Математические методы верификации схем и программ

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

Блок 38

Bounded model checking (BMC)
(постановка)

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

ВМК МГУ, 2023/2024, осенний семестр

Вступление

Вспомним задачу model checking для LTL (MC-LTL)

Дано: конечное множество атомарных высказываний AP, конечная модель Крипке $M = (S, S_0, \mapsto, L)$, ltl-формула φ

Требуется: проверить соотношение $M \models \varphi$

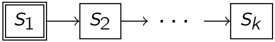
Известно, что это трудная задача (PSPACE-полная)

Но всё же хочется уметь её решать настолько эффективно и в теоретическом, и в практическом смысле, насколько это возможно

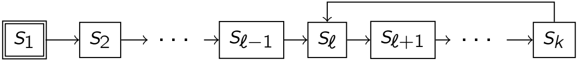
Вступление

Свойство трасс, которое хочется проверить относительно заданной модели на практике, зачастую устроено относительно просто:

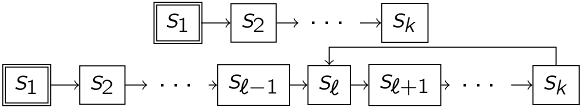
- Это либо свойство безопасности, либо свойство живости
- Если свойство не выполнено, то существует достаточно маленький конечный начальный путь в модели (порядка 10-100 состояний), являющийся «ядром» невыполнимости:
  - Для свойства безопасности это путь, для которого трасса любого продолжения небезопасна



  - Для свойства живости это путь (до состояния s_k) с выделенным состоянием (s_ℓ), обозначающий бесконечный путь с неживой трассой, продолжающийся повторением цикла от s_ℓ до s_k



Отношение ограниченной выполнимости



В предположении о том, что длина пути, представляющего «ядро» невыполнимости свойства, не превосходит k, можно организовать его поиск как перебор всех путей модели длины не более k

k-путём будем называть путь, содержащий k вершин

(k, ℓ)-циклом, где $\ell \leq k$, а также k-циклом будем называть пару (π, π'), где π — ℓ-путь, $\pi\pi'$ — k-путь и существует переход $\pi\pi'[k] \mapsto \pi\pi'[\ell]$

(k, ℓ)-циклу $\Pi = (\pi, \pi')$ отвечает бесконечный путь $\hat{\Pi} = \pi\pi'\pi' \ldots \pi' \ldots$

Отношение ограниченной выполнимости

Далее будем рассматривать ltl-формулы с поднятыми отрицаниями над множеством AP (negation normal form; NNF), то есть задающиеся БНФ

$$\begin{array}{rcl} \varphi & ::= & \mathbb{t} \mid p \mid \neg p \mid \varphi \,\&\, \varphi \mid \varphi \vee \varphi \\ & \mid & \mathbf{X}\varphi \mid \mathbf{F}\varphi \mid \mathbf{G}\varphi \mid \varphi \mathbf{U} \varphi \mid \varphi \mathbf{R} \varphi, \end{array}$$

где φ — nnf-формула и $p \in AP$

Напоминание: для «обычного» LTL верно $\psi_1 \mathbf{R} \psi_2 = \neg(\neg\psi_1 \mathbf{U} \neg\psi_2)$

Это ограничение синтаксиса ltl-формул *аналогично* ограничению, задаваемому для actl*-формул в языке CTL*

Некоторые аналогии можно проследить и для свойств этих двух фрагментов

Отношение ограниченной выполнимости

Рассмотрим nnf-формулу φ и модель Крипке $M = (S, S_0, \mapsto, L)$

Отношение k-выполнимости φ на k-пути или k-цикле π модели M ($M, \pi \models_k \varphi$) зададим так:[1]

- Если π — k-цикл, то
$$M, \pi \models_k \varphi \quad \Leftrightarrow \quad M, \hat{\pi} \models \varphi$$
- Если π — k-путь, то
$$M, \pi \models_k \varphi \quad \Leftrightarrow \quad M, \pi \models_k^1 \varphi$$
- Соотношение $M, \pi \models_k^i \mathbb{t}$ всегда верно
- $M, \pi \models_k^i p$ для $p \in \mathrm{AP} \quad \Leftrightarrow \quad p \in L(\pi[i])$
- $M, \pi \models_k^i \neg p$ для $p \in \mathrm{AP} \quad \Leftrightarrow \quad p \notin L(\pi[i])$
- $M, \pi \models_k^i \psi_1 \,\&\, \psi_2 \quad \Leftrightarrow \quad M, \pi \models_k^i \psi_1$ и $M, \pi \models_k^i \psi_2$
- $M, \pi \models_k^i \psi_1 \vee \psi_2 \quad \Leftrightarrow \quad M, \pi \models_k^i \psi_1$ или $M, \pi \models_k^i \psi_2$

---
1 Biere et al. Bounded Model Checking. 2003

Отношение ограниченной выполнимости

Рассмотрим nnf-формулу φ и модель Крипке $M = (S, S_0, \mapsto, L)$

Отношение k-выполнимости φ на k-пути или k-цикле π модели M ($M, \pi \models_k \varphi$) зададим так:[1]

- Соотношение $M, \pi \models_k^i \mathbf{G}\psi$ всегда неверно
- $M, \pi \models_k^i \mathbf{F}\psi \quad \Leftrightarrow \quad$ существует момент времени j, такой что $i \leq j \leq k$ и $M, \pi \models_k^j \psi$
- $M, \pi \models_k^i \mathbf{X}\psi \quad \Leftrightarrow \quad i < k$ и $M, \pi \models_k^{i+1} \psi$
- $M, \pi \models_k^i \psi_1 \mathbf{U} \psi_2 \quad \Leftrightarrow \quad$ существует момент времени j, такой что
  - $i \leq j \leq k$,
  - $M, \pi \models_k^j \psi_2$ и
  - для любого момента времени m, такого что $i \leq m < j$, верно $M, \pi \models_k^m \psi_1$
- $M, \pi \models_k^i \psi_1 \mathbf{R} \psi_2 \quad \Leftrightarrow \quad M, \pi \models_k^i \psi_2 \mathbf{U} \psi_1$

1 Biere et al. Bounded Model Checking. 2003

Отношение ограниченной выполнимости

Для ограниченной выполнимости очевидным образом неверны некоторые законы, справедливые для «неограниченной» выполнимости

Например, $M, \pi \models_k \mathbf{G}\neg p \quad \not\Leftrightarrow \quad M, \pi \not\models_k \mathbf{F}p$

$\boxed{\text{Для самостоятельного размышления:}}$

1. Какие из законов (равносильностей), приводившихся в лекциях для отношения $\models$, справедливы для $\models_k$, а какие нет?
2. В частности, справедливы ли равносильности, приводившиеся в блоке 28 в доказательстве лемм о том, что предикаты $Sat_M(\mathbf{EG}\varphi)$ и $Sat_M(\mathbf{E}(\varphi\mathbf{U}\psi))$ являются неподвижными точками преобразователей, приведённых в соответствующих леммах?

Отношение ограниченной выполнимости

Утверждение. **Для любых nnf-формулы φ, модели Крипке M, момента времени k, k-пути π и бесконечного пути $\pi\pi'$ в M верно:**

если $M, \pi \models_k \varphi$, то $M, \pi\pi' \models \varphi$

Утверждение

Для любых nnf-формулы φ и модели Крипке M верно:
если $M \not\models \neg\varphi$,
то существует k-путь или k-цикл, такой что $M, \pi \models_k \varphi$

Nnf-формула φ k-выполняется на модели Крипке M ($M \models_k \varphi$), если **существует** начальный k-путь или k-цикл π, такой что он отвечает начальному пути в M или является таким путём и верно $M, \pi \models_k \varphi$

Теорема. **Для любых nnf-формулы φ и модели Крипке M верно:**

$M \not\models \neg\varphi \quad \Leftrightarrow \quad$ **существует момент времени k, такой что $M \models_k \varphi$**

Проверка невыполнимости LTL-формулы φ на модели Крипке M $M \not\models \psi$ может быть записана относительно языка CTL* как $M \not\models \mathbf{A}\psi$
и переписана в виде $M \models \mathbf{E}\neg\psi$,
то есть для ltl-формулы $\varphi = \neg\psi$ — как $M \models \mathbf{E}\varphi$

Постановка задачи bounded model checking

Задача bounded model checking (BMC) формулируется так: для заданных момента времени k, конечной модели Крипке M и nnf-формулы φ проверить соотношение $M \models_k \varphi$

Иными словами, BMC — это задача MC-LTL, переформулированная как поиск пути заданной длины, являющегося «ядром» бесконечного пути, опровергающего выполнимость ltl-формулы с поднятыми отрицаниями