Вестник СПбГУ. Математика. Механика. Астрономия. 2021. Т. 8 (66). Вып. 3
УДК 510.53, 510.652
MSC 03C10, 03B80, 03B25, 11U05

Доказательство теоремы Бельтюкова — Липшица квазиэлиминацией кванторов. I. Определения и НОД-лемма

М. Р. Старчак

Санкт-Петербургский государственный университет,
Российская Федерация, 199034, Санкт-Петербург, Университетская наб., 7–9

Для цитирования: *Старчак М. Р.* Доказательство теоремы Бельтюкова — Липшица квазиэлиминацией кванторов. I. Определения и НОД-лемма // Вестник Санкт-Петербургского университета. Математика. Механика. Астрономия. 2021. Т. 8 (66). Вып. 3. С. 455–466. https://doi.org/10.21638/spbu01.2021.307

Данная работа является первой частью нового доказательства разрешимости экзистенциальной теории структуры $\langle \mathbb{Z}; 0, 1, +, -, \leq, | \rangle$, где $|$ соответствует двухместному отношению делимости. Разрешимость этой теории была доказана в 1976 г. независимо А. П. Бельтюковым и Л. Липшицем. В 1977 г. В. И. Мартьянов получил эквивалентный результат, рассматривая трехместный предикат НОД вместо отношения делимости (эти предикаты экзистенциально выражаются друг через друга с помощью других символов сигнатуры). В работе вводится понятие алгоритма квазиэлиминации кванторов (квази-ЭК), обобщающее в некотором смысле понятие алгоритма элиминации кванторов, а затем строится алгоритм квази-ЭК для позитивной экзистенциальной теории структуры $\langle \mathbb{Z}_{>0}; 1, \{a\cdot\}_{a\in\mathbb{Z}_{>0}}, \text{НОД} \rangle$. К проблеме разрешимости для этой теории сводится проблема разрешимости для экзистенциальной теории структуры $\langle \mathbb{Z}; 0, 1, +, -, \leq, \text{НОД} \rangle$. Алгоритм квази-ЭК, осуществляющий такое сведение, будет построен во второй части доказательства. Преобразования формул основаны на обобщении китайской теоремы об остатках для систем вида $\text{НОД}(a_i, b_i + x) = d_i$ для всех $i \in [1..m]$, где a_i, b_i, d_i — целые числа, такие что $a_i \neq 0$, $d_i > 0$.

Ключевые слова: элиминация кванторов, экзистенциальная теория, делимость, алгоритмическая разрешимость, китайская теорема об остатках.

1. Введение. Работа посвящена разработке нового метода доказательства следующей теоремы, доказанной в 1976 г. независимо А. П. Бельтюковым [1] и Л. Липшицем [2].

Теорема 1 (А. П. Бельтюков [1], Л. Липшиц [2])**.** *Экзистенциальная теория структуры* $\langle \mathbb{Z}; 0, 1, +, -, \leq, \text{НОД} \rangle$ *разрешима.*

В действительности А. П. Бельтюков и Л. Липшиц использовали отношение делимости целых чисел (предполагается, что $0 \mid 0$), а не график функции НОД, как в формулировке теоремы 1. Несложно видеть, что $x \mid y \Leftrightarrow \text{НОД}(x, y) = x \vee \text{НОД}(x, y) = -x$. И, наоборот, из алгоритма Евклида можно получить следующие экзистенциальные определения:

$$\text{НОД}(x, y) = z \;\Leftrightarrow\; 0 \leq z \wedge z \mid x \wedge z \mid y \wedge \exists u \, (x \mid u \wedge y \mid u + z),$$

$$\neg\text{НОД}(x,y)=z \;\Leftrightarrow\; z+1\le 0\vee\neg z \mid x\vee\neg z \mid y\vee\exists v\,(v \mid x\wedge v \mid y\wedge z+1\le v)\,.$$

Таким образом, вопросы разрешимости для экзистенциальных теорий структур $\langle\mathbb{Z};0,1,+,-,\le,|\rangle$ и $\langle\mathbb{Z};0,1,+,-,\le,\text{НОД}\rangle$ сводятся друг к другу. Отметим, что в 1977 г. доказательство теоремы 1 было также получено В. И. Мартьяновым [3].

В связи с теоремой 1 наиболее важными представляются следующие вопросы: какие предикаты экзистенциально выразимы в структуре $\langle\mathbb{Z};0,1,+,-,\le,|\rangle$ и какова алгоритмическая сложность проблемы разрешимости для соответствующей экзистенциальной теории?

Л. Липшицу [4] в 1981 г. удалось сделать некоторые продвижения в обоих направлениях. Он доказал, что для любого фиксированного n задача проверки истинности формул с n переменными при двоичном кодировании коэффициентов линейных полиномов принадлежит **NP**. Кроме того, задача оказывается NP-трудной уже при некотором фиксированном числе делимостей и переменных в формуле.

В той же работе [4] Л. Липшиц доказал, что каждое перечислимое множество выразимо в $\langle\mathbb{N};1,+,|\rangle$ некоторой формулой с кванторной приставкой $\exists\cdots\exists\forall$ ввиду того, что график возведения в квадрат выразим несложной универсальной формулой. Следовательно, неразрешимыми оказываются уже $\exists\forall$- и $\forall\exists$-теории структур $\langle\mathbb{N};1,+,|\rangle$ и $\langle\mathbb{Z};0,1,+,-,\le,|\rangle$.

А. Лечнер, Дж. Оакнин и Дж. Уоррелл в работе 2015 г. [5] внесли ряд усовершенствований в алгоритм Липшица, что позволило доказать принадлежность проблемы разрешимости для $\exists\mathrm{Th}\langle\mathbb{Z};0,1,+,-,\le,|\rangle$ классу **NEXPTIME**. Вопрос о временной сложности в общем случае остается открытым: задача NP-трудна и принадлежит классу **NEXPTIME**.

Известные доказательства разрешимости можно кратко описать следующим образом. Для данной формулы $\varpi(x_1,\ldots,x_n)$ строится дизъюнкция специального вида формул $\varpi_i(x_1,\ldots,x_n)$, выполнимая тогда и только тогда в $\mathbb{Z}$, когда выполнима $\varpi(x_1,\ldots,x_n)$ (*равновыполнимая с* $\varpi(x_1,\ldots,x_n)$ *в* $\mathbb{Z}$). Для каждой $\varpi_i(x_1,\ldots,x_n)$, исходя из вида этой формулы, можно построить константу ν_i такую, что $\varpi_i(x_1,\ldots,x_n)$ выполнима в целых числах тогда и только тогда, когда она выполнима в целых p-адических числах $\mathbb{Z}_p$ для любого простого числа $p\le\nu_i$. Разрешимость теперь следует из разрешимости $\exists\mathrm{Th}\langle\mathbb{Q}_p;1,+,-,=,\mathrm{div}\rangle$ для отношения $\alpha\ \mathrm{div}\ \beta\rightleftharpoons v_p(\alpha)\le v_p(\beta)$, где $v_p(x)$ есть p-показатель числа x. В этом случае достаточно использовать алгоритм элиминации кванторов, представленный В. Виспфеннингом [6]. Отметим, что в недавней работе Ф. Гепена, К. Хаасе и Дж. Уоррелла [7] с помощью методов теории p-автоматов была доказана принадлежность классу **NP** указанной экзистенциальной теории p-адических чисел.

В настоящей работе идеи элиминации кванторов используются для построения нового доказательства разрешимости $\exists\mathrm{Th}\langle\mathbb{Z};0,1,+,-,\le,|\rangle$. В разделе 2 вводится понятие алгоритма квазиэлиминации кванторов (квази-ЭК), которое в некотором смысле обобщает понятие алгоритма ЭК. Для доказательства теоремы 1 строятся алгоритмы квази-ЭК $\mathcal{R}$ и $\mathcal{D}$, первый из которых позволит получить следующий результат.

Теорема 2. *Проблема разрешимости для экзистенциальной теории структуры* $\langle\mathbb{Z};0,1,+,-,\le,\text{НОД}\rangle$ *сводится к проблеме разрешимости для позитивной экзистенциальной теории структуры* $\langle\mathbb{Z}_{>0};1,\{a\cdot\}_{a\in\mathbb{Z}_{>0}},\text{НОД}\rangle$, *где* $a\cdot$ *есть унарный функциональный символ для умножения на положительное целое число* a.

В разделе 4 с помощью алгоритма квази-ЭК $\mathcal{D}$ доказывается разрешимость последней теории. Построению более сложного алгоритма $\mathcal{R}$ будет посвящена вторая часть доказательства. В обоих алгоритмах основным инструментом квазиэлиминации является обобщение китайской теоремы об остатках на системы вида $\text{НОД}(a_i, b_i + x) = d_i$ для всех $i \in [1..m]$, где a_i, b_i, d_i — целые числа, такие что $a_i \neq 0$, $d_i > 0$. Критерий выполнимости таких систем, который будет назван НОД-леммой, доказан в разделе 3.

Из доказательства можно извлечь информацию о выразимости в некоторых подструктурах $\langle \mathbb{Z}; 0, 1, +, -, \leq, \text{НОД} \rangle$. Например, с помощью НОД-леммы несложно показать, что всякое отношение является позитивно экзистенциально выразимым в структуре $\langle \mathbb{Z}; 0, 1, +, -, \perp \rangle$ тогда и только тогда, когда оно является позитивно бесквантворно выразимым в структуре $\langle \mathbb{Z}; 0, 1, +, -, \neq, \perp, \text{НОД}_2, \text{НОД}_3, \ldots \rangle$. Здесь $\perp$ соответствует отношению взаимной простоты целых чисел: $x \perp y \rightleftharpoons \text{НОД}(x, y) = 1$. В качестве следствия получаем разрешимость одного фрагмента $\forall\exists\text{Th}\langle \mathbb{Z}; 0, 1, +, -, \leq, | \rangle$. К этим вопросам мы вернемся в заключительном разделе второй части доказательства.

Нетрудно получить из нашего алгоритма разрешающие процедуры для экзистенциальных теорий таких структур, как $\langle \mathbb{Z}; 0, 1, +, -, \leq, \perp \rangle$ или $\langle \mathbb{N}; 0, S, \text{НОД} \rangle$, где S соответствует функции следования $Sx = x + 1$. Это может помочь ответить на вопрос о принадлежности какой-либо из указанных теорий классу **NP**, что, в свою очередь, было бы полезно при изучении алгоритмической сложности $\exists\text{Th}\langle \mathbb{Z}; 0, 1, +, -, \leq, \text{НОД} \rangle$.

2. Алгоритмы квазиэлиминации кванторов. ***2.1. Основные определения.*** В формулировках утверждений будут использоваться следующие понятия.

Язык первого порядка сигнатуры σ будет обозначаться L_σ; формулу языка $L \subseteq L_\sigma$ назовем *L-формулой*. Пренексная L_σ-формула есть формула вида $Q_1 y_1 \ldots Q_m y_m \varphi(x_1, \ldots, x_n, y_1, \ldots, y_m)$, где $\varphi(x_1, \ldots, x_n, y_1, \ldots, y_m)$ — бесквантворная 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. Аналогично определяются языки $\forall\exists L_\sigma$, $\exists\forall L_\sigma$ и т. д. $\exists L_\sigma$-формулы называются *экзистенциальными*, а $\forall L_\sigma$-формулы — *универсальными L_σ-формулами*.

Бесквантворную формулу будем называть *позитивной*, если она построена из атомарных формул с помощью только логических связок конъюнкции и дизъюнкции. Если в приведенных выше определениях потребовать позитивность формулы $\varphi(x_1, \ldots, x_n, y_1, \ldots, y_m)$, то к обозначению получаемых языков добавится приставка P, а формулы этих языков будут называться *позитивными*. Например, $\text{P}\exists L_\sigma$ есть множество позитивных экзистенциальных L_σ-формул.

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. Множество всех замкнутых L-формул, истинных в структуре $\langle M; \sigma \rangle$, будет называться *$L$-теорией структуры* $\langle M; \sigma \rangle$ и обозначается $L\text{-Th}\langle M; \sigma \rangle$. 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 (а в некоторых случаях и следующий за ним дефис) можно опустить. В частности, $\text{P}\exists L_\sigma$-выразимые в структуре $\langle M; \sigma \rangle$ отношения будут называться *позитивно экзистенциально выразимыми в структуре* $\langle M; \sigma \rangle$ или P$\exists$-выразимыми. $\text{Th}\langle M; \sigma \rangle$

есть *элементарная теория структуры* $\langle M;\sigma\rangle$, а $(\mathrm{P})\exists\mathrm{Th}\langle M;\sigma\rangle$ — *(позитивная) экзистенциальная теория структуры* $\langle M;\sigma\rangle$.

Алгоритмом элиминации кванторов (ЭК) для языка L_σ *в структуре* $\langle M;\sigma\rangle$ называется алгоритм, который по всякой L_σ-формуле вида $\exists x\varphi(x,y_1,\ldots,y_n)$, где $\varphi(x,y_1,\ldots,y_n)$ — бескванторная L_σ-формула, строит эквивалентную ей в этой структуре бескванторную L_σ-формулу $\psi(y_1,\ldots,y_n)$. В качестве следствия получаем, что алгоритм элиминации кванторов позволяет построить по всякой L_σ-формуле эквивалентную в соответствующей структуре бескванторную L_σ-формулу. Отметим, что именно алгоритм из следствия, построение которого сводится к построению алгоритма ЭК в нашем смысле, обычно (например, в [6]) называется алгоритмом ЭК.

2.2. Определение квазиэлиминации кванторов. Пусть имеются два непересекающихся сорта переменных S_1 и S_2. Переменные из S_1 будут обозначаться буквами латинского алфавита (и будут называться *латинскими переменными*), а переменные из S_2 — буквами греческого алфавита (*греческие переменные*). Пусть $L_\sigma^{1,2}$ — язык первого порядка сигнатуры σ с переменными из $S_1\cup S_2$. Обозначим L_σ^1 и L_σ^2 языки первого порядка сигнатуры σ с переменными соответственно из S_1 и S_2.

Обозначим $[\varphi]_t^x$ результат подстановки терма t вместо каждого свободного вхождения переменной x в формулу φ. Множество формул $L\subset L_\sigma$ назовем *эффективно проверяемым*, если существует алгоритм, распознающий L-формулы.

Определение. Пусть дана некоторая структура $\langle M;\sigma\rangle$ с сигнатурой σ и эффективно проверяемое множество формул $L\subset L_\sigma^{1,2}$, такое что все латинские переменные входят свободно, а все греческие связаны кванторами существования. Пусть также для некоторой переменной $x\in S_1$ определено эффективно проверяемое множество L*-формул элиминационного вида* $L^x\subseteq L$ и заданы два шага.

Шаг 1. Построение по всякой формуле $\exists\overline{\alpha}\varphi(\overline{y},\overline{\alpha})\in L$ равновыполнимой в $\langle M;\sigma\rangle$ дизъюнкции $\bigvee\limits_{j\in J}\exists\overline{\alpha}\widetilde{\varphi}_j(\overline{y_j},\overline{\alpha})$ для некоторого конечного множества индексов J и списков латинских переменных $\overline{y_j}$ таких, что для всякого $j\in J$:

1) количество переменных в списке $\overline{y_j}$ не превосходит количества переменных в $\overline{y}$;

2) если список переменных $\overline{y_j}$ не пуст, то найдется переменная $\widetilde{x}_j\in\overline{y_j}$, такая что $[\exists\overline{\alpha}\widetilde{\varphi}_j(\overline{y_j},\overline{\alpha})]_x^{\widetilde{x}_j}\in L^x$.

Шаг 2. Построение по всякой формуле $\exists x\exists\overline{\alpha}\widetilde{\varphi}(x,\overline{z},\overline{\alpha})$, где $\exists\overline{\alpha}\widetilde{\varphi}(x,\overline{z},\overline{\alpha})\in L^x$, эквивалентной в структуре $\langle M;\sigma\rangle$ L-формулы $\exists\overline{\alpha}\exists\overline{\beta}\psi(\overline{z},\overline{\alpha},\overline{\beta})$.

Тогда $\mathcal{A}$ — *алгоритм квазиэлиминации кванторов (квази-ЭК) для языка* L *в структуре* $\langle M;\sigma\rangle$, если по данной на вход L-формуле $\exists\overline{\alpha}\varphi(y_1,\ldots,y_k,\overline{\alpha})$ сначала выполняется шаг 1, а затем для каждой формулы $\exists x\,[\exists\overline{\alpha}\widetilde{\varphi}_j(\overline{y_j},\overline{\alpha})]_x^{\widetilde{x}_j}$ — шаг 2. Таким образом, получается равновыполнимая дизъюнкция L-формул, в каждой из которых число латинских переменных меньше k.

Язык L будет называться *языком алгоритма квази-ЭК* $\mathcal{A}$.

Рассмотрим некоторые свойства алгоритма квази-ЭК $\mathcal{A}$ для $L_{\mathcal{A}}$ в $\langle M;\sigma\rangle$. Для подмножества L бескванторных формул L_σ определим язык $\exists L$ как множество формул вида $\exists\overline{x}\varphi(\overline{x},\overline{y})$ для всякой (бескванторной) L-формулы $\varphi(\overline{x},\overline{y})$. Множество замкнутых $\exists L$-формул обозначим $E(L)$.

Основное назначение $\mathcal{A}$ можно описать следующим образом. Так как $L_{\mathcal{A}} \cap L^1_\sigma$ содержит только бескванторные L_σ-формулы, то определено множество формул $E(L_{\mathcal{A}} \cap L^1_\sigma)$, которое обозначим $L^1_{\mathcal{A}}$, и пусть $L^2_{\mathcal{A}} \rightleftharpoons L_{\mathcal{A}} \cap L^2_\sigma$. Тогда алгоритм $\mathcal{A}$ выполняет сведение проблемы разрешимости для $L^1_{\mathcal{A}}$-теории к проблеме разрешимости для $L^2_{\mathcal{A}}$-теории. Действительно, по всякой (бескванторной) $(L_{\mathcal{A}} \cap L^1_\sigma)$-формуле φ повторным применением алгоритма $\mathcal{A}$ к каждой из $L_{\mathcal{A}}$-формул получаемых дизъюнкций построим дизъюнкцию (замкнутых) $L^2_{\mathcal{A}}$-формул, истинную в $\langle M; \sigma\rangle$ тогда и только тогда, когда φ выполнима в этой структуре.

Если S_2 является пустым сортом переменных, то $L_{\mathcal{A}}$ является подмножеством бескванторных L_σ-формул. В этом случае, если вычисление в $\langle M; \sigma\rangle$ истинностного значения L_σ-формулы без переменных является разрешимой проблемой, то $\mathcal{A}$ позволяет доказать разрешимость $E(L_{\mathcal{A}})$-теории структуры $\langle M; \sigma\rangle$, так как для исследуемой на выполнимость формулы мы построим формулу без переменных. Рассмотрим еще два важных примера.

Пример 1. Если S_2 является пустым сортом переменных и $L^x_{\mathcal{A}} = L_{\mathcal{A}}$ (шаг 1 алгоритма $\mathcal{A}$ становится тривиальным), то множество всех $\exists L_{\mathcal{A}}$-выразимых в $\langle M; \sigma\rangle$ отношений совпадает со множеством отношений, (бескванторно) $L_{\mathcal{A}}$-выразимых в $\langle M; \sigma\rangle$.

Единственный шаг алгоритма позволяет последовательно проэлиминировать каждый квантор данной $\exists L_{\mathcal{A}}$-формулы и получить эквивалентную в $\langle M; \sigma\rangle$ $L_{\mathcal{A}}$-формулу, которая является бескванторной L_σ-формулой.

Пример 2. Если, кроме того, $L_{\mathcal{A}}$ является множеством всех бескванторных L_σ-формул, то $\mathcal{A}$ есть в точности алгоритм элиминации кванторов для L_σ в $\langle M; \sigma\rangle$.

3. НОД-лемма. Под китайской теоремой об остатках мы предполагаем теорему [8], утверждающую существование целочисленного решения у системы делимостей $\bigwedge\limits_{i\in[1..m]} d_i \mid b_i + x$ тогда и только тогда, когда $\bigwedge\limits_{i,j\in[1..m]} \text{НОД}(d_i, d_j) \mid b_i - b_j$.

Для каждого ненулевого целого числа x и простого p величина $v_p(x)$ обозначает p-показатель x, то есть максимальное k, для которого $p^k \mid x$. Будем писать $\text{НОД}(x, y, z)$ вместо $\text{НОД}(\text{НОД}(x, y), z)$. Тогда для системы

$$\bigwedge_{i\in[1..m]} \text{НОД}(a_i, b_i + x) = d_i \tag{1}$$

можно доказать следующую лемму.

Лемма 1 (НОД-лемма)**.** *Определим для системы* (1)*, где* $a_i, b_i, d_i \in \mathbb{Z}$ *и* $a_i \neq 0$*,* $d_i > 0$*,* $i \in [1..m]$*, и всякого простого числа* p *целое число* $M_p = \max\limits_{i\in[1..m]} v_p(d_i)$ *и два множества индексов:* $J_p = \{i \in [1..m] : v_p(d_i) = M_p\}$ *и* $I_p = \{i \in J_p : v_p(a_i) > M_p\}$.

Система (1) *имеет решение в* $\mathbb{Z}$ *тогда и только тогда, когда одновременно выполняются следующие условия:*

(i) $\bigwedge\limits_{i\in[1..m]} d_i \mid a_i$,

(ii) $\bigwedge\limits_{i,j\in[1..m]} \text{НОД}(d_i, d_j) \mid b_i - b_j$,

(iii) $\bigwedge\limits_{i,j\in[1..m]} \text{НОД}(a_i, d_j, b_i - b_j) \mid d_i$,

(iv) для всякого простого $p \le m$ *и всякого* $I \subseteq I_p$ *такого, что* $|I| = p$, *существуют такие* $i, j \in I$, $i \ne j$, *что* $v_p(b_i - b_j) > M_p$.

Перед тем как переходить к доказательству леммы 1, удобно переформулировать ее четвертый пункт. Определим условие

((iv)) для всякого простого p *найдется* $x_p \in \mathbb{Z}$ *такой, что* $\bigwedge\limits_{i\in I_p} v_p(b_i + x_p) = M_p$

и докажем следующую лемму.

Лемма 2. *Пусть для системы вида* (1) *значения* a_i, b_i, d_i, M_p, I_p *определены так же, как в лемме 1, и выполнено условие (ii). Тогда (iv) имеет место тогда и только тогда, когда выполнено ((iv)).*

Доказательство. Рассмотрим простое p, натуральное число M_p и множество индексов I_p. Условие 1 подразумевает совместность системы $\bigwedge\limits_{i\in I_p} p^{M_p} \mid b_i + x$. Возьмем $x_0 \in [0, p^{M_p})$ такое, что $x_0 \equiv -b_i (\mathrm{mod}\ p^{M_p})$ для $i \in I_p$. Тогда получаем, что $x = x_0 + kp^{M_p}$ является решением для любого $k \in \mathbb{Z}$ и, таким образом, имеем

$$\exists x \left(\bigwedge_{i\in I_p} v_p(b_i + x) = M_p \right) \Leftrightarrow \exists k \left(\bigwedge_{i\in I_p} p \nmid \left(\frac{x_0 + b_i}{p^{M_p}} + k \right) \right). \tag{2}$$

Правая часть (2) истинна тогда и только тогда, когда $\left\{ \frac{x_0+b_i}{p^{M_p}} \right\}_{i\in I_p}$ не содержит полной системы вычетов по модулю p. Следовательно, это верно для каждого $p > m$, а для $p \le m$ это условие эквивалентно тому, что для каждого $I \subseteq I_p$ такого, что $|I| = p$, существуют $i, j \in I$, $i \ne j$ такие, что $p \mid \frac{x_0+b_i}{p^{M_p}} - \frac{x_0+b_j}{p^{M_p}}$, или, в терминах p-показателя, $v_p(b_i - b_j) > M_p$. □

Лемму 1 докажем, предполагая, что условие (iv) было заменено на ((iv)).

Доказательство. *Необходимость.* Условие (i), очевидно, необходимо. Так как для каждого $i, j \in [1..m]$ мы имеем $d_i \mid b_i + x$ и $d_j \mid b_j + x$, следовательно $\text{НОД}(d_i, d_j) \mid b_i + x - (b_j + x)$. Таким образом, получаем (ii).

Чтобы доказать (iii), рассмотрим для каждой пары индексов $i, j \in [1..m]$ следующую цепочку равенств:

$$\begin{aligned}\text{НОД}(a_i, d_j, b_i - b_j) &= \text{НОД}(a_i, \text{НОД}(a_j, b_j + x), b_i - b_j) = \\ &= \text{НОД}(a_i, a_j, \text{НОД}(b_i + x, b_j + x)) = \text{НОД}(d_i, d_j).\end{aligned}$$

Для всякого простого числа p имеем $v_p(\text{НОД}(a_i, b_i + x)) = v_p(d_i)$ для любого $i \in [1..m]$. В частности, если $i \in I_p$, то $\min(v_p(a_i), v_p(b_i + x)) = M_p$, причем $v_p(a_i) > M_p$. Следовательно, $v_p(b_i + x) = M_p$, и необходимость условия ((iv)) доказана.

Достаточность. Пусть P_0 — (конечное) множество всех простых чисел p таких, что $p \mid a_i$ для некоторого $i \in [1..m]$. Условие (i) подразумевает, что

$\bigwedge\limits_{i\in[1..m]}\left(\bigwedge\limits_{p\in P_0} v_p(a_i)\geq v_p(d_i)\right)$. Перепишем (1) в виде системы делимостей и неделимостей:

$$\bigwedge_{i\in[1..m]}\left(\bigwedge_{p\in P_0\wedge v_p(a_i)=v_p(d_i)} p^{v_p(d_i)}\mid b_i+x\right)\wedge$$
$$\wedge\left(\bigwedge_{p\in P_0\wedge v_p(a_i)>v_p(d_i)} p^{v_p(d_i)}\mid b_i+x\wedge p^{v_p(d_i)+1}\nmid b_i+x\right). \tag{3}$$

Для каждого простого числа $p\in P_0$ выделим в (3) подсистему, содержащую все делимости и неделимости, в которых делителем является p в некоторой степени. Определим множество индексов $K_p=\{i\in[1..m]\setminus J_p\,:\,v_p(a_i)>v_p(d_i)\}$ и систему

$$\Phi_p(x)\rightleftharpoons\bigwedge_{i\in[1..m]\setminus J_p} p^{v_p(d_i)}\mid b_i+x\wedge\bigwedge_{i\in K_p} p^{v_p(d_i)+1}\nmid b_i+x. \tag{4}$$

Теперь система (3) перепишется следующим образом:

$$\bigwedge_{p\in P_0}\left(\Phi_p(x)\wedge\bigwedge_{i\in J_p} p^{M_p}\mid b_i+x\wedge\bigwedge_{i\in I_p} p^{M_p+1}\nmid b_i+x\right). \tag{5}$$

По китайской теореме об остатках достаточно найти отдельно для каждого простого числа $p\in P_0$ решение соответствующей подсистемы.

Зафиксируем некоторое $p\in P_0$. Сначала построим решение x_p системы делимостей и неделимостей с индексами из J_p, а затем проверим, что имеет место $\Phi_p(x_p)$.

Если $I_p=\emptyset$, то ввиду того, что по условию (ii) $b_i\equiv b_j(\mathrm{mod}\ p^{M_p})$ для всех $i,j\in J_p$, достаточно выбрать любой индекс $j_p\in J_p$ и определить $x_p\in[0,p^{M_p})$, сравнимый с $-b_{j_p}$ по модулю p^{M_p}.

Иначе, если множество индексов I_p не пусто, по условию ((iv)) найдется решение $x_p\in\mathbb{Z}$, такое что

$$\bigwedge_{i\in I_p} p^{M_p}\mid b_i+x_p\wedge\bigwedge_{i\in I_p} p^{M_p+1}\nmid b_i+x_p. \tag{6}$$

Удобно считать, что $x_p\in[0,p^{M_p+1})$. Ввиду условия (ii), в подсистеме делимостей из (6) множество индексов I_p можно заменить на J_p.

Осталось показать, что x_p удовлетворяет системе делимостей и неделимостей (4). Пусть снова j_p является произвольным индексом из J_p. Из условия (ii) следует, что $b_k\equiv b_{j_p}(\mathrm{mod}\ p^{v_p(d_k)})$ для каждого $k\in[1..m]\setminus J_p$ и, значит, $p^{v_p(d_k)}\mid b_k+x_p$, так как $v_p(d_k)<M_p$. Поэтому x_p удовлетворяет подсистеме делимостей из (4).

Чтобы доказать, что x_p также является решением подсистемы неделимостей, предположим, что $p^{v_p(d_k)+1}$ делит x_p+b_k для некоторого $k\in K_p$. Тогда получим $v_p(b_k-b_{j_p})\geq\min\left\{v_p(b_k+x_p),v_p(b_{j_p}+x_p)\right\}\geq v_p(d_k)+1$. Отсюда следует, что

$$\min\left\{\min\left\{v_p(a_k),M_p\right\},v_p(b_k-b_{j_p})\right\}\geq v_p(d_k)+1.$$

Но это противоречит (iii), так как левая часть не должна превосходить $v_p(d_k)$.

Таким образом, получаем решение из системы вида

$$\bigwedge_{p\in P_0} x \equiv x_p (\mathrm{mod}\ p^{\beta_p}),$$

где $\beta_p = M_p + 1$, если множество индексов I_p не пусто, а иначе — $\beta_p = M_p$. □

Итоговая система сравнений позволяет сделать следующее замечание.

Замечание. Если x является решением системы (1), то $x + k \cdot \operatorname{НОК}_{i\in[1..m]}(d_i) \cdot \operatorname{rad}\left(\prod_{i\in[1..m]} \frac{a_i}{d_i}\right)$ также является решением для каждого $k \in \mathbb{Z}$, где $\operatorname{rad}(n)$ — радикал ненулевого целого числа n, т. е. произведение различных простых делителей n.

4. Системы нод-выражений с единственным ненулевым коэффициентом в полиномах. В этом разделе будет построен алгоритм квази-ЭК $\mathcal{D}$, который позволит проверять совместность в положительных целых числах систем $\operatorname{НОД}(f_i(\overline{y}), g_i(\overline{y})) = h_i(\overline{y})$ для всех $i \in [1..m]$, где $f_i(\overline{y})$, $g_i(\overline{y})$ и $h_i(\overline{y})$ суть выражения вида либо a, либо ax для некоторого положительного целого числа a и переменной $x \in \overline{y}$. Выражения вида $\operatorname{НОД}(f(\overline{y}), g(\overline{y})) = h(\overline{y})$ далее будут называться *нод-выражениями*. На шаге 2 алгоритма $\mathcal{D}$ используется следующий частный случай НОД-леммы.

Лемма 3. *Система* $\bigwedge_{i\in[1..m]} \operatorname{НОД}(a_i, x) = d_i$, *где* $a_i, d_i \in \mathbb{Z}$ *и* $a_i \neq 0$, $d_i > 0$ *для каждого* $i \in [1..m]$, *имеет решение в* $\mathbb{Z}$ *тогда и только тогда, когда одновременно выполняются следующие условия:*

(a) $\bigwedge_{i\in[1..m]} d_i \mid a_i$,

(b) $\bigwedge_{1\leq i<j\leq m} \operatorname{НОД}(a_i, d_j) = \operatorname{НОД}(a_j, d_i) = \operatorname{НОД}(d_i, d_j)$.

Доказательство. Поскольку в данном случае все значения b_i из НОД-леммы равны нулю, достаточно рассмотреть условия (i) и (iii). Первое из них остается неизменным, а условие (iii) имеет вид системы следующих пар делимостей:

$$\operatorname{НОД}(a_i, d_j) \mid d_i \wedge \operatorname{НОД}(a_j, d_i) \mid d_j$$

для всяких $1 \leq i < j \leq m$. Делимость, очевидно, вытекает из (b). Обратно, (b) получаем из следующей цепочки равенств:

$$\operatorname{НОД}(a_i, d_j) = \operatorname{НОД}(d_i, \operatorname{НОД}(a_i, d_j)) = \operatorname{НОД}(\operatorname{НОД}(d_i, a_i), d_j)) = \operatorname{НОД}(d_i, d_j).$$

□

Теперь рассмотрим структуру $\langle \mathbb{Z}_{>0}; 1, \{a\cdot\}_{a\in\mathbb{Z}_{>0}}, \operatorname{НОД}\rangle$ и определим алгоритм квази-ЭК $\mathcal{D}$. В этом алгоритме S_2 будет пустым сортом переменных. Язык $L_{\mathcal{D}}$ алгоритма $\mathcal{D}$ будет представлять собой множество формул $\bigvee_{j\in J_1} \varphi_j(\overline{y_j})$ для некоторого конечного множества индексов J_1 и конъюнкций нод-выражений $\varphi_j(\overline{y})$, таких что каждое нод-выражение имеет одну из следующих форм:

($\mathcal{D}$-1) НОД$(au, bv) = dw$,

($\mathcal{D}$-2) НОД$(au, bv) = d$,

($\mathcal{D}$-3) НОД$(a, bv) = d$,

($\mathcal{D}$-4) НОД$(a, b) = d$,

где u и v — различные переменные, w может совпадать с u или v, а a, b, d — положительные целые числа. Кроме того, каждая конъюнкция $\varphi_j(\overline{y})$ для всякой пары переменных $u, v \in \overline{y}$ содержит нод-выражение с левой частью вида НОД(au, bv) для некоторых положительных целых чисел a и b.

Множество формул элиминационного вида $L^x_{\mathcal{D}} \subseteq L_{\mathcal{D}}$ содержит формулы $\bigvee\limits_{j\in J_2} \widetilde{\varphi}_j(x, \overline{z_j})$ для конечного множества индексов J_2 и $\widetilde{\varphi}_j(x, \overline{z})$ вида:

$$\widetilde{\widetilde{\varphi}}_j(\overline{z}) \wedge \bigwedge_{i\in[1..\widetilde{m}_j]} \text{НОД}(\widetilde{f}_{i,j}(\overline{z}), c_{i,j}x) = \widetilde{h}_{i,j}(\overline{z}), \tag{7}$$

так что x не входит в $\overline{z}$, $c_{i,j} > 0$ и $\widetilde{\widetilde{\varphi}}_j(\overline{z})$ есть система нод-выражений с переменными из $\overline{z}$.

Прежде чем определить шаги 1 и 2 алгоритма $\mathcal{D}$, докажем следующую лемму.

Лемма 4. *Проблема разрешимости для* P∃Th$\langle \mathbb{Z}_{>0}; 1, \{a\cdot\}_{a\in\mathbb{Z}_{>0}}, \text{НОД}\rangle$ *сводится к проблеме разрешимости для* $L^1_{\mathcal{D}}$*-теории.*

Доказательство. Рассмотрим систему нод-выражений

$$\bigwedge_{i\in[1..m]} \text{НОД}(f_i(\overline{y}), g_i(\overline{y})) = h_i(\overline{y}) \tag{8}$$

для $f_i(\overline{y}), g_i(\overline{y}), h_i(\overline{y})$ вида либо au, либо a, где a есть некоторое положительное целое число и $u \in \overline{y}$.

Для нод-выражений вида НОД$(au, bu) = h(\overline{y})$ наибольший общий делитель может быть непосредственно вычислен, и мы можем избавиться от одной из переменных. В случае НОД$(a, g(\overline{y})) = du$, где $a, d > 0$, система (8) эквивалентна дизъюнкции по всем положительным делителям d' числа $\frac{a}{d}$ систем, полученных из (8) подстановкой d' вместо каждого вхождения u.

Рассмотрим пары переменных $u, v \in \overline{y}$, для которых в (8) не задано значение НОД(au, bv) ни для каких положительных целых чисел a и b. Введем новую переменную $t_{\{u,v\}}$ для каждой такой пары (u, v) и добавим в систему (8) выражение НОД$(u, v) = t_{\{u,v\}}$. Продолжая этот процесс для новых переменных, мы вводим не более 2^n переменных t_Y для наибольших общих делителей различных подмножеств Y из $\overline{y}$ (так как для каждой пары переменных t_{Y_1} и t_{Y_2} имеем НОД$(t_{Y_1}, t_{Y_2}) = t_{Y_1\cup Y_2}$). □

Теорема 3. P∃Th$\langle \mathbb{Z}_{>0}; 1, \{a\cdot\}_{a\in\mathbb{Z}_{>0}}, \text{НОД}\rangle$ *разрешима.*

Доказательство. Из леммы 4 следует, что если определить алгоритм квази-ЭК $\mathcal{D}$ для языка $L_{\mathcal{D}}$ в $\mathbb{Z}_{>0}$, то получим разрешающую процедуру для теории P∃Th$\langle \mathbb{Z}_{>0}; 1, \{a\cdot\}_{a\in\mathbb{Z}_{>0}}, \text{НОД}\rangle$. Определим два шага $\mathcal{D}$.

Шаг 1. Пусть имеется некоторая $L_{\mathcal{D}}$-формула вида (8). Построим ориентированный граф, вершинами которого являются переменные системы (8), а каждая дуга от вершины u к вершине v соответствует нод-выражению, в котором $h_i(\overline{y})$ имеет вид du, и либо $f_i(\overline{y})$, либо $g_i(\overline{y})$ имеет вид av. В полученном графе будем искать циклы и переписывать (8) в виде дизъюнкции систем с меньшим числом переменных. Видим, что если граф, построенный по системе вида (8), не имеет циклов, то $L_{\mathcal{D}}$-формула (8) содержит переменные, которые не входят в правую часть ни одного из нод-выражений, и, таким образом, является $L^x_{\mathcal{D}}$-формулой.

Предположим, что имеется некоторый цикл $y_1 \to y_2 \to \ldots \to y_s \to y_1$. Он соответствует последовательности делимостей вида

$$a_1y_1 \mid b_1y_2, \ldots, a_{s-1}y_{s-1} \mid b_{s-1}y_s, \gamma y_s \mid \delta y_1.$$

Первые $(s-1)$ делимостей дают делимость вида $\alpha y_1 \mid \beta y_s$. Таким образом, имеем $\beta y_s = k\alpha y_1$ для некоторого положительного целого числа k. Так как $\gamma y_s \mid \delta y_1$, то $\gamma\beta y_s \mid \delta\beta y_1$ и, следовательно, $\gamma k\alpha y_1 \mid \delta\beta y_1$. Поскольку $y_1 > 0$, существует конечное множество таких k, и мы можем исключить одну из переменных, например y_s. Продолжая этот процесс, исключаем все переменные из этого цикла, кроме y_1.

Шаг 2. Рассмотрим подсистему (7) с изолированной переменной x. Несложными преобразованиями формул можно добиться равенства единице коэффициентов $c_{i,j}$. Для этого вычислим $C = \underset{i=1..\widetilde{m}_j}{\text{НОК}}(c_{i,j})$, умножим на $\frac{C}{c_{i,j}}$ нод-выражение с индексом i для всех $i = 1..\widetilde{m}_j$, заменим все вхождения Cx на $\widetilde{x}$ и добавим в систему нод-выражение $\text{НОД}(C, \widetilde{x}) = C$. Поэтому далее будем работать с $L^x_{\mathcal{D}}$-формулой вида

$$\widetilde{\widetilde{\varphi}}(\overline{z}) \wedge \bigwedge_{i\in[1..m]} \text{НОД}(f_i(\overline{z}), x) = h_i(\overline{z}). \tag{9}$$

Применяя лемму 3, рассмотрим каждый пункт отдельно.

(a) В этом случае получаем конъюнкцию $\bigwedge\limits_{i\in[1..m]} \text{НОД}(h_i(\overline{z}), f_i(\overline{z})) = h_i(\overline{z})$.

(b) Для каждой пары $1 \le i < j \le m$ необходимо переписать цепочку равенств

$$\text{НОД}(f_i(\overline{z}), h_j(\overline{z})) = \text{НОД}(f_j(\overline{z}), h_i(\overline{z})) = \text{НОД}(h_i(\overline{z}), h_j(\overline{z})).$$

Рассмотрим два случая.

1. Если $h_i(\overline{z}) = d_i$ или $h_j(\overline{z}) = d_j$ для некоторых положительных целых чисел d_i, d_j, получим следующую дизъюнкцию по всем положительным делителям d_i (предполагая, что имеет место первое равенство):

$$\bigvee_{d\mid d_i} \big(\text{НОД}(f_i(\overline{z}), h_j(\overline{z})) = d \wedge \text{НОД}(f_j(\overline{z}), d_i) = d \wedge \text{НОД}(d_i, h_j(\overline{z})) = d\big).$$

2. Теперь предположим, что нод-выражения с номерами i и j имеют вид ($\mathcal{D}$-1). Для $h_i(\overline{z}) = d_iz_i$ и $h_j(\overline{z}) = d_jz_j$ это условие переписывается следующим образом.

Если $z_i = z_j$, получим конъюнкцию

$$\text{НОД}(f_i(\overline{z}), d_jz_j) = \text{НОД}(d_i, d_j)z_i \wedge \text{НОД}(f_j(\overline{z}), d_iz_i) = \text{НОД}(d_i, d_j)z_i.$$

Пусть теперь $z_i \ne z_j$, тогда система (9) должна содержать нод-выражение вида $\text{НОД}(az_i, bz_j) = h(\overline{z})$. Следовательно, $\text{НОД}(z_i, z_j) = \frac{h(\overline{z})}{\text{НОД}(a,b)l}$ для некоторого делителя l числа $\text{НОК}(a, b)$, а значит, $\text{НОД}(h_i(\overline{z}), h_j(\overline{z}))$ должен быть равным $\frac{\text{НОД}(d_i,d_j)k}{\text{НОД}(a,b)l}h(\overline{z})$ для некоторого $k \mid \text{НОК}(d_i, d_j)$.

Обозначим $M_{k,l} = \frac{\text{НОД}(d_i,d_j)k}{\text{НОД}(a,b)l}$ и перепишем условие (b) для пары (i,j) с помощью следующей дизъюнкции:

$$\bigvee_{k|\text{НОК}(d_i,d_j)} \left(\bigvee_{l|\text{НОК}(a,b)} \text{НОД}(h_i(\overline{z}),h_j(\overline{z})) = M_{k,l}h(\overline{z}) \wedge \right.$$
$$\left. \wedge \text{НОД}(f_i(\overline{z}),h_j(\overline{z})) = M_{k,l}h(\overline{z}) \wedge \text{НОД}(f_j(\overline{z}),h_i(\overline{z})) = M_{k,l}h(\overline{z}) \right).$$

Полученная формула, очевидно, является $L_{\mathcal{D}}$-формулой, что завершает определение алгоритма квази-ЭК $\mathcal{D}$ и доказательство теоремы. □

Теорема 1 теперь следует из теорем 2 и 3. Построению алгоритма квази-ЭК $\mathcal{R}$, который позволит доказать теорему 2, будет посвящена вторая часть доказательства.

Автор благодарен анонимным рецензентам за весьма полезные замечания и советы по оформлению статьи.

Литература

1. Бельтюков А. П. Разрешимость универсальной теории натуральных чисел со сложением и делимостью. *Записки научных семинаров ЛОМИ* **60**, 15–28 (1976).

2. Lipshitz L. The Diophantine problem for addition and divisibility. *Transactions of the American Mathematical Society* **235**, 271–283 (1978). https://doi.org/10.1090/S0002-9947-1978-0469886-1

3. Мартьянов В. И. Универсальные расширенные теории целых чисел. *Алгебра и логика* **16** (5), 588–602 (1977).

4. Lipshitz L. Some remarks on the Diophantine problem for addition and divisibility. *Bull. Soc. Math. Belg. Ser. B* **33**, iss. 1, 41–52 (1981).

5. Lechner A., Ouaknine J., Worrell J. On the complexity of linear arithmetic with divisibility. *Proceedings of the 30th Annual ACM / IEEE Symposium on Logic in Computer Science (LICS)*, 667–676 (2015). https://doi.org/10.1109/LICS.2015.67

6. Weispfenning V. The complexity of linear problems in fields. *Journal of Symbolic Computation* **5**, iss. 1–2, 3–27 (1988). https://doi.org/10.1016/S0747-7171(88)80003-8

7. Guépin F., Haase C., Worrell J. On the existential theories of Büchi arithmetic and linear p-adic fields. *Proceedings of the 34th Annual ACM / IEEE Symposium on Logic in Computer Science (LICS)*, 1–10 (2019). https://doi.org/10.1109/LICS.2019.8785681

8. Schmid H. L., Mahler K. On the Chinese remainder theorem. *Mathematische Nachrichten* **18**, 120–122 (1958).

Статья поступила в редакцию 28 августа 2020 г.;
после доработки 24 января 2021 г.;
рекомендована в печать 19 марта 2021 г.

Контактная информация:

Старчак Михаил Романович — ассистент; m.starchak@spbu.ru

A proof of Bel'tyukov — Lipshitz theorem by quasi-quantifier elimination. I. Definitions and GCD-lemma

M. R. Starchak

St. Petersburg State University, 7–9, Universitetskaya nab., St. Petersburg, 199034, Russian Federation

For citation: Starchak M. R. A proof of Bel'tyukov — Lipshitz theorem by quasi-quantifier elimination. I. Definitions and GCD-lemma. *Vestnik of Saint Petersburg University. Mathematics. Mechanics. Astronomy*, 2021, vol. 8 (66), issue 3, pp. 455–466.
https://doi.org/10.21638/spbu01.2021.307 (In Russian)

This paper is the first part of a new proof of decidability of the existential theory of the structure $\langle \mathbb{Z}; 0, 1, +, -, \leq, | \rangle$, where $|$ corresponds to the binary divisibility relation. The decidability was proved independently in 1976 by A. P. Bel'tyukov and L. Lipshitz. In 1977, V. I. Mart'yanov proved an equivalent result by considering the ternary GCD predicate instead of divisibility (the predicates are interchangeable with respect to existential definability). Generalizing in some sense the notion of quantifier elimination (QE) algorithm, we construct a quasi-QE algorithm to prove decidability of the positive existential theory of the structure $\langle \mathbb{Z}_{>0}; 1, \{a\cdot\}_{a\in\mathbb{Z}_{>0}}, \mathrm{GCD} \rangle$. We reduce to the decision problem for this theory the decision problem for the existential theory of the structure $\langle \mathbb{Z}; 0, 1, +, -, \leq, \mathrm{GCD} \rangle$. A quasi-QE algorithm, which performs this reduction, will be constructed in the second part of the proof. Transformations of formulas are based on a generalization of the Chinese remainder theorem to systems of the form $\mathrm{GCD}(a_i, b_i + x) = d_i$ for every $i \in [1..m]$, where a_i, b_i, d_i are some integers such that $a_i \neq 0$, $d_i > 0$.

Keywords: quantifier elimination, existential theory, divisibility, decidability, Chinese remainder theorem.

References

1. Bel'tyukov A. P. Decidability of the universal theory of the natural numbers with addition and divisibility. *Zapiski Nauchnyh Seminarov LOMI* **60**, 15–28 (1976). (In Russian)

2. Lipshitz L. The Diophantine problem for addition and divisibility. *Transactions of the American Mathematical Society* **235**, 271–283 (1978). https://doi.org/10.1090/S0002-9947-1978-0469886-1

3. Mart'yanov V. I. Universal extended theories of integers. *Algebra i Logika* **16** (5), 588–602 (1977). (In Russian)

4. Lipshitz L. Some remarks on the Diophantine problem for addition and divisibility. *Bull. Soc. Math. Belg. Ser. B* **33**, iss. 1, 41–52 (1981).

5. Lechner A., Ouaknine J., Worrell J. On the complexity of linear arithmetic with divisibility. *Proceedings of the 30th Annual ACM / IEEE Symposium on Logic in Computer Science (LICS)*, 667–676 (2015). https://doi.org/10.1109/LICS.2015.67

6. Weispfenning V. The complexity of linear problems in fields. *Journal of Symbolic Computation* **5**, iss. 1–2, 3–27 (1988). https://doi.org/10.1016/S0747-7171(88)80003-8

7. Guépin F., Haase C., Worrell J. On the existential theories of Büchi arithmetic and linear p-adic fields. *Proceedings of the 34th Annual ACM / IEEE Symposium on Logic in Computer Science (LICS)*, 1–10 (2019). https://doi.org/10.1109/LICS.2019.8785681

8. Schmid H. L., Mahler K. On the Chinese remainder theorem. *Mathematische Nachrichten* **18**, 120–122 (1958).

Received: August 28, 2020
Revised: January 24, 2021
Accepted: March 19, 2021

Author's information:

Mikhail R. Starchak — m.starchak@spbu.ru