УДК 519.217.2

О.А. ВАГІС
Інститут кібернетики ім. В.М. Глушкова НАН України, Київ, Україна,
e-mail: *valexdep135@gmail.com*.

А.М. ГУПАЛ
Інститут кібернетики ім. В.М. Глушкова НАН України, Київ, Україна,
e-mail: *gupalanatol@gmail.com.*

РОЗВ'ЯЗНІСТЬ NP-ПОВНИХ ЗАДАЧ

Анотація. Аналіз нерозв'язності Діофантових рівнянь показав, що задачі розпізнавання властивостей класу NP є розв'язуваними, тобто недетермінований алгоритм або повний перебір на вході задачі дає позитивну чи негативну відповідь. Для поліноміальних Діофантових рівнянь такого недетермінованого алгоритму не існує. З нерозв'язності Діофантових рівнянь випливає простий варіант теореми Геделя про неповноту арифметики.

Ключові слова: NP-повні задачі, Діофантові множини, недетермінований алгоритм.

ВСТУП

Математична теорія, заснована на понятті NP-повноти задач, будується для зручності викладу з використанням задач розпізнавання властивостей. Такі задачі мають лише два можливі розв'язки: «так» чи «ні». Задача розпізнавання П складається з множини D_{Π} всіх можливих індивідуальних задач та множини Y_{Π} $(Y_{\Pi} \subset D_{\Pi})$ індивідуальних задач із відповіддю «так».

Спочатку описують умови задачі у термінах різних компонентів: множин, графів, функцій, чисел тощо. Потім у термінах умови формулюють питання, на яке може бути одна з двох відповідей: «так» чи «ні». Цей опис визначає множини D_{Π} і Y_{Π} очевидним чином. Індивідуальна задача належить D_{Π} у тому й лише тому випадку, коли вона може бути отримана із стандартного опису підстановкою конкретних значень у всі компоненти умови. Індивідуальна задача належить Y_{Π} у тому й лише тому випадку, коли відповіддю на запитання задачі буде «так».

Саме поняття поліноміальної «перевірки» дає змогу виокремити задачі класу NP. Перевірка за поліноміальний час не означає розв'язності за поліноміальний час. Клас NP визначається за допомогою недетермінованого алгоритму [1]. Такий алгоритм складається з двох різних стадій: «угадування» і перевірка. За заданої індивідуальної задачі I на першій стадії відбувається вгадування деякої структури S. Потім I і S разом подаються як вхід на стадію перевірки, яка виконується звичайним детермінованим чином і або закінчується відповіддю «так» чи «ні», або триває нескінченно без зупинки [1]. Останнє твердження, як побачимо далі, неправильне. Недетермінований алгоритм розв'язує задачу П, якщо для будь-якої індивідуальної задачі $I \in D$ виконані такі дві властивості:

1) якщо $I \in Y_{\Pi}$, то існує така структура S, у разі вгадування якої для входу I стадія перевірки, що починає роботу на вході (I, S), закінчується відповіддю «так»;

2) якщо $I \notin Y_{\Pi}$, то немає такої структури S, вгадування якої для входу I забезпечить закінчення стадії перевірки на вході (I, S) відповіддю «так».

Легко бачити, що ці дві властивості виконуються тоді й тільки тоді, коли задачу можна розв'язати, оскільки саме існування недетермінованого алгоритму означає розв'язність задач класу NP. Як буде показано далі, з нерозв'язності Діофантових рівнянь випливає, що не існує будь-якого недетермінованого алгоритму, для якого виконуються властивості 1 і 2.

Недетермінований алгоритм, який розв'язує задачу розпізнавання П працює на протязі «поліноміального часу», якщо може існувати поліном p такий, що для будь-якого $I \in Y_{\Pi}$ знайдеться деяка здогадка S, що приведе на стадії детермінованої перевірки на вході (I, S) до відповіді «так» за час $p(Length[I])$. Звідси випливає, що «розмір» структури S, що вгадується, обмежений поліномом $p(Length[I])$, тому що на перевірку здогадки S може бути витрачено не більше, ніж поліноміальний час.

Клас NP — це клас всіх задач розпізнавання П, які за розумного кодування можуть бути розв'язаними недетермінованим алгоритмом за поліноміальний час. Основне призначення «поліноміального недетермінованого алгоритму» полягає у поясненні поняття «перевірка за поліноміальний час», а не у тому, щоб реально побудувати метод розв'язання задач розпізнавання властивостей.

ПОЛІНОМІАЛЬНА ЗВІДНІСТЬ ТА NP-ПОВНІ ЗАДАЧІ

Основна ідея побудови NP-повних задач ґрунтується на понятті поліноміальної звідності за припущення, що $P \neq NP$.

Задача розпізнавання Π_1 поліноміально зводиться до задачі розпізнавання Π_2, якщо є функція f, яка задовольняє дві умови:

— функція f обчислюється поліноміальним алгоритмом;

— для всіх входів $I \in Y_{\Pi_1}$ тоді і тільки тоді, коли $f(I) \in Y_{\Pi_2}$.

Поліноміальна звідність вводиться для задач із входом $I \in Y_{\Pi}$, тобто існує така структура S, стадія перевірки якої спричиняє на вході (I, S) відповідь «так».

Задача розпізнавання П називається NP-повною, якщо $\Pi \in \text{NP}$ і будь-яка інша задача розпізнавання зводиться до П. За фундаментальною теоремою Кука, задачу розпізнавання з Булевої логіки, яку називають «здійсненність», визначено як першу NP-повну задачу.

Для обґрунтування поліноміальної звідностіі будь-якої задачі розпізнавання $\Pi \in \text{NP}$ до задачі «здійсненність» Кук розглядав шість груп диз'юнкцій, кожна з яких накладає обмеження певного типу на будь-який набір значень істинності [2]. Набір диз'юнкцій задачі «здійсненність» побудований так, що будь-який виконувальний набір значень істинності для диз'юнкцій зобов'язаний відповідати деякому приймальному обчисленню детермінованої програми Тьюринга на вході I. Звідси випливає, що для $f(I)$ існує виконувальний набір значень істинності тоді і тільки тоді, коли $I \in Y_{\Pi}$.

НЕРОЗВ'ЯЗНІСТЬ ДІОФАНТОВИХ РІВНЯНЬ

У 1970 р. було отримано важливий результат, що негативно розв'язує десяту проблему Гільберта: чи існує алгоритм, який за наданим поліномом $p(x_1, \ldots, x_n)$ з цілими коефіцієнтами розпізнає, чи має рівняння $p = 0$ розв'язок у цілих числах. У [3] Ю.В. Матіясевич показав, що такого алгоритму не існує.

Нехай $p(z_1, \ldots, z_n)$ — поліном із цілими коефіцієнтами. Діофантові рівняння

$$p(z_1, \ldots, z_n) = 0 \tag{1}$$

розв'язуються у цілих числах. Частину змінних (1) виокремлюють як параметри і записують (1) у вигляді

$$p(a, x_1, \ldots, x_m) = 0, \tag{2}$$

де параметр може бути векторним, $a = \{a_1, \ldots, a_k\}$, причому всі a_i і x_j належать натуральному ряду $N = \{0, 1, 2, \ldots\}$. Зауважимо, що для Діофантових рівнянь не можна використовувати недетермінований алгоритм чи повний перебір, оскільки областю визначення змінних є лічильна множина натуральних чисел.

Множина A позитивних векторів $a = \{a_1, \ldots, a_k\}$ називається Діофантовою, якщо за будь-якого $a \in A$ і тільки за $a \in A$ рівняння (2) можна розв'язати в цілих позитивних $x_1, \ldots, x_m$. Арифметична мова $L_0 = \{+, \times, =, \exists\}$, де $\exists$ — квантор існування дає змогу записати будь-який поліном $p(a, x)$ у вигляді $\exists x p(a, x) = 0$, де $a = \{a_1, \ldots, a_k\}$, $x = \{x_1, \ldots, x_m\}$.

Відомо, що Діофантові множини — це ті й тільки ті множини, які можна описати мовою L_0. Однак можливості мови L_0 обмежені і цією мовою не вдається описати багато цікавих з теоретико-числової точки зору множин. Наприклад, множина простих чисел має вигляд

$$p > 1 \,\&\, \forall y \leq p \forall z \leq p [yz \neq p \vee y = 1 \vee z = 1],$$

де $\forall_{\leq}$ — обмежений квантор загальності.

Ю.В. Матіясевич вивчив мову $Я_5$, що містить символи $+, \times, \uparrow$ (оператор зведення у ступінь), $=, \neq, >, \geq, |$ (операція поділу), (mod), $\&$, $\vee$, $\exists$, $\forall_{\leq}$. Технічно складними виявилися докази діофантовості експоненти та обмеженого квантора загальності. Йому вдалося довести рівнооб'ємність мов L_0 і $Я_5$, звідки негайно слідує діофантовість множини всіх простих чисел. З іншого боку, у теорії обчислюваних функцій встановлено, що клас множин, описаних мовою $Я_5$, збігається з класом рекурсивно перелічуваних множин. Отже, Ю.В. Матіясевич довів, що всі рекурсивно перераховані множини є Діофантовими.

Відомо, що проблема $x \in W_x$ нерозв'язна, де W_x — область визначення обчислюваної функції з індексом x, W_x — рекурсивно перераховувана множина, а $\overline{W_x}$ — неперераховувана множина. Цей результат є фундаментальним у теорії обчислюваних функцій [4].

Виберемо тепер поліном $p(a, x_1, \ldots, x_m)$, такий що

$$a \in W_a \Leftrightarrow \exists x_1, \ldots, \exists x_m \, (p(a, x_1, \ldots, x_m) = 0).$$

Це можна зробити в результаті діофантовості рекурсивно перераховуваної множини W_a. Тоді, якби існувала розв'язувальна процедура для десятої проблеми Гільберта, то існувала б і розв'язувальна процедура для проблеми $x \in W_x$, звідки випливає, що десята проблема Гільберта є нерозв'язною.

З нерозв'язності Діофантових рівнянь випливає простий варіант теореми Геделя про неповноту арифметики. Поліноми, що не мають позитивних розв'язків, утворюють істинні твердження вигляду

$$\forall x_1, \ldots, \exists x_m \, (p(a, x_1, \ldots, x_m) \neq 0), \tag{3}$$

які за властивістю множини $\overline{W_a}$ неперераховані. Оскільки будь-які докази є скінченними, всі вони можуть бути ефективно перераховані або алгоритмічно перенумеровані. Отже, серед істинних тверджень (3) існують неперераховані тобто недоказні твердження.

ВИСНОВКИ

Аналіз нерозв'язності Діофантових рівнянь показав, що задачі розпізнавання властивостей класу NP є розв'язними, тобто недетермінований алгоритм або повний перебір на вході задачі дає позитивну чи негативну відповідь. Для поліноміальних Діофантових рівнянь такого недетермінованого алгоритму не існує. З нерозв'язності Діофантових рівнянь випливає простий варіант теореми Геделя про неповноту арифметики.

СПИСОК ЛІТЕРАТУРИ

1. Гэри М., Джонсон Л. Вычислительные машины и труднорешаемые задачи. Москва: Мир, 1982. 416 с.
2. Cook S.A. The complexity of theorem-proving procedures. *Proc. 3 rd Ann. ACM Symp. on Theory of Computing Association for Computing Machinery*. New York. 1971. P. 151–158.
3. Матиясевич Ю.В. Диофантовы множнства. *Успехи математических наук.* 1971. Т. 22. Вып. 5. С. 185–222.
4. Катленд Н. Вычислимость. Введение в теорию рекурсивных функций. Москва: Мир, 1983. 256 с.

A.A. Vagis, A.M. Gupal

SOLVABILITY OF NP-COMPLETE PROBLEMS

Abstract. An analysis of the unsolvability of Diophantine equations showed that problems of recognition of properties of the NP class are solvable, i.e., a non-deterministic algorithm or exhaustive search at the input of the problem gives a positive or negative answer. For polynomial Diophantine equations, such a non-deterministic algorithm does not exist. A simple version of Godel's theorem on the incompleteness of arithmetic follows from the unsolvability of Diophantine equations.

Keywords: NP-complete problems, Diophantine equations, non-deterministic algorithm.

Надійшла до редакції 06.04.2022