О НЕКОТОРЫХ ОСОБЕННОСТЯХ ЗАДАЧИ РАЗРЕШИМОСТИ СИСТЕМ БУЛЕВЫХ УРАВНЕНИЙ

***Леонтьев В.К.*[1] *, Гордеев Э.Н.*[2]**

Цель статьи: *представить новые результаты по комбинаторным характеристикам систем булевых уравнений, от которых зависят такие свойства систем как совместность, разрешимость, число решений и ряд других.*

Метод исследования*: сведение прикладных задач к комбинаторным моделям с последующим применением классических методов комбинаторики: метод производящих функций, метод коэффициентов, методы получения асимптотик и пр.*

Полученный результат. *В работе получены результаты, касающиеся разрешимости систем булевых уравнений. Проанализирована сложность задачи «трансформации» несовместной системы в совместную. Описан и обоснован подход к решению задачи о выделении из несовместной системы минимального числа совместных подсистем. Задача сведена к проблеме нахождения минимального протыкающего множества. Получен критерий совместности системы. С помощью метода коэффициентов выведены формулы для нахождения и оценки числа решений при параметризации задачи по правым частям уравнений. Исследуется и максимум этого числа в зависимости от параметра. Получены формулы числа решений для двух частных случаев: при ограничении на число уравнений и на размер параметров задачи.*

Ключевые слова: *NP-полнота, задача булева программирования, совместные системы, линейное преобразование, производящие функции, параметрические задачи.*

Грант РФФИ 20-01-00645.

DOI: 10.21681/2311-3456-2021-1-18-28

Введение

Линейные диофантовы уравнения и неравенства являются стандартным объектом для различного рода математических моделей, относящихся к целочисленной оптимизации, защите информации, теории чисел, геометрии и т.д.

Каноническими целями подобных исследований, обычно, являются следующие:

1. Условия разрешимости.
2. Представление натуральных чисел линейными формами (проблема Фробениуса).
3. Нахождение числа решений уравнения или системы уравнений, оценка этого числа.
4. Нахождение числа целых точек в многогранниках или оценка этого числа.
5. Исследование характеристик задачи при изменении системы ограничений путем удаления или добавления нового ограничения.

История исследований в этой области и перечень даже основных результатов не может быть описана в рамках отдельной статьи, поэтому мы лишь коротко коснемся тех работ, которые либо непосредственно связаны с данной статьей, либо проясняют и дополняют ее содержание.

Классическая задача о ранце с булевыми переменными имеет вид:

$$\sum_{j=1}^{n} A_j x_j \to \max ;$$

$$\sum_{i=1}^{n} a_i x_i \le b \quad , \qquad (1)$$

где $x=(x_1,,x_n)$ – n-мерный булевский вектор.

1 Леонтьев Владимир Константинович, доктор физико-математических наук, профессор, профессор кафедры «Информационная безопасность» (ИУ-8) МГТУ им. Н.Э. Баумана, Москва, Россия. E-mail: vkleontiev@yandex.ru

2 Гордеев Эдуард Николаевич, доктор физико-математических наук, профессор, профессор кафедры «Информационная безопасность» (ИУ-8) МГТУ им. Н.Э.Баумана, Москва, Россия. E-mail: werhorn@yandex.ru

Пусть $L(x_1,\ldots,x_n)$ – линейная форма:

$$L(x_1,\ldots,x_n)=\sum_{i=1}^{n} a_i x_i\,, \qquad (2)$$

где все параметры $\{a_i\}$ и неизвестные $\{x_i\}$ – натуральные числа. Накладывая определенные условие на вид этой формы, можно получить разные частные случаи общей задачи.

Так, в булевой задаче о ранце переменные полагаются булевыми, а множество решений должно удовлетворять условию $\sum_{i=1} a_i x_i \le b$, то есть вектора $x=(x_1,\ldots,x_n)$ должны лежать ниже гиперплоскости $L(x_1,\ldots,x_n)=b$.

Известно, что существуют эквивалентные формы задачи линейного программирования: общая, каноническая и стандартная. (В разных случаях терминология различается). Следуя [1], канонической будем считать задачу с ограничениями в виде равенств.

В матричной форме система ограничений имеет вид

$$\mathrm{Ax=b}, \qquad (3)$$

где $A=\left\|a_{ij}\right\|-(m,n)$ – матрица.

Накладывая определенные ограничения на матрицу A и вектор b, получаем различные частные случаи задачи.

Если все параметры и переменные – произвольные вещественные числа, то вопрос о разрешимости системы решается в терминах ранга матрицы ограничений. Классические результаты линейной алгебры и теории линейного и булева программирования исследуют условия разрешимости и для таких частных случаев рассматриваемой задачи как задача целочисленного линейного программирования и задача булева программирования. См., например, [1], [3].

В области исследования операций и комбинаторной оптимизации данная задача или ее обобщения и сужения занимаю ключевое место, как это показано, например, в [1]. То, что задача целочисленного линейного программирования является NP-полной, было установлено в числе первых результатов подобных исследований. Кроме того, в классической работе [2] можно найти многочисленные примеры известных задач, которые к ней сводятся и наоборот: задача целочисленного линейного программирования (или ее булев вариант) сводится к той или иной проблеме.

В предыдущих работах авторов [4] и [5] для задачи о рюкзаке рассматривался, в частности, и вопрос зависимости числа решений от параметров задачи: вектора целевой и весовой функций и правой части ограничения. Настоящая работа в одной из своих частей является продолжением исследований авторов, опубликованных в [4]-[5]. Ключевую роль в получении результатов там сыграл аппарат производящих функций, который используется и в настоящей статье. Как видно из подробнейшей монографии [6], данный подход позволил в упомянутых работах получить ряд новых и оригинальных результатов по сравнению с ранее известными.

Следует заметить, что вопросы, поставленные в первой части работы, ранее с той или иной точки зрения рассматривались в работах В.К. Леонтьева и Г.П. Тонояна [7] и [8], где исследовались комбинаторные свойства систем булевых уравнений. В монографии [9] ряд результатов также получены на основе комбинаторных подходов в задачах рюкзачного типа.
Заметим, что комбинаторные свойства систем линейных, булевых и диофантовых уравнений тесно связаны с задачами криптографии и используются в криптосистемах.

С прикладной точки зрения, изучаемая проблематика затрагивалась авторами в связи с криптографическими объектами: аннигиляторами и алгебраической иммунностью. Одно из ключевых утверждений работы [10], посвященной аннигиляторам и алгебраической иммунности, базируется на анализе совместимости системы уравнений и нахождению комбинаторной характеристики (аналога ранга) матрицы.
В [10]-[11], где речь идет о линейных булевых полиномах, как частный случай возникают линейные булевы полиномы. Именно им там посвящено наибольшее внимание.

Важность этой тематики с точки зрения криптографии подтверждается многочисленными работами в специализированных журналах. Например, в работах Г.В. Балакина [12] и [13] рассматриваются специфические классы систем булевых уравнений (рекуррентного типа) и их применение в криптографии. В

DOI: 10.21681/2311-3456-2021-1-18-28

работе А.М. Зубкова [14] моментные характеристики весов векторов в случайных двоичных линейных кодах описываются в терминах свойств специальных систем уравнений.

Линеаризация систем булевых уравнений – метод решения систем, состоящий в замене всех мономов степени выше первой новыми переменными, решении полученной линейной системы и последующей проверке полученных решений на корректность. Этому, например, посвящены статьи [15], [16].
Группой ученых под руководством Н. Куртуа были предложены усовершенствования XL4 и XSL5 метода линеаризации для случаев, когда количество уравнений в системе недостаточно для эффективного применения линеаризации в классическом виде [17]. Суть данных методов состоит в дополнении системы новыми уравнениями, которые не меняют множества решений системы, но увеличивают размер системы и ранг линеаризованной системы. Позднее Н. Куртуа и Г.В. Бардом в [18] был предложен еще один метод, основанный на методе линеаризации ElimLin.

Как сказано выше в аннотации, в нашей работе рассматривается задача проверки системы на совместность и разбиение несовместной системы на минимальное число совместных подсистем. Это задача, в частности, тесно связана с проблемой выполнимости КНФ. Результаты на этом пути иллюстрируются работами [19-21]. А в прикладных работах А.С. Мелузова [22] и [23] разработан и имплементирован программный комплекс для решения упомянутой задачи.

В данной статье также рассматривается проблема параметризации системы по ее правой части. Аналоги приведенного здесь подхода авторам неизвестны. В какой-то степени с ним связаны как классические алгоритмы параметрического линейного программирования, так и, например, работа [24], где исследуются линейные уравнения булева типа с «искаженной» правой частью. В работе предложен метод построения множества, содержащего искомый вектор с вероятностью, не менее заданной, и оценена мощность этого множества. Теоретические расчеты параметров метода иллюстрируются результатами экспериментов. Данный подход использует вероятностную постановку, в то время как здесь применяется комбинаторный аппарат.

Настоящая работа состоит из введения и двух разделов. Следующий раздел посвящен подходам к анализу несовместной системе уравнений. Затем рассматривается вопрос существования и числа решений. Некоторые определения, понятия и методы доказательств ранее были использованы авторами в работах [4], [5], [25], [26], [27].

Везде в дальнейшем будем считать, что все параметры рассматриваемой задачи, числа $c_1,\ldots,c_n$; $a_1,\ldots,a_n$; b – неотрицательные целые числа.

1. О «приближенных» решениях несовместных систем уравнений с булевыми переменными

Рассмотрим систему (3) с произвольными переменными.

При использовании задачи линейного программирования в прикладных моделях реальных систем несовместность системы (3) может иметь следующую интерпретацию.

В прикладной математической модели, для описания которой используется, например, система линейных уравнений достаточно естественна следующая ситуация: уравнения, описывающие модель, неравноценны: одни из них описывают «важные и глобальные» аспекты прикладной проблемы, а другие – «второстепенные», причем связь этих частей не выяснена или ошибочно интерпретирована. Это делает естественным на стадии моделирования применение следующих эвристических подходов, которые рассмотрены ниже:

1. В одном из них путем «изменения» вида уравнений или удаление части из них конструируется из несовместной системы совместная.
2. В другом – предлагается разбить исходную систему (множество ее уравнений) на некоторое количество (например, на минимально возможное) совместных подсистем.

Второй подход связан с самым известным и распространенным методом: выделение (за счет отбрасывания минимально возможного количества уравнений) из системы максимальной по мощности совместной подсистемы. На этом пути, как правило, используются варианты переборного алгоритма в сочетании с эвристиками. В прикладном плане подобные работы относятся к различным областям, в первую очередь, видимо, стоит сказать о задачах в сфере распознавания образов.
Обозначим через $a_1,\ldots,a_m$ вектор-строки матрицы A. Вектора $b, a_1,\ldots,a_m$ назовем параметрами системы (3)

Проблема. Пусть система (3) несовместна. Какое минимальное число параметров системы (3) нужно изменить, чтобы новая система стала совместной?

Пример 1. Уравнение $2x_1+3x_2=6$ не имеет решения в булевых переменных, но достаточно изменения одного параметра, чтобы сделать его разрешимым. Например, так измененные уравнения: $3x_1+3x_2=6$ или $2x_1+3x_2=5$ уже имеют решения в булевых переменных.

Теорема 1. Для того, чтобы сделать несовместную систему линейных уравнений вида (3) совместной при $m>1$ достаточно изменения $(m-1)$ параметра. Существуют несовместные системы вида (3), для которых изменение этого числа параметров является необходимым.

Доказательство. Пусть дан вектор $c=(c_1,\ldots,c_n)$. Рассмотрим несовместную систему

$$\begin{cases}(A,x)=b_1\\(c,x)=b_2\\\quad\ldots\\(c,x)=b_m\end{cases}$$

Где $b_i\neq b_j$ для всех $i\neq j$. Ясно, что следующая система

$$\begin{cases}(c,x)=b_1\\(c,x)=b_1\\\quad\ldots\\(c,x)=b_1\end{cases}$$

является совместной и получена из исходной путем изменения $m-1$ параметра, причем изменение вектора $c=(c_1,\ldots,c_n)$ никак не отражаются на свойстве системы быть совместной. Изменение же меньшего числа параметров не приводит к совместности системы.

С другой стороны, если система

$$\begin{cases}(a_1,x)=b_1\\(a_2,x)=b_2\\\quad\ldots\\(a_m,x)=b_m\end{cases}$$

является несовместной, то система

$$\begin{cases}(a_1,x)=b_1\\(a_2,x)=(a_2,x_0)=b_2'\\\quad\ldots\\(a_m,x)=(a_m,x_0)=b_m'\end{cases}$$

является совместной при любом x_0 таком, что $(a_1,x_0)=b_1$. И вновь изменения $m-1$ параметра достаточно.
Теорема доказана.

Замечание. В случае одного уравнения в теореме $m-1$ меняется на m, как это видно из вышеприведенного примера с булевым уравнением.

Проблема. Пусть система (3) несовместна. Требуется разбить ее на минимальное количество совместных подсистем.

Замечание. В ряде работ применительно к данной проблеме используется термин *обобщенное решение* системы уравнений. Под ним понимается следующее. Если несовместная система разбита на r совместных подсистем, то эти системы можно решить. Пусть решениями которых являются вектора $u_1, u_2,\ldots, u_r$. Тогда множество $\{u_1, u_2,\ldots,u_r\}$ и называют *обобщенным решением* системы (3).

Перейдем к описанию метода разбиения несовместной системы на минимальное число совместных.
Рассмотрим систему (3) с булевыми переменными.
Пусть

$$\begin{cases}(a_1,x)=f_1(x)\\(a_2,x)=f_2(x)\\\quad\ldots\\(a_m,x)=f_m(x)\end{cases}$$

И $L^*(f_1),L^*(f_2),\ldots,L^*(f_m)$ – множество значений, принимаемых функциями $f_1,\ldots,f_m$ на B^n.
Пусть x_0 –решение какой-то системы

$$\begin{cases}(a_1,x)=f_1(x)=b_1\\(a_2,x)=f_2(x)=b_2\\\quad\ldots\\(a_m,x)=f_m(x)=b_m\end{cases}\qquad(4)$$

Наличие такого x_0 свидетельствует о совместности (4). Но это означает, что для существования такого решения необходимым и достаточным условием является выполнение соотношения

DOI: 10.21681/2311-3456-2021-1-18-28

$$b_i \in \bigcap_{k=1}^{m} L^*(f_k), i = 1,...,m.$$

Обозначим через $L^*(a)$ - множество решений уравнения $L(x)=a$, т.е. множество булевых векторов, доставляющих значение a линейной форме $L(x)$.

Таким образом система уравнений $L_i(x)=a_i$, $i=1,...,m$, «порождает» систему подмножеств $\{L_i^*(a_i)\} = V_i \subseteq 2^{B^n}$.

Определение. Подмножество $M \subseteq B^n$ называется протыкающим для системы множеств $V=\{V_i\}$, если выполняется условие $M \cap V_i \neq \varnothing$.

Из этого следует, что элементы протыкающего множества имеют «представителей» в каждом из подмножеств системы. В нашем случае это означает, что каждое из уравнений системы (4) «удовлетворяется» хотя бы одной из точек протыкающего множества. В частности, если $|M|=1$, то M является единственным (обычным) решением системы (4).

В общем случае, если $M=\{y_1,...,y_r\}$ – протыкающее множество для V и U_i – множество уравнений из системы (4), для которых точка y_i является решением, тогда разбиение множества уравнений $\{L_i^*(a_i)\} = \bigcup_{i=1}^{r} U_i$ есть разбиение на подсистемы, каждая из которых совместна.

Таким образом мы показали, что нахождение протыкающего множества наименьшей мощности эквивалентно разбиению несовместной системы на минимальное число совместных подсистем.
Формально это выглядит следующим образом.

Определение. Подмножество T строк (0,1) – матрицы A называется покрытием, если в подматрице $A`$, образованной этими строками, нет нулевых столбцов.

Чисто строк $|T|$ называется мощностью покрытия, а минимум этой величины по всем покрытиям матрицы – глубиной матрицы. Обозначим эту величину через $\xi(A)$.
Пусть $B^n = \{x_1, x_2, ..., x_{2^n}\}$ и $V=\{W_1,...,W_m\}$, где $W_i = \{L_i^*(a_i)\}, i = 1,...,m.$ Рассмотрим $(0,1)$-матрицу $W=||w_{ij}||$ размеров $2^n x m$, где

$$w_{ij} = \begin{cases} 1, если & x_j \in W_i \\ 0, если & x_j \notin W_i \end{cases}.$$

Теорема 2. Минимальное число совместных подсистем, на которое можно разбить систему (4) равно глубине матрицы W.

Доказательство непосредственно следует из проведенного выше рассмотрения.

Пример 2. Рассмотрим следующую несовместную систему уравнений:

$$\begin{cases} L_1 = x_1 + x_2 + x_3 = 1 \\ L_2 = x_1 + 2x_2 + x_3 = 2 \\ L_3 = x_1 + 2x_2 + 3x_3 = 3 \end{cases}.$$

Для нее имеем $L_1^*(1) = \{(001),(010),(100)\}$, $L_2^*(2) = \{(010),(101)\}$ $L_3^*(3) = \{(001),(110)\}$. Тогда вышеупомянутая матрица W имеет вид

$$W = \begin{Vmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{Vmatrix}.$$

Покрытиями матрица являются, например, подмножества $\begin{Vmatrix} 101 \\ 010 \end{Vmatrix}, \begin{Vmatrix} 110 \\ 001 \end{Vmatrix}$, а $\xi(W)=2$.

Непосредственной проверкой убеждаемся, что исходная несовместная система из трех уравнений разбивается на две совместные, например, следующие: первое и второе уравнение – это одна система, а третье – другая. Мы видим, что покрытие состоит более, чем из одного множества (т.е. $|M|=2>1$), поэтому и разбиение на подсистемы не одно.

2. О числе решений системы булевых уравнений

Для случая системы булевых уравнений NP-полной проблемой является уже ответ на вопрос: совместна ли эта система уравнений?

Поэтому получение нижней оценки числа решений системы булевых уравнений является достаточно естественной задачей. Если хотя бы в каких-то случаях оценка эта дает значение, не меньшее единицы, то это может иметь практическую пользу, так как дает решение *NP*-полной задачи о разрешимости системы булевых уравнений.

Очевидный алгоритм проверки разрешимости задачи булева программирования – перебор всех 2^n булевых векторов. Но этот метод не дает понимания, от чего зависит разрешимость системы (в отличие от классического случая системы линейных уравнений).

Обозначим через $t_{b_1\ldots b_m}(A)$ – число решений задачи булева программирования с системой ограничений вида Ax=b, где $A=\|a_{ij}\|-(m,n)$ – матрица.

Зафиксируем матрицу ограничений и будем варьировать вектор правых частей. Получим последовательность чисел $\{t_{b_1\ldots b_m}(A)\}$. Для этой последовательности построим производящую функцию $F_A(z_1,\ldots,z_m)$ в виде полинома

$$F_A(z_1,\ldots,z_m)=\sum_{\{b_1,\ldots,b_m\}} z_1^{b_1}z_2^{b_2}\ldots z_m^{b_m}t_{b_1\ldots b_m}(A).$$

Напомним, что согласно введенным обозначениям, вектор $(a_{1k},\ldots,a_{mk})$ – это k-й столбец матрицы ограничений.

Лемма 1. Справедлива формула:

$$F_A(z_1,\ldots,z_m)=\prod_{k=1}^{n}(1+z_1^{a_{1k}}\ldots z_m^{a_{mk}}).$$

Эта лемма дает возможность найти число решений задачи булева программирования в зависимости от параметров A и b. Рассмотрим пример ее использования.

Пример 3. Рассмотрим задачу.

$$x_1+x_2+\ldots+x_n=b_1$$

$$x_2+x_3+\ldots+x_{n+1}=b_2.$$

Здесь матрица ограничений имеет вид $A=\begin{Vmatrix}11\ldots10\\01\ldots11\end{Vmatrix}$.

Из леммы 1 следует, что $F_A(z_1,z_2)=(1+z_1)(1+z_1z_2)^{n-1}(1+z_2)$. Отсюда видно, что мономы с положительными коэффициентами $z_1^{\alpha_1}z_2^{\alpha_2}$ определяют те вектора (b_1,b_2), для которых система ограничений разрешима.

Пример 4. Для n=4 рассмотрим следующий пример.

$$x_1+x_2+x_3=b_1$$

$$x_2+x_3+x_4=b_2$$

Здесь матрица ограничений имеет вид $A=\begin{Vmatrix}1110\\0111\end{Vmatrix}$.

Из леммы 1 следует, что $F_A(z_1,z_2)=$

$=(1+z_1)(1+z_1z_2)^2(1+z_2)=1+z_1+z_2+3z_1z_2+$

$+2z_1^2z_2+2z_1z_2^2+2z_1^2z_2^2+z_1^3z_2^3+z_1^2z_2^3+z_1^3z_2^2$ Отсюда следует, что система разрешима для следующих векторов правых частей: (0,0), (0,1), (1,0), (1,1), (2,1), (1,2), (2,2), (2,3), (3,2), (3,3).

Непосредственно из доказанной леммы 1 следует утверждение.

Следствие. Число разрешимых систем булевых уравнений вида Ax=b равно числу мономов, входящих с ненулевыми коэффициентами в полином $F_A(z_1,\ldots,z_m)$.

Заметим теперь, что число различных мономов в полиноме $F_A(z_1,\ldots,z_m)$ не может превышать его степени. Поэтому отсюда получаем еще одно соотношение.

Следствие. Число разрешимых систем булевых уравнений вида Ax=b не превышает степени полинома $F_A(z_1,\ldots,z_m)$.

Рассмотрим теперь еще одну комбинаторное свойство системы уравнений, которое можно исследовать с помощью доказанной леммы.

Пусть система разрешима. Мы пытаемся решить задачу с помощью какой-нибудь эвристики, задающей правило перебора по всему B^n. Чем больше доля решений, тем быстрее на это решение можно «наткнуться».

В связи с этим интересны оценки числа $t_{b_1\ldots b_m}(A)$. Следующая теорема дает одну такую оценку.

DOI: 10.21681/2311-3456-2021-1-18-28

Теорема 3. Пусть $v = \sum_{k=1}^{n} \max_{r=1,\dots,m} a_{rk}$, тогда справедливо неравенство:

$$\max_{\{b_1,\dots,b_m\}} t_{b_1\dots b_m}(A) \geq \frac{2^n}{m^v} \qquad (5)$$

Конечно, оценка (5) очень слабая и бывает полезна только в специальных случаях. Но так и должно быть, так как проблема проверки разрешимости задачи булева программирования является *NP*- трудной, а проверка соотношения (5) может быть осуществлена за полиномиальное по входу время. (Конечно, нужно заметить, что в этом случае мы имеем не конкретную индивидуальную задачу булева программирования, а семейство таких задач, параметризованное по $\{b_1,\dots,b_m\}$.)

Пример 5. Пусть есть система из двух уравнений и A – (0,1) –матрица.

Тогда $m=2$ и $v \leq n$.

Из (5) получаем $\max_{\{b_1,b_2\}} t_{b_1b_2}(A) \geq 1$.

Используя для анализа системы «комбинацию» из леммы 1 и теоремы 4, можно выбирать наиболее информативный результат. Этот факт иллюстрирует следующие примеры.

Пример 6. Рассмотрим систему уравнений:

$$x_1+2x_2+3x_3+4x_4=b_1$$

$$2x_1+x_2+x_3+3x_4=b_2.$$

Тогда из приведенной выше леммы имеем:

$$F_A(z_1,z_2) = \qquad (6)$$
$$= (1+z_1z_2^2)(1+z_1^2z_2)(1+z_1^3z_2)(1+z_1^4z_2^3)$$

Раскрывая скобки видим, что моном максимальной степени $z_1^{10}z_2^7$. Поэтому правая часть (5) меньше единицы.

Но приводя подобные в (6) видим, что $\max_{\{b_1,b_2\}} t_{b_1b_2}(A) = 2$ и максимум достигается на парах $b_1=4,\ b_2=3$ и $b_1=6,\ b_2=4$. (Для первого случая это решения (0,0,0,1) и (1,0,1,0), а для второго – (0,1,0,1) и (1,1,1,0)).

Пример 7. Рассмотрим систему уравнений:

$$x_1+x_2+x_3+x_4=b_1$$

$$x_2+2x_4=b_2$$

$$F_A(z_1,z_2) = (1+z_1z_2)(1+z_1)^2(1+z_1z_2^2) \qquad (7)$$

Раскрывая скобки видим, что моном максимальной степени $z_1^4z_2^3$. Поэтому правая часть в (5) вновь меньше единицы.

Но приводя подобные в (7) видим, что $\max_{\{b_1,b_2\}} t_{b_1b_2}(A) = 2$ и максимум достигается на парах $b_1=2,\ b_2=1$; $b_1=2,\ b_2=2$ и $b_1=3,\ b_2=3$. (Для первого случая это решения (1,1,0,0) и (0,1,1,0), для второго – (0,0,1,1) и (1,0,0,1), а для третьего – (0,1,1,1) и (1,1,0,1)).

Рассмотрим теперь вопрос о числе решений системы булевых уравнений с несколько иной точки зрения.

Ответ на вопрос, разрешимо ли одно уравнение $L(x_1,\dots,x_n)= \sum_{i=1}^{n} a_ix_i = b$ в булевых переменных, все еще *NP*-полная задача.

Например, к этой задаче сводится известная *NP*-полная задача о камнях (задача о разбиении конечного числа взвешенных объектов (камней) на две части равного веса), состоящая в проверке разрешимости в булевых переменных уравнения:

$$\sum_{i=1}^{n} a_ix_i = \sum_{i=1}^{n} a_i(1-x_i).$$

Пример 8. Требуется разбить множество $M=\{2,3,5,6\}$ на два подмножества с одинаковыми суммами. Тогда вышеприведенное уравнение имеет вид:

$2x_1 + 3x_2 + 5x_3 + 6x_4 = 2(1-x_1) + 3(1-x_2) +$
$+ 5(1-x_3) + 6(1-x_4)$ или $4x_1+6x_2+10x_3+12x_4=16$. Его решением является вектор $x=(1001)$, что соответствует разбиению $M=\{2,6\} \cup \{3,5\}$.

Рассмотрим линейную форму (2) с булевыми переменными. Множество значений этой линейной формы обозначим, как и ранее, через $L^*(a_1,\dots,a_n)$. (А если это не вызывает неопределенности, то просто через L^*).

Сама же форма $L(x_1,\dots,x_n)= \sum_{i=1}^{n} a_ix_i$ зависящая от переменных $x_1,\dots,x_n$, будет для краткости обозначать-

ся через L. Приведем несколько примеров соотношения $a_1,\dots,a_n$ и $L^*(a_1,\dots,a_n)$.

Пример 9. Если $a_i=1,\ i=1,\dots,n,$ то $L^*=\{0,1,2,\dots,n\}$.

Пример 10. Если $a_i=2^{i-1},\ i=1,\dots,n,$ то $L^*=\{0,1,2,\dots,2^n-1\}$.

Пример 11. Если $L(x_1,\dots,x_n)=x_1+x_2+\dots+x_{n-1}+nx_n$, то $L^*=\{0,1,\dots,n,n+1,\dots,2n-1\}$. В этом случае уравнение $L(x_1,\dots,x_n)=b$ имеет решение для всех b, удовлетворяющих условию $0\le b\le 2n-1$.

Пример 12. Если $L(x_1,\dots,x_n)=2x_1+3x_2+3x_3+3x_4$, то $L^*=\{0,2,3,5,6,8,9,11\}$. В этом случае уравнение $L(x_1,\dots,x_n)=b$ имеет решение для всех b, удовлетворяющих условию $0\le b\le 11$, кроме $b=1,4,7,10$.

Просто из введенных определений получаем следующее очевидное утверждение.

Утверждение. Уравнение $L(x)=b$ разрешимо тогда и только тогда, когда $b\in L^*$.

Заметим, что $L^*(a_1,\dots,a_n)$ не зависит от упорядоченности элементов $a_1,\dots,a_n$, поэтому в дальнейшем будем считать, что

$$a_1\le a_2\dots\le a_n. \qquad (8)$$

Определение. Формы $L_1(x_1,\dots,x_n)$ и $L_2(x_1,\dots,x_n)$ называются эквивалентными, если $L_1^* = L_2^*$.
Пусть, как обычно, n –число переменных, а N – целое число такое, что

$$1\le a_k\le N,\ k=1,\dots,n. \qquad (9)$$

Через $t(n,N)$ обозначим число линейных форм с параметрами n и N.

Лемма 2. Справедливо равенство $t(n,N)=C_{N+n-1}^n$.

Доказательство. Каждая линейная форма с условиями (8) и (9) может быть закодирована в алфавите $\{1,\dots,N\}$ словом вида $1^{y_1}2^{y_2}\dots N^{y_N}$, где y_r, $r=1,\dots,N,$ – число коэффициентов равных r, среди чисел $a_1,\dots,a_n$. Отсюда следует, что искомое число слов $t(n,N)$ – это число решений уравнения $y_1+y_2+\dots+y_N=n, y_i\ge 0, i=1,\dots,N$. Но отсюда и следует равенство $t(n,N)=C_{N+n-1}^n$.

Лемма доказана.
Пусть, как и раньше $t_b(a_1,\dots,a_n)$ - число решений уравнения $L(x_1,\dots,x_n)=\sum_{i=1}^n a_ix_i=b$.

Лемма 3. Справедливо соотношение

$$t_b(a_1,\dots,a_n)=\frac{1}{2\pi i}\oint_{|u|=r}\frac{(1+u^{a_1})\dots(1+u^{a_n})}{u^{b+1}}du,\ \rho<1.$$

Рассмотрим теперь вопрос о среднем значении $t_b(a_1,\dots,a_n)$ для фиксированного значения b по всему булеву кубу при условиях (8) и (9).

Обозначим это число через $\overline{t_b}$.

С учетом (8), (9) из леммы 3 имеем следующее соотношение.

$$\overline{t_b}=\frac{1}{C_{n+N-1}^n}\sum_{i=1}^n\sum_{a_i=a_{i-1}}^N t_b(a_1,\dots,a_n).$$

(Здесь считаем, что $a_0=1$).

Лемма 4. Справедлива формула

$$\overline{t_b}=\frac{1}{C_{n+N-1}^n}\frac{1}{2\pi i}\oint_{|u|=\rho}\frac{\left(N+\frac{u-u^{N+1}}{1-u}\right)^n}{u^{b+1}}du,\ \rho<1. \qquad (10)$$

Рассмотрим в качестве примера случай трех переменных при произвольном N. (Здесь ρ<1.)

Теорема 4. Для случая трех переменных справедливо соотношение:

$$\overline{t_b}=\frac{N^2}{C_{N+1}^2}\delta^b+\frac{2N}{C_{N+1}^2}+\frac{2N}{C_{N+1}^2}\delta^{b-N},$$

где δ – некоторая константа.

Рассмотрим теперь случай $N=2$ при произвольном количестве переменных. Пусть, как обычно, $\|x\|=\sum_{i=1}^n x_i$.

Теорема 5. При $N=2$ и произвольном n справедливо соотношение:

$$\overline{t_b}=\frac{1}{n+1}\sum_{k=0}^n C_n^kC_k^{b-k}2^{n-k}. \qquad (11)$$

Пример 13. Пусть $N=2,\ n=3$. Из (11) имеем

$\overline{t_b}=\frac{1}{n+1}\sum_{k=0}^n C_n^kC_k^{b-k}2^{n-k}=\frac{1}{4}\sum_{k=0}^3 C_3^kC_k^{b-k}2^{3-k}$. Отсю-

DOI: 10.21681/2311-3456-2021-1-18-28

да получаем $\bar{t}_1 = \frac{1}{4}(2+3+1+0) = 3/2$, $\bar{t}_2 = \frac{1}{4}(2+3+2+3) = 5/2$, $\bar{t}_3 = \frac{1}{4}(2+1+2+0) = 5/4$, $\bar{t}_4 = \frac{1}{4}(1+0+1+3) = 5/4$, $\bar{t}_5 = \frac{1}{4}$, $\bar{t}_6 = \frac{1}{4}$.

Видно, что максимальное значение $\bar{t}_b$ достигается при $b=2$.

3. Заключение

В работе рассмотрены вопросы, связанные с разрешимостью систем булевых уравнений.

Предложен подход к анализу комбинаторных характеристик систем уравнений с целью выделения из несовместной системы минимального числа совместных подсистем. Рассмотрены возможности трансформации несовместной системы в совместную путем изменения части параметров системы.

Исследованы вопросы нахождения числа решений системы в зависимости от правых частей уравнений.

Полученные в работе результаты могут представлять интерес для прикладных разработок в различных областях дискретной оптимизации и исследования операций, а также в распознавании образов, криптографии и системах защиты информации.

Литература

1. Пападимитриу Х., Стайглиц С. Комбинаторная оптимизация. Алгоритмы и сложность. М.: Мир, 1985. 512 с.
2. Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи М.: Мир, 1982. 416 с.
3. Схрейвер А. Теория линейного и целочисленного программирования. М.: Мир.1991. 360 с.
4. Леонтьев В.К., Гордеев Э.Н. Производящие функции в задаче о ранце // Доклады Академии наук . 2018 . Т. 481. № 5. С. 478 – 480. DOI: 10.31857/S086956520002139-5.
5. Леонтьев В.К., Гордеев Э.Н. О некоторых комбинаторных свойствах задачи о рюкзаке // Журнал вычислительной математики и математической физики. 2019. Т. 59. № 8.С. 1439-1447. DOI: 10.1134/S0044466919080076.
6. Kellerer H., Pferschy U., Pisinger D. Knapsack problems. Berlin: Springer, 2004. 548 p.
7. Леонтьев В.К., Тоноян Г.П. Приближенные решения систем булевых уравнений // Журнал вычислительной математики и математической физики 1993. Т. 33. № 9. С. 1383-1390.
8. Леонтьев В.К., Тоноян Г.П. О системах булевых уравнений // Журнал вычислительной математики и математической физики. 2013. Т. 53. № 5. С. 109-116.
9. Кузюрин Н.Н., Фомин С.А. Эффективные алгоритмы и сложность вычислений. М.: МФТИ, 2007. 311 с. ISBN 5-7417-0198-1
10. Леонтьев В.К., Гордеев Э.Н. Об алгебраической иммунности систем кодирования // Вопросы кибербезопасности, 2019, №1. С. 59-89. DOI: 10.21681/2311-3456-2019-1-59-68.
11. Гордеев Э.Н., Леонтьев В.К., Медведев Н.В. О свойствах булевых полиномов, актуальных для криптосистем // Вопросы кибербезопасности, 2017, №3. С. 63-69. DOI: 10.21681/2311-3456-2017-3-63-69.
12. Балакин Г.В. О решении некоторых классов систем булевых уравнений рекуррентного типа // Математические вопросы криптографии. 2013. Т.4. №1. С. 5–25. DOI: 10.4213/mvk71.
13. Балакин Г.В. О возможности частичного восстановления некоторых последовательностей по наблюдениям // Математические вопросы криптографии. 2013. Т.4. №4. С. 7–25. DOI: 10.4213/mvk97.
14. Зубков А.М. Круглов В.И. Моментные характеристики весов векторов в случайных двоичных линейных кодах // Математические вопросы криптографии. 2013. Т.3. №4. С. 55–70. DOI: 10.4213/mvk67.
15. Faug`re J.-C. A new efficient algorithm for computation Grebner e o bases (F4) // Journal of pure and applied algebra. 1999. Vol. 139. Issues 1–3. P. 61-88. DOI: 10.1016/S0022-4049(99)00005-5.
16. Faug`re J-C. A new efficient algorithm for computation Grebner e o bases without reduction to zero (F5) // Proceedings of the 2002 international symposium on Symbolic and algebraic computation 2002. P.75–83. DOI: 10.1145/780506.780516.
17. Courtois N., Pieprzyk J. Cryptanalysis of block chiphers with overdened systems of equations // Proc. 8th Int. Conf. on the Theory and Application of Cryptology and Information Security. 2002. Springer. P. 267–287.
18. Courtois N, Bard G.V. Algebraic cryptanalysis of the data encryption standard // IMA International Conference on Cryptography and Coding Theory. Lecture Notes in Computer Science. Springer-Verlag. 2007. P. 152-169. DOI: 10.1007/3-540-36178-2_17.
19. Massacci F, Marraro L. Logical Cryptanalysis as a SAT Problem // Journal of Automated Reasoning. Springer Netherlands. 2000. Vol. 24. P. 165-203. DOI:10.1023/A:1006326723002.
20. Fiorini C., Martinelli E., Massacci F. How to fake an RSA signature by encoding modular root nding as a SAT problem // Discrete Applied Mathematics. 2003.Vol. 130. P. 101-127.

21. Mironov I., Zhang L. Applications of SAT Solvers to Cryptanalysis of Hash Functions// In: Biere A., Gomes C.P. (eds) Theory and Applications of Satisfiability Testing - SAT 2006. SAT 2006. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg. Vol. 4121. P. 102-115. DOI: 10.1007/11814948_13
22. Мелузов А.С. Построение эффективных алгоритмов решения систем полиномиальных булевых уравнений методом опробования части переменных // Дискретная математика. 2011. Т. 23. № 4. С. 66–79.
23. Мелузов А.С. О криптоанализе LILI-128, основанном на частичном опробовании и мономиальной совместности систем полиномиальных уравнений // Сборник работ молодых ученых факультета ВМК МГУ. 2011. № 8. С.99–107.
24. Alekseev E.K., Oshkin I.V., Popov V.O., Smyshlyaev S.V., Solving systems of linear Boolean equations with noisy right-hand sides over the reals // Discrete Math. Appl. 2018. Vol. 28. №1. P. 1–5. DOI:10.1515/dma-2018-0001.
25. Леонтьев В.К. О псевдобулевых полиномах // Журнал вычислительной математики и математической физики. 2015. Т. 55. № 11. С. 1952–1958. DOI: 10.7868/S0044466915110113.
26. Леонтьев В.К. Комбинаторика и информация. Часть 1. Комбинаторный анализ. М.: МФТИ, 2015. 174 с.
27. Леонтьев В.К. Комбинаторика и информация. Часть 2. Информационные модели. М.: МФТИ, 2015. 112 с.

ON SOME FEATURES OF THE PROBLEM OF SOLVABILITY OF SYSTEMS OF BOOLEAN EQUATIONS

***Leontiev V. K.*[3] *, Gordeev E. N.*[4]**

The purpose of the article *is to present new results on combinatorial characteristics of systems of Boolean equations, on which such properties of systems as compatibility, solvability, number of solutions and a number of others depend.*

The research method *is the reduction of applied problems to combinatorial models with the subsequent application of classical methods of combinatorics: the method of generating functions, the method of coefficients, methods for obtaining asymptotics, etc.*

Obtained result. *In this paper, we obtain results concerning the solvability of systems of Boolean equations. The complexity of the problem of " transformation" of an incompatible system into a joint one is analyzed. An approach to solving the problem of separating the minimum number of joint subsystems from an incompatible system is described and justified. The problem is reduced to the problem of finding the minimum covering set. The system compatibility criterion is obtained. Using the method of coefficients, formulas for finding and estimating the number of solutions for parameterizing the problem on the right-hand sides of equations are derived. The maximum of this number is also investigated depending on the parameter. Formulas for the number of solutions for two special cases are obtained: with a restriction on the number of equations and on the size of the problem parameters.*

Keywords: *NP-completeness, Boolean programming problem, joint systems, linear transformation, generating functions, parametric problems.*

RFBR grant 20-01-00645

References

1. Papadimitriu KH., Stai`glitc S. Kombinatornaia optimizatciia. Algoritmy` i slozhnost`. M.: Mir, 1985. 512 s.
2. Ge`ri M., Johnson D. Vy`chislitel`ny`e mashiny` i trudnoreshaemy`e zadachi M.: Mir, 1982. 416 s.
3. Skhrei`ver A. Teoriia linei`nogo i tcelochislennogo programmirovaniia. M.: Mir.1991. 360 s.

3 Vladimir Leontiev, Dr.Sc. (in Math.), Professor, professor of the Department of Information Security (IU-8) of Moscow State University, N.E. Bauman, Moscow, Russia. E-mail: vkleontiev@yandex.ru

4 Eduard Gordeev, Dr.Sc. (in Math.), Professor, professor of the Department of Information Security (IU-8) of Moscow State University, N.E. Bauman, Moscow, Russia. E-mail: werhorn@yandex.ru.

DOI: 10.21681/2311-3456-2021-1-18-28

4. Leont`ev V.K., Gordeev E`.N. Proizvodiashchie funktcii v zadache o rantce // Doclady` Akademii nauk . 2018 . T. 481. № 5. S. 478 – 480. DOI: 10.31857/S086956520002139-5.
5. Leont`ev V.K., Gordeev E`.N. O nekotory`kh kombinatorny`kh svoi`stvakh zadachi o riukzake // Zhurnal vy`chislitel`noi` matematiki i matematicheskoi` fiziki. 2019. T. 59. № 8.S. 1439-1447. DOI: 10.1134/S0044466919080076.
6. Kellerer H., Pferschy U., Pisinger D. Knapsack problems. Berlin: Springer, 2004. 548 p.
7. Leont`ev V.K., Tonoian G.P. Priblizhenny`e resheniia sistem bulevy`kh uravnenii` // Zhurnal vy`chislitel`noi` matematiki i matematicheskoi` fiziki 1993. T. 33. № 9. S. 1383-1390.
8. Leont`ev V.K., Tonoian G.P. O sistemakh bulevy`kh uravnenii` // Zhurnal vy`chislitel`noi` matematiki i matematicheskoi` fiziki. 2013. T. 53. № 5. S. 109-116.
9. Kuziurin N.N., Fomin S.A. E`ffektivny`e algoritmy` i slozhnost` vy`chislenii`. M.: MFTI, 2007. 311 s. ISBN 5-7417-0198-1
10. Leont`ev V.K., Gordeev E`.N. Ob algebraicheskoi` immunnosti sistem kodirovaniia // Voprosy` kiberbezopasnosti, 2019, №1. S. 59-89. DOI: 10.21681/2311-3456-2019-1-59-68.
11. Gordeev E`.N., Leont`ev V.K., Medvedev N.V. O svoi`stvakh bulevy`kh polinomov, aktual`ny`kh dlia kriptosistem // Voprosy` kiberbezopasnosti, 2017, №3. S. 63-69. DOI: 10.21681/2311-3456-2017-3-63-69.
12. Balakin G.V. O reshenii nekotory`kh classov sistem bulevy`kh uravnenii` rekurrentnogo tipa // Matematicheskie voprosy` kriptografii. 2013. T.4. №1. S. 5–25. DOI: 10.4213/mvk71.
13. 13. Balakin G.V. O vozmozhnosti chastichnogo vosstanovleniia nekotory`kh posledovatel`nostei` po nabliudeniiam // Matematicheskie voprosy` kriptografii. 2013. T.4. №4. S. 7–25. DOI: 10.4213/mvk97.
14. Zubkov A.M. Kruglov V.I. Momentny`e harakteristiki vesov vektorov v sluchai`ny`kh dvoichny`kh linei`ny`kh kodakh // Matematicheskie voprosy` kriptografii. 2013. T.3. №4. S. 55–70. DOI: 10.4213/mvk67.
15. Faug`re J.-C. A new efficient algorithm for computation Grebner e o bases (F4) // Journal of pure and applied algebra. 1999. Vol. 139. Issues 1–3. P. 61-88. DOI: 10.1016/S0022-4049(99)00005-5.
16. Faug`re J-C. A new efficient algorithm for computation Grebner e o bases without reduction to zero (F5) // Proceedings of the 2002 international symposium on Symbolic and algebraic computation 2002. P.75–83. DOI: 10.1145/780506.780516.
17. Courtois N., Pieprzyk J. Cryptanalysis of block chiphers with overdened systems of equations // Proc. 8th Int. Conf. on the Theory and Application of Cryptology and Information Security. 2002. Springer. P. 267–287.
18. Courtois N, Bard G.V. Algebraic cryptanalysis of the data encryption standard // IMA International Conference on Cryptography and Coding Theory. Lecture Notes in Computer Science. Springer-Verlag. 2007. P. 152-169. DOI: 10.1007/3-540-36178-2_17.
19. Massacci F, Marraro L. Logical Cryptanalysis as a SAT Problem // Journal of Automated Reasoning. Springer Netherlands. 2000. Vol. 24. P. 165-203. DOI:10.1023/A:1006326723002.
20. Fiorini C., Martinelli E., Massacci F. How to fake an RSA signature by encoding modular root nding as a SAT problem // Discrete Applied Mathematics. 2003.Vol. 130. P. 101-127.
21. Mironov I., Zhang L. Applications of SAT Solvers to Cryptanalysis of Hash Functions// In: Biere A., Gomes C.P. (eds) Theory and Applications of Satisfiability Testing - SAT 2006. SAT 2006. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg. Vol. 4121. P. 102-115. DOI: 10.1007/11814948_13
22. Meluzov A.S. Postroenie e`ffektivny`kh algoritmov resheniia sistem polinomial`ny`kh bulevy`kh uravnenii` metodom oprobovaniia chasti peremenny`kh // Diskretnaia matematika. 2011. T. 23. № 4. S. 66–79.
23. Meluzov A.S. O kriptoanalize LILI-128, osnovannom na chastichnom oprobovanii i monomial`noi` sovmestnosti sistem polinomial`ny`kh uravnenii` // Sbornik rabot molody`kh ucheny`kh fakul`teta VMK MGU. 2011. № 8. S.99–107.
24. Alekseev E.K., Oshkin I.V., Popov V.O., Smyshlyaev S.V., Solving systems of linear Boolean equations with noisy right-hand sides over the reals // Discrete Math. Appl. 2018. Vol. 28. №1. P. 1–5. DOI:10.1515/dma-2018-0001.
25. Leont`ev V.K. O psevdobulevy`kh polinomakh // Zhurnal vy`chislitel`noi` matematiki i matematicheskoi` fiziki. 2015. T. 55. № 11. S. 1952–1958. DOI: 10.7868/S0044466915110113.
26. Leont`ev V.K. Kombinatorika i informatciia. Chast` 1. Kombinatorny`i` analiz. M.: MFTI, 2015. 174 s.
27. Leont`ev V.K. Kombinatorika i informatciia. Chast` 2. Informatcionny`e modeli. M.: MFTI, 2015. 112 s.