

Федеральное государственное бюджетное учреждение науки
Институт математики им. С. Л. Соболева
Сибирского отделения Российской академии наук

Федеральное государственное автономное образовательное
учреждение высшего образования
«Новосибирский национальный исследовательский государственный университет»

Международная конференция

МАЛЬЦЕВСКИЕ ЧТЕНИЯ

10–14 ноября 2025 г.

Тезисы докладов



Международный математический центр
в Академгородке

Новосибирск • 2025

Sobolev Institute of Mathematics

Novosibirsk State University

International Conference

MAL'TSEV MEETING

November 10–14, 2025

Collection of Abstracts



International Mathematical Center
in Akademgorodok

Novosibirsk • 2025

О системах с числом линейных уравнений не менее половины от числа переменных

А. В. СЕЛИВЕРСТОВ

Рассмотрим систему из m линейных уравнений от n переменных над полиномиально вычислимым полем K , характеристика которого не равна двум.

$$\begin{cases} \alpha_{11}x_1 + \cdots + \alpha_{1n}x_n + \alpha_{10} = 0 \\ \cdots \\ \alpha_{m1}x_1 + \cdots + \alpha_{mn}x_n + \alpha_{m0} = 0 \end{cases}.$$

Задача о существовании $\{0, 1\}$ -решения, где каждая переменная принимает значения из множества $\{0, 1\}$, NP-полная. Мы рассмотрим алгоритм полиномиального времени, позволяющий при условии $m < n \leq 2m$ сводить почти любую исходную задачу к аналогичной задаче с большим числом линейно независимых уравнений. Хотя на малой доле входов (среди входов как-то ограниченного сверху размера) алгоритм не меняет систему, например, когда $\{0, 1\}$ -решений достаточно много. При этом исходная и новая системы всегда имеют одно и то же множество $\{0, 1\}$ -решений. Этот алгоритм получается небольшим изменением алгоритма из доклада [1], но теперь достаточно добавить лишь одно новое уравнение. Алгоритм основан на приведении к ступенчатому виду матрицы Маколея [2]. Это позволяет ускорить метод ветвей и границ для поиска $\{0, 1\}$ -решения, хотя в худшем случае требуется перебор большого числа оценок переменных.

Теорема. Пусть $\varepsilon > 0$, $m < n \leq 2m$ и произвольно фиксированы коэффициенты $\alpha_{11}, \dots, \alpha_{mn}$ линейных членов системы из m линейно независимых линейных уравнений от n переменных. Если свободные члены α_{i0} линейных уравнений независимо и равномерно распределены на множестве $S \subseteq K$ мощности $\lceil 1/\varepsilon \rceil$, то обсуждаемый алгоритм не добавляет ни одного линейно независимого линейного уравнения с вероятностью не выше числа ε .

Работа выполнена в рамках государственного задания ИППИ РАН, утвержденного Минобрнауки России.

ЛИТЕРАТУРА

- [1] A. V. Seliverstov, The generic-case complexity of finding a binary solution to a system of linear equations, Computer algebra: 6th International Conference Materials, June 23–25, 2025, Moscow: RUDN University (2025), pp.98–101. URL: <http://www.ccas.ru/ca/conference>
- [2] R. La Scala, F. Pintore, S.K. Tiwari, A. Visconti, A multistep strategy for polynomial system solving over finite fields and a new algebraic attack on the stream cipher Trivium, Finite Fields and Their Applications, **98**, No. 102452 (2024), pp.1–33. DOI: 10.1016/j.ffa.2024.102452

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

E-mail: SLVSTV@iitp.ru