

# Математические методы верификации схем и программ

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

## Блок 19

Автоматы Бюхи  
для ltl-формул

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

ВМК МГУ, 2023/2024, осенний семестр

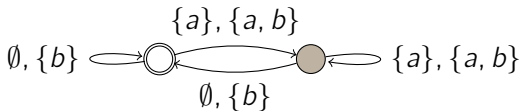
Общая схема автоматного алгоритма model checking для LTL:

1. По модели Крипке  $M$  строится автомат  $A_M$ , распознающий  $\text{Tr}(M)$
2. По ltl-формуле  $\varphi$  строится автомат  $A_{\neg\varphi}$ , распознающий  $\text{Tr}(\neg\varphi)$
3. Строится пересечение  $A_{\cap}$  автоматов  $A_M$  и  $A_{\neg\varphi}$ : автомат, распознающий  $\text{Tr}(M) \cap \text{Tr}(\neg\varphi)$
4. Проверяется **пустота** автомата  $A_{\cap}$ :  $\text{Tr}(M) \cap \text{Tr}(\neg\varphi) \stackrel{?}{=} \emptyset$
5. Выдаётся ответ: «да»  $\Leftrightarrow$  автомат  $A_{\cap}$  пуст

Начнём с примеров ( $AP = \{a, b\}$ )

$$\varphi = \mathbf{GF}a$$

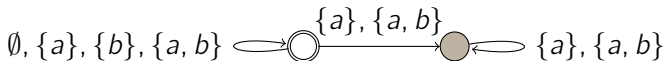
$$A_\varphi = ?$$



Легко видеть, что  $L(A_\varphi) = \text{Tr}(\varphi)$

$$\psi = \mathbf{FG}a$$

$$A_\psi = ?$$

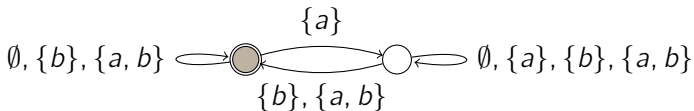


Легко видеть, что  $L(A_\psi) = \text{Tr}(\psi)$

Начнём с примеров ( $AP = \{a, b\}$ )

$$\varphi = \mathbf{G}(a \rightarrow \mathbf{F}b)$$

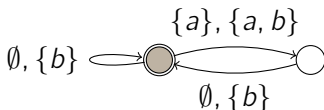
$$A_\varphi = ?$$



Легко видеть, что  $L(A_\varphi) = \text{Tr}(\varphi)$

$$\psi = \mathbf{G}(a \rightarrow \mathbf{X}\neg a)$$

$$A_\psi = ?$$



Легко видеть, что  $L(A_\psi) = \text{Tr}(\psi)$

А как быть с произвольной ltl-формулой?

Опишем способ построения таких автоматов без доказательства

**Дано:** произвольная ltl-формула  $\varphi$

**Требуется:** построить (конструктивно задать) автомат Бюхи  $A_\varphi$ , для которого верно  $L(A_\varphi) = \text{Tr}(\varphi)$

Согласно **теореме о разобобщении автомата Бюхи**, достаточно показать, как построить

**обобщённый** автомат Бюхи  $GA_\varphi$ , такой что  $L(GA_\varphi) = \text{Tr}(\varphi)$

*Без ограничения общности* можно полагать, что  $\varphi$  — формула **без двойных отрицаний**: не содержит подформулы  $\neg\neg\psi$  (т.к.  $\neg\neg\psi \equiv \psi$ )

Формулы вида  $\neg\psi$  далее будем называть **негативными**, а остальные — **позитивными**

**Замыкание Фишера-Ладнера**  $[\varphi]_{fl}$  формулы  $\varphi$  — это множество формул, содержащее следующие формулы и только их:

1. Все **позитивные подформулы** формулы  $\varphi$
2. Для каждой подформулы вида  $\psi\mathbf{U}\chi$  формулы  $\varphi$  — формулу  **$\mathbf{X}(\psi\mathbf{U}\chi)$**

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

**Гипотезой** (для формулы  $\varphi$ ) назовём множество формул вида

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

где  $F \subseteq [\varphi]_{fl}$

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

Гипотезу  $H$  объявим **совместной**, если для любых формул вида  $\psi_1 \& \psi_2$  и  $\chi_1 \mathbf{U} \chi_2$  из  $[\varphi]_{fl}$  верно:

- ▶  $\psi_1 \& \psi_2 \in H \Leftrightarrow \{\psi_1, \psi_2\} \subseteq H$
- ▶  $\chi_1 \mathbf{U} \chi_2 \in H \Leftrightarrow \chi_2 \in H$  или  $\{\chi_1, \mathbf{X}(\chi_1 \mathbf{U} \chi_2)\} \subseteq H$

**Например**, гипотеза  $\{p, \neg q, p \mathbf{U} \neg q, \mathbf{X}(p \mathbf{U} \neg q)\}$  совместна, а  $\{p, \neg q, \neg(p \mathbf{U} \neg q), \mathbf{X}(p \mathbf{U} \neg q)\}$  — нет

**Состояниями автомата  $GA_\varphi$  объявим всевозможные совместные гипотезы для  $\varphi$**

**Начальными состояниями автомата  $GA_\varphi$  объявим все вершины, в которых содержится  $\varphi$**

Гипотезы  $H_1$  и  $H_2$  назовём **локально согласованными**, если для любой формулы вида  $\mathbf{X}\psi$  из  $[\varphi]_{fl}$  верно

$$\mathbf{X}\psi \in H_1 \Leftrightarrow \psi \in H_2$$

**В множество переходов автомата  $GA_\varphi$  включим те и только те переходы  $H_1 \xrightarrow{X} H_2$ , для которых  $X = H_1 \cap AP$  и пара гипотез  $H_1, H_2$  локально согласованна**

Будем говорить, что гипотеза  $H$  **завершает формулу** вида  $\psi\mathbf{U}\chi$  из  $[\varphi]_{fl}$ , если верно хотя бы одно из двух:

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

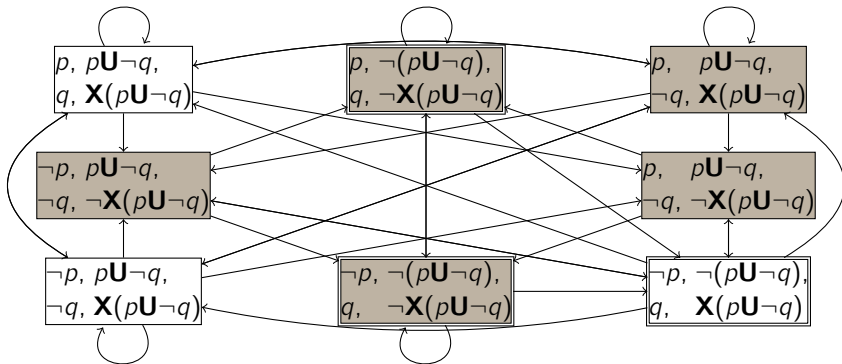
**Произвольно упорядочим все подформулы вида  $\psi_1\mathbf{U}\psi_2$  из  $[\varphi]_{fl}$ :**

$\chi_1, \chi_2, \dots, \chi_k$  — **и добавим в  $GA_\varphi$  допускающие множества  $F_1, \dots, F_k$ :**

$H \in F_i \Leftrightarrow$  **гипотеза  $H$  завершает формулу  $\chi_i$**

## Пример

Обобщённый автомат Бюхи  $GA_{\neg(p \cup \neg q)}$  может быть устроен так:



(Метки дуг опущены: дуга, исходящая из  $N$ , помечена событием  $N \cap AP$ )

Можете попробовать самостоятельно доказать, что автомат, устроенный **согласно полужирному зелёному тексту**, действительно распознаёт свойство формулы (и это непросто!)