Санкт-Петербургский государственный университет

Мишуров Илья Дмитриевич

Выпускная квалификационная работа

Степени двойки и вещественно-целочисленная линейная элиминация кванторов

Уровень образования: бакалавриат

Направление *02.03.03 «Математическое обеспечение и администрирование информационных систем»*

Основная образовательная программа *СВ.5006.2018 «Математическое обеспечение и администрирование информационных систем»*

Профиль *Системное программирование*

Научный руководитель:
профессор кафедры информатики, д.ф.-м.н., Т.М. Косовская

Рецензент:
Программист ООО "ИнтеллиДжей Лабс" Д. С. Косарев

Санкт-Петербург
2022

Saint Petersburg State University

Mishurov Ilya

Bachelor's Thesis

Powers of two and real-integer linear quantifier elimination

Education level: bachelor

Speciality *02.03.03 "Software and Administration of Information Systems"*

Programme *CB.5006.2018 "Software and Administration of Information Systems"*

Profile: *Software Engineering*

Scientific supervisor:
Sc.D, prof. T.M.Kosovskaya

Reviewer:
Software Developer "IntelliJ Labs Co.Ltd" D. S. Kosarev

Saint Petersburg
2022

Оглавление

Введение

В современном мире арифметика Пресбургера нашла применение не только в математике, но и во многих прикладных областях [6]. 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. Вариациии алгоритма Д.Купера [4] дают эффективные на практике алгоритмы элиминации кванторов для этой теории. Позже В.Вайспфеннинг [17] предложил эффективные методы элиминации кванторов для арифметики вещественных чисел со сложением и отношением порядка.

Следуя А.Семёнову и С.Сопрунову [22], определим структуру сигнатуры σ как тройку $\langle D; \sigma, Int \rangle$. Здесь D – это множество (в данной работе это будут множества $\mathbb{N}, \mathbb{Z}, \mathbb{R}$), называемое универсумом (или областью) структуры, Int – это интерпретация, которая каждое n-местное имя отношения из σ отображает в n-арное отношение на D, другими словами — в подмножество D^n, а каждое n-местное имя функции — в функцию из D^n в D. Так как в дальнейшем интерпретация Int будет обычно ясна из контекста, будем записывать просто $\langle D; \sigma \rangle$.

Алгоритм элиминации кванторов для некоторой структуры можно опредеделить следующим образом. Рассмотрим язык первого порядка L_σ некоторой сигнатуры σ, и пусть задана некоторая структура $\langle D; \sigma \rangle$ сигнатуры σ. Алгоритм элиминации кванторов для $\langle D; \sigma \rangle$ – это такой конечный алгоритм, который для любой формулы ϕ языка L_σ предоставляет бескванторную формулу ϕ' этого же языка, такую что формулы ϕ и ϕ' эквивалентны в структуре $\langle D; \sigma \rangle$ и формула ϕ' не содержит связанных переменных.

Есть большое количество результатов, в которых доказывается и явно приводится алгоритм элиминации кванторов для различных структур. Множество из этих алгоритмов реализовано в системе Redlog [5].

Разработка Redlog [5] была начата в 1992 году А. Дольцманом и

Т.Штурмом. Данная система является расширением системы компьютерной алгебры REDUCE [13] и содержит в себе множество эффективных алгоритмов элиминации кванторов для различных теорий. Система REDUCE нашла широкое применение в научных вычислениях, физике, инженерных науках и других областях.

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. Очевидно, что чем более выразителен язык, тем труднее с вычислительной точки зрения окажется алгоритм, и тем чаще в случае произвольных формул соответствующей сигнатуры мы будем сталкиваться с алгоритмичсеки неразрешимыми проблемами. Такого рода чисто теоретические вопросы представляют неменьший интерес.

1. Постановка задачи

Целью данной работы является исследование применимости некоторых алгоритмов элиминации кванторов к теориям, имеющим потенциал практического применения, для которых такой алгоритм еще не известен. Для успешного достижения данной цели были поставлены следующие задачи:

- Исследование известных алгоритмов и подходов для элиминации кванторов, а так же способов доказательства отсутствия таковых алгоритмов для некоторых структур.
- Исследование явного алгоритма для структуры $\langle \mathbb{N}; +, 2^x \rangle$ и преобразование его в алгоритм элиминации кванторов для структуры $\langle \mathbb{Z}; +, 2^x \rangle$.
- Исследование разрешимости экзистенциальной теории структур $\langle \mathbb{N}; 0, 1, +, 2^x, | \rangle$ и $\langle \mathbb{R}; 0, 1, +, -, 2^x, =, <, Z \rangle$, где $|$ соответствует отношению делимости, а Z — одноместный функциональный символ, который интерпретируется с помощью свойства «быть целым числом».

2. Обзор

Элиминация кванторов для арифметики Пресбургера — важнейший инструмент формальной верификации, а также теории автоматов, теории моделей и дискретной геометрии [6]. Но даже довольно простые расширения арифметики Пресбургера неразрешимы. Например, арифметика Пресбургера с умножением, что доказал А.Чёрч в 1936 году [3]. Поэтому для доказательства неразрешимости расширений арифметики Пресбургера достаточно выразить в этом расширении график функции умножения.

Однако во второй половине XX века в ряде работ был представлен алгоритм элиминации кванторов для различных расширений арифметики Пресбургера, из чего следовала разрешимость этих расширений. Во многом этой темой занимался Т.Штурм, например, в работах [10, 8]. А также А.Лазарук в работах [9, 8]. Представленные там алгоритмы сейчас активно используются в системе Redlog [5]. Сейчас исследования различных расширений арифметики Пресбургера продолжаются, например [2]. В данной главе будет произведен обзор важных результатов, а также современных исследований на данную тему.

2.1. Элиминация для структур с вещественными числами

Для некоторых приложений удобно иметь в качестве носителя множество вещественных чисел. Существует несколько алгоритмов реализующих элиминацию кванторов для структур, носителем которых является множество вещественных чисел. В системе Redlog [5] реализованы следующие из них:

- Partial CAD [16]

  Дважды экпоненциальный по числу переменных

  Обычно применяется на практике

  Дает достаточно простые результаты

- Virtual Substitution [17]

  Дважды экпоненциальный по числу изменений квантора

  Ограничивается формулами с полиномами низкой степени

  Производит большое количество атомарных формул

- Hermitian Quantifier Elimination [11]

  Не примитивно рекурсивный

  Нацелен на формулы со многими уравнениями

  Производит огромные многочлены с огромными коэффициентами

В 1999 году В.Вайспфеннинг предложил алгоритм Mixed Real-Integer Quantifier Elimination [18] который реализует алгоритм элиминации кванторов для $\mathrm{Th}\langle\mathbb{R}, 0, 1, +, -, [], =, <, mod_n\rangle$. В частности, данный алгоритм реализует линейную подстановку для элиминации арифметики Пресбургера, т.е. реализует элиминацию кванторов для линейных случаев. Данный алгоритм был также реализован в системе Redlog [5]. Однако, для многих проблем этих средств бывает недостаточно, например, в тех случаях, когда хочется иметь утверждения о битовых векторах. Здесь было бы полезно использовать побитовое отрицание, умножение и сравнение битовых длин. Для решения такого рода задач полезно рассмотреть расширение арифметики Пресбургера.

2.2. Арифметика Бюхи

В последнее время активно ведутся исследования арифметики Бюхи [7], которая представляет собой теорию первого порядка структуры $\langle\mathbb{N}, 0, 1, +, V_p\rangle$, то есть является расширением арифметики Пресбургера с помощью предиката V_p. По определению, V_p есть двухместное отношение, такое что $V_p(x, u)$ принимает значение $true$ тогда и только тогда, когда u является наибольшей степенью p, делящей x без остатка.

Представляя числа как битовые вектора, в этой арифметике появляется возможность выразить побитовые операции над целыми числами,

представленными в системе счисления по основанию p. Например, для $p = 2$ несложно выразить графики функций, осуществляющих побитовые операции «и»/«или».

Известно, что арифметику Бюхи можно разрешить используя конечные автоматы [1]. Однако для данной теории нет алгоритма элиминации кванторов [6], в связи с чем она редко применима на практике и не реализована в Redlog [5]. В своем обзоре [6] Haase говорил про этот метод так: “Насколько известно автору, подход, основанный на автоматах, в наши дни широко не применяется на практике”

2.3. Арифметика Семёнова

В своих работах [14, 15] А.Л. Семёнов рассматривал вопрос разрешимости некоторых расширений арифметики Пресбургера. Так, он доказал что элементарная теория структуры $\langle \mathbb{N}, +, 2^x \rangle$ разрешима и для некоторого расширения этой структуры существует алгоритм элиминации кванторов [15].

Детально алгоритм элиминации кванторов для этой теории был представлен в работе Ф.Пуан [12] в 2007 году. Однако, если расширить данную структуру предикатом из арифметики Бюхи $\langle \mathbb{N}, +, V_2, 2^x \rangle$, то элементарная теория такой структуры окажется неразрешимой [12]. Так же, с помощью одной теоремы Н.К. Косовского [19] можно доказать неразрешимость экзистенциальной теории структуры $\langle \mathbb{N}; 0, 1, +, 2^x, | \rangle$

3. Основные определения

В введении мы ввели понятие структуры и алгоритма элиминации квонторов. В данной главе будут даны основные определения и обозначения, а в дальнейших главах будут получены некоторые утверждения о неразрешимости.

Определение. *Обозначим через L_σ язык первого порядка сигнатуры σ, а формулу языка $L \subseteq L_\sigma$ будем называть L-формулой.*

Определение. *Пренексной L_σ-формулой называется формула вида*

$Q_1 y_1 ... Q_m y_m \ \varphi(x_1, ..., x_n, y_1, ..., y_m)$, где $\varphi(x_1, ..., x_n, y_1, ..., y_m)$ бескванторная L_σ-формула, а Q_i —кванторы.

Если объединить одинаковые кванторы в блоки, то формулы с единственным блоком определяют язык $\exists L_\sigma$, если это кванторы существования, и $\forall L_\sigma$, если это кванторы всеобщности.

Определение. *$\exists L_\sigma$-формулы называются экзистенциальными, а $\forall L_\sigma$-формулы универсальными L_σ-формулами.*

Определение. *Бескванторную формулу будем называть позитивной, если она построена из атомарных формул и логических связок конъюнкции и дизъюнкции.*

Определение. *Для всякого языка $L \subseteq L_\sigma$ назовем отношение*

L-выразимым в структуре $\langle M; \sigma \rangle$, если оно выразимо в $\langle M; \sigma \rangle$ некоторой L -формулой.

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

Если из контекста ясно, о какой структуре идет речь, будем говорить просто об L-выразимости и L-теории. В том случае, когда $L = L_\sigma$, в определениях из предыдущего абзаца символ L можно опустить.

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

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

Определение. *Алгоритмом элиминации кванторов для языка L_σ в структуре $\langle M;\sigma\rangle$ называется алгоритм, который по всякой L_σ-формуле вида $\exists x\varphi(x,y_1,...,y_n)$, где $\varphi(x,y_1,...,y_n)$ 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.

4. Алгоритм элиминации кванторов для расширенной арифметики Пресбургера

В статье [12] Ф.Пуан привела явный алгоритм элиминации кванторов для расширения арифметики Пресбургера $\langle \mathbb{N}, +, 2^x \rangle$. В данной главе будет представлен обзор основных идей этого алгоритма.

Будем считать что все атомарные формулы имеют вид $a \leq b$, где a и b – термы сигнатуры $\langle \mathbb{N}, +, 2^x \rangle$ без связанных переменных.

Будет 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, будет показано что можно ограничить переменную x термом в $\overline{y}$.

Для описания алгоритма понадобятся некоторые обоначения. Если x это переменная, то $n.x$, где $n \in \mathbb{N}^*$, значит $x + ... + x$ (n раз). Так же введем обозначение $z.x$, где $z \in \mathbb{Z} - \{0\}$. В атомарных формулах вида $a + z.x \leq b$, если $z < 0$ это будет обозначать $a \leq b + (-z).x$.

Первым шагом алгоритма является приведение изначальной формулы к виду $\exists \overline{x} \theta_0(\overline{x}, \overline{y})$, где $\theta_0(\overline{x}, \overline{y})$ есть дизъюнкция конъюнкций неравенств между термами следующих двух видов:

1. $\sum_i a_i.2^{c.x_i} + \sum_j^n b_j.x_j + d$, где $a_i, b_j, d \in \mathbb{Z}, c \in \mathbb{N}$, а x_i – связанные переменные, причем x_0 – обозначение x (будем называть их S-термами)

2. термы сигнатуры $\langle \mathbb{N}, +, 2^x \rangle$, без связанных переменных (будем называть их L-термами)

Для этого все нетривиальные вхождения x в термы $t(x, \overline{y})$ заменяются на эквивалентные. В процессе этого преобразования в некоторых случаях вводятся новые переменные. Подробные правила преобраования описаны в [12].

Пусть на этом шаге были введены n новых переменных $\overline{x} : (x_1, ..., x_n)$. Обозначим S_{n+1} группу перестановок на $\{0, 1, ..., n\}$, и $\sigma \in S_{n+1}$.

Определим $\chi_\sigma(x,\overline{x}) := x_{\sigma(0)} \leq ... \leq x_{\sigma(n)}$ и $\theta_{0,\sigma}(x,\overline{x}) := \chi(x,\overline{x})\&\theta_0(x,\overline{x},\overline{y})$. Тогда можно элиминировать квантор в формуле $\exists x_\sigma(n)\theta_{0,\sigma}(x,\overline{x},\overline{y})$, так как эта задача эквивалентна исходной. Далее будет показано, что можно ограничить переменную x произведением $2^{2^{\cdots^{t(\overline{y})}}}$, где $t(\overline{y})$ терм в θ, а число итераций экспоненты равно n и зависит только от коэффициентов перед переменной x и от постоянных членов, входящих в θ.

Для следующего шага необходимо привести $\theta_{0,\sigma}$ к дизъюнктивной нормальной форме, а так же переобозначить $x_{\sigma(n)}$ в x_0, $\theta_{i,0,\sigma}$ в θ_0 и $(x_{\sigma(0)},\ldots,x_{\sigma(n)})$ в $\overline{x}$.

Теперь возможны два случая вхождения связанной переменной x_0: переменная входит в формулу либо линейно, либо экспоненциально.

4.1. Случай линейного вхождения переменной

В данном разделе представлен случай когда переменная x_0 появляется линейно в каждом неравенстве в θ_0. Можно считать, что система неравенств тогда имеет вид:

$$\bigwedge_{1\leq i\leq p,1\leq j\leq q,1\leq k\leq s} f_j(\overline{x}) + g_j(\overline{y}) \leq d_k x_0 \leq f_i(\overline{x}) + g_i(\overline{y})$$

где $f_i(\overline{x}), f_j(\overline{x})$ это S термы, $g_i(\overline{y}), g_j(\overline{y})$ это L термы, $d_k \in \mathbb{Z}$ и зависит от i и j. Пусть d есть наибольшее общее кратное всех d_k. Представим d в виде $d = 2^r.d_0$, где $d_0, r \in \mathbb{N}$, а d_0 нечётное натуральное число. Далее, домножим неравенства так чтобы d был коэфициентом x_0. Тогда для каждого x_i справедливо что:

$$\bigvee_{0\leq k_i\leq d.\varphi(d_0)}(x_i \geq r \& x_i - r = k_i + d.\varphi(d_0).x_i')$$

или

$$\bigvee_{0\leq z\leq r}(x_i = z)$$

Где $\varphi(x)$ – функция Эйлера. Тогда можно заменить каждое неравенство на дизъюнкцию неравенств где произведена замена x_i на $r + k_i + d.\varphi(d_0).x'_i$ или на z где $0 \leq z \leq r$.

Путем таких замен мы получаем дизъюнкцию систем неравенств содержащую ограниченные переменные, которая эквивалентна формуле:

$$\exists x_0 \bigwedge_{1\leq i\leq p, 1\leq j\leq q, 1\leq k\leq s} f_j(\overline{x}) + g_j(\overline{y}) \leq d_k x_0 \leq f_i(\overline{x}) + g_i(\overline{y})$$

Тогда переменную $x_{\sigma(n)}$ можно ограничить с помощью $\frac{1}{d}.max_\rho\{f_{\rho(1)\in S_p}(x_{\sigma(0)}, \ldots, x_{\sigma(n-1)}) + g_{\rho(1)}(\overline{y})\}$. Затем процедура повторяется, рассматривается следующая по вложенности экзистенциальная переменная и применяется случай линейного или экспоненциального вхождения переменной, который будет описан далее. Будет показано, что в случае экспоненциального вхождения переменной можно ограничить переменную либо термом вида $l_2(t(\overline{y})) + 1$, где $t(\overline{y})$ это подтерм, входящий в θ, а $l_2(a) = b \iff 2^b \leq a \leq 2^{b+1}$. Либо $max\{x_i + \alpha, \beta\}$ для некоторого $1 \leq i \leq n$, где α и β — некоторые явные константы, зависящие от коэффициентов, входящих в формулу θ_0. Таким образом, в конце мы получим явным образом терм в $\overline{y}$, ограничивающий x.

4.2. Случай экспоненциального вхождения переменной

В данном разделе рассматривается случай когда x_0 хотя бы в одном неравенстве входит в экспоненциальный терм. Рассмотрим такое неравенство:

$$\mathrm{a}_0.2^{d.x_0} + \sum_i^n a_i.2^{d.x_i} + \sum_j^n b_j.x_j + c \leq t(\overline{y})$$

где $t(\overline{y})$ это L терм, $d \in \mathbb{N}^*$, $a_i, b_j, c \in \mathbb{Z}$, $a_0 \neq 0$. Обозначим это неравенство за $\tau(x_0, \overline{x}, \overline{y})$. Алгоритм заключается в замене τ на L термы в $\overline{y}$ и булеву комбинацию неравенств между S-термами с $x_0, \ldots, x_n$, где x_0

встречается линейно. Для ограничения переменной x вводятся дополнительные переменные, зависящие от коэффициентов в представленном выше неравенстве. Переменная d полагается равной 1. Вводится множество $J := \{0, \ldots, n\}$. Пусть $J_1 := \{j \in J : b_j \geq 0\}$.

Если $J_1 \neq \emptyset$, то $b_+ := 2.(l_2(\sum_{j \in J_1} b_j) + 3)$, а иначе $b_+ := 0$.

Если $J - J_1 \neq \emptyset$, то $b_- := 2.(l_2(\sum_{j \in J_1}(-b_j)) + 4)$, иначе $b_- := 0$.

Если $c > 0$, то вводится переменная $c_+ := l_2(c) + 3$ и переменная $c_- := 0$, иначе $c_+ := 0$, а $c_- := l_2(-c) + 4$.

Введем переменную $\delta := l_2(\sum_i |a_i|) + 3$.

Затем рассматриваются различные случаи в зависимости от значений введенный выше переменных. Строится эквивалентная формула, в которую x_0 входит линейно. В зависимости от значения a_0 переменная x_0 ограничивается разными термами.

Если $a_0 > 0$, то вводится значение $N := max\{b_+, c_+, b_-, c_-\}$. Тогда можно ограничить преемменную x_0 либо значением $max\{N, l_2(t(\overline{y})) + 1 - l_2(a_0)\}$, где $t(\overline{y})$ есть подтерм в θ так что все переменные ограничены данным термом, либо значением $x_i + \delta$ для некоторого $1 \leq i \leq n$.

Если $a_0 < 0$, то вводится значение $N' := max\{b_+, c_+\}$ и значение $\delta' := l_2(\sum_i |a_i|) + 2 - l_2(-a_0)$. Тогда переменную x_0 можно ограничить либо значением N' и все переменные будут ограничены данным термом, либо значением $x_i + \delta'$ для некоторого $1 \leq i \leq n$.

5. Неразрешимость некоторых расширений арифметики Семёнова

Важной теоретиечской задачей является вопрос разрешимости теорий, т.к. иначе в них не может быть построен алгоритм элиминации кванторов. 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". Покажем, что два расширения арифметки Семёнова этими предикатами неразрешимы уже в случае только экзистенциальных формул.

5.1. Расширение предикатом делимости

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

Доказательство. Для доказательства данного утверждения воспользуемся результатами из работы Н.К.Косовского [19].

Определение. *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* $T(x, y)$.

Теперь пусть есть структура $\langle \mathbb{N}, 0, 1, +, |, T \rangle$, где T - предикат степенного роста. По теореме Н.К.Косовского [19] в этой структуре выразимо умножение, из чего, ввиду неразрешимости десятой проблемы

Гильберта [20, 21], получим неразрешимость экзистенциальной теории рассматриваемой структуры.

Определим

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

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

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

По определению, предикат $|y| \leq 3|x|$ является предикатом степенного роста. Следовательно, экзистенциальная теория данной структуры неразрешима. □

5.2. Расширение предикатом "быть целым"

Теперь рассмотрим ещё одно расширение арифметики 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 2. *Экзистенциальная теория структуры* $\langle \mathbb{R}, 0, 1, +, -, 2^x, =, <, Z \rangle$ *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

$$\text{z=x*y} \wedge x > 0 \wedge y > 0 \wedge Z(z) \wedge Z(x) \wedge Z(y) \Leftrightarrow$$

$$\exists u \exists v \left(z = 2^{u+v} \wedge x = 2^u \wedge y = 2^v\right) \wedge Z(z) \wedge Z(x) \wedge Z(y)$$

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. Искомый результат теперь следует из неразрешимости десятой проблемы Гильберта [20, 21]. □

Это утверждение приводит 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 [12] так, чтобы новый алгоритм элиминации кванторов работал с структурой $\langle \mathbb{Z}, +, 2^x \rangle$.

Заключение

В ходе выполнения работы были выполнены следующие задачи:

1. Исследованы известные алгоритмы и подходы для элиминации кванторов
2. Исследован явный алгоритм элиминации кванторов для структуры $\langle \mathbb{N}, +, 2^x \rangle$.
3. Доказаны теоремы о неразрешимости некоторых расширений арифметики Семёнова.

Список литературы

[1] Boigelot Bernard, Wolper Pierre. Representing Arithmetic Constraints with Finite Automata: An Overview // ICLP. — 2002.

[2] Chistikov Dmitry, Haase Christoph, Mansutti Alessio. Quantifier elimination for counting extensions of Presburger arithmetic // Foundations of Software Science and Computation Structures / Ed. by Patricia Bouyer, Lutz Schröder. — Cham : Springer International Publishing, 2022. — P. 225–243.

[3] Church Alonzo. An Unsolvable Problem of Elementary Number Theory // American Journal of Mathematics. — 1936. — Vol. 58, no. 2. — P. 345–363. — URL: http://www.jstor.org/stable/2371045.

[4] Cooper D.C. Theorem proving in arithmetic without multiplication. In B. Meltzer and D. Michie, editors, Machine Intelligence, volume 7, pages 91–100. Edinburgh University Press,. — 1972. — 01. — URL: https://www21.in.tum.de/teaching/logik/SS16/Exercises/Cooper.pdf.

[5] Dolzmann Andreas, Sturm Thomas. REDLOG: Computer Algebra Meets Computer Logic // SIGSAM Bull. — 1997. — jun. — Vol. 31, no. 2. — P. 2–9. — URL: https://doi.org/10.1145/261320.261324.

[6] Haase Christoph. A Survival Guide to Presburger Arithmetic // ACM SIGLOG News. — 2018. — jul. — Vol. 5, no. 3. — P. 67–82. — URL: https://doi.org/10.1145/3242953.3242964.

[7] Haase Christoph. Approaching Arithmetic Theories with Finite-State Automata // Language and Automata Theory and Applications. — 2020. — Vol. 12038. — P. 33 – 43.

[8] Lasaruk Aless, Sturm Thomas. Weak Integer Quantifier Elimination beyond the Linear Case // Proceedings of the 10th International Conference on Computer Algebra in Scientific Computing. — CASC'07. — Berlin, Heidelberg : Springer-Verlag, 2007. — P. 275–294.

[9] Lasaruk Aless, Sturm Thomas. Weak quantifier elimination for the full linear theory of the integers // Applicable Algebra in Engineering, Communication and Computing. — 2007. — Vol. 18. — P. 545–574.

[10] Lasaruk Aless, Sturm Thomas. Effective Quantifier Elimination for Presburger Arithmetic with Infinity // Proceedings of the 11th International Workshop on Computer Algebra in Scientific Computing. — CASC '09. — Berlin, Heidelberg : Springer-Verlag, 2009. — P. 195–212. — URL: https://doi.org/10.1007/978-3-642-04103-7_18.

[11] Loos Rüdiger G. K., Weispfenning Volker. Applying Linear Quantifier Elimination // Comput. J. — 1993. — Vol. 36. — P. 450–462.

[12] Point Françoise. On the expansion (N,+, 2x) of Presburger arithmetic. — 2007. — 01. — URL: https://webusers.imj-prg.fr/~francoise.point/papiers/Pres.pdf.

[13] REDUCE. computer algebra system. — 2022. — URL: http://www.reduce-algebra.com/index.php (online; accessed: 15.02.2022).

[14] Semenov Aleksei L'vovich. ON CERTAIN EXTENSIONS OF THE ARITHMETIC OF ADDITION OF NATURAL NUMBERS // Mathematics of The Ussr-izvestiya. — 1980. — Vol. 15. — P. 401–418.

[15] Semënov A L. LOGICAL THEORIES OF ONE-PLACE FUNCTIONS ON THE SET OF NATURAL NUMBERS // Mathematics of The Ussr-izvestiya. — 1984. — Vol. 22. — P. 587–618.

[16] Sturm Thomas. Applied Effective Quantifier Elimination. — 2012. — 02.

[17] Weispfenning Volker. The Complexity of Linear Problems in Fields // J. Symb. Comput. — 1988. — Vol. 5. — P. 3–27.

[18] Weispfenning Volker. Mixed real-integer linear quantifier elimination // ISSAC '99. — 1999.

[19] Косовский Н. К. О решении систем, состоящих одновременно из уравнений в словах и неравенств в длинах слов. — Изд-во «Наука», Ленинград. отд., 1974. — Зап. научн. сем. ЛОМИ : http://mi.mathnet.ru/znsl2678.

[20] Матиясевич Ю. В. Диофантовость перечислимых множеств // Доклады Академии наук / Российская академия наук. — Vol. 191. — 1970. — P. 279–282.

[21] Матиясевич Ю. В. Десятая проблема Гильберта / Математическая логика и основания информатики. — 1993.

[22] Семенов А.Л. Сопрунов С.Ф. Решетка определимости. Источники и направления исследований. — 2021.