Математические методы верификации схем и программ

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

Блок 17

Базовый алгоритм
model checking для CTL

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

ВМК МГУ, 2022/2023, осенний семестр

Дано:

- Конечная модель Крипке $M = (S, S_0, \to, L)$
  - В описании и анализе алгоритма будут использоваться обозначения S, S_0, $\to$ и L в смысле соответствующих компонентов модели M
- Ctl-формула φ

Требуется: проверить справедливость соотношения $M \models \varphi$

То есть требуется проверить включение $S_0 \subseteq Sat(M, \varphi)$

Базовый алгоритм работает с явным представлением модели Крипке как размеченного ориентированного графа

Алгоритм будет описан как набор рекурсивно вызываемых процедур

Основная процедура, отвечающая алгоритму, устроена так:

- Вычислить множество $X = Sat(M, \varphi)$ при помощи процедуры с соответствующим названием
- Проверить включение $S_0 \subseteq X$
- Вернуть результат проверки предыдущего пункта

Корректность основной процедуры обеспечивается определием выполнимости ctl-формулы на модели

Процедура $Sat(M, \varphi)$:

- Используя известные равносильности, преобразовать φ в равносильную *упрощённую* формулу ψ в базисе **EX**, **EG**, **EU**:
$$\psi \ ::= \ \mathbb{t} \ \mid \ p \ \mid \ \psi \,\&\, \psi \ \mid \ \neg\psi \ \mid \ \mathbf{EX}\psi \ \mid \ \mathbf{EG}\psi \ \mid \ \mathbf{E}(\psi \mathbf{U} \psi)$$

- $Sat(M, \varphi) = Sat'(M, \psi)$, где процедура Sat' отличается от Sat тем, что применяется только к *упрощённым* формулам

Корректность этой процедуры обеспечивается равносильностью формул φ и ψ, из которой следует равенство $Sat(M, \varphi) = Sat(M, \psi)$

Процедура $Sat'(M, \varphi)$:

- Если $\varphi = \mathbb{t}$, то $Sat'(M, \varphi) = S$
- Если $\varphi = p \in \mathrm{AP}$, то $Sat'(M, \varphi) = \{s \mid s \in S,\ p \in L(s)\}$
- Если $\varphi = \psi_1 \,\&\, \psi_2$, то $Sat'(M, \varphi) = Sat'(M, \psi_1) \cap Sat'(M, \psi_2)$
- Если $\varphi = \neg\psi$, то $Sat'(M, \varphi) = S \setminus Sat'(M, \psi)$
- Если $\varphi = \mathbf{EX}\psi$, то $Sat'(M, \varphi) = Sat_{\mathbf{EX}}(M, \psi)$
- Если $\varphi = \mathbf{EG}\psi$, то $Sat'(M, \varphi) = Sat_{\mathbf{EG}}(M, \psi)$
- Если $\varphi = \mathbf{E}(\psi_1 \mathbf{U} \psi_2)$, то $Sat'(M, \varphi) = Sat_{\mathbf{EU}}(M, \psi_1, \psi_2)$

Корректность этой процедуры для первых четырёх пунктов очевидна (обеспечивается семантикой формул)

Осталось предложить подходящие процедуры $Sat_{\mathbf{EX}}$, $Sat_{\mathbf{EG}}$ и $Sat_{\mathbf{EU}}$

Для графа Γ и его вершины v записью $Pre(\Gamma, v)$ обозначим множество вершин, из которых v достижима по одной дуге:
$Pre(v) = \{v' \mid (v \to v') \in \Gamma\}$
Для графа Γ и множества вершин V записью $Pre(\Gamma, V)$ обозначим множество вершин, из которых хотя бы одна вершина V достижима по одной дуге: $Pre(\Gamma, V) = \bigcup\limits_{v \in V} Pre(\Gamma, v)$

Утверждение. Для любой модели Крипке M и любой ctl-формулы φ справедливо равенство $Sat(M, \mathbf{EX}\varphi) = Pre(M, Sat(M, \varphi))$

Доказательство.

$s \in Sat(M, \mathbf{EX}\varphi) \Leftrightarrow M, s \models \mathbf{EX}\varphi \Leftrightarrow$
существует состояние s', такое что $s \to s'$ и $M, s' \models \varphi \Leftrightarrow$
хотя бы одно состояние (s') множества $Sat(M, \varphi)$ достижимо из s по одной дуге $\Leftrightarrow$
$s \in Pre(Sat(M, \varphi))$ ▼

Процедура $Sat_{\mathbf{EX}}(M, \varphi)$ естественно вытекает из утверждения:

- Вычислить $X = Sat'(M, \varphi)$
- Вернуть множество $Pre(X)$

Утверждение. **Для любой конечной модели Крипке M и любых ctl-формул φ_1, φ_2 верно следующее:**
$s \in Sat(M, \mathbf{E}(\varphi_1 \mathbf{U} \varphi_2)) \Leftrightarrow$ **в** M **существует путь** $s_0 \to \cdots \to s_k$**, такой что** $s_1 = s$**,** $s_k \in Sat(M, \varphi_2)$ **и** $\{s_1, \ldots, s_{k-1}\} \subseteq Sat(M, \varphi_1)$

Доказательство.

$s \in Sat(M, \mathbf{E}(\varphi_1 \mathbf{U} \varphi_2)) \Leftrightarrow$

$M, s \models \mathbf{E}(\varphi_1 \mathbf{U} \varphi_2) \Leftrightarrow$

существуют бесконечный путь π из s в M и момент времени k, такие что $M, \pi[k] \models \varphi_2$ и для любого момента времени i, меньшего k, верно $M, \pi[i] \models \varphi_1 \Leftrightarrow$

в M существует путь $s_0 \to \cdots \to s_k$ (префикс пути π), такой что $M, s_k \models \varphi_2$ и для всех $i \in \{0, \ldots, k-1\}$ верно $M, s_i \models \varphi_1 \Leftrightarrow$

в M существует путь $s_0 \to \cdots \to s_k$, такой что $s_k \in Sat(M, \varphi_2)$ и $\{s_0, \ldots, s_{k-1}\} \subseteq Sat(M, \varphi_1)$ ▼

Процедура $Sat_{\mathsf{EU}}(M, \varphi_1, \varphi_2)$ строит требуемое множество состояний согласно последнему утверждению обратным проходом по дугам:

- Вычислить $X_0 = Y_0 = Sat'(M, \varphi_2)$
- Вычислить $Z = Sat'(M, \varphi_1)$
- Последовательно вычислять пары множеств $(X_1, Y_1), (X_2, Y_2), \ldots$ по следующей схеме, пока для очередной вычисленной пары (X_i, Y_i) не будет получено равенство $Y_i = \emptyset$:
  - $X_i = X_{i-1} \cup (Pre(Y_{i-1}) \cap Z)$
  - $Y_i = X_i \setminus X_{i-1}$
- Вернуть последнее вычисленное множество X_i

Корректность процедуры обосновывается

- последним доказанным утверждением,
- наблюдением «на грани очевидного» о том, что в множество X_i входят все вершины всех путей вида $s_0 \to \cdots \to s_i$, где $s_i \in Sat(M, \varphi_2)$ и $\{s_0, \ldots, s_{i-1}\} \subseteq Sat(M, \varphi_1)$, и
- гарантированным равенством $Y_i = \emptyset$ хотя бы для одного i в связи с конечностью M

Утверждение. **В конечном ориентированном графе Γ из вершины s исходит хотя бы один бесконечный путь $\Leftrightarrow$ в Γ из s достижима хотя бы одна нетривиальная компонента сильной связности**

Доказательство.

($\Leftarrow$) Пусть π — путь из s, оканчивающийся в вершине v нетривиальной компоненте сильной связности

По определению нетривиальной компоненты сильной связности, существует путь из v в v, содержащий хотя бы две вершины

Пусть π' — указанный путь из v в v без первой вершины v

Тогда в Γ содержится и бесконечный путь, исходящий из s: $\pi\pi'\pi'\ldots\pi'\ldots$

($\Rightarrow$) Рассмотрим бесконечный путь π в Γ, исходящий из s

Так как граф Γ конечен, то в π содержится хотя бы одна вершина v, встречающасяся хотя бы два раза: $\pi[i] = \pi[i+k] = v$, $k > 0$

Тогда все вершины множества $\{\pi[i+1], \ldots, \pi[i+k]\}$ достижимы друг из друга, то есть входят в некоторую компоненту сильной связности, и эта компонента достижима из s по пути $\pi[0] \to \cdots \to \pi[i]$ ▼

Для графа Γ и подмножества V его вершин записью $\Gamma|_V$ обозначим подграф графа Γ, порождённый множеством V:

- Множество вершин $\Gamma|_V$ — это V
- Дуга (s_1, s_2) входит в $\Gamma|_V \Leftrightarrow \{s_1, s_2\} \in V$ и эта дуга входит в Γ
- Метки вершин и дуг переносятся из Γ в $\Gamma|_V$

Утверждение. **Для любой конечной модели Крипке M и любой ctl-формулы φ верно следующее: $s \in Sat(M, \mathbf{EG}\varphi) \Leftrightarrow$ в графе $M|_{Sat(M,\varphi)}$ содержится вершина s и из неё достижима хотя бы одна нетривиальная компонента сильной связности**

Доказательство.

$s \in Sat(M, \mathbf{EG}\varphi) \Leftrightarrow M, s \models \mathbf{EG}\varphi \Leftrightarrow$
в M существует бесконечный путь π, исходящий из s и такой что $M, \pi[i] \models \varphi$ для каждого момента времени $i \Leftrightarrow$
в $\Gamma = M|_{Sat(M,\varphi)}$ существует бесконечный путь, исходящий из $s \Leftrightarrow$
в Γ содержится s и из неё достижима хотя бы одна нетривиальная компонента сильной связности ▼

Процедура $Sat_{\mathbf{EG}}(M, \varphi)$ строит требуемое множество состояний согласно последнему утверждению обратным проходом по дугам:

- Вычислить множество $X = Sat(M, \varphi)$
- Вычислить граф $\Gamma = M|_X$
- Каким-либо известным эффективным алгоритмом вычислить множество Y_0 всех вершин, входящих в какие-либо нетривиальные компоненты сильной связности графа Γ
- Присвоить $Z_0 = Y_0$, и последовательно вычислять пары множеств $(Y_1, Z_1), (Y_2, Z_2), \ldots$ по следующей схеме, пока не будет получено равенство $Z_i = \emptyset$:
  - $Y_i = Y_{i-1} \cup Pre(\Gamma, Z_{i-1})$
  - $Z_i = Y_i \setminus Y_{i-1}$
- Вернуть последнее вычисленное множество Y_i

Корректность этой процедуры показывается аналогично корректности процедуры $Sat_{\mathbf{EU}}$

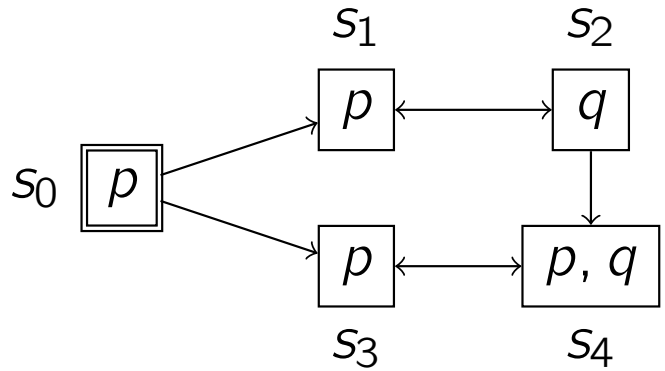
Пусть модель Крипке M содержит n вершин и m дуг, и формула φ содержит k операций

Если под сложностью алгоритма понимать общее число выполняемых элементарных теоретико-множественных и графовых операций, то при подходящем способе представления графов:

- Процедура Sat' вызывается не более k раз
- Если не считать рекурсивные вызовы Sat', то каждый вызов Sat' имеет сложность $O(n + m)$
- Следовательно, суммарная сложность алгоритма — $O((n + m) \cdot k)$

Пример

M:



$\varphi = \mathbf{EX}p \,\&\, \neg\mathbf{E}(q\mathbf{UEG}p)$

В процессе работы алгоритмом строятся следующие множества состояний

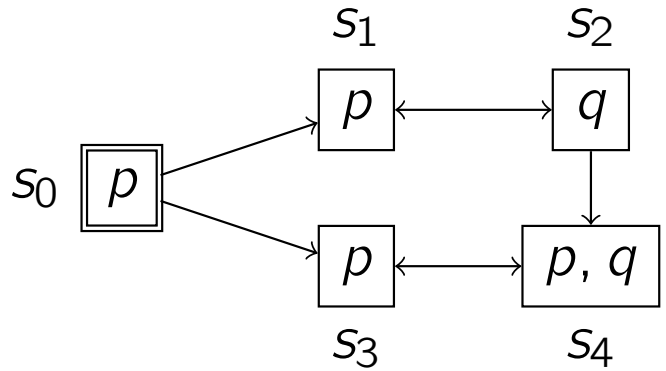
$Sat'(M, p) = \{s_0, s_1, s_3, s_4\}$

$Sat'(M, \mathbf{EX}p) = Sat_{\mathbf{EX}}(M, p) = Pre(Sat'(M, p)) = \{s_0, s_2, s_3, s_4\}$

$Sat'(M, q) = \{s_2, s_4\}$

Пример

M:



$\varphi = \mathbf{EX}p \,\&\, \neg\mathbf{E}(q\mathbf{UEG}p)$

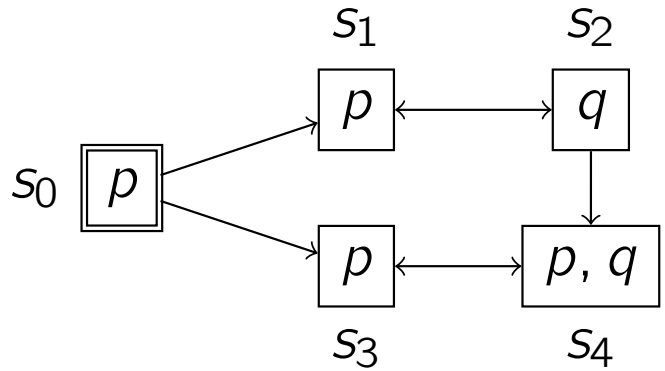
В процессе работы алгоритмом строятся следующие множества состояний

$Sat'(M, \mathbf{EG}p) = Sat_{\mathbf{EG}}(M, p)$:

- $X = Sat'(M, p) = \{s_0, s_1, s_3, s_4\}$
- $Y_0 = Z_0 = \{s_3, s_4\}$
- $Y_1 = Y_0 \cup Pre(M|_X, Z_0) = \{s_0, s_3, s_4\}$
- $Z_1 = Y_1 \setminus Z_0 = \{s_0\}$
- $Y_2 = Y_1 \cup Pre(M|_X, Z_1) = Y_1$
- $Z_2 = Y_2 \setminus Y_1 = \emptyset$
- $Sat_{\mathbf{EG}}(M, p) = Y_2 = \{s_0, s_3, s_4\}$

Пример

M:



$\varphi = \mathbf{EX}p \,\&\, \neg\mathbf{E}(q\mathbf{UEG}p)$

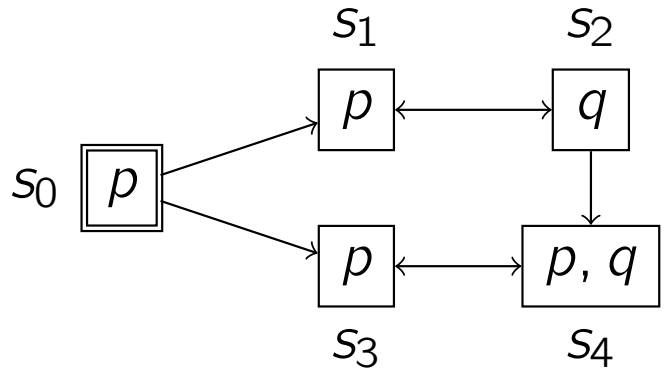
В процессе работы алгоритмом строятся следующие множества состояний

$Sat'(M, \mathbf{E}(q\mathbf{UEG}p)) = Sat_{\mathbf{EU}}(M, q, \mathbf{EG}p)$:

- $X_0 = Y_0 = Sat'(M, \mathbf{EG}p) = \{s_0, s_3, s_4\}$
- $Z = Sat'(M, q) = \{s_2, s_4\}$
- $X_1 = X_0 \cup (Pre(Y_0) \cap Z) = \{s_0, s_2, s_3, s_4\}$
- $Y_1 = X_1 \setminus X_0 = \{s_2\}$
- $X_2 = X_1 \cup (Pre(Y_1) \cap Z) = X_1$
- $Y_2 = X_2 \setminus X_1 = \emptyset$
- $Sat_{\mathbf{EU}}(M, q, \mathbf{EG}p) = X_2 = \{s_0, s_2, s_3, s_4\}$

Пример

M:



$\varphi = \mathbf{EX}p \,\&\, \neg\mathbf{E}(q\mathbf{UEG}p)$

В процессе работы алгоритмом строятся следующие множества состояний

$Sat'(M, \neg\mathbf{E}(q\mathbf{UEG}p)) = S \setminus Sat'(M, \mathbf{E}(q\mathbf{UEG}p)) = \{s_1\}$

$Sat'(M, \varphi) = Sat'(M, \mathbf{EX}p) \cap Sat'(M, \neg\mathbf{E}(q\mathbf{UEG}p)) = \emptyset$

Так как $\{s_0\} \not\subseteq \emptyset$, можно заключить, что $M \not\models \varphi$