

Математические методы верификации схем и программ

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

Блок 14

Автоматы Бюхи
для моделей Крипке
и ltl-формул

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

Напоминание

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 φ 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

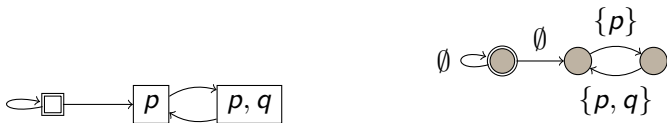
Модель Крипке \rightarrow автомат Бюхи

Для модели Крипке $M = (S, S_0, \rightarrow, L)$ над AP определим автомат Бюхи

$A_M = (S', S'_0, \mapsto, F)$ над 2^{AP} так:

- ▶ $S' = F = S$
- ▶ $S'_0 = S_0$
- ▶ $s_1 \xrightarrow{x} s_2 \Leftrightarrow s_1 \rightarrow s_2$ и $L(s_1) = x$

Пример (слева — модель Крипке M , справа — автомат A_M)



Теорема (о трансляции модели Крипке в автомат Бюхи). Для любой модели Крипке M верно $\text{Tr}(M) = L(A_M)$

Доказательство. Очевидно? (Трасса вычисления M является словом, порождающим то же вычисление A_M , и наоборот; и все вычисления A_M успешны)

Напоминание

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 φ 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

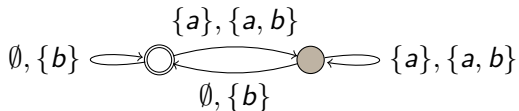
Ltl-формула \rightarrow автомат Бюхи

Начнём с примеров

(AP = {a, b})

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

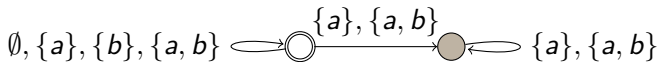
$$A_\varphi = ?$$



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

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

$$A_\psi = ?$$



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

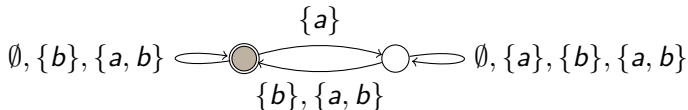
Ltl-формула \rightarrow автомат Бюхи

Начнём с примеров

(AP = {a, b})

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

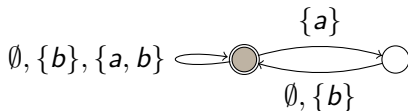
$$A_\varphi = ?$$



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

Ltl-формула \rightarrow автомат Бюхи

Дано: произвольная ltl-формула φ

Требуется: построить (конструктивно задать) автомат Бюхи A_φ , такой что $L(A_\varphi) = \text{Tr}(\varphi)$

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

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

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

Замыкание Фишера-Ладнера $[\varphi]_{\#}$ 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, $[\neg(p\mathbf{U}\neg q)]_{\#} = \{p, q, p\mathbf{U}\neg q, \mathbf{X}(p\mathbf{U}\neg q)\}$

Ltl-формула \rightarrow автомат Бюхи

Гипотезой (для формулы φ) назовём множество формул вида

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

где $F \subseteq [\varphi]_{\#}$

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 $[\varphi]_{\#}$ 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

Ltl-формула \rightarrow автомат Бюхи

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 $X = H_1 \cap AP$ 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:

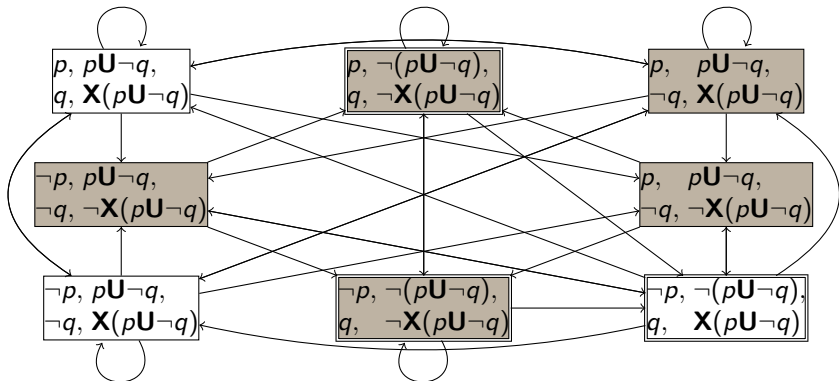
1. $\chi \in H$
2. $\mathbf{X}(\psi \mathbf{U} \chi) \notin H$

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

Ltl-формула \rightarrow автомат Бюхи

Пример

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



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

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