Математические методы верификации схем и программ

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

Блок 16

Пересечение автоматов Бюхи

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

ВМК МГУ, 2025, сентябрь–декабрь

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

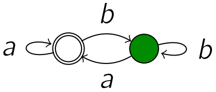
Автомат Бюхи A будем называть
пересечением автоматов Бюхи A_1 и A_2, если $L(A) = L(A_1) \cap L(A_2)$

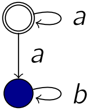
Записью $A' \otimes A''$
для автоматов Бюхи $A' = (S', S'_0, \rightarrow, F')$ и $A'' = (S'', S''_0, \mapsto, F'')$
обозначим синхронную композицию этих автоматов,
то есть **обобщённый** автомат Бюхи $(S, S_0, \Rightarrow, \mathcal{F})$ следующего вида:

- $S = S' \times S''$
- $S_0 = S'_0 \times S''_0$
- $\mathcal{F} = \{F' \times S'', S' \times F''\}$
- $(s'_1, s''_1) \overset{x}{\Rightarrow} (s'_2, s''_2) \Leftrightarrow s'_1 \xrightarrow{x} s'_2$ и $s''_1 \overset{x}{\mapsto} s''_2$

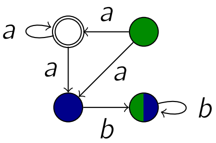
Пример

Синхронной композицией автоматов Бюхи

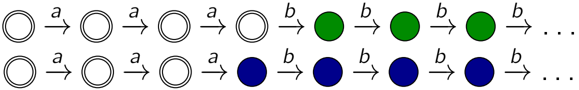




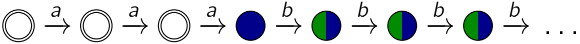
является обобщённый автомат Бюхи



Паре вычислений исходных автоматов



взаимно соответствует вычисление композиции



Теорема о пересечении автоматов Бюхи

Для любой пары автоматов Бюхи A', A'' разобобщение автомата $A' \otimes A''$ является их пересечением

Доказательство

По теореме о разобобщении автомата Бюхи,
достаточно показать, что верно $L(A' \otimes A'') = L(A') \cap L(A'')$

Пусть, для определённости,

- $A' = (S', S'_0, \rightarrow, F')$
- $A'' = (S'', S''_0, \mapsto, F'')$
- $A' \otimes A'' = (S, S_0, \Rightarrow, \{F_1, F_2\})$

Теорема о пересечении автоматов Бюхи

Для любой пары автоматов Бюхи A', A''
разобобщение автомата $A' \otimes A''$ является их пересечением

Доказательство ($L(A' \otimes A'') \subseteq L(A') \cap L(A'')$)

$(A' = (S', S'_0, \to, F'),\ A'' = (S'', S''_0, \mapsto, F''),\ A' \otimes A'' = (S, S_0, \Rightarrow, \{F_1, F_2\}))$

Рассмотрим произвольное ω-слово $w \in L(A' \otimes A'')$

В $A' \otimes A''$ существует успешное вычисление ρ вида

$$(s'_1, s''_1) \xRightarrow{w[1]} (s'_2, s''_2) \xRightarrow{w[2]} \dots$$

По заданию автомата $A' \otimes A''$, верно следующее:

- $\rho' = (s'_1 \xrightarrow{w[1]} s'_2 \xrightarrow{w[2]} \dots)$ — вычисление автомата A'
  - Так как $inf(\rho) \cap (F' \times S'') \neq \emptyset$, то и $inf(\rho') \cap F' \neq \emptyset$
  - Значит, вычисление ρ' успешно
- $\rho'' = (s''_1 \xmapsto{w[1]} s''_2 \xmapsto{w[2]} \dots)$ — вычисление автомата A''
  - Аналогично, вычисление ρ'' успешно

Значит, $w \in L(A')$ и $w \in L(A'')$, то есть $w \in L(A') \cap L(A'')$

Теорема о пересечении автоматов Бюхи

Для любой пары автоматов Бюхи A', A''
разобобщение автомата $A' \otimes A''$ является их пересечением

Доказательство ($L(A' \otimes A'') \supseteq L(A') \cap L(A'')$)
$(A' = (S', S'_0, \rightarrow, F'),\ A'' = (S'', S''_0, \mapsto, F''),\ A' \otimes A'' = (S, S_0, \Rightarrow, \{F_1, F_2\}))$

Рассмотрим ω-слово $w \in L(A') \cap L(A'')$

Тогда существуют успешные вычисления ρ', ρ'' соответственно вида

$$(s'_1 \xrightarrow{w[1]} s'_2 \xrightarrow{w[2]} \dots) \quad \text{и} \quad (s''_1 \xmapsto{w[1]} s''_2 \xmapsto{w[2]} \dots)$$

По заданию автомата $A' \otimes A''$, верно следующее:

- $\rho = ((s'_1, s''_1) \xRightarrow{w[1]} (s'_2, s''_2) \xRightarrow{w[2]} \dots)$ — вычисление $A' \otimes A''$
- Так как $inf(\rho') \cap F' \neq \emptyset$, то и $inf(\rho) \cap (F' \times S'') \neq \emptyset$
- Аналогично, $inf(\rho) \cap (S' \times F'') \neq \emptyset$

Значит, вычисление ρ успешно, и $w \in L(A' \otimes A'')$ ▼