Математическая логика

(mk.cs.msu.ru → Лекционные курсы → Математическая логика (группы 318, 241))

Лекция 17

Табличный алгоритм model checking для LTL
Замыкание Фишера-Ладнера
Системы Хинтикки

Лектор:
Подымов Владислав Васильевич

E-mail:
valdus@yandex.ru

ВМК МГУ, 2019, весенний семестр

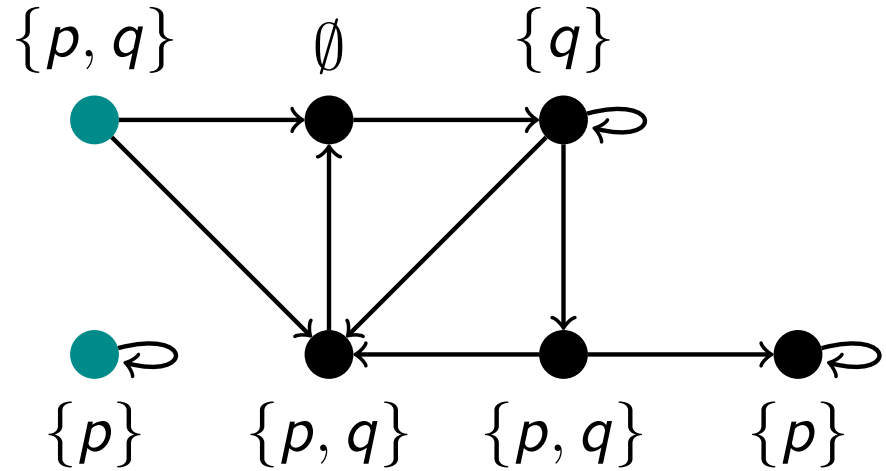
Вступление

AP — конечное множество *элементарных событий*

Ltl-формула:

$$\mathbf{F}p \to q\mathbf{U}\mathbf{X}p$$

Система переходов:



Задача верификации моделей (*model checking*) для LTL формулируется так:

для заданных ltl-формулы φ и системы переходов M проверить справедливость соотношения $M \models \varphi$

Вступление

Задача верификации моделей для LTL не так проста, как кажется:

- система переходов конечна, но содержит **бесконечно много** вычислений в худшем случае
- каждым вычислением порождается **бесконечная** интерпретация

Тем не менее, существуют способы решения этой задачи *за разумное время*

Рассмотрим подробно табличный алгоритм решения задачи

Для технической далее полагаем, что **true** — формула, выполняющаяся во всех интерпретациях во все моменты времени

Упрощение ltl-формул

Ltl-формулу будем называть упрощённой, если она

- содержит только операции **true**, $\neg$, $\&$, **X**, **U** и
- не содержит **двойных отрицаний**: подформул вида $\neg\neg\varphi$

Утверждение. Для любой ltl-формулы существует равносильная упрощённая ltl-формула

Доказательство. Достаточно заметить, что из произвольной ltl-формулы можно поочерёдно исключить

- **G**: $\mathbf{G}\psi \approx \neg\mathbf{F}\neg\psi$
- **F**: $\mathbf{F}\psi \approx \mathbf{true}\mathbf{U}\psi$
- $\rightarrow$: $\psi \rightarrow \chi \approx \neg\psi \vee \chi$
- $\vee$: $\psi \vee \chi \approx \neg(\neg\psi \,\&\, \neg\chi)$
- двойные отрицания: $\neg\neg\psi \approx \psi$

Упрощение ltl-формул

Предварительный этап работы табличного алгоритма состоит в упрощении ltl-формулы

Пример упрощения:

$$\mathbf{G}\neg(p \to \mathbf{X}q)$$
$$\approx$$
$$\neg\mathbf{F}\neg\neg(p \to \mathbf{X}q)$$
$$\approx$$
$$\neg(\mathbf{true}\mathbf{U}\neg\neg(p \to \mathbf{X}q))$$
$$\approx$$
$$\neg(\mathbf{true}\mathbf{U}\neg\neg(\neg p \vee \mathbf{X}q))$$
$$\approx$$
$$\neg(\mathbf{true}\mathbf{U}\neg\neg\neg(\neg\neg p \,\&\, \neg\mathbf{X}q))$$
$$\approx$$
$$\neg(\mathbf{true}\mathbf{U}\neg(p \,\&\, \neg\mathbf{X}q))$$

Далее *без ограничения общности* все рассматриваемые формулы полагаются упрощёнными

Упрощение ltl-формул

Основной этап работы табличного алгоритма начинается со следующих рассуждений:

- $M \not\models \varphi \Leftrightarrow$ в M существует вычисление τ, такое что $\mathcal{I}_M(\tau) \not\models \varphi$
- попробуем доказать или опровергнуть наличие такого вычисления

Модель M далее считается заданной по умолчанию

Запись вида $\ldots \models H$, где H — множество формул, означает следующее: для любой формулы ψ множества H верно $\ldots \models \varphi$

Запись вида $\tau, \ldots \models \ldots$, где τ — трасса, используется как синоним записи $\mathcal{I}_M(\tau), \ldots \models \ldots$

τ^k — суффикс трассы τ, начинающийся с k-го элемента трассы

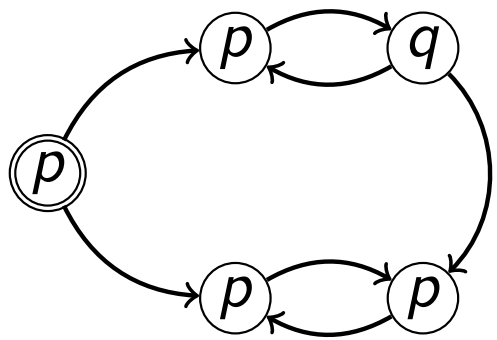
Записью $\overline{\psi}$, где ψ — формула, будем обозначать:

- формулу χ, если $\psi = \neg\chi$
- формулу $\neg\psi$, если ψ не представима в виде, описанном выше

Краткое описание табличного алгоритма

Иллюстрация

φ: $p\mathbf{U}q$ M:



Краткое описание табличного алгоритма

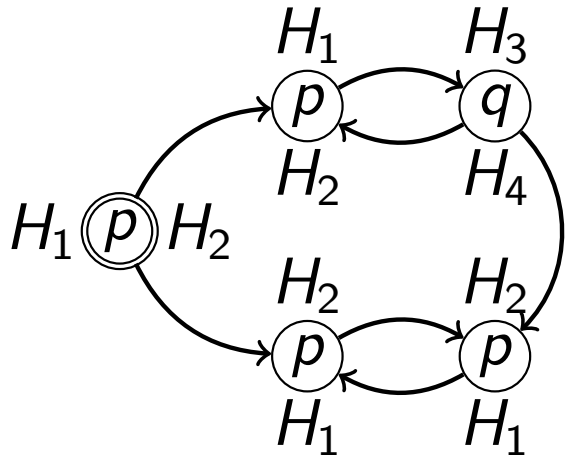
Состояния с.п. M размечаются **гипотезами** — особыми конечными множествами формул, содержащими одну из формул φ, $\overline{\varphi}$

Каждое состояние может быть помечено любым числом гипотез

Содержательная трактовка гипотезы H, помечающей состояние s:
возможно, что в M из состояния s исходит трасса τ,
такая что $\tau \models H$

Иллюстрация

φ: $p\mathbf{U}q$



$$H_1 = \{p, \neg q, \quad \mathbf{X}(p\mathbf{U}q), \quad p\mathbf{U}q\ \} \quad H_3 = \{\neg p, q, \quad \mathbf{X}(p\mathbf{U}q), p\mathbf{U}q\}$$
$$H_2 = \{p, \neg q, \neg\mathbf{X}(p\mathbf{U}q), \neg(p\mathbf{U}q)\} \quad H_4 = \{\neg p, q, \neg\mathbf{X}(p\mathbf{U}q), p\mathbf{U}q\}$$

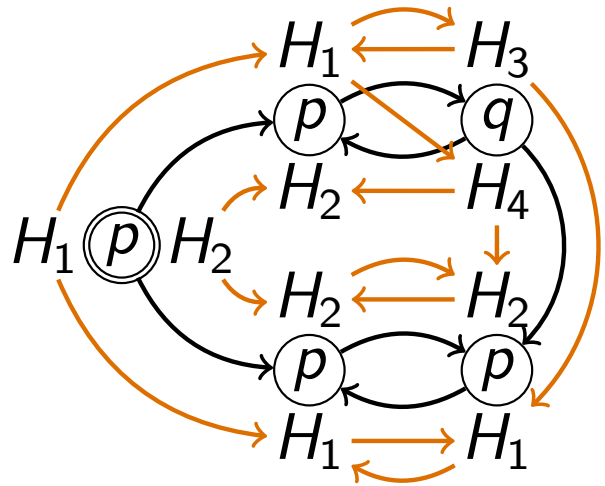
Краткое описание табличного алгоритма

Некоторые пары (состояние, гипотеза) соединяются дугами

Содержательная трактовка дуги $(s_1, H_1) \to (s_2, H_2)$:
возможно, что в M содержится трасса τ: $s_1 \to s_2 \to \ldots$, такая что $\tau \models H_1$ и $\tau^2 \models H_2$

Иллюстрация

φ: $p\mathbf{U}q$



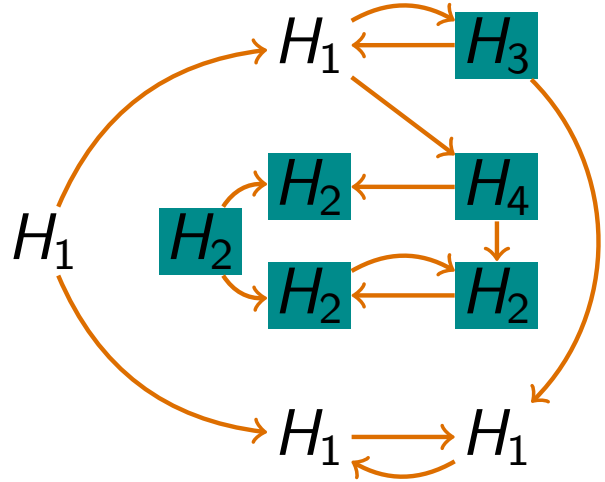
$$H_1 = \{p, \neg q, \quad \mathbf{X}(p\mathbf{U}q), \quad p\mathbf{U}q\ \} \quad H_3 = \{\neg p, q, \quad \mathbf{X}(p\mathbf{U}q), p\mathbf{U}q\}$$
$$H_2 = \{p, \neg q, \neg\mathbf{X}(p\mathbf{U}q), \neg(p\mathbf{U}q)\} \quad H_4 = \{\neg p, q, \neg\mathbf{X}(p\mathbf{U}q), p\mathbf{U}q\}$$

Краткое описание табличного алгоритма

В получившемся графе соединения пар (состояние, гипотеза) — **системе Хинтикки** — рассматриваются бесконечные маршруты, соответствующие трассам M, на которых **действительно** выполняются все формулы соответствующих гипотез

Иллюстрация

φ: $p\mathbf{U}q$



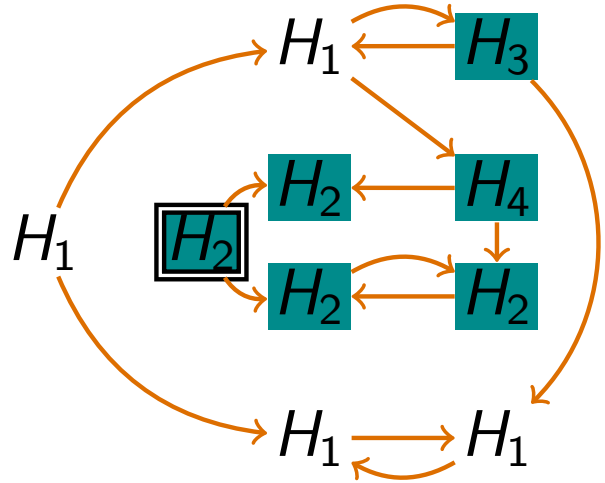
$$H_1 = \{p, \neg q, \quad \mathbf{X}(p\mathbf{U}q), \quad p\mathbf{U}q\ \} \quad H_3 = \{\neg p, q, \quad \mathbf{X}(p\mathbf{U}q), p\mathbf{U}q\}$$
$$H_2 = \{p, \neg q, \neg\mathbf{X}(p\mathbf{U}q), \neg(p\mathbf{U}q)\} \quad H_4 = \{\neg p, q, \neg\mathbf{X}(p\mathbf{U}q), p\mathbf{U}q\}$$

Краткое описание табличного алгоритма

$M \not\models \varphi$ тогда и только тогда, когда существует рассматриваемый маршрут в системе Хинтикки, начинающийся с пары (s, H), где s — начальное состояние M и $\varphi \notin H$

Иллюстрация

φ: $p\mathbf{U}q$



$H_1 = \{p, \neg q, \quad \mathbf{X}(p\mathbf{U}q), \quad p\mathbf{U}q \}$ $\quad H_3 = \{\neg p, q, \quad \mathbf{X}(p\mathbf{U}q), p\mathbf{U}q\}$

$H_2 = \{p, \neg q, \neg\mathbf{X}(p\mathbf{U}q), \neg(p\mathbf{U}q)\}$ $\quad H_4 = \{\neg p, q, \neg\mathbf{X}(p\mathbf{U}q), p\mathbf{U}q\}$

Замыкание Фишера-Ладнера

Формулы вида $\neg\psi$ далее называются негативными,
а все остальные — позитивными

Замыкание Фишера-Ладнера $[\varphi]_{fl}$ формулы φ — это
множество формул, состоящее из

1. всех позитивных подформул формулы φ и
2. формул $\mathbf{X}(\psi\mathbf{U}\chi)$ для всех подформул вида $\psi\mathbf{U}\chi$ формулы φ

Пример: $[\neg(p\mathbf{U}\neg q)]_{fl} = \{p, q, p\mathbf{U}\neg q, \mathbf{X}(p\mathbf{U}\neg q)\}$

Гипотеза (для формулы φ) — это множество формул вида

$$F \cup \{\neg\psi \mid \psi \in [\varphi]_{fl} \setminus F\},$$

где $F \subseteq [\varphi]_{fl}$

Пример: $\{\neg p, \neg q, p\mathbf{U}\neg q, \neg\mathbf{X}(p\mathbf{U}\neg q)\}$ — гипотеза для $\neg(p\mathbf{U}\neg q)$

Гипотезы табличного алгоритма

Гипотеза H совместна, если
для любых формул $\psi_1 \,\&\, \psi_2$ и $\chi_1 \mathbf{U} \chi_2$ из $[\varphi]_{fl}$ верно следующее:

1. $\psi_1 \,\&\, \psi_2 \in H \quad \Leftrightarrow \quad \{\psi_1, \psi_2\} \subseteq H$
2. $\chi_1 \mathbf{U} \chi_2 \in H \quad \Leftrightarrow \quad \chi_2 \in H$ или $\{\chi_1, \mathbf{X}(\chi_1 \mathbf{U} \chi_2)\} \subseteq H$

Пояснение: $\chi_1 \mathbf{U} \chi_2 = \chi_2 \vee \chi_1 \,\&\, \mathbf{X}(\chi_1 \mathbf{U} \chi_2)$
(*закон неподвижной точки для* $\mathbf{U}$, *отражённый в пункте 2*)

Пример:

- $\{\neg p, q, \neg \mathbf{X}(p \mathbf{U} q), \quad p \mathbf{U} q\ \}$ — совместная гипотеза
- $\{\neg p, q, \quad \mathbf{X}(p \mathbf{U} q), \neg(p \mathbf{U} q)\}$ — несовместная гипотеза

$[\varphi]^{-}_{fl} = \{\neg\psi \mid \psi \in [\varphi]_{fl}\}$

$H^k_{\mathcal{I}}$ — множество всех формул ψ из $[\varphi]_{fl} \cup [\varphi]^{-}_{fl}$, таких что $\mathcal{I}, k \models \psi$
($\mathcal{I}$ — *интерпретация*, k — *индекс*)

Гипотезы табличного алгоритма

Лемма(о совместности)

Для любой интерпретации $\mathcal{I}$ и любого индекса t множество $H^t_{\mathcal{I}}$ является совместной гипотезой

Доказательство.

Для каждой формулы ψ из $[\varphi]_{fl}$ **ровно одна** из формул ψ, $\neg\psi$ выполняется в $\mathcal{I}^t$

Значит, по *определению* $H^t_{\mathcal{I}}$, ровно одна из формул ψ, $\neg\psi$ содержится в $H^t_{\mathcal{I}}$

При этом в $H^t_{\mathcal{I}}$ содержатся только формулы множества $[\varphi]_{fl} \cup [\varphi]^-_{fl}$

Значит, $H^t_{\mathcal{I}}$ — гипотеза

$$\begin{array}{lcl} \psi \,\&\, \chi \in H^t_{\mathcal{I}} & \Leftrightarrow & (\textit{определение } H^t_{\mathcal{I}}) \\ \mathcal{I}, t \models \psi \,\&\, \psi & \Leftrightarrow & (\textit{семантика } \&) \\ \mathcal{I}, t \models \psi \text{ и } \mathcal{I}, t \models \chi & \Leftrightarrow & (\textit{определение } H^t_{\mathcal{I}}) \\ \{\psi, \chi\} \subseteq H^t_{\mathcal{I}} & & \end{array}$$

Значит, выполнен

первый пункт определения совместности гипотезы

Гипотезы табличного алгоритма

Лемма(*о совместности*)

Для любой интерпретации $\mathcal{I}$ и любого индекса t множество $H^t_{\mathcal{I}}$ является совместной гипотезой

Доказательство.

$\psi \mathbf{U} \chi \in H^t_{\mathcal{I}}$ $\Leftrightarrow$ (*определение* $H^t_{\mathcal{I}}$)

$\mathcal{I}, t \models \psi \mathbf{U} \chi$ $\Leftrightarrow$ (*закон неподвижной точки*)

$\mathcal{I}, t \models \chi \vee \psi \,\&\, \mathbf{X}(\psi \mathbf{U} \chi)$ $\Leftrightarrow$ (*семантика* $\vee$ *и* $\&$)

$\mathcal{I}, t \models \chi$

или ($\mathcal{I}, t \models \psi$ и $\mathcal{I}, t \models \mathbf{X}(\psi \mathbf{U} \chi)$) $\Leftrightarrow$ (*определение* $H^t_{\mathcal{I}}$)

$\chi \in H^t_{\mathcal{I}}$ или $\{\psi, \mathbf{X}(\psi \mathbf{U} \chi)\} \in H^t_{\mathcal{I}}$

Значит, выполнен

второй пункт определения совместности гипотезы ▼

Гипотезы табличного алгоритма

Гипотезы H_1, H_2 локально согласованны, если для любой формулы вида $\mathbf{X}\chi$ из $[\varphi]_{fl}$ верно: $\mathbf{X}\chi \in H_1 \Leftrightarrow \chi \in H_2$

Пример:

- Гипотезы $\{\neg p, q, \mathbf{X}(p\mathbf{U}q), p\mathbf{U}q\}$ и $\{p, \neg q, \mathbf{X}(p\mathbf{U}q), p\mathbf{U}q\}$ локально согласованны
- Гипотезы $\{\neg p, q, \mathbf{X}(p\mathbf{U}q), p\mathbf{U}q\}$ и $\{p, \neg q, \neg\mathbf{X}(p\mathbf{U}q), \neg(p\mathbf{U}q)\}$ не являются локально согласованными

Лемма(о локальной согласованности). **Для любой интерпретации $\mathcal{I}$ и любого индекса t гипотезы $H^t_{\mathcal{I}}$ и $H^{t+1}_{\mathcal{I}}$ локально согласованны**

Доказательство.

$$
\begin{array}{lcl}
\mathbf{X}\psi \in H^t_{\mathcal{I}} & \Leftrightarrow & (\textit{определение } H^t_{\mathcal{I}}) \\
\mathcal{I}, t \models \mathbf{X}\psi & \Leftrightarrow & (\textit{семантика } \mathbf{X}) \\
\mathcal{I}, t+1 \models \psi & \Leftrightarrow & (\textit{определение } H^{t+1}_{\mathcal{I}}) \\
\psi \in H^{t+1}_{\mathcal{I}} & & \blacktriangledown
\end{array}
$$

Гипотезы табличного алгоритма

Гипотеза H завершает формулу $\psi \mathbf{U} \chi$ из $[\varphi]_{fl}$, если выполнено хотя бы одно из двух условий:

1. $\chi \in H$
2. $\mathbf{X}(\psi \mathbf{U} \chi) \notin H$

Бесконечная последовательность гипотез $\mathfrak{H}$ глобально согласованна, если для каждой формулы вида $\psi \mathbf{U} \chi$ из $[\varphi]_{fl}$ в $\mathfrak{H}$ бесконечно часто встречаются гипотезы, завершающие эту формулу

Пример

Пусть $H_1 = \{p, \neg q, \mathbf{X}(p \mathbf{U} q), p \mathbf{U} q\}$ и $H_2 = \{\neg p, q, \mathbf{X}(p \mathbf{U} q), p \mathbf{U} q\}$:

- Гипотеза H_2 завершает формулу $p \mathbf{U} q$, а гипотеза H_1 не завершает
- Последовательность $H_1, H_2, H_1, H_2, \ldots$ глобально согласованна
- Последовательность $H_1, H_1, H_1, H_1, \ldots$ не является глобально согласованной

Гипотезы табличного алгоритма

Лемма(*о глобальной согласованности*). Для любой интерпретации $\mathcal{I}$ последовательность гипотез $H^1_\mathcal{I}, H^2_\mathcal{I}, H^3_\mathcal{I}, \ldots$ глобально согласованна

Доказательство.

Рассмотрим произвольный индекс t

$$
\begin{array}{lcl}
\psi \mathbf{U} \chi \notin H^{t+1}_\mathcal{I} & \Rightarrow & (\textit{определение } H^{t+1}_\mathcal{I}) \\
\mathcal{I}, t+1 \not\models \psi \mathbf{U} \chi & \Rightarrow & (\textit{семантика } \mathbf{X}) \\
\mathcal{I}, t \not\models \mathbf{X}(\psi \mathbf{U} \chi) & \Rightarrow & (\textit{определение } H^t_\mathcal{I}) \\
\mathbf{X}(\psi \mathbf{U} \chi) \in H^t_\mathcal{I} & \Rightarrow & (\textit{определение завершающей гипотезы})
\end{array}
$$

гипотеза $H^t_\mathcal{I}$ завершает формулу $\psi \mathbf{U} \chi$

Гипотезы табличного алгоритма

Лемма(*о глобальной согласованности*). Для любой интерпретации $\mathcal{I}$ последовательность гипотез $H^1_\mathcal{I}, H^2_\mathcal{I}, H^3_\mathcal{I}, \ldots$ глобально согласованна

Доказательство.

Рассмотрим произвольный индекс t

$\psi \mathbf{U} \chi \in H^{t+1}_\mathcal{I}$ $\Rightarrow$ (*определение* $H^{t+1}_\mathcal{I}$)

$\mathcal{I}, t+1 \not\models \psi \mathbf{U} \chi$ $\Rightarrow$ (*семантика* $\mathbf{U}$)

существует индекс i, такой что $i \geq t+1$ и $\mathcal{I}, i \models \chi$

$\Rightarrow$ (*определение* $H^i_\mathcal{I}$)

$\chi \in H^i_\mathcal{I}$ $\Rightarrow$ (*определение завершающей гипотезы*)

гипотеза $H^i_\mathcal{I}$ завершает формулу $\psi \mathbf{U} \chi$

Значит, для любого индекса j ($j = t-1$) существует индекс i, такой что $i \geq j$ и гипотеза $H^i_\mathcal{I}$ завершает формулу $\psi \mathbf{U} \chi$

Последнее утверждение справедливо только в том случае, если таких гипотез $H^i_\mathcal{I}$ бесконечно много ▼

Гипотезы табличного алгоритма

Если $\mathfrak{H} = (H_0, H_1, H_2, \dots)$ — бесконечная последовательность гипотез, то $\mathcal{I}_{\mathfrak{H}}$ — интерпретация вида $H_0 \cap AP, H_1 \cap AP, H_2 \cap AP, \dots$

Лемма(*основная*)
Пусть $\mathfrak{H}$ — глобально согласованная последовательность совместных гипотез, такая что каждая пара соседних элементов последовательности локально согласованна. Тогда для любого индекса t верно $\mathfrak{H}[t] = H^t_{\mathcal{I}_{\mathfrak{H}}}$

Доказательство.

По *определению* $H^t_{\mathcal{I}}$, достаточно показать, что для любой формулы ψ из $[\varphi]_{fl}$ и любого индекса t верно

$$\psi \in \mathfrak{H}[t] \Leftrightarrow \mathcal{I}_{\mathfrak{H}}, t \models \psi$$

Покажем это индукцией по построению формулы

Доказательство основной леммы

$$\psi \in \mathfrak{H}[t] \Leftrightarrow \mathcal{I}_{\mathfrak{H}}, t \models \psi \ ?$$

База:

$$\begin{array}{lcl} p \in \mathfrak{H}[t] & \Leftrightarrow & (\textit{определение } \mathcal{I}_{\mathfrak{H}}) \\ p \in \mathcal{I}_{\mathfrak{H}}[t] & \Leftrightarrow & (\textit{семантика событий}) \\ \mathcal{I}_{\mathfrak{H}}, t \models p & & \end{array}$$

Шаг 1:

$$\begin{array}{lcl} \neg\chi \in \mathfrak{H}[t] & \Leftrightarrow & (\textit{определение гипотезы}) \\ \chi \notin \mathfrak{H}[t] & \Leftrightarrow & (\textit{индуктивное предположение}) \\ \mathcal{I}_{\mathfrak{H}}, t \not\models \chi & \Leftrightarrow & (\textit{семантика } \neg) \\ \mathcal{I}_{\mathfrak{H}}, t \models \neg\chi & & \end{array}$$

Доказательство основной леммы

$$\psi \in \mathfrak{H}[t] \Leftrightarrow \mathcal{I}_{\mathfrak{H}}, t \models \psi \ ?$$

Шаг 2:

$\chi_1 \,\&\, \chi_2 \in \mathfrak{H}[t]$ $\Leftrightarrow$ (*совместность гипотезы*)

$\{\chi_1, \chi_2\} \subseteq \mathfrak{H}[t]$ $\Leftrightarrow$ (*индуктивное предположение*)

$\mathcal{I}_{\mathfrak{H}}, t \models \chi_1$ и $\mathcal{I}_{\mathfrak{H}}, t \models \chi_2$ $\Leftrightarrow$ (*семантика* &)

$\mathcal{I}_{\mathfrak{H}}, t \models \chi_1 \,\&\, \chi_2$

Шаг 3:

$\mathbf{X}\chi \in \mathfrak{H}[t]$ $\Leftrightarrow$ (*локальная согласованность*)

$\chi \in \mathfrak{H}[t+1]$ $\Leftrightarrow$ (*индуктивное предположение*)

$\mathcal{I}_{\mathfrak{H}}, t+1 \models \chi$ $\Leftrightarrow$ (*семантика* $\mathbf{X}$)

$\mathcal{I}_{\mathfrak{H}}, t \models \mathbf{X}\chi$

Доказательство основной леммы

$$\psi \in \mathfrak{H}[t] \Leftrightarrow \mathcal{I}_{\mathfrak{H}}, t \models \psi \ ?$$

Шаг 4: $\chi_1 \mathbf{U} \chi_2 \in \mathfrak{H}[t] \stackrel{?}{\Rightarrow} \mathcal{I}_{\mathfrak{H}} \models \chi_1 \mathbf{U} \chi_2$

Пусть $\chi_1 \mathbf{U} \chi_2 \in \mathfrak{H}[t]$

Случай 1: существует индекс k, такой что $k \geq t$ и $\chi_2 \in \mathfrak{H}[k]$

Рассмотрим наименьший такой индекс: $\chi_2 \notin \mathfrak{H}[t] \cup \cdots \cup \mathfrak{H}[k-1]$

$$\mathcal{I}[t] \longrightarrow \mathcal{I}[t+1] \longrightarrow \cdots \longrightarrow \mathcal{I}[k-1] \longrightarrow \mathcal{I}[k] \longrightarrow \cdots$$

$$\mathbf{U}\ \overline{\chi_2} \qquad \overline{\chi_2} \qquad \overline{\chi_2} \qquad \chi_2$$

Доказательство основной леммы

$$\psi \in \mathfrak{H}[t] \Leftrightarrow \mathcal{I}_{\mathfrak{H}}, t \models \psi \ ?$$

Шаг 4: $\chi_1 \mathbf{U} \chi_2 \in \mathfrak{H}[t] \stackrel{?}{\Rightarrow} \mathcal{I}_{\mathfrak{H}} \models \chi_1 \mathbf{U} \chi_2$

Пусть $\chi_1 \mathbf{U} \chi_2 \in \mathfrak{H}[t]$

Случай 1: существует индекс k, такой что $k \geq t$ и $\chi_2 \in \mathfrak{H}[k]$

Рассмотрим наименьший такой индекс: $\chi_2 \notin \mathfrak{H}[t] \cup \cdots \cup \mathfrak{H}[k-1]$

$$\mathcal{I}[t] \longrightarrow \mathcal{I}[t+1] \longrightarrow \cdots \longrightarrow \mathcal{I}[k-1] \longrightarrow \mathcal{I}[k] \longrightarrow \cdots$$

$\mathbf{U}\,\overline{\chi_2}$ $\quad$ $\overline{\chi_2}$ $\quad$ $\overline{\chi_2}$ $\quad$ χ_2

$\mathbf{X}\,\chi_1$

По *совместности гипотез*, $\{\chi_1, \mathbf{X}(\chi_1 \mathbf{U} \chi_2)\} \subseteq \mathfrak{H}[t]$

Доказательство основной леммы

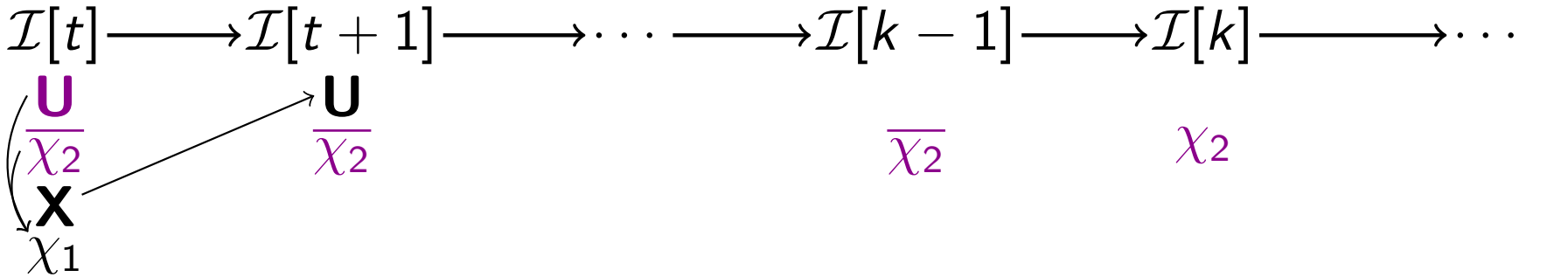
$$\psi \in \mathfrak{H}[t] \Leftrightarrow \mathcal{I}_{\mathfrak{H}}, t \models \psi \ ?$$

Шаг 4: $\chi_1 \mathbf{U} \chi_2 \in \mathfrak{H}[t] \stackrel{?}{\Rightarrow} \mathcal{I}_{\mathfrak{H}} \models \chi_1 \mathbf{U} \chi_2$

Пусть $\chi_1 \mathbf{U} \chi_2 \in \mathfrak{H}[t]$

Случай 1: существует индекс k, такой что $k \geq t$ и $\chi_2 \in \mathfrak{H}[k]$

Рассмотрим наименьший такой индекс: $\chi_2 \notin \mathfrak{H}[t] \cup \cdots \cup \mathfrak{H}[k-1]$



По *совместности гипотез*, $\{\chi_1, \mathbf{X}(\chi_1 \mathbf{U} \chi_2)\} \subseteq \mathfrak{H}[t]$

По *локальной согласованности*, $\chi_1 \mathbf{U} \chi_2 \in \mathfrak{H}[t+1]$

Доказательство основной леммы

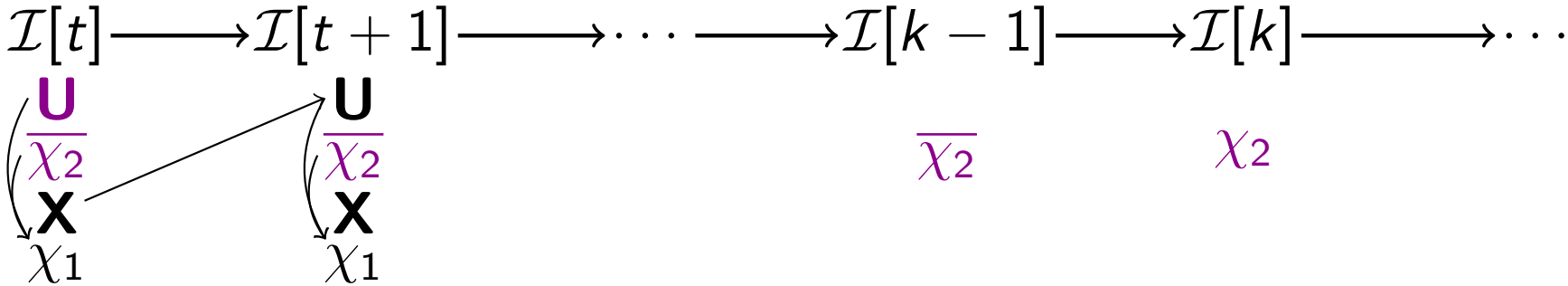
$$\psi \in \mathfrak{H}[t] \Leftrightarrow \mathcal{I}_{\mathfrak{H}}, t \models \psi \ ?$$

Шаг 4: $\chi_1 \mathbf{U} \chi_2 \in \mathfrak{H}[t] \stackrel{?}{\Rightarrow} \mathcal{I}_{\mathfrak{H}} \models \chi_1 \mathbf{U} \chi_2$

Пусть $\chi_1 \mathbf{U} \chi_2 \in \mathfrak{H}[t]$

Случай 1: существует индекс k, такой что $k \geq t$ и $\chi_2 \in \mathfrak{H}[k]$

Рассмотрим наименьший такой индекс: $\chi_2 \notin \mathfrak{H}[t] \cup \cdots \cup \mathfrak{H}[k-1]$



По *совместности гипотез*, $\{\chi_1, \mathbf{X}(\chi_1 \mathbf{U} \chi_2)\} \subseteq \mathfrak{H}[t]$

По *локальной согласованности*, $\chi_1 \mathbf{U} \chi_2 \in \mathfrak{H}[t+1]$

По *совместности гипотез*, $\{\chi_1, \mathbf{X}(\chi_1 \mathbf{U} \chi_2)\} \subseteq \mathfrak{H}[t+1]$

Доказательство основной леммы

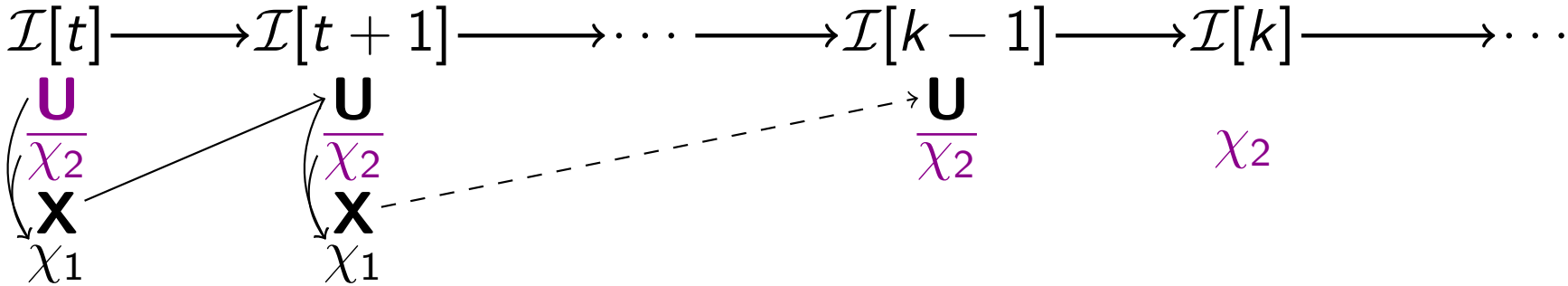
$$\psi \in \mathfrak{H}[t] \Leftrightarrow \mathcal{I}_{\mathfrak{H}}, t \models \psi \ ?$$

Шаг 4: $\chi_1 \mathbf{U} \chi_2 \in \mathfrak{H}[t] \stackrel{?}{\Rightarrow} \mathcal{I}_{\mathfrak{H}} \models \chi_1 \mathbf{U} \chi_2$

Пусть $\chi_1 \mathbf{U} \chi_2 \in \mathfrak{H}[t]$

Случай 1: существует индекс k, такой что $k \geq t$ и $\chi_2 \in \mathfrak{H}[k]$

Рассмотрим наименьший такой индекс: $\chi_2 \notin \mathfrak{H}[t] \cup \cdots \cup \mathfrak{H}[k-1]$



По *совместности гипотез*, $\{\chi_1, \mathbf{X}(\chi_1 \mathbf{U} \chi_2)\} \subseteq \mathfrak{H}[t]$

По *локальной согласованности*, $\chi_1 \mathbf{U} \chi_2 \in \mathfrak{H}[t+1]$

По *совместности гипотез*, $\{\chi_1, \mathbf{X}(\chi_1 \mathbf{U} \chi_2)\} \subseteq \mathfrak{H}[t+1]$

...

По *локальной согласованности*, $\chi_1 \mathbf{U} \chi_2 \in \mathfrak{H}[k-1]$

Доказательство основной леммы

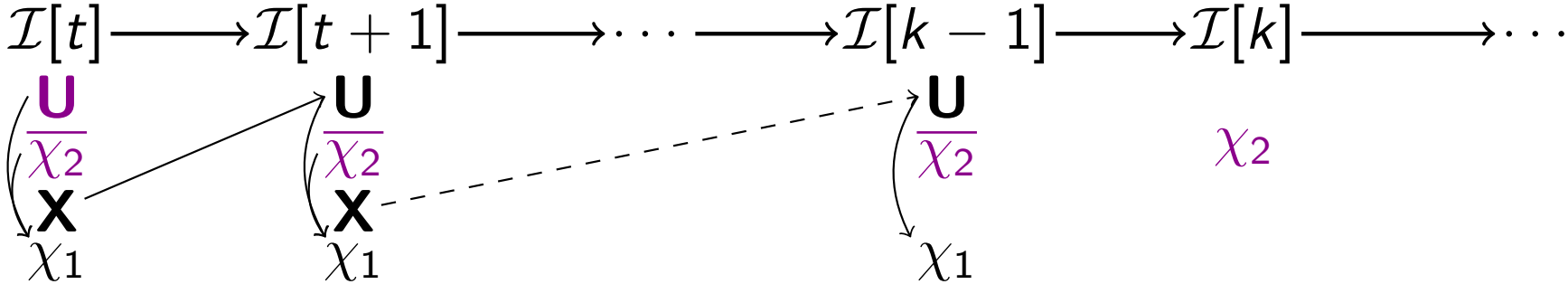
$$\psi \in \mathfrak{H}[t] \Leftrightarrow \mathcal{I}_{\mathfrak{H}}, t \models \psi \ ?$$

Шаг 4: $\chi_1 \mathbf{U} \chi_2 \in \mathfrak{H}[t] \stackrel{?}{\Rightarrow} \mathcal{I}_{\mathfrak{H}} \models \chi_1 \mathbf{U} \chi_2$

Пусть $\chi_1 \mathbf{U} \chi_2 \in \mathfrak{H}[t]$

Случай 1: существует индекс k, такой что $k \geq t$ и $\chi_2 \in \mathfrak{H}[k]$

Рассмотрим наименьший такой индекс: $\chi_2 \notin \mathfrak{H}[t] \cup \cdots \cup \mathfrak{H}[k-1]$



По *совместности гипотез*, $\{\chi_1, \mathbf{X}(\chi_1 \mathbf{U} \chi_2)\} \subseteq \mathfrak{H}[t]$

По *локальной согласованности*, $\chi_1 \mathbf{U} \chi_2 \in \mathfrak{H}[t+1]$

По *совместности гипотез*, $\{\chi_1, \mathbf{X}(\chi_1 \mathbf{U} \chi_2)\} \subseteq \mathfrak{H}[t+1]$

...

По *локальной согласованности*, $\chi_1 \mathbf{U} \chi_2 \in \mathfrak{H}[k-1]$

По *совместности гипотез*, $\{\chi_1, \mathbf{X}(\chi_1 \mathbf{U} \chi_2)\} \subseteq \mathfrak{H}[k-1]$

Доказательство основной леммы

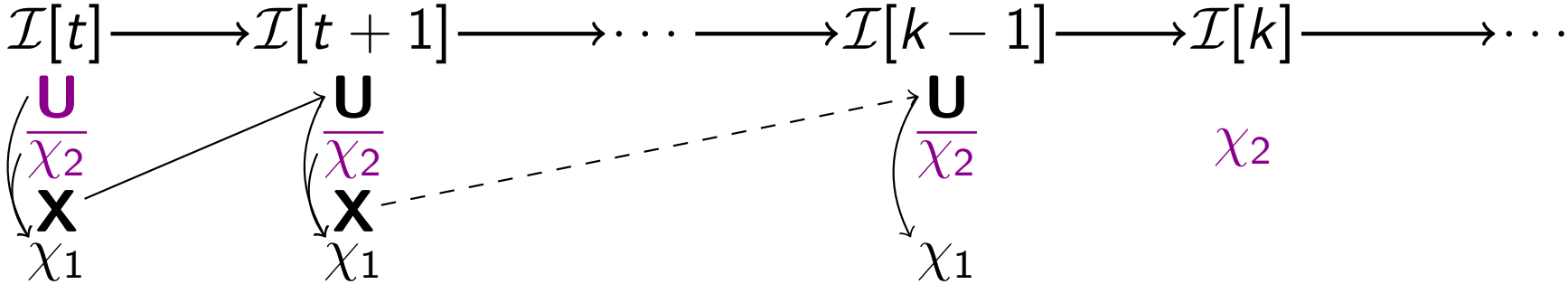
$$\psi \in \mathfrak{H}[t] \Leftrightarrow \mathcal{I}_{\mathfrak{H}}, t \models \psi \ ?$$

Шаг 4: $\chi_1 \mathbf{U} \chi_2 \in \mathfrak{H}[t] \stackrel{?}{\Rightarrow} \mathcal{I}_{\mathfrak{H}} \models \chi_1 \mathbf{U} \chi_2$

Пусть $\chi_1 \mathbf{U} \chi_2 \in \mathfrak{H}[t]$

Случай 1: существует индекс k, такой что $k \geq t$ и $\chi_2 \in \mathfrak{H}[k]$

Рассмотрим наименьший такой индекс: $\chi_2 \notin \mathfrak{H}[t] \cup \cdots \cup \mathfrak{H}[k-1]$



По *индуктивному предположению*:

$$\mathcal{I}_{\mathfrak{H}}, t \models \chi_1; \quad \ldots; \quad \mathcal{I}_{\mathfrak{H}}, k-1 \models \chi_1; \quad \mathcal{I}_{\mathfrak{H}}, k \models \chi_2$$

По *семантике* $\mathbf{U}$, $\mathcal{I}_{\mathfrak{H}}, t \models \chi_1 \mathbf{U} \chi_2$

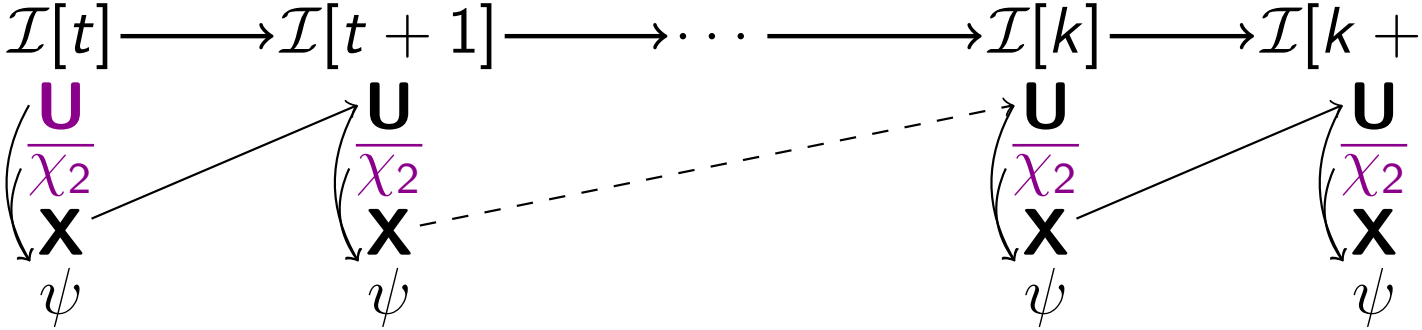
Доказательство основной леммы

$$\psi \in \mathfrak{H}[t] \Leftrightarrow \mathcal{I}_{\mathfrak{H}}, t \models \psi \ ?$$

Шаг 4: $\chi_1 \mathbf{U} \chi_2 \in \mathfrak{H}[t] \stackrel{?}{\Rightarrow} \mathcal{I}_{\mathfrak{H}} \models \chi_1 \mathbf{U} \chi_2$

Пусть $\chi_1 \mathbf{U} \chi_2 \in \mathfrak{H}[t]$

Случай 2: для любого индекса k, такого что $k \geq t$, верно $\chi_2 \notin \mathfrak{H}[k]$



Теми же рассуждениями, что и в *случае 1*, можно легко получить следующий факт:

для любого индекса k, такого что $k \geq t$, верно $\mathbf{X}(\chi_1 \mathbf{U} \chi_2) \in \mathfrak{H}[k]$

Значит, ни одна из гипотез $\mathfrak{H}[t], \mathfrak{H}[t+1], \ldots$ не является завершающей для $\chi_1 \mathbf{U} \chi_2$

Тогда последовательность $\mathfrak{H}$ не является глобально согласованной, то есть случай 2 **невозможен** по условию леммы

Доказательство основной леммы

$$\psi \in \mathfrak{H}[t] \Leftrightarrow \mathcal{I}_{\mathfrak{H}}, t \models \psi \ ?$$

Шаг 5: $\chi_1 \mathbf{U} \chi_2 \in \mathfrak{H}[t] \overset{?}{\Leftarrow} \mathcal{I}_{\mathfrak{H}} \models \chi_1 \mathbf{U} \chi_2$

Пусть $\mathcal{I}_{\mathfrak{H}} \models \chi_1 \mathbf{U} \chi_2$

По *семантике* **U**, существует индекс k, такой что $k \geq t$ и

$$\mathcal{I}_{\mathfrak{H}}, t \models \chi_1; \quad \ldots; \quad \mathcal{I}_{\mathfrak{H}}, k-1 \models \chi_1; \quad \mathcal{I}_{\mathfrak{H}}, k \models \chi_2$$

Рассмотрим наименьший такой индекс k:

$$\mathcal{I}_{\mathfrak{H}}, t \not\models \chi_2; \quad \ldots; \quad \mathcal{I}_{\mathfrak{H}}, k-1 \not\models \chi_2$$

По *индуктивному предположению*:

$$\{\chi_1, \overline{\chi_2}\} \subseteq \mathfrak{H}[t], \quad \ldots, \quad \{\chi_1, \overline{\chi_2}\} \subseteq \mathfrak{H}[k-1], \quad \chi_2 \in \mathfrak{H}[k]$$

Рассуждениями о совместности и локальной согласованности, аналогичными рассуждениям *шага 4*, можно легко получить справедливость соотношения $\chi_1 \mathbf{U} \chi_2 \in \mathfrak{H}[t]$

Гипотезы табличного алгоритма

Лемма(*основная*)
Пусть $\mathfrak{H}$ — глобально согласованная последовательность совместных гипотез, такая что каждая пара соседних элементов последовательности локально согласованна. Тогда для любого индекса t верно $\mathfrak{H}[t] = H^t_{\mathcal{I}_{\mathfrak{H}}}$

Контрпример, показывающий важность глобальной согласованности:

- гипотеза $H = \{p, \neg q, \mathbf{X}(p\mathbf{U}q), p\mathbf{U}q\}$ совместна
- пара гипотез H, H локально согласованна
- бесконечная последовательность гипотез $H, H, H, \ldots$ **не является** глобально согласованной
- $\mathcal{I}_{H,H,H,\ldots} = (\{p\}, \{p\}, \{p\}, \ldots) \not\models p\mathbf{U}q$

Системы Хинтикки

Гипотеза H адекватна состоянию s системы переходов $M = (S, S_0, \to, \rho)$, если $\rho(s) = H \cap \mathrm{AP}$

Система Хинтикки $\mathcal{HS}(M, \varphi)$ для системы переходов M и ltl-формулы φ — это размеченный ориентированный граф следующего вида:

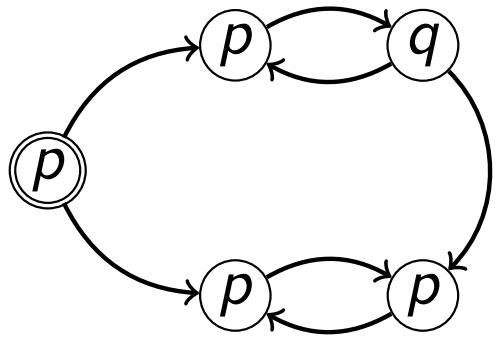
- вершинами являются всевозможные пары (s, H), где $s \in S$ и H — совместная гипотеза, адекватная состоянию s
- дуга $(s_1, H_1) \to (s_2, H_2)$ содержится в графе $\Leftrightarrow$ $s_1 \to s_2$ и гипотезы H_1, H_2 локально согласованны
- вершина (s, H) является начальной $\Leftrightarrow$ $s \in S_0$ и $\varphi \notin H$
- каждой формуле вида $\psi \mathbf{U} \chi$ из $[\varphi]_{fl}$ сопоставлен уникальный цвет $c_{\psi \mathbf{U} \chi}$
- вершина (s, H) помечена цветом c_Φ $\Leftrightarrow$ гипотеза H завершает формулу Φ

Системы Хинтикки

Пример

φ: $p \mathbf{U} q$

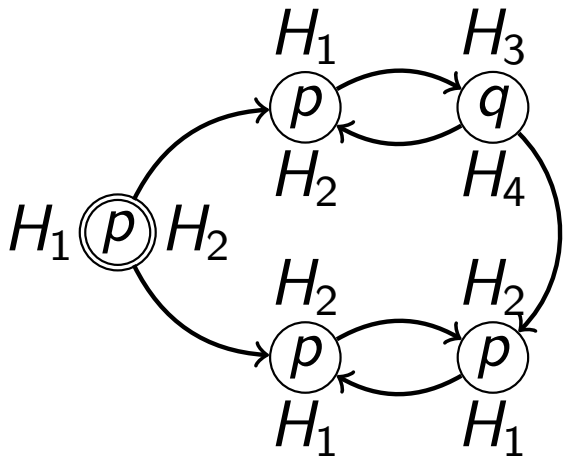
M:



Системы Хинтикки

Пример

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



$$H_1 = \{p, \neg q, \quad \mathbf{X}(p\mathbf{U}q), \quad p\mathbf{U}q\ \} \quad H_3 = \{\neg p, q, \quad \mathbf{X}(p\mathbf{U}q), p\mathbf{U}q\}$$
$$H_2 = \{p, \neg q, \neg\mathbf{X}(p\mathbf{U}q), \neg(p\mathbf{U}q)\} \quad H_4 = \{\neg p, q, \neg\mathbf{X}(p\mathbf{U}q), p\mathbf{U}q\}$$

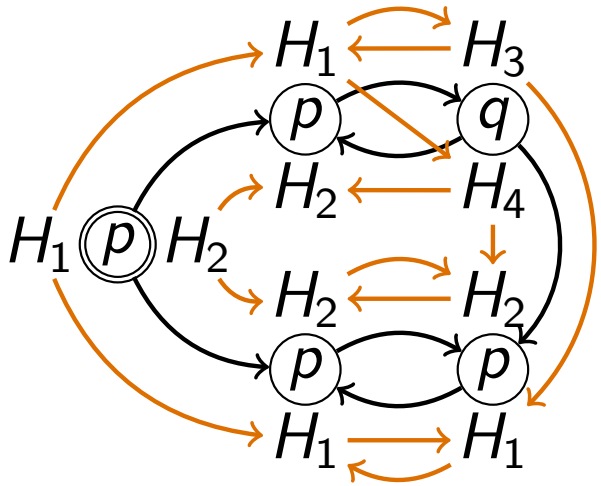
H_1 и H_2 — все совместные гипотезы, адекватные состоянию, помеченному множеством $\{p\}$

H_3 и H_4 — все совместные гипотезы, адекватные состоянию, помеченному множеством $\{q\}$

Системы Хинтикки

Пример

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



$$H_1 = \{p, \neg q, \quad \mathbf{X}(p\mathbf{U}q), \quad p\mathbf{U}q\ \} \quad H_3 = \{\neg p, q, \quad \mathbf{X}(p\mathbf{U}q), p\mathbf{U}q\}$$
$$H_2 = \{p, \neg q, \neg\mathbf{X}(p\mathbf{U}q), \neg(p\mathbf{U}q)\} \quad H_4 = \{\neg p, q, \neg\mathbf{X}(p\mathbf{U}q), p\mathbf{U}q\}$$

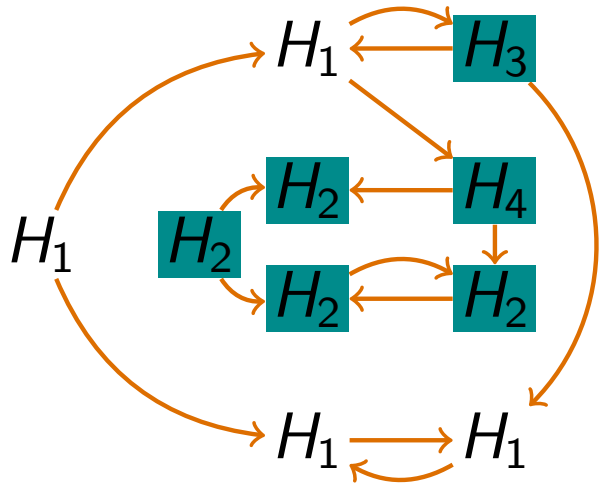
Локально согласованная пара гипотез H_i, H_j:

$$\mathbf{X}(p\mathbf{U}q) \in H_i \Leftrightarrow p\mathbf{U}q \in H_j$$

Системы Хинтикки

Пример

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



$$H_1 = \{p, \neg q, \quad \mathbf{X}(p\mathbf{U}q), \quad p\mathbf{U}q\ \} \quad H_3 = \{\neg p, q, \quad \mathbf{X}(p\mathbf{U}q), p\mathbf{U}q\}$$
$$H_2 = \{p, \neg q, \neg\mathbf{X}(p\mathbf{U}q), \neg(p\mathbf{U}q)\} \quad H_4 = \{\neg p, q, \neg\mathbf{X}(p\mathbf{U}q), p\mathbf{U}q\}$$

Гипотезы H_3, H_4 завершают формулу $p\mathbf{U}q$: $q \in H_3 \cap H_4$

Гипотеза H_2 завершает формулу $p\mathbf{U}q$: $\mathbf{X}(p\mathbf{U}q) \notin H_2$

Гипотеза H_1 **не** завершает формулу $p\mathbf{U}q$:

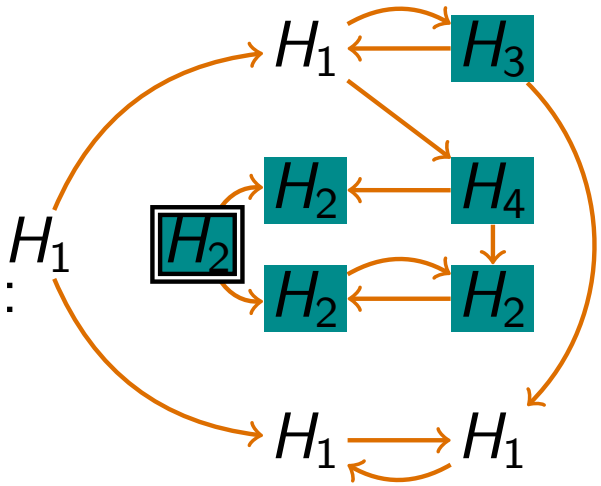
- $q \notin H_1$
- $\mathbf{X}(p\mathbf{U}q) \in H_1$

Системы Хинтикки

Пример

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

$\mathcal{HS}(M, \varphi)$:



$$H_1 = \{p, \neg q, \quad \mathbf{X}(p\mathbf{U}q), \quad p\mathbf{U}q\ \} \quad H_3 = \{\neg p, q, \quad \mathbf{X}(p\mathbf{U}q), p\mathbf{U}q\}$$
$$H_2 = \{p, \neg q, \neg\mathbf{X}(p\mathbf{U}q), \neg(p\mathbf{U}q)\} \quad H_4 = \{\neg p, q, \neg\mathbf{X}(p\mathbf{U}q), p\mathbf{U}q\}$$

Начальная вершина (s, H):

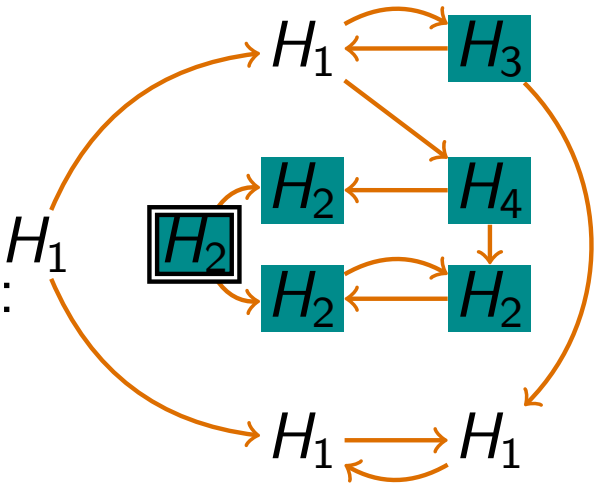
- s — начальное состояние модели M
- $p\mathbf{U}q \notin H$

Системы Хинтикки

Пример

φ: $p\mathbf{U}q$

$\mathcal{HS}(M,\varphi)$:



$$H_1 = \{p, \neg q, \quad \mathbf{X}(p\mathbf{U}q), \quad p\mathbf{U}q\ \} \quad H_3 = \{\neg p, q, \quad \mathbf{X}(p\mathbf{U}q), p\mathbf{U}q\}$$
$$H_2 = \{p, \neg q, \neg\mathbf{X}(p\mathbf{U}q), \neg(p\mathbf{U}q)\} \quad H_4 = \{\neg p, q, \neg\mathbf{X}(p\mathbf{U}q), p\mathbf{U}q\}$$

Радужным маршрутом назовём бесконечный маршрут в системе Хинтикки, исходящий из начальной вершины и для каждого цвета c содержащий бесконечно много вершин, помеченных этим цветом

Теорема(*основная*). $M \not\models \varphi \Leftrightarrow$ **в системе Хинтикки** $\mathcal{HS}(M,\varphi)$ **содержится радужный маршрут**

Системы Хинтикки

Теорема(*основная*). $M \not\models \varphi \Leftrightarrow$ **в системе Хинтикки** $\mathcal{HS}(M, \varphi)$ **содержится радужный маршрут**

Доказательство.

($\Leftarrow$): Пусть в системе $\mathcal{HS}(M, \varphi)$ содержится радужный маршрут

$$(s_1, H_1) \to (s_2, H_2) \to \dots$$

Тогда по *определению системы Хинтикки*:

- $\tau = (s_1 \to s_2 \to \dots)$ — вычисление с.п. M
- $\mathfrak{H} = (H_1, H_2, \dots)$ — последовательность совместных гипотез, такая что любые две соседних гипотезы локально согласованны
- $\mathcal{I}_{\mathfrak{H}} = \rho(s_1), \rho(s_2), \dots$, где ρ — функция разметки с.п. M
- $\varphi \notin H_1$, а значит, *по определению гипотезы*, $\overline{\varphi} \in H_1$

По *определениям системы Хинтикки* и *радужного маршрута*, последовательность $\mathfrak{H}$ глобально согласованна

По *основной лемме*, $\tau \models H_1$, а значит, и $\tau \models \overline{\varphi}$

По *семантике* $\neg$, $\tau \not\models \varphi$, и следовательно, $M \not\models \varphi$

Системы Хинтикки

Теорема(*основная*). $M \not\models \varphi \Leftrightarrow$ **в системе Хинтикки** $\mathcal{HS}(M, \varphi)$ **содержится радужный маршрут**

Доказательство.

($\Rightarrow$): Пусть $M \not\models \varphi$

Тогда существует вычисление τ, такое что $\tau \not\models \varphi$

Рассмотрим последовательность гипотез $\mathfrak{H} = (H^1_\tau, H^2_\tau, \dots)$

По *лемме о совместности*, каждая гипотеза H^i_τ совместна

По *лемме о локальной согласованности*, каждая пара гипотез H^i_τ, H^i_τ локально согласованна

По *определению системы Хинтикки*, в $\mathcal{HS}(M, \varphi)$ содержится маршрут p следующего вида: $(\tau[1], H^1_\tau) \to (\tau[2], H_{\tau^2}) \to \dots$

По *лемме о глобальной согласованности*, последовательность $\mathfrak{H}$ глобально согласованна

По *определениям системы Хинтикки* и *радужного маршрута*, маршрут p — радужный

Системы Хинтикки

Ориентированный граф Γ называется сильно связным, если для любой пары вершин u, v в Γ содержится маршрут из u в v

Компонентой сильной связности графа Γ называется сильно связный подграф, максимальный по включению вершин и дуг

Компонента сильной связности тривиальна, если содержит ровно одну вершину и не содержит ни одной дуги, и нетривиальна в остальных случаях

Радужной компонентой системы Хинтикки назовём нетривиальную компоненту сильной связности, содержащую вершины всех цветов

Теорема(*вспомогательная*). В системе Хинтикки $\mathcal{HS}(M, \varphi)$ содержится радужный маршрут $\Leftrightarrow$ в $\mathcal{HS}(M, \varphi)$ из начальной вершины достижима радужная компонента

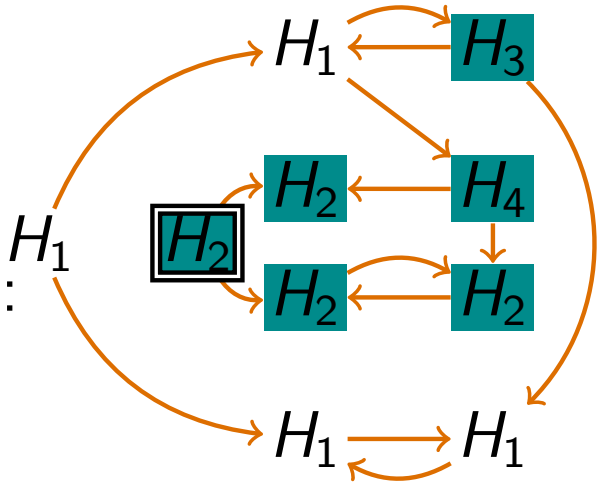
Доказательство. На грани очевидного ▼

Системы Хинтикки

Пример

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

$\mathcal{HS}(M, \varphi)$:



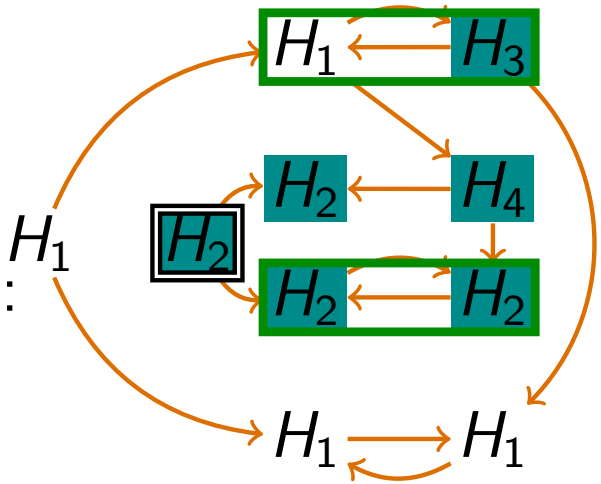
$$H_1 = \{p, \neg q, \quad \mathbf{X}(p\mathbf{U}q), \quad p\mathbf{U}q\ \} \quad H_3 = \{\neg p, q, \quad \mathbf{X}(p\mathbf{U}q), p\mathbf{U}q\}$$
$$H_2 = \{p, \neg q, \neg\mathbf{X}(p\mathbf{U}q), \neg(p\mathbf{U}q)\} \quad H_4 = \{\neg p, q, \neg\mathbf{X}(p\mathbf{U}q), p\mathbf{U}q\}$$

Системы Хинтикки

Пример

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

$\mathcal{HS}(M,\varphi)$:



$$H_1 = \{p, \neg q, \quad \mathbf{X}(p\mathbf{U}q), \quad p\mathbf{U}q\} \quad H_3 = \{\neg p, q, \quad \mathbf{X}(p\mathbf{U}q), p\mathbf{U}q\}$$
$$H_2 = \{p, \neg q, \neg\mathbf{X}(p\mathbf{U}q), \neg(p\mathbf{U}q)\} \quad H_4 = \{\neg p, q, \neg\mathbf{X}(p\mathbf{U}q), p\mathbf{U}q\}$$

В $\mathcal{HS}(M,\varphi)$ содержится только один цвет

Радужные компоненты системы $\mathcal{HS}(M,\varphi)$
обведены прямоугольниками

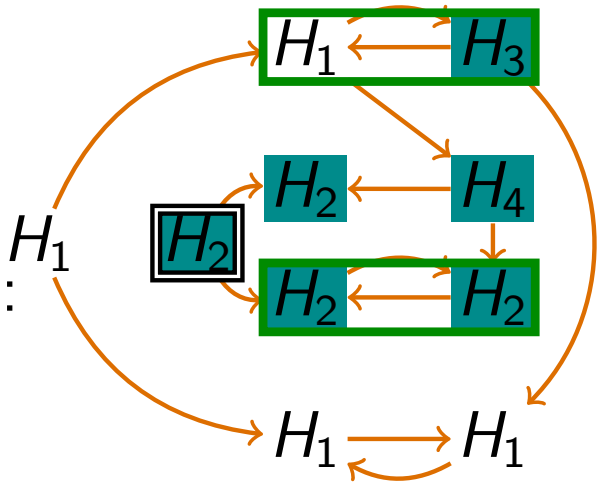
Нижняя компонента достижима из начальной вершины

Системы Хинтикки

Пример

φ: $p\mathbf{U}q$

$\mathcal{HS}(M,\varphi)$:



$$H_1 = \{p, \neg q, \quad \mathbf{X}(p\mathbf{U}q), \quad p\mathbf{U}q\ \} \quad H_3 = \{\neg p, q, \quad \mathbf{X}(p\mathbf{U}q), p\mathbf{U}q\}$$
$$H_2 = \{p, \neg q, \neg\mathbf{X}(p\mathbf{U}q), \neg(p\mathbf{U}q)\} \quad H_4 = \{\neg p, q, \neg\mathbf{X}(p\mathbf{U}q), p\mathbf{U}q\}$$

По *вспомогательной теореме*, в $\mathcal{HS}(M,\varphi)$ содержится радужный маршрут — например, такой: $(\textcircled{\textcircled{p}}, H_2) \to (\textcircled{p}, H_2) \to (\textcircled{p}, H_2) \to \ldots$

По *основной теореме*, это означает, что $M \not\models \varphi$

Из вида радужной компоненты можно извлечь и **вычисление** τ с.п. M, такое что $\tau \not\models \varphi$: $\textcircled{\textcircled{p}} \to \textcircled{p} \to \textcircled{p} \to \ldots$

Заключение

Несколько вопросов, размышление над которыми поможет лучше понять, как устроен табличный алгоритм model checking для LTL:

- Сколько формул содержится в множестве $[\varphi]_{fl}$?
  (*например, относительно числа операций в* φ)
- Сколько вершин содержится в системе Хинтикки $\mathcal{HS}(M, \varphi)$?
  (*например, относительно числа состояний в* M
  и числа операций в φ)
- Какую сложность имеет описанный алгоритм? (*например, относительно числа состояний в* M *и числа операций в* φ)
- Можно ли изменить определение системы Хинтикки так, чтобы теоремы остались справедливыми, но в системе содержался **ровно один цвет**?
- Можно ли устроить алгоритм model checking так, чтобы система Хинтикки **не строилась целиком**?