Компьютерные инструменты в образовании, 2018
№ 6: 5–15
УДК: 510.652
http://ipo.spb.ru/journal
doi:10.32603/2071-2340-2018-6-5-15

информатика

НЕКОТОРЫЕ ПРОБЛЕМЫ РАЗРЕШИМОСТИ И ВЫРАЗИМОСТИ ДЛЯ ПРЕДИКАТА ДЕЛИМОСТИ НА ДВА ПОСЛЕДОВАТЕЛЬНЫХ ЧИСЛА

Старчак М. Р.

Санкт-Петербургский государственный университет, Санкт-Петербург, Россия

Аннотация

Предикат делимости на два последовательных числа $DW(x,y) \rightleftharpoons x \mid y \wedge 1+x \mid y$ был предложен Л. ван ден Дрисом и А. Уилки в работе, посвященной изучению свойств подмножеств натуральных чисел, экзистенциально выразимых с помощью единицы, сложения и делимости.

В настоящей работе доказывается неразрешимость множества истинных в натуральных числах экзистенциальных формул, записанных с помощью только DW и умножения, а также выразимость всех арифметических предикатов с помощью только сложения и DW или только DW и делимости. Кроме того, получены некоторые результаты о выразимости для DW и отношения порядка.

Ключевые слова: *делимость на два последовательных числа, арифметическая выразимость, экзистенциальная теория натуральных чисел со сложением и делимостью, алгоритмическая разрешимость, слабые арифметики.*

Цитирование: Старчак М. Р. Некоторые проблемы разрешимости и выразимости для предиката делимости на два последовательных числа // Компьютерные инструменты в образовании. 2018. № 6. С. 5–15. doi:10.32603/2071-2340-2018-6-5-15

Благодарности: *Автор благодарен Косовскому Николаю Кирилловичу за постановку задачи.*

1. ВВЕДЕНИЕ

Известный результат о разрешимости экзистенциальной арифметики с единицей, сложением и делимостью, независимо полученный А. П. Бельтюковым [1] и Л. Липшицем [2], естественно ставит вопрос о сложности проблемы распознавания формул этой теории. Будем обозначать эту теорию $\exists\mathrm{Th}\langle\mathbb{N};1,+,|\rangle$, а более подробно об обозначениях будет сказано в конце данного раздела.

Задача NP-трудна, ибо включает в себя экзистенциальную арифметику со сложением и единицей. Более того, при условии, что коэффициенты линейных выражений имеют двоичную запись,она является NP-трудной уже при некотором фиксированном числе делимостей и переменных, как было показано Л. Липшицем в [3]. В работе [4] было показано, что для всякой выполнимой в неотрицательных целых числах бесквантворной фор-

мулы $\varphi(x_1,...,x_n)$ сигнатуры $\langle 1,+,|\rangle$ найдётся такой выполняющий набор значений переменных, длина записи которого для некоторого фиксированного полинома $poly$ ограничена сверху $2^{poly(|\varphi(x_1,...,x_n)|)}$. Как обычно, будем обозначать $|\varphi(x_1,...,x_n)|$ длину записи формулы $\varphi(x_1,...,x_n)$, предполагая двоичную запись натуральных коэффициентов линейных выражений в формуле. Получаем, что задача, во всяком случае, лежит в классе **NEXPTIME**. Более точной оценки временной сложности этой проблемы на данный момент не известно.

Результат Бельтюкова и Липшица нашёл широкое применение в компьютерных науках. Укажем только некоторые недавние работы. Сведением к проблеме распознавания формул $\exists\mathrm{Th}\langle\mathbb{N};1,+,|\rangle$ в [5, Lemma 4.2.2] была доказана разрешимость проблемы достижимости для параметрической односчётчиковой машины (П1СМ). Более того, имеет место и обратная сводимость [5, Lemma 4.2.1]. Установлению связей между проблемами достижимости для П1СМ и для некоторых разновидностей параметрических временных автоматов посвящена работа [6]. Отметим, что в обоих случаях алгоритмическая сложность соответствующих проблем зависит от решения вопроса о сложности $\exists\mathrm{Th}\langle\mathbb{N};1,+,|\rangle$ (см., например, заключение в [6]).

Изучению подмножеств $S\subseteq\mathbb{N}^n$, экзистенциально выразимых с помощью формул рассматриваемой сигнатуры, посвящена работа Л. ван ден Дриса и А. Уилки [7]. В ней указанные множества называются множествами делимости (*divisibility sets*), если выражающая формула бескванторная, и множествами субделимости (*subdivisibility sets*), если формула содержит кванторы. В частности, ими было показано (Corollary 1.3), что если график некоторой функции $f: S\to\mathbb{N}$ для $S\subseteq\mathbb{N}^n$ является множеством субделимости, то найдётся $c\geq 1$, такое что для всякого ненулевого набора $(x_1,...,x_n)\in S$ $f(x_1,...,x_n)\leq c(x_1+...+x_n)$. С другой стороны (см. Corollary 1.6), для всякой неограниченной функции f найдётся такое вещественное $c\in(0,1)$, что для бесконечного числа наборов $(x_1,...,x_n)\in S$ $f(x_1,...,x_n)>(x_1+...+x_n)^c$. Кроме того, в заключительном примечании в [7, с. 526] приводится простой пример, показывающий, что невозможно улучшить нижнюю оценку до линейной. Именно, достаточно рассмотреть предикат $DW(x,y)\rightleftharpoons x\mid y\wedge 1+x\mid y$ и функцию, с его помощью определяемую,

$$f(x,y)=\begin{cases}x, & x>0\wedge y>0\wedge DW(x,y)\\ 0, & \text{иначе}\end{cases}. \tag{1.1}$$

Несложно увидеть, что $f(x,y)$ является неограниченной функцией, для которой $f(x,y)<(x+y)^{\frac{1}{2}}$ для любых $(x,y)\in\mathbb{N}^2$.

В действительности предикат DW использовал уже Липшиц в [3] для установления неразрешимости всякой формулы всё той же сигнатуры $\langle 1,+,|\rangle$, но с кванторной приставкой вида $\exists x_1...\exists x_n\forall y$. Авторам [4] этот предикат служит для демонстрации того факта, что верхняя оценка на наименьший выполняющий набор для выполнимой в натуральных числах формулы не может быть улучшена. Действительно, для истинности формулы

$$\bigwedge_{i=1}^{m} DW(x_{i-1},x_i)\wedge x_i\neq 0 \tag{1.2}$$

необходимо, чтобы $x_0\geq 1$, $x_1\geq x_0^2+x_0\geq 2$, ..., $x_m\geq x_{m-1}^2+x_{m-1}\geq 2^{2^{m-1}}$. Таким образом, $|x_m|\geq 2^{m-1}$, из чего следует, что невозможно понизить до полиномиальной верхнюю оценку на длину записи выполняющего набора.

Заметим, что, даже заменив в сигнатуре сложение на функтор S, такой что $Sx = x + 1$, ввиду указанного примера, экспоненциальную верхнюю оценку на длину записи выполняющего набора улучшить нельзя.

В [8] показано, что NP-трудной будет уже проблема распознавания формул теории $\exists\mathrm{Th}\langle\mathbb{N}; S, \perp\rangle$, подкванторные выражения которых суть конъюнкции атомарных формул или их отрицаний. Здесь $x \perp y$ есть предикат взаимной простоты натуральных чисел x и y, экзистенциально выразимый вместе со своим отрицанием, с помощью S и делимости. Так как выражение $x = 0$ эквивалентно $DW(x, x)$ (будем считать, что $0 \mid 0$, полагая формально $x \mid y \rightleftharpoons \exists z(y = z \cdot x)$), для записи формулы 1.2 достаточно только предиката DW. Таким образом, полезно было бы отдельно изучить этот предикат в смысле выразимости с его помощью арифметических предикатов, разрешимости некоторых связанных с этим предикатом теорий, таких как $\exists\mathrm{Th}\langle\mathbb{N}; \cdot, DW\rangle$, а также сложности проблем распознавания для теорий $\exists\mathrm{Th}\langle\mathbb{N}; DW\rangle$ и $\exists\mathrm{Th}\langle\mathbb{N}; S, DW\rangle$. В настоящей работе будут рассмотрены только первые два вопроса, а алгоритмическая сложность проблем распознавания для указанных теорий должна стать предметом отдельной статьи.

Опишем основные понятия, используемые в формулировках и доказательствах утверждений.

Для всякой формулы языка первого порядка L_σ некоторой сигнатуры σ в качестве носителя интерпретации будет использоваться множество натуральных чисел $\mathbb{N} = \{0, 1, 2, ...\}$, а всякому функциональному и предикатному символу будет сопоставляться естественным образом определяемая функция и предикат. Например, символу S ставится в соответствие функция $f_S : \mathbb{N} \to \mathbb{N}$, такая что $f_S(x) = x + 1$. Если некоторая формула $\Phi(x_1, ..., x_n)$ языка L_σ выражает в такой интерпретации n-местное отношение R, будем говорить, что «R выразимо в структуре $\langle\mathbb{N}; \sigma\rangle$». Экзистенциальной формулой языка L_σ назовём формулу вида $\exists y_1 ... \exists y_m \varphi(x_1, ..., x_n, y_1, ..., y_m)$, где $\varphi(x_1, ..., x_n, y_1, ..., y_m)$ — бесквантворная формула. Отношение называется экзистенциально выразимым в структуре $\langle\mathbb{N}; \sigma\rangle$, если существует экзистенциальная формула L_σ, его выражающая. Элементарной теорией структуры $\langle\mathbb{N}; \sigma\rangle$ называется множество всех истинных в $\mathbb{N}$ замкнутых формул языка L_σ и обозначается $\mathrm{Th}\langle\mathbb{N}; \sigma\rangle$. Экзистенциальная теория $\exists\mathrm{Th}\langle\mathbb{N}; \sigma\rangle$ есть, соответственно, множество всех истинных замкнутых зкзистенциальных формул языка L_σ. Теория структуры $\langle\mathbb{N}; \sigma\rangle$ называется разрешимой, если существует алгоритм, определяющий по всякой формуле L_σ, принадлежит ли она данной теории или нет.

В своеобразной энциклопедии результатов по арифметической выразимости [9] используется удобное для формулировки результатов понятие полноты по выразимости некоторой структуры. Именно, для любых арифметических предикатов $X_1, ..., X_n$ (то есть выразимых в структуре $\langle\mathbb{N}; +, \cdot, =\rangle$) структура $\langle\mathbb{N}; X_1, ..., X_n\rangle$ называется *полной по выразимости* (def-полной), если в ней выразимы графики функций сложения и умножения (трёхместные предкаты $x + y = z$ и $x \cdot y = z$).

Изложенные в статье результаты можно разделить на две части. В первой исследуются вопросы разрешимости и выразимости для предиката DW и функции умножения. Доказана def-полнота $\langle\mathbb{N}; DW, |\rangle$, а также неразрешимость теории $\exists\mathrm{Th}\langle\mathbb{N}; \cdot, DW\rangle$, в то время как известна разрешимость теорий $\mathrm{Th}\langle\mathbb{N}; \cdot, |\rangle$ и $\exists\mathrm{Th}\langle\mathbb{N}; DW, |\rangle$. Во второй части из доказательства def-полноты $\langle\mathbb{N}; +, DW\rangle$ будет следовать неразрешимость $\exists\forall\mathrm{Th}\,\langle\mathbb{N}; 1, +, \leq, DW\rangle$. Завершается статья некоторыми результатами о выразимости в терминах отношения порядка $x < y$ и DW.

Рассматриваемые вопросы входят в контекст исследований по так называемым слабым арифметикам (Weak Arithmetics). С ключевыми результатами и направлениями развития этой области можно ознакомиться по обзорной статье Д. Ришара [10].

2. ПРЕДИКАТ DW И АРИФМЕТИЧЕСКИЕ ПРЕДИКАТЫ, ВЫРАЗИМЫЕ С ПОМОЩЬЮ УМНОЖЕНИЯ

Определим сначала некоторые простые предикаты, выразимые с помощью только $DW(x,y)$.

Лемма 1. Свойства $x=0$, $x=1$ и отношение $x=y$ выразимы в структуре $\langle\mathbb{N};DW\rangle$.

Доказательство. $x=0 \Leftrightarrow DW(x,x)$. $x=1 \Leftrightarrow \forall y\forall z(DW(z,y)\Rightarrow DW(x,y))$. Действительно, если $y=2$ и $z=1$, то необходимо, чтобы $x=1$, в то время как для всяких y, для которых $DW(z,y)$ при некотором z, формула $DW(1,y)$ всегда истинна. Наконец, $x=y \Leftrightarrow \forall z(DW(x,z)\Longleftrightarrow DW(y,z))$. В случае $x=0$ и $y>0$ достаточно рассмотреть $z=y(y+1)$, если же оба аргумента положительны и, например, $x<y$, то возьмём $z=x(x+1)$. □

Рассмотрим вопросы разрешимости теорий с DW и арифметическими предикатами, выразимыми с помощью только умножения и равенства.

Теорема 1. Структура $\langle\mathbb{N};DW,|\rangle$ def-полна.

Доказательство. По известной теореме Дж. Робинсон, структура $\langle\mathbb{N};S,|\rangle$ def-полна (см. [9, 11]). Поэтому достаточно определить отношение $y=Sx$.

Отношение $x\perp y$ выразимо с помощью $\forall t(t\mid x\wedge t\mid y\Rightarrow t=1)$. Тогда получаем следующее определение: $y=Sx \Leftrightarrow (x=0\wedge y=1)\vee(\neg x=0\wedge x\perp y\wedge\forall z(DW(x,z)\Leftrightarrow x\mid z\wedge y\mid z))$. Импликация вправо очевидна, покажем, что импликация верна в обратную сторону. Если $x\neq 0$, то для $z=x(x+1)$, ввиду того, что $y\mid z$ и $x\perp y$, необходимо $y\neq 0$ и $y\mid Sx$, следовательно, $0<y\leq Sx$. Если предположить, что $y<Sx$, то получим противоречие для $z=x$, так как $x\cdot y<x(x+1)$. □

Как элементарная теория с делимостью $\mathrm{Th}\langle\mathbb{N};|\rangle$, так и элементарная теория с взаимной простотой $\mathrm{Th}\langle\mathbb{N};\perp\rangle$ разрешимы. Это следует из выразимости этих предикатов с помощью умножения и равенства (делимость — по определению; предикат взаимной простоты – по формуле из доказательства Теоремы 1 и $x=1 \Leftrightarrow \forall y(x\cdot y=y)$) и разрешимости арифметики Сколема $\mathrm{Th}\langle\mathbb{N};\cdot,=\rangle$, доказанной А. Мостовским в [12]. Для предиката $DW(x,y)$ имеем следствие Теоремы 1.

Следствие. Отношение $DW(x,y)$ нельзя выразить в структуре $\langle\mathbb{N};\cdot,=\rangle$.

Если теперь обратиться к только экзистенциальным теориям, то разрешимость $\exists\mathrm{Th}\langle\mathbb{N};|,DW\rangle$ очевидна, ввиду того, что всякая формула этой теории принадлежит разрешимой теории $\exists\mathrm{Th}\langle\mathbb{N};1,+,|\rangle$. Исследуем вопрос о разрешимости $\exists\mathrm{Th}\langle\mathbb{N};\cdot,DW\rangle$. В первую очередь, хотелось бы получить экзистенциальные выражения для $x=1$, $x=y$ в $\langle\mathbb{N};\cdot,DW\rangle$. Для этого понадобится следующая лемма.

Лемма 2. Для всяких целых чисел $x\geq 1$ и $y\geq 0$ выполняется $y(x+1)+1\mid x^2 \Leftrightarrow y=0\vee y=x-1$.

Доказательство. Импликация влево очевидна, докажем её в обратную сторону.

Ясно, что $y=0$ удовлетворяет делимости, и, кроме того, необходимо, чтобы $y\in[0,x-1]$. Пусть $y=x-k$ для некоторого $k\in[1,x)$. Тогда для левой части эквивалентности из условия леммы имеем

$$y(x+1)+1\mid x^2 \Leftrightarrow \exists k(y(y+k+1)+1\mid(y+k)^2\wedge y=x-k). \tag{2.1}$$

Делимость из подкванторного выражения перепишем, вычитая из правого аргумента левый. Вынесем сразу в получающемся выражении $(k-1)y+k^2-1$ множитель $k-1$.

$$y(y+k+1)+1\mid(y+k)^2 \Leftrightarrow y(y+k+1)+1\mid(k-1)(y+k+1).$$

Так как $y > 0$, то, во-первых, $y(y+k+1)+1 \perp y+k+1$, а значит, $y(y+k+1)+1 \mid k-1$, а во-вторых, $y(y+k+1)+1 > k+1$, поэтому $k = 1$ и $y = x-1$, что и завершает доказательство леммы. □

Заметим, что в Лемме 1 было получено бесквантворное выражение для $x = 0$. Далее, имеет место лемма.

Лемма 3. Свойства $x \neq 1$, $x = 1$ и отношения $x = y$, $y = x^2 - 1$, $x \mid y$ экзистенциально выразимы в структуре $\langle \mathbb{N}; \cdot, DW \rangle$.

Доказательство. Для первого предиката можно воспользоваться отрицанием формулы для $x = 1$ из Леммы $1 x \neq 1 \Leftrightarrow \exists y \exists z (DW(z, y) \wedge \neg DW(x, y))$. Далее, из Леммы 2 следует, что

$$x > 1 \wedge y > 1 \wedge y = x^2 - 1 \Leftrightarrow x \neq 0 \wedge y \neq 0 \wedge DW(x, xy) \wedge DW(y, yx^2). \tag{2.2}$$

Действительно, $DW(x, xy) \Leftrightarrow x+1 \mid y$, а $DW(y, yx^2) \Leftrightarrow y+1 \mid x^2$ для положительных x и y, из чего и следует эквивалентность. Теперь, используя предикат $x > 1 \wedge y > 1 \wedge y = x^2 - 1$ из 2.2, получим, что

$$\begin{gathered} x > 1 \wedge y > 1 \wedge x = y \Leftrightarrow \\ \exists u \exists v (x > 1 \wedge u > 1 \wedge u = x^2 - 1 \wedge DW(u, y^2 u) \wedge \\ y > 1 \wedge v > 1 \wedge v = y^2 - 1 \wedge DW(v, x^2 v)). \end{gathered} \tag{2.3}$$

С помощью такого "ограниченного" равенства можно выразить второй из искомых предикатов $x = 1 \Leftrightarrow \exists y \exists z (y > 1 \wedge z > 1 \wedge y = z \wedge y > 1 \wedge xz > 1 \wedge y = xz)$. Теперь можно, во-первых, выразить равенство $x = y \Leftrightarrow \big(x = 0 \wedge y = 0\big) \vee \big(x = 1 \wedge y = 1\big) \vee \big(x > 1 \wedge y > 1 \wedge x = y\big)$, а во-вторых, с помощью выражения 2.2 определить аналогичным образом отношение $y = x^2 - 1$. Обладая равенством, делимость получаем по определению $x \mid y \Leftrightarrow \exists z (y = xz)$. □

Известно (см. [11]), что график сложения $z = x + y$ выразим бесквантворной формулой с помощью умножения, функтора S и равенства. Так как экзистенциальная арифметика неразрешима, то для доказательства неразрешимости $\exists \mathrm{Th} \langle \mathbb{N}; \cdot, DW \rangle$ достаточно выразить экзистенциальной формулой отношение $y = Sx$. Докажем сначала ещё одно вспомогательное утверждение.

Лемма 4. Для целых чисел $x > 1$ и $y \geq 0$ выполняется $yx+1 \mid x^2 - 1 \Leftrightarrow y = 0 \vee y = 1$.

Доказательство. Значения $y = 0$ и $y = 1$, очевидно, удовлетворяют делимости. Покажем, что других таких y нет.

Пусть $y \geq 2$. Из того, что $yx+1 \mid x^2 - 1$, следует $y \leq x-1$, то есть $y = x-k$ для некоторого $k \in [1, x-2]$. Прибавим левый аргумент делимости к правому и вынесем множитель $y+k$

$$yx+1 \mid x^2 - 1 \Leftrightarrow y(y+k)+1 \mid (y+k)^2 - 1 \Leftrightarrow y(y+k)+1 \mid (y+k)(2y+k). \tag{2.4}$$

Так как $y > 0$, получаем, что $y(y+k)+1 \perp y+k$. Следовательно, необходимо $y(y+k)+1 \mid 2y+k$, где правый аргумент положителен и меньше $y^2 + ky + 1$ для всякого $y \geq 2$. Из этого заключаем, что при $y \geq 2$ делимость не имеет места. □

Теперь можно выразить «ограниченное» отношение $y = Sx$.

Лемма 5. Отношение $x > 2 \wedge y = Sx$ экзистенциально выразимо в структуре $\langle \mathbb{N}; \cdot, DW \rangle$.

Доказательство. Будем пользоваться предикатами из Леммы 3. Свойство $x > 1$ определяется как $x \neq 0 \wedge x \neq 1$.

Покажем, что

$$x > 2 \wedge y = x + 1 \Leftrightarrow \\ \exists z \exists t \left(z > 1 \wedge x > 1 \wedge DW(x, xy) \wedge yz = x^2 - 1 \wedge t = z^2 - 1 \wedge x \mid t \right). \tag{2.5}$$

Если $y = x + 1$ для некоторого $x > 2$, то возьмём $z = x - 1$ и $t = (x-1)^2 - 1$.

Обратно, пусть $x > 1$, тогда $DW(x, xy) \Leftrightarrow x + 1 \mid y$, а значит, $y = k(x+1)$ для некоторого $k \geq 0$ и $k(x+1)z = (x+1)(x-1)$. Следовательно, $kz = x - 1$. Получается, что $kz + 1 \mid z^2 - 1$ для некоторого $k \geq 0$, из чего по Лемме 4 следует, что $k = 0 \vee k = 1$. Поскольку $k = 0$ влечёт $x = 1$, остаётся единственная возможность $k = 1$ и $z = x - 1$, а значит, $y = x + 1$. □

Теорема 2. Отношения $x = y$ и $y = Sx$ экзистенциально выразимы в $\langle \mathbb{N}; \cdot, DW \rangle$, следовательно, теория $\exists \mathrm{Th} \langle \mathbb{N}; \cdot, DW \rangle$ неразрешима.

Доказательство. Достаточно выразить свойство $x = 2$, так как $y = 3 \Leftrightarrow \exists x (x = 2 \wedge y = x^2 - 1)$, а для случая $x > 2$ имеем определение 2.5 из Леммы 5. Покажем, что

$$x = 2 \Leftrightarrow \exists y \exists z \exists t \left(zx > 2 \wedge y = zx + 1 \wedge x \mid z \wedge t = y^2 - 1 \wedge DW(z, t) \right).$$

Если $x = 2$, то возьмём $z = 2$, $y = 5$ и $t = 24$.

Для доказательства в обратную сторону перепишем выражение в скобках в виде $z(z+1) \mid (zx+1)^2 - 1 \wedge x \mid z$ и, так как $z \neq 0$, избавимся от z в первой делимости $z+1 \mid x(zx+2)$. Ввиду того, что $x \mid z$, получаем, что $z+1 \perp x$, и поэтому $z+1 \mid zx+2$. Эта делимость истинна тогда и только тогда, когда $z + 1 \mid 2 - x$ или $x \equiv 2 (\mathrm{mod}\ z+1)$, но $0 < x < z + 1$, значит, $x = 2$.

Итого, $x = y$ экзистенциально выразимо в $\langle \mathbb{N}; \cdot, DW \rangle$ по Лемме 3, экзистенциальная выразимость $y = Sx$ следует из определений для $x = 0$, $x = 1$ из Леммы 3, полученного выражения для $x = 2$ и $x = 3$, а также $x > 2 \wedge y = Sx$ из Леммы 5. Неразрешимость теории $\exists \mathrm{Th} \langle \mathbb{N}; \cdot, DW \rangle$ следует, как было указано выше, из выражения $z = x + y \Leftrightarrow \left(x = 0 \wedge y = 0 \wedge z = 0 \right) \vee (z \neq 0 \wedge S(zx)S(zy) = S(z^2 S(xy)))$ из [11] и неразрешимости $\exists \mathrm{Th} \langle \mathbb{N}; +, \cdot, = \rangle$ из [13, 14]. □

3. ПРЕДИКАТ DW И АРИФМЕТИЧЕСКИЕ ПРЕДИКАТЫ, ВЫРАЗИМЫЕ С ПОМОЩЬЮ СЛОЖЕНИЯ

Переходя к проблемам выразимости и разрешимости для теорий натуральных чисел с DW и некоторыми выразимыми с помощью сложения предикатами, докажем следующую теорему.

Теорема 3. Структура $\langle \mathbb{N}; +, DW \rangle$ def-полна.

Доказательство. Ввиду известной формулы $x \cdot y = z \Leftrightarrow (x + y)^2 = x^2 + y^2 + 2z$, выражающей график умножения с помощью сложения и возведения в квадрат, достаточно выразить двухместное отношение $y = x^2$. Используя то, что $x \leq y \Leftrightarrow \exists z (x + z = y)$, получим следующее определение:

$$y = x^2 \Leftrightarrow DW(x, x + y) \wedge \forall z (DW(x, x + z) \Rightarrow y \leq z). \tag{3.1}$$

Так как $DW(x, x + y)$, то x и y могут быть равны нулю только одновременно. Для ненулевых значений параметров y — наименьшее число, для которого $x(x+1) \mid x + y$, то есть, $x^2 + x = x + y$. □

Заметим, что предложенное в 3.1 определение аналогично выражению, указанному Л. Липшицем в [3] для $y = x^2$ в структуре $\langle \mathbb{N}; 1, +, | \rangle$:

$$y = x^2 \Leftrightarrow x \mid y \wedge x + 1 \mid x + y \wedge \forall z (x \mid z \wedge x + 1 \mid x + z \Rightarrow x + y \mid x + z). \tag{3.2}$$

Видим, что $x \mid y \wedge x+1 \mid x+y \Leftrightarrow DW(x, x+y)$. Используя определение 3.1, получаем следствие из теоремы. Здесь $\exists\forall\mathrm{Th}\langle\mathbb{N}; 1, +, \leq, DW\rangle$ есть множество всех истинных в $\mathbb{N}$ замкнутых формул языка $L_{1,+,\leq,DW}$ с кванторными приставками вида $\exists x_1 \ldots \exists x_n \forall y_1 \ldots \forall y_m$.

Следствие Теория $\exists\mathrm{Th}\langle\mathbb{N}; 1, +, \leq, DW\rangle$ разрешима, а $\exists\forall\mathrm{Th}\langle\mathbb{N}; 1, +, \leq, DW\rangle$ неразрешима.

Первое утверждение непосредственно следует из разрешимости $\exists\mathrm{Th}\langle\mathbb{N}; 1, +, |\rangle$. Доказательство второго утверждения аналогично доказательству неразрешимости $\exists\forall\mathrm{Th}\langle\mathbb{N}; 1, +, |\rangle$ из [3] и следует из неразрешимости $\exists\mathrm{Th}\langle\mathbb{N}; +, \cdot, =\rangle$ из [13, 14] и указанной выше бесквантворной формулы, выражающей график умножения с помощью сложения и возведения в квадрат.

Естественным усилением Теоремы 3 могло бы служить доказательство def-полноты структуры $\langle\mathbb{N}; <, DW\rangle$. Эта проблема выглядит труднее, и ниже будет доказано только некоторое достаточное условие def-полноты и выразимость в $\langle\mathbb{N}; <, DW\rangle$ отношений $y = 2x$ и $y = x^2$.

В доказательстве Теоремы 4 достаточно более слабого результата, чем теорема Робинсон о def-полноте структуры $\langle\mathbb{N}; S, |\rangle$. Так как отношение $y = Sx$ выразимо формулой $x < y \wedge \forall z(x < z \Rightarrow y = z \vee y < z)$, то структура $\langle\mathbb{N}; <, |\rangle$ также def-полна. Выразимостью $y = Sx$ будем пользоваться во всех последующих утверждениях.

Теорема 4. Если свойство $\exists y(x = 2^y)$ выразимо в структуре $\langle\mathbb{N}; <, DW\rangle$, то теория $\mathrm{Th}\langle\mathbb{N}; <, DW\rangle$ неразрешима. Если же в этой структуре выразимо отношение $x = 2^y$, то $\langle\mathbb{N}; <, DW\rangle$ def-полна.

Доказательство. Воспользуемся тем фактом (см. [15]), что $\mathrm{НОД}(\alpha^x - \beta^x, \alpha^y - \beta^y) = \alpha^{\mathrm{НОД}(x,y)} - \beta^{\mathrm{НОД}(x,y)}$ для всяких $\alpha > \beta \geq 0$, таких что $\alpha \perp \beta$ и $x > y \geq 0$. Получаем, что $\mathrm{НОД}(2^x-1, 2^y-1) = 2^{\mathrm{НОД}(x,y)}-1$, откуда следует, что $\mathrm{НОД}(x, y) = x \Leftrightarrow \mathrm{НОД}(2^x-1, 2^y-1) = 2^x-1$ и

$$(2^x - 1)2^x \mid (2^y - 1)2^y \Leftrightarrow 2^x - 1 \mid 2^y - 1 \wedge 2^x \mid 2^y \Leftrightarrow x \mid y. \tag{3.3}$$

Отношение $y = x(x+1)$ выражается формулой $\neg y = 0 \wedge \forall z(\neg z = 0 \wedge DW(x, z) \Rightarrow y = z \vee y < z)$. Теперь выражаем отношение $x(x+1) \mid y(y+1)$ с помощью формулы $\exists z(z = y(y+1) \wedge DW(x, z))$. Если в структуре $\langle\mathbb{N}; <, DW\rangle$ выразим предикат $x = 2^y$, то из 3.3 получаем, что $x \mid y \Leftrightarrow \exists u\exists v\,(Su = 2^x \wedge Sv = 2^y \wedge u(u+1) \mid v(v+1))$. Второе утверждение теоремы теперь следует из def-полноты $\langle\mathbb{N}; <, |\rangle$.

Докажем первое утверждение теоремы. Для этого укажем подструктуру $\langle\mathbb{N}; <, DW\rangle$, изоморфную $\langle\mathbb{N}; <, |\rangle$, то есть определим множество $A \subseteq \mathbb{N}$ и отношения $y\widetilde{<}x$ и $x\widetilde{|}y$ на A, что имеется биекция $f : \mathbb{N} \to A$, такая что $x < y \Leftrightarrow f(x)\widetilde{<}f(y)$ и $x \mid y \Leftrightarrow f(y)\widetilde{|}f(x)$. Из выразимости в $\langle\mathbb{N}; <, |\rangle$ отношений $x \in A$, $y\widetilde{<}x$ и $x\widetilde{|}y$ получим неразрешимость $\mathrm{Th}\langle\mathbb{N}; <, DW\rangle$.

Пусть $A = \{y : \exists x(y = 2^x - 1 \;\&\; x \geq 0)\}$ и $f(x) = 2^x - 1$. Тогда с помощью $\exists y(x = 2^y)$ отношение $x \in A$ определяется формулой $\exists y(\exists z(y = 2^z) \wedge Sx = y)$. Так как $x < y \Leftrightarrow 2^x - 1 < 2^y - 1$, то, определив $x\widetilde{|}y \rightleftharpoons x(x+1) \mid y(y+1)$, из 3.3 получим изоморфность $\langle\mathbb{N}; <, |\rangle$ и $\langle A; <, \widetilde{|}\rangle$. □

Автору не известно, выразимо ли в структуре $\langle\mathbb{N}; <, DW\rangle$ отношение $y = 2^x$ или хотя бы $\exists y(x = 2^y)$. Утверждения 1 и 2 могут оказаться полезными при построении формул, выражающих эти отношения.

Утверждение 1. Отношение $y = 2x$ выразимо в структуре $\langle\mathbb{N}; <, DW\rangle$.

Доказательство. В Теореме 4 было определено отношение $y = x(x+1)$. Теперь можем определить отношение $y = 2x(x+1)$ с помощью формулы $\neg y = 0 \wedge \neg y = x(x+1) \wedge \forall z(\neg z = 0 \wedge \neg z = x(x+1) \wedge DW(x, z) \Rightarrow y = z \vee y < z)$. Обозначим его $L_2(x, y)$. Аналогичным образом

определяем последовательно для $i = 3,4$ отношения $L_i(x,y) \rightleftharpoons y = ix(x+1)$, в обоих случаях добавляя конъюнктивно в формулу и в посылку импликации в подкванторном выражении $\neg L_{i-1}(x,y)$ и $\neg L_{i-1}(x,z)$ соответственно. Отсюда очевидно выразимо $y = (2x+1)^2$, а отношение $x > 0 \wedge y = (2x-1)^2$ задаётся формулой $\exists z \exists t(Sz = x \wedge L_4(z,t) \wedge y = St)$.

Следующая формула определяет искомый предикат:

$$y = 2x \Leftrightarrow (x = 0 \wedge y = 0) \vee \exists z_1 \exists z_2 \exists z_3 \exists z_4 (x > 0 \wedge z_1 = (2x-1)^2 \wedge z_2 = y(y-1) \wedge \\ \wedge z_3 = y(y+1) \wedge z_4 = (2x+1)^2 \wedge z_1 < z_2 \wedge z_3 < z_4).$$

Выражение в правой части требует, чтобы $y \geq 2x \wedge y \leq 2x$. □

Следующая лемма будет нужна при доказательстве выразимости в $\langle \mathbb{N}; <, DW \rangle$ отношения $y = x^2$.

Лемма 6. Отношение $y = x(x+1)(x+2)(x+3)$ выразимо в структуре $\langle \mathbb{N}; <, DW \rangle$.

Доказательство. Если $y \neq 0$ и удовлетворяет $DW(x,y) \wedge DW(SSx,y)$, то есть $x \mid y \& (x+1) \mid y \& (x+2) \mid y \& (x+3) \mid y$, то при условии $3 \mid x$, $y = \frac{k}{6}x(x+1)(x+2)(x+3)$ для некоторого $k \in \mathbb{N}$, а при $3 \nmid x$, получаем $y = \frac{k}{2}x(x+1)(x+2)(x+3)$ для некоторого $k \in \mathbb{N}$.

Выразим сначала свойство $3 \mid x$. С помощью $x = 0$ и S, определяются $2 \mid x \Leftrightarrow \exists y(y = 0 \wedge DW(Sy,x))$ и $6 \mid x \Leftrightarrow \exists y(y = 0 \wedge DW(SSy,x))$. Тогда $3 \mid x \Leftrightarrow 6 \mid x \vee 2 \nmid x \wedge 6 \nmid Sx \wedge \exists y(Sy = x \wedge 6 \nmid y)$.

Следуя той же схеме, что и в Утверждении 1, определяем $S_1(x,y) \Leftrightarrow \neg y = 0 \wedge DW(x,y) \wedge DW(SSx,y) \wedge \forall z(\neg z = 0 \wedge DW(x,z) \wedge DW(SSx,z) \Rightarrow y \leq z)$, и, далее, для $i = 2,\ldots,6$ последовательно конъюнктивно добавляем в формулу и в посылку импликации в подкванторном выражениии $\neg S_{i-1}(x,y)$ и $\neg S_{i-1}(x,z)$ соответственно. В итоге получаем

$$y = x(x+1)(x+2)(x+3) \Leftrightarrow (3 \mid x \wedge S_6(x,y)) \vee (3 \nmid x \wedge S_2(x,y)).$$ □

Утверждение 2. Отношение $y = x^2$ выразимо в структуре $\langle \mathbb{N}; <, DW \rangle$.

Доказательство. Покажем, что имеет место следующая равносильность:

$$y = x^2 \Leftrightarrow (x = 0 \wedge y = 0) \vee (x = 1 \wedge y = 1) \vee (x = 2 \wedge y = 4) \vee \\ \vee (x > 2 \wedge y > 2 \wedge \forall z(z = y(y-1) \Rightarrow DW(x,z) \wedge DW(x-1,z) \wedge \\ \wedge (x-2)(x-1)x(x+1) < z \wedge (x-1)x(x+1)(x+2) > z)). \tag{3.4}$$

Заключение импликации в подкванторном выражении должно служить тому, что $z = x^2(x^2-1)$, и для этого требуем делимость z на $x-1$, x, $x+1$ и заключаем z в интервал от $x^2(x^2-1) - 2x(x^2-1)$ до $x^2(x^2-1) + 2x(x^2-1)$.

Истинность импликации вправо очевидна.

Обратно, пусть $x, y \geq 3$. Если $DW(x,z) \wedge DW(x-1,z)$, то есть $(x-1) \mid z \& x \mid z \& (x+1) \mid z$, то $z = \frac{k}{2}(x-1)x(x+1)$, поэтому получим $(x-2) < \frac{k}{2} < x+2$. Следовательно, имеются три возможности: $z = (x-1)^2x(x+1)$, $z = (x-1)x^2(x+1)$ и $z = (x-1)x(x+1)^2$.

Предположим, что $y > x^2$. Если $z = y(y-1)$, то $z > x^2(x^2-1)$, и остаётся только возможность $y(y-1) = (x-1)x(x+1)^2 = (x^2-1)(x^2+x)$. Так как ясно, что $y < x^2 + x$, положим $y = x^2 + k$ для некоторого $k \in [1, x-1]$. Получим, что $x^2 - 1 \mid (x^2+k)(x^2+k-1)$, или, иными словами, $(x^2+k)(x^2+k-1) \equiv (k+1)k \equiv 0 \pmod{x^2-1}$. Ввиду ограничений на k, имеем $0 < k(k+1) \leq x(x-1)$, из чего следует (для $x, y \geq 3$), что такого k, а поэтому и y, не существует.

Если $y < x^2$, то для $z = y(y-1)$ имеется единственная возможность $y(y-1) = (x-1)^2x(x+1) = (x^2-x)(x^2-1)$, из чего следует $y > x^2 - x$. Снова положим $y = x^2 - k$ для некоторого $k \in [1, x-1]$ и получим, что $(x^2-k)(x^2-k-1) \equiv (k-1)k \equiv 0 \pmod{x^2-1}$. Если

$k = 1$, то исходное равенство имеет вид $(x^2-1)(x^2-2) = (x^2-1)(x^2-x)$, поэтому либо $x = 1$, либо $x = 2$, но эти случаи нами исключены. Если же $k > 1$, то $0 < k(k-1) < x^2 - 1$, из чего следует отсутствие таковых k и y, что и завершает доказательство утверждения. □

4. ЗАКЛЮЧЕНИЕ

Сделаем несколько замечаний по поводу рассмотренных в работе вопросов.

Хотя Теорема 4 даёт только условный ответ на вопрос о def-полноте структуры $\langle \mathbb{N}; <, DW\rangle$, положительное решение этого вопроса выглядит значительно легче аналогичной проблемы для $\langle \mathbb{N}; S, DW\rangle$, а также вопроса о разрешимости $\mathrm{Th}\langle \mathbb{N}; DW\rangle$. Отметим, что в $\langle \mathbb{N}; S, DW\rangle$ выразимо отношение $x \perp_2 y \rightleftharpoons \text{НОД}(x(x+1), y(y+1)) = 2$ формулой $\exists z(DW(x,z) \wedge DW(y, SSz))$, близкое к отношению $x \perp y$. На исследование структур, связанных с отношением взаимной простоты, были потрачены значительные усилия (главным образом, А. Вудсом в [16] и Д. Ришаром [17]), и, например, вопрос о def-полноте $\langle \mathbb{N}; S, \perp\rangle$, поставленный ещё в 1949 году Дж. Робинсон в [11], остаётся открытым (см. также [9, с. 126] и [10]).

В связи с определением 3.2 Л. ван ден Дрисом и А. Уилки был сделан вывод об экзистенциальной выразимости в структуре $\langle \mathbb{N}; 1, +, |\rangle$ дополнительного к $\{(x, y) \in \mathbb{N} : y = x^2\}$ множества и был поставлен вопрос об экзистенциальной выразимости в этой структуре множества всех чисел, не являющихся квадратами ([7, с. 505]). Интересно было бы помимо этого выяснить, является ли экзистенциальная теория $\exists\mathrm{Th}\langle \mathbb{N}; 1, +, |, Sq\rangle$ неразрешимой, где $Sq(x) \rightleftharpoons \exists y(x = y^2)$. Хорошо известно, что вопрос о разрешимости $\exists\mathrm{Th}\langle \mathbb{N}; 1, +, =, Sq\rangle$ является открытым и связан с так называемой проблемой Бюхи (см. [18]). С другой стороны, как следует из [19], для неразрешимости $\exists\mathrm{Th}\langle \mathbb{N}; 1, +, |, Sq\rangle$ достаточно показать экзистенциальную выразимость в соответствующей структуре какого-нибудь предиката степенного роста.

С практической точки зрения более важным является вопрос об алгоритмической сложности $\exists\mathrm{Th}\langle \mathbb{N}; 1, +, |\rangle$. Изначальным намерением автора было изучение сложности проблем распознавания формул экзистенциальных теорий $\exists\mathrm{Th}\langle \mathbb{N}; DW\rangle$ и $\exists\mathrm{Th}\langle \mathbb{N}; S, DW\rangle$. Ввиду примера 1.2, уже для формул этих теорий невозможно улучшить оценку из [4]. Поэтому, если надеяться получить принадлежность $\exists\mathrm{Th}\langle \mathbb{N}; 1, +, |\rangle$ классу **NP**, имеет смысл начать с исследования верхней оценки сложности для указанных более узких классов формул.

Список литературы

1. *Бельтюков А. П.* Разрешимость универсальной теории натуральных чисел со сложением и делимостью // Записки научных семинаров ЛОМИ. 1975. Т. 60. С. 15–28.
2. *Lipshitz L.* The Diophantine problem for addition and divisibility // Transactions of the American Mathematical Society. 1976. Vol. 235. P. 271–283. doi:10.2307/1998219
3. *Lipshitz L.* Some remarks on the Diophantine problem for addition and divisibility // Bull. Soc. Math. Belg. Ser. B. 1981. Vol. 33, no. 1. P. 41–52.
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). 2015. P. 667–676. doi:10.1109/LICS.2015.67
5. *Haase C.* On the complexity of model checking counter automata. Ph.D. Thesis. University of Oxford. 2012.
6. *Bundala D., Ouaknine J.* On parametric timed automata and one-counter machines // Information and Computation. 2017. Vol. 253. P. 272–303. doi:10.1016/j.ic.2016.07.011

7. *van den Dries L., Wilkie A.J.* The laws of integer divisibility, and solution sets of linear divisibility conditions // The Journal of Symbolic Logic. 2003. Vol. 68, no. 2. P. 503–526. doi:10.2178/jsl/1052669061
8. *Starchak M. R., Kosovskii N. K., Kosovskaya T. M.* Some NP-Hard Problems for the Simultaneous Coprimeness of Values of Linear Polynomials // Global Journal of Computer Science and Technology. 2017. Vol. 17, no. 4. P. 21–25.
9. *Korec I.* A list of arithmetical structures complete with respect to the first-order definability // Theoretical Computer Science. 2001. Vol. 257, no. 1–2. P. 115–151. doi:10.1016/S0304-3975(00)00113-4
10. *Richard D.* What are Weak Arithmetics? // Theoretical Computer Science. 2001. Vol. 257. P. 17–29.
11. *Robinson J.* Definability and decision problems in arithmetic // The Journal of Symbolic Logic. 1949. Vol. 14. P. 98–114. doi:10.2307/2266510
12. *Mostowski A.* On direct products of theories // The Journal of Symbolic Logic. 1952. Vol. 17, no. 1. P. 1–31. doi:10.2307/2267454
13. *Матиясевич Ю. В.* Диофантовость перечислимых множеств // Докл. АН СССР. 1970. Т. 191, № 2. С. 278–282.
14. *Матиясевич Ю. В.* Десятая проблема Гильберта. М.: Физматлит. 1993.
15. *Carmichael L. C.* On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$ // Ann. Math. 1913. Vol. 15, no. 2. P. 30–69. doi:10.2307/1967798
16. *Woods A.* Some problems in logic and number theory. PhD Thesis. University of Manchester. 1981.
17. *Richard D.* All arithmetical sets of powers of primes are first-order definable in terms of the successor function and the coprimeness predicate // Discrete Mathematics. 1985. Vol. 53. P. 221–247. doi:10.1016/0012-365X(85)90144-X
18. *Lipshitz L.* Quadratic forms, the five square problem, and diophantine equations // The collected works of J. Richard Büchi (S. MacLane and Dirk Siefkes, eds.). Springer. 1990. P. 677–680.
19. *Косовский Н. К.* О решении систем, состоящих одновременно из уравнений в словах и неравенств в длинах слов // Записки научных семинаров ЛОМИ. 1974. Т. 40. С. 24–29.

Поступила в редакцию 05.11.2018, окончательный вариант – 06.12.2018.

Computer tools in education, 2018
№ 6: 5–15
http://ipo.spb.ru/journal
doi:10.32603/2071-2340-2018-6-5-15

SOME DECIDABILITY AND DEFINABILITY PROBLEMS FOR THE PREDICATE OF THE DIVISIBILITY ON TWO CONSECUTIVE NUMBERS

Starchak M. R.

Saint Petersburg State University, Saint Petersburg, Russia

Abstract

The predicate of divisibility on two consecutive numbers $DW(x, y) \rightleftharpoons x \mid y \wedge 1 + x \mid y$ was introduced by L. van den Dries and A. Wilkie when they studied some properties of subsets of natural numbers, existentially definable with unit, addition and divisibility.

Undecidability of the existential theory of natural numbers with multiplication and DW and definability of addition and multiplication in terms of DW and divisibility is proved in the paper. Then the definability of multiplication in the terms of addition and DW is proved. Some definability questions for order and DW are also considered in the paper.

Keywords: *divisibility on two consecutive numbers, arithmetical definability, existential theory of natural numbers with addition and divisibility, algorithmic decidability, weak arithmetics.*

Citation: Starchak M. R. “Some Decidability and Definability Problems for the Predicate of the Divisibility on Two Consecutive Numbers”, *Computer tools in education*, no. 6, pp. 5–15, 2018 (in Russian). doi:10.32603/2071-2340-2018-6-5-15

Acknowledgements: *The author is grateful to Nikolai K. Kosovskii for posing the problem.*

Received 05.11.2018, the final version — 06.12.2018.

Mikhail R. Starchak, postgraduate student, department of informatics SPbSU, 199034 Saint Petersburg, University emb., 7/9, mikhstark@gmail.com

Старчак Михаил Романович,
аспирант кафедры информатики СПбГУ;
199034 Санкт-Петербург, Университетская наб., 7/9,
mikhstark@gmail.com