать, что маршрут

$$(tr[0], B_0), (tr[1], B_1), (tr[2], B_2), \dots, (tr[n], B_n), (tr[n{+}1], B_{n+1}), \dots$$

является радужным.

Рассмотрим произвольное число n, $n \geq 0$ и произвольную формулу $\psi_i \in URSub_{\varphi_1}$. Покажем, что существует такое k, $k \geq 0$, что вершина $(tr[n+k], B_{n+k})$ окрашена в цвет i.

ТАБЛИЧНЫЙ МЕТОД ВЕРИФИКАЦИИ

Ограничимся рассмотрением Until-формулы $\psi_i = \chi' \mathbf{U} \chi_2$.
(Для формул вида $\psi_i = \chi' \mathbf{R} \chi_2$ доказательство проведите 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 j встречаются в нашем маршруте бесконечно часто. Поскольку ψ_i была произвольной (Until-Release)-формулой, это означает, что наш маршрут в графе $\Gamma_{\varphi_1, M}$ является радужным. $\square$

АЛГОРИТМ ВЕРИФИКАЦИИ МОДЕЛЕЙ ПРОГРАММ

Но как проверить, что из заданной вершины в графе $\Gamma_{\varphi_1,M}$ не исходит ни одного радужного маршрута?

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

Всякий максимальный сильно связный подграф графа Γ называется компонентой сильной связности .

Компоненту сильной связности графа (системы Хинтикки) $\Gamma_{\varphi_1,M}$ будем называть радужной, если в ней содержатся вершины **всех** цветов.

АЛГОРИТМ ВЕРИФИКАЦИИ МОДЕЛЕЙ ПРОГРАММ

Теорема.

Из вершины v в графе $\Gamma_{\varphi_1, M}$ 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.

Самостоятельно. Здесь все очевидно.

АЛГОРИТМ ВЕРИФИКАЦИИ МОДЕЛЕЙ ПРОГРАММ

Исходные данные: формула PLTL φ и LTS $M = \langle \mathcal{AP}, S, S_0, \longrightarrow, \rho \rangle$.

1. Построить равносильную позитивную форму φ_1.
2. Построить систему Хинтикки $\Gamma_{\varphi_1, M}$.
3. Выделить множество подформул $URSub_{\varphi_1}$ и раскрасить вершины графа $\Gamma_{\varphi_1, M}$.
4. Выделить радужные компоненты сильной связности в графе $\Gamma_{\varphi_1, M}$.
5. Выделить множество V' всех вершин графа $\Gamma_{\varphi_1, M}$, из которых достижимы радужные компоненты сильной связности.
6. Выделить множество V'' всех вершин (s_0, B_0), для которой выполняется $s_0 \in S_0$, $\varphi_1 \notin B_0$.
7. Вычислить $V = V' \cap V''$.

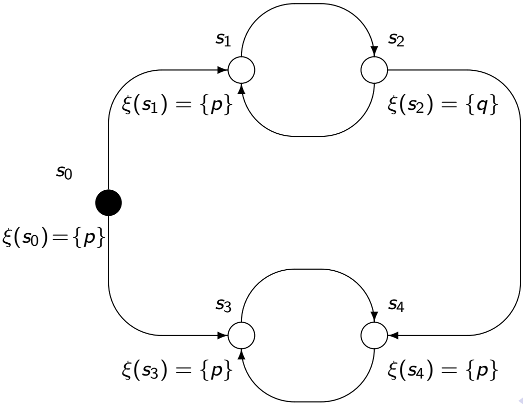
Результат: $M \models \varphi \iff V = \varnothing$.

АЛГОРИТМ ВЕРИФИКАЦИИ МОДЕЛЕЙ ПРОГРАММ

Пример.

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

LTS M:



АЛГОРИТМ ВЕРИФИКАЦИИ МОДЕЛЕЙ ПРОГРАММ

Пример.

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

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

АЛГОРИТМ ВЕРИФИКАЦИИ МОДЕЛЕЙ ПРОГРАММ

Пример.

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

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

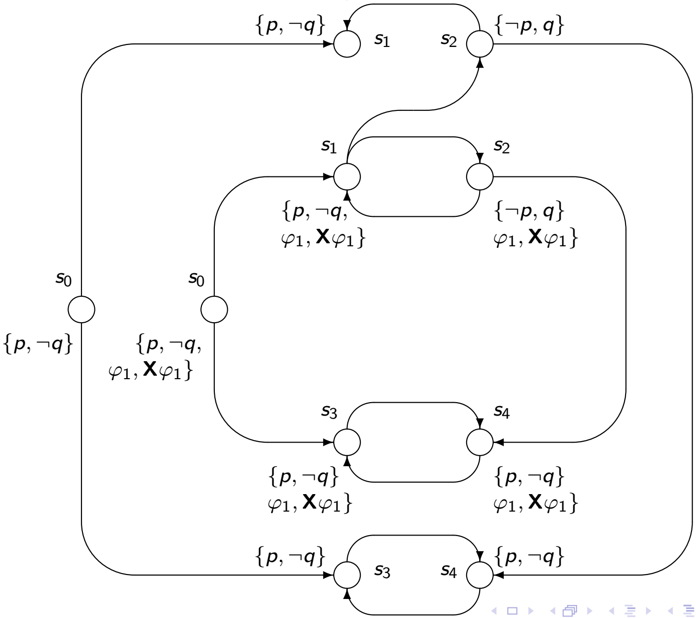
$FLSub_{\varphi_1} = \{p, \neg p, q, \neg q, p\mathbf{U}q, \mathbf{X}(p\mathbf{U}q)\};$

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

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

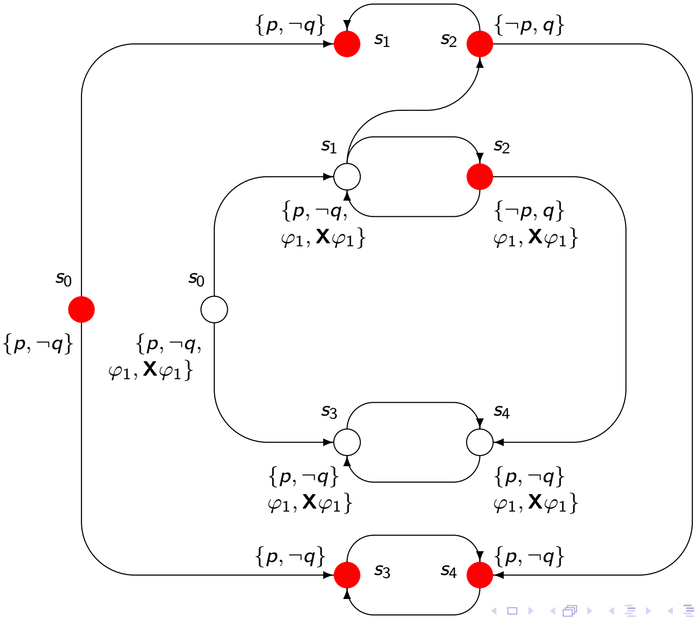
АЛГОРИТМ ВЕРИФИКАЦИИ

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



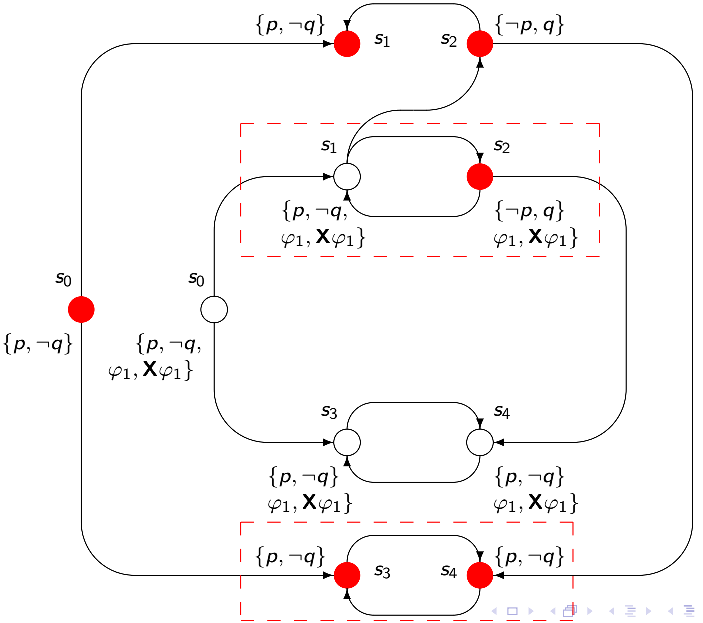
АЛГОРИТМ ВЕРИФИКАЦИИ

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



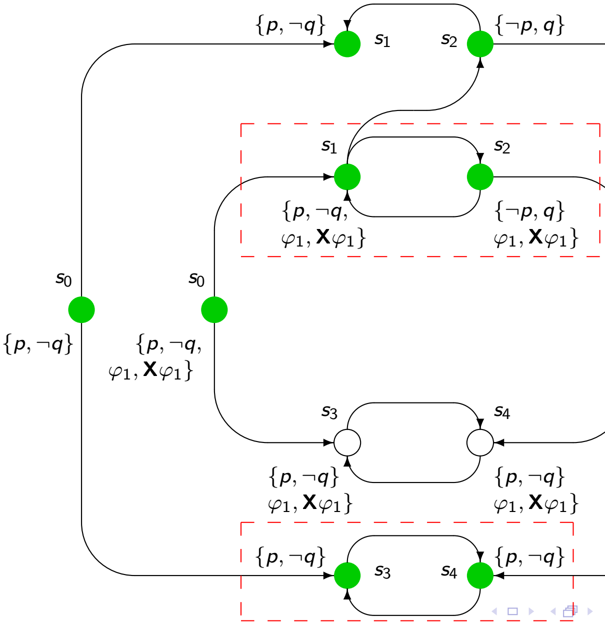
АЛГОРИТМ ВЕРИФИКАЦИИ

4. Выделяем радужные компоненты сильной связности



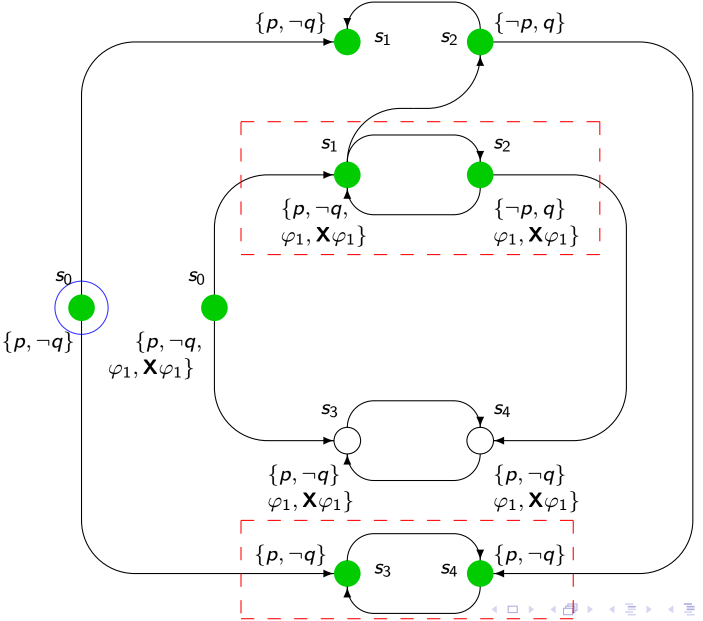
АЛГОРИТМ ВЕРИФИКАЦИИ

5. Выделяем вершины из которых достижимы радужные компоненты



АЛГОРИТМ ВЕРИФИКАЦИИ

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



Алгоритм верификации моделей программ

Описанный здесь подход к верификации распределенных программ реализован в программно-инструментальной системе верификации **SPIN** .

Модели параллельных взаимодействующих процессов описываются на языке **PROMELA** (Process Meta Language), снабжаются темпоральными спецификациями (PLTL формулами), а затем выполнимость этих формул проверяется системой верификации **SPIN** .

В системе **SPIN** применяется табличный алгоритм верификации моделей распределенных программ. Для повышения его эффективности используется ряд приемов:

- проверка модели «на лету»;
- редукции частичных порядков;
- символьное представление данных и др.

АЛГОРИТМ ВЕРИФИКАЦИИ МОДЕЛЕЙ ПРОГРАММ

Более подробно о системе верификации **SPIN** вам расскажет

Константин Олегович Савенков

в курсе

«Верификация программ на моделях»

в весеннем семестре.

КОНЕЦ ЛЕКЦИИ 23

И КОНЕЦ ВСЕМУ КУРСУ ЛЕКЦИЙ!

ЭКЗАМЕН (ВЕРОЯТНО) СОСТОИТСЯ 15 ЯНВАРЯ В 10.00

КОНСУЛЬТАЦИЯ (ВЕРОЯТНО) СОСТОИТСЯ 14 ЯНВАРЯ В 15.00