УДК 511.528

О ДВОИЧНЫХ РЕШЕНИЯХ СИСТЕМ УРАВНЕНИЙ[1]

А. В. Селиверстов

Институт проблем передачи информации им. А. А. Харкевича Российской академии наук, г. Москва, Россия

Решение называется двоичным, если каждая переменная равна нулю или единице. Хорошо известно, что трудно найти двоичное решение системы алгебраических уравнений, коэффициенты которых являются целыми числами с малыми абсолютными значениями. Целью данной статьи является обоснование эффективного вероятностного сведения системы к одному новому уравнению в случае, когда существует небольшая разница между числом двоичных решений первого уравнения и числом двоичных решений всей системы. Более того, если первое уравнение линейное, то существует алгоритм псевдополиномиального времени для проверки правильности такого сведения к новому уравнению в общем случае.

Ключевые слова: *алгебраическое уравнение, вероятностный алгоритм, вычислительная сложность.*

DOI 10.17223/20710410/XX/1

ON BINARY SOLUTIONS TO SYSTEMS OF EQUATIONS

A. V. Seliverstov

Institute for Information Transmission Problems of the Russian Academy of Sciences (Kharkevich Institute), Moscow, Russia

E-mail: slvstv@iitp.ru

A solution is called binary if each variable is equal to either zero or one. It is well known that it is hard to find a binary solution to the system of algebraic equations whose coefficients are integers with small absolute values. The aim of the article is to propose an effective probabilistic reduction from the system to a new equation when there is a small difference between the number of binary solutions to the first equation and the number of binary solutions to the whole system. Moreover, if the first equation is linear, then there exists a pseudo-polynomial time algorithm to check the correctness of the reduction to the new equation in the general case.

Keywords: *algebraic equation, probabilistic algorithm, computational complexity.*

Введение

Рассмотрим поиск двоичных решений системы алгебраических уравнений с целыми коэффициентами. Иначе такие решения называют булевыми. Рассмотрим сведение исходной системы уравнений к системе с меньшим числом уравнений так, чтобы максимальная степень уравнений не возрастала, а коэффициенты новых уравнений были целыми числами, абсолютные величины которых не слишком велики по сравнению с коэффициентами в исходных уравнениях.

[1]Работа поддержана грантом РФФИ №18-29-13037.