

# Математические методы верификации схем и программ

[mk.cs.msu.ru](http://mk.cs.msu.ru) → Лекционные курсы  
→ Математические методы верификации схем и программ

## Блок 13

Пересечение автоматов Бюхи  
Проверка пустоты автомата Бюхи

Лектор:  
Подымов Владислав Васильевич  
E-mail:  
**[valdus@yandex.ru](mailto: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  $\varphi$  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

# Пересечение автоматов Бюхи

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

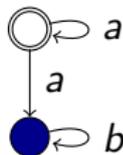
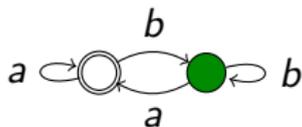
Записью  $A' \otimes A''$  для автоматов Бюхи  $A' = (S', S'_0, \rightarrow, F')$  и  $A'' = (S'', S''_0, \mapsto, F'')$  обозначим **синхронную композицию** этих автоматов, то есть **обобщённый** автомат Бюхи  $(S, S_0, \Rightarrow, \mathcal{F})$  следующего вида:

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

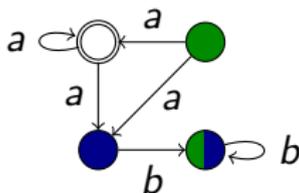
# Пересечение автоматов Бюхи

## Пример

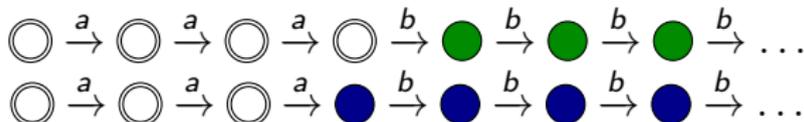
Синхронной композицией автоматов Бюхи



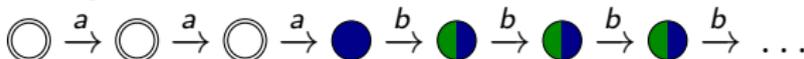
является обобщённый автомат Бюхи



Паре вычислений исходных автоматов



взаимно соответствует вычисление композиции



## Теорема о пересечении автоматов Бюхи

Для любой пары автоматов Бюхи  $A'$ ,  $A''$  разобобщение их синхронной композиции 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 их синхронной композиции является их пересечением

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

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

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

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

$(s'_0, s''_0) \xrightarrow{w[0]} (s'_1, s''_1) \xrightarrow{w[1]} \dots$

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

- ▶  $\rho' = (s'_0 \xrightarrow{w[0]} s'_1 \xrightarrow{w[1]} \dots)$  — вычисление автомата  $A'$ 
  - ▶ Так как  $\text{inf}(\rho) \cap (F' \times S'') \neq \emptyset$ , то и  $\text{inf}(\rho') \cap F' \neq \emptyset$
  - ▶ Значит, вычисление  $\rho'$  успешно
- ▶  $\rho'' = (s''_0 \xrightarrow{w[0]} s''_1 \xrightarrow{w[1]} \dots)$  — вычисление автомата  $A''$ 
  - ▶ Аналогично, вычисление  $\rho''$  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 их синхронной композиции 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  $\omega$ -слово  $w \in L(A') \cap L(A'')$

Тогда существуют успешные вычисления  $\rho'$ ,  $\rho''$  соответственно вида  $(s'_0 \xrightarrow{w[0]} s'_1 \xrightarrow{w[1]} \dots)$  и  $(s''_0 \xrightarrow{w[0]} s''_1 \xrightarrow{w[1]} \dots)$

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

- ▶  $\rho = ((s'_0, s''_0) \xrightarrow{w[0]} (s'_1, s''_1) \xrightarrow{w[1]} \dots)$  — вычисление  $A' \oplus A''$
- ▶ Так как  $\text{inf}(\rho') \cap F' \neq \emptyset$ , то и  $\text{inf}(\rho) \cap (F' \times S'') \neq \emptyset$
- ▶ Аналогично,  $\text{inf}(\rho) \cap (S' \times F'') \neq \emptyset$

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

# 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  $\varphi$  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

# Проверка пустоты автомата Бюхи

Автомат Бюхи  $A$  **пуст**, если им распознаётся пустой язык, и **непуст** иначе

Для лучшего понимания теоремы, сводящей проверку пустоты автомата Бюхи к графовым задачам, полезно напомнить (или ввести) соответствующие термины

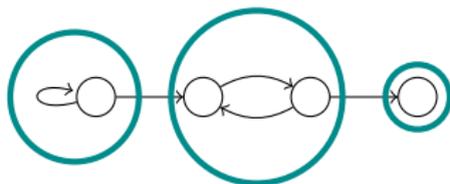
Вершина  $u$  ориентированного графа **достижима** из вершины  $v$ , если в этом графе существует путь из  $v$  в  $u$  (быть может, тривиальный, если  $u = v$ )

Ориентированный граф называется **сильно связным**, если любые две его вершины достижимы друг из друга

# Проверка пустоты автомата Бюхи

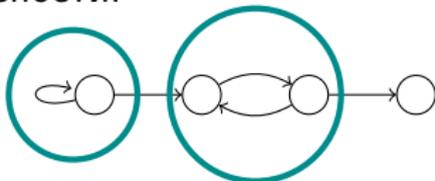
**Компонента сильной связности** ориентированного графа — это максимальный по включению вершин и дуг сильно связный подграф этого графа

**Например,** ниже в графе обведены окружностями все компоненты сильной связности:



Компонента сильной связности **нетривиальна**, если в ней содержится хотя бы одна дуга

**Например,** ниже в графе обведены окружностями все нетривиальные компоненты сильной связности:



# Проверка пустоты автомата Бюхи

**Теорема (о проверке пустоты автомата Бюхи).** Автомат Бюхи  $A$  непуст  $\Leftrightarrow$  в нём существует начальное состояние, из которого достижима хотя бы одна нетривиальная компонента сильной связности, содержащая хотя бы одно допускающее состояние

## Доказательство

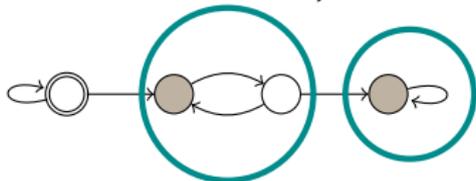
Если справедлива правая часть теоремы, то можно легко получить успешное вычисление: это путь из указанной начальной вершины к указанной компоненте, продолженный произвольным бесконечным обходом вершин этой компоненты

Если справедлива левая часть теоремы, то достаточно выбрать произвольное успешное вычисление, выделить в нём повторяющуюся вершину, такую что в подпути между выделенными повторами есть хотя бы одно допускающее состояние, и заметить, что тогда в автомате есть компонента сильной связности, содержащая вершины и дуги этого подпути (т.е. нетривиальная) ▼

# Проверка пустоты автомата Бюхи

## Примеры

Следующий автомат Бюхи непуст (компоненты сильной связности, упомянутые в теореме, обведены кругами):



Следующий автомат Бюхи пуст (не содержит требуемых в теореме компонент сильной связности):



Поиск компонент сильной связности в ориентированном графе — это известная задача, для которой известны эффективные решающие алгоритмы («лобовой» через транзитивное замыкание, Косарайю, Тарьяна, стековый, ...)