Вестник СПбГУ. Математика. Механика. Астрономия. 2021. Т. 8 (66). Вып. 4
УДК 510.53, 510.652
MSC 03C10, 03B80, 03B25, 11U05

Доказательство теоремы Бельтюкова — Липшица квазиэлиминацией кванторов. II. Основное сведение

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. II. Основное сведение // Вестник Санкт-Петербургского университета. Математика. Механика. Астрономия. 2021. Т. 8 (66). Вып. 4. С. 608–619.
https://doi.org/10.21638/spbu01.2021.406

Работа является второй частью нового доказательства теоремы Бельтюкова — Липшица о разрешимости экзистенциальной теории структуры $\langle \mathbb{Z}; 0, 1, +, -, \leq, | \rangle$. Строится алгоритм квази-ЭК (понятие введено в первой части доказательства), осуществляющий сведение проблемы разрешимости для экзистенциальной теории структуры $\langle \mathbb{Z}; 0, 1, +, -, \leq, \text{НОД} \rangle$ к проблеме разрешимости для позитивной экзистенциальной теории структуры $\langle \mathbb{Z}_{>0}; 1, \{a\cdot\}_{a \in \mathbb{Z}_{>0}}, \text{НОД} \rangle$. Так как разрешимость последней теории была доказана в первой части, построенное сведение завершит доказательство теоремы. На шаге отделения переменной для квазиэлиминации используются аналоги двух лемм из доказательства Липшица. Шаг квазиэлиминации основан на НОД-лемме, доказанной в первой части.

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

1. Краткое введение. Данная работа является продолжением доказательства с помощью алгоритмов квазиэлиминации кванторов (квази-ЭК) теоремы Бельтюкова — Липшица [1, 2] о разрешимости экзистенциальной теории структуры $\langle \mathbb{Z}; 0, 1, +, -, \leq, \text{НОД} \rangle$. Определение таких алгоритмов было дано в первой части [3]; также предполагаются известными и основные определения, введенные в указанной работе.

Будет построен алгоритм квази-ЭК $\mathcal{R}$, который осуществляет сведение проблемы разрешимости для экзистенциальной теории структуры $\langle \mathbb{Z}; 0, 1, +, -, \leq, \text{НОД} \rangle$ 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. Для окончания доказательства теоремы Бельтюкова — Липшица останется воспользоваться теоремой о разрешимости последней теории, доказанной в первой части [3, теорема 3] с помощью алгоритма квази-ЭК $\mathcal{D}$.

В разделе 2 будут введены основные леммы, используемые при построении шагов алгоритма $\mathcal{R}$, а затем будут заданы языки $L_{\mathcal{R}}$ и $L^x_{\mathcal{R}}$. В разделе 5 мы покажем, что преобразования, описанные в разделах 3 и 4, действительно определяют ша-

ги 1 и 2 алгоритма квази-ЭК для $L_{\mathcal{R}}$. Из определения $L_{\mathcal{R}}$ будет непосредственно следовать тот факт, что алгоритм $\mathcal{R}$ осуществляет искомое сведение.

2. Описание алгоритма. В этом разделе мы зададим языки алгоритма квази-ЭК $\mathcal{R}$, который определен для структуры $\langle \mathbb{Z}; 0, 1, +, -, \leq, \text{НОД} \rangle$.

Заметим, что $\neg\text{НОД}(x, y) = z \Leftrightarrow \exists t\,(\text{НОД}(x, y) = t \wedge t \neq z)$ для $t \neq z \Leftrightarrow t \leq z - 1 \vee z + 1 \leq t$, причем $\neg x \leq y \Leftrightarrow y + 1 \leq x$. Удобно выделить в формулах отдельно системы уравнений и неравенств, записанные в матричном виде. Таким образом, введением (возможно) некоторых новых переменных, сводим задачу разрешимости для $\exists\text{Th}\langle \mathbb{Z}; 0, 1, +, -, \leq, \text{НОД} \rangle$ к проблеме выполнимости в $\mathbb{Z}$ формул вида

$$\varphi(\overline{x}) \rightleftharpoons A\overline{x} = b \wedge C\overline{x} \geq d \wedge \bigwedge_{i \in [1..m]} \text{НОД}(f_i(\overline{x}), g_i(\overline{x})) = h_i(\overline{x}), \tag{1}$$

где $\overline{x}$ — это список переменных $x_1, \ldots, x_n$, $f_i(\overline{x}), g_i(\overline{x}), h_i(\overline{x})$ — линейные полиномы с целыми коэффициентами; A и C — целочисленные матрицы; b, d — некоторые целочисленные векторы. Выражения вида $\text{НОД}(f(\overline{x}), g(\overline{x})) = h(\overline{x})$ далее будут называться *нод-выражениями*.

2.1. Лемма о линейных системах и НОД-лемма. Преобразования, выполняемые на шаге 1 алгоритма $\mathcal{R}$, используют следующую лемму о линейных системах (ЛС-лемма), которая в более сильной форме представлена в работе А. Лечнер с соавторами [4, теорема 3]. Это утверждение было доказано Й. фон цур Гаттеном и М. Сивкингом [5]; Л. Липшиц использовал некоторый его аналог (см. [2, лемма 1]).

Лемма 1 (лемма о линейных системах (ЛС-лемма) [2, лемма 1; 5] в форме [4, теорема 3])**.** *Пусть даны целочисленная матрица A размера $p \times n$ ранга r, целочисленная матрица C размера $q \times n$, целочисленные столбцы b и d размеров p и q соответственно. Существует алгоритм построения конечного множества целочисленных матриц $E^{(j)}$ размера $n \times (n - r)$ и столбцов $u^{(j)}$ размера n для $j \in J$ таких, что*

$$\{\overline{x} \in \mathbb{Z}^n \,:\, A\overline{x} = b \wedge C\overline{x} \geq d\} = \bigcup_{j \in J} \left\{ E^{(j)}\overline{y} + u^{(j)} \,:\, \overline{y} \in \mathbb{N}^{n-r} \right\}.$$

Разделим список $\overline{x}$ на две части $\overline{s} = x_1, \ldots, x_l$ и $\overline{t} = x_{l+1}, \ldots, x_n$. Пусть система $A\overline{x} = b \wedge C\overline{x} \geq d$ распадается на две подсистемы: $S(\overline{s}) \rightleftharpoons A_1\overline{s} = b_1 \wedge C_1\overline{s} \geq d_1$ и $T(\overline{x}) \rightleftharpoons A_2\overline{x} = b_2 \wedge C_2\overline{x} \geq d_2$, где матрица A_1 имеет ранг r_1. Под *применением ЛС-леммы к подсистеме $S(\overline{s})$ формулы $\varphi(\overline{x})$* мы будем предполагать следующее. Пусть для системы $S(\overline{s})$ построены матрицы $E^{(j)}$ и столбцы $u^{(j)}, j \in J$. Построим множество формул $\{\psi_j\}_{j \in J}$, где

$$\psi_j(\overline{y}, \overline{t}) \rightleftharpoons \widetilde{T}_j(\overline{y}, \overline{t}) \wedge \overline{y} \geq 0 \wedge \bigwedge_{i \in [1..m]} \text{НОД}(\widetilde{f}_{i,j}(\overline{y}, \overline{t}), \widetilde{g}_{i,j}(\overline{y}, \overline{t})) = \widetilde{h}_{i,j}(\overline{y}, \overline{t}), \tag{2}$$

как результат подстановки $E^{(j)}\overline{y} + u^{(j)}$ вместо $\overline{s}$ в $T(\overline{s}, \overline{t}) \wedge \bigwedge_{i \in [1..m]} \text{НОД}(f_i(\overline{s}, \overline{t}), g_i(\overline{s}, \overline{t})) = h_i(\overline{s}, \overline{t})$. Таким образом, мы преобразовали $\varphi(\overline{x})$ в равновыполнимую в целых числах дизъюнкцию $\bigvee_{j \in J} \psi_j(\overline{y}, \overline{t})$, в которой число переменных уменьшилось на r_1.

Применением ЛС-леммы к подсистеме $\bigwedge\limits_{i\in[1..m]} h_i(\overline{x}) \geq 0 \wedge A\overline{x} = b \wedge C\overline{x} \geq d$ формулы $\bigwedge\limits_{i\in[1..m]} h_i(\overline{x}) \geq 0 \wedge \varphi(\overline{x})$ (равновыполнимой с $\varphi(\overline{x})$ в $\mathbb{Z}$ ввиду того, что правые части нод-выражений могут принимать только неотрицательные значения) мы получаем следующую вспомогательную лемму.

Лемма 2. *Для всякой формулы вида* (1) *можно построить равновыполнимую в* $\mathbb{Z}$ *дизъюнкцию формул вида*

$$\overline{y} \geq 0 \wedge \bigwedge_{i\in[1..m]} \text{НОД}(f_i(\overline{y}), g_i(\overline{y})) = h_i(\overline{y}), \tag{3}$$

где $\overline{y}$ *есть список переменных* $y_1, \ldots, y_k$, $k \leq n$; $f_i(\overline{y}), g_i(\overline{y}), h_i(\overline{y})$ *суть линейные полиномы с целыми коэффициентами и, кроме того, коэффициенты* $h_i(\overline{y})$ *неотрицательные.*

Аналогичный прием получения неотрицательных коэффициентов в линейных полиномах с помощью ЛС-леммы будет применяться на шаге 1 изолирования переменной, который описан в разделе 3.

В первой части [3] было доказано следующее обобщение китайской теоремы об остатках, которое будет использовано на шаге 2 квазиэлиминации в разделе 4.

Для каждого положительного целого числа x и простого p выражение $v_p(x)$ 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

$$\bigwedge_{i\in[1..m]} \text{НОД}(a_i, b_i + x) = d_i \tag{4}$$

имеет место следующее утверждение.

Лемма 3 (НОД-лемма [3])**.** *Определим для системы* (4)*, 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 (4) *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 $p \leq m$ *и всякого* $I \subseteq I_p$ *такого, что* $|I| = p$, *существуют такие* $i, j \in I$, $i \neq j$, *что* $v_p(b_i - b_j) > M_p$.

Леммы 1 и 3 позволят определить два шага алгоритма квазиэлиминации кванторов $\mathcal{R}$, в результате работы которого получим дизъюнкцию систем нод-выражений с линейными полиномами вида $a\zeta$ либо a для некоторого положительного целого числа a.

2.2. Основной алгоритм квази-ЭК. Алгоритм квази-ЭК $\mathcal{R}$ осуществляет сведение проблемы выполнимости в $\mathbb{Z}$ формул вида (1) к проблеме разрешимости для позитивной экзистенциальной теории структуры $\langle \mathbb{Z}_{>0}; 1, \{a\cdot\}_{a\in\mathbb{Z}_{>0}}, \text{НОД}\rangle$.

Язык $L_{\mathcal{R}}$ алгоритма квази-ЭК $\mathcal{R}$ есть множество формул $\exists\overline{\alpha} \bigvee\limits_{j\in J_1} \varphi_j(\overline{y_j},\overline{\alpha})$ для некоторого конечного множества индексов J_1 и формул $\varphi_j(\overline{y},\overline{\alpha})$ вида

$$\overline{\alpha} \geq 1 \wedge \overline{y} \geq 0 \wedge \bigwedge_{i\in[1..m_j]} \text{НОД}(f_{i,j}(\overline{y},\overline{\alpha}), g_{i,j}(\overline{y},\overline{\alpha})) = h_{i,j}(\overline{y},\overline{\alpha}), \tag{5}$$

где все линейные полиномы $h_{i,j}(\overline{y},\overline{\alpha})$ имеют неотрицательные целые коэффициенты и, кроме того, каждое нод-выражение имеет одну из следующих форм:

($\mathcal{R}$-1) $\text{НОД}(f(\overline{y}), g(\overline{y})) = h(\overline{y})$;

($\mathcal{R}$-2) $\text{НОД}(f(\overline{y}), g(\overline{y})) = a\zeta$;

($\mathcal{R}$-3) $\text{НОД}(a\zeta, g(\overline{y})) = b\eta$;

($\mathcal{R}$-4) $\text{НОД}(a\zeta, b\eta) = c\theta$,

где ζ, η, θ — греческие переменные (возможно, одинаковые), а a, b, c — положительные целые числа. Кроме того, всякая греческая переменная ζ, входящая в выражения вида ($\mathcal{R}$-2), входит в правые части ($\mathcal{R}$-3) и ($\mathcal{R}$-4) только в нод-выражениях вида $\text{НОД}(a\zeta, g(\overline{y})) = b\zeta$ или $\text{НОД}(a\zeta, b\zeta) = c\zeta$.

Последнее ограничение на вид нод-выражений необходимо по следующей причине. Пусть из нод-выражения ($\mathcal{R}$-2) удалось получить равенство $l(\overline{y}) = a\zeta$. Подставим в систему (5) всюду $\frac{l(\overline{y})}{a}$ вместо ζ и домножим соответствующие нод-выражения на a. Указанные ограничения на нод-выражения с переменной ζ гарантируют, что полученная формула останется $L_{\mathcal{R}}$-формулой.

Будем называть нод-выражения $\text{НОД}(f(\overline{z},\overline{\alpha}), g(\overline{z},\overline{\alpha}) + cx) = h(\overline{z},\overline{\alpha})$ *регулярными нод-выражениями*, если линейные полиномы $f(\overline{z},\overline{\alpha})$ и $h(\overline{z},\overline{\alpha})$ имеют один из следующих видов: либо $a\zeta$ для некоторой греческой переменной ζ и положительного целого числа a, либо линейного полинома $l(\overline{z})$ с неотрицательными целыми коэффициентами и положительным свободным членом. Ввиду того, что в $L_{\mathcal{R}}$-формулах $\overline{\alpha} \geq 1 \wedge \overline{z} \geq 0$, полиномы $f(\overline{z},\overline{\alpha})$ и $h(\overline{z},\overline{\alpha})$ могут принимать только положительные значения, поэтому к системам регулярных нод-выражений можно применять НОД-лемму.

Множество формул элиминационного вида $L^x_{\mathcal{R}} \subseteq L_{\mathcal{R}}$ состоит из формул $\exists\overline{\alpha} \bigvee\limits_{j\in J_2} \widetilde{\varphi}_j(x,\overline{z_j},\overline{\alpha})$ для некоторого конечного множества индексов J_2 и формул $\widetilde{\varphi}_j(x,\overline{z},\overline{\alpha})$ вида

$$\overline{\alpha} \geq 1 \wedge \overline{z} \geq 0 \wedge x \geq 0 \wedge \widetilde{\widetilde{\varphi}}_j(\overline{z},\overline{\alpha}) \wedge \bigwedge_{i\in[1..\widetilde{m}_j]} \text{НОД}(\widetilde{f}_{i,j}(\overline{z},\overline{\alpha}), \widetilde{g}_{i,j}(\overline{z}) + c_{i,j}x) = \widetilde{h}_{i,j}(\overline{z},\overline{\alpha}), \tag{6}$$

где x не содержится в $\overline{z}$, $c_{i,j} > 0$, каждое нод-выражение с x является регулярным нод-выражением, а $\widetilde{\widetilde{\varphi}}_j(\overline{z},\overline{\alpha})$ есть система нод-выражений без вхождений x.

3. Шаг 1: отделение латинской переменной. Опустим индексы j в (5) и рассмотрим $L_{\mathcal{R}}$-формулу $\exists\overline{\alpha}\varphi(\overline{y},\overline{\alpha})$, где

$$\varphi(\overline{y},\overline{\alpha}) \rightleftharpoons \overline{\alpha} \geq 1 \wedge \overline{y} \geq 0 \wedge \bigwedge_{i\in[1..m]} \text{НОД}(f_i(\overline{y},\overline{\alpha}), g_i(\overline{y},\overline{\alpha})) = h_i(\overline{y},\overline{\alpha}). \tag{7}$$

Пусть, как и в подразделе 2.1, список $\overline{y}$ разделен на $\overline{s} = y_1, \ldots, y_l$ и $\overline{t} = y_{l+1}, \ldots, y_n$. Сформулируем два замечания.

Замечание 1. Применением ЛС-леммы к подсистеме вида $A\overline{s} = b \wedge C\overline{s} \geq d \wedge \overline{s} \geq 0$ формулы $A\overline{s} = b \wedge C\overline{s} \geq d \wedge \varphi(\overline{y}, \overline{\alpha})$ мы получаем дизъюнкцию формул $\psi_j(\overline{z}, \overline{t}, \overline{\alpha})$, таких, что $\exists \overline{\alpha} \psi_j(\overline{z}, \overline{t}, \overline{\alpha})$ является $L_{\mathcal{R}}$-формулой, и, кроме того, всякому регулярному нод-выражению в $\varphi(\overline{y}, \overline{\alpha})$ с изолированной переменной из $\overline{t}$ будет соответствовать регулярное нод-выражение в $\psi_j(\overline{z}, \overline{t}, \overline{\alpha})$.

Доказательство. Действительно, ввиду того, что в систему линейных уравнений и неравенств входит $\overline{s} \geq 0$, вместо каждой переменной из $\overline{s}$ подставляется линейное выражение $l(\overline{z})$ с неотрицательными целыми коэффициентами. Поэтому каждый линейный полином $f(\overline{y})$ с неотрицательными коэффициентами (и положительным свободным членом) сохраняет это свойство после подстановки $E^{(j)}\overline{z} + u^{(j)}$ вместо $\overline{s}$. □

Замечание 2. Можно считать, что в системе (7) нет нод-выражений вида ($\mathcal{R}$-1) и ($\mathcal{R}$-2) таких, что $k_1 f_i(\overline{y}) = k_2 g_i(\overline{y})$ для некоторых не равных одновременно нулю целых чисел k_1 и k_2.

Доказательство. Предположим, что $k_1 f_i(\overline{y}) = k_2 g_i(\overline{y})$ для $k_1 \neq 0$. В таком случае можно вычислить наибольший общий делитель и перейти к дизъюнкции по $\sigma \in \{-1, 1\}$, заменяя в (7) соответствующее нод-выражение на равенство $\sigma\text{НОД}(k_1, k_2) g_i(\overline{y}) = k_1 h_i(\overline{y}, \overline{\alpha})$. Для нод-выражений вида ($\mathcal{R}$-1) это равенство либо всегда истинно, либо может быть использовано для получения дизъюнкции систем с меньшим на единицу числом переменных, как результат применения ЛС-леммы к подсистеме $\overline{y} \geq 0 \wedge \sigma\text{НОД}(k_1, k_2) g_i(\overline{y}) = k_1 h_i(\overline{y})$ формулы (7).

Если же $h_i(\overline{y}, \overline{\alpha}) = a_i \zeta_i$, удалим $\sigma\text{НОД}(k_1, k_2) g_i(\overline{y}) = a_i k_1 \zeta_i$ из системы, подставим всюду $\sigma\text{НОД}(k_1, k_2) g_i(\overline{y})/(a_i k_1)$ вместо ζ_i и домножим линейные выражения на $a_i k_1$. В частности, вместо $\zeta_i \geq 1$ появится неравенство $\sigma\text{НОД}(k_1, k_2) g_i(\overline{y}) \geq a_i k_1$; по определению языка $L_{\mathcal{R}}$ все нод-выражения в результате подстановки снова будут иметь вид ($\mathcal{R}$-1)–($\mathcal{R}$-4). Осталось применить ЛС-лемму к подсистеме $\overline{y} \geq 0 \wedge \sigma\text{НОД}(k_1, k_2) g_i(\overline{y}) \geq a_i k_1$. □

Теперь покажем, как получить равновыполнимую в целых числах дизъюнкцию формул вида (6).

В первом случае существует латинская переменная x, которая не встречается в правой части никакого нод-выражения (7). Используя алгоритм Евклида, каждое нод-выражение вида ($\mathcal{R}$-1) или ($\mathcal{R}$-2) $\text{НОД}(f(\overline{z}) + ax, g(\overline{z}) + bx) = h(\overline{z}, \overline{\alpha})$ для $a, b \neq 0$ и линейных полиномов $f(\overline{z})$ и $g(\overline{z})$ может быть переписано таким образом, что коэффициент при x не равен нулю только в одном из полиномов. Пусть $a > b > 0$ и $a = qb + r$ для $r \in [0, b)$. Тогда имеем

$$\text{НОД}(f(\overline{z}) + ax, g(\overline{z}) + bx) = \text{НОД}(f(\overline{z}) - qg(\overline{z}) + rx, g(\overline{z}) + bx).$$

Повторяя этот шаг, получим формулу вида $\text{НОД}(\widetilde{f}(\overline{z}), \widetilde{g}(\overline{z}) + cx) = h(\overline{z}, \overline{\alpha})$. Ввиду замечания 2 полином $\widetilde{f}(\overline{z})$ не является тождественно нулевым.

В другом случае каждая латинская переменная входит в правую часть хотя бы одного нод-выражения. Выделим в (7) подсистему нод-выражений вида ($\mathcal{R}$-1) и перепишем (7) следующим образом:

$$\overline{\alpha} \geq 1 \wedge \overline{y} \geq 0 \wedge \bigwedge_{i \in [1..l]} \text{НОД}(f_i(\overline{y}), g_i(\overline{y})) = h_i(\overline{y}) \wedge \bigwedge_{i \in [l+1..m]} \text{НОД}(f_i(\overline{y}, \overline{\alpha}), g_i(\overline{y}, \overline{\alpha})) = h_i(\overline{\alpha}). \tag{8}$$

Для каждой переменной $x \in \overline{y}$ найдется индекс $i_x \in [1..l]$ такой, что эта переменная входит с ненулевым коэффициентом в $h_{i_x}(\overline{y})$ (то есть $h_{i_x}(\overline{y}) = h'_{i_x}(\overline{y}\backslash x) + c_{i_x}x$ для некоторого положительного целого c_{i_x}). По замечанию 2 случай $u_1 f_{i_x}(\overline{y}) = v_1 h_{i_x}(\overline{y})$ и $u_2 g_{i_x}(\overline{y}) = v_2 h_{i_x}(\overline{y})$ для некоторых целых u_1, v_1, u_2, v_2 невозможен, поэтому можно считать, что $u f_{i_x}(\overline{y}) \neq v h_{i_x}(\overline{y})$ для всяких целых u и v. Тогда получим, что система (7) эквивалентна следующей дизъюнкции:

$$\bigvee_{x \in \overline{y}} \left(\bigvee_{-S_x \leq k \leq S_x} \overline{\alpha} \geq 1 \wedge \Psi_{x,k}(\overline{y}) \wedge \bigwedge_{i \in [1..m] \wedge i \neq i_x} \text{НОД}(f_i(\overline{y}, \overline{\alpha}), g_i(\overline{y}, \overline{\alpha})) = h_i(\overline{y}, \overline{\alpha}) \right), \quad (9)$$

где

$$\Psi_{x,k}(\overline{y}) \rightleftharpoons \overline{y} \geq 0 \wedge \bigwedge_{x' \in \overline{y}} x \geq x' \wedge k(h_{i_x}(\overline{y})) = f_{i_x}(\overline{y})$$

и S_x есть сумма абсолютных значений коэффициентов $f_{i_x}(\overline{y})$. Это следует из того факта, что все коэффициенты $h_{i_x}(\overline{y})$ неотрицательны, $c_{i_x} > 0$, переменные $\overline{y}$ неотрицательны и x принимает максимальное значение среди переменных из $\overline{y}$.

Применение ЛС-леммы к подсистеме $\Psi_{x,k}(\overline{y})$ каждого дизъюнкта (9) даст дизъюнкцию систем вида (7), каждая из которых содержит на единицу меньшее число переменных и на единицу меньшее число нод-выражений. Ввиду замечания 1, если обозначить эту дизъюнкцию $\psi(\overline{z}, \overline{\alpha})$, мы имеем $\exists\overline{\alpha}\psi(\overline{z}, \overline{\alpha}) \in L_{\mathcal{R}}$.

На этом разбор второго случая завершается, и далее в каждой системе из $\psi(\overline{z}, \overline{\alpha})$ мы снова пытаемся отделить латинскую переменную, которая не встречается в правой части никакого нод-выражения, пока не получится дизъюнкция формул вида (6).

Теперь предположим, что искомая дизъюнкция получена. Опустим индексы j в (6) и обозначим эту формулу $\widetilde{\varphi}(x, \overline{z}, \overline{\alpha})$. Преобразуем $\exists\overline{\alpha}\widetilde{\varphi}(x, \overline{z}, \overline{\alpha})$ в равновыполнимую в целых числах дизъюнкцию формул того же вида (6), но с регулярными нод-выражениями.

Поскольку $\exists\overline{\alpha}\widetilde{\varphi}(x, \overline{z}, \overline{\alpha})$ является $L_{\mathcal{R}}$-формулой, нерегулярными могут быть лишь нод-выражения вида ($\mathcal{R}$-1) или ($\mathcal{R}$-2). Пусть нод-выражения из $\widetilde{\varphi}(x, \overline{z}, \overline{\alpha})$ с индексами $i = 1..k$ содержат все нерегулярные нод-выражения вида ($\mathcal{R}$-1), а с индексами $i = k+1..l$ все нерегулярные нод-выражения вида ($\mathcal{R}$-2), для которых положим $\widetilde{h}_i(\overline{z}, \overline{\alpha}) = a_i\zeta_i$.

Перепишем $\widetilde{\varphi}(x, \overline{z}, \overline{\alpha})$ в виде $\overline{\alpha} \geq 1 \wedge \overline{z} \geq 0 \wedge x \geq 0 \wedge \widetilde{\widetilde{\varphi}}(\overline{z}, \overline{\alpha}) \wedge \Delta(x, \overline{z}, \overline{\alpha})$, где

$$\Delta(x, \overline{z}, \overline{\alpha}) \rightleftharpoons \bigwedge_{i \in [1..k]} \text{НОД}(\widetilde{f}_i(\overline{z}), \widetilde{g}_i(\overline{z}) + c_i x) = \widetilde{h}_i(\overline{z}) \wedge \bigwedge_{i \in [k+1..l]} \text{НОД}(\widetilde{f}_i(\overline{z}), \widetilde{g}_i(\overline{z}) + c_i x) =$$
$$= a_i\zeta_i \wedge \bigwedge_{i \in [l+1..m]} \text{НОД}(\widetilde{f}_i(\overline{z}, \overline{\alpha}), \widetilde{g}_i(\overline{z}) + c_i x) = \widetilde{h}_i(\overline{z}, \overline{\alpha}),$$

и построим равновыполнимую с $\exists\overline{\alpha}\widetilde{\varphi}(x, \overline{z}, \overline{\alpha})$ формулу $\exists\overline{\alpha}\Big(\widetilde{\Phi}_0(\overline{z_0}, \overline{\alpha}) \vee \widetilde{\Phi}_1(\overline{z_1}, \overline{\alpha}) \vee \widetilde{\Phi}_2(x, \overline{z_2}, \overline{\alpha})\Big)$. Здесь $\widetilde{\Phi}_0(\overline{z_0}, \overline{\alpha})$ и $\widetilde{\Phi}_1(\overline{z_1}, \overline{\alpha})$ являются дизъюнкциями систем вида (7) таких, что список $\overline{z_0}$ содержит на две, а $\overline{z_1}$ на одну переменную меньше, чем $x, \overline{z}$. В полученных системах снова отделяем латинскую переменную, а затем добиваемся регулярности нод-выражений с изолированной переменной. Так как число латинских

переменных постоянно уменьшается, этот процесс обязательно остановится. В то же время $\widetilde{\Phi}_2(x, \overline{z_2}, \overline{\alpha})$ окажется дизъюнкцией искомого вида, то есть $\exists\overline{\alpha}\widetilde{\Phi}_2(x, \overline{z_2}, \overline{\alpha})$ будет некоторой $L^x_{\mathcal{R}}$-формулой.

Дизъюнкции $\widetilde{\Phi}_0(\overline{z_0}, \overline{\alpha})$ и $\widetilde{\Phi}_1(\overline{z_1}, \overline{\alpha})$ соответствуют случаям равенства нулю $\widetilde{f}_i(\overline{z})$: для индексов $i = 1..k$ и для $i = k+1..l$ соответственно. Построение дизъюнкций аналогично разбору двух случаев из замечания 2. Именно, $\widetilde{\Phi}_0(\overline{z_0}, \overline{\alpha}) \rightleftharpoons \bigvee\limits_{i\in[1..k]}\bigvee\limits_{\sigma\in\{-1,1\}} \Omega_{i,\sigma}(\overline{z_0}, \overline{\alpha})$ и $\widetilde{\Phi}_1(\overline{z_1}, \overline{\alpha}) \rightleftharpoons \bigvee\limits_{i\in[k+1..l]}\bigvee\limits_{\sigma\in\{-1,1\}} \Omega_{i,\sigma}(\overline{z_1}, \overline{\alpha})$, где дизъюнкции $\Omega_{i,\sigma}(\overline{z_0}, \overline{\alpha})$ и $\Omega_{i,\sigma}(\overline{z_1}, \overline{\alpha})$ будут получены с помощью ЛС-леммы.

Обозначим $\Delta_i(x, \overline{z}, \overline{\alpha})$ системы, полученные исключением из $\Delta(x, \overline{z}, \overline{\alpha})$ подвыражения с индексом $i \in [1..l]$. Тогда для $i = 1..k$ дизъюнкция $\Omega_{i,\sigma}(\overline{z_0}, \overline{\alpha})$ есть результат применения ЛС-леммы к подсистеме

$$\Phi_{i,\sigma}(x, \overline{z}, \overline{\alpha}) \rightleftharpoons \overline{z} \geq 0 \wedge x \geq 0 \wedge \widetilde{f}_i(\overline{z}) = 0 \wedge c_i x = \sigma\widetilde{h}_i(\overline{z}) - \widetilde{g}_i(\overline{z})$$

формулы $\overline{\alpha} \geq 1 \wedge \Phi_{i,\sigma}(x, \overline{z}, \overline{\alpha}) \wedge \widetilde{\widetilde{\varphi}}(\overline{z}, \overline{\alpha}) \wedge \Delta_i(x, \overline{z}, \overline{\alpha})$.

Для индексов $i = k+1..l$ обозначим $\widetilde{\Delta}_{i,\sigma}(x, \overline{z}, \overline{\alpha})$ результат подстановки $\frac{\sigma(\widetilde{g}_i(\overline{z}) + c_i x)}{a_i}$ вместо ζ_i в формулу $\overline{\alpha} \geq 1 \wedge \widetilde{\widetilde{\varphi}}(\overline{z}, \overline{\alpha}) \wedge \Delta_i(x, \overline{z}, \overline{\alpha})$ и домножения полученных выражений на a_i. Применение ЛС-леммы к подсистеме $\Phi_i(x, \overline{z}, \overline{\alpha}) \rightleftharpoons \overline{z} \geq 0 \wedge x \geq 0 \wedge \widetilde{f}_i(\overline{z}) = 0$ формулы $\Phi_i(x, \overline{z}, \overline{\alpha}) \wedge \widetilde{\Delta}_{i,\sigma}(x, \overline{z}, \overline{\alpha})$ даст нам дизъюнкцию $\Omega_{i,\sigma}(\overline{z_1}, \overline{\alpha})$. Осталось заметить, что уменьшение числа переменных в списках $\overline{z_0}$ и $\overline{z_1}$ следует из того, что полином $\widetilde{f}_i(\overline{z})$ не равен тождественно нулю для всякого $i = 1..l$.

Теперь разберем случай не равных нулю значений $\widetilde{f}_i(\overline{z})$:

$$\bigvee_{\overline{\sigma}\in\{-1,1\}^l} \Bigg(\overline{\alpha} \geq 1 \wedge \overline{z} \geq 0 \wedge x \geq 0 \wedge \widetilde{\widetilde{\varphi}}(\overline{z}, \overline{\alpha}) \wedge \bigwedge_{i\in[1..k]} \Big(\sigma_i \widetilde{f}_i(\overline{z}) \geq 1 \wedge \widetilde{h}_i(\overline{z}) \geq 1\Big) \wedge$$
$$\wedge \bigwedge_{i\in[k+1..l]} \sigma_i \widetilde{f}_i(\overline{z}) \geq 1 \wedge \bigwedge_{i\in[1..m]} \text{НОД}(\widetilde{f}_i(\overline{z}, \overline{\alpha}), \widetilde{g}_i(\overline{z}) + c_i x) = \widetilde{h}_i(\overline{z}, \overline{\alpha}) \Bigg).$$

Дизъюнкция $\widetilde{\Phi}_2(x, \overline{z_2}, \overline{\alpha})$ есть результат применения в каждом дизъюнкте этой формулы ЛС-леммы к подсистемам, содержащим все линейные уравнения и неравенства, зависящие от переменных $\overline{z}$. Из замечания 1 следует регулярность подвыражений в полученных системах.

4. Шаг 2: применение НОД-леммы. Теперь рассмотрим подсистему (6) с изолированной переменной x. Без потери общности можно считать, что все $c_{i,j}$ равны 1, поскольку мы можем вычислить $C = \underset{i=1..\widetilde{m}_j}{\text{НОК}}(c_{i,j})$, умножить каждое подвыражение на $\frac{C}{c_{i,j}}$, заменить все вхождения Cx на $\widetilde{x}$ и добавить в систему подвыражение $\text{НОД}(C, \widetilde{x}) = C$.

С помощью новых положительных целых греческих переменных $\overline{\beta}$ перепишем формулу $\exists x\widetilde{\varphi}(x, \overline{z}, \overline{\alpha})$ для $L^x_{\mathcal{R}}$-формулы $\exists\overline{\alpha}\widetilde{\varphi}(x, \overline{z}, \overline{\alpha})$, где

$$\widetilde{\varphi}(x, \overline{z}, \overline{\alpha}) \rightleftharpoons \overline{\alpha} \geq 1 \wedge \overline{z} \geq 0 \wedge x \geq 0 \wedge \widetilde{\widetilde{\varphi}}(\overline{z}, \overline{\alpha}) \wedge \bigwedge_{i\in[1..m]} \text{НОД}(f_i(\overline{z}, \overline{\alpha}), g_i(\overline{z}) + x) = h_i(\overline{z}, \overline{\alpha}), \tag{10}$$

чтобы получить эквивалентную в $\mathbb{Z}$ формулу вида $\exists\overline{\beta}\psi(\overline{z},\overline{\alpha},\overline{\beta})$ так, что $\exists\overline{\alpha}\exists\overline{\beta}\psi(\overline{z},\overline{\alpha},\overline{\beta})$ является некоторой $L_{\mathcal{R}}$-формулой. Это преобразование определит шаг 2 алгоритма квази-ЭК $\mathcal{R}$.

Обозначим $\overline{u}$ список переменных $\overline{z},\overline{\alpha}$ и рассмотрим условия (i)–(iv) НОД-леммы.

(i). В этом случае введение новых переменных не требуется. Мы получаем конъюнкцию $\bigwedge\limits_{i\in[1..m]} \text{НОД}(h_i(\overline{u}), f_i(\overline{u})) = h_i(\overline{u})$.

(ii). Для каждой упорядоченной пары (i,j), $1 \le i < j \le m$ вводится новая переменная $\zeta_{i,j}$, так что второе условие может быть записано в виде

$$\bigwedge_{1\le i<j\le m} \exists\zeta_{i,j}\left(\text{НОД}(h_i(\overline{u}),h_j(\overline{u})) = \zeta_{i,j} \wedge \text{НОД}(\zeta_{i,j}, g_i(\overline{z}) - g_j(\overline{z})) = \zeta_{i,j}\right).$$

Эта формула может быть приведена к пренексному виду, так как соответствующие переменные появляются только в одной паре нод-выражений.

(iii). Для каждой упорядоченной пары (i,j), $i,j \in [1..m]$, вводятся две новые переменные $\eta_{i,j}$ и $\theta_{i,j}$ для того, чтобы переписать $\text{НОД}(f_i(\overline{u}), h_j(\overline{u}), g_i(\overline{z}) - g_j(\overline{z})) \mid h_i(\overline{u})$ в следующем виде:

$$\exists\eta_{i,j}\exists\theta_{i,j}(\text{НОД}(f_i(\overline{u}),h_j(\overline{u})) = \eta_{i,j} \wedge \\ \wedge \text{НОД}(\eta_{i,j}, g_i(\overline{z}) - g_j(\overline{z})) = \theta_{i,j} \wedge \text{НОД}(\theta_{i,j}, h_i(\overline{u})) = \theta_{i,j}).$$

(iv). Необходимо записать тот факт, что для каждого простого числа $p \le m$ и множества индексов $I \subseteq [1..m]$ таких, что $|I| = p$, или ложно условие

$$\bigwedge_{i\in I}\left(v_p(h_i(\overline{u})) = \max_{j\in[1..m]} v_p(h_j(\overline{u})) \wedge v_p(f_i(\overline{u})) > v_p(h_i(\overline{u}))\right),$$

или найдутся такие $i,j \in I, i \ne j$, что $v_p\left(g_i(\overline{z}) - g_j(\overline{z})\right) > v_p\left(h_i(\overline{u})\right)$. Построим формулу $\Omega_{p,I}(\overline{u})$ такую, что это условие переписывается в виде следующей конъюнкции:

$$\bigwedge_{p\le m\wedge p\in\mathbb{P}}\left(\bigwedge_{I\subseteq[1..m]\wedge|I|=p} \Omega_{p,I}(\overline{u})\right),$$

где $\mathbb{P}$ есть множество простых чисел.

В первом случае множество индексов I не является подмножеством J_p. Либо не для всех $i \in I$ значение $v_p(h_i(\overline{u}))$ одинаково, либо не максимальное $\bigvee\limits_{i\in I\wedge j\in[1..m]} v_p(h_i(\overline{u})) < v_p(h_j(\overline{u}))$. Отношение $v_p(x) < v_p(y)$ выражается формулой

$$\exists\iota\left(\text{НОД}(\iota,x) = \iota \wedge \text{НОД}(p\iota,x) = \iota \wedge \text{НОД}(\iota,y) = \iota \wedge \text{НОД}(p\iota,y) = p\iota\right). \tag{11}$$

Теперь исключим множества I такие, что $\bigvee\limits_{i\in I} v_p(f_i(\overline{u})) = v_p(h_i(\overline{u}))$, так как в противном случае I не является подмножеством I_p. Для отношения равенства p-показателей $v_p(x) = v_p(y)$ используем экзистенциальную формулу

$$\exists\iota\left(\text{НОД}(\iota,x) = \iota \wedge \text{НОД}(\iota,y) = \iota \wedge \text{НОД}(p\iota,x) = \iota \wedge \text{НОД}(p\iota,y) = \iota\right). \tag{12}$$

Если ни одна из дизъюнкций не истинна (т. е. $I \subseteq I_p$), необходимо записать условие «существуют такие $i, j \in I$, $i \neq j$, что $v_p(g_i(\overline{z}) - g_j(\overline{z})) > v_p(h_i(\overline{u}))$». Объединяя дизъюнкции, получим $\Omega_{p,I}(\overline{u})$.

$$\Omega_{p,I}(\overline{u}) \rightleftharpoons \bigvee_{i\in I\wedge j\in[1..m]} v_p(h_i(\overline{u})) < v_p(h_j(\overline{u})) \vee \bigvee_{i\in I} v_p(h_i(\overline{u})) = v_p(f_i(\overline{u})) \vee \\ \vee \bigvee_{i,j\in I\wedge i\neq j} v_p(g_i(\overline{z}) - g_j(\overline{z})) > v_p(h_i(\overline{u})).$$

Введем новые греческие переменные для каждого дизъюнкта с помощью (11) и (12) и перепишем последнюю формулу в желаемом виде. На этом завершается преобразование (10) с использованием НОД-леммы. Поскольку все нод-выражения с x в (10) являются регулярными, переменные $\overline{\beta}$ могут принимать только положительные значения. Присоединением $\overline{\beta} \geq 1$ к итоговой формуле получим искомую формулу $\exists\overline{\beta}\psi(\overline{z}, \overline{\alpha}, \overline{\beta})$.

5. Теорема о сведении. Теперь мы можем доказать основную теорему. Напомним, что позитивную экзистенциальную теорию некоторой структуры S мы обозначаем $\mathrm{P}\exists\mathrm{Th}S$.

Теорема 1. *Проблема разрешимости для* $\exists\mathrm{Th}\langle\mathbb{Z}; 0, 1, +, -, \leq, \text{НОД}\rangle$ *сводится к проблеме разрешимости для* $\mathrm{P}\exists\mathrm{Th}\langle\mathbb{Z}_{>0}; 1, \{a\cdot\}_{a\in\mathbb{Z}_{>0}}, \text{НОД}\rangle$.

Доказательство. Из леммы 2 следует, что достаточно проверить выполнимость в $\mathbb{Z}$ формул вида (3). Так как (3) является $L_{\mathcal{R}}$-формулой, докажем, что шаги 1 и 2 из разделов 3 и 4 действительно определяют алгоритм квазиэлиминации кванторов $\mathcal{R}$.

То, что шаг 1 удовлетворяет определению, следует из построения.

Для шага 2, во-первых, заметим, что условие (i) вводит нод-выражения, каждое из которых имеет вид ($\mathcal{R}$-1), ($\mathcal{R}$-3) или ($\mathcal{R}$-4); при переписывании (ii) и (iii) вводятся выражения следующих видов: ($\mathcal{R}$-2), ($\mathcal{R}$-3) или ($\mathcal{R}$-4), а для условия (iv) — нод-выражения ($\mathcal{R}$-3) либо ($\mathcal{R}$-4).

Теперь проверим, что выполняются ограничения на вид нод-выражений, содержащих греческую переменную из некоторого нод-выражения вида ($\mathcal{R}$-2). Видим, что для всех (новых) греческих переменных, введенных при переписывании условий (ii) и (iii), ограничение выполняется. В то же время для всякой греческой переменной ζ, входившей в нод-выражение вида ($\mathcal{R}$-2) системы (10), появление ζ в правой части нод-выражения, полученного на шаге 2, может быть связано лишь с условием (i). Так как $\exists\overline{\alpha}\widetilde{\varphi}(x, \overline{z}, \overline{\alpha})$ является $L^x_{\mathcal{R}}$-формулой, всякое нод-выражение с x, в правой части которого находится переменная ζ, имеет вид либо $\text{НОД}(f(\overline{z}), g(\overline{z}) + x) = a\zeta$, либо $\text{НОД}(a\zeta, g(\overline{z}) + x) = b\zeta$. Следовательно, из (i) имеем нод-выражения вида $\text{НОД}(a\zeta, f(\overline{z})) = a\zeta$ либо $\text{НОД}(b\zeta, a\zeta) = b\zeta$. Таким образом, формула $\exists\overline{\alpha}\exists\overline{\beta}\psi(\overline{z}, \overline{\alpha}, \overline{\beta})$, полученная в результате выполнения шага 2, действительно является $L_{\mathcal{R}}$-формулой.

Для завершения доказательства достаточно заметить, что каждая $L^2_{\mathcal{R}}$-формула (см. определения языков $L^1_{\mathcal{R}}$ и $L^2_{\mathcal{R}}$ в [3]) является формулой вида $\exists\overline{\alpha}\left(\overline{\alpha} \geq 1 \wedge \bigvee\limits_{j\in J} \varphi_j(\overline{\alpha})\right)$ для конечного множества индексов J, где $\varphi_j(\overline{\alpha})$ есть конъюнкция атомарных формул вида $\text{НОД}(a', b') = c'$, $\text{НОД}(a', b') = c\zeta$, $\text{НОД}(a\zeta, b') = c\eta$

или НОД$(a\zeta, b\eta) = c\theta$ для некоторых положительных целых чисел a, b, c и неотрицательных целых чисел a', b', c'. Несложными преобразованиями избавимся от случаев равенства нулю a', b', c' и получим искомую P$\exists$-формулу. □

6. Заключение. Проблема разрешимости для $\exists\mathrm{Th}\langle\mathbb{Z}; 0, 1, +, -, \leq, \text{НОД}\rangle$ была сведена к проблеме разрешимости для $\mathrm{P}\exists\mathrm{Th}\langle\mathbb{Z}_{>0}; 1, \{a\cdot\}_{a\in\mathbb{Z}_{>0}}, \text{НОД}\rangle$, разрешимость которой была доказана ранее [3]. Идеи как сведения, так и доказательства разрешимости были, по существу, одинаковы: изолировать переменную и затем преобразовать формулу с помощью НОД-леммы. Для формализации этой идеи было введено понятие алгоритма квазиэлиминации кванторов и были построены алгоритмы квази-ЭК $\mathcal{R}$ и $\mathcal{D}$.

Отметим, что для доказательства разрешимости $\mathrm{P}\exists\mathrm{Th}\langle\mathbb{Z}_{>0}; 1, \{a\cdot\}_{a\in\mathbb{Z}_{>0}}, \text{НОД}\rangle$ можно было вместо применения алгоритма $\mathcal{D}$ воспользоваться разрешимостью элементарной теории структуры $\langle\mathbb{Z}_{>0}; \{a\}_{a\in\mathbb{Z}_{>0}}, \cdot, =\rangle$. Доказательство разрешимости этой теории проводится несложным сведением [6] к арифметике Сколема $\mathrm{Th}\langle\mathbb{Z}_{>0}; \cdot, =\rangle$, разрешимость которой показал в 1952 г. А. Мостовский [7]. Видим, что ввиду выразимости отношения НОД с помощью формулы

$$\text{НОД}(x, y) = z \Leftrightarrow z \mid x \wedge z \mid y \wedge \forall t(t \mid x \wedge t \mid y \Rightarrow t \mid z),$$

где $x \mid y \rightleftharpoons \exists z(y = z \cdot x)$, разрешимой оказывается элементарная теория структуры $\langle\mathbb{Z}_{>0}; 1, \{a\cdot\}_{a\in\mathbb{Z}_{>0}}, \text{НОД}\rangle$.

Шаг 1 алгоритма $\mathcal{R}$ значительно упрощается в случае, когда отношение НОД в сигнатуре заменятся на отношение взаимной простоты. В этом случае нод-выражения имеют вид либо НОД$(f(\overline{x}), g(\overline{x})) = d$ для выражений с отношением взаимной простоты, либо, для их отрицаний, НОД$(f(\overline{x}), g(\overline{x})) = a\zeta$, где $\zeta \geq 2$ и a, d — положительные целые числа, в изначальной формуле равные единице. Более того, использования греческих переменных в алгоритме $\mathcal{R}$ можно избежать, если рассматривать только P$\exists$-формулы сигнатуры $\sigma_\perp = \langle 0, 1, +, -, \neq, \text{НОД}_1, \text{НОД}_2, \ldots\rangle$, где $\text{НОД}_d(x, y) \rightleftharpoons \text{НОД}(x, y) = d$. В этом случае алгоритм может быть легко преобразован в алгоритм построения по всякой P$\exists L_{\sigma_\perp}$-формуле, эквивалентной в $\mathbb{Z}$ позитивной бескванторной $L_{\sigma_\perp}$-формулы. Подробное доказательство этого утверждения и изучение связанных вопросов выразимости и разрешимости может стать предметом другого исследования.

Автор благодарен анонимным рецензентам работы за весьма полезные замечания, способствовавшие значительному улучшению качества изложения.

Литература

1. Бельтюков А. П. Разрешимость универсальной теории натуральных чисел со сложением и делимостью. *Записки научных семинаров ЛОМИ* **60**, 15–28 (1975).

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

4. 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

5. von zur Gathen J., Sieveking M. A bound on solutions of linear integer equalities and inequalities. *Proceedings of the American Mathematical Society* **72**, iss. 1, 155–158 (1978). https://doi.org/10.2307/2042554

6. Barth D., Beck M., Dose T., Glaßer C., Michler L., Technau M. Emptiness problems for integer circuits. *Electronic Colloquium on Computational Complexity*, TR17-012 (2017). Доступно на: https://eccc.weizmann.ac.il/report/2017/012/ (дата обращения: 25.08.2021).

7. Mostowski A. On direct products of theories. *The Journal of Symbolic Logic* **17**, iss. 1, 1–31 (1952). https://doi.org/10.2307/2267454

Статья поступила в редакцию 28 августа 2020 г.;
после доработки 24 марта 2021 г.;
рекомендована в печать 17 июня 2021 г.

Контактная информация:

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

A proof of Bel'tyukov — Lipshitz theorem by quasi-quantifier elimination. II. The main reduction

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. II. The main reduction. *Vestnik of Saint Petersburg University. Mathematics. Mechanics. Astronomy*, 2021, vol. 8 (66), issue 4, pp. 608–619.
https://doi.org/10.21638/spbu01.2021.406 (In Russian)

This paper is the second part of a new proof of the Bel'tyukov — Lipshitz theorem, which states that the existential theory of the structure $\langle \mathbb{Z}; 0, 1, +, -, \leq, | \rangle$ is decidable. We construct a quasi-quantifier elimination algorithm (the notion was introduced in the first part of the proof) to reduce the decision problem for the existential theory of $\langle \mathbb{Z}; 0, 1, +, -, \leq, \mathrm{GCD} \rangle$ to the decision problem for the positive existential theory of the structure $\langle \mathbb{Z}_{>0}; 1, \{a\cdot\}_{a \in \mathbb{Z}_{>0}}, \mathrm{GCD} \rangle$. Since the latter theory was proved decidable in the first part, this reduction completes the proof of the theorem. Analogues of two lemmas of Lipshitz's proof are used in the step of variable isolation for quasi-elimination. In the quasi-elimination step we apply GCD-Lemma, which was proved in the first part.

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. 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* **8 (66)**, iss. 3, 455–466 (2021). https://doi.org/10.21638/spbu01.2021.307 (In Russian) [Engl. transl.: *Vestnik St. Petersb. Univ. Math.* **54**, iss. 3, 264–272 (2021). https://doi.org/10.1134/S1063454121030080].

4. 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

5. von zur Gathen J., Sieveking M. A bound on solutions of linear integer equalities and inequalities. *Proceedings of the American Mathematical Society* **72**, iss. 1, 155–158 (1978). https://doi.org/10.2307/2042554

6. Barth D., Beck M., Dose T., Glaßer C., Michler L., Technau M. Emptiness problems for integer circuits. *Electronic Colloquium on Computational Complexity*, TR17-012 (2017). Available at: https://eccc.weizmann.ac.il/report/2017/012/ (accessed: August 25, 2021).

7. Mostowski A. On direct products of theories. *The Journal of Symbolic Logic* **17**, iss. 1, 1–31 (1952). https://doi.org/10.2307/2267454

Received: August 28, 2020
Revised: March 24, 2021
Accepted: June 17, 2021

Author's information:

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