Математические методы верификации схем и программ

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

Блок 40

Решение BMC при помощи SAT

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

ВМК МГУ, 2023/2024, осенний семестр

Вступление

Задача BMC *трудна*

Задача SAT *тоже трудна, но не очень сильно*: NP-полна

При этом в некотором смысле задача SAT *проста*: имеются до некоторой степени эффективные средства её решения

Обсудим то, как можно использовать практически эффективное решение задачи SAT для повышения эффективности решения задачи BMC

BMC→SAT: общая схема

Покажем, как по входным данным задачи BMC (число k, модель Крипке M, nnf-формула φ) построить формулу $\Phi^k_{M,\varphi}$, такую что

$$\Phi^k_{M,\varphi} \text{ выполнима} \quad \Leftrightarrow \quad M \models_k \varphi$$

Тогда решение задачи BMC можно устроить так:

1. Построить формулу $\Phi^k_{M,\varphi}$
2. Проверить выполнимость этой формулы (*или соответствующей КНФ*)
3. Вернуть результат этой проверки как ответ к задаче

Если формула $\Phi^k_{M,\varphi}$ будет иметь *достаточно небольшой* размер относительно (k, M, φ), то такое решение можно считать эффективным (*настолько же, насколько эффективны современные SAT-решатели*)

BMC→SAT: общая схема

Формулу $\Phi^k_{M,\varphi}$ устроим так:

$$\Phi^k_{M,\varphi} = \Phi^k_M \,\&(\Phi^k_\varphi \vee \Psi^k_\varphi), \text{ где}$$

- Φ^k_M представляет множество всех начальных k-путей модели M
- Φ^k_φ представляет множество всех начальных k-путей, на которых k-выполнена φ
- $\Psi^k_\varphi = \bigvee\limits_{\ell=1}^{k} (\Psi^k_\ell \,\&\, \Psi^k_{\ell,\varphi})$, где
  - Ψ^k_ℓ — условие, отвечающее возможности разбить k-путь на (k,ℓ)-цикл, и
  - $\Psi^k_{\ell,\varphi}$ представляет множество всех (k,ℓ)-циклов, на которых k-выполнена φ

BMC→SAT: пути модели

Рассмотрим символьное представление модели Крипке $M = (S, S_0, \mapsto, L)$:

- Для кодирования состояний выбрано m переменных: $u_1, \dots, u_m$
- Каждому состоянию s сопоставлена элементарная конъюнкция χ_s от переменных $u_1, \dots, u_m$
- Множествам S, S_0 и отношению $\mapsto$ сопоставлены стандартные представления χ_S, χ_{S_0} и $\chi_{\mapsto}$
- Для простоты положим, что $AP = S$ и для каждого состояния s верно $L(s) = \{s\}$

$[\vec{u}/\vec{w}]$ — так сократим запись $[u_1/w_1, \dots, u_m/w_m]$

Состоянию $\pi[i]$ начального k-пути π сопоставим переменные $x_1^i, \dots, x_m^i$

Формула, представляющая множество всех начальных k-путей:

$$\Phi_M^k = \chi_{S_0}[\vec{u}/\vec{x}^1] \,\&\, \mathop{\&}_{i=2}^{k} \chi_{\mapsto}[\vec{u}/\vec{x}^{i-1}, \vec{u}'/\vec{x}^i]$$

BMC→SAT: k-пути формулы

Формула, представляющая множество всех начальных k-путей, на которых k-выполнена φ: $\Phi^k_\varphi = \Phi^k_{1,\varphi}$

Для $i \leq k$:

- $\Phi^k_{i,s} = \chi_s[\vec{u}/\vec{x}^i]$
- $\Phi^k_{i,\neg s} = \neg\chi_s[\vec{u}/\vec{x}^i]$
- $\Phi^k_{i,\psi_1 \,\&\, \psi_2} = \Phi^k_{i,\psi_1} \,\&\, \Phi^k_{i,\psi_2}$
- $\Phi^k_{i,\psi_1 \vee \psi_2} = \Phi^k_{i,\psi_1} \vee \Phi^k_{i,\psi_2}$
- $\Phi^k_{i,\mathbf{X}\psi} = \Phi^k_{i+1,\psi}$
- $\Phi^k_{i,\mathbf{F}\psi} = \Phi^k_{i,\psi} \vee \Phi^k_{i+1,\mathbf{F}\psi}$
- $\Phi^k_{i,\mathbf{G}\psi} = 0$
- $\Phi^k_{i,\psi_1\mathbf{U}\psi_2} = \Phi^k_{i,\psi_2} \vee (\Phi^k_{i,\psi_1} \,\&\, \Phi^k_{i+1,\psi_1\mathbf{U}\psi_2})$
- $\Phi^k_{i,\psi_1\mathbf{R}\psi_2} = \Phi^k_{i,\psi_2\mathbf{U}\psi_1}$

Кроме того, для любой nnf-формулы ψ и любого m, $m > k$, верно $\Phi^k_{m,\psi} = 0$

BMC→SAT: (k,ℓ)-циклы формулы

Легко видеть, что k-путь π можно разбить на (k,ℓ)-цикл $\Leftrightarrow$ в отношении $\mapsto$ содержится дуга $(\pi[k],\pi[\ell])$

Формула, обозначающая, что k-путь может быть разбит на (k,ℓ)-цикл для заданного ℓ:

$$\Psi_\ell^k = \psi_{\mapsto}[\vec{u}/\vec{x}^k, \vec{u}'/\vec{x}^\ell]$$

$next_\ell^k(i)$ — так обозначим номер состояния, следующего за i-м в (k,ℓ)-цикле:

- Если $i < k$, то $next_\ell^k(i) = i + 1$
- $next_\ell^k(k) = \ell$

BMC→SAT: (k, ℓ)-циклы формулы

Формула, представляющая множество всех (k, ℓ)-циклов, на которых k-выполнена φ: $\Psi^k_{\ell,\varphi} = \Psi^k_{1,\varphi}$

- $\Psi^k_{i,s} = \chi_s[\vec{u}/\vec{x}^i]$
- $\Psi^k_{i,\neg s} = \neg\chi_s[\vec{u}/\vec{x}^i]$
- $\Psi^k_{i,\psi_1 \,\&\, \psi_2} = \Psi^k_{i,\psi_1} \,\&\, \Psi^k_{i,\psi_2}$
- $\Psi^k_{i,\psi_1 \vee \psi_2} = \Psi^k_{i,\psi_1} \vee \Psi^k_{i,\psi_2}$
- $\Psi^k_{i,\mathbf{X}\psi} = \Psi^k_{next^k_\ell(i),\psi}$
- $\Psi^k_{i,\mathbf{F}\psi} = \Psi^{k,k}_{i,\mathbf{F}\psi}$, $\Psi^{k,m}_{i,\mathbf{F}\psi} = \Psi^k_{i,\psi} \vee \Psi^{k,m-1}_{next^k_\ell(i),\mathbf{F}\psi}$ для $m > 1$, $\Psi^{k,1}_{i,\mathbf{F}\psi} = \Psi^k_{i,\psi}$
- $\Psi^k_{i,\mathbf{G}\psi} = \Psi^{k,k}_{i,\mathbf{G}\psi}$, $\Psi^{k,m}_{i,\mathbf{G}\psi} = \Psi^k_{i,\psi} \,\&\, \Psi^{k,m-1}_{next^k_\ell(i),\mathbf{G}\psi}$ для $m > 1$, $\Psi^{k,1}_{i,\mathbf{G}\psi} = \Psi^k_{i,\psi}$
- $\Psi^k_{i,\psi_1\mathbf{U}\psi_2} = \Psi^{k,k}_{i,\psi_1\mathbf{U}\psi_2}$
  $\Psi^{k,m}_{i,\psi_1\mathbf{U}\psi_2} = \Psi^k_{i,\psi_2} \vee (\Psi^k_{i,\psi_1} \,\&\, \Psi^{k,m-1}_{next^k_\ell(i),\psi_1\mathbf{U}\psi_2})$ для $m > 1$
  $\Psi^{k,1}_{i,\psi_1\mathbf{U}\psi_2} = \Psi^k_{i,\psi_2}$
- $\Psi^k_{i,\psi_1\mathbf{R}\psi_2} = \Psi^k_{i,\psi_2\mathbf{U}\psi_1}$

BMC→SAT: заключение

Теорема. **Для любых модели Крипке M, натурального числа k и nnf-формулы φ верно:**

$$M \models_k \varphi \quad \Leftrightarrow \quad \text{булева формула } \Phi^k_{M,\varphi} \text{ выполнима}$$

Можете попробовать доказать это сами (и это технически непросто)

А какой размер имеет булева формула $\Phi^k_{M,\varphi}$ относительно числа k, количества состояний n и переходов m модели M и относительно числа операций q в формуле φ?

Описанная трансляция не очень эффективна, но можно её улучшить настолько, чтобы размер $\Phi^k_{M,\varphi}$ оказался линейным

Это в сочетании с использованием символьного представления, эффективностью SAT-решателей и тезисом о том, что на практике верхняя граница для числа k, за пределы которой увеличивать k нет смысла, невысока, обеспечивает эффективность решения задачи BMC, основанного на SAT