ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 55 **2019** **Вып. 2**

УДК 621.391.1 : 519.7

© 2019 г. **М.Н. Вялый**[1], **В.К. Леонтьев**[2]

ГЕОМЕТРИЯ СДВИГОВ В БУЛЕВОМ КУБЕ

У операции сложения Минковского геометрических фигур есть дискретный аналог – сложение подмножеств булева куба как векторного пространства над полем из двух элементов. Относительно такой операции подмножества булева куба (или булевы функции от нескольких переменных) образуют моноид. Этот моноид представляет интерес как в классическом дискретном анализе, так и в ряде задач, связанных с теорией информации. Рассматриваются различные аспекты сложности этого моноида: структурный, алгоритмический, алгебраический.

Ключевые слова: сложение Минковского, булев куб, моноид, порождающие элементы, примитивные элементы, последовательности кратных.

DOI: 10.1134/S0555292319020049

§ 1. Введение

Пусть $\mathbb{B} = \{0,1\}$, а $\mathbb{B}^n = \{0,1\}^n$ – множество, которое можно понимать по-разному, в зависимости от той или иной конкретной задачи.

С комбинаторной точки зрения $\mathbb{B}^n$ – это *булев куб*: множество двоичных слов, т.е. слов в алфавите $\mathbb{B}$, длины n.

Геометрически $\mathbb{B}^n$ является множеством вершин единичного куба E^n в n-мерном пространстве:

$$E^n = \{x \in \mathbb{R}^n : \, 0 \leqslant x_i \leqslant 1, \, 1 \leqslant i \leqslant n\}.$$

Если понимать под 0 и 1 элементы поля $\mathbb{F}_2$, то $\mathbb{B}^n$ совпадает с n-мерным координатным векторным пространством $\mathbb{F}_2^n$ над этим полем.

Для нас будет важно именно последнее представление. Сложение векторов в векторном пространстве определяет естественным образом сложение подмножеств:

$$A + B = \{x : \, x = y \oplus z, \, y \in A, \, z \in B\}.$$

В геометрии такая операция называется *суммой Минковского*, мы сохраним это название для этой операции с подмножествами $\mathbb{B}^n$.

В дальнейшем мы обозначаем операцию сложения в $\mathbb{F}_2^n$ через $\oplus$, сохраняя обозначение $+$ для суммы Минковского.

[1] Работа выполнена частично в рамках государственного задания по теме 0063-2016-0003, а также при частичной финансовой поддержке Российского фонда фундаментальных исследований (номер проекта 17-01-00300), исследование также финансировалось в рамках программы государственной поддержки ведущих университетов Российской Федерации “5-100”.

[2] Работа выполнена частично в рамках государственного задания по теме 0063-2016-0003, а также при частичной финансовой поддержке Российского фонда фундаментальных исследований (номер проекта 17-01-00300).

Пример 1. Приведем несколько простых примеров сложения Минковского подмножеств булева куба:

1. $\mathbb{B}^n + A = \mathbb{B}^n$ для любого $A \subseteq \mathbb{B}^n$;
2. $A + A = A$, если A – подпространство $\mathbb{B}^n$.

Операция сложения Минковского обладает следующими легко проверяемыми свойствами:

1. $\{0^n\} + A = A$ (существование нейтрального элемента);
2. $A + (B + C) = (A + B) + C$ (ассоциативность);
3. $A + B = B + A$ (коммутативность);
4. $(A \cup B) + C = (A + C) \cup (B + C)$ (дистрибутивность по объединению);
5. $\bigcup\limits_{i=1}^{m} (A + B_i) = A + \bigcup\limits_{i=1}^{m} B_i$.

Подмножества $\mathbb{B}^n$ находятся во взаимно-однозначном соответствии с булевыми функциями – функции $f\colon \mathbb{B}^n \to \mathbb{B}$ сопоставляется множество ее единиц $N_f = \{x \in \mathbb{B}^n : f(x) = 1\}$. Функцию, соответствующую множеству S, будем называть *характеристической функцией множества* и обозначать через χ_S.

Такое соответствие позволяет определить сумму Минковского и для булевых функций: сумма Минковского функций f_1 и f_2 – это такая функция f_3, что $N_{f_3} = N_{f_1} + N_{f_2}$. Таким образом, чтобы сложить две булевы функции по Минковскому, нужно сложить по Минковскому множества их единиц.

В соответствии с принятым выше соглашением сумму Минковского булевых функций обозначаем через $f_1 + f_2$, а поточечную сумму по модулю 2 значений функций (XOR) – через $f_1 \oplus f_2$.

Для суммы Минковского булевых функций имеется формула

$$(f + g)(x) = \bigvee_{y \in B^n} f(y)g(x \oplus y), \tag{1}$$

напоминающая свертку.

Пример 2.

1. Если $F(x_1, \ldots, x_n) \equiv 1$, то $f + F = F$ для любой булевой функции f от n аргументов;
2. Если $f(x_1, \ldots, x_n) = x_1 \oplus x_2$, $f_2(x_1, \ldots, x_n) = x_2$, то $f_1 + f_2 \equiv 1$;
3. Будем обозначать $2f(x) = f(x) + f(x)$. Если $0^n \in N_f$, то $N_f \subseteq N_{2f}$;
4. Сумма по Минковскому симметрических булевых функций является симметрической булевой функцией.

Напомним, что *моноидом* называется множество M, снабженное ассоциативной бинарной операцией $+\colon M \times M \to M$, относительно которой в M существует нейтральный элемент $e \in M$. Иными словами, для любого $m \in M$ выполняются равенства $e + m = m + e = m$, и для любой тройки m_1, m_2, m_3 элементов M выполняется равенство $m_1 + (m_2 + m_3) = (m_1 + m_2) + m_3$.

Как видно из сформулированных выше свойств 1 и 2 сложения Минковского, подмножества n-мерного булева куба с операцией сложения Минковского образуют моноид. Мы будем называть его моноидом Минковского и обозначать через $\mathcal{M}^n$. Нейтральный элемент в моноиде Минковского будем обозначать через $\mathbb{O} = \{0^n\}$.

Моноид Минковского представляет определенный интерес как в классическом дискретном анализе (см. [1, 2]), так и в целом ряде задач, связанных с теорией информации (см. [3, 4]).

Нас интересует сложность операции сложения Минковского. Есть разные способы описывать сложность операции: структурный, алгоритмический, алгебраический. В последующем изложении мы приведем примеры таких способов и уточним формулировки.

§ 2. Вычисление суммы Минковского

В этом параграфе мы обсудим вопрос о том, насколько трудно найти сумму Минковского двух множеств. Такая задача подразумевает алгоритмическую постановку. Чтобы точно ее сформулировать, нужно зафиксировать способ представления подмножества булева куба (или булевой функции). Таких способов много, и для каждого получаем конкретную алгоритмическую задачу, сложность которой можно оценивать.

Простейший способ – табличный. Подмножество $X \subseteq \mathbb{B}^n$ задается таблицей значений характеристической функции, т.е. для каждого элемента $x \in \mathbb{B}^n$ указано, принадлежит ли он множеству X. Описание множества в таком формате имеет битовую длину 2^n.

Легко видеть, что для вычисления суммы Минковского двух множеств в табличном представлении существует полиномиальный алгоритм: вычисление по формуле (1) всей таблицы значений $f + g$ занимает время $O(n2^{2n})$, а длина входа $2 \cdot 2^n$.

Более естественный способ "прямого" задания подмножества X булева куба $\mathbb{B}^n$ состоит в том, чтобы записать список элементов этого множества. Битовая длина такого представления равна $O(n|X|)$ (так как элементы задаются битовыми строками длины n), эта длина может быть много меньше 2^n для некоторых множеств X и не превосходит $O(n2^n)$. Поэтому алгоритмическая сложность задач при таком способе представления подмножеств булева куба может оказаться выше, чем при табличном.

Однако прямое применение определения дает и в этом случае полиномиальный алгоритм вычисления суммы Минковского.

И для табличного способа представлений подмножества, и для задания подмножества списком существуют также алгоритмы вычисления суммы Минковского на памяти, логарифмической по длине входа.

Напомним модель вычисления на памяти $s(n)$, где $s(\cdot)$ – некоторая числовая функция. Это машина Тьюринга с тремя лентами. На входной ленте записан вход задачи, и эту ленту разрешается только читать. На рабочей ленте разрешены и чтение, и запись. Требуется, чтобы размер области, содержащей непустые ячейки на рабочей ленте, в любой момент вычисления на любом входе длины n не превосходил $s(n)$. Наконец, на выходной ленте разрешена только запись. Состояние этой ленты в конце вычисления является результатом работы.

Поскольку общее количество конфигураций рабочей ленты не превосходит $s(n)2^{O(s(n))}$, время вычисления на логарифмической памяти, когда $s(n) = O(\log n)$, всегда полиномиально по n.

Заметим также, что при вычислениях на логарифмической по длине входа памяти возможна произвольная адресация к входным данным: если на рабочей ленте записан адрес входного символа, то переместить головку на входной ленте на этот символ можно, используя на рабочей ленте счетчик, размер которого $O(\log n)$.

Легко видеть, что вычисление по формуле (1) возможно на памяти $O(n)$, логарифмической по длине таблиц, задающих слагаемые. Для этого достаточно поддерживать два указателя на x и y.

Сумму Минковского подмножеств X и Y, заданных списками элементов, также можно вычислить на памяти, логарифмической по длине входа, т.е. по длине списков, задающих множества.

Сложение по модулю 2 двух битовых строк длины n возможно на памяти $O(\log n)$, для чего достаточно двух указателей (на i-й бит каждой из строк). Используя еще два указателя на элементы множеств-слагаемых, можно вычислить все попарные суммы элементов X и Y и построить на логарифмической памяти список элементов $X + Y$. Но этот список может содержать повторения. Избавиться от повторений возможно ценой некоторого усложнения алгоритма.

Предложение 1. *Существует алгоритм, работающий на логарифмической по длине входа памяти, который по входным спискам без повторений множеств X, Y булева куба порождает список без повторений множества $X + Y$.*

Доказательство. Пусть $(x_1, \ldots, x_k)$, $(y_1, \ldots, y_\ell)$, где $x_i, y_j \in \mathbb{B}^n$, – списки элементов на входе алгоритма. Алгоритм перебирает все пары (i, j), где $1 \leqslant i \leqslant k$, $1 \leqslant j \leqslant \ell$, в лексикографическом порядке и для каждой такой пары перебирает все пары (i', j'), которые меньше (i, j) в лексикографическом порядке. Для каждой четверки i, j, i', k' алгоритм проверяет равенство $x_i \oplus y_j = x_{i'} \oplus y_{j'}$. Это возможно на логарифмической памяти, как описано выше. Если для данной пары (i, j) и всех меньших в лексикографическом порядке пар (i', j') равенство не выполняется, алгоритм включает в результирующий список битовую строку $x_i \oplus y_j$.

Корректность алгоритма очевидна: он включает в результирующий список элемент $z \in X + Y$ только один раз и не включает в список никаких элементов, не принадлежащих $X + Y$. ▲

Замечание 1. Время работы алгоритма, описанного в предложении 1, оценивается как $O((k + n)^2 \ell^2 n) = O(N^5)$, где N – длина входа. Мы не обсуждаем здесь вопросы наиболее эффективного вычисления суммы Минковского, ограничиваясь лишь достаточно грубой классификацией сложности алгоритмических задач, принятой в теории сложности вычислений (полиномиальное время, логарифмическая память и т.п.).

Подмножества булева куба (или булевы функции, что по существу то же самое) можно задавать многими другими способами. В теории сложности вычислений довольно часто рассматривается *сжатое представление*. В этом представлении используются булевы схемы. Напомним, что булева схема C (в стандартном базисе) с входными переменными $x_1, \ldots, x_n$ – это такая последовательность булевых функций $f_1, f_2, \ldots, f_s$, что каждый ее член либо является входной переменной, либо получается *присваиванием* из предыдущих. Более точно, для каждого $1 \leqslant k \leqslant s$ выполняется одно из следующих условий:

- $f_k = x_k$ для всех $1 \leqslant k \leqslant n$;
- $f_k = \neg f_i$ для $i < k$;
- $f_k = f_i \vee f_j$ для $i, j < k$;
- $f_k = f_i \wedge f_j$ для $i, j < k$.

Последняя функция f_s называется *значением схемы* и обозначается через $C(x)$. Число $s - n$ (количество присваиваний в схеме) называется *размером* схемы. Если рассматривать схему как программу вычисления функции, то размер схемы пропорционален длине программы.

Сжатое представление множества X – это такая булева схема $C_X(x)$, что $C_X(x) = 1$ равносильно $x \in X$. Сжатое представление не единственно и может быть намного короче как табличного представления, так и представления списком элементов. Поэтому неудивительно, что алгоритмическая сложность задач в сжатом представлении обычно намного выше, чем при других, более явных представлениях.

Вычисление суммы Минковского подмножеств в сжатом представлении оказывается трудной задачей в предположении стандартных гипотез теории сложности вычислений.

Напомним определения сложностных классов P и NP и их основные свойства (более подробное изложение можно найти в [5] или [6, часть I]).

Сложностные классы состоят из *языков* – подмножеств слов в некотором алфавите (далее без ограничения общности считаем, что алфавит двоичный). Язык формализует понятие вычислительной задачи разрешения свойств.

Класс P образуют те языки, для которых проверка принадлежности слова языку осуществима за полиномиальное от длины слова время. Допуская вольность речи,

говорят также о принадлежности классу P предикатов от двух и более слов. Формально это означает принадлежность классу P языка описаний тех пар (троек и т.д.) слов, для которых предикат истинен.

Если $L \in \mathrm{P}$, то для каждого n существует булева схема $C_{L,n}$ от n переменных, размер которой полиномиально ограничен по n и которая вычисляет характеристическую функцию языка L, ограниченную на слова длины n: $C_{L,n}(x) = 1$ равносильно тому, что $x \in L \cap \{0,1\}^n$.

Класс NP образуют те языки L, для которых существуют такие полином $q(\cdot)$ и предикат от двух переменных $R(x,y)$ из класса P, что $x \in L$ равносильно существованию y, для которого $|y| = q(|x|)$ и верно $R(x,y)$.

Класс NP замкнут относительно *полиномиальных сводимостей*. Говорят, что язык L_1 полиномиально сводится к языку L_2 (обозначение $L_1 \leqslant_p L_2$), если существует такая функция $f\colon \{0,1\}^* \to \{0,1\}^*$ на двоичных словах, которая вычислима за полиномиальное от длины входа время и для всех x выполняется следующее условие: $x \in L_1$ равносильно $f(x) \in L_2$.

Язык L называется NP-*полным*, если для любого языка $L' \in \mathrm{NP}$ выполняется $L' \leqslant_p L$.

Одной из основных гипотез теории сложности вычислений является утверждение $\mathrm{P} \neq \mathrm{NP}$. Нетрудно проверить, что $\mathrm{P} = \mathrm{NP}$ равносильно тому, что для какого-нибудь NP-полного языка L выполняется $L \in \mathrm{P}$.

Теорема 1. *Если* $\mathrm{P} \neq \mathrm{NP}$, *то не существует полиномиального алгоритма вычисления суммы Минковского для подмножеств в сжатом представлении.*

Доказательство. Достаточно доказать, что сумма Минковского двух булевых функций схемной сложности s может иметь сверхполиномиальную по s схемную сложность.

Рассмотрим какой-нибудь NP-полный язык L. По определению это означает, что существуют такие полином $q(\cdot)$ и предикат $R(x,y) \in \mathrm{P}$, что $x \in L$ равносильно существованию такого y, что $|y| = q(|x|)$ и верно $R(x,y)$.

Поскольку R полиномиально вычислим, то для всех достаточно больших n существуют такие булевы схемы $C_{R,n}$ от $n + q(n)$ переменных размера $\mathrm{poly}(n)$, что $C_{R,n}(x,y) = R(x,y)$ для всех $x \in \mathbb{B}^n$, $y \in \mathbb{B}^{q(n)}$.

Пусть f_n – булева функция от $n + q(n)$ переменных, задаваемая схемой $C_{R,n}$, а g_n – булева функция от $n + q(n)$ переменных, для которой $g(x,y) = 1$ тогда и только тогда, когда $x = 0^n$. Очевидно, что такую функцию можно представить схемой размера $O(n)$.

Теперь заметим, что $(f_n + g_n)(x, 0^{q(n)}) = 1$ тогда и только тогда, когда $x \in L$. Поэтому по схеме вычисления $f_n + g_n$ размера s легко строится алгоритм для задачи разрешения $x \stackrel{?}{\in} L$, время работы которого $\mathrm{poly}(n,s)$. Это означает, что в предположении $\mathrm{NP} \neq \mathrm{P}$ размер s сверхполиномиален по n. ▲

§ 3. О размере суммы Минковского

Размер суммы Минковского может изменяться в значительных пределах.

Лемма 1 [1]. *Справедливы следующие оценки*:

$$\max\{|X|, |Y|\} \leqslant |X + Y| \leqslant |X| \cdot |Y|. \tag{2}$$

Оценки (2) являются прямым следствием переформулировки определения суммы Минковского

$$X + Y = \bigcup_{i=1}^{N} (X + \{y_i\}), \quad \text{где } Y = \{y_1, \ldots, y_N\},$$

и равенства $|X + \{a\}| = |X|$ для любого $a \in \mathbb{B}^n$.

Обе границы в (2) достижимы. Нижняя достигается, если $X = Y$ – подпространство в $\mathbb{B}^n$, а верхняя – если подпространства X и Y пересекаются только по вектору 0^n. Заметим также, что для любых подпространств X, Y выполняется соотношение

$$|X + Y| = \frac{|X| \cdot |Y|}{|X \cap Y|}.$$

Это соотношение можно обобщить. Пусть V – подпространство в $\mathbb{B}^n$, т.е. подгруппа аддитивной группы $\mathbb{F}_2^n$. *Смежным классом* по подгруппе V называется множество вида $\{a\} + V = \{x : \ x = a \oplus v, \ v \in V\}$. Легко видеть, что смежные классы не пересекаются или совпадают. Для множества $X \subseteq \mathbb{B}^n$ обозначим через $t_V(X)$ количество смежных классов по подгруппе V, пересекающихся с X.

Лемма 2. *Если V – подпространство в $\mathbb{B}^n$, то*

$$|V + X| = t_V(X)|V|.$$

Доказательство. По определению

$$V + X = \bigcup_{i=1}^{N} (V + \{x_i\}), \quad \text{где } X = \{x_1, \ldots, x_N\},$$

т.е. $V + X$ является объединением тех смежных классов $V + \{a\}$, в которые попадают элементы из X. Лемма теперь следует из того, что смежные классы по подгруппе не пересекаются или совпадают. ▲

Эта лемма является некоторым аналогом теоремы Лагранжа из теории групп.

Пример 3. Если V имеет размерность $n - 1$ (и потому содержит 2^{n-1} элементов), то имеется ровно один смежный класс Y, отличный от V. Получаем $V + Y = Y$ и $|V + Y| = |V| = 2^{n-1}$.

Действие аддитивной группы $\mathbb{F}_2^n$ сдвигами на себе самой и, тем самым, на $\mathbb{B}^n$ продолжается до действия на подмножествах $\mathbb{B}^n$: $X \overset{a}{\mapsto} X + \{a\}$. Обозначим через $\operatorname{Stab} X$ стабилизатор множества X при таком действии:

$$\operatorname{Stab} X = \{a : \ X = X + \{a\}\}.$$

Заметим, что $|X + \operatorname{Stab} X| = |X|$, так что на паре X, $\operatorname{Stab} X$ достигается нижняя оценка в (2). Оказывается, что общий случай достижимости нижней оценки в (2) сводится к данному с незначительными усложнениями.

Предложение 2. *Условие $|X + Y| = |X|$ равносильно $Y + Y \subseteq \operatorname{Stab} X$.*

Доказательство. Пусть $|X + Y| = |X|$. Тогда для любых $y_1, y_2 \in Y$ должно выполняться равенство $X + \{y_1\} = X + \{y_2\}$. Поэтому для любого $x \in X$ вектор $x \oplus y_1 \oplus y_2 \in X$ (напомним, что мы рассматриваем поле характеристики 2, в котором $x \oplus x = 0$ и вычитание совпадает со сложением). Это и означает, что $Y + Y \subseteq \operatorname{Stab} X$.

В обратную сторону: пусть $Y + Y \subseteq \operatorname{Stab} X$. Тогда из $z \in X + \{y_1\}$ следует $z \in X + \{y_2\}$, так как из $z \oplus y_1 \in X$ следует $z \oplus y_2 = z \oplus y_1 \oplus (y_1 \oplus y_2) \in X + \{y_1 \oplus y_2\} = X$. Аналогично проверяем включение $X + \{y_2\} \subseteq X + \{y_1\}$. ▲

Лемма 3. *Нижняя граница в* (2) *достигается в точности для тех пар* X, Y, $|Y| \leqslant |X|$, *для которых существуют такие вектор* a *и подмножество* $S \subseteq \operatorname{Stab} X$, *что* $Y + \{a\} = S$.

Доказательство. В силу предложения 2 достаточно проверить, что $Y + Y \subseteq \operatorname{Stab} X$ равносильно существованию такого вектора a, что $Y + \{a\} \subseteq \operatorname{Stab} X$.

Если множество A лежит в подпространстве V, то $A + A$ также лежит в V. Заметим также, что $(A + \{b\}) + (A + \{b\} = A + A$ для любых $A \subseteq \mathbb{B}^n$, $b \in \mathbb{B}^n$. Поэтому из $Y + \{a\} \subseteq \operatorname{Stab} X$ следует $(Y + \{a\}) + (Y + \{a\}) = Y + Y \subseteq \operatorname{Stab} X$.

В другую сторону: пусть $Y + Y \subseteq \operatorname{Stab} X$. Если $Y \subseteq \operatorname{Stab} X$, то $Y + \{0^n\} \subseteq \operatorname{Stab} X$. В противном случае выберем вектор $y_0 \in Y \setminus \operatorname{Stab} X$. Поскольку $y_0 \oplus y \in \operatorname{Stab} X$ для любого $y \in Y$, то $Y + \{y_0\} \subseteq \operatorname{Stab} X$. ▲

Отсюда получаем простое описание всех случаев достижимости нижней границы в (2). Каждая такая пара X, Y, $|Y| \leqslant |X|$, задается (неоднозначно) выбором подпространства V в $\mathbb{F}_2^n$, подмножества X_0 в $\mathbb{F}_2^n/V$, подмножества $Y_0 \subseteq V$ и вектора $a \in \mathbb{F}_2^n$.

При таком выборе X состоит из объединения смежных классов по V, входящих в X_0, а $Y = \{a\} + Y_0$. Поскольку $V \subseteq \operatorname{Stab} X$, условия леммы 3 выполнены, т.е. на паре X, Y достигается нижняя оценка в (2).

И обратно, если $|X + Y| = |X|$, $|Y| \leqslant |X|$, то в обозначениях леммы 3 такая пара представляется подпространством $V = \operatorname{Stab} X$, подмножеством X_0 тех смежных классов по V, которые входят в X (из определения стабилизатора ясно, что каждый смежный класс либо целиком содержится в X, либо не пересекается с ним), и подмножеством стабилизатора $Y_0 = S = Y + \{a\}$ для вектора a, существование которого гарантирует лемма 3.

Это показывает "структурную простоту" вопроса о достижимости нижней оценки.

Для вопроса о достижимости верхней оценки в (2) ситуация иная.

Приведем достаточное условие достижимости верхней оценки на размер суммы Минковского.

Определим для произвольного множества $X \subseteq \mathbb{B}^n$ *метрический спектр* X как множество всех возможных попарных расстояний между различными точками множества:

$$R(X) = \{r : \ r = \rho(x', x''),\ x' \neq x'',\ x' \in X,\ x'' \in X\}.$$

Мы используем стандартные норму и расстояние Хэмминга на булевом кубе: $\|x\|$ – количество единиц в двоичном слове x, а $\rho(x, y) = \|x \oplus y\|$ – количество координат, в которых различаются двоичные слова x и y.

Предложение 3. *Если* $R(X) \cap R(Y) = \varnothing$, *то* $|X + Y| = |X| \cdot |Y|$.

Доказательство. Пусть $x' \oplus y' = x'' \oplus y''$ для каких-то различных пар элементов из X и Y. Тогда $x' \oplus x'' = y'' \oplus y'$, и метрические спектры множеств X и Y пересекаются. Таким образом, в условиях предложения все попарные суммы элементов X и Y различны. ▲

Отметим простое следствие этого утверждения. Обозначим

$$d(X) = \min(r : \ r \in R(X)), \quad D(X) = \max(r : \ r \in R(X)).$$

Следствие 1. *Если* $D(Y) \leqslant d$ *и* $d(X) \geqslant d + 1$ *для некоторого числа* d, *то* $|X + Y| = |X| \cdot |Y|$.

Отсюда видим, что верхняя оценка в (2) достигается для любого кода $C \subseteq \mathbb{B}^n$ с кодовым расстоянием d и хэммингова шара радиуса $d - 1$ с центром в точке 0^n.

Хэмминговым шаром радиуса r с центром a мы называем множество

$$B_r^n(a) = \{x \in \mathbb{B}^n : \|x - a\| \leqslant r\}. \tag{3}$$

Учитывая сложность теории корректирующих кодов, можно заключить из этого наблюдения "трудность" задачи описания всех случаев достижимости верхней оценки в (2).

§ 4. Сложение фигур в $\mathbb{B}^n$

Геометрические фигуры в $\mathbb{B}^n$ имеют большой содержательный и практический смысл. Такими фигурами являются сферы, шары, грани, линейные многообразия.

4.1. Сложение сфер в $\mathbb{B}^n$. Сферой радиуса r (r-м слоем булева куба) называем множество

$$S_r^n = \{x \in \mathbb{B}^n : \|x\| = r\}.$$

Другими словами, сфера S_r^n – это множество точек $\mathbb{B}^n$, находящихся на расстоянии (Хэмминга) r от нулевой точки (начала координат).

Перестановки координат задают действие симметрической группы S_n на булевом кубе $\mathbb{B}^n$: если $g \in S_n$, то

$$g(x) = g(x_1, x_2, \ldots, x_n) = (x_{g(1)}, x_{g(2)}, \ldots, x_{g(n)}).$$

Это действие естественным образом продолжается на подмножества $\mathbb{B}^n$, как и рассмотренное ранее действие $\mathbb{F}_2^n$ сдвигами. Если $M \subseteq \mathbb{B}^n$ и $g \in S_n$, то

$$g(M) = \bigcup_{x \in M} g(x).$$

Отметим следующие простые свойства действия группы S_n и операций сложения точек и множеств:

1. $g(x \oplus y) = g(x) \oplus g(y)$ для $x, y \in \mathbb{B}^n$;
2. $g(U + V) = g(U) + g(V)$ для $U, V \subseteq \mathbb{B}^n$.

Сферы являются орбитами этого действия. (Напомним, что *орбита* действия группы G на множестве X – это множество вида $O_{x_0} = \{x \in X : x = g(x_0),\ g \in G\}$.) Сумма Минковского двух орбит, очевидно, замкнута относительно этого действия: если $x \in S_p^n + S_q^n$, то $x = u \oplus v$, где $u \in S_p^n$, $v \in S_q^n$. Учитывая указанное выше свойство, имеем $g(x) = g(u) \oplus g(v)$ для любой $g \in S_n$. Поэтому $g(x) \in S_p^n + S_q^n$.

Поэтому сумма сфер является объединением некоторых сфер.

Лемма 4 [1]. *При $p \leqslant q$ справедлива формула*

$$S_p^n + S_q^n = \bigcup_{s=0}^{\min\{p, n-q\}} S_{q-p+2s}^n. \tag{4}$$

Замечание 2. Рассмотрим следующую производящую функцию:

$$\Phi_{n,p,q}(z) = \sum_{\substack{x \in S_p^n \\ y \in S_q^n}} z^{\|x \oplus y\|}.$$

Аналогично доказательству леммы 4, данному в [1], можно получить разложение этой функции

$$\Phi_{n,p,q}(z) = z^{q-p}\binom{n}{q}\sum_{s=0}^{\min\{p,n-q\}}\binom{n-q}{s}\binom{q}{p-s}z^{2s}.$$

Следствие 2. *Справедливы соотношения*

$$S_p^n + S_q^n = S_{n-p}^n + S_{n-q}^n,$$
$$S_p^n + S_{n-q}^n = S_{n-p}^n + S_q^n.$$

Доказательство. Первое соотношение получается из второго заменой q на $n-q$. Второе следует из равенств $|p-(n-q)| = |(n-p)-q|$ и $\min\{p, n-(n-q)\} = \min\{n-(n-p), q\} = \min\{p,q\}$. ▲

Пример 4. Выпишем таблицу сложения для сфер малого радиуса:

$+$	S_0^n	S_1^n	S_2^n
S_0^n	S_0^n	S_1^n	S_2^n
S_1^n	S_1^n	$S_0^n \cup S_2^n$	$S_1^n \cup S_3^n$
S_2^n	S_2^n	$S_1^n \cup S_3^n$	$S_0^n \cup S_2^n \cup S_4^n$

.

Симметрическая булева функция f удовлетворяет условию $f(x) = f(g(x))$ для всех $x \in \mathbb{B}^n$ и $g \in S_n$. Значение симметрической функции одинаково на всех векторах булева куба одинакового веса. Поэтому такая функция однозначно задается множеством "рабочих чисел" $W_f = \{w_1, \ldots, w_k\} \subseteq \{0, 1, 2, \ldots, n\}$:

$$f(x) = \begin{cases} 1, & \text{если } \|x\| \in W_f, \\ 0 & \text{в противном случае.} \end{cases}$$

С помощью формулы (4) можно найти "рабочие числа" для суммы Минковского двух симметрических функций f, g с заданными множествами рабочих чисел A, B. Из свойств сложения Минковского имеем равенство

$$N_f + N_g = \left(\bigcup_{a\in A} S_a^n\right) + \left(\bigcup_{b\in B} S_b^n\right) = \bigcup_{\substack{a\in A\\ b\in B}} (S_a^n + S_b^n).$$

Далее, из формулы (4) получаем

$$N_f + N_g = \bigcup_{\substack{a\in A\\ b\in B}} \bigcup_{s=0}^{\min\{a,n-a,b,n-b\}} S_{|a-b|+2s}^n. \tag{5}$$

Пример 5. Пусть множества рабочих чисел для симметрических булевых функций f, g от n переменных ($n \geqslant 9$) равны $\{1,3,4\}$ и $\{4,5\}$ соответственно. Тогда

$$S_1^n + S_3^n = S_2^n \cup S_4^n, \qquad S_3^n + S_3^n = S_0^n \cup S_2^n \cup S_4^n \cup S_6^n,$$
$$S_1^n + S_5^n = S_4^n \cup S_6^n, \qquad S_3^n + S_5^n = S_2^n \cup S_4^n \cup S_6^n \cup S_8^n,$$
$$S_4^n + S_3^n = S_1^n \cup S_3^n \cup S_5^n \cup S_7^n, \qquad S_4^n + S_5^n = S_1^n \cup S_3^n \cup S_5^n \cup S_7^n \cup S_9^n.$$

Из этих соотношений и формулы (5) получаем

$$N_{f+g} = S_0^n \cup S_1^n \cup S_2^n \cup S_3^n \cup S_4^n \cup S_5^n \cup S_6^n \cup S_7^n \cup S_8^n \cup S_9^n = \bigcup_{i=0}^{9} S_i^n.$$

4.2. Сумма шаров в $\mathbb{B}^n$. Под шаром радиуса r с центром a понимаем, как и выше, множество, задаваемое формулой (3). Отметим, что по определению $B_r^n(a) = \mathbb{B}^n$, если $r \geqslant n$.

Лемма 5 [1]. *Имеет место соотношение*

$$B_p^n(a) + B_q^n(b) = B_{p+q}^n(a \oplus b). \tag{6}$$

Частным случаем этой формулы является следующее утверждение: каждый шар является сдвигом шара с центром в 0^n. Действительно, $B_0^n(a) = \{a\}$ для $a \in \mathbb{B}^n$, и из формулы (6) получаем $B_r^n(a) = B_r^n(0^n) + \{a\}$.

Обобщение определения шара приводит к понятию r-окрестности множества $A \subseteq \mathbb{B}^n$ ("обобщенного шара"):

$$B_r^n(A) = \bigcup_{a \in A} B_r^n(a).$$

Для окрестностей множеств справедливо соотношение, аналогичное (6).

Лемма 6 [1]. *Имеет место соотношение*

$$B_p^n(A) + B_q^n(B) = B_{p+q}^n(A + B).$$

Следствие 3. *Справедливы формулы*

$$B_p^n(B_q^n(A)) = B_{p+q}^n(A),$$
$$B_p^n(A) = A + B_p^n(0^n),$$
$$B_p^n(A + B) = B_p^n(A) + B = A + B_p^n(B),$$
$$B_p^n(A) + B_p^n(B) = A + B + B_{2p}^n(0^n).$$

4.3. Суммы граней в $\mathbb{B}^n$. *Грань* (подкуб, интервал) в $\mathbb{B}^n$ – это множество точек, удовлетворяющих условию

$$J = \{x \in \mathbb{B}^n : a \leqslant x \leqslant b\}.$$

Здесь $\leqslant$ – обычное покоординатное отношение частичного порядка на булевом кубе:

$$x = (x_1, \ldots, x_n) \leqslant y = (y_1, \ldots, y_n) \quad \stackrel{\text{def}}{\iff} \quad x_i \leqslant y_i \text{ для всех } 1 \leqslant i \leqslant n.$$

По-другому интервал J может быть задан словом $\lambda(J)$ длины n над алфавитом $A = \{0, 1, *\}$, которое мы будем называть *кодом интервала*, по следующему правилу: $x \in J$, если x согласовано с $\lambda(J)$, т.е. $x_i = \lambda(J)_i$ для всех i, для которых $\lambda(J)_i \neq *$. Другими словами, если $\lambda(J) = (\lambda_1 \lambda_2 \ldots \lambda_n)$ – код интервала J, то точки интервала получаются всеми возможными заменами символа $*$ на нули или единицы.

Соответствие между этими двумя представлениями устанавливается очень простым способом. Код $\lambda(J) = \lambda_1 \lambda_2 \ldots \lambda_n$ непустого интервала

$$J = \{\alpha_1 \alpha_2 \ldots \alpha_n \leqslant x \leqslant \beta_1 \beta_2 \ldots \beta_n\}$$

вычисляется по формуле

$$\lambda_i = \begin{cases} \alpha_i, & \text{если } \alpha_i = \beta_i, \\ *, & \text{если } \alpha_i < \beta_i. \end{cases}$$

Пример 6.

1. Если $J = \{0100 \leqslant x \leqslant 0111\}$, то $\lambda(J) = (01**)$;
2. Если $J = \mathbb{B}^n = \{00\ldots0 \leqslant x \leqslant 11\ldots1\}$, то $\lambda(\mathbb{B}^n) = **\ldots*$.

Количество символов $*$ в коде интервала J – это размерность $\dim J$ интервала. Количество точек в интервале равно $2^{\dim J}$.

Коды интервалов удобны для нас тем, что в этих терминах легко выражается сумма Минковского двух интервалов.

Введем на множестве $A = \{0, 1, *\}$ операцию $\circledast$, продолжающую сумму по модулю 2 на множестве $\{0, 1\}$:

$\circledast$	0	1	$*$
0	0	1	$*$
1	1	0	$*$
$*$	$*$	$*$	$*$

.

К словам в алфавите A операцию $\circledast$ будем применять покомпонентно.

Лемма 7 [7]. *Если J_1, J_2 – интервалы, то $J_1 + J_2$ также является интервалом и $\lambda(J_1 + J_2) = \lambda(J_1) \circledast \lambda(J_2)$.*

Пример 7.

1. Пусть $\lambda(J_1) = (01*)$, $\lambda_2(J_2) = (100)$. Тогда $\lambda(J_1 + J_2) = (11*)$. Поскольку интервал J_2 состоит из одного вектора, сумма равна сдвигу интервала J_1 на этот вектор;
2. Пусть $\lambda(J) = (1**)$. Тогда $\lambda(J + J) = (0**)$, т.е. $J + J \neq J$;
3. Однако для любого интервала J выполняется равенство $J + J + J = J$. Как видно из таблицы операции $\circledast$, в коде суммы $J + J$ звездочки стоят на тех же местах, что и в коде J, а на остальных местах стоят нули. Добавляя к такому интервалу интервал J еще раз, получаем интервал J;
4. Найдем сумму шара и грани. С точностью до сдвигов достаточно рассмотреть случай $B_r^n(0^n) + \Gamma$, где $\lambda(\Gamma) = (\underbrace{**\ldots*}_{k \text{ штук}}00\ldots0)$.

   Ясно, что в этом случае $x = (\alpha_1\ldots\alpha_k\beta_1\ldots\beta_{n-k}) \in B_r^n(0^n) + \Gamma$, если и только если $\|\beta_1\ldots\beta_{n-k}\| \leqslant r$. Поэтому

$$|B_r^n(0^n) + \Gamma| = 2^k\left(1 + \binom{n-k}{1} + \ldots + \binom{n-k}{r}\right) = 2^k|B_r^n(0^n)|.$$

Из того, что интервалы замкнуты относительно суммы Минковского, следует продолжение начатого в § 2 анализа сложения Минковского для множеств, заданных сжатым представлением. Если вместо общих булевых схем использовать для представления множеств только схемы частного вида, а именно дизъюнктивные нормальные формы (ДНФ), то вычисление суммы Минковского двух функций в таком представлении уже возможно за полиномиальное от длины входа время.

Напомним, что *литералом* называется переменная или ее отрицание. При записи литералов часто используется показательная запись: $x^1 = x$, $x^0 = \neg x$. *Конъюнктом* называется конъюнкция литералов, среди которых нет одинаковых. *ДНФ* – это дизъюнкция конъюнктов, среди которых нет одинаковых.

Интервалы являются множествами единиц конъюнктов. По коду интервала легко выписывается соответствующий конъюнкт в показательной записи:

$$J = N_f, \quad \text{где } f = \bigwedge_{i:\, \lambda(J)_i \neq *} x_i^{\lambda(J)_i}.$$

Сумма Минковского двух ДНФ

$$D_1 = \bigvee_{i=1}^{k} C'_i \quad \text{и} \quad D_2 = \bigvee_{i=1}^{m} C''_i$$

в силу дистрибутивности по объединению равна

$$\bigvee_{i=1}^{k} \bigvee_{j=1}^{m} (C'_i + C''_j).$$

В этой дизъюнкции не более чем квадратичное количество членов. Удаляя повторения литералов применением тождества $\ell \wedge \ell = \ell$ и затем повторения конъюнктов применением тождества $C \vee C = C$, получаем эквивалентную ДНФ, размер которой не более чем квадратичен относительно размеров ДНФ-слагаемых. Такая ДНФ легко строится полиномиальным алгоритмом (и даже алгоритмом, работающим на логарифмической памяти).

Заметим также, что из леммы 7 следует, что количество литералов в сумме Минковского двух конъюнктов не превосходит количества литералов в каждом из них.

4.4. Сумма подпространств $\mathbb{B}^n$. Сложение Минковского подпространств $\mathbb{B}^n$ совпадает с обычным определением суммы подпространств, используемым в линейной алгебре. Если U, V – подпространства $\mathbb{B}^n$, то $U+V$ – тоже подпространство, причем для размерностей этих подпространств выполняется известное соотношение

$$\dim(U+V) = \dim U + \dim V - \dim(U \cap V),$$

откуда следует формула для размера суммы

$$|U+V| = \frac{|U| \cdot |V|}{|U \cap V|}.$$

Таким образом, теория "сложения подпространств" является хорошо развитым разделом линейной алгебры и позволяет давать ответы на многие вопросы, имеющие отношение к данной проблематике.

§ 5. Алгебраические свойства сложения Минковского

В этом параграфе мы рассмотрим несколько вопросов, относящихся к алгебраическим свойствам моноида Минковского.

5.1. Обратимые и идемпотентные элементы. Как нетрудно увидеть из определения, нейтральным элементом относительно сложения Минковского является одноэлементое множество $\{0^n\}$, будем обозначать его через $\mathbb{O}$:

$$A + \mathbb{O} = A \quad \text{для всех } A \subseteq \mathbb{B}^n.$$

Есть два поглощающих элемента: пустое множество $\varnothing$ и весь куб $\mathbb{B}^n$:

$$A + \varnothing = \varnothing, \quad A + \mathbb{B}^n = \mathbb{B}^n \quad \text{для всех } A \subseteq \mathbb{B}^n.$$

Других поглощающих множеств, как нетрудно проверить, нет. Действительно, если $X \neq \varnothing$ (скажем, $x \in X$) и $y \notin X$, то $\{x \oplus y\} + X \neq X$, так как $\{x \oplus y\} + X$ содержит y.

Опишем обратимые элементы $\mathcal{M}_n$. Это в точности одноэлементные множества.

Предложение 4. *Элемент $A \in \mathcal{M}_n$ обратим тогда и только тогда, когда $A = \{a\}$, $a \in \mathbb{B}^n$.*

Доказательство. Обратимость множеств $\{a\}$ следует из равенства $a \oplus a = 0^n$ (заметим также, что каждое такое множество совпадает со своим обратным).

Пусть $A \in \mathcal{M}_n$ обратим, т.е. $A + B = \mathbb{O}$ для некоторого множества B. Это означает, что $a \oplus b = 0^n$ для всех $a \in A$, $b \in B$, т.е. $a = b$ для всех $a \in A$, $b \in B$. Это и означает, что A состоит из одного элемента и $B = A$. ▲

Идемпотентный элемент x в моноиде удовлетворяет равенству $x + x = x$ (мы используем аддитивную запись операции в моноиде). Опишем все идемпотентные элементы моноида Минковского.

Предложение 5. *Если A – идемпотентный элемент моноида Минковского, то A – либо пустое множество, либо подпространство пространства $\mathbb{B}^n$.*

Доказательство. Если для непустого A выполняется равенство $A + A = A$, то $0^n \in A$, так как $a \oplus a = 0^n$ для любого $a \in \mathbb{B}^n$. Осталось заметить, что для любых $a', a'' \in A$ сумма $a' \oplus a''$ принадлежит $A + A = A$. ▲

5.2. Подмоноиды, порожденные одним элементом. *Подмоноидом* называется подмножество элементов моноида, которое образует моноид относительно той же операции. Подмоноидом, порожденным множеством S, называется наименьший по включению подмоноид, содержащий S. Нетрудно видеть, что если S состоит из одного элемента a, то порожденный этим элементом подмоноид содержит нейтральный элемент и все кратные элемента a: a, $2a = a + a$, $3a = a + a + a$, … (Мы используем знак суммы для обозначения операции в моноиде, поэтому говорим о кратных.)

Последовательность кратных элемента любого конечного моноида является периодической: как только в этой последовательности элементы повторились, т.е. $kx = \ell x$, $\ell - k = p > 0$, все остальные кратные периодически повторяются с периодом p: $tx = (k + r)x$, где r – остаток от деления t на p. Число $k - 1$ назовем длиной предпериода (уточним, что мы выбирали первое повторение в последовательности). Если $k = 1$, будем говорить, что последовательность чисто периодическая.

Пример 8.

1. Пусть $A = \{a, b\}$. Тогда $2A = \{0^n, a \oplus b\}$, $3A = \{a, b\} = A$. Последовательность кратных чисто периодическая с периодом 2;
2. Пусть $A = \{a, b, c\}$. Тогда $2A = \{0^n, a \oplus b, b \oplus c, a \oplus c\}$, $3A = \{a, b, c, a \oplus b \oplus c\}$, $4A = \{0^n, a \oplus b, b \oplus c, a \oplus c\} = 2A$. Период 2, длина предпериода 1;
3. Если в предыдущем примере $a \oplus b \oplus c = 0^n$, то уже $3A = \{0^n, a, b, c\} = 2A$.

Приведенные примеры по сути исчерпывают все разнообразие периодов.

Введем обозначение, удобное для дальнейшего анализа. Через $G_k(A)$ обозначим суммы k попарно различных элементов из множества A. В частности, $G_1(A) = A$. Для удобства дальнейших вычислений полагаем также $G_0(A) = \{0^n\}$ и $G_k(A) = \varnothing$, если $k < 0$ или $k > |A|$.

Если занумеровать все элементы A, т.е. $A = \{a_1, a_2, \ldots, a_N\}$, где $N = |A|$, то множества $G_k(\cdot)$ задаются формулой

$$G_k(A) = \bigcup_{1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant N} (a_{i_1} \oplus a_{i_2} \oplus \ldots \oplus a_{i_k}).$$

Заметим, что для множеств $G_k(\cdot)$ выполняется свойство монотонности: если $A \subseteq B$, то $G_k(A) \subseteq G_k(B)$.

Предложение 6. *При $0 \leqslant p \leqslant N$ имеют место равенства*

$$G_p(A) + A = G_{p-1}(A) \cup G_{p+1}(A). \tag{7}$$

Доказательство. Действительно, если добавлять к суммам p различных элементов A элементы A, то будут получаться суммы $p-1$ и суммы $p+1$ различных элементов. (Напомним, что $a \oplus a = 0^n$ для всех $a \in \mathbb{B}^n$.) В граничных случаях $p = 0$ и $p = N$ равенство выполняется в силу принятых выше соглашений. ▲

Из дистрибутивности сложения Минковского по объединению, равенств (7) и начального условия $A = G_1(A)$ легко проверить индукцией по количеству слагаемых, что каждое кратное множества A является объединением каких-то множеств вида $G_k(A)$, $0 \leqslant k \leqslant N$. Будем нумеровать такие объединения булевыми векторами длины $N+1$: вектор $(\gamma_0, \gamma_1, \ldots, \gamma_N)$ соответствует множеству

$$\bigcup_{i:\, \gamma_i = 1} G_i(A).$$

Пусть $g(k)$ – вектор, соответствующий kA. Тогда равенства (7) задают для этих векторов рекуррентные соотношения

$$g(k+1)_p = g(k)_{p-1} \vee g(k)_{p+1}$$

(дизъюнкция берется почленно).

Вычислив несколько первых членов этой рекурренты, легко увидеть правило, по которому они строятся:

$$g(1) = (0,1,0,0,0,0,0,\ldots),$$
$$g(2) = (1,0,1,0,0,0,0,\ldots),$$
$$g(3) = (0,1,0,1,0,0,0,\ldots),$$
$$g(4) = (1,0,1,0,1,0,0,\ldots),$$
$$g(5) = (0,1,0,1,0,1,0,\ldots),$$
$$g(6) = (1,0,1,0,1,0,1,\ldots).$$

Как видно из этих равенств (и легко доказывается индукцией по p), в слове $g(p)$, $p \leqslant |A|$, самая правая единица стоит на позиции с номером p (обратите внимание, что нумерация позиций начинается с 0), а на предыдущих позициях нули и единицы чередуются.

Пример 9. Рассмотрим еще один пример, обобщающий предыдущие. Пусть $A = \{a_1, \ldots, a_d\}$ и все a_i линейно независимы.

Тогда все множества $G_k(A)$ различны при $0 \leqslant k \leqslant d$ и

$$|G_k(A)| = \binom{d}{k}.$$

Поэтому все кратные вплоть до dA будут различными, а кратное $(d+1)A$ будет равно $(d-1)A$. Далее последовательность $(d-1)A, dA$ будет периодически повторяться в последовательности кратных.

Легко также описать множества, лежащие в этом периоде. Обозначим через $\mathbb{F}_2\langle a_1, \ldots, a_d\rangle$ пространство, натянутое на векторы $a_1, \ldots, a_d$, а через E_0 – подпространство векторов четного веса в базисе $a_1, \ldots, a_d$, т.е.

$$E_0 = \bigcup_{i=0}^{d/2} G_{2i}(A).$$

Это пространство коразмерности 1, поэтому в нем содержится ровно половина точек из $\mathbb{F}_2\langle a_1, \ldots, a_d\rangle$. Остальные точки образуют линейное многообразие $E_1 = E_0 + \{a_1\}$. Другими словами,

$$E_1 = \bigcup_{i=0}^{d/2} G_{2i+1}(A).$$

В периоде кратных A будут как раз E_0 и E_1. Действительно, если d нечетно, то $(d-1)A = E_0$, тогда $dA = E_1$. Если d четно, то порядок обратный: $(d-1)A = E_1$ и $dA = E_0$.

Для анализа общей ситуации нам потребуется связать с подмножеством $A \subseteq \mathbb{B}^n$ из N элементов подпространство координатного пространства $\mathbb{F}_2^N$ (или линейный код). Пусть $A = \{a_1, \ldots, a_N\}$ – список элементов множества A без повторений. Определим

$$C(A) = \left\{ u \in \mathbb{F}_2^N : \bigoplus_{i=1}^{N} u_i a_i = 0^n \right\}.$$

По сути, $C(A)$ состоит из тех линейных комбинаций элементов множества A, которые равны 0^n. (Напомним, что мы рассматриваем векторные пространства над полем $\mathbb{F}_2$, поэтому коэффициенты линейных комбинаций равны 0 или 1.)

Заметим, что любой линейный код представляется в виде $C(A)$ для некоторого множества A: достаточно взять проверочную матрицу кода, множество A будет состоять из ее столбцов.

Через $C^\perp(A)$ обозначим ортогональное дополнение к $C(A)$:

$$C^\perp(A) = \left\{ v \in \mathbb{F}_2^N : \bigoplus_{i=1}^{N} v_i u_i = 0 \text{ для всех } u \in C(A) \right\}.$$

Определение. Назовем подмножество $A \subseteq \mathbb{B}^n$ *четным*, если $\mathbb{1} \in C^\perp(A)$. Здесь $\mathbb{1}$ обозначает вектор из одних единиц. В противном случае будем называть множество A *нечетным*.

Например, любой базис B в $\mathbb{B}^n$ является четным множеством, так как $C(B) = \{0^N\}$, а $C(B)^\perp = \mathbb{F}_2^N$. (В данном случае $N = n$.)

Замечание 3. Конструкция $C(A)$ зависит от упорядочения элементов множества A. Однако коды, отвечающие разным упорядочениям, эквивалентны: они переводятся друг в друга перестановками координат. Так что свойства кода $C(A)$, инвариантные относительно перестановок координат, зависят только от множества A и не зависят от выбранного на A упорядочения.

В частности, определение четности множества как раз является примером такого свойства. Четность множества не зависит от упорядочения, выбранного для построения кода $C(A)$.

Как уже говорилось, векторы кода $C(A)$ задают линейные комбинации элементов множества A, равные нулю. Далее нам будет удобно использовать характеризацию четных и нечетных множеств в этих терминах.

Лемма 8. *Подмножество $A \subseteq \mathbb{B}^n$ четное, если и только если из $\bigoplus_{a \in S \subseteq A} a = 0^n$ следует, что $|S|$ четное.*

Доказательство. Сопоставим каждому подмножеству $S \subseteq A$ его характеристический вектор:

$$u_i^S = \begin{cases} 1, & \text{если } a_i \in S, \\ 0 & \text{в противном случае} \end{cases}$$

(предполагаем, что множество задано упорядоченным списком без повторений $A = \{a_1, \ldots, a_N\}$). Условие $\bigoplus\limits_{i \in S} a_i = 0^n$ равносильно тому, что $u^S \in C(A)$. При этом количество единиц в характеристическом векторе u^S равно количеству элементов в множестве S.

Равенство $\bigoplus\limits_{i=1}^{N} \mathbb{1}_i u_i = 0$ равносильно тому, что в векторе $u \in \mathbb{F}_2^N$ четное количество единиц.

Если множество A четное, то в любом $u \in C(A)$ четное количество единиц. Значит, равенство $\bigoplus\limits_{a \in S \subseteq A} a = 0^n$ возможно лишь при четном $|S|$.

И наоборот, если множество A нечетное, то существует такой вектор $u = u^S \in C(A)$, что $\bigoplus\limits_{i=1}^{N} \mathbb{1}_i u_i^S = 1$. Тогда в S нечетное количество элементов, но $\bigoplus\limits_{i \in S} a_i = 0^n$. ▲

Обозначим через $L(A)$ линейную оболочку множества A, а через d – размерность $L(A)$. В множестве A заведомо содержится хотя бы один базис линейной оболочки. Для четных и нечетных множеств разложения элементов A по базисам линейной оболочки, состоящим из элементов A, устроены по-разному.

Предложение 7. *Пусть A нечетное. Тогда существуют базис $B \subseteq A$ линейной оболочки $L(A)$ и элемент $a_B \in A$, такие что разложение a_B по базису B является суммой четного количества элементов базиса.*

Доказательство. Выберем наименьшее по включению множество S нечетного размера, для которого $\bigoplus\limits_{a \in S \subseteq A} a = 0^n$ (такие множества существуют, так как A нечетное).

Тогда для любого $S' \subset S$ выполняется неравенство $\bigoplus\limits_{a \in S' \subseteq A} a \neq 0^n$, так как в противном случае одно из множеств S' или $S \setminus S'$ будет собственным подмножеством S нечетного размера, суммирование по которому дает 0^n.

Значит, если выбрать какой-элемент $a_B \in S$, то остальные элементы из S (обозначим их $b_1, \ldots, b_k$) линейно независимы. Продолжим их до базиса $L(A)$ элементами $b_{k+1}, \ldots b_d \in A$: $B = \{b_1, \ldots, b_k, b_{k+1}, \ldots, b_d\}$. Разложение a_B по этому базису состоит из четного числа элементов, так как $k = |S| - 1$ четно. ▲

Заметим, что если $A = \{a_1, \ldots, a_N\}$ и $a_1 = 0^n$, то построение в доказательстве дает множество $S = \{a_1\}$ (1 – наименьшее положительное нечетное число, а список элементов множества не содержит повторений). Поэтому $a_B = a_1 = 0^n$ (других элементов в S нет). Базисом B при этом можно выбрать произвольный базис $L(A)$, состоящий из элементов A.

Второе замечание: из леммы 8 следует, что для четных множеств не существует базиса $L(A)$, состоящего из элементов A и такого, что какой-то элемент A разлагается в сумму четного числа базисных элементов.

Выбранный в предложении 7 базис важен для анализа кратных в силу следующего утверждения.

Предложение 8. *Если A нечетное, то $(d+1)A = L(A)$, где $d = \dim L(A)$.*

Доказательство. По предложению 7 существует базис $B \subset A$ линейной оболочки множества A, по которому некоторый элемент $a_B \in A$ разлагается в сумму четного количества базисных векторов. Для a_B и вектора $x \in G_k(A)$ рассмотрим

разложения по базису B

$$a_B = \bigoplus_{b\in S} b, \quad S \subseteq B, \quad |S| \equiv 0 \pmod 2,$$
$$x = \bigoplus_{b\in X} b, \quad X \subseteq B. \tag{8}$$

Для x есть другое разложение в сумму элементов множества A:

$$x = a_B \oplus \bigoplus_{b\in X\oplus S} b. \tag{9}$$

Здесь через $X \oplus S$ обозначена симметрическая разность множеств, т.е. $X \oplus S = X \setminus S \cup S \setminus X$.

Четность количества слагаемых в этих двух разложениях разная. Действительно, поскольку в S четное количество элементов, то $|S \setminus X|$ и $|X \cap S|$ имеют одинаковую четность. Поэтому

$$|X \oplus S| = |X \setminus S| + |S \setminus X| \equiv |X \setminus S| + |X \cap S| = |X| \pmod 2,$$

а в разложении (9) есть еще один вектор a_B помимо тех $|X \oplus S|$, которые стоят под знаком суммы.

Таким образом, для x есть два разложения, четность количества слагаемых в которых различна. Количество слагаемых в (8) не превосходит d, а в (9) не превосходит $d+1$. Поэтому $x \in G_j(A)$, где j имеет отличную от k четность и $j \leqslant d+1$.

Отсюда получаем включения

$$G_k(A) \subseteq \bigcup_{\substack{j\leqslant d+1\\ j+k\equiv 1 \pmod 2}} G_j(A). \tag{10}$$

Поэтому для четного d из (10), монотонности кратных и вычислений в примере 9 получаем

$$\begin{aligned} &(d+1)A \supseteq dA \supseteq dB = E_0,\\ &(d+1)A \supseteq (d+1)B = (d-1)B = E_1, \end{aligned} \tag{11}$$

т.е. $(d+1)A \supseteq E_0 \cup E_1 = L(A)$. (Здесь использованы те же обозначения, что и в примере 9.)

Для нечетного d рассуждение аналогично: в первой строке (11) будет включение E_1 в $(d+1)A$, а во второй – E_0. ▲

Теперь дадим общее описание множества кратных.

Теорема 2. *Если A – нечетное множество, то период последовательности кратных A равен* 1, *элемент в периоде – линейная оболочка A, а длина предпериода не больше $d = \dim L(A)$.*

Если A – четное множество, то период последовательности кратных A равен 2, *элементы в периоде – подпространство коразмерности* 1 *в $L(A)$ и его сдвиг, а длина предпериода не больше* $\max(0, d-2)$.

Доказательство. Так как $A \subseteq L(A)$, то $L(A) + A = L(A)$, и первая часть теоремы прямо следует из предложений 7 и 8.

Далее считаем, что A – четное множество и $B \subseteq A$ – базис в $L(A)$.

Пусть $d = \dim L(A)$ четное. Тогда $(d-1)A \supseteq (d-1)B = (d+1)B = E_1$ (используем те же обозначения, что и в примере 9).

Предположим, что $x \in (d-1)A \setminus E_1$. Это означает, что $x \in E_0$, т.е. x раскладывается в сумму четного числа базисных векторов. С другой стороны, $x \in (d-1)A$ и поэтому раскладывается в сумму нечетного числа попарно различных векторов из A. Из этих двух выражений для x получаем сумму нечетного числа векторов из A, равную 0^n. Это противоречит определению четного множества. Значит, $(d-1)A = E_1$.

Теперь заметим, что $dA \supseteq dB = E_0$. Если $x \in dA \setminus E_0$, то рассуждением, аналогичным предыдущему, опять приходим к противоречию с четностью множества A, поскольку для такого x есть разложение в сумму как нечетного количества базисных векторов ($x \in E_1 = L(A) \setminus E_0$), так и четного ($x \in dA$ и поэтому раскладывается в сумму четного числа попарно различных векторов из A). Значит, $dA = E_0$.

Поэтому дальнейшая последовательность кратных повторяется с периодом 2. Длина предпериода не больше $d-2$ при $d \geqslant 2$. Если $d = 1$, то A – одноэлементое множество, в этом случае длина предпериода равна 0.

Анализ в случае нечетного $d = \dim A$ аналогичен. В этом случае $(d-1)A = E_0$, а $dA = E_1$. ▲

Оценка длины предпериода в доказательстве теоремы 2 в некоторых случаях далека от точной. Скажем, для любого подпространства V последовательность кратных чисто периодическая с периодом 1.

Обсудим вычислительную сложность определения периода и предпериода последовательности кратных множества A.

Проверка множества на четность возможна за полиномиальное время даже в том случае, если множество задано списком элементов, а не полной таблицей значений характеристической функции. Достаточно применить алгоритм Гаусса и найти базис в пространстве $C(A)$, после чего проверить, что каждый базисный вектор содержит четное количество единиц.

Дело обстоит иначе с вычислением предпериода последовательности кратных множества A.

Так как длина предпериода не превосходит $n+1$ для любого множества $A \subseteq \mathbb{B}^n$, то если множество A задано таблицей значений характеристической функции, то вычисление всей последовательности кратных вплоть до периода занимает время, полиномиальное от размера этой таблицы (длины входа).

Если же множество задано списком элементов, то задача определения длины предпериода оказывается NP-трудной, поскольку она связана с оценкой радиуса покрытия кода $C(A)$. Радиус покрытия кода – это минимально возможное s, такое что на расстоянии (Хэмминга) s от любой точки есть точка из кода. Применив это определение к коду $C(A)$, получаем, что радиус покрытия s равен минимуму по таким t, что суммами $\leqslant t$ элементов A можно представить любой вектор пространства $L(A)$. Из теоремы 2 следует, что длина предпериода разве что на 1 отличается от радиуса покрытия кода $C(A)$.

В работе [8] показано, что даже приближенное вычисление радиуса покрытия кода является NP-трудной задачей. Более точно, в этой работе доказана NP-трудность семейства алгоритмических задач $\mathrm{GapCRPcodes}_c$ с априорной информацией (promise problem). Здесь $c > 0$ – произвольное положительное число (точность приближения). Входом задачи $\mathrm{GapCRPcodes}_c$ является матрица H над полем $\mathbb{F}_2$ (проверочная матрица кода) и число d. Задача состоит в том, чтобы различить два случая: (i) радиус покрытия кода $C_H = \{x : Hx = 0\}$ не превосходит d и (ii) радиус покрытия кода C_H больше cd. Результатом работы алгоритма должен быть ответ “да” в первом случае и “нет” во втором. На остальных входах результат работы алгоритма может быть произвольным.

NP-трудность задачи $\mathrm{GapCRPcodes}_c$ означает, что если для нее существует алгоритм решения за полиномиальное время, то P = NP. Отсюда сразу следует NP-труд-

ность определения длины предпериода последовательности кратных множества A, если оно задано списком своих элементов: как сказано выше, эта длина отличается от радиуса покрытия кода $C(A)$ не более чем на 1, и любой код может быть представлен в виде $C(A)$, если взять в качестве множества A столбцы проверочной матрицы кода.

5.3. Множества порождающих. Из теоремы 2 следует оценка мощности подмоноида Минковского, порожденного несколькими элементами (т.е. подмножествами булева куба).

Следствие 4. *Рассмотрим подмоноид* $M = \langle A_1, \ldots, A_s \rangle$, *порожденный множествами* $A_1, \ldots, A_s$. *Тогда*

$$|M| \leqslant \prod_{i=1}^{s} (\dim L(A_i) + 2),$$

где $L(A)$ *обозначает линейную оболочку элементов множества* $A \subseteq \mathbb{F}_2^n$.

Доказательство. Любой элемент из моноида M имеет вид

$$k_1 A_1 + k_2 A_2 + \ldots + k_s A_s, \quad k_i \geqslant 0.$$

Из теоремы 2 следует, что у множества $A \subseteq \mathbb{B}^n$ всего имеется не более $\dim L(A) + 2$ различных кратных (включая кратное с множителем 0). ▲

Отсюда получаем оценку на размер семейства $\mathcal{G}$ множеств, порождающих весь моноид Минковского:

$$(n+2)^{|\mathcal{G}|} \geqslant 2^{2^n},$$

т.е. $|\mathcal{G}| = 2^{n(1-o(1))}$.

Если от описания на языке подмножеств перейти к описанию на языке булевых функций, то подмоноиды, порожденные некоторым набором подмножеств (функций), задают класс функций, выражаемых через порождающие очень простым образом (как сумма кратных). Сама операция, впрочем, достаточно сложна. Тем не менее представляется интересным вопросом описание классов функций, порождаемых как суммы Минковского некоторого выбранного набора "базисных" функций.

Теперь приведем аргументы против существования "простого" набора порождающих у моноида Минковского. Более точно, мы докажем значительное усиление оценки количества элементов в порождающем семействе множеств (см. следствие 5 ниже). Оказывается, в любом таком семействе содержится дважды экспоненциальное количество множеств. Из обычных мощностных соображений отсюда следует, например, что в таком множестве обязаны присутствовать множества, соответствующие функциям экспоненциальной схемной сложности.

Примитивные элементы моноида Минковского – такие A, что A необратим в моноиде, а из разложения $A = X + Y$ следует, что X или Y обратим в моноиде.

Разложения в сумму Минковского вида $A = B + X$, где X обратим в моноиде, будем называть *тривиальными*. По предложению 4 все тривиальные разложения имеют вид $A = B + \{c\}$, $c \in \mathbb{B}^n$ (так как обратимыми являются только одноэлементные множества).

В силу равенства $X + Y = (X + \{a\}) + (Y + \{a\})$ далее предполагаем без ограничения общности, что для слагаемых разложения $A = X + Y$ выполняются свойства $0^n \in X$, $Y \subseteq A$.

Пусть $f\colon \mathbb{B}^k \to \mathbb{B}^s$ – некоторое отображение k-мерного булева куба в s-мерный. График этого отображения

$$\Gamma_f = \{(x, y) \in \mathbb{B}^{k+s} : \ y = f(x)\}$$

является подмножеством $\mathbb{B}^{k+s}$. Сформулируем достаточное условие примитивности графика Γ_f как элемента моноида $\mathcal{M}_{k+s}$.

Предложение 9. *Пусть для любого двумерного аффинного подпространства* $\{a, a+b, a+c, a+b+c\} \subseteq \mathbb{F}_2^k$ *выполняется неравенство*

$$f(a) \oplus f(a+b) \oplus f(a+c) \oplus f(a+b+c) \neq 0^s.$$

Тогда множество Γ_f *примитивно.*

Доказательство. Если $\Gamma_f = X + Y$ – нетривиальное разложение графика отображения f, то $|X| > 1$, $|Y| > 1$. Считаем, как сказано выше, что $Y \subseteq \Gamma_f$ и $0^{k+s} \in X$. Выберем два элемента из Y, обозначим их (x_1, f_1) и (x_2, f_2), и какой-то ненулевой элемент из X, обозначим его (Δ_x, Δ_y).

Тогда $(x_1 \oplus \Delta_x, f_1 \oplus \Delta_y) \in \Gamma_f$ и $(x_2 \oplus \Delta_x, f_2 \oplus \Delta_y) \in \Gamma_f$, т.е. для двумерного подпространства

$$\{x_1, x_1 \oplus (x_1 \oplus x_2), x_1 \oplus \Delta_x, x_1 \oplus (x_1 \oplus x_2) \oplus \Delta_x\}$$

в $\mathbb{F}_2^k$ получаем

$$f(x_1) = f_1,$$
$$f(x_1 \oplus (x_1 \oplus x_2)) = f_2,$$
$$f(x_1 \oplus \Delta_x) = f_1 \oplus \Delta_y,$$
$$f(x_1 \oplus (x_1 \oplus x_2) \oplus \Delta_x) = f_2 \oplus \Delta_y.$$

Сумма значений f по этому подпространству равна 0^s, что противоречит условию предложения. ▲

Это достаточное условие позволяет доказать дважды экспоненциальную нижнюю оценку на количество примитивных элементов в моноиде Минковского.

Теорема 3. *Количество примитивных элементов в моноиде Минковского* $\mathcal{M}_n$ *не меньше* $2^{2^{\Omega(n)}}$.

Доказательство. Двумерное аффинное подпространство в $\mathbb{B}^k$ задается тремя векторами, так что общее количество таких подпространств не превосходит 2^{3k}.

Функция $f\colon \mathbb{B}^k \to \mathbb{B}^s$ задается $s2^k$ булевыми переменными: $\varphi(i, x) = 1$ равносильно тому, что $f(x)_i = 1$. В пространстве $\mathbb{F}_2^{s2^k}$, координатами которого являются эти переменные, условие равенства нулю суммы значений функции $f\colon \mathbb{B}^k \to \mathbb{B}^s$ на некотором двумерном аффинном подпространстве задает систему из s линейно независимых однородных линейных уравнений. Решения такой системы составляют долю 2^{-s} от общего количества функций $\mathbb{B}^k \to \mathbb{B}^s$.

Поэтому доля функций $f\colon \mathbb{B}^k \to \mathbb{B}^s$, удовлетворяющих достаточному условию примитивности из предложения 9, не меньше $1 - 2^{3k-s}$ (оценка объединения). Значит, при $3k < s$ хотя бы половина функций удовлетворяет этому условию и количество примитивных элементов в $\mathcal{M}_{k+s}$ не меньше 2^{s2^k-1}. Выберем $s = 3k+1$, тогда $n = k + s = 4k + 1$, и в моноиде Минковского $\mathcal{M}_n$ не менее чем

$$2^{(3k+1)2^k-1} = 2^{2^{\Omega(n)}}$$

примитивных элементов. ▲

Следствие 5. *Пусть семейство* $\mathcal{G}$ *множеств порождает моноид Минковского. Тогда* $|\mathcal{G}| = 2^{2^{\Omega(n)}}$.

Доказательство. Пусть A – примитивный элемент моноида Минковского. В любой системе порождающих моноида Минковского должен содержаться *ассоци-*

ированный с A элемент моноида, т.е. такое множество B, что $A = B + X$, где X обратим в моноиде.

Отношение ассоциированности – это отношение эквивалентности, классы эквивалентности этого отношения называются классами ассоциированных элементов.

В моноиде Минковского обратимыми элементами, как проверено выше (предложение 4), являются одноэлементные множества и только они. Поэтому размер класса ассоциированных элементов в моноиде Минковского равен 2^n.

Таким образом, в любую систему порождающих должен входить хотя бы один элемент из каждого класса ассоциированных элементов. Поэтому из теоремы 3 получаем искомую оценку на размер семейства $\mathcal{G}$. ▲

§ 6. Дубли Минковского

Простейшим уравнением в моноиде Минковского является уравнение вида

$$X + Y = A. \tag{12}$$

Его решения задают возможные факторизации A как элемента моноида Минковского.

У уравнения (12) всегда есть тривиальные решения: $X = \{x\}$, $Y = A + \{x\}$. Напомним, что одноэлементные множества обратимы в моноиде Минковского. Эти тривиальные решения отвечают как раз таким тривиальным факторизациям A.

Если A таково, что других решений у уравнения (12) нет, то A – примитивный элемент моноида Минковского (см. п. 5.3).

Пример 10.

1. Если $A = \mathbb{B}^n$, то в качестве X можно взять $\mathbb{B}^n$, а в качестве Y любое подмножество $\mathbb{B}^n$;
2. Если A – подпространство $\mathbb{B}^n$, то $A + A = A$, и таким образом, одним из решений уравнения (12) является $X = Y = A$.

Родственное уравнение

$$X + X = A \tag{13}$$

уже не всегда имеет решение. Те множества, для которых (13) имеет решение, будем называть *дублями Минковского*.

Пример 11. Если A – подпространство $\mathbb{B}^n$, то $A + A = A$, и поэтому A является дублем Минковского.

Уравнение (13) представляет интерес по нескольким причинам.

В метрических задачах на булевом кубе оно возникает при характеризации взаимных расстояний между точками множества. Приведем краткое изложение этой связи (подробнее см. в [2]).

Напомним, что мы используем на булевом кубе норму Хэмминга $\|x\|$ (количество единиц в x) и расстояние Хэмминга $\rho(x, y) = \|x \oplus y\|$ (количество позиций, в которых различаются слова x и y).

Определим норму множества как

$$\|A\| = \min_x \{\|x\| : x \in A\}.$$

Тогда $\|A + B\|$ совпадает с расстоянием Хаусдорфа между множествами:

$$\rho(A, B) = \min_{\substack{x \in A \\ y \in B}} \rho(x, y) = \min_{\substack{x \in A \\ y \in B}} \|x \oplus y\| = \min_{z \in A+B} \|z\| = \|A + B\|.$$

Множество

$$R(A,B)=\{\rho(a,b):\ a\in A,\ b\in B\}$$

характеризует "взаимный" спектр расстояний между точками множеств A и B. Напомним, что $R(A,A)=R(A)$ называется метрическим спектром множества A. Таким образом, множество $A+A$ однозначно определяет метрический спектр.

Пример 12. Если $X+X=A\cup\{0^n\}$ и $A\subseteq S_m^n$, то X – эквидистантный код с расстоянием m между любыми двумя различными точками.

Таким образом, задачи построения эквидистантных кодов и разрешимости уравнения (13) оказываются связанными.

Понятие дубля Минковского тесно связано с изучением эквивалентности аддитивных каналов [3], где описание класса эквивалентности связано с нахождением всех решений уравнения (13). В частности, при описании эквивалентности аддитивных каналов оказывается важным следующее простое наблюдение.

Пусть $\mathrm{GL}_2(n)$ – группа обратимых матриц порядка n с элементами из поля $\mathbb{F}_2$. Эта группа действует на векторах координатного пространства $\mathbb{F}_2^n$, и это действие естественно переносится на подмножества $\mathbb{F}_2^n$:

$$gA=\{x:\ x=ga,\ a\in A\}.$$

Обозначим через G_A стабилизатор этого действия.

Предложение 10. *Пусть $g\in G_A$. Тогда равенства $X+X=A$ и $gX+gX=A$ равносильны.*

Доказательство. Если $X+X=A$, то $gX+gX=g(X+X)=gA=A$.

Обратное утверждение следует из прямого, если заметить, что g^{-1} также принадлежит G_A. ▲

Дубли Минковского имеют также естественную характеризацию в терминах анализа Фурье на булевом кубе. Напомним основные обозначения и определения, относящиеся к такому анализу.

С элементом $s\in\mathbb{F}_2^d$ свяжем моном

$$x^s=\prod_i x_i^{s_i}=\prod_{i:\ s_i=1} x_i.$$

Мономы такого вида образуют ортонормированный базис в пространстве функций $\{\pm1\}^d\to\mathbb{R}$ относительно скалярного произведения

$$\langle f,g\rangle=\frac{1}{2^d}\sum_{a\in\{\pm1\}^d} f(a)g(a).$$

Коэффициенты разложения функции $f\colon\{\pm1\}^d\to\mathbb{R}$ по этому базису называются коэффициентами Фурье:

$$f(x)=\sum_{s\in\mathbb{F}_2^d}\widehat{f}(s)x^s,\quad \widehat{f}(s)=\langle f,x_s\rangle.$$

Легко проверяется формула свертки

$$\widehat{fg}(s)=\sum_{q\in\mathbb{F}_2^d}\widehat{f}(q)\widehat{g}(s\oplus q). \tag{14}$$

Обозначим через $\widehat{\operatorname{spec}} f = \{s : \widehat{f}(s) \neq 0\}$ носитель функции $\widehat{f}$, который мы будем называть Фурье-носителем функции. Следствием формулы свертки (14) является

Предложение 11. *Пусть $\widehat{g}(s) \geqslant 0$ для всех $s \in \mathbb{F}_2^d$. Тогда*

$$\widehat{\operatorname{spec}}(g^2) = \widehat{\operatorname{spec}}\, g + \widehat{\operatorname{spec}}\, g.$$

Из этого предложения, в свою очередь, получаем характеризацию дублей Минковского в терминах анализа Фурье на булевом кубе.

Лемма 9. *Дубли Минковского – это в точности Фурье-носители квадратов функций с неотрицательными коэффициентами Фурье.*

Доказательство. В одну сторону утверждение леммы совпадает с предложением 11. В другую сторону: пусть $A = B + B$. Рассмотрим функцию

$$\check{\chi}_B = \sum_s \chi_B(s) x^s = \sum_{s \in B} x^s.$$

У нее коэффициенты Фурье неотрицательные, поэтому $\widehat{\operatorname{spec}}(\check{\chi}_B)^2 = A$. ▲

Множество дублей Минковского образует подмоноид моноида Минковского.

Предложение 12 [1]. *Если A и B – дубли, то и $A + B$ – дубль.*

Из $A = X + X$ и $B = Y + Y$ с учетом ассоциативности и коммутативности сложения Минковского получаем

$$A + B = (X + Y) + (X + Y) = (X + X) + (Y + Y).$$

Таким образом, отображение $\tau\colon X \mapsto X + X$ является эндоморфизмом (морфизмом в себя) моноида Минковского, а дубли Минковского – это образ моноида Минковского при действии эндоморфизма τ.

Характеризация дублей Минковского и вычислительная сложность проверки того, что множество является дублем Минковского, – трудные открытые вопросы в этой области.

СПИСОК ЛИТЕРАТУРЫ

1. *Leontiev V., Movsisyan G., Margaryan Zh.* On Addition of Sets in Boolean Space // J. Inf. Secur. 2016. V. 7. № 4. P. 232–244.
2. *Leontiev V., Movsisyan G., Margaryan Zh.* Algebra and Geometry of Sets in Boolean Space // Open J. Discrete Math. 2016. V. 6. № 2. P. 25–40.
3. *Леонтьев В.К., Мовсисян Г.Л., Осипян А.А.* Классификация подмножеств B^n и аддитивные каналы // Вестн. Моск. ун-та. Сер. 1. Матем., мех. 2014. № 5. С. 23–29.
4. *Leontiev V., Movsisyan G., Osipyan A., Margaryan Zh.* On the Matrix and Additive Communication Channels // J. Inf. Secur. 2014. V. 5. № 4. P. 178–191.
5. *Sipser M.* Introduction to the Theory of Computation. Boston: Thomson Course Technology, 2006.
6. *Китаев А., Шень А., Вялый М.* Классические и квантовые вычисления. М.: МЦНМО, 1999.
7. *Леонтьев В.К.* О гранях единичного n-мерного куба // Ж. вычисл. матем. и матем. физ. 2008. Т. 48. № 6. С. 1126–1139.
8. *Guruswami V., Micciancio D., Regev O.* The Complexity of the Covering Radius Problem on Lattices and Codes // Proc. 19th IEEE Annual Conf. on Computational Complexity (CCC'04). Amherst, MA, USA. June 21–24, 2004. Washington, DC, USA: IEEE Comput. Soc., 2004. P. 161–173.

Вялый Михаил Николаевич
Вычислительный центр им. А.А. Дородницына РАН
Московский физико-технический институт
(государственный университет)
Национальный исследовательский университет
"Высшая школа экономики"
vyalyi@gmail.com
Леонтьев Владимир Константинович
Вычислительный центр им. А.А. Дородницына РАН
vkleontiev@yandex.ru

Поступила в редакцию
24.02.2019
После доработки
26.04.2019
Принята к публикации
21.05.2019