

Санкт-Петербургский Государственный Университет
Математико-механический факультет

Кафедра системного программирования

Программная инженерия

Суханова Анжела Кирилловна

Реализация элиминации кванторов для арифметики Пресбургера, обогащённой функцией возведения двойки в степень

Производственная практика

Научный руководитель:
ассистент кафедры ИАС Смирнов К. К.

Санкт-Петербург
2020

Оглавление

Введение	3
1. Постановка задачи	5
2. Теоретический обзор и описание реализации	6
2.1. Алгоритм элиминации кванторов для расширенной арифметики Пресбургера	6
2.2. Реализации случая линейного вхождения связанной переменной	7
2.3. Формат ввода формул	8
3. Текущие результаты	9
Список литературы	10

Введение

Современный этап развития индустрии программных систем характеризуется значительным усложнением процесса их разработки, что приводит к увеличению числа ошибок, возникающих при проектировании программного обеспечения. В таких условиях крайне важными оказываются проверка и доказательство корректности разрабатываемой программы, ведь они необходимы для контроля соответствия поведения программы ожидаемому и обеспечения её безопасности. Существуют разные методы, направленные на разработку качественного программного обеспечения, отвечающего поставленным требованиям: одним из них является формальная верификация.

Формальная верификация — это доказательство соответствия или несоответствия программы её формальному описанию или, что более распространено на практике, проверка формализованных условий, описывающих ожидаемое или недопустимое поведение программы (часто у разработчиков нет формального описания программы, но есть представление о ”запрещённых” состояниях, в которые она не должна попадать). В основу этой проверки нередко ложится решение задачи выполнимости формул в теориях¹ (SMT²), так как условия программы и ограничения, накладываемые на неё требованиями, могут быть сведены к определению выполнимости логических формул. Существуют SMT-решатели (SMT-солверы), автоматически определяющие выполнимость формулы в теориях. SMT-решатели используются инструментами формальной верификации, такими как [Frama-C](#), [BLAST](#), [Java Pathfinder](#) и другие.

Обычно легче определить, выполнима ли формула без кванторов, поэтому полезно уметь преобразовывать формулы, содержащие кванторы, в семантически эквивалентные бескванторные. Процесс такого преобразования называется элиминацией кванторов (*quantifier elimination*,

¹Теория — множество предложений (формул без свободных переменных).

²SMT — задача выполнимости формул в логике первого порядка, где функциональные и предикатные символы интерпретируются согласно конкретным теориям. В дальнейшем будет использоваться эта аббревиатура.

QE).

Так как в основе архитектуры компьютера лежат операции с битовыми векторами, то необходимо уметь решать SMT в теории битовых векторов, что вызывает интерес к упрощающим это решение алгоритмам исключения кванторов из формул над двоичными векторами. Операции над последними можно свести к вычислениям в арифметике Пресбургера³, обогащённой функцией 2^x . Доказательство того, что эта теория допускает элиминацию кванторов, а также алгоритм элиминации, сопутствующий построению доказательства, впервые были представлены А. Л. Семёновым [6], а затем более подробно описаны в других работах [4, 5]. Однако реализации данного алгоритма пока нет, чему и посвящена эта работа.

В настоящее время существует несколько поддерживаемых, конкурентоспособных SMT-решателей, работающих с двоичными векторами: [Boolector](#), [Z3](#), [CVC4](#) и другие. В рамках этой курсовой будет осуществляться работа с Boolector, так как он специализируется на теории битовых векторов, а также в течение многих лет побеждал в The SMT Competition⁴ (за исключением 2020-го года, в котором актуальная версия Boolector-а не принимала участие в соревновании).

³Арифметика Пресбургера — это теория первого порядка, описывающая натуральные числа со сложением и названная в честь предложившего её Мойжеша Пресбургера.

⁴The SMT Competition или SMT-COMP — ежегодное соревнование между SMT-солверами:
<https://smt-comp.github.io/2020/index.html>

1. Постановка задачи

Целью данной работы является реализация элиминации кванторов для арифметики Пресбургера, расширенной функцией возведения двойки в степень⁵. Для её достижения были поставлены следующие задачи.

- Изучение алгоритма элиминации кванторов для расширенной арифметики Пресбургера.
- Реализация изученного алгоритма.
- Внедрение реализаций в SMT-решатель Boolector.

⁵Далее она иногда будет упоминаться как "расширенная арифметика Пресбургера", но имеется в виду, что теория расширяется функцией 2^x .

2. Теоретический обзор и описание реализации

2.1. Алгоритм элиминации кванторов для расширенной арифметики Пресбургера

Заметим, что формулу, содержащую квантор всеобщности, $\forall x F$ можно заменить эквивалентной ей формулой $\neg \exists x \neg F$, а все кванторы существования можно элиминировать последовательно от самого внутреннего к внешнему. Также любая формула первого порядка может быть представлена в конъюнктивной нормальной форме. Таким образом, алгоритм элиминации сводится к устранению квантора существования из формулы вида $\exists x \theta(x, \bar{y})$, где \bar{y} — свободные переменные, а сама функция $\theta(x, \bar{y})$ — конъюнкт литералов. Это устранение квантора будет построено по материалу, изложенному в [5] (обозначения также будут согласованы с этой работой).

Первым шагом в элиминации кванторов для рассматриваемой арифметики является преобразование формулы под квантором в дизъюнкт конъюнктов неравенств между термами следующего вида:

- $\sum_{i=0}^n a_i * 2^{d * x_i} + \sum_{i=0}^n b_i * x_i + c$, где $a_i, b_i, c \in \mathbb{Z}$, $d \in \mathbb{N}$, а x_i — связанные переменные, причём x_0 — обозначение x (будем называть их S -термами);
- термы сигнатуры арифметики Пресбургера, обогащённой функцией возведения двойки в степень, без связанных переменных (будем называть их L -термами).

Это преобразование осуществляется посредством введения новых переменных, связанных кванторами существования — отсюда и возникают x_i (подробнее об этом шаге можно прочитать в [5]).

Существует два варианта вида преобразованной формулы.

- x появляется во всех неравенствах линейно. Тогда можно считать, что формула под кванторами выглядит следующим образом:

$\bigwedge_{1 \leq i \leq p, 1 \leq j \leq q, 1 \leq k \leq s} f_j(\bar{x}) + g_j(\bar{y}) \leq d_k * x \leq f_i(\bar{x}) + g_i(\bar{y})$,
где $d_k \in \mathbb{Z}$ и зависит от i и j , \bar{y} — свободные переменные, а $\bar{x} = (x_1, x_2, \dots, x_n)$, то есть $g_j(\bar{y})$, $g_i(\bar{y})$ — L -термы, а $f_j(\bar{x})$, $f_i(\bar{x})$ — S -термы.

- Хотя бы в одно неравенство x входит в экспоненциальном терме, то есть существует неравенство, имеющее вид:

$$a_0 * 2^{d*x_0} + \sum_{i=1}^n a_i * 2^{d*x_i} + \sum_{j=0}^n b_j * x_j + c \leq t(\bar{y}), \quad t(\bar{y}) \text{ — } L\text{-терм, } a_i, b_i, c \in \mathbb{Z}, a_0 \neq 0, d \in \mathbb{N}^*.$$

Таким образом, реализация подразумевает разбор двух случаев: линейного и экспоненциального вхождения x .

2.2. Реализации случая линейного вхождения связанной переменной

Работа над этим случаем была начата с упрощённого варианта, а именно с элиминации кванторов для формул с единственной связанной переменной: $\exists x \bigwedge_{1 \leq i \leq p, 1 \leq j \leq q, 1 \leq k \leq s} g_j(\bar{y}) \leq d_k * x \leq +g_i(\bar{y})$.

При $d_k = 1 \ \forall k$ искомая формула без квантора — $\bigvee_{\rho \in S_p} \bigvee_{\tau \in S_q} g_{\tau(q)}(\bar{y}) \leq \dots \leq g_{\tau(1)}(\bar{y}) \leq g_{\rho(1)}(\bar{y}) \leq \dots \leq g_{\rho(p)}(\bar{y})$, где S_p — группа перестановок элементов множества $\{0, \dots, p-1\}$, а S_q — группа перестановок элементов множества $\{0, \dots, q-1\}$.

Если существует $d_k \neq 1$, то ситуация усложняется. По алгоритму все неравенства домножаются так, чтобы x встречался в них с одинаковым коэффициентом d (d — НОК всех d_k). Однако в отличие от арифметики Пресбургера, позволяющей работать с натуральными числами без ограничения сверху, арифметика битовых векторов работает с векторами фиксированного размера, то есть накладывает ограничение на значения переменных и величину констант, а также поддерживает переполнение. Из-за этого результирующая формула, полученная по алгоритму, может быть не эквивалентна исходной. Решение этого затруднения пока не найдено.

2.3. Формат ввода формул

Изначально в качестве формата ввода рассматривались стандарты Btor [2] и Btor2 [3]. Оба формата не поддерживают работу с кванторами, и хотя это неудобство может быть преодолено (например, договорённостью, что первые введённые переменные связаны кванторами существования), было принято решение работать со стандартом SMT-LIB v.2 [1], в котором можно записывать формулы с кванторами. Парсеры всех вышеупомянутых стандартов записи встроены в Boolector.

Работая с Boolector-ом, можно задать любую формулу над битовыми векторами (даже с кванторами) программно, используя функции решателя, но такой ввод не очень удобен. К тому же важно, чтобы программа могла работать с общепринятым, распространённым форматом, ведь в нём записывались и пишутся условия и ограничения, накладываемые на реальное программное обеспечение. Идея написать собственный парсер выражений над битовыми векторами также была отброшена из-за неоправданной трудоёмкости.

3. Текущие результаты

- Изучен описанный в [5] алгоритм элиминации кванторов для расширенной арифметики Пресбургера.
- Изучен исходный код Boolector-a.
- Рассмотрены различные форматы ввода формул над битовыми векторами (Btor, Btor2, SMT-LIB, SMT-LIB v.2), и, как следствие, выбран один из них, а именно стандарт SMT-LIB v.2.
- Реализована элиминация кванторов для формул вида
$$\bigwedge_{1 \leq i \leq p, 1 \leq j \leq q} g_j(\bar{y}) \leq x \leq g_i(\bar{y}),$$
где $g_j(\bar{y})$, $g_i(\bar{y})$ — линейные комбинации свободных переменных \bar{y} .
- Начата реализация алгоритма для случая, когда связанная переменная встречается в экспоненциальном терме.

Список литературы

- [1] The SMT-LIB Standard: Version 2.0 : Rep. / Department of Computer Science, The University of Iowa ; Executor: Clark Barrett, Aaron Stump, Cesare Tinelli : 2010. — Available at www.SMT-LIB.org.
- [2] Brummayer Robert, Biere Armin, Lonsing Florian. [BTOR: Bit-Precise Modelling of Word-Level Problems for Model Checking](#) // Proceedings of the Joint Workshops of the 6th International Workshop on Satisfiability Modulo Theories and 1st International Workshop on Bit-Precise Reasoning. — SMT '08/BPR '08. — New York, NY, USA : Association for Computing Machinery, 2008. — P. 33–38. — Access mode: <https://doi.org/10.1145/1512464.1512472>.
- [3] Btor2 , BtorMC and Boolector 3.0 / Aina Niemetz, Mathias Preiner, Clifford Wolf, Armin Biere // Computer Aided Verification / Ed. by Hana Chockler, Georg Weissenbacher. — Cham : Springer International Publishing, 2018. — P. 587–595.
- [4] Cherlin Gregory, Point Françoise. On extensions of Presburger arithmetic // Proc. 4th Easter Model Theory conference, Gross Körös. — 1986. — P. 17–34.
- [5] Point Françoise. On the expansion $(\mathbb{N}, +, 2^x)$ of Presburger arithmetic. — 2007. — 01.
- [6] Semenov A. L. Logical theories of one-place functions on the set of natural numbers // Math. USSR, Izv. — 1984. — Vol. 22. — P. 587–618.