

УДК 510.652

ОБ ИНТЕРПРЕТАЦИЯХ АРИФМЕТИКИ ПРЕСБУРГЕРА В АРИФМЕТИКАХ БЮХИ

© 2023 г. А. А. Запругаев^{1,*}

Представлено академиком РАН Л.Д. Беклемишевым

Поступило 14.11.2022 г.

После доработки 31.01.2023 г.

Принято к публикации 03.02.2023 г.

Арифметики Бюхи \mathbf{BA}_n , $n \geq 2$, являются расширениями арифметики Пресбургера унарным функциональным символом $V_n(x)$, обозначающим наибольшую степень n , делящую x . Определимость множества в \mathbf{BA}_n эквивалентна распознаванию его конечным автоматом, принимающим числа в n -ичной записи. Мы рассматриваем интерпретации арифметики Пресбургера в стандартной модели \mathbf{BA}_n и показываем, что для всякой такой интерпретации внутренняя модель изоморфна стандартной. Это дает ответ на вопрос А. Виссера, касающийся интерпретаций некоторых слабых арифметических теорий в себя.

Ключевые слова: формальные арифметики, интерпретации, автоматные структуры, автоматные абелевы группы

DOI: 10.31857/S2686954322600641, **EDN:** XHJOFS

1. ВВЕДЕНИЕ

Арифметической теорией называется первопрядковая теория, моделью которой служат натуральные числа \mathbb{N} с некоторыми операциями над ними.

Согласно первой теореме Гёделя о неполноте, арифметика Пеано \mathbf{PA} , язык которой содержит как сложение, так и умножение, является неполной и неразрешимой теорией. В связи с этим представляет интерес изучение арифметических теорий с менее выразительным языком, для которых устанавливаются полнота и разрешимость. Такие теории называют *слабыми арифметиками*. В частности, в литературе рассматриваются *арифметика Пресбургера* $\mathbf{PrA} = \mathbf{Th}(\mathbb{N}; =, +)$ [6] и *арифметика Сколема* $\mathbf{Th}(\mathbb{N}; =, \cdot)$.

Арифметики Бюхи являются важным классом расширений арифметики Пресбургера, поскольку сохраняют свойство разрешимости и находят применение в описании множеств, принимаемых конечными автоматами.

Определение 1. Арифметикой Бюхи \mathbf{BA}_n , $n \geq 2$, называется элементарная теория $\mathbf{Th}(\mathbb{N}, =, +, V_n)$, где V_n – унарный функциональный символ такой,

что $V_n(x)$ – наибольшая степень n , делящая x . Для определенности полагаем $V_n(0) = 0$.

Серия теорий \mathbf{BA}_n была предложена Ю. Бюхи [1] в качестве инструмента для описания распознаваемости подмножеств \mathbb{N} в конечных автоматах на арифметическом языке. Эта связь явно устанавливается посредством следующего классического результата В. Брюйер [2, 3]:

Теорема 1.1. Пусть $\varphi(x_1, \dots, x_m)$ – формула в языке \mathbf{BA}_n . Тогда существует и эффективно строится автомат \mathcal{A} такой, что (a_1, \dots, a_m) принимается \mathcal{A} тогда и только тогда, когда $\mathbb{N} \models \varphi(a_1, \dots, a_m)$.

Наоборот, пусть \mathcal{A} – конечный автомат, обрабатывающий m -кортежи n -ичных натуральных чисел. Тогда существует и эффективно строится формула $\varphi(x_1, \dots, x_m)$ в языке \mathbf{BA}_n такая, что $\mathbb{N} \models \varphi(a_1, \dots, a_m)$ тогда и только тогда, когда (a_1, \dots, a_m) принимается \mathcal{A} .

Здесь подразумевается, что автомат \mathcal{A} получает на вход m -кортежи натуральных чисел в виде последовательных m -кортежей последних, затем предпоследних и т.д. цифр их n -ичной записи. Теорема Кобхэма-Семёнова [4, 5] утверждает, что для мультипликативно независимых натуральных чисел n, m (пара чисел n, m называется мультипликативно независимой, если уравнение $n^k = m^l$ не имеет решений в целых числах, кроме $k = l = 0$), всякое множество, определяемое в \mathbf{BA}_n и \mathbf{BA}_m , на

¹ Национальный исследовательский университет “Высшая школа экономики”, Москва, Россия

*E-mail: azapryagaev@hse.ru

самом деле определимо в арифметике Пресбургера PrA .

Мы рассматриваем интерпретации \mathbf{BA}_n в себя. А. Виссер поставил следующий вопрос: *если дана слабая арифметическая теория T , верно ли, что всякая интерпретация (одномерная или многомерная) T в себя изоморфна тождественной, и если так, то всегда ли возникающий изоморфизм выражим формулой T ?* Этот вопрос был положительно разрешен в случае арифметики Пресбургера PrA в работе автора с Ф. Пахомовым [7]. Поскольку арифметики Бюхи являются консервативными расширениями PrA с добавлением нового функционального символа, они являются естественным классом теорий для дальнейшего рассмотрения.

В настоящей работе мы доказываем, что даже для всякой интерпретации PrA в \mathbf{BA}_n внутренняя модель изоморфна стандартной, что дает частичный положительный ответ на вопрос Виссера. Остается открытым вопросом, обязательно ли этот изоморфизм является \mathbf{BA}_n -определимым.

Можно показать, что для всякой m -мерной интерпретации ι некоторой структуры A в \mathbf{BA}_n , существует одномерная интерпретация ι' , изоморфная ι , но не обязательно определимо. Тем самым, в многомерном случае вопрос наличия изоморфизма (но не его \mathbf{BA}_n -определимости) также разрешен положительно.

2. ПРЕДВАРИТЕЛЬНЫЕ СВЕДЕНИЯ

Мы рассматриваем одномерные непараметрические интерпретации арифметик Бюхи согласно [8, с. 20–21]. Интерпретацией ι языка первого порядка \mathcal{H} в структуре \mathfrak{B} языка \mathcal{L} называют следующую совокупность формул в языке \mathcal{L} :

1. $D_\iota(y)$, задающая множество $\mathbf{D}_\iota \subseteq \mathfrak{B}$ (область определения);
2. $P_\iota(x_1, \dots, x_n)$ для всякого предикатного символа $P(x_1, \dots, x_n)$ из \mathcal{H} ;
3. $f_\iota(x_1, \dots, x_n, y)$ для всякого функционального символа $f(x_1, \dots, x_n)$ из \mathcal{H} .

Здесь от всех f_ι требуется, чтобы они задавали график некоторой функции (по модулю интерпретации предиката равенства).

Естественным образом ι и \mathfrak{B} задают модель \mathfrak{A} языка \mathcal{H} с носителем $\mathbf{D}_\iota / \sim_\iota$, где отношение эквивалентности \sim_ι задается $=_\iota(x_1, x_2)$. \mathfrak{A} называют *внутренней моделью* \mathcal{H} .

Если к тому же $\mathfrak{A} \models T$, то ι называют *интерпретацией теории T в \mathfrak{B}* . Если для теории первого порядка U интерпретация ι является интерпретацией T вне зависимости от выбора $\mathfrak{B} \models U$, то ι называют интерпретацией теории T в U .

Мы будем рассматривать интерпретации \mathbf{BA}_n в себя. Поскольку \mathbf{BA}_n является элементарной теорией $(\mathbb{N}; =, +, V_n)$, это эквивалентно рассмотрению интерпретаций в стандартной модели \mathbf{BA}_n , т.е. \mathbb{N} . Наша задача состоит в установлении, для всякой ли интерпретации ι теории \mathbf{BA}_n получающаяся внутренняя модель изоморфна стандартной. Тем самым требуется определить, интерпретируема ли какая-либо нестандартная модель \mathbf{BA}_n в арифметике Бюхи. Порядковые типы нестандартных моделей \mathbf{BA}_n описывает следующий стандартный результат.

Теорема 2.1. *Всякая нестандартная модель $\mathfrak{A} \models \mathbf{BA}_n$ имеет порядковый тип $\mathbb{N} + \mathbb{Z} \cdot A$, где $\langle A, <_A \rangle$ – некоторый плотный линейный порядок без первой и последней точек. В частности, всякая счетная нестандартная модель \mathbf{BA}_n имеет порядковый тип $\mathbb{N} + \mathbb{Z} \cdot \mathbb{Q}$.*

Забывая о $V_n(x)$, становится возможным рассматривать интерпретацию нестандартной модели \mathbf{BA}_n в арифметике Бюхи как интерпретацию одного сложения (т.е., интерпретацию арифметики Пресбургера PrA). Согласно теореме 1.1, всякая интерпретация произвольной структуры A в \mathbf{BA}_n является ее автоматным представлением; в частности, интерпретация $(\mathbb{N}; =, +)$ индуцирует автоматный моноид в качестве своей внутренней модели.

Следующее необходимое условие для автоматных групп установили Браун и Штрюнгманн [9, теорема 10].

Теорема 2.2. *Пусть $(A, +)$ – автоматная абелева группа без кручения. Тогда в A существует подгруппа B , изоморфная \mathbb{Z}^m для некоторого m такая, что факторгруппа $C = A/B$ является прямой суммой конечного числа групп вида $\mathbb{Z}(p^\infty)$. В частности, порядки элементов C могут делиться лишь на конечный список различных простых p_1, \dots, p_s .*

Понятно, что внутренняя модель, индуцируемая интерпретацией PrA , является не абелевой группой, а лишь моноидом, поскольку ни один из элементов, кроме нуля, не наделен аддитивным обратным. Однако это легко исправить, введя отрицательные числа отдельно и определив покомпонентное сложение. Тем самым, всякая интерпретация PrA в \mathbf{BA}_n на самом деле порождает интерпретацию соответствующей абелевой группы.

Лемма 2.1. Пусть PrA интерпретируется в \mathbf{BA}_n посредством интерпретации ι . Тогда она продолжается до интерпретации упорядоченной абелевой группы таким образом, что интерпретация PrA соответствует неотрицательным целым числам.

3. ТЕОРЕМА И ДОКАЗАТЕЛЬСТВО

Лемма 3.1. Пусть ι — интерпретация PrA в стандартной модели \mathbb{N} арифметики Бюхи \mathbf{BA}_n . Тогда внутренняя модель \mathcal{A} , индуцированная ι , изоморфна тождественной.

Доказательство. Предположим противное. Пусть ι — такая интерпретация PrA , что внутренняя модель нестандартна. Поскольку \mathbb{N} счетна, по теореме 2.1 получаем, что порядковый тип внутренней модели равен $\mathbb{N} + \mathbb{Z} \cdot \mathbb{Q}$.

Применяя лемму 2.1, можем перейти к интерпретации ι' упорядоченной абелевой группы \mathcal{B} , порядковый тип которой изоморфен $\mathbb{Z} \cdot \mathbb{Q} + \mathbb{Z} + \mathbb{Z} \cdot \mathbb{Q} = \mathbb{Z} \cdot \mathbb{Q}$.

Поскольку порядковый тип упорядоченной абелевой группы \mathcal{B} равен $\mathbb{Z} \cdot \mathbb{Q}$, можно рассматривать галактики, т.е. множества вида $[c] := \{d \in \mathcal{B} \mid |c - d| \text{ — стандартное натуральное число}\}$. В частности, стандартные целые числа являются одной из галактик, а именно содержащей нуль (нейтральный элемент \mathcal{B}). Стандартным образом, по аналогии с доказательством теоремы 2.1, устанавливается следующая

Лемма 3.1. Сложение на галактиках $[c + d] := [c] + [d]$, а также порядок $[c] < [d] \stackrel{\text{def}}{=} c < d \wedge [c] \neq [d]$, корректно определены.

Иными словами, на множестве \mathcal{B}/\mathbb{Z} , где \mathbb{Z} — стандартные целые числа, индуцируется структура группы, упорядоченной в соответствии с индуцированным порядком. Более того, выполнена следующая лемма:

Лемма 3.2. \mathcal{B}/\mathbb{Z} содержит подгруппу \mathcal{Q} , изоморфную $(\mathbb{Q}, +)$.

Доказательство. Зафиксируем произвольную положительную нестандартную галактику $[c]$. Мы определим изоморфизм $\varphi : \mathbb{Q} \rightarrow \mathcal{B}/\mathbb{Z}$ следующим образом. Для всякого $n \in \mathbb{Z}$ положим $\varphi(n) := [nc]$. Согласно лемме 3.1, это корректно определенное вложение \mathbb{Z} в \mathcal{B}/\mathbb{Z} .

Пусть теперь k/l — рациональное число. Зададим $\varphi(k/l)$ как такую галактику $[x]$, что $l \cdot x = kc + t$ для некоторого стандартного t . Поскольку в арифметике Пресбургера ровно одно из чисел $kc, kc + 1,$

$\dots, kc + l - 1$ всегда делится l , такие t и x всегда возможно подобрать. Теперь покажем, что определение $\varphi(k/l)$ корректно.

Класс $[x]$ не зависит от выбора t . В самом деле, пусть t и t' — разные стандартные числа, и $lx = kc + t, lx' = kc + t'$. Тогда $l(x - x') = (t - t')$ — стандартное число. Поэтому $x - x'$ стандартно, откуда $[x] = [x']$.

Класс $[x] = \varphi(k/l)$ не зависит от представления k/l . Пусть $k_1/l_1 = k_2/l_2$, т.е., $l_2k_1 = l_1k_2$, и $\varphi(k_i/l_i) = [x_i], i = 1, 2$. Это означает, что $l_i \cdot x_i = k_i c + t_i$. Поэтому

$$l_1 l_2 (x_1 - x_2) = (l_2 k_1 - l_1 k_2) c + (l_2 t_1 - l_1 t_2) = l_2 t_1 - l_1 t_2.$$

Поскольку $l_2 t_1 - l_1 t_2$ стандартно, $x_1 - x_2$ тоже стандартно, и $[x_1] = [x_2]$.

Сложение согласовано со сложением на \mathbb{Q} . Пусть $k_1/l_1, k_2/l_2 \in \mathbb{Q}$, и $\varphi(k_i/l_i) = [x_i], i = 1, 2$. В \mathbb{Q} мы имеем $k_1/l_1 + k_2/l_2 = (k_1 l_2 + k_2 l_1)/l_1 l_2$. Пусть y — такой элемент \mathcal{B}/\mathbb{Z} , что для некоторого t выполнено $l_1 l_2 y = k_1 l_2 c + k_2 l_1 c + t$. Требуется показать, что $[x_1] + [x_2] = [y]$. Запишем $l_i \cdot x_i = k_i c + t_i$. Умножая равенства на l_2 и l_1 соответственно и складывая, получаем

$$l_1 l_2 (x_1 + x_2) = k_1 l_2 c + k_2 l_1 c + (l_1 t_2 + l_2 t_1).$$

Следовательно, $y - (x_1 + x_2) = t - (l_1 t_2 + l_2 t_1)$, что является стандартным числом φ инъективно. Пусть $k_1/l_1 \neq k_2/l_2, \varphi(k_i/l_i) = [x_i], i = 1, 2$. Нужно показать, что $[x_1] \neq [x_2]$. Предположим, что $[x_1] = [x_2]$. Тогда $x_1 - x_2$ стандартно. Но в таком случае $[0] = [x_1 - x_2] = \varphi(k_1/l_1 - k_2/l_2)$, где $k_1/l_1 - k_2/l_2$ — ненулевое рациональное число. По определению это означает, что $0 = (k_1 l_2 - l_1 k_2) c + t$ для некоторого t . Но t — стандартно, а $(k_1 l_2 - l_1 k_2) c$ — нет, поэтому указанное равенство невозможно. Доказательство леммы завершено.

Вернемся к доказательству Теоремы 3.1 и покажем, что \mathcal{B} не может быть автоматной. Предположим противное: пусть \mathcal{B} автоматна. Тогда она удовлетворяет условиям Теоремы 2.2. Таким образом, в \mathcal{B} существует подгруппа \mathcal{E} , изоморфная \mathbb{Z}^m , такая, что $\mathcal{F} = \mathcal{B}/\mathcal{E}$ — группа кручения, и порядки всех ее элементов делятся только на простые из списка p_1, \dots, p_s . Мы покажем, что это противоречит лемме 3.2 о существовании подгруппы $\mathcal{Q} \subseteq \mathcal{B}/\mathbb{Z}$, изоморфной \mathbb{Q} . Далее под \mathbb{Z} понимается конкретная подгруппа стандартных целых чисел в \mathcal{B} .

Пусть $\mathcal{G} = \langle \mathbb{Z}, \mathcal{E} \rangle$ – подгруппа \mathcal{B} , порожденная \mathbb{Z} и \mathcal{E} , и $\pi: \mathcal{B}/\mathbb{Z} \rightarrow \mathcal{B}/\mathcal{G}$ – естественный сюръективный гомоморфизм, переводящий всякий из классов эквивалентности в содержащий его класс из \mathcal{B}/\mathcal{G} . Рассмотрев цепочку сюръективных гомоморфизмов $\mathcal{B} \xrightarrow{\rho} \mathcal{B}/\mathbb{Z} \xrightarrow{\pi} \mathcal{B}/\mathcal{G}$, мы видим, что $\mathcal{G} = \text{Ker}(\pi \circ \rho) = \rho^{-1}(\text{Ker}(\pi))$, откуда $\text{Ker}(\pi) = \mathcal{G}/\mathbb{Z}$.

Теперь установим образ Q под действием π . В общем случае, если имеется сюръективный гомоморфизм между группами $\sigma: A \rightarrow B$ и S – подгруппа A , то выполнено $\sigma(S) \cong S/(S \cap \text{Ker}(\sigma))$. В самом деле, два элемента $a, b \in S$ попадают в один и тот же класс $S/(S \cap \text{Ker}(\sigma))$ тогда и только тогда, когда $(a - b) \in \text{Ker}(\sigma)$, что эквивалентно $\sigma(a) = \sigma(b)$. В нашем случае, находим, что $\pi(Q) \cong Q/(Q \cap \text{Ker}(\pi)) = Q/(Q \cap \mathcal{G}/\mathbb{Z})$.

Группа \mathcal{G}/\mathbb{Z} конечно порождена как факторгруппа конечно порожденной. Она не обязательно свободна, но, согласно теореме о классификации конечно порожденных абелевых групп, может быть представлена в виде прямой суммы \mathbb{Z}^r для некоторого r и компонента кручения $T = \mathbb{Z}_{q_1} \oplus \dots \oplus \mathbb{Z}_{q_r}$. Поскольку $Q \cap T = \{0\}$, имеем $Q/(Q \cap \mathcal{G}/\mathbb{Z}) \cong Q/\mathbb{Z}^r$. Следующая лемма показывает, что Q/\mathbb{Z}^r изоморфно $Q/h\mathbb{Z}$ для некоторого рационального h :

Лемма 3.3. Множество, порожденное в $(\mathbb{Q}, +)$ набором элементов

$$\{(k_1/l_1, \dots, k_r/l_r) \in \mathbb{Q} \setminus \{0\}\},$$

изоморфно \mathbb{Z} и может быть порождено единственным $d/(l_1 \dots l_r)$, где $d := \text{НОД}(k_1 l_2 l_3 \dots l_r, l_1 k_2 l_3 \dots l_r, \dots, l_1 l_2 \dots k_r)$.

Доказательство. Приведем дроби к общему знаменателю:

$$k_i/l_i = (l_1 \dots k_i \dots l_r)/(l_1 \dots l_r).$$

Для d из формулировки леммы согласно алгоритму Евклида существует представление в виде линейной комбинации $a_1 \cdot k_1 l_2 l_3 \dots l_r + a_2 \cdot l_1 k_2 l_3 \dots l_r + \dots + a_r \cdot l_1 l_2 \dots k_r = d$, причем любая линейная комбинация с другими коэффициентами равна кратному d . Поэтому $a_1 \cdot k_1/l_1 + \dots + a_r \cdot k_r/l_r = d/(l_1 \dots l_r)$, и всякая прочая линейная комбинация равна кратному $d/(l_1 \dots l_r)$.

Итак, $\mathbb{Q}/\mathbb{Z}^r = \mathbb{Q}/h\mathbb{Z}$, где $h := d/(l_1 \dots l_r)$ найдено в доказательстве Леммы 3.3. Пусть q – простое, отсутствующее в списке p_1, \dots, p_s . Тогда элемент $[h/q] \in \mathbb{Q}/(Q \cap \mathcal{G}/\mathbb{Z}) \subseteq \mathcal{B}/\mathcal{G}$ имеет в точности порядок q . Однако, поскольку $\mathcal{F} = \mathcal{B}/\mathcal{E}$ является группой кручения с ограничением на порядки элементов, это же выполнено и для \mathcal{B}/\mathcal{G} , где отождествлено больше элементов. Следова-

но, мы указали элемент \mathcal{B}/\mathcal{G} с порядком, разложение которого не ограничено p_1, \dots, p_s . Противоречие с Теоремой 2.2.

БЛАГОДАРНОСТИ

Автор благодарен Л.Д. Беклемишеву за предложение темы для исследования и многочисленные полезные обсуждения.

ИСТОЧНИК ФИНАНСИРОВАНИЯ

Исследование осуществлено в рамках Программы фундаментальных исследований НИУ ВШЭ.

СПИСОК ЛИТЕРАТУРЫ

1. Büchi J.R. Weak second-order arithmetic and finite automata // *Mathematical Logic Quarterly*. 1960. V. 6. № 1–6. P. 66–92. <https://doi.org/10.1002/malq.19600060105>
2. Bruyère V. Entiers et automates finis // *Mémoire de fin d'études*, Université de Mons (1985).
3. Bruyère V. et al. Logic and p-recognizable sets of integers // *Bulletin of the Belgian Mathematical Society Simon Stevin*. 1994. V. 1. № 2. P. 191–238. <https://doi.org/10.36045/bbms/1103408547>
4. Cobham A. On the base-dependence of sets of numbers recognizable by finite automata // *Mathematical systems theory*. 1969. V. 3. № 2. P. 186–192. <https://doi.org/10.1007/BF01746527>
5. Семёнов А.Л. Пресбургеровость предикатов, регулярных в двух системах счисления // *Сибирский математический журнал*. 1977. Т. 18. № 2. С. 403–418. <https://doi.org/10.1007/BF00967164>
6. Presburger M. Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt // *Comptes Rendus du I congrès de Mathématiciens des Pays Slaves* 92–101, 1929.
7. Pakhomov F., Zapryagaev A. Multi-dimensional interpretations of Presburger arithmetic in itself // *Journal of Logic and Computation*. 2020. V. 30. № 8. P. 1681–1693. <https://doi.org/10.1093/logcom/exaa050>
8. Tarski A., Mostowski A., Robinson R.M. Undecidable theories. North-Holland, 1953. 98 p.
9. Braun G., Strüningmann L. Breaking up finite automata presentable torsion-free abelian groups // *International Journal of Algebra and Computation*. 2011. V. 21. № 08. P. 1463–1472. <https://doi.org/10.1142/S0218196711006625>

ON INTERPRETATIONS OF PRESBURGER ARITHMETIC IN BÜCHI ARITHMETICS

A. A. Zapryagaev^a

^a National Research University "Higher School of Economics", Moscow, Russian Federation

Presented by Academician of the RAS L.D. Beklemishev

Büchi arithmetics \mathbf{BA}_n , $n \geq 2$, are extensions of Presburger arithmetic with an unary functional symbol $V_n(x)$ denoting the largest power of n that divides x . Definability of a set in \mathbf{BA}_n is equivalent to its recognizability by a finite automaton receiving numbers in their n -ary expansion. We consider the interpretations of Presburger Arithmetic in the standard model of \mathbf{BA}_n and show that each such interpretation has an internal model isomorphic to the standard one. This answers a question by A. Visser on the interpretations of certain weak arithmetical theories in themselves.

Keywords: formal arithmetics, interpretations, automatic structures, automatic abelian groups