Оптимизация, системный анализ и исследование операций

© 2021 г. В.К. ЛЕОНТЬЕВ, д-р физ.-мат. наук (vkleontiev@yandex.ru)
(ВЦ им. А.А. Дородницына ФИЦ ИУ РАН, Москва),
Э.Н. ГОРДЕЕВ, д-р физ.-мат. наук (werhorn@yandex.ru)
(МГТУ им. Н.Э. Баумана, Москва)

О ЧИСЛЕ РЕШЕНИЙ СИСТЕМЫ БУЛЕВЫХ УРАВНЕНИЙ[1]

Рассматриваются вопросы, касающиеся разрешимости и числа решений систем булевых уравнений. Многие математические модели, возникающие как в исследовании операций, так и в криптографии, описываются на языке таких систем. Это связано, в частности, и с тем, что в общем виде проблема проверки совместности таких систем уравнений является NP-полной, поэтому исследование качественных свойств системы булевых уравнений дает дополнительную информацию, позволяющую либо выделить полиномиально разрешимые частные случаи, либо повысить эффективность переборных схем. Основное внимание уделено двум аспектам. Первый касается исследования наличия и числа решений булева уравнения и системы уравнений при параметризации задачи по правым частям. Даются формулы и оценки для подсчета этого числа как в общем, так и в частных случаях. Исследуется и его максимум в зависимости от указанного параметра. Второй аспект посвящен частному случаю задачи, когда уравнение задается так называемой непрерывной линейной формой. Изучаются свойства таких форм и различные критерии непрерывности.

Ключевые слова: NP-полнота, булевы уравнения, задача булева программирования, линейное преобразование, непрерывная линейная форма.

DOI: 10.31857/S0005231021090063

1. 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.

Классическая задача о ранце с булевыми переменными имеет вид

$$\sum_{j=1}^{n} c_j x_j \to \max, \qquad \sum_{i=1}^{n} a_i x_i \le b, \tag{1}$$

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

[1] Работа выполнена при поддержке Российского фонда фундаментальных исследований (проект № 20-01-00645).

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

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

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.

Таким образом, множество допустимых решений должно удовлетворять условию $\sum_{i=1}^{n} a_i x_i \le b$, т.е. векторы $x = (x_1, \ldots, x_n)$ должны лежать ниже гиперплоскости $L(x_1, \ldots, x_n) = b$.

В матричной форме система ограничений имеет вид

$$\mathbf{A}\mathbf{x} = \mathbf{b}, \tag{3}$$

где $\mathbf{A} = (a_{ij})_{m \times n}$ – матрица.

Накладывая определенные ограничения на матрицу $\mathbf{A}$ и вектор $\mathbf{b}$, получаем различные частные случаи задачи, см., например, [1, 2].

Если все параметры и переменные – произвольные вещественные числа, то вопрос о разрешимости системы решается в терминах ранга матрицы ограничений.

Из этих результатов линейной алгебры можно получить необходимые условия разрешимости и для таких частных случаев задачи, как задача целочисленного линейного программирования и задача булева программирования, см., например, [1–3].

В области исследования операций и комбинаторной оптимизации данная задача целочисленного линейного программирования или ее обобщения и сужения занимают ключевое место, как это показано, например, в [1]. То, что задача является NP-полной, было установлено в числе первых результатов подобных исследований. Кроме того, в классической публикации [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.

Данная статья в одной из своих частей является продолжением исследований авторов этой работы, опубликованных в [4, 5], где речь шла про задачу о рюкзаке. 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 получить ряд новых и оригинальных результатов.

Следует заметить, что вопросы, поставленные в статье, ранее с той или иной точки зрения, рассматривались в статьях В.К. Леонтьева и Г.П. Тонояна [7, 8]. В монографии [9] ряд результатов получен на основе комбинаторных подходов в задачах рюкзачного типа.

С прикладной точки зрения, изучаемая проблематика затрагивалась авторами в связи с криптографическими объектами: аннигиляторами и алгеб-

раической иммунностью. Одно из ключевых утверждений публикации [10], посвященной аннигиляторам и алгебраической иммунности, базируется на анализе совместимости системы уравнений и сводится к нахождению комбинаторной характеристики (аналога ранга) матрицы.

В [10, 11], где речь идет о булевых полиномах, как частный случай возникают линейные булевы полиномы.

Исследования в той же области, но другими методами проводились в институтах Екатеринбурга и Новосибирска. В качестве примеров можно привести работы [12, 13].

Статья состоит из четырех разделов. Раздел 2 посвящен применению метода производящих функций для исследования решений системы уравнений. Затем рассматривается как общий случай, так и частные случаи задачи. Раздел 3 посвящен комбинаторным свойствам линейных форм $L(x_1, \ldots, x_n)$. В разделе 4 приведены выводы.

Некоторые определения, понятия и методы доказательств ранее были использованы авторами этой статьи в публикациях [4, 5, 14–16].

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.

2. О числе решений системы булевых уравнений

Актуальность исследования наличия решений системы булевых уравнений вытекает из того факта, что NP-полной проблемой является уже ответ на вопрос: совместна ли система булевых 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 прикладное значение, так как решается NP-полная задача. Кроме того, получение такой оценки основывается на учете комбинаторики задачи, в то время как очевидный алгоритм проверки разрешимости задачи булева программирования – перебор всех 2^m булевых векторов – 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 $\mathbf{Ax} = \mathbf{b}$, где $\mathbf{A} = (a_{ij})_{m \times n}$ – матрица.

Зафиксируем матрицу ограничений и будем варьировать вектор правых частей. Получим последовательность чисел $\{t_{b_1 \ldots b_m}(A)\}$, где $t_{b_1 \ldots b_m}(A)$ – количество решений системы для фиксированного вектора правых частей.

Для этой последовательности имеем производящую функцию $F_A(z_1, \ldots, z_n)$ в виде полинома

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

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

Лемма 1. Справедлива формула

$$F_A(z_1, \ldots, z_m) = \prod_{k=1}^{n} (1 + z_1^{a_{1k}} \ldots z_m^{a_{mk}}). \tag{4}$$

Доказательство.

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

$$= \sum_{x \in B^n} z_1^{a_{11}x_1 + \ldots + a_{1n}x_n} z_2^{a_{21}x_1 + \ldots + a_{2n}x_n} \ldots z_m^{a_{m1}x_1 + \ldots + a_{mn}x_n} =$$

$$= \sum_{x_1=0}^{1} z_1^{a_{11}x_1} z_2^{a_{21}x_1} \ldots z_m^{a_{m1}x_1} \sum_{x_2=0}^{1} z_1^{a_{21}x_2} z_2^{a_{22}x_2} \ldots z_m^{a_{m2}x_2} \ldots$$

$$\ldots \sum_{x_B=0}^{1} z_1^{a_{1n}x_n} z_2^{a_{2n}x_n} \ldots z_m^{a_{mn}x_n} =$$

$$= (1 + z_1^{a_{11}} z_2^{a_{21}} \ldots z_m^{a_{m1}})(1 + z_1^{a_{12}} z_2^{a_{22}} \ldots z_m^{a_{m2}}) \ldots (1 + z_1^{a_{1n}} z_2^{a_{2n}} \ldots z_m^{a_{mn}}) =$$

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

Лемма 1 доказана.

Этот подход дает возможность найти число решений задачи булева программирования в зависимости от параметров $\mathbf{A}$ и $\mathbf{b}$.

Пример 1. Рассмотрим задачу:

$$x_1 + x_2 + \ldots + x_n = b_1,$$
$$x_2 + x_3 + \ldots + x_{n+1} = b_2.$$

Здесь матрица ограничений задана и имеет вид

$$\mathbf{A} = \begin{pmatrix} 11 \ldots 10 \\ 01 \ldots 11 \end{pmatrix}.$$

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

В частности, для $n = 3$ рассмотрим следующий пример:

$$x_1 + x_2 + x_3 = b_1,$$
$$x_2 + x_3 + x_4 = b_2.$$

Здесь матрица ограничений задана и имеет вид

$$\mathbf{A} = \begin{pmatrix} 1110 \\ 0111 \end{pmatrix}.$$

Из леммы 1 следует, что

$$F_A(z_1, z_2) = (1 + z_1)(1 + z_1 z_2)^2(1 + z_2) =$$
$$= 1 + z_1 + z_2 + 3z_1 z_2 + 2z_1^2 z_2 + 2z_1 z_2^2 + 2z_1^2 z_2^2 + z_1^3 z_2^3.$$

Отсюда видим, 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).

Кроме того, непосредственно из доказанной леммы 1 следует утверждение.

Следствие 1. Число разрешимых систем булевых уравнений вида $\mathbf{Ax} = \mathbf{b}$ *равно числу мономов, входящих с ненулевыми коэффициентами в полином* $F_A(z_1, \ldots, z_n)$.

Так как в рассматриваемом случае матрица системы фиксируется, то будем считать, что различные *разрешимые системы* отличаются значением вектора правых частей, при котором обе системы имеют решение. Заметим теперь, что число различных мономов в полиноме $F_A(z_1, \ldots, z_n)$ не может превышать его степени. Поэтому отсюда получаем еще одно утверждение.

Следствие 2. Число разрешимых систем булевых уравнений вида $\mathbf{Ax} = \mathbf{b}$ *не превышает степени полинома* $F_A(z_1, \ldots, z_n)$.

Рассмотрим теперь еще одну комбинаторную задачу, которую можно решить с помощью доказанной леммы 1.

Пусть система разрешима. Мы ищем ее решения с помощью какой-нибудь эвристики, задающей правило перебора по всему B^n. Чем больше у системы решений, тем быстрее на какое-то из них можно "наткнуться". Если решаем не произвольную систему уравнений, а отражающую специфику некоторой прикладной задачи исследования операций, то особенности этой задачи отражаются на параметрах системы, в частности на векторе правых частей.

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

Теорема 1. Пусть $v = \sum\limits_{k=1}^{n} \max\limits_{r=1,\ldots,m} a_{rk}$, *тогда справедливо неравенство*

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

Доказательство. С одной стороны, сумма всех коэффициентов полинома $F_A(z_1, \ldots, z_n)$ *равна* $F_A(1, \ldots, 1)$, *т.е. равна* 2^n.

Из леммы 1 имеем

$$F_A(z_1, \ldots, z_n) = \sum_{\{b_1,\ldots,b_m\}} z_1^{b_1} z_2^{b_2} \ldots z_n^{b_m} t_{b_1 \ldots b_m}(A) = \prod_{k=1}^{n} (1 + z_1^{a_{1k}} \ldots z_m^{a_{mk}}). \tag{6}$$

Поэтому, с другой стороны, можно оценить общее число мономов в (6).

Положим по определению, что степень монома $W = z_1^{v_1} \dots z_m^{v_m}$ равна

$$\deg W = \max_{i=1,\dots,m} v_i.$$

Тогда справедливо неравенство:

$$\deg(W_1 W_2) \le \deg W_1 + \deg W_2.$$

Теперь имеем сначала равенство

$$\deg W = \deg(z_1^{a_{1k}} \dots z_m^{a_{mk}}) = \max_{r=1,\dots,m} a_{rk},$$

а затем получаем соотношение

$$\deg\left(\prod_{k=1}^{n} (1 + z_1^{a_{1k}} \dots z_m^{a_{mk}})\right) = \sum_{k=1}^{n} \max_{r=1,\dots,m} a_{rk} = v.$$

Отсюда следует, что степень любого монома в (6) не превосходит v. Поэтому общее число мономов на превосходит m^v.

Но это означает, что хотя бы один коэффициент у полинома $F_A(z_1, \dots, z_n)$ не меньше $\frac{2^n}{m^v}$.

Теорема 1 доказана.

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) осуществляется с полиномиальной трудоемкостью. (Заметим, что в рассматриваемой ситуации имеем не конкретную индивидуальную задачу булева программирования, а семейство таких задач, параметризованное по $\{b_1, \dots, b_m\}$.)

Пример 2. Пусть есть два уравнения и $\mathbf{A} = (a_{ij})_{2\times n}$ – матрица из нулей и единиц.

Тогда при $m = 2$ и $v \le n$ из (5) получаем, что $\max\limits_{\{b_1,b_2\}} t_{b_1 b_2}(A) \ge 1$.

Но это очевидно, так как число единиц в строке матрицы определяет вектор правых частей того набора, на котором достигается максимум. В более сложных случаях структура подобного набора не всегда очевидна. Однако и сам подход к проблеме нахождения $\max\limits_{\{b_1,b_2\}} t_{b_1 b_2}(A)$ на основе схемы доказательства теоремы 1 может быть полезен, что показывает следующий пример.

Пример 3. Рассмотрим систему уравнений:

$$x_1 + 2x_2 + 3x_3 + 4x_4 = b_1,$$
$$2x_1 + x_2 + x_3 + 3x_4 = b_2.$$

$$F_A(z_1, z_2) = \left(1 + z_1 z_2^2\right)\left(1 + z_1^2 z_2\right)\left(1 + z_1^3 z_2\right)\left(1 + z_1^4 z_2^3\right). \tag{7}$$

Раскрывая скобки, видим, что моном максимальной степени $z_1^{10} z_2^7$. Поэтому правая часть (5) меньше единицы: $\frac{2^n}{m^\nu} = \frac{2^4}{2^{17}} < 1$.

Но приводя подобные в (7), видим, что $\max\limits_{\{b_1,b_2\}} t_{b_1b_2}(A) = 2$ 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 4. Рассмотрим систему уравнений:

$$x_1 + x_2 + x_3 + x_4 = b_1,$$
$$x_2 + 2x_4 = b_2.$$
$$F_A(z_1, z_2) = (1 + z_1z_2)(1 + z_1)^2(1 + z_1z_2^2). \tag{8}$$

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

Но приводя подобные в (8), видим, что $\max\limits_{\{b_1,b_2\}} t_{b_1b_2}(A) = 2$ 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. Пусть дана линейная форма (2) с булевыми переменными. Множество значений этой линейной формы обозначим через $L^*(a_1, \ldots, a_n)$. (А если это не вызывает неопределенности, то просто через L^*.)

Сама же форма $L^*(x_1, \ldots, x_n) = \sum_{i=1}^n a_ix_i$, зависящая от переменных $x_1, \ldots, x_n$, будет для краткости обозначаться через L.

Пример 5. Если $a_i = 1$, $i = 1, \ldots, n$, то $L^* = \{0, 1, 2, \ldots, n\}$.

Пример 6. Если $a_i = 2^{i-1}$, $i = 1, \ldots, n$, то $L^* = \{0, 1, 2, \ldots, 2^n - 1\}$.

Пример 7. Если $L(x_1, \ldots, x_n) = x_1 + x_2 + \ldots + x_{n-1} + nx_n$, то $L^* = \{0, 1, \ldots, n, n + 1, \ldots, 2n - 1\}$.

В этом случае уравнение $L(x_1, \ldots, x_n) = b$ имеет решение для всех b, удовлетворяющих условию $0 \le b \le 2n - 1$.

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

Просто из введенных определений получаем следующее утверждение.

Утверждение 1. Уравнение $L(x) = b$ разрешимо тогда и только тогда, когда $b \in L^*$.

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

$$a_1 \le a_2 \ldots \le a_n. \tag{9}$$

Определение 1. Формы $L_1(x_1, \ldots, x_n)$ и $L_2(x_1, \ldots, x_n)$ называются эквивалентными, если $L_1^* = L_2^*$.

Пусть, как обычно, n – число переменных, а N – целое число такое, что

$$1 \le a_k \le N, \quad k = 1, \dots, n. \tag{10}$$

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

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

Доказательство. Каждая линейная форма с условиями (9) и (10) 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 $t(n, N) = C^n_{N+n-1}$.

Лемма 2 доказана.

Пусть, как и раньше, $t_b(a_1, \dots, a_n)$ – число решений уравнения $L(x_1, \dots, x_n) = \sum_{i=1}^n a_i x_i = b$, а $nt_b(a_1, \dots, a_n)$ – число решений неравенства $L(x_1, \dots, x_n) = \sum_{i=1}^n a_i x_i \le b$. Исследуем эти величины. Обозначим через V_b множество решений соответствующей задачи (уравнения или неравенства).

Пусть производящая функция для числа решений неравенства

$$P_b(z_1, \dots, z_n) = \sum_{x \in V_b} z_1^{a_1 x_1} z_2^{a_2 x_2} \dots z_n^{a_n x_n} nt_b(a_1, \dots, a_n). \tag{11}$$

Лемма 3. Справедлива формула

$$\sum_{b=0}^{\infty} P_b(z_1, \dots, z_n) u^b = \frac{(1 + (z_1 u)^{a_1}) \dots (1 + (z_n u)^{a_n})}{1 - u}. \tag{12}$$

Доказательство. Преобразуем сумму (11), используя метод коэффициентов (в первом равенстве цепочки нижеприведенных выкладок учтено соотношение $\sum_{i=1}^n a_i x_i \le b$),

$$P_b(z_1, \dots, z_n) = \sum_{t=0}^{b} \sum_{x \in V_t} z_1^{a_1 x_1} z_2^{a_2 x_2} \dots z_n^{a_n x_n} \underset{u}{Coef} \left\{ \frac{u^{\sum_{i=1}^n a_i x_i}}{u^{t+1}} \right\} =$$

$$= \underset{u}{Coef} \left\{ \sum_{t=0}^{b} \frac{1}{u^{t+1}} \sum_{x=0}^{1} (z_1 u)^{a_1 x_1} \dots \sum_{x=0}^{1} (z_n u)^{a_n x_n} \right\} =$$

$$= \underset{u}{Coef} \left\{ \frac{\frac{1}{u} - \frac{1}{u^{b+2}}}{1 - \frac{1}{u}} \prod_{k=1}^{n} (1 + (z_k u)^{a_k}) \right\} =$$

$$= \underset{u}{Coef} \left\{ \frac{1}{u^{b+1}(1-u)} \prod_{k=1}^{n} (1 + (z_k u)^{a_k}) \right\}. \tag{13}$$

Сравним (12) и (13) и увидим, что (12) просто “содержится” в (13).

Лемма 3 доказана.

Рассмотрим теперь следствие 3 из леммы 3 и с его помощью проиллюстрируем ее смысл. (Все нижеприведенные интегралы берутся по контуру, который указан под знаком интеграла.)

Следствие 3. Пусть $0 < \rho < 1$. *Тогда для объема области решений имеет место равенство*

$$nt_b(a_1, \ldots, a_n) = \frac{1}{2\pi i} \oint\limits_{|u|=\rho} \frac{(1+u^{a_1}) \ldots (1+u^{a_n})}{(1-u)u^{b+1}} du. \tag{14}$$

Сам смысл метода коэффициентов – это выражение коэффициента при минус первой степени переменной (оно представлено формулой (13)) через сумму вычетов, что представлено формулой (14). Именно это и приведено в качестве следствия 3 из леммы 3.

Пример 9. Пусть все $a_j = 0$, $j = 1, \ldots, n$.

Очевидно, что в этом случае множество решений совпадает со всем булевым кубом. Но это и следует из (14):

$$|V_b| = \frac{1}{2\pi i} \oint\limits_{|u|=\rho} \frac{(1+u^{a_1}) \ldots (1+u^{a_n})}{(1-u)u^{b+1}} du =$$

$$= \frac{1}{2\pi i} \oint\limits_{|u|=\rho} \frac{1}{(1-u)u^{b+1}} du = \frac{2^n}{2\pi i} \oint\limits_{|u|=\rho} \left\{ \sum_{k=0}^{\infty} u^{k-b+1} \right\} du = 2^n.$$

Пример 10. Пусть все $a_j = 1,\ j = 1, \ldots, n$.

Очевидно, что в этом случае объем множества решений равен $\sum_{k=0}^{b} C_n^k$. Но это и следует из (14):

$$|V_b| = \frac{1}{2\pi i} \oint\limits_{|u|=\rho} \frac{(1+u^{a_1}) \ldots (1+u^{a_n})}{(1-u)u^{b+1}} du =$$

$$= \frac{1}{2\pi i} \oint\limits_{|u|=\rho} \frac{(1+u)^n}{(1-u)u^{b+1}} du = \sum_{k=0}^{b} C_n^k.$$

Пример 11. Пусть все $a_j = 2^{j-1},\ j = 1, \ldots, n$. Тогда в неравенстве $\sum_{i=1}^{n} a_i x_i \le b$ слева стоит некоторая двоичная запись натурального числа. Поэтому при $b > 2^n$ допустимые решения – весь булев куб. В противном случае решений ровно b, так как любое натуральное число однозначно представимо в двоичной записи. Отсюда следует, что объем множества решений равен $\min\{b, 2^n\}$.

В рассматриваемом случае из (14) следует:

$$|V_b| = \frac{1}{2\pi i} \oint\limits_{|u|=\rho} \frac{(1+u^{a_1})\dots(1+u^{a_n})}{(1-u)u^{b+1}}du =$$

$$= \frac{1}{2\pi i} \oint\limits_{|u|=\rho} \frac{(1+u)(1+u^2)\dots(1+u^{2^{n-1}})}{(1-u)u^{b+1}}du =$$

$$= \frac{1}{2\pi i} \oint\limits_{|u|=\rho} \left\{\sum_{m=0}^{2^n-1} u^m\right\} du = \sum_{k=0}^{2^n-1} \left(\frac{1}{2\pi i} \oint\limits_{|u|=\rho} \frac{1}{(1-u)u^{b-k+1}}du \right) = \min\left\{b, 2^n\right\}.$$

Здесь тот факт, что любое натуральное число однозначно представимо в двоичной системе исчисления, заключается в использовании соотношения

$$\prod_{k=0}^{n-1}(1+u^{2^k}) = \sum_{m=0}^{2^n-1} u^m.$$

Очевидно, что интеграл в последнем равенстве равен единице при $b > k-1$ и нулю в противном случае. (Заметим, что единица не является особой точкой!)

Теперь перейдем к рассмотрению числа решений уравнения.

Лемма 4. Справедливо соотношение

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

Доказательство. Из леммы 1 совершенно аналогично доказательству леммы 3 получаем:

$$F_A(z_1,\dots,z_n) = \sum_{x\in V_b} z_1^{a_1x_1}\dots z_n^{a_nx_n} \underset{u}{Coef}\left\{\frac{u^{\sum\limits_{i=1}^{n} a_ix_i}}{u^{b+1}}\right\} =$$

$$= \underset{u}{Coef}\left\{\frac{1}{u^{b+1}}\sum_{x=0}^{1}(z_1u)^{a_1x_1}\dots\sum_{x=0}^{1}(z_nu)^{a_nx_n}\right\} =$$

$$= \underset{u}{Coef}\left\{\frac{1}{u^{b+1}}\prod_{k=1}^{n}(1+(z_ku)^{a_k})\right\}. \tag{15}$$

Откуда и следует утверждение леммы. Лемма 4 доказана.

Рассмотрим теперь вопрос о среднем значении $t_b(a_1,\dots,a_n)$ для фиксированного значения b по всему булеву кубу при условиях (9) и (10).

Обозначим это число через $\overline{t_b}$. (То есть это среднее значение $\overline{t_b}(a_1,\dots,a_n)$ по всему множеству $1\le a_k\le N$, $k=1,\dots,n$.)

С учетом (9), (10) из леммы 4 имеем следующее соотношение

$$\overline{t_b}=\frac{1}{C^n_{n+N-1}}\sum_{i=1}^{n}\sum_{a_i=a_{i-1}}^{N}t_b(a_1,\dots,a_n). \tag{16}$$

Здесь считаем, что $a_0=1$.

Лемма 5. Справедлива формула

$$\overline{t_b}=\frac{1}{C^n_{n+N-1}}\frac{1}{2\pi i}\oint\limits_{|u|=\rho}\frac{\left(N+\frac{u-u^{N+1}}{1-u}\right)^n}{u^{b+1}}du,\quad \rho<1. \tag{17}$$

Для доказательства леммы 5 непосредственно подставляем (15) в (16) и проводим суммирование, используя наличие геометрической прогрессии.

Рассмотрим в качестве примера случай трех переменных при произвольном N. (Всюду далее считаем, что $\rho<1$.)

В этом случае $C^n_{N+n-1}=C^3_{N+2}$, а отсюда

$$\left(N+\frac{u-u^{N+1}}{1-u}\right)^3=N^3+3N^2\left(\frac{u-u^{N+1}}{1-u}\right)+$$
$$+3N\left(\frac{u-u^{N+1}}{1-u}\right)^2+\left(\frac{u-u^{N+1}}{1-u}\right)^3.$$

Из (17) следует

$$\overline{t_b}=\frac{1}{C^3_{N+2}}\frac{1}{2\pi i}\oint\limits_{|u|=\rho}\frac{N^3+3N^2\left(\frac{u-u^{N+1}}{1-u}\right)+3N\left(\frac{u-u^{N+1}}{1-u}\right)^2+\left(\frac{u-u^{N+1}}{1-u}\right)^3}{u^{b+1}}du=$$
$$=\frac{N^3}{C^3_{N+2}}\frac{1}{2\pi i}\oint\limits_{|u|=\rho}\frac{1}{u^{b+1}}du+\frac{3N^2}{C^3_{N+2}}\frac{1}{2\pi i}\oint\limits_{|u|=\rho}\frac{1-u^N}{(1-u)u^b}du+$$
$$+\frac{3N}{C^3_{N+2}}\frac{1}{2\pi i}\oint\limits_{|u|=\rho}\frac{\left(1-u^{N-1}\right)^2}{(1-u)^2u^{b-1}}du+\frac{1}{C^3_{N+2}}\frac{1}{2\pi i}\oint\limits_{|u|=\rho}\frac{\left(1-u^{N-2}\right)^3}{(1-u)^3u^{b-2}}du.$$

Для двух переменных при произвольном N имеем следующее.

В этом случае $C_{N+n-1}^{n} = C_{N+1}^{2}$, а отсюда

$$\left(N + \frac{u - u^{N+1}}{1-u}\right)^2 = N^2 + 2N\left(\frac{u-u^{N+1}}{1-u}\right) + \left(\frac{u-u^{N+1}}{1-u}\right)^2.$$

Из (17) следует

$$\overline{t_b} = \frac{1}{C_{N+1}^2}\frac{1}{2\pi i}\oint\limits_{|u|=\rho} \frac{N^2 + 2N\left(\frac{u-u^{N+1}}{1-u}\right) + \left(\frac{u-u^{N+1}}{1-u}\right)^2}{u^{b+1}}du =$$

$$= \frac{N^2}{C_{N+1}^2}\frac{1}{2\pi i}\oint\limits_{|u|=\rho}\frac{1}{u^{b+1}}du + \frac{2N}{C_{N+1}^2}\frac{1}{2\pi i}\oint\limits_{|u|=\rho}\frac{1-u^N}{(1-u)u^b}du +$$

$$+ \frac{1}{C_{N+1}^2}\frac{1}{2\pi i}\oint\limits_{|u|=\rho}\frac{\left(1-u^N\right)^2}{(1-u)^2u^{b-1}}du =$$

$$= \frac{N^2}{C_{N+1}^2}\frac{1}{2\pi i}\oint\limits_{|u|=\rho}\frac{1}{u^{b+1}}du + \frac{2N}{C_{N+1}^2}\frac{1}{2\pi i}\oint\limits_{|u|=\rho}\frac{1-u^N}{(1-u)u^b}du +$$

$$+ \frac{1}{C_{N+1}^2}\frac{1}{2\pi i}\oint\limits_{|u|=\rho}\frac{(1-u)^{-2}}{u^{b-1}}\left(1-u^N\right)^2du =$$

$$= \frac{N^2}{C_{N+1}^2}\frac{1}{2\pi i}\oint\limits_{|u|=\rho}\frac{1}{u^{b+1}}du + \frac{2N}{C_{N+1}^2}\frac{1}{2\pi i}\oint\limits_{|u|=\rho}\frac{du}{(1-u)u^b} +$$

$$+ \frac{2N}{C_{N+1}^2}\frac{1}{2\pi i}\oint\limits_{|u|=\rho}\frac{du}{(1-u)u^{b-N}} + \frac{1}{C_{N+1}^2}\frac{1}{2\pi i}\oint\limits_{|u|=\rho}\frac{(1-u)^{-2}\left(1-2u^N+u^{2N}\right)}{u^{b-1}}du.$$

Представим это выражение в виде двух слагаемых, которые рассмотрим по отдельности, т.е. $\overline{t_b} = \mathrm{A} + \mathrm{B}$, где

$$\mathrm{A} = \frac{N^2}{C_{N+1}^2}\frac{1}{2\pi i}\oint\limits_{|u|=\rho}\frac{1}{u^{b+1}}du + \frac{2N}{C_{N+1}^2}\frac{1}{2\pi i}\oint\limits_{|u|=\rho}\frac{du}{(1-u)u^b} +$$

$$+ \frac{2N}{C_{N+1}^2}\frac{1}{2\pi i}\oint\limits_{|u|=\rho}\frac{du}{(1-u)u^{b-N}},$$

$$\mathrm{B} = \frac{1}{C_{N+1}^2}\frac{1}{2\pi i}\oint\limits_{|u|=\rho}\frac{(1-u)^{-2}\left(1-2u^N+u^{2N}\right)}{u^{b-1}}du.$$

Пусть δ – некоторая константа. Тогда первое слагаемое можно представить в виде

$$\mathrm{A} = \frac{N^2}{C_{N+1}^2}\frac{1}{2\pi i}\oint\limits_{|u|=\rho}\frac{1}{u^{b+1}}du + \frac{2N}{C_{N+1}^2}\frac{1}{2\pi i}\oint\limits_{|u|=\rho}\frac{\sum\limits_{j=0}^{\infty}u^j}{u^b}du +$$

$$+\frac{2N}{C_{N+1}^2}\frac{1}{2\pi i}\oint\limits_{|u|=\rho}\frac{\sum\limits_{j=0}^{\infty}u^j}{u^{b-N}}du = \frac{N^2}{C_{N+1}^2}\delta^b + \frac{2N}{C_{N+1}^2} + \frac{2N}{C_{N+1}^2}\delta^{b-N}.$$

А второе имеет вид

$$\mathrm{B} = \frac{1}{C_{N+1}^2}\frac{1}{2\pi i}\oint\limits_{|u|=\rho}\frac{(1-u)^{-2}\left(1-2u^N+u^{2N}\right)}{u^{b-1}}du.$$

Далее получаем

$$\frac{1}{2\pi i}\oint\limits_{|u|=\rho}\frac{(1-u)^{-2}\left(1-2u^N+u^{2N}\right)}{u^{b-1}}du =$$

$$= \frac{1}{2\pi i}\oint\limits_{|u|=\rho}\frac{(1-u)^{-2}}{u^{b-1}}du + \frac{1}{2\pi i}\oint\limits_{|u|=\rho}\frac{(1-u)^{-2}}{u^{b-N}}du + \frac{1}{2\pi i}\oint\limits_{|u|=\rho}\frac{(1-u)^{-2}}{u^{b-2N-1}}du =$$

$$= (-1)^{b-2}C_{b-2}^{-2} + 2(-1)^{b-N-2}C_{b-N-2}^{-2} + (-1)^{b-2N-2}C_{b-2N-2}^{-2} =$$

$$= C_{2+b-2-1}^{b-2} + 2C_{2+b-N-2-1}^{b-N-2} + C_{2+b-2N-2-1}^{b-2N-2} =$$

$$= C_{b-1}^{b-2} + 2C_{b-N-1}^{b-N-2} + C_{b-2N-1}^{b-2N-2} =$$

$$= (b-1) - 2C_{b-N-1}^{1} + C_{b-2N-1}^{1} = 0.$$

Окончательно имеем:

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

Рассмотрим теперь случай $N=2$ при произвольном количестве переменных. Пусть, как обычно, $\|x\| = \sum_{i=1}^n x_i$. В рассматриваемом случае b можно представить в виде $b = \sum_{i=1}^p x_i + 2\sum_{i=p+1}^n x_i$. Очевидно, что $b \le p + 2(n-p) = 2n-p$.

Утверждение 2. При $N=2$ справедливо соотношение

$$\overline{t_b} = \frac{1}{n+1}\sum_{k=0}^{n} C_n^k C_k^{b-k} 2^{n-k}. \tag{18}$$

Доказательство. В рассматриваемом случае из (17) имеем

$$\overline{t_b} = \frac{1}{C^n_{n+N-1}} \frac{1}{2\pi i} \oint\limits_{|u|=\rho} \frac{\left(N + \frac{u-u^{N+1}}{1-u}\right)^n}{u^{b+1}} du = \frac{1}{C^n_{n+1}} \frac{1}{2\pi i} \oint\limits_{|u|=\rho} \frac{\left(2 + \frac{u-u^3}{1-u}\right)^n}{u^{b+1}} du =$$

$$= \frac{1}{n+1} \frac{1}{2\pi i} \oint\limits_{|u|=\rho} \frac{(2+u(1+u))^n}{u^{b+1}} du = \frac{1}{n+1} \frac{1}{2\pi i} \oint\limits_{|u|=\rho} \frac{\sum\limits_{k=0}^{n} C^k_n u^k (1+u)^k 2^{n-k}}{u^{b+1}} du =$$

$$= \frac{1}{n+1} \sum_{k=0}^{n} C^k_n 2^{n-k} \frac{1}{2\pi i} \oint\limits_{|u|=\rho} \frac{u^k (1+u)^k}{u^{b+1}} du = \frac{1}{n+1} \sum_{k=0}^{n} C^k_n C^{b-k}_k 2^{n-k},$$

где $b/2 \le k \le b$.

Утверждение 2 доказано.

Пример 12. Пусть $N = 2$, $n = 3$. Из (12) имеем

$$\overline{t_b} = \frac{1}{n+1} \sum_{k=0}^{n} C^k_n C^{b-k}_k 2^{n-k} = \frac{1}{4} \sum_{k=0}^{3} C^k_3 C^{b-k}_k 2^{3-k}.$$

Отсюда получаем

$$\overline{t_1} = \frac{1}{4}(2+3+1+0) = 3/2, \quad \overline{t_2} = \frac{1}{4}(2+3+2+3) = 5/2,$$

$$\overline{t_3} = \frac{1}{4}(2+1+2+0) = 5/4, \quad \overline{t_4} = \frac{1}{4}(1+0+1+3) = 5/4, \quad \overline{t_5} = \frac{1}{4}, \quad \overline{t_6} = \frac{1}{4}.$$

Видно, что максимальное значение достигается при $b = 2$.

3. О некоторых свойствах множества L^*

3.1. Структура множества L^*

Следуя обозначениям и определениям, введенным ранее, напомним, что множество значений линейной формы $L(x_1, \ldots, x_n) = \sum_{i=1}^n a_i x_i$ (сама эта форма, если это не вызывает неопределенности, обозначается через $L(x)$ или даже через L) обозначено через $L^*(a_1, \ldots, a_n)$ (или просто через L^*).

Уравнение $L(x) = b$ разрешимо тогда и только тогда, когда $b \in L^*$. В связи с этим актуальной задачей является исследование структуры и свойств множества L^*.

Очевидно следующее утверждение.

Утверждение 3. Справедливо соотношение

$$|L^*| \le \min\left\{2^n, 1 + \sum_{i=1}^{n} a_i\right\}.$$

Следствие 4. Если $a_i \le N$, $i = 1, \ldots, n$, *то* $|L^*| \le \min\{2^n, 1 + nN\}$.

Лемма 6. Если $L(x) = \sum_{i=1}^{n} ix_i$, *то* $L^* = \left[0, C_{n+1}^2\right]$.

Эта лемма следует из того факта, доказанного в [12], что при $L(x) = \sum_{i=1}^{n} ix_i$ форма $L(x)$ принимает на булевом кубе все значения от нуля до $\sum_{i=1}^{n} i = C_{n+1}^2$.

3.2. Множества L^* и сложение по Минковскому

Определение 2. Пусть M_1 *и* M_2 *– два множества из натуральных чисел. Их суммой по Минковскому называется множество* $M = M_1 \oplus M_2 = \{a + b, a \in M_1, b \in M_2\}$.

Пример 13. Если Z_{2n} – множество всех четных чисел, а $M = \{0, 1\}$, то $Z_{2n} \oplus M$ – весь натуральный ряд.

Пример 14. Сумма по Минковскому двух отрезков натурального ряда – это отрезок натурального ряда: $[a, b] \oplus [c, d] = [a + b, c + d]$.

Обозначим через P_L множество переменных формы $L(x_1, \ldots, x_n)$, т.е. $P_L = \{x_1, \ldots, x_n\}$.

Лемма 7. Если $P_{L_1} \cap P_{L_2} = \varnothing$, *то* $(L_1 + L_2)* = L_1^* \oplus L_2^*$.

Доказательство. По определению

$$(L_1 + L_2)* = \left(\sum_{i=1}^{p} a_i x_i + \sum_{i=p+1}^{q} a_i x_i \right)^* = \{a_i + a_j, 1 \le i \le p, p + 1 \le j \le q\}.$$

Далее замечаем, что $\{a_i + a_j, 1 \le i \le p, p + 1 \le j \le q\} = L_1^* \oplus L_2^*$.

Лемма 7 доказана.

Приведем некоторые соотношения, связывающие обычное сложение линейных форм, сложение по Минковскому и стандартные теоретико-множественные операции.

1. $(L_1 + L_2) = \sum_{i=1}^{n} (a_i + a_i) x_i = \sum_{i=1}^{n} c_i x_i$.
2. $L^* = \left\{ \sum_{i=1}^{n} a_i x_i, x \in B^n \right\}$.
3. $A \oplus B = \{a + b, a \in A, b \in B\}$.
4. $(L_1 + L_2)* = L_1^* \oplus L_2^*$ при $P_{L_1} \cap P_{L_2} = \varnothing$.
5. Если $L_1(x_1, \ldots, x_n) = \sum_{i=1}^{n} a_i x_i$, $L_2 = a_{n+1} x_{n+1}$ и $a_{n+1} \le \sum_{i=1}^{n} a_i$,

   а $L_1^* = \left[0, \sum_{i=1}^{n} a_i\right]$, то $(L_1 + L_2)^* = \left[0, \sum_{i=1}^{n+1} a_i\right]$.

3.3. Непрерывные линейные формы

Рассмотрим один специальный класс линейных форм.

Определение 3. Форма $L(x_1, \ldots, x_n) = \sum_{i=1}^{n} a_i x_i$ *называется непрерывной, если* $L^* = [0, \sum_{i=1}^{n} a_i]$.

Таким образом, непрерывная форма принимает все значения от минимально возможного до максимального. (Напоминаем, что переменные булевы, а коэффициенты – целые положительные числа.) Впервые данное определение было введено в [14].

Пример 15. Следующие классы функций являются непрерывными:

1. $L(x) = \sum_{i=1}^{n} x_i$;
2. $L(x) = \sum_{i=1}^{n} i x_i$;
3. $L(x) = \sum_{i=1}^{n} x_i 2^{i-1}$;
4. $L(x) = \sum_{i=1}^{n-1} x_i + n x_n$;
5. $L(x) = \sum_{i=2}^{n} 2x_i + x_1$.

При $n = 2$ существует всего две непрерывные формы: $L_1 = x_1 + x_2$; $L_2 = x_1 + 2x_2$.

При $n = 3$ существует пять непрерывных форм: $L_1 = x_1 + x_2 + x_3$, $L_2 = x_1 + x_2 + 2x_3$, $L_3 = x_1 + 2x_2 + 2x_3$, $L_4 = x_1 + 2x_2 + 3x_3$, $L_5 = x_1 + 2_2 + 4x_3$.

Для $n = 4$ таких форм уже 13: $L_1 = x_1 + x_2 + x_3 + x_4$, $L_2 = x_1 + x_2 + x_3 + 2x_4$, $L_3 = x_1 + x_2 + 2x_3 + 2x_4$, $L_4 = x_1 + 2x_2 + 2x_3 + 2x_4$, $L_5 = x_1 + 2x_2 + 2x_3 + 3x_4$, $L_6 = x_1 + x_2 + x_3 + 3x_4$, $L_7 = x_1 + x_2 + 3x_3 + 3x_4$, $L_8 = x_1 + 2x_2 + 3x_3 + 3x_4$, $L_9 = x_1 + 2x_2 + 3x_3 + 4x_4$, $L_{10} = x_1 + 2x_2 + 4x_3 + 4x_4$, $L_{11} = x_1 + x_2 + 2x_3 + 5x_4$, $L_{12} = x_1 + x_2 + 3x_3 + 5x_4$, $L_{13} = x_1 + 3x_2 + 3x_3 + 5x_4$.

Важность и актуальность проверки линейной формы на непрерывность объясняется следующим их свойством. Решение системы булевых уравнений, левые части которых образованы непрерывными линейными формами, становится простой задачей. Достаточно для каждого уравнения взять правую часть b и сравнить с $\sum_{i=1}^{n} a_i$ в правой части. Если $b \le \sum_{i=1}^{n} a_i$, то уравнение разрешимо, например, на единичном векторе. А если $b > \sum_{i=1}^{n} a_i$, то решения оно не может иметь.

Замечание 1. Сумма непрерывных функций не обязана быть непрерывной.

Пример 16. Функции $L_1 = x_1 + x_2$ и $L_2 = x_1 + 2x_2$ являются непрерывными, а их сумма $L_3 = 2x_1 + 3x_2$ не является непрерывной (она не принимает значений 1 и 4).

Однако если это функции от разных переменных, то справедливо утверждение.

Утверждение 4. Если L_1 и L_2 – две непрерывные линейные формы, зависящие от разных переменных, то форма $L_1 + L_2$ является непрерывной.

Доказательство. Так как L_1 и L_2 – непрерывны, то $L_1^* = [0, a]$, $L_2^* = [0, b]$ для некоторых a и b. Из леммы 7 следует: $[L_1 + L_2]^* = L_1^* \oplus L_2^* = [0, a] \oplus [0, b] = [0, a + b]$.

Утверждение 4 доказано.

Утверждение 5. Если форма $L = \sum_{i=1}^{n} a_i x_i$ является непрерывной и $L \neq 0$, то справедливы соотношения: $a_k \leq \sum_{i=1}^{k-1} a_i + 1$, $k = 2, 3, \ldots, n$.

Доказательство. Так как выполняется (9), $L \neq 0$ и $L^* = [0, \sum_{i=1}^{n} a_i]$, то $a_1 = 1$ в силу того, что $1 \in L^*$. Далее берем минимальное $k > 1$ такое, что $a_k \neq 0$. Вновь в силу (9) имеем $a_k \leq 2$, так как $L^* = [0, \sum_{i=1}^{n} a_i]$ и $2 \in L^*$. И так для всех $k = 2, 3, \ldots, n$.

Утверждение 5 доказано.

Пусть теперь $L = \sum_{i=1}^{n} a_i x_i$ и все $a_i \leq N$, $i = 1, \ldots, n$. Обозначим множество таких форм через $L(n, N)$ и пусть $l(n, N) = \max_{L(n,N)} |L^*|$.

Значение $l(n, N)$и его оценки могут представлять интерес при оценке качества переборных алгоритмов.

Тогда справедливо следующее соотношение.

Теорема 2. Если $N = n$, то

$$l(n, N) \sim n^2.$$

Доказательство. Для доказательства получим верхнюю и нижнюю границу этой асимптотики, а из их равенства установим утверждение теоремы. Верхняя граница здесь очевидна и имеет вид

$$l(n, n) \leq \min\left\{2^n, n^2\right\} = n^2. \tag{19}$$

Для получения нижней оценки рассмотрим линейную форму специального вида

$$L = x_1 + \sum_{i=2}^{m} ix + n \sum_{i=m+1}^{n} x_i.$$

Здесь m – некоторый параметр. Теперь выберем m из условия:

$$C_{m+1}^2 \geq n.$$

Отсюда следует, что $L^*\left(x_1+\sum_{i=2}^{m} ix\right)=\left[0, C_{m+1}^2\right]$, а с учетом вида выбранной линейной формы начинаем добавлять слагаемые. При добавлении первого слагаемого получаем:

$$L^*\left(x_1+\sum_{i=1}^{m} ix+nx_{m+1}\right)=\left[0, n+C_{m+1}^2\right].$$

И далее, продолжая добавлять слагаемые, имеем:

$$L^*\left(x_1+\sum_{i=2}^{m} ix_i+n\sum_{i=m+1}^{n} x_i\right)=\left[0, n(n-m)+C_{m+1}^2\right].$$

Из этого равенства видно, что для завершения доказательства теоремы 2 требуется выбрать параметр $m\sim\sqrt{2n}$. При таком выборе мощность множества значений линейной формы удовлетворяет соотношению:

$$\left|L^*\left(x_1+\sum_{i=2}^{m} ix_i+n\sum_{i=m+1}^{n} x_i\right)\right|\sim n^2. \tag{20}$$

Из (19) и (20) следует утверждение теоремы.

Теорема 2 доказана.

Замечание 2. Для доказательства нижней оценки в теореме использовалась линейная форма достаточно специального вида, поэтому на практике, видимо, следует ожидать для $|L^*|$ значений существенно меньших. Вопрос же о среднем значении этой величины – отдельная задача теории чисел.

4. Заключение

В статье рассмотрены вопросы, связанные с разрешимостью систем булевых уравнений. Даны формулы и оценки числа допустимых решений системы в зависимости от значения правых частей уравнений. Эта часть работы использует метод производящих функций и является продолжением предыдущих исследований авторов.

Рассмотрен один частный случай систем, когда уравнения ограничений задаются так называемыми непрерывными линейными формами.

Результаты могут представлять интерес для конструирования прикладных алгоритмов в различных областях дискретной оптимизации и исследования операций, а также в распознавании образов, криптографии и системах защиты информации.

СПИСОК ЛИТЕРАТУРЫ

1. *Пападимитриу Х., Стайглиц С.* Комбинаторная оптимизация. М.: Мир, 1989.
2. *Гэри М., Джонсон Д.* Вычислительные машины и труднорешаемые задачи. М.: Мир, 1982.

3. *Схрейвер А.* Теория линейного и целочисленного программирования. М.: Мир, 1991.

4. *Леонтьев В.К., Гордеев Э.Н.* Производящие функции в задаче о ранце // ДАН. 2018. Т. 481. № 5. С. 478–480. https://doi.org/10.31857/S086956520002139-5.

5. *Леонтьев В.К., Гордеев Э.Н.* О некоторых комбинаторных свойствах задачи о рюкзаке // Журн. вычисл. матем. и матем. физ. 2019. Т. 59. № 8. С. 1439–1447. https://doi.org/10.1134/S0044466919080076.

6. *Kellerer H., Pferschy U., Pisinger D.* Knapsack problems. Berlin: Springer, 2004.

7. *Леонтьев В.К., Тоноян Г.П.* Приближенные решения систем булевых уравнений // Журн. вычисл. матем. и матем. физ. 1993. Т. 33. № 9. С. 1383–1390.

8. *Леонтьев В.К., Тоноян Г.П.* О системах булевых уравнений // Журн. вычисл. матем. и матем. физ. 2013. Т. 53. № 5. С. 109–116.

9. *Кузюрин Н.Н., Фомин С.А.* Эффективные алгоритмы и сложность вычислений. М.: МФТИ, 2007.

10. *Леонтьев В.К., Гордеев Э.Н.* Об алгебраической иммунности систем кодирования // Вопросы кибербезопасности. 2019. № 1. С. 59–89.

    https://doi.org/ 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. https://doi.org/10.21681/2311-3456-2017-3-63-69.

12. *Мазуров И.Д., Хачай М.Ю.* Комитеты систем линейных неравенств // АиТ. 2004. № 2. С. 43–54.

    Mazurov V.D., Khachai M.Yu. Committees of Systems of Linear Inequalities // Autom. Remote Control. 2004. V. 65. No. 2. P. 193–203.

    https://doi.org/10.1023/ B:AURC.0000014716.77510.61.

13. *Береснев В.Л.* Эффективный алгоритм решения задачи минимизации полиномов от булевых переменных, обладающих свойством связности // Дискретн. анализ и исслед. операций. Сер. 2. 2005. Т. 12. № 1. С. 3–11.

14. *Леонтьев В.К.* О псевдобулевых полиномах // Журн. вычисл. матем. и матем. физ. 2015. Т. 55. № 11. С. 1952–1958. https://doi.org/10.7868/S0044466915110113.

15. *Леонтьев В.К.* Комбинаторика и информация. Ч. 1. Комбинаторный анализ. М.: МФТИ, 2015.

16. *Леонтьев В.К.* Комбинаторика и информация. Ч. 2. Информационные модели. М.: МФТИ, 2015.

Статья представлена к публикации членом редколлегии Д.Е. Пальчуновым.

Поступила в редакцию 12.01.2021

После доработки 01.03.2021

Принята к публикации 16.03.2021