Степени двойки и вещественно-целочисленная линейная элиминация кванторов

И.Д Мишуров, студент СПбГУ, ilucha556@gmail.com

Аннотация

В докладе сделан обзор известных алгоритмов и подходов для элиминации кванторов, явного алгоритма элиминации кванторов для арифметики целых чисел с предикатом возведения двойки в степень, а так же доказаны теоремы о неразрешимости двух расширений арифметики Семёнова. Исследование нацелено на поиск алгоритмов элиминации кванторов, которые могут стать расширением пакета RedLog.

Введение

В современном мире арифметика Пресбургера нашла применение не только в математике, но и во многих прикладных областях [2]. Арифметика Пресбургера представляет собой элементарную теорию целых чисел с нулём, единицей, сложением и отношением порядка.

Уже долгое время ведутся исследования как самой арифметики, так и вопросов, связанных с различными ее расширениями. Большая часть исследований была посвящена проблемам сложности и разрешимости этой теории, а в дальнейшем и различных расширений этой теории.

Есть большое количество результатов, в которых доказывается и явно приводится алгоритм элиминации кванторов для различных структур. Обработка на компьютере формул, содержащих кванторы, требует больших затрат времени, так как каждый квантор рассматривается как цикл по всем значениям переменных, принимающих значения из предметной области. В связи с этим задача элиминации (удаления) кванторов той или иной теории является весьма актуальной в теоретической информатике. Множество из этих алгоритмов реализовано в системе Redlog [1].

Важной задачей является нахождение достаточно выразительных структур (в частности, расширений арифметики Пресбургера), для которых существует алгоритм элиминации кванторов. Такие алгоритмы затем могут быть внедрены в систему RedLog для отдельных классов формул, для которых применение элиминации кванторов оказывается достаточно эффективным. Такого рода чисто теоретические вопросы представляют неменьший интерес.

В статье [3] Ф.Пуан привела явный алгоритм элиминации кванторов для расширения арифметики Пресбургера $\langle \mathbb{N}, \leq, +, 2^x \rangle$. В этой же статье Ф.Пуан было показано что любая формула вида $\exists x \theta(x, \overline{y})$, где $\theta(x, \overline{y})$ – это конъюнкция атомарных формул, эквивалентна некоторой открытой формуле. Также, было показано что можно ограничить переменную x термом в $\overline{y}$.

Основные определения

В этом разделе будут даны основные определения и обозначения, а в дальнейшем будут получены некоторые утверждения о неразрешимости.

Определение 1. *Через L_σ обозначается язык первого порядка сигнатуры σ, а формула языка L_σ называется L-формулой.*

Определение 2. *Через $\exists L_\sigma$ будем обозначать экзичтенциальные формулы, а через $\forall L_\sigma$ - универсальные L_σ-формулы.*

Определение 3. *Множество всех замкнутых L-формул, истинных в структуре $\langle M; \sigma \rangle$, называеься L-теорией структуры $\langle M; \sigma \rangle$ и обозначается $L - Th\langle M; \sigma \rangle$.*

Определение 4. *$\exists L_\sigma$-выразимые в структуре $\langle M; \sigma \rangle$ отношения называются экзистенциально выразимыми в структуре $\langle M; \sigma \rangle$.*

Определение 5. *$Th\langle M; \sigma \rangle$ есть элементарная теория структуры $\langle M; \sigma \rangle$, а $\exists Th\langle M; \sigma \rangle$ экзистенциальная теория структуры $\langle M; \sigma \rangle$.*

Определение 6. *Алгоритмом элиминации кванторов для языка L_σ в структуре $\langle M; \sigma \rangle$ называется алгоритм, который по всякой L_σ-формуле вида $\exists x \phi(x, y_1, ..., y_n)$, где $\phi(x, y_1, ..., y_n)$ бескванторная L_σ-формула, строит эквивалентную ей в этой структуре бескванторную L_σ-формулу $\psi(y_1, ..., y_n)$.*

Алгоритм элиминации кванторов позволяет построить по всякой L_σ-формуле эквивалентную в соответствующей структуре бескванторную L_σ-формулу.

Неразрешимость некоторых расширений арифметики Семёнова

С прикладной точки зрения полезно иметь достаточно выразительные структуры с алгоритмом элиминации кванторов. Однако, в действительности, не для всех интересующих нас теорий такой алгоритм существует. В рамках данной работы были доказаны две теоремы о неразрешимости экзистенциальных теорий структур $\langle \mathbb{N}, 0, 1, +, 2^x, | \rangle$ и $\langle \mathbb{R}, 0, 1, +, -, 2^x, =, <, Z \rangle$.

Напомним, что $|$ есть двуместный предикат делимости целых чисел, а Z соответствует свойству "быть целым числом".

Расширение предикатом делимости

Определение 7. *Заданный на натуральных числах двухместный предикат T является предикатом степенного роста, если существуют положительные рациональные числа c, d, c_1, d_1, такие что $d_1 > 1$ и*

1. *Каковы бы ни были натуральные числа x, y, если имеет место $T(x, y)$ и $x > 0$, то $y \leq cx^d$*

2. *для всякого натурального числа x существует натуральное число y, такое, что имеют место $y \geq c_1 x^{d_1}$ и $T(x, y)$.*

Теорема 1 ([4]). *Пусть есть структура $\langle \mathbb{N}; 0, 1, +, |, T \rangle$, где T - предикат степенного роста. Тогда в этой структуре выразимо умножение.*

Теорема 2. *Экзистенциальная теория структуры $\langle \mathbb{N}; 0, 1, +, 2^x, | \rangle$ неразрешима.*

Доказательство. Для доказательства данного утверждения воспользуемся результатами из работы Н.К.Косовского [4].

В данной структуре выразим предикат равенства, а именно $y = x \iff y|x \wedge x|y$, полагая что верно $0|0$.

Выразим в структуре предикат, обозначающий длину записи числа, обычно определяемый как:

$$||x|| = \begin{cases} 1 & \text{если } x = 0 \\ [log x] + 1 & \text{если } x > 0 \end{cases}$$

В структуре $\langle \mathbb{N}; 0, 1, +, 2^x, | \rangle$ выразим формально данный предикат $||y|| \leq 3||x||$:

1. $y \leq x \iff \exists z(x = y + z)$
2. $y < x \iff y \leq x \wedge \neg(y = x)$
3. $y = ||x|| \iff \exists z(2^y > x \geq 2^z \wedge z + 1 = y)$
4. $||y|| \leq 3||x|| \iff \exists t_1 \exists t_2 (t_1 = ||y|| \wedge t_2 = ||x|| \wedge t_1 \leq 3t_2)$

По определению, предикат $||y|| \leq 3||x||$ является предикатом степенного роста. Для доказательства этого достаточно взять в определении 7 значения $c = 2^3, d = 1, c_1 = 2^{-3}, d_1 = 1$. Из теоремы 1 тогда следует что данная структура содержит в себе арифметику натуральных чисел со сложением и умножением. Из неразрешимости десятой проблемы Гильберта [5] следует что такая структура неразрешима.

Расширение предикатом быть целым

Рассмотрим ещё одно расширение арифментики Семёнова. Несложно показать, что если дополнить структуру из теоремы В.Вайспфеннинга функцией 2^x, то это позволит выразить в ней умножение с помощью экзистенциальной формулы, что приведёт к неразрешимости уже экзистенциальной теории этой структуры.

Теорема 3. *Экзистенциальная теория структуры* $\langle \mathbb{R}, Z, 0, 1, +, -, 2^x, =, < \rangle$, *где* Z *— одноместный предикатный символ, который интерпретируется с помощью свойства «быть целым числом», неразрешима.*

Доказательство. Для доказательства утверждения сначала заметим, что для всякого положительного целого y имеет место $\exists x(y = 2^x)$, где x является вещественной переменной. Теперь несложно видеть, что можно выразить умножение натуральных чисел следующим образом

$$z = x \cdot y \ \wedge \ x > 0 \ \wedge \ y > 0 \ \wedge \ Z(z) \ \wedge \ Z(x) \ \wedge \ Z(y) \Leftrightarrow$$
$$\exists u \exists v \, (z = 2^{u+v} \ \wedge \ x = 2^u \ \wedge \ y = 2^v) \ \wedge \ Z(z) \ \wedge \ Z(x) \ \wedge \ Z(y)$$

Таким образом, ввиду того, что в сигнатуре имеется унарный минус, в данной структуре экзистенциально выразим график функции умножения. Для этого достаточно рассмотреть различные знаки переменных x, y, z. Тогда данная структура содержит в себе арифметику натуральных чисел со сложенем и умножением. Из неразрешимости десятой проблемы Гильберта [5] следует что такая структура неразрешима.

Заключение

В рамках данной работы были доказаны две теоремы о неразрешимости экзистенциальных теорий структур $\langle \mathbb{N}, 0, 1, +, 2^x, | \rangle$ и $\langle \mathbb{R}, 0, 1, +, -, 2^x, =, <, Z \rangle$. Следовательно, для данных структур не существует алгоритмов элиминации кванторов. Эти результаты приводят к следующему вопросу. Пусть $2^{[]}$ — это функция возведения 2 в степень целой части числа, можно ли тогда построить алгоритм элиминации кванторов для $\langle \mathbb{R}, 0, 1, +, -, 2^{[x]}, =, <, Z \rangle$. Если ожидать положительного решения этого вопроса, то первой задачей является преобразование алгоритма Ф.Пуан [3] так, чтобы новый алгоритм элиминации кванторов работал со структурой $\langle \mathbb{Z}, =, +, 2^x \rangle$. Дальнейшие исследования планируется продолжать с решения этой задачи.

Список литературы

[1] Andreas Dolzmann, Thomas Sturm. Redlog: Computer algebra meets computer logic // SIGSAM Bull. — 1997. — Т. 31 С. 2–9 https://doi.org/10.1145/261320.261324

[2] Christoph Haase. A survival guide to presburger arithmetic // ACM SIGLOG News. — 2018. — Т. 5 С. 67–82 https://doi.org/10.1145/3242953.3242964

[3] Francoise Poin.On the expansion (n,+, 2x) of presburger arithmetic // — 2007. — https://webusers.imj-prg.fr/ francoise.point/papiers/Pres.pdf

[4] Н. К. Косовский. О решении систем, состоящих одновременно из уравнений в словах и неравенств в длинах слов // Исследования по конструктивной математике и математической логике. VI, Зап. научн. сем. ЛОМИ. — 1974. — Т. 40 С. 24–29 http://mi.mathnet.ru/znsl2678

[5] Ю. В. Матиясевич. Диофантовость перечислимых множеств // Докл. АН СССР. — 1970. — Т. 191 С. 279–282 http://mi.mathnet.ru/dan35274