

Математические методы верификации схем и программ

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

Блок 22

Базовый алгоритм
model checking для CTL

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

ВМК МГУ, 2023/2024, осенний семестр

Дано:

- ▶ Конечная модель Крипке $M = (S, S_0, \rightarrow, L)$
- ▶ Ctl-формула Φ

Требуется проверить справедливость соотношения $M \models \Phi$

То есть требуется проверить включение $S_0 \subseteq \text{Sat}(M, \Phi)$

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

Алгоритм будет описан как набор рекурсивно вызываемых процедур

Основная процедура \mathfrak{P}_{MC} , отвечающая алгоритму, устроена так

Дано: конечная модель Крипке $M = (S, S_0, \rightarrow, L)$, ctl-формула Φ

Требуется проверить соотношение $M \models \Phi$

Устройство процедуры:

1. Вычислить множество $X = Sat(M, \Phi)$ при помощи описанной далее процедуры \mathfrak{P}_{sat}
2. Проверить включение $S_0 \subseteq X$
3. Вернуть результат проверки предыдущего пункта

Корректность основной процедуры обеспечивается

- ▶ определением выполнимости ctl-формулы на модели и
- ▶ обсуждающейся далее корректностью процедуры \mathfrak{P}_{sat}

Процедура \mathfrak{P}_{sat}

Дано: конечная модель Крипке $M = (S, S_0, \rightarrow, L)$, ctl-формула Φ

Требуется вычислить множество $Sat(M, \Phi)$

Устройство процедуры:

1. Используя **известные равносильности**, преобразовать Φ в равносильную *упрощённую* формулу Ψ в базисе **EX, EG, EU**:
$$\Psi ::= \top \mid p \mid \Psi \ \& \ \Psi \mid \neg \Psi \mid \mathbf{EX} \Psi \mid \mathbf{EG} \Psi \mid \mathbf{E}(\Psi \mathbf{U} \Psi)$$
2. $\mathfrak{P}_{sat}(M, \Phi) = \mathfrak{P}'_{sat}(M, \Psi)$
 - ▶ Процедура \mathfrak{P}'_{sat} вычисления множества Sat для упрощённых формул будет описана дальше

Корректность этой процедуры обеспечивается равенством $Sat(M, \Phi) = Sat(M, \Psi)$, следующим из равносильности $\Phi \sim \Psi$

Процедура \mathfrak{P}'_{sat}

Дано: конечная модель Крипке $M = (S, S_0, \rightarrow, L)$, упрощённая ctl-формула Φ

Требуется вычислить множество $Sat(M, \Phi)$

Устройство процедуры:

- ▶ Если $\Phi = \top$, то $\mathfrak{P}'_{sat}(M, \Phi) = S$
- ▶ Если $\Phi = p \in AP$, то $\mathfrak{P}'_{sat}(M, \Phi) = \{s \mid s \in S, p \in L(s)\}$
- ▶ Если $\Phi = \Psi_1 \ \& \ \Psi_2$, то $\mathfrak{P}'_{sat}(M, \Phi) = \mathfrak{P}'_{sat}(M, \Psi_1) \cap \mathfrak{P}'_{sat}(M, \Psi_2)$
- ▶ Если $\Phi = \neg\Psi$, то $\mathfrak{P}'_{sat}(M, \Phi) = S \setminus \mathfrak{P}'_{sat}(M, \Psi)$
- ▶ Если $\Phi = \mathbf{EX}\Psi$, то $\mathfrak{P}'_{sat}(M, \Phi) = \mathfrak{P}_{EX}(M, \Psi)$
- ▶ Если $\Phi = \mathbf{EG}\Psi$, то $\mathfrak{P}'_{sat}(M, \Phi) = \mathfrak{P}_{EG}(M, \Psi)$
- ▶ Если $\Phi = \mathbf{E}(\Psi_1 \mathbf{U}\Psi_2)$, то $\mathfrak{P}'_{sat}(M, \Phi) = \mathfrak{P}_{EU}(M, \Psi_1, \Psi_2)$

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

Осталось предложить подходящие процедуры \mathfrak{P}_{EX} , \mathfrak{P}_{EG} и \mathfrak{P}_{EU}

Для ориентированного графа Γ и его вершины v и множества вершин V записями $Pre(\Gamma, v)$ и $Pre(\Gamma, V)$ обозначим множество вершин, из которых достижимы по одной дуге соответственно вершина v и хотя бы одна вершина множества V :

$$Pre(v) = \{v' \mid (v \rightarrow v') \in \Gamma\}$$
$$Pre(V) = \bigcup_{v \in V} Pre(\Gamma, v)$$

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

Доказательство.

$$s \in Sat(M, \mathbf{EX}\Phi)$$

$$\Leftrightarrow M, s \models \mathbf{EX}\Phi$$

$$\Leftrightarrow \text{существует состояние } s', \text{ такое что } s \rightarrow s' \text{ и } M, s' \models \Phi$$

\Leftrightarrow хотя бы одно состояние (s') множества $Sat(M, \Phi)$ достижимо из s по одной дуге

$$\Leftrightarrow s \in Pre(Sat(M, \Phi)) \quad \blacktriangledown$$

Процедура \mathfrak{R}_{EX}

Дано: конечная модель Крипке $M = (S, S_0, \rightarrow, L)$, упрощённая ctl-формула Φ

Требуется вычислить множество $Sat(M, EX\Phi)$

Устройство процедуры:

1. Вычислить $X = \mathfrak{R}'_{sat}(M, \Phi)$
2. Вернуть множество $Pre(X)$

Корректность этой процедуры следует из

- ▶ последнего утверждения и
- ▶ предполагаемой (по индукции) корректности процедуры \mathfrak{R}'_{sat}

Утверждение. Для любых конечной модели Крипке M , состояния s и ctl-формул Φ_1, Φ_2 верно следующее:

$s \in \text{Sat}(M, \mathbf{E}(\Phi_1 \mathbf{U} \Phi_2)) \Leftrightarrow$ в M существует путь $s_1 \rightarrow \dots \rightarrow s_k$, такой что $s_1 = s$, $s_k \in \text{Sat}(M, \Phi_2)$ и $\{s_1, \dots, s_{k-1}\} \subseteq \text{Sat}(M, \Phi_1)$

Доказательство.

$$s \in \text{Sat}(M, \mathbf{E}(\Phi_1 \mathbf{U} \Phi_2))$$

$$\Leftrightarrow M, s \models \mathbf{E}(\Phi_1 \mathbf{U} \Phi_2)$$

\Leftrightarrow существуют бесконечный путь π из s в M и момент времени k , такие что $M, \pi[k] \models \Phi_2$ и для любого момента времени i , меньшего k , верно $M, \pi[i] \models \Phi_1$

\Leftrightarrow в M существует путь $s_1 \rightarrow \dots \rightarrow s_k$ ($\pi[1] \rightarrow \dots \rightarrow \pi[k]$), такой что $M, s_k \models \Phi_2$ и для всех $i \in \{1, \dots, k-1\}$ верно $M, s_i \models \Phi_1$

\Leftrightarrow в M существует путь $s_1 \rightarrow \dots \rightarrow s_k$, такой что $s_k \in \text{Sat}(M, \Phi_2)$ и $\{s_1, \dots, s_{k-1}\} \subseteq \text{Sat}(M, \Phi_1)$ ▼

Процедура \mathfrak{F}_{EU}

Дано: конечная модель Крипке $M = (S, S_0, \rightarrow, L)$, упрощённые ctl-формулы Φ, Ψ

Требуется вычислить множество $Sat(M, \mathbf{E}(\Phi \mathbf{U} \Psi))$

Устройство процедуры:

1. Вычислить $Z = \mathfrak{F}'_{sat}(M, \Phi)$
2. Вычислить $X_0 = \mathfrak{F}'_{sat}(M, \Psi)$
3. Последовательно вычислять множества X_1, X_2, \dots по следующей схеме, пока для очередного вычисленного множества X_i не будет получено равенство $X_i = X_{i-1}$:
$$X_i = X_{i-1} \cup (Pre(X_{i-1}) \cap Z)$$
4. Вернуть последнее вычисленное множество X_i

Корректность процедуры обосновывается

- ▶ последним утверждением,
- ▶ наблюдением «на грани очевидного» о том, что в множество X_i входят все вершины всех путей вида $s_1 \rightarrow \dots \rightarrow s_j$, где $j \leq i$, $s_j \in Sat(M, \Phi_2)$ и $\{s_1, \dots, s_{j-1}\} \subseteq Sat(M, \Phi_1)$, и
- ▶ гарантированным равенством $X_i = X_{i-1}$ 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 этого утверждения несложно извлекается из теоремы о проверке пустоты автомата Бюхи

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 $\Gamma|_V \Leftrightarrow \{s_1, s_2\} \subseteq V$ 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: $s \in \text{Sat}(M, \mathbf{EG}\Phi) \Leftrightarrow$ в графе $M|_{\text{Sat}(M, \Phi)}$ содержится вершина s и из неё достижима хотя бы одна нетривиальная компонента сильной связности

Доказательство.

$s \in \text{Sat}(M, \mathbf{EG}\Phi) \Leftrightarrow M, s \models \mathbf{EG}\Phi$

\Leftrightarrow в M существует бесконечный путь Φ , исходящий из s и такой что $M, \pi[i] \models \varphi$ для каждого момента времени i

\Leftrightarrow в $\Gamma = M|_{\text{Sat}(M, \Phi)}$ существует бесконечный путь, исходящий из s

\Leftrightarrow в Γ содержится s и из неё достижима хотя бы одна нетривиальная компонента сильной связности ▼

Процедура \mathfrak{F}_{EG}

Дано: конечная модель Крипке $M = (S, S_0, \rightarrow, L)$, упрощённая ctl-формула Φ

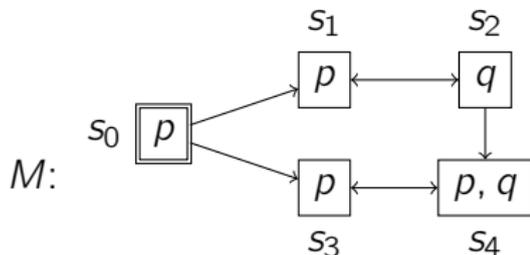
Требуется вычислить множество $Sat(M, \mathbf{EG}\Phi)$

Устройство процедуры:

1. Вычислить множество $Z = Sat(M, \Phi)$
2. Вычислить граф $\Gamma = M|_Z$
3. Каким-либо известным эффективным алгоритмом вычислить множество X_0 всех вершин, входящих в какие-либо нетривиальные компоненты сильной связности графа Γ
4. Последовательно вычислять множества X_1, X_2, \dots по следующей схеме, пока не будет получено равенство $X_i = X_{i-1}$:
$$X_i = X_{i-1} \cup Pre(\Gamma, X_{i-1})$$
5. Вернуть последнее вычисленное множество X_i

Корректность этой процедуры показывается аналогично корректности процедуры Sat_{EU}

Пример



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

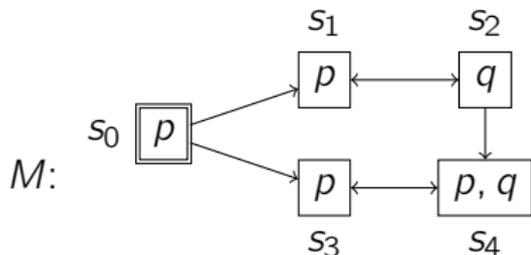
В процессе работы алгоритмом строятся следующие множества состояний

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

$$\text{Sat}(M, \mathbf{EX}p) = \mathfrak{P}_{\mathbf{EX}}(M, p) = \text{Pre}(\text{Sat}(M, p)) = \{s_0, s_2, s_3, s_4\}$$

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

Пример



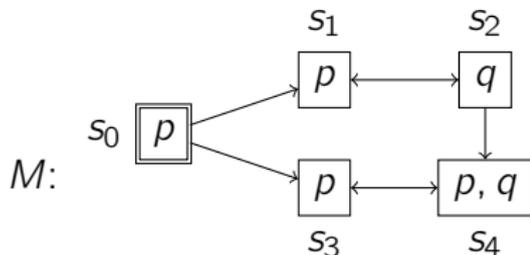
$$\varphi = \mathbf{EX}p \ \& \ \neg \mathbf{E}(q \mathbf{UEG} p)$$

В процессе работы алгоритмом строятся следующие множества состояний

$$Sat(M, \mathbf{EG}p) = \mathfrak{F}_{\mathbf{EG}}(M, p):$$

- ▶ $Z = Sat(M, p) = \{s_0, s_1, s_3, s_4\}$
- ▶ $X_0 = \{s_3, s_4\}$ (все вершины н.к.с.с. в $M|_Z$)
- ▶ $X_1 = X_0 \cup Pre(M|_X, X_0) = \{s_0, s_3, s_4\}$
- ▶ $X_2 = X_1 \cup Pre(M|_X, X_1) = X_1$
- ▶ $\mathfrak{F}_{\mathbf{EG}}(M, p) = X_2 = \{s_0, s_3, s_4\}$

Пример



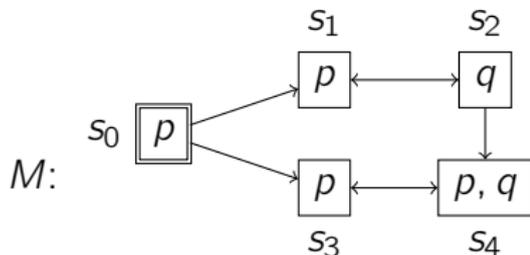
$$\varphi = \mathbf{EX}p \ \& \ \neg \mathbf{E}(q \mathbf{UEG} p)$$

В процессе работы алгоритмом строятся следующие множества состояний

$$\text{Sat}(M, \mathbf{E}(q \mathbf{UEG} p)) = \mathfrak{P}_{\text{EU}}(M, q, \mathbf{EG} p):$$

- ▶ $Z = \text{Sat}(M, q) = \{s_2, s_4\}$
- ▶ $X_0 = \text{Sat}(M, \mathbf{EG} p) = \{s_0, s_3, s_4\}$
- ▶ $X_1 = X_0 \cup (\text{Pre}(X_0) \cap Z) = \{s_0, s_2, s_3, s_4\}$
- ▶ $X_2 = X_1 \cup (\text{Pre}(X_1) \cap Z) = X_1$
- ▶ $\mathfrak{P}_{\text{EU}}(M, q, \mathbf{EG} p) = X_2 = \{s_0, s_2, s_3, s_4\}$

Пример



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

В процессе работы алгоритмом строятся следующие множества состояний

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

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

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

А какова сложность базового алгоритма относительно количества вершин и дуг в модели и количества операций в формуле?