

Математические методы верификации схем и программ

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

Блок 17

Проверка пустоты автомата Бюхи

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 Кripке 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

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

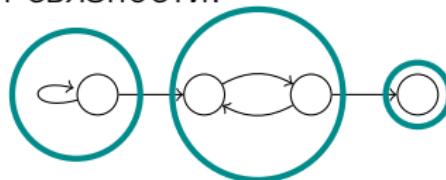
Для лучшего понимания теоремы,
сводящей проверку пустоты автомата Бюхи к графовым задачам,
полезно напомнить/ввести соответствующие понятия из теории графов

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

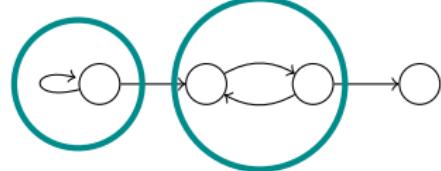
Компонента сильной связности (к.с.с.) ориентированного графа — это максимальный по включению вершин и дуг сильно связный подграф этого графа

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



Компонента сильной связности **нетривиальна** (н.к.с.с.), если в ней содержится хотя бы одна дуга

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



Теорема (о проверке пустоты автомата Бюхи)

Для любого автомата Бюхи A верно следующее: $L(A) \neq \emptyset \Leftrightarrow$
в A хотя бы из одного начального состояния достижима хотя бы
одна н.к.с.с., содержащая хотя бы одно допускающее состояние

Доказательство

(\Leftarrow) Если в A из начального состояния по пути $s_1 \rightarrow \dots \rightarrow s_k$
достижима н.к.с.с. с путём $s_k \rightarrow \pi \rightarrow s_k$ через допускающее состояние,
то $s_1 \rightarrow \dots \rightarrow s_k (\rightarrow \pi \rightarrow s_k)^\infty$ — успешное вычисление A

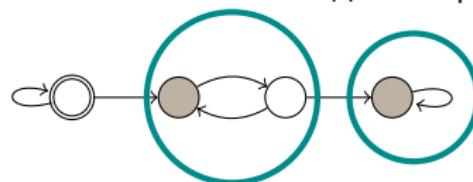
(\Rightarrow) Если $L(A) \neq \emptyset$, то в A существует успешное вычисление ρ

По бесконечности и успешности, ρ содержит префикс вида
 $s_1 \rightarrow \dots \rightarrow s_k \rightarrow \pi \rightarrow s_k$ с допускающим состоянием в подпуть $\pi \rightarrow s_k$

Тогда состояния подпути $\pi \rightarrow s_k$ входят в искомую н.к.с.с. ▼

Примеры

Следующий автомат Бюхи непуст
(н.к.с.с. с допускающим состоянием обведены кругами):



Следующий автомат Бюхи пуст
(не содержит н.к.с.с. с допускающим состоянием):



Поиск н.к.с.с. в ориентированном графе — это известная задача, для которой известны эффективные решающие алгоритмы, выходящие за рамки курса: [«лобовой» с транзитивным замыканием](#), [Косарайю](#), [Тарьяна](#), [стековый](#), ...