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.

© О.А. Вагіс, А.М. Гупал, 2022