

# Математические методы верификации схем и программ

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

## Блок 32

Решение BMC при помощи SAT

Лектор:

**Подымов Владислав Васильевич**

E-mail:

**valdus@yandex.ru**

# Вступление

Задача BMC *очень трудна*: если не ограничивать параметр  $k$  длины рассматриваемых путей, то PSPACE-полна

Задача SAT *трудна, но не очень*: 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  $M$ , pnf-формула  $\varphi$ ) построить формулу  $\Phi_{M,\varphi}^k$ , такую что

$$\Phi_{M,\varphi}^k \text{ выполнима} \Leftrightarrow M \models_k \varphi$$

Тогда решение задачи BMC можно устроить так:

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

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

## BMC → SAT: общая схема

Формулу  $\Phi_{M,\varphi}^k$  устроим так:

$$\Phi_{M,\varphi}^k = \Phi_M^k \& (\Phi_\varphi^k \vee \Psi_\varphi^k), \text{ где}$$

- ▶  $\Phi_M^k$  представляет множество всех начальных  $k$ -путей модели  $M$
- ▶  $\Phi_\varphi^k$  представляет множество всех начальных  $k$ -путей, на которых  $k$ -выполнена  $\varphi$
- ▶  $\Psi_\varphi^k = \bigvee_{\ell=0}^k (\Psi_\ell^k \& \Psi_{\ell,\varphi}^k)$ , где  $\Psi_\ell^k$  представляет число  $\ell$ , разбивающее  $k$ -путь на  $(k, \ell)$ -цикл, и  $\Psi_{\ell,\varphi}^k$  представляет множество всех  $(k, \ell)$ -циклов, на которых  $k$ -выполнена  $\varphi$

## 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  $\chi_s$  от переменных  $u_1, \dots, u_m$
- ▶ Множествам  $S$ ,  $S_0$  и отношению  $\mapsto$  сопоставлены стандартные представления  $\chi_S$ ,  $\chi_{S_0}$  и  $\chi_{\mapsto}$
- ▶ Для простоты положим, что  $AP = S$  и для каждого состояния  $s$  верно  $L(s) = \{s\}$

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

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

Формула, представляющая множество всех начальных  $k$ -путей:

$$\Phi_M^k = \chi_{S_0}[\bar{u}/\bar{x}^0] \& \&_{i=1}^k \chi_{\mapsto}[\bar{u}/\bar{x}^{i-1}, \bar{u}'/\bar{x}^i]$$

## BMC → SAT: $k$ -пути формулы

Формула, представляющая множество всех начальных  $k$ -путей, на которых  $k$ -выполнена  $\varphi$ :  $\Phi_{\varphi}^k = \Phi_{0,\varphi}^k$

Для  $i \leq k$ :

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

Кроме того, для любой ппф-формулы  $\psi$  и любого  $m$ ,  $m > k$ , верно  $\Phi_{m,\psi}^k = 0$

## BMC $\rightarrow$ SAT: $(k, \ell)$ -циклы формулы

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

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

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

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

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

## BMC → SAT: $(k, \ell)$ -циклы формулы

Формула, представляющая множество всех  $(k, \ell)$ -циклов, на которых  $k$ -выполнена  $\varphi$ :  $\Psi_{\varphi}^k = \Psi_{0, \varphi}^k$

$$\Psi_{i, s}^k = \chi_s[\bar{u}/\bar{x}^i]$$

$$\Psi_{i, \neg s}^k = \neg \chi_s[\bar{u}/\bar{x}^i]$$

$$\Psi_{i, \psi_1 \& \psi_2}^k = \Psi_{i, \psi_1}^k \& \Psi_{i, \psi_2}^k$$

$$\Psi_{i, \psi_1 \vee \psi_2}^k = \Psi_{i, \psi_1}^k \vee \Psi_{i, \psi_2}^k$$

$$\Psi_{i, X\psi}^k = \Psi_{next_{\ell}^k(i), \psi}^k$$

$$\Psi_{i, F\psi}^k = \Psi_{i, F\psi}^{k, k}, \quad \Psi_{i, F\psi}^{k, m} = \Psi_{i, \psi}^k \vee \Psi_{next_{\ell}^k(i), F\psi}^{k, m-1} \text{ для } m > 0, \quad \Psi_{i, F\psi}^{k, 0} = \Psi_{i, \psi}^k$$

$$\Psi_{i, G\psi}^k = \Psi_{i, G\psi}^{k, k}, \quad \Psi_{i, G\psi}^{k, m} = \Psi_{i, \psi}^k \& \Psi_{next_{\ell}^k(i), G\psi}^{k, m-1} \text{ для } m > 0, \quad \Psi_{i, G\psi}^{k, 0} = \Psi_{i, \psi}^k$$

$$\Psi_{i, \psi_1 U \psi_2}^k = \Psi_{i, \psi_1 U \psi_2}^{k, k}$$

$$\Psi_{i, \psi_1 U \psi_2}^{k, m} = \Psi_{i, \psi_2}^k \vee (\Psi_{i, \psi_1}^k \& \Psi_{next_{\ell}^k(i), \psi_1 U \psi_2}^{k, m-1}) \text{ для } m > 0$$

$$\Psi_{i, \psi_1 U \psi_2}^{k, 0} = \Psi_{i, \psi_2}^k$$

$$\Psi_{i, \psi_1 R \psi_2}^k = \Psi_{i, \psi_2 U \psi_1}^k$$



## BMC → SAT: заключение

**Теорема.** Для любых модели Крипке  $M$ , натурального числа  $k$  и pnf-формулы  $\varphi$  верно:

$$M \models_k \varphi \quad \Leftrightarrow \quad \text{булева формула } \Phi_{k,M,\varphi} \text{ выполнима}$$

**Доказательство.** Можете попробовать 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  $\varphi$ ?

Описанная трансляция не очень эффективна, и можно её улучшить настолько, чтобы получить оценку, **линейную** относительно всех этих параметров

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