БИБЛИОТЕКА
ЧЕБЫШЁВСКОГО
СБОРНИКА

Алгебра, теория чисел и дискретная геометрия: современные проблемы и приложения

Материалы
XV Международной конференции,
посвященной столетию
со дня рождения профессора
Николая Михайловича Коробова

Р Ф И

Библиотека Чебышевского сборника

Министерство образования и науки Российской Федерации
Российская академия наук
Московский государственный университет имени М. В. Ломоносова
Математический институт им. В. А. Стеклова РАН
Институт истории естествознания и техники им. С. И. Вавилова РАН
Московский педагогический государственный университет
Тульский государственный педагогический университет им. Л. Н. Толстого
Тульский государственный университет
Чебышевский фонд

АЛГЕБРА, ТЕОРИЯ ЧИСЕЛ И ДИСКРЕТНАЯ ГЕОМЕТРИЯ: СОВРЕМЕННЫЕ ПРОБЛЕМЫ И ПРИЛОЖЕНИЯ

Материалы XV Международной конференции, посвященной столетию со дня рождения профессора Николая Михайловича Коробова

Тула,
28–31 мая 2018 г.

Тула
ТГПУ им. Л. Н. Толстого
2018

ББК 22.132
УДК 511.6
А45

Алгебра, теория чисел и дискретная геометрия: современные проблемы
А45 и приложения: Материалы XV Междунар. конф., посвященной столетию со дня рождения профессора Николая Михайловича Коробова.– Тула: ТГПУ им. Л. Н. Толстого, 2018. – 382 с.

ISBN 978-5-6040489-4-8

ББК 22.132
УДК 511.6

Конференция проводится при финансовой поддержке РФФИ,
грант № 18-01-20030_г

ISBN 978-5-6040489-4-8

Теорема 1. *Пусть* $k \in \overline{1, n-1}$, *матрица* $A_k^{(n)}$ *и вектор-столбец* $b_k^{(n)}$ *построены на* k*-ом шагу алгоритма метода быстрых вращений. Тогда решение системы линейных уравнений (1) совпадает с точностью до перестановки координат с решением системы линейных уравнений (1) при* $k = 0$, *если* $\det(A_0^{(n)}) \neq 0$.

Теорема 2. *В условиях определения 1 решение системы линейных уравнений (1) при* $k = 0$ *может быть получено с помощью* $2n-1$ *шагов алгоритма метода быстрых вращений, если* $\det(A_0^{(n)}) \neq 0$.

Теорема 3. *Пусть* $n > 2$ *и* $\exists r, m \in \overline{2, n}, r < m : (a_{1,1}^{(n)})_r \neq 0, (a_{1,1}^{(n)})_m \neq 0$. *Пусть* $Q_1^{(n)}$ — *суперпозиция* $n-1$ *плоских вращений, определенных в [2], переводящих вектор-столбец* $a_{1,1}^{(n)}$ *в вектор-столбец* $||a_{1,1}^{(n)}||_2 \cdot \hat{\mathbf{e}}_1^{(n)}$, *и* $T_1^{(n)}$ *определено формулами (2), (3) при* $k = 1$. *Тогда*

$$(Q_1^{(n)}\hat{\mathbf{e}}_1^{(n)})_r = -\frac{(A^{(n)})_{r1}}{\sqrt{\sum\limits_{1\le k\le r}(A_k^{(n)})^2}} \neq (T_1^{(n)}\hat{\mathbf{e}}_1^{(n)})_r = -\frac{(A^{(n)})_{r1}}{\sqrt{\sum\limits_{1\le k\le n}(A^{(n)})_{k,1}^2}}.$$

Теорема 4. *Пусть* $k \in \overline{n+1, 2n-1}$ *и* $\hat{\mathbf{k}} = 2n - k \in n-1, ..., 1$. *Тогда в условиях определения 1 справедливо:*

$$\max_{\hat{\mathbf{k}}+1\le i\le n} |(A_{n-1}^{(n)})_{i,\hat{\mathbf{k}}}/(A_{n-1}^{(n)})_{\hat{\mathbf{k}},\hat{\mathbf{k}}}| \le 1, \quad |(A_{n-1}^{(n)})_{\hat{\mathbf{k}},\hat{\mathbf{k}}}| \ge |(A_{n-1}^{(n)})_{\hat{\mathbf{k}}+1,\hat{\mathbf{k}}+1}|.$$

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Уилкинсон Дж. Алгебраическая проблема собственных значений. — М.: Наука, 1970. 564 с., Wilkinson J.H. The algebraic eigenvalue problem. Clarendon press, Oxford, 1965.
2. Givens W. Computation of plane initary rotations transforming a general matrix to triangular form. J. Soc. Industrial Appl. Math, 1958, 6, 26-50.
3. Сорокин П. Н., Ченцова Н. Н. Расчетные формулы для модифицированного метода вращений // 25-ая международная конференция "Математика. Компьютер. Образование": тезисы докладов. Международная конференция (Пущино, 29 января - 3 февраля 2018 г.) — Москва-Ижевск, 2018, С. 151.
4. Деммел Дж. Вычислительная линейная алгебра. — М.: Мир, 2001, 430 с..

Московский государственный университет имени М. В. Ломоносова
Федеральной государственное учреждение Федеральный научный центр Научно-исследовательский институт системных исследований РАН (ФГУ ФНЦ НИИСИ РАН)
Lomonosov Moscow State University
The Federal National Promotion The Federal Scientific Centre Science Research Institute of the System Analyze at Russian Academy of Science (FNP FSC SRISA RAS)

УДК 511.528

Замечание о двоичных решениях некоторых систем алгебраических уравнений

А. В. Селиверстов (Россия, г. Москва)
slvstv@iitp.ru

Note on binary solutions to some systems of algebraic equations

A. V. Seliverstov (Russia, Moscow)
slvstv@iitp.ru

Рассмотрим $(0,1)$-решения системы алгебраических уравнений с целыми коэффициентами. Такие решения называются также двоичными или булевыми. Цель работы — 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.

Ограничение на степень уравнения существенно, поскольку любая система уравнений вида $\ell_k(\mathbf{x}) = 0$ эквивалентна над полем вещественных чисел одному уравнению $\sum_k \ell_k^2(\mathbf{x}) = 0$.

Ограничение на абсолютную величину коэффициентов тоже существенно, поскольку при достаточно быстро возрастающей последовательности чисел γ_k эта система имеет те же $(0,1)$-решения, что и одно уравнение $\sum_k \gamma_k \ell_k(\mathbf{x}) = 0$.

Теорема 1. *Дана система из m алгебраических уравнений $\ell_k(\mathbf{x}) = 0$, где числа $m > r > 0$. Пусть подсистема, состоящая из первых r уравнений $\ell_1(\mathbf{x}) = 0, \ldots, \ell_r(\mathbf{x}) = 0$ имеет не более μ избыточных $(0,1)$-решений, которые не служат решениями всей системы. Существуют такие целые числа $\gamma_{r+1}, \ldots, \gamma_m$ из отрезка от нуля до μ, что каждое $(0,1)$-решение новой системы алгебраических уравнений $\ell_1(\mathbf{x}) = 0, \ldots, \ell_r(\mathbf{x}) = 0$ и $\gamma_{r+1}\ell_{r+1}(\mathbf{x}) + \cdots + \gamma_m \ell_m(\mathbf{x}) = 0$ служит решением исходной системы.*

Доказательство. Если рассматриваемая подсистема не имеет $(0,1)$-решений или каждое $(0,1)$-решение подсистемы служит решением полной системы, то можно положить все искомые коэффициенты равными нулю: $\gamma_{r+1} = \cdots = \gamma_m = 0$.

Иначе определим подмножество множества всех $(0,1)$-точек

$$\mathcal{S} = \{\mathbf{x} \in \{0,1\}^n : \ell_1(\mathbf{x}) = 0 \wedge \cdots \wedge \ell_r(\mathbf{x}) = 0 \wedge (\exists k \leqslant m)\ell_k(\mathbf{x}) \neq 0\}.$$

Его мощность не превышает числа μ. Определим многочлен

$$f(y_{r+1}, \ldots, y_m) = \prod_{\mathbf{x} \in \mathcal{S}} \left(\sum_{k=r+1}^{m} \ell_k(\mathbf{x}) y_k \right)$$

Если множество $\mathcal{S}$ пустое, то полагаем $f = 1$, но этот случай уже рассмотрен в начале доказательства. Если некоторая последовательность чисел $\gamma_{r+1}, \ldots, \gamma_m$ достаточно быстро возрастает, то значение $f(\gamma_{r+1}, \ldots, \gamma_m)$ отлично от нуля. Следовательно, многочлен f не равен нулю тождественно. С другой стороны, выполнено неравенство $\deg f \leqslant \mu$. По лемме Шварца–Зиппеля [1], существуют искомые целые числа $\gamma_{r+1}, \ldots, \gamma_m$ из отрезка от нуля до μ.

□

Наиболее интересен случай, когда все уравнения линейные, абсолютные величины коэффициентов малы и первое уравнение имеет много $(0,1)$-решений, но почти каждое из них служит решением всей системы. Тогда исходная система сводится к одному линейному уравнению с малыми коэффициентами. Число всех его $(0,1)$-решений и некоторое $(0,1)$-решение можно вычислить за псевдополиномиальное время [2, 3]. Более точно, теорема позволяет свести эту систему линейных уравнений к системе двух уравнений. Переход от двух уравнений к одному, равному их линейной комбинации, приводит к относительно небольшому увеличению коэффициентов.

Требование, чтобы число μ было маленьким, существенно для практического применения рассмотренной сводимости, поскольку в общем случае задача распознавания существования некоторого $(0,1)$-решения у системы линейных уравнений с коэффициентами из множества $\{-1,0,1\}$ является NP-полной. С другой стороны, число μ является лишь верхней границей; не требуется знание точного значения разности чисел $(0,1)$-решений подсистемы и всей системы уравнений.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Schwartz J. T. Fast probabilistic algorithms for verification of polynomial identities // J. ACM 1980. Vol. 27, № 4. P. 701–717. doi:10.1145/322217.322225

2. Смолев В. В. Об одном подходе к решению булевого линейного уравнения с целыми положительными коэффициентами // Дискрет. матем. 1993. Т. 5, № 3. С. 81–89. Перевод: Smolev V. V. On an approach to the solution of a Boolean linear equation with positive integer coefficients // Discrete Math. Appl. 1993. Vol. 3, № 5. P. 523–530. doi:10.1515/dma.1993.3.5.523

3. Koiliaris K., Xu C. A faster pseudopolynomial time algorithm for subset sum // SODA '17 Proceedings of the Twenty-Eighth Annual ACM-SIAM Symposium on Discrete Algorithms, pp. 1062–1072. Society for Industrial and Applied Mathematics. Philadelphia, PA, USA, 2017.

Институт проблем передачи информации им. А.А. Харкевича Российской академии наук
Institute for Information Transmission Problems of the Russian Academy of Sciences (Kharkevich Institute)

УДК 511.32

Пути в дистанционных графах в конечномерных пространствах над конечным полем[1]

Ю. Н. Штейников (Россия, г. Москва)
yuriishte@mail.ru

Paths in the distance graphs in vector spaces over finite fields

Yu. N. Shteinikov (Rissia, Moscow)
yuriishte@mail.ru

Пусть $E \subset \mathbb{F}_q^d$ некоторое подмножество векторного пространства размерности $d-$ над конечным полем из q элементов. Мы определяем дистанционный граф на множестве вершин E так : две вершины x, y из E соединены ребром если $\| x-y \| = (x_1-y_1)^2 + \ldots + (x_d-y_d)^2 = 1$. В своем докладе я расскажу о больших путях в этом графе и представлю оценку на длину такого пути. Я также представлю некоторые результаты о таких дистанционных графах по работам [1], [2].

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. M. Bennett, J. Chapman, D. Covert, D. Hart, Al. Iosevich and J. Pakianathan // Long paths in the distance graph over large subsets of vector spaces over finite fields., J. Korean Math. Soc., 53 (1) (2016), 115–126.

[1]