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, 2024/2025, осенний семестр

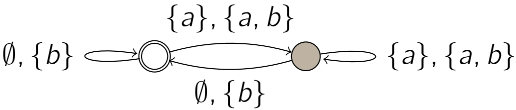
Общая схема автоматного алгоритма проверки моделей для LTL:

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

Начнём с примеров ($AP = \{a, b\}$)

$\varphi = \mathbf{GF}a$

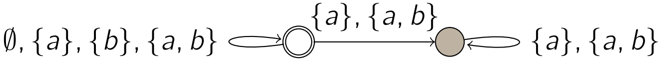
$A_\varphi = ?$



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

$\psi = \mathbf{FG}a$

$A_\psi = ?$

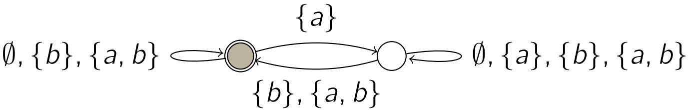


Легко видеть, что $L(A_\psi) = \mathrm{Tr}(\psi)$

Начнём с примеров (AP $= \{a, b\}$)

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

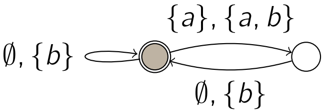
$A_\varphi = ?$



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

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

$A_\psi = ?$



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

А как быть с произвольной ltl-формулой?

Опишем способ построения таких автоматов без доказательства

Дано: произвольная ltl-формула φ

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

Согласно теореме о разобобщении автомата Бюхи, достаточно показать, как построить **обобщённый** автомат Бюхи GA_φ, такой что $L(GA_\varphi) = \mathrm{Tr}(\varphi)$

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

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

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

1. Все позитивные подформулы формулы φ
2. Для каждой подформулы вида $\psi\mathbf{U}\chi$ формулы φ — 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 φ) 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_φ объявим всевозможные совместные гипотезы для φ

Начальными состояниями автомата GA_φ объявим все вершины, в которых содержится φ

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_φ включим те и только те переходы $H_1 \xrightarrow{X} H_2$, для которых $X = H_1 \cap \mathrm{AP}$ и пара гипотез H_1, H_2 локально согласованна

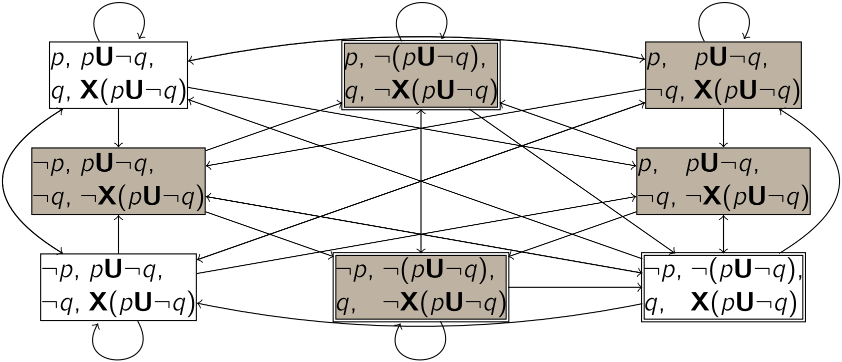
Будем говорить, что гипотеза H завершает формулу вида $\psi\mathbf{U}\chi$ из $[\varphi]_{fl}$, если верно хотя бы одно из двух:

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_φ допускающие множества $F_1, \dots, F_k$: $H \in F_i \Leftrightarrow$ гипотеза H завершает формулу χ_i

Пример

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



(*Метки дуг опущены: дуга, исходящая из H, помечена событием* $H \cap \mathrm{AP}$)

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