Реализация элиминации кванторов для арифметики Пресбургера, обогащённой функцией 2^x

Автор: Суханова Анжела Кирилловна, 371 группа (18.Б11-мм)
Научный руководитель: ассистент кафедры ИАС К. К. Смирнов

Санкт-Петербургский государственный университет
Кафедра системного программирования

24 апреля 2021г.

Введение

- Проверка и доказательство корректности разрабатываемой программы очень важны, ведь они необходимы для контроля соответствия поведения программы ожидаемому и обеспечения её безопасности
- Одним из методов формальной верификации является решение задачи выполнимости формул в теориях (SMT)
- Так как в основе архитектуры компьютера лежат операции с битовыми векторами, то необходимо уметь решать SMT в теории битовых векторов

Подходы к решению

- Можно ввести пропозициональные переменные для всех битов исходных термов и решать задачу выполнимости булевых формул
- Это сработает, но такой подход очень трудоёмкий

Элиминация кванторов

- Легче определить, выполнимы ли формулы без кванторов
- Элиминация кванторов[1] — это процесс преобразования формулы, содержащей кванторы, в эквивалентную бескванторную формулу
- Пример
  Пусть есть формула $\exists x : 3 \leqslant x \leqslant z$. Такой x найдётся, если $3 \leqslant z$ (например, $x = 3$)

[1] теория T допускает элиминацию кванторов, если для любой формулы этой теории ϕ существует формула ψ без кванторов, такая что $T \vDash \forall y.\phi(y) \leftrightarrow \psi(y)$

Обогащенная арифметика Пресбургера

- Операции над битовыми векторами можно свести к вычислениям в арифметике Пресбургера, обогащённой функцией 2^x: $< 0, 1, +, \leqslant, 2^x >$
- Доказательство того, что эта теория допускает элиминацию кванторов, а также алгоритм элиминации, сопутствующий построению доказательства, впервые были представлены А. Л. Семёновым

Постановка задачи

Целью данной работы является реализация элиминации кванторов для арифметики битовых векторов на основе элиминации кванторов в обогащённой арифметике Пресбургера

Задачи:

- Выбрать SMT-решатель
- Реализовать сведение формул над булевыми векторами к формулам в расширенной арифметике Пресбургера и наоборот
- Изучить алгоритм элиминации кванторов для расширенной арифметики Пресбургера и реализовать его в рамках выбранного SMT-решателя

Выбор SMT-решателя и формата ввода

- Существует несколько поддерживаемых, конкурентоспособных SMT-решателей, работающих с двоичными векторами: Boolector, Z3, CVC4 и другие
- Boolector специализируется на теории битовых векторов, а также в течение многих лет побеждал в ежегодном соревновании между SMT-солверами — The SMT Competition
- Из различных форматов ввода формул над битовыми векторами (Btor, Btor2, SMT-LIB, SMT-LIB v.2) выбран стандарт SMT-LIB v.2

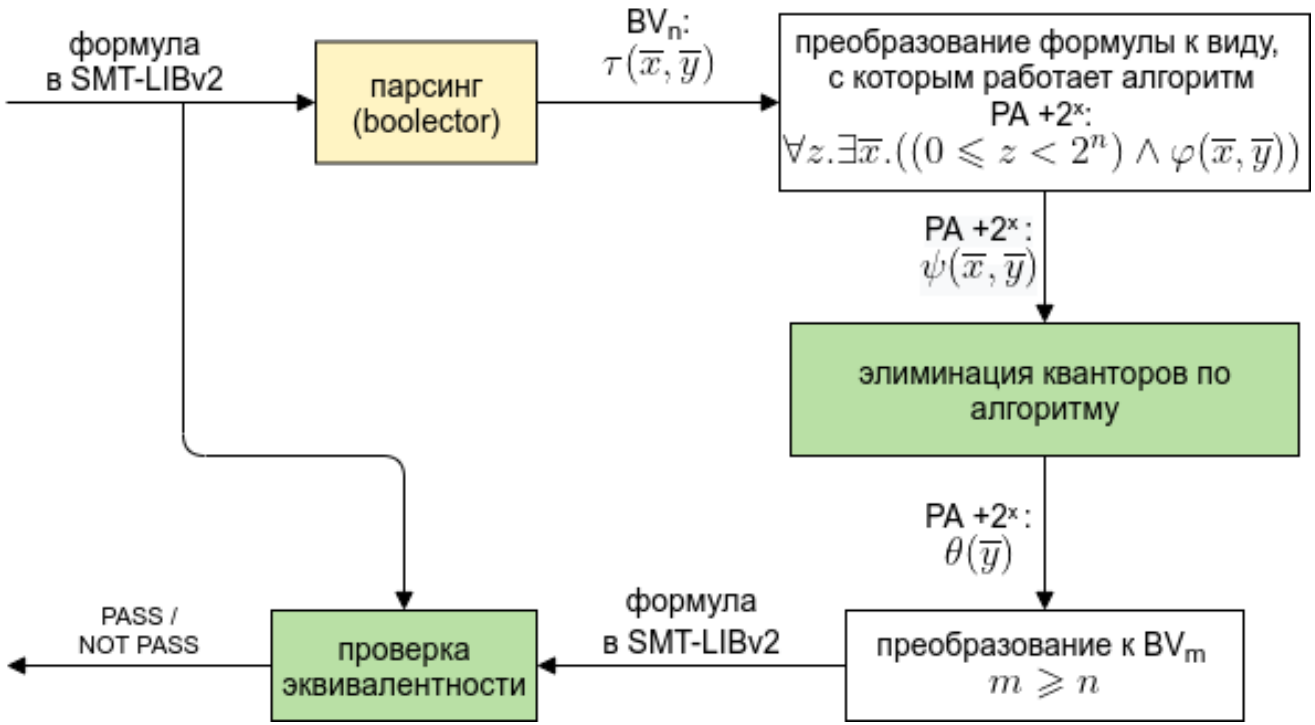
Сравнение теорий

Обогащенная арифметика Пресбургера	Теория битовых векторов (синтаксис SMT-LIB)
Носитель: $\mathbb{N}$	Носитель: битовые векторы фикс. размеров (_ BitVec n)
$t_1 \leqslant t_2$	bvslte t_1 t_2 (bvulte t_1 t_2)
$t_1 + t_2$	bvadd t_1 t_2
2^t	bvshl 1 t
	bvand, bvor, bvnot, bvslt/bvult, bvsgt(e)/bvugt(e) и другие

По алгоритму А. Л. Семёнова можно проэлиминировать только ограниченное подмножество формул в арифметике битовых векторов без сведения к арифметике натуральных чисел

Реализация (1/2)

- Сведение формулы в теории битовых векторов размера n к формуле в обогащённой арифметике Пресбургера
- Элиминация кванторов по алгоритму
- Вывод результирующей формулы в теории битовых векторов размера $m \geqslant n$



Реализация (2/2)

Boolector:

- Си
- Парсер преобразует полученную формулу
- Формулы хранятся не в виде AST, а в стеке подвыражений

Идея проверки формул на эквивалентность:

- Пусть φ — исходная формула, а θ — результат, тогда $\varphi \oplus \theta$ должна быть невыполнима

Преобразование формул из BV_n в $PA + 2^x$

$$Tr(\varphi \wedge \psi) = Tr(\varphi) \wedge Tr(\psi)$$
$$Tr(\varphi \vee \psi) = Tr(\varphi) \vee Tr(\psi)$$
$$Tr(\varphi \to \psi) = Tr(\varphi) \to Tr(\psi)$$
$$Tr(\neg\varphi) = \neg Tr(\varphi)$$
$$Tr(t_1 \ op \ t_2) = (Tr(t_1) \ op \ Tr(t_2)) \ mod \ 2^n$$
$$Tr(x) = x$$

Текущие результаты

- Реализован алгоритм элиминации кванторов для следующих базовых формул (вместо $\leqslant$ может быть $<$ или $=$):
  1. $\exists x : \bigwedge_{i,j}(g_i(\overline{y}) \leqslant x \wedge x \leqslant g_j(\overline{y}))$, где $g_i(\overline{y}), g_j(\overline{y})$ — термы в арифметике битовых векторов, представляющие из себя линейные комбинации констант, свободных переменных($\overline{y}$) и сдвигов $1 \ll y$
  2. $\exists x : \bigwedge_{i}((1 \ll x) \leqslant g_i(\overline{y}))$
  3. Конъюнкции этих формул
- Реализована проверка эквивалентности исходной и результирующей формул

  https://github.com/AnzhelaSukhanova/QE_expPA