ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ

УДК 510.652

О НЕРАЗРЕШИМОСТИ АДДИТИВНЫХ И МУЛЬТИПЛИКАТИВНЫХ ТЕОРИЙ НАТУРАЛЬНЫХ ЧИСЕЛ С ОПЕРАТОРОМ ТРАНЗИТИВНОГО ЗАМЫКАНИЯ[1]

Золотов А.С.
Кафедра информатики

Поступила в редакцию 23.09.2014, после переработки 26.09.2014.

Мы продолжаем рассматривать вопрос о разрешимости обогащений разрешимых арифметических теорий оператором транзитивного замыкания. В данной работе рассматривается вопрос о разрешимости арифметики Пресбургера и арифметики Сколема с оператором транзитивного замыкания. Показано, что данные теории являются неразрешимыми, если допускать оператор транзитивного замыкания по одной паре переменных.

Ключевые слова: разрешимость, арифметика, транзитивное замыкание.

Вестник ТвГУ. Серия: Прикладная математика. 2014. № 3. С. 117–125.

Введение

Вопрос о разрешимости теорий является одной из центральных проблем математической логики. К настоящему моменту в этой области получен ряд результатов о разрешимости и неразрешимости математических теорий.

В 1929 году Пресбургером было доказано, что арифметика без умножения разрешима (см. [6], [11]). В доказательстве этого факта был использован метод эффективной элиминации кванторов: по заданной формуле эффективно строится новая, эквивалентная исходной формула, не содержащая кванторов. Таким образом, можно перейти к рассмотрению бескванторных формул, истинность которых устанавливается алгоритмически.

Хорошо известен тот факт, что арифметика без сложения и функции следования (арифметика Сколема) является разрешимой. Впервые это было показано в [13], однако в дальнейшем были найдены и другие доказательства данного факта (см. [10]).

Интерес представляет также тот факт, что несмотря на разрешимость аддитивной и мультипликативной арифметики, «обычная» арифметика натуральных чисел со сложением и умножением является неразрешимой (см. например [6]).

Примеры неразрешимых теорий можно найти в [6], [7] и [8].

[1] Работа выполнена при финансовой поддержке РФФИ, гранты № 13-01-00382 и № 13-01-00643.

В работах [4] и [5] рассматриваются обогащения арифметики Пресбургера функциями, согласованными со сложением, а также редкими предикатами. Доказано, что оба варианта являются разрешимыми.

Другими примерами разрешимых математических теорий являются теория вещественно-замкнутых полей (см. [2], [14]), теория булевых алгебр (см. [15]).

В [1] приведен целый ряд результатов, принадлежащих отечественным математикам.

После начала использования различных СУБД и появления в стандарте SQL возможности строить рекурсивные запросы начато активное исследование итеративных операторов, таких как оператор транзитивного замыкания или оператор инфляционной фиксированной точки.

Активное исследование оператора транзитивного замыкания и его свойств началось в работе [9].

В работе [3] рассматривается вопрос о применении оператора транзитивного замыкания по одной паре переменных к формулам с функцией следования и предикатами делимости, показано, как можно элиминировать оператор транзитивного замыкания. Также показано, что оператор транзитивного замыкания по двум парам переменных приводит к неразрешимой теории.

В данной работе рассматриваются обогащения арифметики Пресбургера и арифметики Сколема оператором транзитивного замыкания по одной паре переменных. Показано, что такие обогащения неразрешимы.

1. Основные определения

Считаем, что формулы строятся по обычным для логики первого порядка правилам, за исключением оператора транзитивного замыкания.

Определение 1. *Пусть $\psi(\bar{x},\bar{y})$ – формула, при этом наборы переменных $\bar{x},\bar{y}$ совпадают по количеству элементов, не пересекаются и состоят из переменных, свободно входящих в ψ. Тогда $T_{\bar{x},\bar{y}}(\psi(\bar{x},\bar{y}))$ – также формула, называемая транзитивным замыканием формулы $\psi(\bar{x},\bar{y})$ по переменным $\bar{x},\bar{y}$.*

Рассматривается следующая интерпретация I. Ее областью являются натуральные числа. Здесь и далее $I(x)$ – элемент интерпретации, приписываемый переменной x. Интерпретация I приписывает символу 0 нуль, символу s – функцию прибавления единицы. Также I предписывает, что $x < y$ должно быть истинно тогда и только тогда, когда $I(x)$ меньше $I(y)$, $x = y$ должно быть истинно тогда и только тогда, когда $I(x)$ равно $I(y)$. Также будем считать, что двухместные функциональные символы $\cdot$ и $+$ интерпретируются как умножение и сложение соответственно (знак умножения иногда будем опускать).

Определение 2. *Считаем $T_{\bar{x},\bar{y}}(\psi(\bar{x},\bar{y}))$ истинным, если $I(\bar{x}) = I(\bar{y})$ или если существует последовательность наборов элементов области интерпретации $\bar{a}_1,\dots,\bar{a}_n$, такая, что выполнено*

$$\psi(\bar{a}_1,\bar{a}_2)\wedge\psi(\bar{a}_2,\bar{a}_3)\wedge\cdots\wedge\psi(\bar{a}_{n-1},\bar{a}_n)\wedge I(\bar{x})=\bar{a}_1\wedge I(\bar{y})=\bar{a}_n.$$

2. Арифметика Пресбургера

Под арифметикой Пресбургера будем понимать теорию натуральных чисел со сложением, но без умножения.

Чтобы продемонстрировать неразрешимость арифметики Пресбургера, обогащенной оператором транзитивного замыкания по одной паре переменных, покажем, что в ней можно выразить делимость натуральных чисел.

Замечание 1. Нетрудно видеть, что предикаты делимости на константу $D_2, \ldots, D_n, \ldots$ можно выразить в арифметике Пресбургера.

Лемма 1. *С использованием оператора транзитивного замыкания можно выразить отношение делимости натуральных чисел. Существует формула $\varphi(x, y)$ истинная тогда и только тогда, когда $I(x)$ делится на $I(y)$.*

Доказательство. Легко видеть, что искомая формула может иметь вид

$$\exists v(T_{x,v}(x = v + y) \wedge v = 0).$$

Действительно, данная формула будет истинна либо при $I(x) = I(v)$, либо при $I(x) = kI(y) + I(v)$ для некоторого положительного k. Остается только заметить, что $I(v) = 0$. □

Хорошо известен результат (см. [12]), говорящий о том, что арифметика Пресбургера, обогащенная предикатом делимости, является неразрешимой.

Теорема 1. *Арифметика Пресбургера с оператором транзитивного замыкания даже по одной паре переменных является неразрешимой.*

3. Арифметика Сколема

Под арифметикой Сколема будем понимать теорию натуральных чисел с умножением, но без сложения и функции следования.

Перечислим вспомогательные определимые предикаты.

- Предикат равенства единице $E(x) \equiv (\forall u)(u = ux)$.
- Предикат равенства нулю $Z(x) \equiv (\forall u)(x = ux)$.
- Предикат делимости $D(x, y) \equiv (\exists u)(x = uy)$.
- Предикат простоты $P(x) \equiv \neg(Z(x)) \wedge \neg(E(x)) \wedge (\forall v)(D(x, v) \to (v = x \vee E(v)))$.
- Предикат «x является степенью y» $Pw(x, y) \equiv (\exists t)(E(t) \wedge T_{x,t}(x = yt))$.

Лемма 2. *Существует формула $\Phi(x, y, p, p_1)$, такая что $I \models \Phi$, тогда и только тогда, когда*

1. *$I(p)$ и $I(p_1)$ – различные простые числа;*
2. *$I(x) = (I(p))^k$ для некоторого $k \geq 0$;*
3. *$I(y) = (I(p_1))^k$ для k из п. 1.*

Доказательство. Рассмотрим формулу

$$\Phi(x, y, p, p_1) \equiv P(p) \wedge P(p_1) \wedge Pw(x, p) \wedge \neg(p = p_1) \wedge T_{x,y}(yp = xp_1) \wedge \neg D(y, p)).$$

Пусть $I \models \Phi$. Условия 1 и 2 тривиально истинны в силу определения предикатов P и Pw.

Поскольку $I \models \Phi$, то $I \models T_{x,y}(yp = xp_1)$. Возможны два варианта:

(a) $I(x) = I(y) = (I(p))^k$.

(b) Существуют такие $a_1, \ldots, a_n, n \geq 2$, что

$$a_2 I(p) = a_1 I(p_1) \wedge \cdots \wedge a_n I(p) = a_{n-1} I(p),$$

причем $a_1 = I(x) = (I(p))^k$ и $a_n = I(y)$.

Пусть истинно условие a. Тогда $(I(p))^k$ не делится на $I(p)$ в силу того, что $I \models \neg D(y, p)$. Но тогда $k = 0$, а $I(x) = I(y) = 1$, так что пункт 3 выполняется.

Теперь пусть истинно условие b. Покажем, что

$$a_i = (I(p))^{k-(i-1)}(I(p_1))^{i-1}, 1 \leq i \leq n$$

индукцией по i.

Базис: $i = 1$. Тогда

$$a_1 = I(x) = (I(p))^k = (I(p))^{k-(1-1)}(I(p_1))^{1-1}.$$

Шаг индукции: пусть $a_i = (I(p))^{k-(i-1)}(I(p_1))^{i-1}$. Тогда

$$a_{i+1} I(p) = a_i I(p_1) = (I(p))^{k-(i-1)}(I(p_1))^{i-1} I(p_1) = (I(p))^{k-(i-1)}(I(p_1))^i.$$

Отсюда $a_{i+1} = (I(p))^{k-i}(I(p_1))^i$, что и требовалось.

Тогда $I(y) = a_n = (I(p))^{k-(n-1)}(I(p_1))^{n-1}$. Заметим, что $n = k+1$. От противного, если $n < k+1$, то a_n делится на $I(p)$, что противоречит $I \models \neg D(y, p)$. Если же $n > k+1$, то $k - (n-1) < 0$, а поскольку $I(p)$ и $I(p_1)$ – простые числа, то a_n не является натуральным.

Таким образом, $n = k+1$, тогда $I(y) = a_n = (I(p_1))^k$, что и означает истинность пункта 3.

Импликация в обратную сторону тривиальна. Из 1 и 2 следует, что

$$I \models P(p) \wedge P(p_1) \wedge Pw(x, p) \wedge \neg(p = p_1).$$

Из 1 и 3 следует, что $I \models \neg D(y, p)$. Чтобы показать, что $I \models T_{x,y}(yp = xp_1)$, построим последовательность $a_i = (I(p))^{k-(i-1)}(I(p_1))^{i-1}$, она годится в качестве последовательности из определения 2. □

Используя формулу $\Phi(x, y, p, p_1)$ из леммы 2, построим некоторый аналог возведения в степень.

Лемма 3. *Существует формула $\Theta(x, y, z, p)$ такая, что $I \models \Theta$, тогда и только тогда, когда*

1. $I(x) = (I(p))^{k_1}, I(y) = (I(p))^{k_2}$ *для некоторых* $k_1, k_2 \geq 0$.

2. $I(z) = (I(p))^{k_1 k_2}$.

3. $I(p)$ *– простое число.*

Доказательство. Рассмотрим формулу

$$\Theta(x,y,z,p) \equiv (\exists t)(\exists p_1)(Pw(x,p) \wedge Pw(y,p) \wedge \Phi(x,t,p,p_1) \wedge \\ \wedge T_{t,z}(ty = zp_1) \wedge \neg D(z,p_1)).$$

Пусть $I \models \Theta$, тогда существует интерпретация

$$I' \models Pw(x,p) \wedge Pw(y,p) \wedge \Phi(x,t,p,p_1) \wedge T_{t,z}(ty = zp_1) \wedge \neg D(z,p_1).$$

При этом значения $I(x), I(y), I(z), I(p)$ совпадают с $I'(x), I'(y), I'(z), I'(p)$ соответственно. Про интерпретацию I' можно сказать следующее:

- $I'(p)$ и $I'(p_1)$ – различные простые числа в силу леммы 2. Отсюда следует истинность пункта 3.
- $I'(x) = (I'(p))^{k_1}, I'(y) = (I'(p))^{k_2}$ для некоторых $k_1, k_2 \geq 0$ в силу того, что $I' \models Pw(x,p) \wedge Pw(y,p)$. Отсюда следует истинность пункта 1.
- $I'(t) = (I'(p_1))^{k_1}$ в силу леммы 2.

Поскольку $I' \models T_{t,z}(ty = zp_1)$, возможны два варианта:

(I) $I'(t) = I'(z)$.

(II) Существуют такие $a_1, \dots a_n$, что

$$a_1 I'(y) = a_2 I'(p_1) \wedge \dots \wedge a_{n-1} I'(y) = a_n I'(p_1).$$

При этом $I'(t) = a_1, I'(z) = a_n$.

Пусть истинно условие I. Тогда $I'(z) = I'(t) = (I'(p_1))^{k_1}$. Поскольку $I' \models \neg D(z,p_1)$, то $k_1 = 0$. Тогда $I'(z) = 1 = (I(p))^0$. Таким образом, пункт 2 выполняется.

Пусть истинно условие II. Рассуждениями, аналогичными доказательству леммы 2, можно показать, что $a_i = (I'(p_1))^{k_1-(i-1)}(I'(y))^{i-1}$. С учетом того, что $I'(y) = (I'(p))^{k_2}$, получаем $a_i = (I'(p_1))^{k_1-(i-1)}(I'(p))^{k_2(i-1)}$. Покажем, что $k_1 + 1 = n$. От противного, если $k_1 > n-1$, то a_n делится на $I'(p_1)$, что противоречит тому, что $I'(z) = a_n$ и $I' \models \neg D(z,p_1)$. Если же $k_1 < n-1$, то $k_1 - n + 1 < 0$, а поскольку $I'(p)$ и $I'(p_1)$ – простые, число a_n не является натуральным.

Таким образом,

$$I(z) = I'(z) = a_n = (I'(p_1))^0 (I'(p))^{k_2 k_1} = (I(p))^{k_2 k_1}.$$

Это означает истинность пункта 2.

Импликация в обратную сторону тривиальна. В качестве значения p_1 годится любое простое число, отличное от $I(p)$, в качестве значения t годится $I(p_1)^{k_1}$, согласно лемме 2. Из 1–3 следует, что

$$I \models Pw(x,p) \wedge Pw(y,p) \wedge \Phi(x,t,p,p_1) \wedge \neg D(z,p_1).$$

Чтобы показать, что $I \models T_{t,z}(ty = zp_1)$, построим последовательность $a_i = (I'(p_1))^{k_1-(i-1)}(I'(y))^{i-1}$. Нетрудно показать, что она удовлетворяет условиям из определения 2. $\square$

Лемма 4. *Пусть $I \models \theta$, где θ – формула арифметики (не обязательно замкнутая), $x_1, \ldots, x_n$ – переменные, входящие в θ, d – некоторое простое число, $J(x_i) = d^{I(x_i)}, i = 1 \ldots n, J(p) = d, J(e) = 1; p, e$ – новые переменные. Тогда существует формула θ' арифметики Сколема с оператором транзитивного замыкания, такая что $I \models \theta \iff J \models \theta'$.*

Доказательство. Считаем, что все термы в θ являются простыми. Проведем доказательство индукцией по построению формулы.

Базис. Пусть θ является атомной формулой.

- Если $\theta \equiv (x_{i_1} = x_{i_2})$, то искомая $\theta' \equiv (x_{i_1} = x_{i_2})$.
- Если $\theta \equiv (x_{i_3} = x_{i_1} + x_{i_2})$, то $\theta' \equiv (x_{i_3} = x_{i_1} x_{i_2})$. Действительно, $I(x_{i_1}) = I(x_{i_2}) + I(x_{i_3})$ тогда и только тогда, когда $d^{I(x_{i_1})} = d^{I(x_{i_2})} d^{I(x_{i_3})}$.
- Если $\theta \equiv (x_{i_1} = 0)$, то $\theta' \equiv (x_{i_1} = e)$.
- Если $\theta \equiv (x_{i_1} = 1)$, то $\theta' \equiv (x_{i_1} = p)$.
- Если $\theta \equiv (x_{i_3} = x_{x_1} x_{i_2})$, то $\theta' \equiv \Theta(x_{i_1}, x_{i_2}, x_{i_3}, p)$, где Θ – формула из леммы 3. Условие выполняется в силу этой леммы.

Пусть для формул θ_1 и θ_2 построены искомые формулы θ_1' и θ_2' соответственно. Пусть $\theta \equiv (\theta_1 \wedge \theta_2)$. Тогда искомая $\theta' \equiv (\theta_1' \wedge \theta_2')$. Действительно, по индукционному предположению

$$(I \models \theta_1 \iff J \models \theta_1') \text{ и } (I \models \theta_2 \iff J \models \theta_2').$$

Эти условия выполняются тогда и только тогда, когда выполнено

$$I \models (\theta_1 \wedge \theta_2) \iff J \models (\theta_1' \wedge \theta_2').$$

Аналогично, если $\theta \equiv (\theta_1 \vee \theta_2)$, то $\theta' \equiv (\theta_1' \vee \theta_2')$ и если $\theta \equiv \neg\theta_1$, то $\theta' \equiv \neg\theta_1'$.

Пусть $\theta \equiv (\exists x_k)(\theta_1)$ и x_k входит в θ_1 свободно. Тогда рассмотрим формулу $\theta' \equiv (\exists x_k)(Pw(x_k, p) \wedge \theta_1')$.

Пусть $I \models \theta$, тогда существует $I_1 \models \theta_1$,$I(p) = I_1(p), I(e) = I_1(e)$, $I(x_j) = I_1(x_j)$ для всех x_j, входящих в θ,$j \neq k$,и $I_1(x_k) = a$. По индукционному предположению, $J_1(x_j) = d^{I_1(x_j)}, J_1(x_k) = d^a$ и $J_1 \models \theta_1'$, но тогда $J_1 \models Pw(x_k, p)$, поэтому $J \models \theta'$.

Пусть $J \models \theta'$, тогда существует $J_1 \models Pw(x_k, p) \wedge \theta_1'$,$J(p) = J_1(p), J(e) = J_1(e)$, $J_1(x_j) = J(x_j) = d^{I(x_j)}, j \neq k$. Из $J_1 \models Pw(x_k, p)$ следует $J_1(x_k) = J_1(p)^a = d^a$ для некоторого a. По индукционному предположению, $I_1(x_j) = I(x_j), j \neq k$, $I_1(x_k) = a$ и $I_1 \models \theta_1$. Тогда $I \models \theta$. □

Следствие 1. *В лемме 4 формула θ' строится по формуле θ эффективно.*

Лемма 5. *Для всякой замкнутой формулы φ формальной арифметики можно эффективно построить замкнутую формулу $\bar{\varphi}$ арифметики Сколема с оператором транзитивного замыкания такую, что φ истинна тогда и только тогда, когда $\bar{\varphi}$ истинна.*

Доказательство. Искомая формула $\bar{\varphi}$ будет иметь вид

$$\bar{\varphi} \equiv (\exists p)(\exists e)(P(p) \wedge E(e) \wedge \varphi').$$

Здесь формула φ' строится согласно лемме 4 по формуле φ. Утверждение данной леммы непосредственно следует из леммы 4. □

Из данных утверждений непосредственно следует наша основная теорема об арифметике Сколема с оператором транзитивного замыкания.

Теорема 2. *Арифметика Сколема с оператором транзитивного замыкания даже по одной паре переменных неразрешима.*

Заключение

В данной работе мы рассмотрели арифметику Пресбургера и арифметику Сколема, обогащенные оператором транзитивного замыкания по одной паре переменных. Для обеих теорий мы показали неразрешимость таких обогащений.

В арифметике Пресбургера с оператором транзитивного замыкания становится определимой делимость, что делает теорию неразрешимой. В арифметике Сколема с оператором транзитивного замыкания определимы некоторые аналоги сложения и умножения натуральных чисел, что позволяет доказать ее неразрешимость.

Интересен следующий вопрос. Существуют ли нетривиальные разрешимые обогащения теории натуральных чисел с функцией следования, которые при добавлении оператора транзитивного замыкания остаются разрешимыми?

Список литературы

[1] Адян С.И., Дурнев В.Г. Алгоритмические проблемы для групп и полугрупп // Успехи математических наук. 2000. Т. 55, № 2. С. 3–94.

[2] Верещагин Н.К., Шень А.М. Языки и исчисления. М.: Московский центр непрерывного математического образования, 2002. 288 с.

[3] Золотов А.С. Применение оператора транзитивного замыкания для формул с одной функции следования и предикатами делимости // Вестник ТвГУ. Серия: Прикладная математика. 2013. № 1(28). С. 101–117.

[4] Семенов А.Л. Логические теории одноместных функций на натуральном ряде // Известия Академии наук СССР. 1983. № 47(3). С. 623–658.

[5] Семенов А.Л. О некоторых расширениях арифметики сложения натуральных чисел // Известия Академии наук СССР. 1979. № 43(5). С. 1175–1195.

[6] Boolos G.S., Jefferey R.C. Computability and Logic. Cambridge University Press, 1994.

[7] Church A. A note on the Entscheidungs problem // The Journal of Symbolic Logic. 1936. № 1. Pp. 40–41.

[8] Church A. An unsolvable problem of elementary number theory // American Journal of Mathematics. 1936. № 58. Pp. 345–363.

[9] Fagin R. Monadic generalized spectra // Zeitschrift fur mathematische Logik und Grundlagen der Mathematik. 1975. № 21. Pp. 89–96.

[10] Mostowski A. On direct products of theories // The Journal of Symbolic Logic. 1952. № 17. Pp. 1–31.

[11] Presburger M. Uber die Vollstandigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt // Comptes Rendus du I congres de Mathematiciens des Pays Slaves. 1929. Pp. 92—101.

[12] Robinson J. Definability and decision problems in arithmetic // The Journal of Symbolic Logic. 1949. № 14. Pp. 98–114.

[13] Skolem T. Uber gewisse satzfunktionen in der arithmetik // Skrifter utgitt av Det Norske videnskaps-akademi i Oslo. 1930. № 7. Pp. 154–180.

[14] Tarski A. A Decision Method for Elementary Algebra and Geometry. Berkeley, Los Angeles: University of California Press, 1951.

[15] Tarski A. Arithmetical classes and types of Boolean algebras: Preliminary report // Bulletin of the American Mathematical Society. 1949. № 55. Pp. 64–64.

Библиографическая ссылка

Золотов А.С. О неразрешимости аддитивных и мультипликативных теорий натуральных чисел с оператором транзитивного замыкания // Вестник ТвГУ. Серия: Прикладная математика. 2014. № 3. С. 117–125.

Сведения об авторах

1. **Золотов Александр Сергеевич**
аспирант кафедры информатики Тверского государственного университета.

Россия, 170100, г. Тверь, ул. Желябова, д. 33, ТвГУ.

ON UNDECIDABILITY OF ADDITIVE AND MULTIPLICATIVE THEORIES OF NATURAL NUMBERS WITH THE TRANSITIVE CLOSURE OPERATOR

Zolotov Alexander Sergeyevich
PhD student of Computer Science department, Tver State University
Russia, 170100, Tver, 33 Zhelyabova str., TSU.

Received 23.09.2014, revised 26.09.2014.

We prove that the transitive closure operator extensions of Presburger arithmetic and Skolem arithmetic are undecidable.

Keywords: decidability, arithmetic, transitive closure.

Bibliographic citation

Zolotov A.S. On undecidability of additive and multiplicative theories of natural numbers with the transitive closure operator. *Vestnik TvGU. Seriya: Prikladnaya matematika* [Herald of Tver State University. Series: Applied Mathematics], 2014, no. 3, pp. 117–125. (in Russian)