НАЦИОНАЛЬНАЯ АКАДЕМИЯ НАУК БЕЛАРУСИ
Институт математики

МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

XIV БЕЛОРУССКАЯ МАТЕМАТИЧЕСКАЯ КОНФЕРЕНЦИЯ,

посвященная 65-летию Института математики НАН Беларуси

Материалы Международной научной конференции

В трех частях

Часть 3

Алгебра, геометрия и топология

Вычислительная математика

Математическая криптография и анализ данных

Дискретная математика и математическая кибернетика

Минск, 28 октября – 1 ноября 2024 года

Минск
«Беларуская навука»
2024

УДК 51
ББК 22.1
Ч-54

Составитель

кандидат физико-математических наук Т. С. Бусел

Ч-54 **XIV Белорусская математическая конференция, посвященная 65-летию Института математики НАН Беларуси :** материалы Международной научной конференции, Минск, 28 октября – 1 ноября 2024 г. В трех частях. Часть 3. – Минск : Беларуская навука, 2024. – 163 с.

ISBN 978-985-08-3224-5.

Третья часть сборника материалов на Международной научной конференции «XIV Белорусская математическая конференция» содержит доклады по следующим направлениям: алгебра, геометрия и топология, вычислительная математика, математическая криптография и анализ данных, дискретная математика и математическая кибернетика.

Для научных работников, преподавателей и студентов, а также всех, кто интересуется математикой.

УДК 51
ББК 22.1

ISBN 978-985-08-3224-5 (ч. 3)
ISBN 978-985-08-3221-4

давно начались и до сих пор не утихают споры о том, что следует считать величиной [2]. Важно подчеркнуть, что величина является одним из важнейших исходных понятий теории измерений, да и всей современной науки. Известные специалисты по теории шкал, выражают обеспокоенность что несмотря на очевидную важность конструктивной теории измерений, до сих пор не нашлось желающих построить такую теорию или хотя бы наметить ее структуру [2].

Концепция измерения отношений предлагает вернуться к классической теории измерений, которую следует дополнить следующими принципами:

1. Все однородные величины равноправны: каждая величина может быть единицей измерения.
2. Отношения величин не зависят от выбора шкалы измерений.

Такой подход является конструктивным и включает обоснованную классификацию шкал измерений [3].

Литература

1. Michell J. *Quantitative science and the definition of measurement in psychology* //British journal of Psychology. 1997. Vol. 88, No 3. P. 353–383.

2. Кнорринг В. Г. *Философия и измерительная наука* // Труды. СПбГТУ. 2008. № 8. С. 87–92.

3. Романчак В. М., *Субъективные измерения (теория рейтингов)* // Журнал Белорусского государственного университета. Философия. Психология. 2020. № 3. С. 87–98.

О СИСТЕМАХ НЕСКОЛЬКИХ УРАВНЕНИЙ ПО МОДУЛЮ ТРИ

А.В. Селиверстов, О.А. Зверков

Институт проблем передачи информации им. А.А. Харкевича Российской академии наук,
Большой Каретный переулок 19, с. 1, 127051 Москва, Россия, {slvstv,zverkov}@iitp.ru

Обозначим через $GF(3)$ поле вычетов по модулю три. Мы называем $(0,1)$-решением такое решение системы уравнений, в котором каждая переменная принимает значения из множества $\{0,1\}$. Получены достаточные условия существования $(0,1)$-решения у системы линейных уравнений над полем $GF(3)$, в которой число уравнений мало по сравнению с числом переменных. Новые результаты дополняют ранее полученные [1, 2].

Рассмотрим систему линейных уравнений, нетривиально зависящую от переменной x_k. Новая система линейных уравнений получена из исходной системы исключением переменной x_k, если новая система не зависит от переменной x_k, а исходная система эквивалентна объединению новой системы и ровно одного уравнения, равного линейной комбинации уравнений исходной системы. В геометрии исключение переменной соответствует проекции на координатное подпространство.

Лемма 1. *Даны натуральные числа n и m, удовлетворяющие неравенствам $n \geqslant 5$, $m \geqslant 2$ и $m \leqslant \log_3(2n-1)$, и система из m линейных уравнений от n переменных над полем $GF(3)$. Пусть для каждого индекса $1 \leqslant k \leqslant n$ существует уравнение, нетривиально зависящее от переменной x_k. Если у этой системы нет $(0,1)$-решения, то существует такой индекс $k \leqslant n$, что исключение переменной x_k приводит к новой системе, у которой нет $(0,1)$-решения. Более того, эта новая система может быть найдена за полиномиальное время $O(mn\log_2(n+1))$.*

Набросок доказательства. Для системы $A\mathbf{x} = \mathbf{b}$ исключаются переменные, соответствующие пропорциональным друг другу столбцам в матрице A. Это возможно над полем $GF(3)$.

Замечание. Лемма 1 позволяет перейти от исходной системы, содержащей достаточно мало уравнений, к новой системе от меньшего числа переменных и с меньшим числом уравнений. Далее неравенство из условия леммы 1 может быть нарушено, что помешает сделать следующий шаг. Поэтому в условии указанной ниже теоремы предполагается выполнение более сильного ограничения. С другой стороны, вычислительные эксперименты со случайными матрицами позволяют надеяться, что такой рекурсивный спуск возможен для почти всех исходных систем при условии типа $m = O(\log_3 n)$, близком к неравенству из леммы 1.

Лемма 2. *Дана система линейных уравнений от n переменных над полем $GF(3)$*

$$\left\{\begin{array}{rcl} a_{11}x_1+\cdots+a_{1n}x_n & = & b_1 \\ \cdots & & \\ a_{m1}x_1+\cdots+a_{mn}x_n & = & b_m \end{array}\right.$$

и целое число $1 \leqslant s \leqslant n$. Эта система имеет $(0,1)$-решение тогда и только тогда, когда $(0,1)$-решение имеет новая система, в которой для каждого $1 \leqslant j \leqslant m$ в j-ом уравнении коэффициент a_{js} при переменной x_s заменяется линейной комбинацией коэффициентов

$$c_j = 2b_j - \sum_{k=1}^{n} a_{jk}.$$

Теорема. *Существует алгоритм полиномиального времени, который получает на вход систему из m линейных уравнений от n переменных над полем $GF(3)$ и при выполнении условия $m \leqslant \log_3 \log_3 (2n-1)$ принимает вход тогда и только тогда, когда система имеет $(0,1)$-решение.*

Обсуждаемый алгоритм реализован на языке Python. Листинг программы и примеры доступны по адресу http://lab6.iitp.ru/-/havoc. Входом служит $m \times (n+1)$ матрица M. Обозначим через $\mathbf{b}$ последний столбец этой матрицы, а через A подматрицу, расположенную в первых n столбцах, кроме последнего. Столбец $\mathbf{b}$ содержит свободные члены уравнений, а матрица A состоит из коэффициентов линейных членов. Соответствующая система уравнений имеет вид $A\mathbf{x} = \mathbf{b}$.

Если матрица A пустая, то линейные части всех уравнений равны нулю, а сами уравнения превращаются в тождества $0 = 0$ или ложные равенства $0 = 1$ или $0 = 2$. Матрица M изменяется так, что новая система линейных уравнений имеет $(0,1)$-решение тогда и только тогда, когда исходная система уравнений имеет $(0,1)$-решение. При этом числа строк и столбцов никогда не возрастают. В цикле выполняются шаги, соответствующие леммам 1 и 2, пока матрица M не стабилизируется или не будет выполнено дополнительное условие остановки. При этом для полученной системы уравнений существование или отсутствие $(0,1)$-решения легко проверяется при выполнении условий теоремы.

Пример. Системе уравнений от двух переменных x_1 и x_2 над полем $GF(3)$

$$\left\{\begin{array}{rcl} 2x_1+2x_2 & = & 1 \\ x_1+2x_2 & = & 1 \end{array}\right.$$

соответствует расширенная матрица

$$M = \begin{pmatrix} 2 & 2 & 1 \\ 1 & 2 & 1 \end{pmatrix}.$$

Среди первых двух столбцов нет линейно зависимых, но можно применить лемму 2. Столбец

$$\mathbf{c} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$$

пропорционален первому столбцу в матрице M. Заменяя второй столбец, получаем матрицу

$$\begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \end{pmatrix}.$$

Поскольку первые два столбца пропорциональны друг другу, возможно исключение переменных, которое приводит к ложному равенству $0 = 2$. Следовательно, $(0,1)$-решений нет.

Экспериментально показано, что алгоритм намного эффективнее для разреженных систем уравнений. Более того, метод двоичного поиска позволяет найти некоторое $(0,1)$-решение системы, когда оно существует, хотя перечисление всех $(0,1)$-решений может быть слишком трудным. Это открывает возможность практического использования для решения тех прикладных задач, которые легко свести к поиску $(0,1)$-решения системы линейных алгебраических уравнений, в частности, для решения задач математической биологии.

Работа выполнена с использованием вычислительных ресурсов Межведомственного суперкомпьютерного центра Российской академии наук (МСЦ РАН).

Исследование выполнено за счет гранта Российского научного фонда № 24-44-00099, https://rscf.ru/project/24-44-00099/.

Литература

1. Бойков А. А., Селиверстов А. В. *О кубе и проекциях подпространства* // Вестник Удмуртского университета. Математика. Механика. Компьютерные науки. 2023. Т. 33, № 3. С. 402–415. DOI: 10.35634/vm230302

2. Zverkov O. A., Seliverstov A. V. *Effective lower bounds on the matrix rank and their applications* // Programming and Computer Software. 2023. Vol. 49, No. 5. P. 441–447. DOI: 10.1134/S0361768823020160

СИНТЕЗ ГИПЕРКОНТАКТНЫХ И КОНТАКТНО-ТРАНСФОРМАТОРНЫХ СХЕМ

Ю.Г. Таразевич

Белорусский государственный университет,
Независимости 4, 220030 Минск, Беларусь, tarazevichyg@mail.ru

В классах $\text{РМ}_F^{(n)}$ *расширенных матриц над кольцами полиномов с идемпотентными переменными* [1] определяются подклассы (*гиперконтактных схем*): $\text{ГС}_F^{(n)}$ (над произвольным полем F) и $\text{ГС}_Z^{(n)}$ (над кольцом Z целых чисел), — алгебраически расширяющие класс матриц инциденций *контактных схем* [2] ($\text{КС}^{(n)}$) и реализующие произвольные *булевы функции* (БФ), зависящие от n переменных, со сложностью менее $3\sqrt{2}\cdot 2^{n/2}$ контактов. Для матриц класса $\text{ГС}_Z^{(n)}$ предлагается физическая интерпретация в виде матриц инциденций-зацеплений *контактно-трансформаторных схем* ($\text{ТКС}^{(n)}$) [3].

1. Гиперконтактные схемы. Обозначим: F — произвольное поле; $F[X^{(n)}]$ — *кольцо полиномов с идемпотентными переменными* [1], $X^{(n)} = \{x_1, \ldots, x_n\}$; $\ominus$ и $*$ — вычитание и умножение в $F[X^{(n)}]$.

Из элементов поля F построим произвольную $k\times(l+1)$-матрицу

$$\begin{array}{|c|c|c|c|c|}\hline A_1 & A_2 & \cdots & A_l & B \\ \hline \end{array} \tag{1}$$

с выделенным столбцом B (k и $l+1$ — произвольные натуральные числа). При $l > 0$ каждый столбец A_j умножим на какой-нибудь полином $p_j \in \{x_1, 1\ominus x_1, x_2, 1\ominus x_2, \ldots, x_n, 1\ominus x_n, 1\} \subset\subset F[X^{(n)}]$. В результате получим $\text{РМ}_F^{(n)}$-*матрицу* [1] следующего специального вида:

$$\begin{array}{cccc} & & & f \\ \hline \multicolumn{1}{|c|}{p_1{*}A_1} & \multicolumn{1}{c|}{p_2{*}A_2} & \multicolumn{1}{c|}{\cdots\ p_l{*}A_l} & \multicolumn{1}{c|}{B} \\ \hline \end{array} = \begin{array}{ccccc} p_1 & p_2 & \cdots & p_l & f \\ \hline \multicolumn{1}{|c|}{A_1} & \multicolumn{1}{c|}{A_2} & \multicolumn{1}{c|}{\cdots} & \multicolumn{1}{c|}{A_l} & \multicolumn{1}{c|}{B} \\ \hline \end{array}, \tag{2}$$

реализующую (в соответствии с [1]) на выделенном столбце B некоторую булеву функцию (БФ) $f(x_1, \ldots, x_n)$. Справа в (2) матрица представлена в «удобном» для нее *окаймленном виде* [3], т.е. с метками-множителями p_j над константными столбцами A_j и «нейтральной» (т.е. не являющейся множителем) меткой f выделенного столбца.

Определение. Любую $\text{РМ}_F^{(n)}$-матрицу вида (2) будем называть $\text{ГС}_F^{(n)}$-*матрицей* или, иначе, *гиперконтактной схемой над полем* F, ее выделенный столбец B — *источником*, столбцы $1{*}A_j$ — *проводниками*, столбцы $x_i{*}A_j$ или $(1\ominus x_i){*}A_j$ — *контактами*, константную матрицу (1) — *топологической матрицей* гиперконтактной схемы (2) [3].

Замечание. Для любого поля F через $\text{КС}_F^{(n)}$ обозначим множество всех $\text{ГС}_F^{(n)}$-матриц, в каждом ненулевом столбце топологической матрицы которых ровно два ненулевых элемента — единица и минус единица поля F. Любая $\text{КС}_F^{(n)}$-матрица M, записанная в окаймленном виде (см. (2)), естественным образом, независимо от поля F, рассматривается как *матрица инциденций* [4] двухполюсной *контактной схемы* [2] S_M, дополненной *источниковым ребром* [1], соединяющим полюсы, и содержащей обычные (*свободно ориентируемые* [3]) замыкающие (x_i) и размыкающие ($\bar{x}_i = 1\ominus x_i$) контакты, проводники (с меткой 1) и «свободные» петли (инцидентные произвольным вершинам), соответствующие нулевым (или пустым) столбцам $\text{КС}_F^{(n)}$-матрицы M.