S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports
http://semr.math.nsc.ru

Том 12, стр. 185–189 (2015) УДК 510.652
DOI 10.17377/semi.2015.12.015 MSC 11U99

ГЕНЕРИЧЕСКАЯ НЕПОЛНОТА ФОРМАЛЬНОЙ АРИФМЕТИКИ

А.Н. РЫБАЛОВ

Abstract. Famous Gödel's incompleteness theorem states that formal arithmetic (if it is consistent) has a statement that is unprovable and incontrovertible by any recursive systems of axioms. In this paper we prove that Gödel's theorem remains true if we restrict the set of all arithmetic statements by some natural subsets of „almost all“ statements (so called strongly generic sets).

Keywords: formal arithmetic, generic complexity.

1. Введение

В последнее десятилетие в математической логике и теории алгоритмов активно развивается так называемый генерический подход. В рамках этого подхода изучаются свойства, которые присущи случайным или типичным объектам из данного множества, или, другими словами, „почти всем“ объектам. Понятие „почти все“ формализуется введением естественной меры на множестве, тесно связанной с процедурами генерации случайных объектов заданного размера. Причем, вполне может оказаться так, что все объекты из данного множества не обладают неким свойством, но для „почти всех“ объектов оно выполняется. В теории алгоритмов такой подход приводит к понятию генерического алгоритма, который работает эффективно и корректно решает алгоритмическую проблему для почти всех входов и выдает неопределенный ответ на оставшемся множестве редких плохих входов. С точки зрения практики, генерические алгоритмы так же хороши, как и быстрые алгоритмы для всех входов. Классическим примером такого алгоритма является симплекс-метод – он за полиномиальное время решает задачу линейного программирования для

Rybalov, A.N., Generic incompleteness of formal arithmetic.

Работа поддержана грантом Российского научного фонда (проект №14-11-00085).
Поступила 10 июля 2014 г., опубликована 14 марта 2015 г.

большинства входных данных, но имеет экспоненциальную сложность в худшем случае. Более того, может так оказаться, что проблема трудноразрешима или вообще неразрешима в классическом смысле, но легкоразрешима на генерическом множестве. В работах [2, 3] было доказано, что таким поведением обладают многие алгоритмические проблемы алгебры, а в работе [1] была доказана генерическая разрешимость проблемы остановки для машин Тьюринга с лентой, бесконечной в одном направлении. В работах [4, 5, 6, 8, 9, 10, 11] генерический подход применяется ко многим классическим алгоритмическим проблемам.

Знаменитая теорема Геделя о неполноте утверждает, что если формальная арифметика непротиворечива, то она неполна, то есть в ней существует недоказуемое и неопровержимое утверждение. Возникает вопрос, а если ограничиться не всеми утверждениями, а „почти всеми“, что можно сказать о такой генерической полноте формальной арифметики? Другими словами, верно ли, что для „почти любой“ (случайной) замкнутой формулы арифметики выводима из некоторого рекурсивного списка аксиом либо сама формула, либо ее отрицание? В данной работе доказывается, что даже если ограничиться некоторым классом множеств „почти всех“ арифметических формул, неполнота арифметики сохранится. Другими словами, в любом таком множестве „почти всех“ формул (они называются строго генерическими множествами) существует формула, которая сама не выводима и не выводимо ее отрицание. Так же как и теорема Геделя, подобный результат можно получить для любой формальной системы, которая содержит арифметику.

2. Генерические и пренебрежимые множества

Пусть A – счетное множество некоторых объектов. На множестве A определена функция размера $size : A \to \mathbb{N}$, сопоставляющая каждому элементу $a \in A$ его размер $size(a)$. Допустим, что для любого n множество A_n элементов из A размера n конечно.Для любого подмножества $S \subseteq A$ определим следующую последовательность

$$\rho_n(S) = \frac{|S \cap A_n|}{|A_n|},\ n = 1, 2, 3, \ldots$$

Величина $\rho_n(S)$ это вероятность получить вход из множества S при случайной и равномерной генерации элементов из A_n. *Асимптотической плотностью* S назовем следующий предел (если он существует)

$$\rho(S) = \lim_{n\to\infty} \rho_n(S).$$

Множество S называется *генерическим*, если $\rho(S) = 1$ и *пренебрежимым*, если $\rho(S) = 0$. Очевидно, что S генерическое тогда и только тогда, когда его дополнение $A \setminus S$ пренебрежимо. Следуя [2], назовем множество S *строго пренебрежимым*, если последовательность $\rho_n(S)$ экспоненциально быстро сходится к 0, т.е. существуют константы $0 < \sigma < 1$ и $C > 0$ такие, что для любого n

$$\rho_n(S) < C\sigma^n.$$

Теперь S называется *строго генерическим*, если его дополнение $I \setminus S$ строго пренебрежимо. Непосредственно из определения следует, что если $T \subseteq A$ не строго пренебрежимо и $S \subseteq A$ – строго генерическое, то $S \cap T \neq \varnothing$.

Понятие генерического множества является некоторой формализацией интуитивного понятия множества „почти всех“ элементов множества A в том смысле, что при увеличении размера элемента вероятность попасть в генерическое множество при случайной генерации элементов, стремится к 1.

3. Представление арифметических формул

В этой главе, следуя работе [8], мы рассмотрим естественное представление замкнутых арифметических формул языка $\{+, \times, 1\}$ с помощью двоичных деревьев. Это представление, с одной стороны настолько же компактно как и стандартное представление строками символов (с точностью до линейного множителя). С другой стороны, оно удобно для различного рода подсчетов. Кроме того, достаточно просто написать компьютерную программу для случайной генерации формул, заданных с помощью этого представления.

Назовем замкнутую арифметическую формулу Φ *простой атомарной* если она имеет следующий вид:

1) $x_i = x_j + x_k$,
2) $x_i = x_j x_k$,
3) $x_i = 1$.

Мы говорим, что замкнутая арифметическая формула Φ имеет *натуральную пренексную* форму, если она имеет вид:

$$\Phi = Q_1 x_1 \dots Q_t x_t \phi,$$

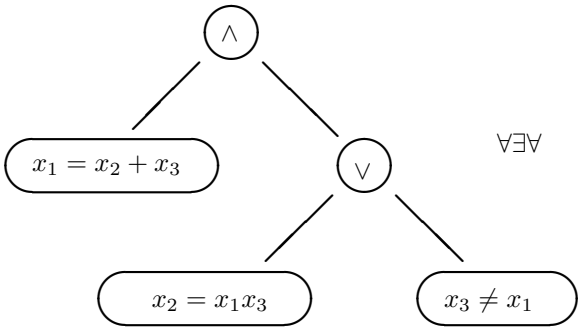
где $Q_i \in \{\forall, \exists\}$ – кванторы, ϕ бескванторная формула, полученная с помощью конъюнкций, дизъюнкций из простых атомарных формул или их отрицаний. Заметим, что любая замкнутая формула может быть приведена с помощью эквивалентных преобразований к натуральной пренексной форме. При этом размер формулы увеличивается не более чем линейно.

Пусть теперь ϕ – бескванторная формула, которая является булевой комбинацией простых атомарных формул и их отрицаний. Естественным образом можно сопоставить формуле ϕ бинарное дерево T_ϕ, которое представляет конструкцию ϕ из простых атомарных формул и их отрицаний с помощью конъюнкций и дизъюнкций. Внутренние вершины T_ϕ помечены символами $\vee$ и $\wedge$, а листья T_ϕ помечены простыми атомарными или их отрицаниями. С другой стороны, по любому такому бинарному дереву можно восстановить бескванторную формулу. Это дает взаимно-однозначное представление бескванторных частей замкнутых арифметических формул в натуральной пренексной форме размеченными бинарными деревьями. Если T_ϕ имеет n листьев, то не более $3n$ переменных могут встетиться в T_ϕ, поэтому в дальнейшем будем полагать, что все переменные T_ϕ лежат в множестве $x_1, \dots, x_{3n}$.

Пусть $\Phi = Q_1 x_1 \dots Q_t x_t \phi$ – формула в натуральной пренексной форме. *Представление* Φ состоит из бинарного дерева T_ϕ, которое кодирует бескванторную часть ϕ, и кванторной приставки $Q_1 x_1 \dots Q_t x_t$. Если T_ϕ имеет n листьев, то длина кванторной приставки не более $3n$. Поэтому число n листьев в дереве T_ϕ дает линейную верхнюю оценку на число нефиктивных переменных и кванторов в Φ. Заметим также, что число булевых операций в бескванторной части Φ равно $n - 1$. Под размером формулы Φ будем понимать число n. Для

упрощения подсчетов считается, что формула Φ размера n зависит от всех переменных $\{x_1, \ldots, x_{3n}\}$ и кванторы навешаны на все эти переменные (то есть кванторная приставка содержит ровно $3n$ кванторов).

Например, вот представление формулы $\forall x_1 \exists x_2 \forall x_3 \Big((x_1 = x_2 + x_3) \wedge \big((x_2 = x_1 x_3) \vee (x_3 \neq x_1) \big) \Big)$:



В дальнейшем будем отождествлять замкнутые арифметические формулы с их представлениями.

4. Основной результат

Для любой арифметической формулы Φ определим множество

$$AND(\Phi)^+ = \{\Phi \wedge \Psi,\ \Psi \text{ – произвольная истинная формула}\}.$$

В работе [8] было доказано следующее утверждение (лемма 3):

Лемма 1. *Для любой формулы Φ множество $AND(\Phi)^+$ не строго пренебрежимо.*

Напомним, что понятия строгой пренебрежимости и генеричности множеств формул рассматриваются относительно представления формул в виде деревьев, описанных в предыдущем параграфе.

Теперь все готово, чтобы доказать основной результат.

Теорема 1. *Не существует строго генерического множества арифметических формул $\mathcal{G}$ такого, что для любой формулы $\Phi \in \mathcal{G}$ либо Φ, либо $\neg\Phi$ выводится из фиксированного рекурсивного множества аксиом.*

Доказательство. Допустим противное, то есть, что существует такое строго генерическое множество формул $\mathcal{G}$. По теореме Геделя о неполноте, существует такая арифметическая формула Φ, что ни Φ, ни $\neg\Phi$ невыводимы. Рассмотрим множества $AND(\Phi)^+$ и $AND(\neg\Phi)^+$. По лемме 1 эти множества не строго пренебрежимы, а, значит $AND(\Phi)^+ \cap \mathcal{G} \neq \varnothing$ и $AND(\neg\Phi)^+ \cap \mathcal{G} \neq \varnothing$. Таким образом, существуют истинные формулы Ψ_1 и Ψ_2 такие, что $\Phi \wedge \Psi_1 \in \mathcal{G}$ и $\neg\Phi \wedge \Psi_2 \in \mathcal{G}$. В множестве $\mathcal{G}$ любая формула или ее отрицание доказуемы, поэтому одна из формул

$$\Phi \wedge \Psi_1,\ \neg\Phi \vee \neg\Psi_1,$$

доказуема, и одна из формул

$$\neg\Phi \wedge \Psi_2,\ \Phi \vee \neg\Psi_2,$$

доказуема. Обе формулы $\neg\Phi \vee \neg\Psi_1$ и $\Phi \vee \neg\Psi_2$ не могут быть доказуемы, так как одна из них обязательно будет ложной (напомним, что Ψ_1 и Ψ_2 истины). Поэтому либо $\Phi \wedge \Psi_1$, либо $\neg\Phi \wedge \Psi_2$ доказуема. Отсюда следует, что либо Φ, либо $\neg\Phi$ доказуема, а это противоречит теореме Геделя. □

References

[1] J.D. Hamkins, A. Miasnikov, *The halting problem is decidable on a set of asymptotic probability one*, Notre Dame Journal of Formal Logic, **47**:4 (2006), 515–524. MR2272085

[2] I. Kapovich, A. Myasnikov, P. Schupp, V. Shpilrain, *Generic-case complexity, decision problems in group theory and random walks*, Journal of Algebra, **264**:2 (2003), 665–694. MR1981427

[3] I. Kapovich, A. Myasnikov, P. Schupp, V. Shpilrain, *Average-case complexity for the word and membership problems in group theory*, Advances in Mathematics, **190** (2005), 343–359. MR2102661

[4] A.Myasnikov, A. Rybalov, *Generic complexity of undecidable problems*, Journal of Symbolic Logic, **73**:2 (2008), 656–673. MR2414470

[5] A.Rybalov, *On the strongly generic undecidability of the Halting Problem*, Theoretical Computer Science, **377** (2007), 268–270. MR2323401

[6] A. Rybalov, *Generic Complexity of Presburger Arithmetic*, Theory of Computing Systems, **46**:1 (2010), 2–8. MR2574642

[7] A. Rybalov, *Generic complexity of first-order theories*, Siberian Electronic Mathematical Reports, **8** (2011), 168–178. MR2876556

[8] A. Rybalov, *On generic undecidability of Hilbert's tenth problem*, Herald of Omsk University, **4** (2011) 19–22.

[9] A. Rybalov, *On generic complexity of the Boolean truthfulness problem*, Herald of Omsk University, **4** (2012) 36–40.

[10] A. Rybalov, *Generic complexity of the Diophantine problem*, Groups Complexity Cryptology, **5**:1 (2013), 25–30. MR3065446

[11] A. Rybalov, *On generic complexity of the Boolean satisfiability problem*, Herald of Omsk University, **4** (2013), 52–56.

Alexander Nikolaevich Rybalov
Omsk State Technical University,
prospekt Mira 11,
Omsk 644050, Russia
E-mail address: alexander.rybalov@gmail.com