Федеральное государственное бюджетное учреждение науки «Институт математики им. С. Л. Соболева Сибирского отделения Российской академии наук (ИМ СО РАН)»

На правах рукописи
УДК 519.7

Облаухов Алексей Константинович

Метрически регулярные множества в булевом кубе: конструкции и свойства

Специальность 01.01.09 —
«Дискретная математика и математическая кибернетика»

Диссертация на соискание учёной степени
кандидата физико-математических наук

Научный руководитель:
кандидат физико-математических наук
Токарева Наталья Николаевна

Новосибирск — 2020

Оглавление

Стр.

Введение 4

Глава 1. Определения, обозначения и примеры 14
1.1 Определения 14
1.2 Примеры 17

Глава 2. Конструкции метрически регулярных множеств 19
2.1 Сходимость операции взятия метрического дополнения 19
2.2 Итеративные конструкции строго метрически регулярных множеств 21
2.3 Количество множеств, получаемых итеративной конструкцией . . . 26

Глава 3. Оценки мощностей метрически регулярных множеств 30
3.1 Наименьшее и наибольшее метрически регулярные множества . . 30
3.2 Оценка мощности метрически регулярных множеств при фиксированном радиусе покрытия 32
3.3 Построение семейств больших метрически регулярных множеств . 34
3.4 Оценка мощности наибольших метрически регулярных множеств . 36

Глава 4. Метрические дополнения и метрическая регулярность линейных подпространств 40
4.1 Базовые свойства 40
4.2 Линейные подпространства с базисом малого веса 42
4.3 Метрические дополнения аффинных подпространств 44
4.4 Метрически регулярные подпространства 44

Глава 5. Метрическая регулярность кодов Рида-Маллера 47
5.1 Определения 48
5.2 Код Рида-Маллера $\mathcal{R}_{1,5}$ 49
5.3 Коды Рида-Маллера порядков 0, m, $m-1$ и $m-2$ 52
5.4 Коды Рида-Маллера порядка $m-3$: метод синдромных матриц . . 53
5.5 Коды Рида-Маллера порядка $m-3$: радиус покрытия 56

Стр.

5.6 Коды Рида-Маллера порядка $m-3$: m чётно 58
5.6.1 Радиус покрытия и метрическое дополнение выколотого кода 59
5.6.2 Радиус покрытия и метрическое дополнение невыколотого кода 60
5.6.3 Метрическая регулярность 63
5.7 Коды Рида-Маллера порядка $m-3$: m нечётно 65
5.7.1 Радиус покрытия и метрическое дополнение выколотого кода 65
5.7.2 Радиус покрытия и метрическое дополнение невыколотого кода 67
5.7.3 Метрическая регулярность 72
5.8 Код Рида-Маллера $\mathcal{RM}(2,6)$ 75

Заключение 81

Список литературы 82

Приложение А. Приложение к доказательству леммы 5.17 из раздела 5.8 88

Введение

В данной работе изучаются метрические свойства подмножеств пространства $\mathbb{F}_2^n$ (часто называемого *булевым кубом* размерности n), в частности, свойство метрической регулярности и связанные с ним понятия и объекты.

Приведём несколько необходимых определений.

Пусть $\mathbb{F}_2^n = \{0,1\}^n$ — множество двоичных наборов длины n, рассматриваемое как векторное пространство над полем $\mathbb{F}_2$. *Расстоянием Хэмминга* между двумя двоичными векторами называется число таких координат, в которых эти векторы различаются. *Радиусом покрытия* $\rho(X)$ множества $X \subseteq \mathbb{F}_2^n$ называется наибольшее из расстояний от векторов $\mathbb{F}_2^n$ до множества X. Назовём *метрическим дополнением* $\widehat{X}$ множества X множество всех векторов $\mathbb{F}_2^n$, находящихся на максимальном возможном расстоянии от данного множества. Множество называется *метрически регулярным*, если его второе метрическое дополнение (метрическое дополнение метрического дополнения, $\widehat{\widehat{X}}$) совпадает с ним самим.

Задача изучения метрического дополнения множества тесно связана с задачами покрытия и упаковки, как в булевом кубе, так и в других метрических пространствах. *Задача упаковки сфер* в евклидовом пространстве $\mathbb{R}^n$ заключается в поиске наиболее плотного расположения одинаковых сфер в пространстве при условии, что никакие две сферы не перекрываются. *Задача покрытия сферами* требует найти наименее плотное расположение сфер, при котором объединение объёмов всех сфер покрывает пространство целиком.

Задачи покрытия и упаковки в пространстве $\mathbb{R}^n$ очень часто решаются при помощи решётчатых упаковок. *Решёткой* называется подмножество евклидова пространства $\mathbb{R}^n$, образующее группу по сложению, а *решётчатой упаковкой* называется множество сфер, центры которых лежат в узлах соответствующей решётки. *Глубокой дырой* решётки называется точка пространства, удалённая на максимальное возможное расстояние от узлов решётки. Таким образом, множество всех глубоких дыр решётки есть не что иное, как её метрическое дополнение.

Метрическое дополнение решётки используется [11] для итеративного построения упаковок сфер в пространстве $\mathbb{R}^n$. Пусть $X \subseteq \mathbb{R}^n$ — решётка, а Λ — упаковка сфер в $\mathbb{R}^n$, соответствующая решётке X. *Слоем сфер* в пространстве $\mathbb{R}^{n+1}$ назовём множество сфер таких, что их центры лежат на гиперплоскости

$\mathbb{R}^n$ в узлах решётки X, а сечение данных сфер гиперплоскостью совпадает с упаковкой Λ. Построим плотную упаковку сфер в $\mathbb{R}^{n+1}$ путём складывания подобных слоёв друг на друга. Расположим соседние слои таким образом, чтобы множество центров X упаковки Λ одного слоя было расположено напротив подмножества точек $\widehat{X}$ другого слоя. При подобном расположении всех слоёв сфер друг относительно друга во многих случаях получается достаточно плотная упаковка в пространстве $\mathbb{R}^{n+1}$. В случае, если $\widehat{X}$ имеет существенно большую мощность, чем X, иногда таким способом возможно построить несколько неэквивалентных друг другу упаковок. Большое количество известных плотных (в том числе наиболее плотных) упаковок сфер построено при помощи данной итеративной конструкции из более простых упаковок меньших размерностей.

Метрическое дополнение решётки также рассматривалось при нахождении радиуса покрытия одной из наиболее известных решёток — решётки Лича Λ_{24} [1, 27, 28, 46, 51]. Данная решётка порождает наиболее плотную упаковку шаров [5, 6] в пространстве $\mathbb{R}^{24}$, а также имеет [38] наибольшее возможное в данном пространстве контактное число (максимальное количество шаров, одновременно соприкасающихся с шаром такого же размера).

Вскоре после открытия данной решётки Дж. Лич высказал гипотезу, что её радиус покрытия равен радиусу упаковки $e(\Lambda_{24})$, умноженному на $\sqrt{2}$. В 1982 году С. Нортон [37] доказал оценку $\rho(\Lambda_{24}) \leqslant 1.452\ldots \cdot e(\Lambda_{24})$, а чуть позже, в том же году, гипотеза была доказана Дж. Конвеем, Р. Паркером и Н. Слоэном в работе [10]. Доказательство заключается в исследовании метрического дополнения решётки: авторы установили, что существует 23 неэквивалентных класса глубоких дыр, и поставили в соответствие каждому классу одну из так называемых решёток Нимайера [36], радиус покрытия каждой из которых равен $\sqrt{2}$.

Нетрудно заметить, что точки метрического дополнения любого множества в евклидовом пространстве являются вершинами так называемых *областей Дирихле* (*областей диаграммы Вороного*) данного множества.

Задачи вычисления радиуса покрытия и плотной упаковки сфер активно изучаются также в пространстве двоичных векторов $\mathbb{F}_2^n$, снабжённом метрикой Хэмминга. *Двоичным кодом* называется произвольное подмножество пространства $\mathbb{F}_2^n$. Пусть $C \subseteq \mathbb{F}_2^n$ — двоичный код. *Кодовым расстоянием* d называется кратчайшее из расстояний между векторами кода C. *Радиусом упаковки* $e(C)$ кода $C \subseteq \mathbb{F}_2^n$ называется наибольшее число e такое, что сферы радиуса e с центрами в векторах кода C не пересекаются. Радиус упаковки кода $e(C)$ равен

$\lfloor \frac{d-1}{2} \rfloor$ и отражает количество ошибок, потенциально возникших при передаче кодированной информации, которые может исправить данный код. *Параметрами кода* называют тройку $(n,|C|,d)$, отражающую его длину, мощность и кодовое расстояние. Код C называется *линейным*, если он является линейным подпространством булева куба, т.е. если сумма любых двух векторов кода лежит в нём же. Для линейных кодов параметрами кода называют тройку $[n,k,d]$, где k обозначает размерность кода как линейного подпространства булева куба $\mathbb{F}_2^n$.

Минимизация мощности двоичного кода при заданном радиусе покрытия, как и двойственная к ней задача минимизации радиуса покрытия при заданной мощности, имеют разнообразные приложения как в теории кодирования информации, так и в других областях математики. В книге “Covering codes” Дж. Коэна и др. [9] приводятся оценки оптимальных параметров покрывающих двоичных кодов, а также обзор различных конструкций покрывающих кодов. Помимо этого, изучается радиус покрытия кодов из многих известных семейств, таких как коды Рида-Маллера, коды БЧХ, коды Рида-Соломона и др.

Метрическую регулярность можно рассматривать как одно из расширений понятия *совершенности* кода. Код $C \subseteq \mathbb{F}_2^n$ называется *совершенным*, если шары радиуса $e(C)$ покрывают всё пространство $\mathbb{F}_2^n$, то есть радиус покрытия кода равен радиусу упаковки. Легко видеть, что всякий совершенный код является метрически регулярным. Совершенные коды имеют наилучшие параметры для кодирования информации. В то же время, количество различных наборов параметров, которыми могут обладать нетривиальные совершенные коды, невелико, что было доказано в работах В. Зиновьева, В. Леонтьева [54] и А. Тиетвайнена [45]. Так, каждый нетривиальный двоичный совершенный код имеет параметры кода Хэмминга $[2^r - 1, 2^r - r - 1,3]$ [19, 31] или кода Голея $[23,12,7]$ [16, 31].

Одним из ослаблений совершенных кодов являются так называемые почти совершенные коды [13]. Код называется *почти совершенным*, если его мощность достигает модифицированной границы Джонсона [21]. К. Линдстрём в 1977 году установил, что все двоичные почти совершенные коды уже найдены, а всякий почти совершенный код над полем другого размера является совершенным [29]. Тем самым, все почти совершенные коды описаны в работе [13], а представленные в ней конструкции приводят к метрически регулярным кодам: тривиальные коды повторений, укороченные коды Хэмминга, коды Препарата и др.

Почти совершенные коды являются подмножеством полностью регулярных кодов [12, 44]. Одно из определений таких кодов [35] гласит, что код C называется *полностью регулярным*, если любой вектор $x \in C_i$ находится на расстоянии 1 от a_i векторов из множества C_{i-1} и от b_i векторов из множества C_{i+1}. Здесь $C_i = \{x \in \mathbb{F}_2^n \,|\, d(x,C) = i\}$ — множество векторов на расстоянии i от кода, а числа a_i, b_i зависят лишь от расстояния i, но не зависят от выбора кодового слова. Из этого определения легко следует, что всякий полностью регулярный код является метрически регулярным. Обратное в общем случае неверно — контрпримером является метрически регулярный код $\{(000),(011)\}$ в $\mathbb{F}_2^3$, не являющийся полностью регулярным. Обзор конструкций и свойств полностью регулярных кодов можно найти в работах [2, 41].

С другой стороны, почти совершенные коды содержатся во множестве *квази-совершенных* кодов [17, 52]. Код называется *квази-совершенным*, если его радиус покрытия на единицу больше радиуса упаковки. Класс квази-совершенных кодов достаточно велик, и в общем случае квази-совершенный код не является метрически регулярным: тривиальным контрпримером является код $\{(00),(01),(10)\}$ в $\mathbb{F}_2^2$. Изучаются также другие усиления квази-совершенных кодов — например, равномерно упакованные коды (включая равномерно упакованные коды в сильном и слабом смыслах) [4, 14, 43], некоторые из которых являются полностью регулярными, и, следовательно, метрически регулярными.

Булевой функцией f от m переменных называется произвольное отображение из $\mathbb{F}_2^m$ в $\mathbb{F}_2$. *Вектором значений* булевой функции называется двоичный вектор длины 2^m, содержащий значения данной функции на всех булевых векторах длины m, упорядоченных некоторым образом. Расстояние между булевыми функциями определяется как расстояние между их векторами значений. *Аффинной булевой функцией* от m переменных называется функция вида $a_1x_1 + a_2x_2 + \ldots + a_mx_m + c$, где $a_i, c \in \mathbb{F}_2$. Здесь и далее при проведении операций с булевыми векторами/функциями, знаком "+" обозначается сложение в поле $\mathbb{F}_2$ (по модулю 2). *Код Рида-Маллера порядка k от m переменных* [33] определяется как множество всех функций (либо их векторов значений), алгебраическая степень которых не превосходит k; в частности, множество аффинных булевых функций является кодом Рида-Маллера первого порядка. Код Рида-Маллера порядка k от m переменных имеет параметры $[2^m, \sum_{i=0}^{k} \binom{m}{i}, 2^{m-k}]$.

Задача исследования и классификации метрически регулярных множеств в булевом кубе была впервые поставлена Н. Токаревой [48, 49] при изучении

метрических свойств бент-функций [39]. Булева функция f от чётного числа переменных m называется *бент-функцией*, если она находится на максимальном возможном расстоянии $2^{m-1} - 2^{\frac{m}{2}-1}$ от множества аффинных функций. Иными словами, множество бент-функций — это метрическое дополнение множества аффинных функций. Бент-функции имеют разнообразные применения в криптографии, теории кодирования и комбинаторике [7,32,49]. В 2010 году Н. Токарева доказала, что множество аффинных функций является метрическим дополнением множества бент-функций [47, 48], и тем самым установила, что множества аффинных функций и бент-функций являются метрически регулярными.

Изучением метрических дополнений и метрически регулярных множеств занимаются как отечественные, так и зарубежные авторы. Так, в одной из своих работ [42], П. Станица, Т. Сасао и Дж. Батлер вводят понятие *множеств функций разбиения* и изучают метрические дополнения и метрическую регулярность таких множеств. Множество $\mathcal{S}$ булевых функций называется *множеством функций разбиения* относительно разбиения $\mathcal{U}$ пространства $\mathbb{F}_2^m$, если каждая функция из $\mathcal{S}$, будучи ограниченной на любой класс из разбиения $\mathcal{U}$, является постоянной (то есть все векторы класса отображаются либо в 0, либо в 1), и все функции, соответствующие каждой возможной комбинации значений на классах, включены в множество $\mathcal{S}$. Множества функций разбиения включают, например, множество симметрических функций, поворотно-симметрических (rotation symmetric) функций, анти-самодуальных функций и другие.

Следующая теорема является основным результатом их работы. Она описывает радиус покрытия и метрическое дополнение множества функций разбиения:

Теорема. *Рассмотрим множество функций разбиения $\mathcal{S}$. Обозначим через $\rho_{\mathcal{S}}$ радиус покрытия множества $\mathcal{S}$, а через $N_{\mathcal{S}}$ — количество булевых функций на расстоянии $\rho_{\mathcal{S}}$ от множества $\mathcal{S}$. Тогда,*

$$\rho_{\mathcal{S}} = \sum_{i=1}^{l} \lfloor k_i/2 \rfloor \text{ и } N_{\mathcal{S}} = \prod_{i=1}^{l} \frac{1}{2 - k_i \mod 2} \left(\binom{k_i}{\lfloor k_i/2 \rfloor} + \binom{k_i}{\lceil k_i/2 \rceil} \right),$$

где k_i — мощность i-го блока разбиения $\mathcal{U}$.

Доказательство теоремы конструктивно и явно описывает метрическое дополнение множества $\mathcal{S}$. Из этого описания без труда доказывается, что $\widehat{\widehat{\mathcal{S}}} = \mathcal{S}$, то есть любое множество функций разбиения метрически регулярно.

Затем авторы переходят к изучению множеств симметрических и поворотно-симметрических функций. Они вычисляют радиусы покрытия для обоих множеств, описывают множество максимально асимметрических функций (метрическое дополнение множества симметрических функций) и вычисляют количество таких функций. Авторы описывают весовое распределение максимально асимметрических функций и их алгебраические степени, а затем приводят классификацию всех булевых функций относительно расстояния до множества симметрических функций.

А. Куценко изучались метрические свойства двух подклассов бент-функций, называемых *самодуальными* и *анти-самодуальными* бент-функциями. В работе [26] автор доказывает, что множество самодуальных бент-функций является метрическим дополнением множества анти-самодуальных бент-функций и наборот, устанавливая тем самым метрическую регулярность обоих множеств. Другие метрические свойства бент-функций (например, свойства графа минимальных расстояний между бент-функциями) также изучались Н. Коломейцем в работах [22–25].

Целью данной работы является изучение свойства метрической регулярности и связанных понятий:

1. Описание конструкций метрически регулярных множеств; оценка количества метрически регулярных множеств.
2. Получение оценок мощности метрически регулярных множеств и их метрических дополнений.
3. Изучение свойств и вида метрических дополнений линейных кодов; изучение метрической регулярности линейных кодов.

Научная новизна и значимость работы: Все результаты, представленные в работе, являются новыми. Работа носит теоретический характер. Полученные конструкции и теоретические результаты могут быть применены при дальнейших исследованиях метрически регулярных множеств, а также при исследовании свойств бент-функций и различных линейных кодов.

Методология и методы исследования. В работе применялись методы комбинаторики, дискретного анализа и теории кодирования. Для выдвижения гипотез и проверки некоторых частных случаев были использованы компьютерные эксперименты.

Основные положения, выносимые на защиту:

1. Представлены различные конструкции метрически регулярных множеств: доказана сходимость операции взятия метрического дополнения, получены итеративные конструкции строго метрически регулярных множеств и найдено число множеств, полученных при помощи данных конструкций.
2. Показано, что задача поиска наибольшего по мощности метрически регулярного множества сводится к задаче поиска наименьшего покрывающего кода радиуса 1.
3. Получена нижняя оценка суммы мощностей метрически регулярного множества и его метрического дополнения, зависящая от радиуса покрытия множества. Представлены конструкции семейств метрически регулярных множеств большой мощности, получена нижняя оценка мощности наибольшего метрически регулярного множества при заданном радиусе покрытия.
4. Получена общая характеризация первого и второго метрических дополнений линейных кодов.
5. Доказана метрическая регулярность кодов Рида-Маллера $\mathcal{RM}(k,m)$ для $k = 0$, $k \geqslant m - 3$, а также кодов $\mathcal{RM}(1,5)$ и $\mathcal{RM}(2,6)$. Описаны метрические дополнения всех перечисленных кодов, за исключением кода $\mathcal{RM}(2,6)$.

Апробация работы. Основные результаты работы докладывались на научных семинарах Института математики им. С.Л. Соболева СО РАН: «Криптография и криптоанализ», «Дискретный анализ» и «Теория кодирования»; на научном семинаре исследовательской группы Selmer Center (г. Берген, Норвегия, 2019, 2020); а также на международной конференции «Boolean Functions and their Applications (BFA)» (2019, 2020), на всероссийской конференции «Сибирская научная школа-семинар с международным участием “Компьютерная безопасность и криптография”» Sibecrypt (2015, 2017, 2018) и на Международной студенческой конференции МНСК (2015-2018).

Публикации. Основные результаты по теме диссертации изложены в работах [55–64], из них 5 статей опубликованы в журналах из списка ВАК.

Объем и структура работы. Диссертация состоит из введения, 5 глав, заключения и приложения. Полный объём диссертации составляет 93 страницы, включая 1 рисунок и 5 таблиц. Список литературы содержит 64 наименования.

Приведём структуру данной работы.

В **первой главе** приводятся необходимые определения. Вводятся понятия метрического дополнения множества, метрической регулярности и строгой метрической регулярности. Приводятся примеры, иллюстрирующие введённые понятия.

Во **второй главе** предложены различные конструкции метрически регулярных множеств. Напомним, что метрическое дополнение множества X обозначается $\widehat{X}$.

Утверждение 2.1. *Пусть X — произвольное подмножество пространства $\mathbb{F}_2^n$. Рассмотрим следующую последовательность множеств: $X_0 = X$, $X_{k+1} = \widehat{X}_k$ для $k \geqslant 0$. Тогда существует число $M \leqslant n$ такое, что для любого $m \geqslant M$ множество X_m является метрически регулярным.*

Данное утверждение показывает, что из произвольного подмножества булева куба можно построить метрически регулярное множество, причём не более, чем за n операций нахождения метрического дополнения.

Представлены итеративные конструкции строго метрически регулярных множеств. Пусть $X \subseteq \mathbb{F}_2^n$ — произвольное подмножество булева куба. Множество X называется *строго метрически регулярным*, если сумма расстояний $d(y,X) + d(y,\widehat{X})$ постоянна для всех векторов $y \in \mathbb{F}_2^n$ и равна радиусу покрытия множества X. *Послойным представлением* пространства $\mathbb{F}_2^n$ относительно множества X называется множество слоёв, определённых следующим образом:

$$X_k := \{y \in \mathbb{F}_2^n \mid d(y,X) = k\}, k = 0,1,\ldots,r.$$

Доказана следующая теорема.

Теорема 2.4. *Пусть $A \subseteq \mathbb{F}_2^n$ — строго метрически регулярное множество с радиусом покрытия $r > 0$. Пусть $0 \leqslant i_1 < i_2 < \ldots < i_{s-1} < i_s \leqslant r$ — некоторая последовательность индексов. Тогда объединение $C = \bigcup\limits_{k=1}^{s} A_{i_k}$ является строго метрически регулярным множеством тогда и только тогда, когда существует число $q > 0$ такое, что выполняются следующие условия:*

1. *для любого $k \in \{1,\ldots,s-1\}$ разность $i_{k+1} - i_k$ равна 1, $2q$ или $2q+1$;*
2. *для любого $k \in \{2,\ldots,s-1\}$ как минимум одна из разностей $i_{k+1} - i_k, i_k - i_{k-1}$ больше единицы;*
3. *i_1 равно либо q, либо 0, и если $i_1 = 0$, а i_2 существует, то $i_2 - i_1 = 2q$ или $2q+1$;*

4. i_s *равно либо* $r-q$, *либо* r, *и если* $i_s = r$, *а* i_{s-1} *существует, то* $i_s - i_{s-1} = 2q$ *или* $2q+1$;

При выполнении указанных условий число q *является радиусом покрытия множества* C.

Затем в теореме 2.5 подсчитывается количество различных строго метрически регулярных множеств, которые можно получить при помощи данной конструкции.

Третья глава посвящена оценкам мощностей метрически регулярных множеств. Показано, что всякое метрически регулярное множество вкладывается в метрически регулярное множество с радиусом покрытия 1. Исходя из этого факта доказывается, что задача нахождения наибольшего метрически регулярного множества сводится к задаче нахождения наименьшего покрывающего кода радиуса 1.

Получена нижняя оценка суммы мощностей метрически регулярного множества и его метрического дополнения при фиксированном радиусе покрытия:

Теорема 3.4. *Пусть* $A \subseteq \mathbb{F}_2^n$ *— метрически регулярное множество с радиусом покрытия* r. *Тогда*

$$|A| + |\widehat{A}| \geqslant \frac{2^{n+1}}{1 + \sum\limits_{k=0}^{r-1} \binom{n}{k}}.$$

При помощи конструкций из главы 2 строятся семейства больших строго метрически регулярных множеств, размер которых позволяет оценить мощность наибольшего метрически регулярного множества в булевом кубе заданной размерности с заданным радиусом покрытия.

Теорема 3.6. *Пусть* A *— наибольшее метрически регулярное множество с радиусом покрытия* r *в булевом кубе размерности* n *(*$n \geqslant 2r$*), и пусть* s *— остаток от деления* $n+1$ *на* $2r+1$. *Тогда*

$$|A| \geqslant \max\left\{2^n\left(\frac{2}{2r+1} - \frac{2}{\sqrt{n-s+1}}\right), 2^{n-2r}\binom{2r}{r}\right\}. \qquad (1)$$

В **четвёртой главе** рассматриваются свойства метрических дополнений линейных подпространств (линейных кодов) булева куба. Известно, что радиус

покрытия линейного подпространства размерности k в булевом кубе размерности n не превышает $n-k$. Рассматривается канонический базис подпространства и с его помощью доказываются следующие утверждения:

Теорема 4.4. *Пусть L — линейное подпространство размерности k. Равенство $\rho(L) = n - k$ достигается тогда и только тогда, когда веса всех векторов канонического базиса подпространства L не превосходят 2. Метрическое дополнение $\widehat{L}$ состоит в этом случае из одного смежного класса пространства L.*

Теорема 4.5. *Пусть $L \subseteq \mathbb{F}_2^n$ — линейное подпространство размерности k, $wt(e_i^*) \leqslant 3$ для всех векторов e_i^* из канонического базиса и существует индекс j такой, что $wt(e_j^*) = 3$. Тогда $\rho(L) = n - k - 1$ тогда и только тогда, когда $supp(e_i^*) \cap supp(e_j^*) \neq \varnothing$ для всех i,j таких, что $wt(e_i^*) = wt(e_j^*) = 3$. При этом метрическое дополнение $\widehat{L}$ состоит из одного, двух или трёх смежных классов L, в зависимости от мощности пересечения носителей всех векторов канонического базиса веса 3.*

Приводится характеристика второго метрического дополнения линейного подпространства булева куба.

Теорема 4.7. *Пусть $L \subseteq \mathbb{F}_2^n$ — линейное подпространство. Тогда $x \in \widehat{\widehat{L}}$ тогда и только тогда, когда $\widehat{L}$ инвариантно относительно сдвига на x, т.е. $\widehat{L} = x + \widehat{L}$.*

В **пятой главе** рассматривается известное семейство линейных кодов — коды Рида-Маллера. Доказывается метрическая регулярность кодов Рида-Маллера $\mathcal{RM}(k,m)$ для $k = 0$, $k \geqslant m-2$. Затем, опираясь на метод нахождения радиуса покрытия кода $\mathcal{RM}(m-3,m)$, описанный в книге [9], описывается метрическое дополнение и устанавливается метрическая регулярность кодов Рида-Маллера порядка $m-3$ от m переменных. Также в данной главе доказывается метрическая регулярность кодов $\mathcal{RM}(1,5)$ и $\mathcal{RM}(2,6)$. В совокупности с результатом Н. Токаревой о метрической регулярности множества аффинных функций, тем самым устанавливается метрическая регулярность всех кодов Рида-Маллера, радиус покрытия которых известен, за исключением двух: $\mathcal{RM}(1,7)$ и $\mathcal{RM}(2,7)$. Высказывается гипотеза о метрической регулярности всех кодов Рида-Маллера.

В **приложении А** содержатся выкладки и таблицы, необходимые для доказательства леммы 5.17 из раздела 5.8 главы 5.

Глава 1. Определения, обозначения и примеры

В данной главе вводятся основные определения и приводятся простейшие примеры метрических дополнений и метрически регулярных множеств в булевом кубе.

1.1 Определения

Пусть $\mathbb{F}_2^n = \{0,1\}^n$ — множество двоичных наборов длины n, рассматриваемое как векторное пространство над полем $\mathbb{F}_2$. В данной работе множество $\mathbb{F}_2^n$ будем часто называть *булевым кубом* размерности n. *Расстоянием Хэмминга* между двумя двоичными векторами называется количество координат, в которых они различаются. *Весом Хэмминга* $wt(\cdot)$ двоичного вектора называется количество его ненулевых координат. При работе с булевыми векторами и функциями обычным знаком сложения "+" будет обозначаться сложение по модулю 2.

Пусть $X \subseteq \mathbb{F}_2^n$ — непустое подмножество булева куба (всюду в дальнейшем будут рассматриваться исключительно непустые подмножества), а $y \in \mathbb{F}_2^n$ — некоторый вектор. Расстояние $d(y,X)$ от вектора y до множества X определяется как $\min\limits_{x \in X} d(y,x)$. *Радиус покрытия* множества X определяется следующим образом:

$$\rho(X) = \max_{z \in \mathbb{F}_2^n} d(z,X).$$

Множество X, радиус покрытия которого равен r, называют *покрывающим кодом* [9] радиуса r.

Рассмотрим множество

$$\widehat{X} = \{y \in \mathbb{F}_2^n : d(y,X) = \rho(X)\}$$

всех векторов булева куба, находящихся на наибольшем возможном расстоянии от множества X. Данное множество назовём *метрическим дополнением* [55] множества X. Если $\widehat{\widehat{X}} = X$, то множество X называют *метрически регулярным* [48].

Заметим, что метрически регулярные множества всегда существуют парами, т.е. если X — метрически регулярное множество, то его метрическое дополнение $\widehat{X}$ также является метрически регулярным множеством.

Пусть множество $X \subseteq \mathbb{F}_2^n$ имеет радиус покрытия r. Назовём множество X *строго метрически регулярным*, если для любого вектора $y \in \mathbb{F}_2^n$ выполняется

$$d(y,X) + d(y,\widehat{X}) = r.$$

Другими словами, любой вектор пространства находится на некотором кратчайшем пути между множествами X и $\widehat{X}$. Легко видеть, что всякое строго метрически регулярное множество является метрически регулярным: из приведённого равенства немедленно следует, что радиус покрытия множества $\widehat{X}$ не превышает r, а условие $d(y,\widehat{X}) = r$ эквивалентно условию $d(y,X) = 0$, то есть $y \in X$.

Однако не все метрически регулярные множества являются строго метрически регулярными. В качестве одной из задач на международной олимпиаде по криптографии NSUCRYPTO 2016 [50] участникам предлагалась задача нахождения метрически регулярного подмножества булева куба, не являющегося строго метрически регулярным (либо доказательства, что такого множества не существует), и несколько участников нашли различные решения. Наименьший известный пример такого множества содержится в булевом кубе размерности 7.

Послойным представлением пространства $\mathbb{F}_2^n$ относительно множества X называется множество слоёв, определённых следующим образом:

$$X_k := \{y \in \mathbb{F}_2^n \mid d(y,X) = k\}, k = 0,1,\ldots,r,$$

где r — радиус покрытия множества X. Послойное представление позволяет определить строго метрически регулярные множества следующим образом [57]:

Определение 1. Множество X является строго метрически регулярным тогда и только тогда, когда для любого $0 \leqslant k \leqslant r$ имеет место $X_k = \widehat{X}_{r-k}$, где r — радиус покрытия обоих множеств.

Множество $C \subseteq \mathbb{F}_2^n$ называется *полностью регулярным кодом*, если любой вектор $x \in C_i$ находится на расстоянии 1 от a_i векторов из множества C_{i-1} и от b_i векторов из множества C_{i+1}, где числа a_i, b_i зависят лишь от расстояния i, но не зависят от выбора кодового слова. Поскольку для каждого вектора из множества

C_i существуют векторы как из множества C_{i-1}, так и из множества C_{i+1}, находящиеся на расстоянии 1 от данного вектора (если соответствующие множества определены), то всякий вектор находится на кратчайшем пути между множествами C и $\widehat{C}$. Тем самым, всякий полностью регулярный код строго метрически регулярен. Обратное в общем случае неверно — контрпримером является строго метрически регулярное множество $\{(000),(011)\}$ в $\mathbb{F}_2^3$, не являющееся полностью регулярным кодом.

Булевой функцией f от m переменных называется произвольное отображение из $\mathbb{F}_2^m$ в $\mathbb{F}_2$. *Вектором значений* булевой функции называется двоичный вектор длины 2^m, содержащий значения данной функции на всех булевых векторах длины m, упорядоченных некоторым образом. Расстояние между булевыми функциями определяется как расстояние между соответствующими векторами значений. Представление булевой функции f в виде

$$f(x_1,\dots,x_m) = a_0 + \sum_{k=1}^{m} \sum_{1\leqslant i_1<\dots<i_k\leqslant m} a_{i_1\dots i_k} x_{i_1}\dots x_{i_k},\ \text{где } a_0, a_{i_1\dots i_k} \in \mathbb{F}_2$$

называется *алгебраической нормальной формой* (*АНФ*) или *полиномом Жегалкина* функции f. Член вида $x_{i_1}\dots x_{i_k}$ называется *мономом степени* k, числа $a_{i_1\dots i_k}, a_0$ — *коэффициентами* при мономах. *Степенью* $\deg f$ функции f называется длина монома наибольшей степени среди таких мономов, коэффициент при которых отличен от нуля. Степень тождественно нулевой функции полагается равной 0. Известно, что любая булева функция имеет единственное представление в виде АНФ.

Аффинной булевой функцией называется булева функция, степень которой не превышает 1. Булева функция f от чётного числа переменных m называется *бент-функцией*, если она находится на максимально возможном расстоянии от множества аффинных функций, то есть наиболее сильно отличается от любой линейной/аффинной функции. Если рассматривать булевы функции как векторы значений, то множество бент-функций можно определить как метрическое дополнение множества аффинных функций.

Непустое множество $L \subseteq \mathbb{F}_2^n$ называется *линейным подпространством (линейным кодом)* пространства $\mathbb{F}_2^n$, если для любых $a, b \in L$ верно $a + b \in L$. Обозначим через $y + X$, где $y \in \mathbb{F}_2^n$ и $X \subseteq \mathbb{F}_2^n$, *сдвиг* множества X, а именно $y + X = \{y + x \mid x \in X\}$. Сдвиг линейного подпространства называется *аффинным подпространством* (либо *смежным классом* подпространства).

1.2 Примеры

Рассмотрим несколько простых примеров метрических дополнений и метрически регулярных множеств в булевом кубе. Пусть x — произвольный вектор из пространства $\mathbb{F}_2^n$.

1. Пусть $X = \{x\}$ — множество, состоящее из одного вектора. Его радиус покрытия равен n, а его метрическое дополнение $\widehat{X} = \{x + \mathbf{1}\}$ состоит лишь из одного "противоположного" вектора (здесь $\mathbf{1}$ обозначает вектор, состоящий из единиц). Отсюда следует, что $\widehat{\widehat{X}} = X$, то есть X — метрически регулярное множество. Более того, поскольку любой вектор $x \in \mathbb{F}_2^n$, находящийся на расстоянии k от множества X, находится на расстоянии $(n-k)$ от множества $\widehat{X}$, множество X является также строго метрически регулярным;
2. Рассмотрим *шар* радиуса r с центром в x, т.е. $X = \{y \in \mathbb{F}_2^n | d(x,y) \leqslant r\}$. Вектор $x + \mathbf{1}$ находится на расстоянии $n - r$ от множества X, в то время как любой другой вектор находится на меньшем расстоянии. Следовательно, радиус покрытия множества X равен $n - r$, а его метрическое дополнение также состоит из одного вектора: $\widehat{X} = \{x + \mathbf{1}\}$. Тогда $\widehat{\widehat{X}} = \{x\}$, откуда следует, что, за исключением случая $r = 0$, шар радиуса r не является метрически регулярным множеством;
3. *Гранью* размерности $(n-k)$ в пространстве $\mathbb{F}_2^n$ называется множество всех векторов с фиксированными значениями в выбранных k координатах. Пусть X — $(n-k)$-мерная грань со значениями $a_1, a_2, \ldots, a_k$ в координатах $1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant n$ соответственно. Для любого вектора $y \in \mathbb{F}_2^n$ найдётся вектор x из грани, совпадающий с y в координатах $\{1,...,n\} \backslash \{i_r : r = 1, \ldots, k\}$, поэтому расстояние от y до X определяется только теми координатами вектора y, которые в грани фиксированы. Отсюда следует, что $\rho(X) = k$, а $\widehat{X}$ — это $(n-k)$-мерная грань с противоположными значениями, фиксированными в тех же координатах, что и у грани X. Как и в первом примере, легко видеть, что X — строго метрически регулярное множество;
4. Рассмотрим значительно менее тривиальный пример. Пусть $\mathcal{A}_m \subseteq \mathbb{F}_2^{2^m}$ — $(m+1)$-мерное линейное подпространство всех аффинных булевых функций от m переменных, m чётно. По определению, $\widehat{\mathcal{A}_m} = \mathcal{B}_m$ —

множество *бент-функций* [39] от n переменных. В статье [47] доказано, что $\widehat{\mathcal{B}_m} = \mathcal{A}_m$, то есть подпространство аффинных функций метрически регулярно. В то же время, подпространство аффинных функций в общем случае не является строго метрически регулярным. Например, уже при $m = 4$ функция x_1x_2 находится на расстоянии 4 как от множества аффинных функций, так и от множества бент-функций, при том что радиус покрытия обоих множеств равен 6.

Глава 2. Конструкции метрически регулярных множеств

В данной главе предложены различные итеративные конструкции метрически регулярных множеств. Доказывается, что последовательное применение операции нахождения метрического дополнения множества стабилизируется на паре метрически регулярных множеств за ограниченное число шагов. Получены итеративные конструкции строго метрически регулярных множеств, основывающиеся на паре данных строго метрически регулярных множеств. Все утверждения, представленные в данной главе, являются новыми. Результаты главы опубликованы в работах [56, 57, 62].

2.1 Сходимость операции взятия метрического дополнения

Примеры метрических дополнений из главы 1 показывают, что не всякое подмножество булева куба является метрически регулярным. Отсюда следует, что, последовательно применяя операцию взятия метрического дополнения множества много раз, мы, возможно, будем получать новые множества. В силу конечности пространства очевидно, что этот процесс рано или поздно стабилизируется. Утверждение 2.1 описывает “скорость” такой сходимости.

Утверждение 2.1 (см. [56]). *Пусть X — произвольное подмножество $\mathbb{F}_2^n$. Рассмотрим следующую последовательность множеств: $X_0 = X$, $X_{k+1} = \widehat{X}_k$ для $k \geqslant 0$. Тогда существует число $M \leqslant n$ такое, что для любого $m \geqslant M$ множество X_m является метрически регулярным.*

Доказательство. Если $\rho(X) = 0$, то $X = \mathbb{F}_2^n$ и утверждение очевидно. Пусть $\rho(X) > 0$. Очевидно, что всякая точка множества X находится на расстоянии не меньшем, чем $\rho(X)$, от множества $\widehat{X}$. Значит, $\rho(\widehat{X}) \geqslant \rho(X)$, и следовательно,

$$\rho(X_0) \leqslant \rho(X_1) \leqslant \ldots \leqslant \rho(X_k) \leqslant \ldots. \tag{2.1}$$

Поскольку радиус покрытия, как и расстояние, может принимать лишь ограниченное число значений, то существует такое $N \leqslant n-1$, что $\rho(X_N) = \rho(X_{N+1})$. Выберем наименьшее число N с этим свойством. Тогда, как было упомянуто в

начале доказательства, точки множества X_N находятся на расстоянии не меньшем, чем $\rho(X_N)$, от множества X_{N+1}. Но $\rho(X_{N+1}) = \rho(X_N)$, а значит, все точки X_N находятся на расстоянии в точности $\rho(X_N)$ от множества X_{N+1}, откуда следует, что $X_N \subseteq \widehat{X}_{N+1} = X_{N+2}$.

Заметим, что из $X_N \subseteq X_{N+2}$ следует $\rho(X_{N+2}) \leqslant \rho(X_N)$. Учитывая серию неравенств 2.1, мы получаем, что $\rho(X_{N+2})$ в точности равно $\rho(X_N)$. При помощи аналогичных рассуждений легко показать, что $\rho(X_{N+k})$ равно $\rho(X_N)$ для всякого $k > 0$. Таким образом, если $\rho(X_{N+1}) = \rho(X_N)$ для некоторого N, то $\rho(X_{N+k}) = \rho(X_N)$ для всех $k > 0$.

Поскольку $\rho(X_{N+k}) = \rho(X_N)$ для всех $k \geqslant 0$, и, как было показано выше, из $\rho(X_N) = \rho(X_{N+1})$ следует $X_N \subseteq X_{N+2}$, то $X_{N+1} \subseteq X_{N+3}$. Заметим следующий тривиальный факт: если A, B — два подмножества булева куба такие, что $A \subseteq B$ и $\rho(A) = \rho(B)$, то $\widehat{B} \subseteq \widehat{A}$. Отсюда следует, что $X_{N+3} = \widehat{X}_{N+2} \subseteq \widehat{X}_N = X_{N+1}$. Тем самым, показаны оба включения, а значит, X_{N+1} совпадает с X_{N+3}, и множество X_{N+1} является метрически регулярным. Аналогичными рассуждениями легко показать, что всякое X_m при $m \geqslant N+1$ является метрически регулярным. Число $M := N+1$ является искомой константой из условия утверждения. □

Утверждение 2.1 показывает, что, взяв произвольное подмножество булева куба и последовательно применяя операцию взятия метрического дополнения к нему, а затем к результату предыдущей операции, мы сойдёмся (не более, чем за n шагов) к метрически регулярному множеству.

Используя данное утверждение, множество всех подмножеств $\mathcal{F}(\mathbb{F}_2^n)$ булева куба можно разбить на классы эквивалентности, положив два множества X,$Y \subseteq \mathbb{F}_2^n$ эквивалентными тогда и только тогда, когда пара метрически регулярных множеств A,$\widehat{A}$, получаемых из множества X последовательным взятием метрического дополнения, совпадает с парой метрически регулярных множеств B,$\widehat{B}$, получаемых из множества Y (с точностью до порядка множеств в паре).

Утверждение 2.1 также имеет приложения при проведении вычислительных экспериментов, связанных с метрически регулярными множествами, с ипользованием ЭВМ.

2.2 Итеративные конструкции строго метрически регулярных множеств

Строгая метрическая регулярность множеств позволяет строить новые строго метрически регулярные множества на основе существующих. Следующая лемма необходима для доказательств основных конструкций данного раздела. Напомним, что *послойным представлением* пространства относительно множества A называется набор множеств $A_k = \{x \in \mathbb{F}_2^n \mid d(x,A) = k\}$, $0 \leqslant k \leqslant \rho(A)$.

Лемма 2.2 (см. [57]). *Пусть $A \subseteq \mathbb{F}_2^n$ — строго метрически регулярное множество с радиусом покрытия r. Тогда для любых $i,j \in \{0,1,\ldots,r\}$ и для любого вектора $x \in A_i$ имеет место*

$$d(x,A_j) = |i-j|.$$

Доказательство. Если $i = j$, то утверждение очевидно.

Пусть $i > j$. По определению послойного представления пространства, $d(x,A) = i$, а значит, существует некоторый кратчайший путь длины i от множества A до вектора x. Обозначим его вершины через $x_0, x_1, \ldots, x_i = x$, где $x_0 \in A$. Поскольку последовательные вершины в пути различаются лишь в одной координате, и векторы из множеств A_s и A_t могут встречаться в пути подряд только если $|s-t| \leqslant 1$, то с необходимостью $x_k \in A_k$ для любого $k = 0,\ldots,i$. Значит, вектор x_j из данного пути принадлежит слою A_j и находится на расстоянии $i-j$ от вектора x, и следовательно, $d(x,A_j) \leqslant i-j$. Расстояние не может быть меньше $i-j$, поскольку в таком случае расстояние $d(x,A)$ было бы меньше i, что противоречит условию леммы. Таким образом, $d(x,A_j) = i-j$.

Если $i < j$, то, используя альтернативное определение 1 строго метрически регулярного множества из первой главы, мы можем заменить A_i на $\widehat{A}_{r-i}$, A_j на $\widehat{A}_{r-j}$ и использовать $\widehat{A}$ вместо A в доказательстве предыдущего случая. □

Из леммы 2.2 следует, что для любых $i,j \in \{0,1,\ldots,r\}$, все векторы из множества A_i находятся на расстоянии $|i-j|$ от множества A_j и наоборот. Данный факт используется для существенного облегчения проведения доказательств нижеследующих теорем, и в дальнейшем в данном разделе мы будем ссылаться на него в следующей формулировке: “расстояние между слоями A_i и A_j равно $|i-j|$”.

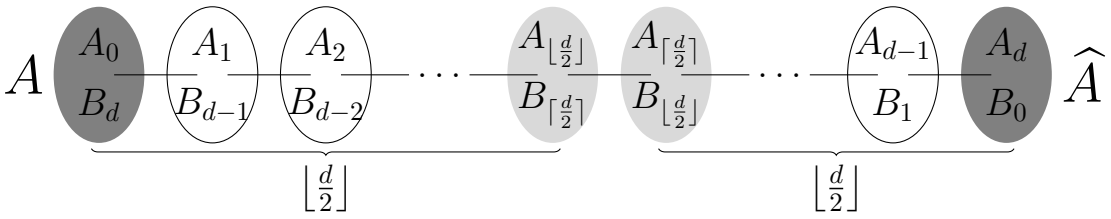

Рисунок 2.1 — Послойное представление пространства. Множество $C = A \cup \widehat{A}$ из теоремы 2.3 окрашено тёмно-серым, его метрическое дополнение в центре — светло-серым.

Рассмотрим теперь несколько способов построения новых строго метрически регулярных множеств с использованем уже имеющихся.

Теорема 2.3 (см. [57]). *Пусть $A \subseteq \mathbb{F}_2^n$ — строго метрически регулярное множество с радиусом покрытия r. Тогда множество $C = A \cup \widehat{A}$ является строго метрически регулярным с радиусом покрытия $\lfloor \frac{r}{2} \rfloor$.*

Доказательство. Поскольку $\widehat{A} = A_r$, множество C является объединением множеств A_0 и A_r. По лемме 2.2, все векторы множества A_k находятся на расстоянии k от множества A_0 и на расстоянии $r - k$ от множества A_r. Таким образом, $d(A_k,C) = \min\{k,r-k\}$. Максимум этого значения достигается при k равном $\lfloor \frac{r}{2} \rfloor$ и $\lceil \frac{r}{2} \rceil$, поэтому $\widehat{C} = A_{\lceil \frac{r}{2} \rceil} \cup A_{\lfloor \frac{r}{2} \rfloor}$, а радиус покрытия C равен $\lfloor \frac{r}{2} \rfloor$.

Вновь используя лемму 2.2, нетрудно заметить, что множества A_0 и A_r являются наиболее удалёнными от множества $\widehat{C}$. Значит $\widehat{\widehat{C}} = A_0 \cup A_r = C$, то есть множество C является метрически регулярным. Поскольку для любого вектора $x \in A_k$ выполняется

$$d(x,C) + d(x,\widehat{C}) = \min\{k,r-k\} + \min\left\{\left|k - \left\lceil \frac{r}{2} \right\rceil\right|, \left|k - \left\lfloor \frac{r}{2} \right\rfloor\right|\right\} = \left\lfloor \frac{r}{2} \right\rfloor,$$

то C — строго метрически регулярное множество. □

Теорема 2.3 обобщается на случай объединения большего количества слоёв. Поскольку (по лемме 2.2) расстояние между слоями A_i и A_j равно $|i-j|$, почти всюду в нижеследующем доказательстве разница индексов отражает расстояние между соответствующими слоями в послойном представлении пространства относительно множества A.

Теорема 2.4 (см. [57]). *Пусть $A \subseteq \mathbb{F}_2^n$ — строго метрически регулярное множество с радиусом покрытия $r > 0$ (случай $r = 0$ тривиален). Пусть $0 \leqslant i_1 < i_2 < \ldots < i_{s-1} < i_s \leqslant r$ — некоторая последовательность индексов. Тогда*

объединение $C = \bigcup_{k=1}^{s} A_{i_k}$ *является строго метрически регулярным множеством тогда и только тогда, когда существует число* $q > 0$ *такое, что выполняются следующие условия:*

1. *для любого* $k \in \{1, \ldots, s-1\}$ *разность* $i_{k+1} - i_k$ *равна* 1, $2q$ *или* $2q+1$*;*
2. *для любого* $k \in \{2, \ldots, s-1\}$ *как минимум одна из разностей* $i_{k+1} - i_k, i_k - i_{k-1}$ *больше единицы;*
3. i_1 *равно либо* q*, либо* 0*, и если* $i_1 = 0$*, а* i_2 *существует, то* $i_2 - i_1 = 2q$ *или* $2q+1$*;*
4. i_s *равно либо* $r-q$*, либо* r*, и если* $i_s = r$*, а* i_{s-1} *существует, то* $i_s - i_{s-1} = 2q$ *или* $2q+1$*;*

При выполнении указанных условий число q *является радиусом покрытия множества* C*.*

Доказательство. Прежде, чем начать более формальное доказательство, рассмотрим перечисленные условия.

Условие 1 утверждает, что любые два слоя, идущие друг за другом в последовательности, находятся на расстоянии 1, $2q$ или $2q+1$ друг от друга.

Условие 2 утверждает, что не существует трёх последовательных слоёв таких, что каждый последующий находится на расстоянии 1 от предыдущего. Другими словами, никакой слой из последовательности не может быть “зажат” между следующим и предыдущим слоями последовательности.

Условие 3 утверждает, что первый слой в последовательности является либо нулевым слоем (множество A), либо q-ым, и в первом случае он не может быть “прижат” вторым слоем последовательности. Четвёртое условие симметрично третьему.

$\Longrightarrow$

Пусть объединение C является метрически регулярным множеством. Обозначим его радиус покрытия через q. Докажем, что все четыре условия, перечисленные в утверждении теоремы, выполняются.

Предположим, что не выполняется первое условие. Это значит, что существует число k такое, что $i_{k+1} - i_k \neq 2q, 2q+1$ и $i_{k+1} - i_k > 1$. Если $i_{k+1} - i_k > 2q+1$, то легко проверить, что множество A_{i_k+q+1} находится на расстоянии как минимум $q+1$ как от A_{i_k}, так и от $A_{i_{k+1}}$ (и ещё дальше от всех других слоёв, составляющих C), а значит радиус покрытия C превышает q, противоречие.

Если $i_{k+1}-i_k < 2q$, то все множества $A_{i_k+1}, \ldots, A_{i_{k+1}-1}$ будут на расстоянии меньшем, чем q, либо от слоя A_{i_k}, либо от $A_{i_{k+1}}$. Это означает, что никакие слои между A_{i_k} и $A_{i_{k+1}}$ не содержатся в метрическом дополнении множества C. Таким образом, лишь векторы из слоёв с индексами, меньшими i_k или большими i_{k+1}, могут содержаться в $\widehat{C}$. Но это означает, что все слои $A_{i_k+1}, \ldots, A_{i_{k+1}-1}$ находятся дальше от $\widehat{C}$ чем слои A_{i_k} и $A_{i_{k+1}}$, и, следовательно, A_{i_k} и $A_{i_{k+1}}$ не могут содержаться в $\widehat{\widehat{C}}$. Это противоречит метрической регулярности множества C. Тем самым, условие 1 выполняется.

Предположим, что не выполняется условие 2, то есть существует число k такое, что $(i_{k+1} - i_k) = (i_k - i_{k-1}) = 1$. Таким образом, три последовательных (в послойном представлении) слоя с индексами i_{k-1},i_k,i_{k+1} содержатся в C. Но тогда слой A_{i_k} находится дальше от $\widehat{C}$, чем слои $A_{i_{k-1}}$ и $A_{i_{k+1}}$, поскольку он "зажат" между ними. Следовательно, данные два слоя $A_{i_{k-1}}$ и $A_{i_{k+1}}$ не могут содержаться в $\widehat{\widehat{C}}$, что противоречит метрической регулярности C. Условие 2 выполняется.

Рассмотрим условие 3. Предположим, что i_1 больше q. Тогда расстояние от A до A_{i_1} будет превосходить радиус покрытия C, противоречие. Пусть $0 < i_1 < q$. В этом случае никакие из множеств $A_0, A_1, \ldots, A_{i_1-1}$ не могут содержаться в $\widehat{C}$ (поскольку они слишком близки к A_{i_1}), и все они будут дальше от $\widehat{C}$, чем A_{i_1}, что противоречит метрической регулярности C. Следовательно, i_1 равно либо 0, либо q. Если i_1 равно 0, но $i_2 - i_1 = 1$, то вновь A_{i_1} будет дальше от $\widehat{C}$, чем A_{i_2}, что противоречит метрической регулярности C. Условие 3 доказано.

Заметим, что условие 4 аналогично условию 3 и может быть доказано теми же рассуждениями с другими индексами.

$\Longleftarrow$

Пусть существует число q такое, что все четыре условия выполняются. Найдём метрическое дополнение множества $C = \bigcup\limits_{k=1}^{s} A_{i_k}$. Поскольку C состоит целиком из полных слоёв, то из леммы 2.2 следует, что $\widehat{C}$ также состоит из полных слоёв. Очевидно, кандидатами на наиболее удалённые от C слои являются A_0, A_r и средние слои между A_{i_k} и $A_{i_{k+1}}$ для всех k.

Рассмотрим слои между A_{i_k} и $A_{i_{k+1}}$. В силу условия 1, между этими слоями либо нет векторов (если $i_{k+1} - i_k = 1$), либо (если $i_{k+1} - i_k = 2q$ или $2q + 1$) множества A_{i_k+q} и $A_{i_{k+1}-q}$ находятся на расстоянии q от C, а все другие слои между A_{i_k} и $A_{i_{k+1}}$ находятся на меньшем расстоянии.

Из условий 3 и 4 следует, что A_0 и A_r либо лежат в C, либо находятся на расстоянии q от него (не обязательно одновременно).

Также из условий 3 и 4 мы видим, что слои на расстоянии q от множества C существуют: если $i_1 = q$, то таким слоем является A_0, если $i_1 = 0$ и $s > 1$, то существуют средние слои между A_{i_1} и A_{i_2}, а если последовательность состоит лишь из одного элемента i_1, то A_{i_1} находится на расстоянии q либо от A_0, либо от A_r.

Таким образом, мы показали, что радиус покрытия множества C равен q, и можем записать его метрическое дополнение в явном виде:

$$\widehat{C} = \bigcup_{\substack{k=1 \\ i_{k+1}-i_k>1}}^{s-1} (A_{i_k+q} \cup A_{i_{k+1}-q}) \cup (A_0 \setminus C) \cup (A_r \setminus C).$$

Обозначим последовательность индексов всех слоёв, включенных в это дополнение, через $j_1, \ldots, j_t$.

Изучим свойства слоёв, оказавшихся в $\widehat{C}$ в результате построения. Нетрудно видеть, что:

1. любые два слоя с последовательными индексами из $j_1, \ldots, j_t$ находятся на расстоянии
   - $2q$, если это слои A_{i_k-q} и A_{i_k+q} для некоторого k,
   - $2q+1$, если это слои A_{i_k-q} и $A_{i_{k+1}+q}$ для некоторого k, где i_k и i_{k+1} различаются на единицу,
   - 1, если это слои A_{i_k+q} и $A_{i_{k+1}-q}$, где $i_{k+1} - i_k = 2q+1$;
2. не существует более двух слоёв с последовательными индексами из $j_1, \ldots, j_t$ таких, что каждый следующий находится на расстоянии 1 от предыдущего;
3. если i_1 равняется q, то $j_1 = 0$ и $j_2 > 1$ (если j_2 существует); если i_1 равняется 0, то $j_1 = q$;
4. если i_s равняется $r - q$, то $j_t = r$ и $j_{t-1} < r - 1$ (если j_{t-1} существует); если i_s равняется r, то $j_t = r - q$;

Таким образом, условия 1–4 из утверждения теоремы выполняются также для последовательности $j_1, \ldots, j_t$, причём с такой же постоянной q. Следовательно, радиус покрытия $\widehat{C}$ равен q и

$$\widehat{\widehat{C}} = \bigcup_{\substack{k=1 \\ j_{k+1}-j_k>1}}^{t-1} (A_{j_k+q} \cup A_{j_{k+1}-q}) \cup (A_0 \setminus \widehat{C}) \cup (A_r \setminus \widehat{C}).$$

Внимательно сравнив индексы, мы видим, что $\widehat{\widehat{C}}$ состоит в точности из тех же самых слоёв, что и C, то есть эти множества совпадают и C метрически регулярно.

Строгая метрическая регулярность прямо следует из того факта, что C и $\widehat{C}$ состоят из слоёв послойного представления относительно строго метрически регулярного множества A, и леммы 2.2. □

Теорема 2.4 позволяет строить большое число новых метрически регулярных множеств с меньшим радиусом покрытия из данного строго метрически регулярного множества с радиусом покрытия r. Например, рассмотрим метрически регулярное множество A с радиусом покрытия 20. Тогда, если мы возьмём объединение слоёв A_i с индексами $\{2,3,7,12,16,20\}$, то оно будет метрически регулярным множеством с радиусом покрытия 2, а его метрическое дополнение будет состоять из слоёв с индексами $\{0,5,9,10,14,18\}$.

2.3 Количество множеств, получаемых итеративной конструкцией

В данном разделе мы подсчитаем, сколько метрически регулярных множеств с заданным радиусом покрытия q можно построить с использованием теоремы 2.4, имея в качестве основы данное строго метрически регулярное множество A с радиусом покрытия r. Заметим, что, поскольку слои $A_0, A_1, \ldots, A_r$ однозначно определяются множеством A, никакие два объединения слоёв послойного представления не могут совпадать, если только мы не объединяем один и тот же набор слоёв. Следовательно, все подсчитываемые в следующей теореме множества различны.

Теорема 2.5 (см. [57]). *Пусть $A \subseteq \mathbb{F}_2^n$ — строго метрически регулярное множество с радиусом покрытия $r > 0$. Количество $G_q(r)$ различных строго метрически регулярных множеств с радиусом покрытия q, которые можно построить объединением слоёв послойного представления пространства относительно множества A, применяя теорему 2.4, можно вычислить при помощи*

следующих рекуррентных формул:

$$G_q(r) = \begin{cases} G_q(r-q) + G_q(r-q-1), & \textit{при } r > q, \\ 2, & \textit{при } r = q, \\ 0, & \textit{при } 0 \leqslant r < q. \end{cases}$$

Характеристическое уравнение данной рекуррентной последовательности имеет вид $x^{q+1} = x + 1$. Данное уравнение не разрешимо в радикалах при $q \geqslant 4$, однако разрешимо при меньших q.

Доказательство. Заметим, что, как только радиусы покрытия r и q исходного и искомого множеств соответственно зафиксированы, задача нахождения последовательности индексов, удовлетворяющих условиям теоремы 2.4, становится числовой задачей, а содержание множеств и слоёв не имеет значения. Задача формулируется следующим образом: “для данных параметров r,q необходимо найти последовательность чисел $0 \leqslant i_1 < i_2 < \ldots < i_{s-1} < i_s \leqslant r$ такую, что она удовлетворяет условиям теоремы 2.4 с константой q”. Поэтому в доказательстве данной теоремы мы будем работать исключительно с числовыми последовательностями. Последовательность, удовлетворяющую условиям теоремы 2.4 с параметрами r и q, мы будем называть “правильной (r,q)-последовательностью”. Таким образом, наша цель заключается в нахождении количества правильных (r,q)-последовательностей.

Из условия 3 теоремы 2.4 мы знаем, что всякая правильная (r,q)-последовательность $i_1, \ldots, i_s$ должна начинаться либо с 0, либо с q. Обозначим за $E_q(r)$ количество правильных (r,q)-последовательностей, начинающихся с нуля, а за $F_q(r)$ — количество правильных (r,q)-последовательностей, начинающихся с q. Очевидно, что $G_q(r) = E_q(r) + F_q(r)$.

Заметим, что, по условиям 1 и 3, всякая последовательность, начинающаяся с 0, должна иметь вторым элементом либо $2q$, либо $2q + 1$. Пусть дана правильная (r,q)-последовательность $i_1, \ldots, i_s$ с $i_1 = 0$ и $i_2 = 2q$. Построим новую последовательность $j_1, \ldots, j_{s-1}$, где

$$j_k := i_{k+1} - q, k = 1, \ldots, s-1.$$

Легко проверить, что эта последовательность является правильной $(r - q,q)$-последовательностью и начинается с индекса q.

Таким образом, мы отобразили правильную (r,q)-последовательность с $i_1 = 0, i_2 = 2q$, в правильную $(r-q,q)$-последовательность, начинающуюся с q. По построению отображения очевидно, что оно инъективно, то есть отображает разные последовательности с заданными параметрами в разные.

Мы можем так же легко вычислить обратное отображение: пусть дана правильная $(r-q,q)$-последовательность с $i_1 = q$. Тогда мы можем построить правильную (r,q)-последовательность с $j_1 = 0, j_2 = 2q$, полагая $j_1 := 0$ и $j_{k+1} := i_k + q, k = 1, \ldots, s$.

Таким образом, мы построили биекцию между всеми правильными (r,q)-последовательностями, имеющими $i_1 = 0$, $i_2 = 2q$, и всеми правильными $(r-q,q)$-последовательностями, начинающимися с q.

Аналогичным образом строится биекция между всеми правильными (r,q)-последовательностями, имеющими $i_1 = 0, i_2 = 2q+1$, и всеми правильными $(r-q-1,q)$-последовательностями, начинающимися с q. В данном отображении мы снова убираем первый элемент последовательности, но уменьшаем все остальные элементы на $q+1$.

Следовательно, число всех правильных (r,q)-последовательностей, начинающихся с 0, равно числу всех правильных $(r-q,q)$-последовательностей и $(r-q-1,q)$-последовательностей, начинающихся с q. Используя ранее введённые обозначения, это соотношение можно записать в следующем виде:

$$E_q(r) = F_q(r-q) + F_q(r-q-1).$$

Схожие рассуждения применимы к правильным (r,q)-последовательностям, начинающимся с q. В силу условия 1, второй элемент в таких последовательностях равен $q+1$, $3q$ или $3q+1$.

1. Если второй элемент равен $q+1$, то, убирая первый элемент последовательности и уменьшая все остальные на $q+1$, мы получаем правильную $(r-q-1,q)$-последовательность $i_2, i_3, \ldots, i_s$, начинающуюся с 0.
2. Если второй элемент равен $3q$ или $3q+1$, то, уменьшая все элементы на q, мы получаем правильную $(r-q,q)$-последовательность, вновь начинающуюся с нуля.

Данные преобразования также легко обратимы, поэтому

$$F_q(r) = E_q(r-q) + E_q(r-q-1).$$

Мы получили реккурентные соотношения для $E_q(r)$ и $F_q(r)$, осталось лишь задать начальные значения. Легко видеть, что не существует правильных

(r,q)-последовательностей при $0 \leqslant r < q$. Нетрудно также заметить, что при $r = q$ существует лишь одна правильная (r,q)-последовательность, начинающаяся с 0, и одна — начинающаяся с q. Следовательно, мы имеем следующую систему соотношений:

$$\begin{cases} G_q(r) = E_q(r) + F_q(r), \\ E_q(r) = F_q(r-q) + F_q(r-q-1) \text{ при } r > q, \\ F_q(r) = E_q(r-q) + E_q(r-q-1) \text{ при } r > q, \\ E_q(q) = F_q(q) = 1, \\ E_q(r) = F_q(r) = 0 \text{ при } 0 \leqslant r < q. \end{cases}$$

Мы видим, что $E_q(r)$ и $F_q(r)$ удовлетворяют абсолютно одинаковым рекуррентным соотношениям и имеют одинаковые начальные значения, следовательно, эти числа совпадают для всех r и q. Заменяя $F_q(r)$ на $E_q(r)$, подставляя $G_q(r) = 2E_q(r)$ и убирая лишние формулы, мы получаем требуемую систему из формулировки теоремы. □

Заметим, что при $q = 1$ рекуррентное соотношение для последовательности $G_1(r)$ имеет вид

$$G_1(r) = G_1(r-1) + G_1(r-2) \text{ для } r > 1,$$

то есть совпадает с соотношением для последовательности Фибоначчи. Начальные значения $G_1(r)$ в два раза больше, чем у последовательности Фибоначчи. Таким образом,

$$G_1(r) = 2F_r = \frac{2}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^r - \left(\frac{1-\sqrt{5}}{2}\right)^r\right)$$

где F_r — r-ое число Фибоначчи. Поскольку $A = \{\mathbf{0}\}, \mathbf{0} \in \mathbb{F}_2^n$ — строго метрически регулярное множество с радиусом покрытия n, то, применяя теорему 2.4, мы можем легко получить из него $2F_n$ метрически регулярных множеств с радиусом покрытия 1.

Глава 3. Оценки мощностей метрически регулярных множеств

В данной главе проводится оценка возможных, наибольших и наименьших мощностей метрически регулярных множеств. Поскольку разрыв между известными верхними и нижними оценками количества бент-функций крайне велик, изучение мощностей множеств представляет интерес как возможный способ улучшения данных оценок.

В данной главе доказывается, что задача поиска наибольшего метрически регулярного множества в булевом кубе сводится к известной открытой задаче теории кодирования, в то время как задача поиска наименьшего метрически регулярного множества тривиальна. Получена нижняя оценка суммы мощностей метрически регулярного множества и его метрического дополнения при фиксировании радиуса покрытия. С использованием результатов предыдущей главы построены два семейства больших (относительно размера булева куба $\mathbb{F}_2^n$) метрически регулярных множеств с заданным радиусом покрытия. Множества из этих семейств дают представление о том, насколько большими могут быть метрически регулярные множества. Все утверждения, представленные в данной главе, являются новыми. Результаты главы опубликованы в работах [56, 57, 61, 62].

3.1 Наименьшее и наибольшее метрически регулярные множества

Пусть x — произвольный вектор $\mathbb{F}_2^n$. Множество $\{x\}$ метрически регулярно, следовательно, наименьшие метрически регулярные множества в булевом кубе имеют мощность 1. Решение не приходит настолько просто для наибольших метрически регулярных множеств. Тем не менее, в этом случае общую задачу можно свести к частной, для множеств с фиксированным радиусом покрытия. Напомним, что *послойным представлением* пространства относительно множества A называется набор множеств $A_k = \{x \in \mathbb{F}_2^n \mid d(x,A) = k\}$, $0 \leqslant k \leqslant \rho(A)$.

Теорема 3.1 (см. [56]). *Пусть A — метрически регулярное множество. Тогда существует метрически регулярное множество B с радиусом покрытия 1, содержащее A.*

Доказательство. Пусть радиус покрытия A равен r. Построим множества B и B' следующим образом:

$$B = \bigcup_{\substack{0\leqslant k\leqslant r,\\ k \text{ чётно}}} A_k, \qquad B' = \bigcup_{\substack{0\leqslant k\leqslant r,\\ k \text{ нечётно}}} A_k. \tag{3.1}$$

Заметим, что множества B и B' не пересекаются и покрывают весь булев куб. Докажем, что $\widehat{B} = B', \widehat{B'} = B$.

Пусть x — произвольный вектор из B'. По построению, существует нечётный номер $m \geqslant 1$ такой, что $x \in A_m$. По определению послойного представления, вектор x находится на расстоянии 1 от множества $A_{m-1} \subseteq B$. Таким образом, всякий вектор из B' находится на расстоянии 1 от множества B.

Пусть x — произвольный вектор из B. По построению, существует чётный номер m такой, что $x \in A_m$. Если m больше нуля, то по аналогичным рассуждениям вектор x находится на расстоянии 1 от множества B'. Предположим, что $m = 0$, то есть что $x \in A$. Поскольку $A = \widehat{\widehat{A}}$, существует путь $x = x_0,x_1,\ldots,x_{r-1},x_r = y$ длины r от некоторого вектора $y \in \widehat{A} = A_r$ к вектору $x \in A = A_0$. По определению послойного представления, ребро между множествами A_i и A_j может существовать только при $|i - j| \leqslant 1$. Отсюда следует, что $x_k \in A_k$ для всех k, и x_1 содержится в $A_1 \subseteq B'$. Следовательно, $d(x,B') = d(x,x_1) = 1$. Поскольку вектор x был выбран произвольно, множество B находится на расстоянии 1 от множества B'.

Таким образом, $\widehat{B} = B'$, $\widehat{B'} = B$ (то есть множества B и B' метрически регулярны), и радиус покрытия обоих равен 1. По построению, $A \subseteq B$. □

Теорема 3.1 показывает, что для всякого метрически регулярного множества в булевом кубе существует метрически регулярное надмножество с радиусом покрытия 1, содержащее данное. Следовательно, наибольшее метрически регулярное множество в булевом кубе имеет радиус покрытия, равный единице, и является (метрическим) дополнением наименьшего метрически регулярного множества с радиусом покрытия 1.

Напомним, что *покрывающим кодом* [9] радиуса r называется подмножество $\mathbb{F}_2^n$ с радиусом покрытия r.

Утверждение 3.2 (см. [56]). *Если множество $C \subseteq \mathbb{F}_2^n$ является покрывающим кодом радиуса 1 наименьшего размера, то C метрически регулярно.*

Доказательство. Поскольку C имеет радиус покрытия 1, любой вектор булева куба содержится либо в C, либо в его метрическом дополнении: $\mathbb{F}_2^n = C \cup \widehat{C}$. Если $\rho(\widehat{C}) = 1$, то, аналогично, $\mathbb{F}_2^n = \widehat{C} \cup \widehat{\widehat{C}}$, откуда следует, что $C = \widehat{\widehat{C}}$. Предположим, что $\rho(\widehat{C}) > 1$. Тогда существует вектор $y \in C$ такой, что $d(y,\widehat{C}) > 1$, и, следовательно, все соседи (векторы на расстоянии 1) вектора y содержатся в C. Но тогда $C\backslash\{y\}$ также является покрывающим кодом радиуса 1, что противоречит минимальности кода C. □

Из утверждения 3.2 следует, что наименьший покрывающий код радиуса 1 является также наименьшим метрически регулярным множеством с данным радиусом покрытия. Таким образом, задача нахождения наибольшего метрически регулярного множества эквивалентна задаче нахождения наименьшего покрывающего кода радиуса 1. Данная задача является открытым вопросом теории кодирования и решена, в основном, для частных случаев и небольших значений размерности булева куба. [9].

По аналогии с утверждением 3.2, автором высказана гипотеза о минимальных покрывающих кодах большего радиуса:

Гипотеза 3.3 (см. [56]). *Если множество $C \subseteq \mathbb{F}_2^n$ является покрывающим кодом радиуса r наименьшего размера, то C метрически регулярно.*

Гипотеза была проверена для некоторых наименьших покрывающих кодов длины $n = 2r + 3$,$n = 2r + 4$, где радиус r равен 2 или 3. Конструкции этих кодов можно найти в работах [8, 18].

3.2 Оценка мощности метрически регулярных множеств при фиксированном радиусе покрытия

Вспомним, что множество бент-функций $\mathcal{B}_m$ имеет радиус покрытия $2^{m-1} - 2^{\frac{m}{2}-1}$. Рассмотрим теперь задачу изучения размеров метрически регулярных множеств при фиксированном радиусе покрытия, отличном от нуля и от размерности пространства.

Размеры таких метрически регулярных множеств можно оценить косвенно, оценивая размер объединения множества и его метрического дополнения.

Теорема 3.4 (см. [56]). *Пусть $A \subseteq \mathbb{F}_2^n$ — метрически регулярное множество с радиусом покрытия r. Тогда*

$$|A| + |\widehat{A}| \geqslant \frac{2^{n+1}}{1 + \sum\limits_{k=0}^{r-1} \binom{n}{k}}.$$

Доказательство. Рассмотрим послойное представление $\mathbb{F}_2^n$ относительно A. Тогда $A_0 = A$, $A_r = \widehat{A}$, и

$$2^n = |\mathbb{F}_2^n| = \sum_{k=0}^{r} |A_k| = |A| + |\widehat{A}| + \sum_{k=1}^{r-1} |A_k|. \tag{3.2}$$

Поскольку на расстоянии k от любого вектора пространства $\mathbb{F}_2^n$ находятся не более $\binom{n}{k}$ векторов, мы имеем

$$|A_k| \leqslant \binom{n}{k} \cdot |A_0| = \binom{n}{k} \cdot |A|.$$

Используя эту оценку совместно с (3.2), получаем

$$|A| + |\widehat{A}| = 2^n - \sum_{k=1}^{r-1} |A_k| \geqslant 2^n - \sum_{k=1}^{r-1} \binom{n}{k} \cdot |A|. \tag{3.3}$$

Аналогично,

$$|A| + |\widehat{A}| = 2^n - \sum_{k=1}^{r-1} |A_k| \geqslant 2^n - \sum_{k=1}^{r-1} \binom{n}{k} \cdot |\widehat{A}|. \tag{3.4}$$

Складывая неравенства (3.3) и (3.4), мы получаем

$$2(|A| + |\widehat{A}|) \geqslant 2^{n+1} - (|A| + |\widehat{A}|) \sum_{k=1}^{r-1} \binom{n}{k}.$$

Сгруппировав все слагаемые, содержащие $|A| + |\widehat{A}|$, и поделив на соответствующий коэффициент, мы получаем искомое неравенство. □

Данная оценка очень схожа с границей сферической упаковки (границей Хэмминга) кода, известной в теории кодирования.

3.3 Построение семейств больших метрически регулярных множеств

Рассмотрим метрически регулярное множество $A = \{\mathbf{0}\}$ в пространстве $\mathbb{F}_2^n$. При помощи теоремы 2.4 (глава 2), на основе данного множества можно построить большое (относительно мощности всего булева куба) метрически регулярное множество, подходящим образом выбирая слои для включения в объединение. По интуитивным соображениям, для получения множества наибольшей мощности необходимо объединить как можно большее число слоёв. Следовательно, если мы хотим построить большое метрически регулярное множество с радиусом покрытия r, то расстояние между последовательными слоями, включаемыми в объединение, должно быть наименьшим — равняться единице, если это возможно, и $2r$ в противном случае.

Предположим, что $(n+1)$ делится на $(2r+1)$, т.е. $(n+1) = t(2r+1)$ для некоторого $t \geqslant 1$. Тогда последовательность индексов

$$\{i_1, i_2, \ldots, i_{2t}\} = \{0, 2r, 2r+1, 4r+1, 4r+2, \ldots, n-(2r+1), n-2r, n\}$$

удовлетворяет условиям теоремы 2.4 с параметром r. Следовательно, множество

$$Y_n^r = \bigcup_{k=1}^{2t} A_{i_k}$$

является строго метрически регулярным с радиусом покрытия r.

Вычислим мощность множества Y_n^r. Поскольку множество A содержит лишь нулевой вектор, то A_k — множество всех векторов веса k. Следовательно,

$$|Y_n^r| = \sum_{k=1}^{2t} \binom{n}{i_k} = \binom{n}{0} + \binom{n}{2r} + \binom{n}{2r+1} + \ldots + \binom{n}{n-2r} + \binom{n}{n}.$$

Поскольку $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$ и $\binom{n}{n} = \binom{n}{0} = 1$, мы можем преобразовать это выражение следующим образом:

$$\begin{aligned} |Y_n^r| = \binom{n+1}{0} + \binom{n+1}{2r+1} + \binom{n+1}{2(2r+1)} + \ldots + \binom{n+1}{(t-1)(2r+1)} + \\ + \binom{n+1}{n+1} = \sum_{k=0}^{t} \binom{n+1}{k(2r+1)}. \end{aligned} \tag{3.5}$$

Последнее выражение — сумма каждого $(2r+1)$-го биномиального коэффициента. Известно [15], что для любого $n \geqslant 0$ и $s \geqslant 1$ имеет место следующее соотношение:

$$\sum_{k \geqslant 0} \binom{n}{ks} = \frac{1}{s} \sum_{j=0}^{s-1} (1+\omega^j)^n,$$

где $\omega = e^{\frac{i2\pi}{s}}$ — примитивный корень из единицы и $\binom{n}{k} = 0$ при $k > n$.

Подставляя в данное выражение $2r+1$ вместо s и $n+1$ вместо n, получаем

$$|Y_n^r| = \frac{1}{2r+1} \sum_{j=0}^{2r} (1+\omega^j)^{n+1} = \frac{1}{2r+1} \left(2^{n+1} + \sum_{j=1}^{2r} (1+\omega^j)^{n+1} \right), \tag{3.6}$$

где $\omega = e^{\frac{i2\pi}{2r+1}}$.

Предположим теперь, что $n+1$ не делится на $2r+1$, т. е. $n+1 = t(2r+1)+s$ для некоторых $t \geqslant 1, 0 < s < 2d+1$. Расширим проведённую выше конструкцию для пространства размерности n при таких условиях.

Нетрудно показать, что прямое произведение C двух множеств A и B двоичных векторов длины n и m соответственно имеет радиус покрытия, равный сумме радиусов покрытия A и B, а его метрическое дополнение $\widehat{C}$ равно прямому произведению дополнений $\widehat{A}$ и $\widehat{B}$. Отсюда следует, что, если множества A и B метрически регулярны, то метрически регулярно также и их прямое произведение C.

Булев куб размерности s, очевидно, является метрически регулярным множеством с радиусом покрытия 0. Построив по конструкции выше метрически регулярное множество Y_{n-s}^r в булевом кубе размерности $n-s$, (поскольку $n-s+1$ делится на $2r+1$), мы можем расширить его до метрически регулярного множества в булевом кубе размерности n при помощи прямого произведения с булевым кубом размерности s:

$$Y_n^r := Y_{n-s}^r \times \mathbb{F}_2^s \tag{3.7}$$

Таким образом, мы построили метрически регулярное множество Y_n^r для произвольного $n \geqslant 2r$. Размер такого множества равен, соответственно:

$$|Y_n^r| = 2^s |Y_{n-s}^r| = \frac{1}{2r+1} \left(2^{n+1} + 2^s \sum_{j=1}^{2r} (1+\omega^j)^{n-s+1} \right), \tag{3.8}$$

где $\omega = e^{\frac{i2\pi}{2r+1}}$. Заметим, что данная формула подходит для вычисления размера множества Y_n^r и в случае, когда $2r+1$ делит $n+1$ без остатка (с нулевым остатком). Установим асимптотику полученной величины.

Утверждение 3.5. *Размер метрически регулярного множества Y_n^r с радиусом покрытия r, содержащегося в булевом кубе размерности n ($n \geqslant 2r$), имеет следующее асимптотическое поведение:*

$$|Y_n^r| \sim \frac{2}{2r+1} 2^n. \tag{3.9}$$

Доказательство. Для любого $1 \leqslant j \leqslant 2r$ абсолютное значение $|1+\omega^j|$ не превосходит некоторой константы c, строго меньшей 2. Тем самым, второе слагаемое в скобке формулы 3.8 пренебрежимо мало в сравнении с первым слагаемым при фиксированном r и растущем n. □

Таким образом, при $n \to \infty$ метрически регулярное множество Y_n^r, построенное данным методом, покрывает значительную долю булева куба.

Построим теперь ещё одно семейство больших множеств $\{Z_n^r\}$. Рассмотрим множество всех векторов веса r в булевом кубе размерности $2r$. Оно является метрически регулярным и имеет размер $\binom{2r}{r}$. Как и в предыдущей конструкции, мы можем расширить данное множество, взяв его прямое произведение с пространством $\mathbb{F}_2^{n-2r}$. В результате получается метрически регулярное множество Z_n^r размера

$$|Z_n^r| = 2^{n-2r} \binom{2r}{r} \tag{3.10}$$

в булевом кубе размерности n.

Поскольку $\binom{2r}{r} \sim \frac{2^{2r}}{\sqrt{\pi r}}$, множества Z_n^r покрывают приблизительно $\frac{1}{\sqrt{\pi r}}$-ую часть булева куба при достаточно больших r.

3.4 Оценка мощности наибольших метрически регулярных множеств

Оценим мощности множеств Y_n^r, используя комплексные формулы 3.8, выведенные в предыдущем разделе. В паре с известными размерами множеств Z_n^r, эта оценка приводит к следующему результату:

Теорема 3.6 (см. [57]). *Пусть A — наибольшее метрически регулярное множество с радиусом покрытия r в булевом кубе размерности n ($n \geqslant 2r$), и пусть s — остаток от деления $n+1$ на $2r+1$. Тогда*

$$|A| \geqslant \max\left\{2^n\left(\frac{2}{2r+1} - \frac{2}{\sqrt{n-s+1}}\right), 2^{n-2r}\binom{2r}{r}\right\}. \tag{3.11}$$

Доказательство. Оценим снизу мощность множества Y_n^r при помощи формулы 3.8 и неравенства треугольника:

$$\begin{aligned} |Y_n^r| &= \frac{1}{2r+1}\left(2^{n+1} + 2^s\sum_{j=1}^{2r}(1+\omega^j)^{n-s+1}\right) \geqslant \\ &\geqslant \frac{1}{2r+1}\left(2^{n+1} - 2^s\left|\sum_{j=1}^{2r}(1+\omega^j)^{n-s+1}\right|\right), \end{aligned} \tag{3.12}$$

Докажем теперь следующую оценку:

$$\left|\sum_{j=1}^{2r}(1+\omega^j)^{n-s+1}\right| \leqslant 2^{n-s+1}\frac{2r+1}{\sqrt{n-s+2}}. \tag{3.13}$$

Для этого используем сначала неравенство треугольника и тот факт, что $|1+\omega^j| = |1+\omega^{2r+1-j}|$:

$$\left|\sum_{j=1}^{2r}(1+\omega^j)^{n-s+1}\right| \leqslant \sum_{j=1}^{2r}|1+\omega^j|^{n-s+1} = 2\sum_{j=1}^{r}|1+\omega^j|^{n-s+1}. \tag{3.14}$$

Вычислим теперь $|1+\omega^j|$. Обозначим $\phi_j = \frac{2\pi j}{2r+1}$. По определению модуля комплексного числа и свойствам косинуса, мы имеем

$$\begin{aligned} |1+\omega^j| = |1+\cos\phi_j + i\sin\phi_j| &= \sqrt{1+2\cos\phi_j+\cos^2\phi_j+\sin^2\phi_j} = \\ = \sqrt{2(1+\cos\phi_j)} &= \sqrt{2\cdot 2\cos^2\frac{\phi_j}{2}} = 2\cos\frac{\phi_j}{2} = 2\cos x_j, \end{aligned} \tag{3.15}$$

где $x_j = \phi_j/2 = \frac{\pi j}{2r+1}$. Обозначим $\Delta x_j = x_j - x_{j-1}$. Подставив 3.15 в 3.14, умножив и поделив всё выражение на $\frac{\pi}{2r+1}$, мы получаем

$$\begin{aligned} 2\sum_{j=1}^{r}|1+\omega^j|^{n-s+1} &= 2^{n-s+2}\sum_{j=1}^{r}(\cos x_j)^{n-s+1} = \\ = 2^{n-s+2}\frac{2r+1}{\pi}\sum_{j=1}^{r}\frac{\pi}{2r+1}(\cos x_j)^{n-s+1} &= 2^{n-s+2}\frac{2r+1}{\pi}\sum_{j=1}^{r}\Delta x_j(\cos x_j)^{n-s+1}. \end{aligned} \tag{3.16}$$

Последняя сумма в 3.16 является интегральной суммой для функции $f(x) = (\cos x)^{n-s+1}$ на промежутке $[0, \frac{\pi r}{2r+1}]$, причём значения функции взяты в правом конце каждого подынтервала $[\frac{\pi(j-1)}{2r+1}, \frac{\pi j}{2r+1}]$, где $j = 1, \ldots, r$. Поскольку косинус (как и его степени) является убывающей неотрицательной функцией на промежутке $[0, \frac{\pi}{2}]$, мы можем оценить сумму интегралом:

$$\sum_{j=1}^{r} \Delta x_j (\cos x_j)^{n-s+1} \leqslant \int_0^{\frac{\pi}{2}} (\cos x)^{n-s+1} \mathrm{r}x = \begin{cases} \frac{\pi(n-s)!!}{2(n-s+1)!!}, & \text{если } n-s+1 \text{ чётно,} \\ \frac{(n-s)!!}{(n-s+1)!!}, & \text{иначе.} \end{cases} \tag{3.17}$$

Последнее равенство получается вычислением интеграла по частям. Используя простую оценку $\frac{n-1}{n} \leqslant \sqrt{\frac{n-1}{n+1}}$, легко показать, что

$$\frac{(n-1)!!}{n!!} \leqslant \begin{cases} \sqrt{\frac{1}{n+1}}, & \text{если } n \text{ чётно,} \\ \sqrt{\frac{2}{n+1}}, & \text{иначе.} \end{cases} \tag{3.18}$$

Объединяя 3.17 и 3.18, мы получаем следующую оценку суммы:

$$\sum_{j=1}^{r} \Delta x_j (\cos x_j)^{n-s+1} \leqslant \begin{cases} \frac{\pi}{2\sqrt{n-s+2}}, & \text{если } n-s+1 \text{ чётно,} \\ \frac{\sqrt{2}}{\sqrt{n-s+2}}, & \text{иначе.} \end{cases} \leqslant \frac{\pi}{2\sqrt{n-s+2}} \tag{3.19}$$

Подставляя в 3.16, получаем

$$2 \sum_{j=1}^{r} |1 + \omega^j|^{n-s+1} \leqslant 2^{n-s+2} \frac{2r+1}{\pi} \frac{\pi}{2\sqrt{n-s+2}} = 2^{n-s+1} \frac{2r+1}{\sqrt{n-s+2}}, \tag{3.20}$$

что совместно с 3.14 даёт искомое неравенство 3.13.

Используя неравенство 3.13, мы можем избавиться от всех комплексных слагаемых в 3.12:

$$\begin{aligned} |Y_n^r| &\geqslant \frac{1}{2r+1} \left(2^{n+1} - 2^s \left| \sum_{j=1}^{2r} (1 + \omega^j)^{n-s+1} \right| \right) \geqslant \\ &\geqslant \frac{1}{2r+1} 2^{n+1} \left(1 - \frac{2r+1}{\sqrt{n-s+2}} \right) = 2^{n+1} \left(\frac{1}{2r+1} - \frac{1}{\sqrt{n-s+2}} \right). \end{aligned} \tag{3.21}$$

Выражение 3.21, вместе с формулой 3.10 мощности множеств Z_n^r , построенных в предыдущем разделе, даёт оценку, сформулированную в условии теоремы. □

Очевидно, что вычитаемое $\frac{1}{\sqrt{n-s+1}}$ в формуле 3.21 стремится к нулю при $n \to \infty$, следовательно, полученная в доказательстве нижняя оценка имеет такую же асимптотику, как и действительный размер Y_n^r (см. 3.9). Таким образом, множество Y_n^r покрывает примерно $\frac{2}{2r+1}$-ую от всего булева куба при достаточно больших n. Поскольку $\binom{2r}{r} \sim \frac{2^{2r}}{\sqrt{\pi r}}$, множество Z_n^r покрывает примерно $\frac{1}{\sqrt{\pi r}}$-ую от булева куба при достаточно больших r, поэтому множества Z_n^r больше, чем множества Y_n^r, начиная с некоторого r. Однако для небольших значений r, множества Y_n^r имеют большую мощность.

Глава 4. Метрические дополнения и метрическая регулярность линейных подпространств

Линейные подпространства являются одним из наиболее изучаемых классов подмножеств булева куба. Различные семейства линейных подпространств булева куба (линейных кодов) находят применения во многих областях дискретной математики и за её пределами. Множество аффинных булевых функций является линейным подпространством. Всё это вызывает естественный интерес к изучению метрических дополнений линейных подпространств $\mathbb{F}_2^n$. Структурные особенности линейных подпространств булева куба наталкивают на мысли о структурных особенностях их метрических дополнений. В данной главе описан общий вид метрического дополнения линейного подпространства, получено явное описание для подпространств с каноническим базисом специального вида. Получена характеризация второго метрического дополнения линейного подпространства, также предоставляющая критерий проверки метрической регулярности линейного подпространства. Результаты главы опубликованы в работах [55, 60].

4.1 Базовые свойства

Пусть L — произвольное линейное подпространство $\mathbb{F}_2^n$. Общий вид метрического дополнения $\widehat{L}$ описывается следующим тривиальным утверждением.

Лемма 4.1. *Пусть $L \subseteq \mathbb{F}_2^n$ — линейное подпространство, a — двоичный вектор длины n и $d(a,L) = k$. Тогда для любого вектора y из смежного класса $a+L$ имеет место $d(y,L) = k$, и, следовательно, множество $\widehat{L}$ является объединением смежных классов подпространства L.*

Приведём без доказательства следующее утверждение, которое нам понадобится в дальнейшем.

Лемма 4.2. *Пусть $L \subseteq \mathbb{F}_2^n$ — линейное подпространство размерности k. Тогда в L существует единственный базис $e_1, \ldots, e_k$ такой, что матрица, составлен-*

ная из векторов этого базиса, имеет вид

$$M = \begin{array}{c} \\ \\ \\ \\ \\ \end{array} \begin{array}{c} \begin{array}{cccccccccccc} & & & s_1 & & s_2 & & s_3 & & & & s_k & \\ \end{array} \\ \begin{pmatrix} 0 & \dots & 0 & 1 & * & 0 & * & 0 & * & \dots & * & 0 & * \\ 0 & \dots & \dots & \dots & 0 & 1 & * & 0 & * & \dots & * & 0 & * \\ 0 & \dots & \dots & \dots & \dots & \dots & 0 & 1 & * & \dots & \vdots & \vdots & \vdots \\ 0 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & * & 0 & * \\ 0 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0 & 1 & * \end{pmatrix} \end{array}$$

Матрица такого вида называется матрицей Гаусса-Жордана.

Этот базис будем называть *каноническим*, а его векторы в общем случае будем обозначать как e_i^*, $i = 1, \dots, k$. Понадобится нам также множество $S = \{s_i : i = 1, \dots, k\}$, где s_i — номер позиции, в которой у i-го вектора канонического базиса подпространства L стоит первая единица. Обозначим $\overline{S} = \{1, \dots, n\} \setminus S$.

Рассмотрим множество X_L векторов, у которых в координатах из множества S находятся нули. Легко видеть, что в любом смежном классе подпространства L найдётся единственный вектор из множества X_L. В силу леммы 4.1, векторов из этого множества достаточно для полного исследования метрического дополнения подпространства. В дальнейшем нам пригодится вектор максимального веса $n - k$ из X_L, поэтому введём для него специальное обозначение: $a_L = \arg\max\limits_{b \in X_L} wt(b)$. Заметим, что вектор a_L имеет следующий вид:

$$a_L = \begin{array}{c} \begin{array}{cccccccccccccc} & & & s_1 & & & & s_2 & & & & s_k & & \\ \end{array} \\ \Big(1 \quad \dots \quad 1 \quad 0 \quad 1 \quad \dots \quad 1 \quad 0 \quad 1 \quad \dots \quad 1 \quad 0 \quad 1 \quad \dots \quad 1\Big), \end{array}$$

то есть единицы содержатся во всех координатах из множества $\overline{S}$.

Введённый канонический базис позволяет получить оценки радиуса покрытия линейного подпространства. Следующий результат хорошо известен в теории покрывающих кодов, однако может быть легко установлен при помощи леммы 4.1 и введённого множества представителей смежных классов X_L.

Теорема 4.3 (см. [9]). *Пусть $L \subseteq \mathbb{F}_2^n$ — линейное подпространство размерности k. Тогда*

$$\rho(L) \leqslant n - k.$$

4.2 Линейные подпространства с базисом малого веса

Рассмотрим подпространства, векторы канонического базиса которых имеют малые веса. Для некоторых из них нетрудно в явном виде найти метрическое дополнение.

Теорема 4.4 (см. [55]). *Пусть $L \subseteq \mathbb{F}_2^n$ — линейное подпространство размерности k, а $e_1^*, \ldots, e_k^*$ — его канонический базис. Равенство в оценке теоремы 4.3 достигается тогда и только тогда, когда $wt(e_i^*) \leqslant 2$ для всех $i \in \{1,\ldots,k\}$. В этом случае $\widehat{L} = a_L + L$.*

Доказательство. ($\Rightarrow$) Если $\rho(L) = n - k$, то, очевидно, вес всякого $b \in X_L \cap \widehat{L}$ равен $n - k$. Таким образом, $X_L \cap \widehat{L} = \{a_L\}$. Если вес какого-либо вектора e_i^* превосходит 2, то легко видеть, что вектор a_L удалён от вектора e_i^* на расстояние, меньшее $n - k$, что противоречит тому, что $\rho(L) = n - k$.

($\Leftarrow$) Пусть веса векторов канонического базиса не превосходят 2. Тогда для каждого e_i^* из канонического базиса $|supp(e_i^*) \cap S| = 1$, $|supp(e_i^*) \cap \overline{S}| \leqslant 1$. Покажем, что для любого $x \in L$ имеет место $wt(x + a_L) \geqslant n - k$. Пусть $x \in L$ и $x = e_{i_1}^* + \ldots + e_{i_l}^*$ — разложение x по каноническому базису. Тогда, как можно видеть из матрицы канонического базиса, $|supp(x) \cap S| = l$ и $|supp(x) \cap \overline{S}| \leqslant l$. Так как $supp(a_L) = \overline{S}$, отсюда следует, что $wt(a_L + x) \geqslant wt(a_L) + l - l = wt(a_L) = n - k$. Таким образом, $d(a_L, L) = n - k$ и $a_L + L \subseteq \widehat{L}$. Включение можно заменить на равенство в силу того, что вес любого $b \in X_L$, отличного от a_L, строго меньше $n - k$, а с ним и расстояние до нулевого вектора, содержащегося в подпространстве. □

Теорема 4.5 (см. [55]). *Пусть $L \subseteq \mathbb{F}_2^n$ — линейное подпространство размерности k с каноническим базисом $e_1^*, \ldots, e_k^*$. Пусть $wt(e_i^*) \leqslant 3$ для всех $i = 1, \ldots, k$ и существует индекс j такой, что $wt(e_j^*) = 3$. Тогда $\rho(L) = n - k - 1$ тогда и только тогда, когда $supp(e_i^*) \cap supp(e_j^*) \neq \varnothing$ для всех i,j таких, что $wt(e_i^*) = wt(e_j^*) = 3$. При этом $a_L + L \subseteq \widehat{L}$. Более того,*

1. *если $\bigcap\limits_{i:wt(e_i^*)=3} supp(e_i^*) = \varnothing$, то $\widehat{L} = a_L + L$;*
2. *если $\bigcap\limits_{i:wt(e_i^*)=3} supp(e_i^*) = \{m\}$, то $\widehat{L} = (a_L + L) \cup (b + L)$, где $b \in X_L$ — вектор веса $n - k - 1$ с нулями только в координатах из множества $\{m\} \cup S$;*

3. *если* $\bigcap\limits_{i:wt(e_i^*)=3} supp(e_i^*) = \{m,l\}$, *то* $\widehat{L} = (a_L + L) \cup (b + L) \cup (c + L)$, *где* $b,c \in X_L$ — *векторы веса* $n-k-1$ *с нулями только в координатах из множеств* $\{m\} \cup S$ *и* $\{l\} \cup S$ *соответственно.*

Доказательство. ($\Rightarrow$) Пусть $\rho(L) = n-k-1$. Предположим, что существуют i,j такие, что $wt(e_i^*) = wt(e_j^*) = 3$, но $supp(e_i^*) \cap supp(e_j^*) = \varnothing$. Тогда $wt(e_i^* + e_j^*) = 6$, причём $|supp(e_i^* + e_j^*) \cap S| = 2$, $|supp(e_i^* + e_j^*) \cap supp(a_L)| = 4$, откуда $d(a_L, e_i^* + e_j^*) = wt(a_L + e_i^* + e_j^*) = wt(a_L) + 2 - 4 = n - k - 2$.

Пусть $b \in X_L$ имеет вес $n-k-1$. Тогда у b только в одной координате из $\overline{S}$ стоит ноль, пусть в m-ой. Либо у e_i^*, либо у e_j^* в позиции m также находится ноль, так как иначе бы их носители пересекались. Для определённости, пусть у e_i^*. Но тогда $d(b, e_i^*) = wt(b + e_i^*) = wt(b) + 1 - 2 = n - k - 2$.

Таким образом, никакой вектор $b \in X_L$ веса больше $n-k-2$ не удалён от L на расстояние $n-k-1$ (а меньшего веса тем более), что противоречит тому, что $\rho(L) = n-k-1$. Следовательно, носители любых двух векторов веса 3 пересекаются.

($\Leftarrow$) Пусть носители любых двух базисных векторов веса 3 пересекаются. Докажем, что $\rho(a_L, L) = n-k-1$. Заметим, что векторы канонического базиса, веса которых не превосходят 2, не влияют на расстояние до a_L, как было показано в теореме 4.4. Пусть в разложении x присутствует чётное число векторов веса 3. Тогда их можно разбить на пары $\{e_{1i}^*, e_{2i}^*\}$, причём $|supp(e_{i_1}^* + e_{i_2}^*) \cap S| = 2$, а, так как носители e_{1i}^* и e_{2i}^* пересекаются, $|supp(e_{i_1}^* + e_{i_2}^*) \cap \overline{S}| \leqslant 2$. Отсюда $d(a_L, x) = wt(a_L + x) \geqslant wt(a_L) = n - k$. Если в разложении x нечётное число векторов веса 3, то, вычтя из x один из них, получим вектор y такой, что $d(a_L, y) \geqslant n-k$ по только что доказанному. Убранный вектор имеет одну единицу на позиции из S и две — на позициях из $\overline{S}$. Тем самым, $d(a_L, x) \geqslant d(a_L, y) + 1 - 2 \geqslant n - k - 1$. Таким образом, вектор a_L удалён от L на расстояние $n-k-1$.

1. Пусть $\bigcap\limits_{i:wt(e_i^*)=3} supp(e_i^*) = \varnothing$, и пусть вектор $b \in X_L, b \neq a_L$ имеет вес $n-k-1$. В какой-то из координат множества $\overline{S}$ у вектора b есть ноль, и, так как пересечение носителей всех базисных векторов веса 3 пусто, существует базисный вектор e_i^* веса 3 с нулём в той же позиции, что и у b. Тогда $d(b, e_i^*) = wt(b + e_i^*) = (n-k-1) + 1 - 2 = n - k - 2$, то есть вектор b не может (вместе с соответствующим сдвигом) лежать в метрическом дополнении.

2. Пусть $\bigcap\limits_{i:wt(e_i^*)=3} supp(e_i^*) = \{m\}$. Тогда, убрав m-ую координату у всех векторов пространства, получим k-мерное подпространство L' в $\mathbb{F}_2^{n-1}$, удовлетворяющее условиям теоремы 2. Значит, $\rho(L') = n-k-1$ и $\widehat{L'} = a_{L'} + L'$. Вернув m-ую координату вектору $a_{L'}$ (заполнив её единицей и нулём соответственно), получим n-мерные векторы a_L и b веса $n-k$ и $n-k-1$ соответственно, причём

$$d(a_L,L) = \min_{x\in L} d(a_L,x) \geqslant \min_{x'\in L'} d(a_{L'},x') = n-k-1.$$

Эта же оценка расстояния верна и для вектора b. Тем самым, $(a_L + L) \cup (b + L) \subseteq \widehat{L}$. Доказательство отсутствия других сдвигов в $\widehat{L}$ проводится точно так же, как в п.1.

3. Повторяем доказательство п.2 для координат m и l.

□

4.3 Метрические дополнения аффинных подпространств

Нетрудно убедиться, что все приведённые выше результаты верны и для аффинных подпространств. В самом деле, пусть $A \subseteq \mathbb{F}_2^n$ — аффинное подпространство и $A = a + L$, где L — линейное подпространство. Пусть $\rho(L) = r$. Тогда, поскольку сдвиг всего пространства $\mathbb{F}_2^n$ на вектор a является изометрией, то сразу получаем, что $\rho(A) = r$ и $\widehat{A} = a + \widehat{L}$. Это наблюдение позволяет свести задачу нахождения радиуса покрытия и метрического дополнения аффинного подпространства к этой же задаче для соответствующего ему линейного подпространства и использовать для её решения результаты предыдущих разделов данной главы.

4.4 Метрически регулярные подпространства

Метрические свойства метрического дополнения линейного подпространства напрямую связаны с метрическими свойствами самого подпространства:

Утверждение 4.6 (см. [55]). *Пусть $L \subseteq \mathbb{F}_2^n$ — линейное подпространство, $\rho(L) = k$. Тогда $\rho(\widehat{L}) = k$ и $L \subseteq \widehat{\widehat{L}}$.*

Доказательство. Очевидно, что для всякого $x \in L$ выполняется $d(x,\widehat{L}) = k$. Предположим, что $\rho(\widehat{L}) > k$, т.е. существует вектор z такой, что $d(z,\widehat{L}) = l > k$. Пусть $b \in X_L \cap \widehat{L}$. Тогда $d(z+b,L) = d(z,b+L) \geqslant d(z,\widehat{L}) = l > k$, что противоречит максимальности радиуса покрытия $\rho(L)$. □

Известно, что подпространство аффинных функций является метрически регулярным. Быть может, любое линейное подпространство обладает этим свойством? Оказывается, что нет.

Теорема 4.7 (см. [55]). *Пусть $L \subseteq \mathbb{F}_2^n$ — линейное подпространство. Тогда $x \in \widehat{\widehat{L}}$ тогда и только тогда, когда $\widehat{L}$ инвариантно относительно сдвига на x, т.е. $\widehat{L} = x + \widehat{L}$.*

Доказательство. По предыдущему утверждению, $\rho(L) = \rho(\widehat{L})$.

($\Rightarrow$) Пусть $z \in \widehat{\widehat{L}}$. Это означает, что для любого $y \in \widehat{L}$ выполняется $d(z,y) \geqslant d(L)$. Зафиксируем произвольный y из $\widehat{L}$. Так как $y+L$ целиком содержится в $\widehat{L}$, то для всех $x \in L$ имеет место $d(z,y+x) \geqslant d(L)$, то есть $d(z+y,L) \geqslant d(L)$, а это означает, что $(z+y) \in \widehat{L}$. В силу произвольности y и инъективности операции прибавления вектора z, мы заключаем, что $\widehat{L} = z + \widehat{L}$.

($\Leftarrow$) Пусть $\widehat{L} = z + \widehat{L}$. Это в точности означает, что для любого $y \in \widehat{L}$ выполнено $d(z+y,L) = \rho(L)$. Следовательно, $wt(z+y) \geqslant \rho(L)$ для всех $y \in \widehat{L}$, то есть $z \in \widehat{\widehat{L}}$, что и требовалось доказать. □

Следствие 4.8. *Пусть $L \subseteq \mathbb{F}_2^n$ — линейное подпространство, а $\widehat{L}$ — аффинное подпространство, то есть $\widehat{L} = a + L_1$, где $L_1 \subseteq \mathbb{F}_2^n$ — линейное подпространство. Тогда $\widehat{\widehat{L}} = L_1$.*

С помощью следствия 4.8 и теоремы 4.5 нетрудно построить пример линейного подпространства, не являющегося метрически регулярным. Так, метрическое дополнение линейного подпространства $L = \{(00000),(10110),(01011),(11101)\}$ в $\mathbb{F}_2^5$ состоит из двух смежных классов $a+L$, $b+L$ по п. 2 теоремы 4.5, а любые два смежных класса линейного подпространства образуют аффинное подпространство. По следствию 4.8, $\widehat{\widehat{L}} = L \cup a+b+L$.

Также, используя следствие 4.8, можно сразу выделить класс метрически регулярных подпространств таких, что $|L| = |\widehat{L}|$, то есть имеющих лишь один максимально удалённый сдвиг.

Глава 5. Метрическая регулярность кодов Рида-Маллера

В данной главе изучается метрическая регулярность кодов Рида-Маллера. Метрическая регулярность кода $\mathcal{RM}(1,m)$ — множества аффинных функций — при чётных m была установлена Н. Токаревой в работе [47].

Опишем известные результаты, касающиеся радиуса покрытия кодов Рида-Маллера. Среди кодов высоких порядков, радиусы покрытия известны только для кодов $\mathcal{RM}(k,m)$ при $k \geqslant m-3$. Радиус покрытия кода $\mathcal{RM}(1,m)$ неизвестен при нечётных $m > 7$, однако вычислен [3] для кода $\mathcal{RM}(1,5)$ и для кода $\mathcal{RM}(1,7)$ [20, 34]. В работе [40], Дж. Шац определил радиус покрытия кода $\mathcal{RM}(2,6)$, а совсем недавно К. Ванг вычислил радиус покрытия кода $\mathcal{RM}(2,7)$ [53]. При $m > 7$ радиусы покрытия кодов $\mathcal{RM}(2,m)$ на данный момент неизвестны. В данной главе доказывается метрическая регулярность кодов $\mathcal{RM}(k,m)$ при $k = 0$ и $k \geqslant m-3$, а также кодов $\mathcal{RM}(1,5)$ и $\mathcal{RM}(2,6)$. В большинстве случаев в процессе доказательства получено описание метрического дополнения кода.

Глава построена следующим образом. После приведения необходимых определений доказывается метрическая регулярность кода $\mathcal{RM}(1,5)$. Затем устанавливается метрическая регулярность кодов Рида-Маллера порядка 0, порядков $m-2$ и выше, после чего рассматриваются коды порядка $m-3$. Для рассмотрения данного случая описывается “метод синдромных матриц”, который вводится в книге “Covering codes” [9] с целью нахождения радиуса покрытия кода $\mathcal{RM}(m-3,m)$. Следуя изложению книги, при помощи данного метода вычисляется радиус покрытия кода $\mathcal{RM}(m-3,m)$, а затем описывается его метрическое дополнение. Описание дополнения позволяет доказать метрическую регулярность кода $\mathcal{RM}(m-3,m)$. После этого устанавливается метрическая регулярность кода $\mathcal{RM}(2,6)$. Доказательство основывается на результатах, полученных для кодов $\mathcal{RM}(2,5)$ и $\mathcal{RM}(1,5)$, поскольку код $\mathcal{RM}(2,6)$ может быть построен из вышеупомянутых кодов при помощи конструкции Плоткина ($(\mathbf{u},\mathbf{u}+\mathbf{v})$-конструкции). Главу завершает обзор полученных результатов и гипотеза о метрической регулярности кодов Рида-Маллера. Результаты главы опубликованы в работах [58, 59, 63, 64].

5.1 Определения

Пусть $\mathcal{F}^m$ — множество всех булевых функций от m переменных. Код Рида-Маллера порядка k от m переменных определяется следующим образом:

$$\mathcal{RM}(k,m) = \{f \in \mathcal{F}^m : \deg(f) \leqslant k\},$$

где $\deg(\cdot)$ обозначает степень *алгебраической нормальной формы (АНФ)* функции. Код Рида-Маллера порядка k от m переменных имеет параметры $[2^m, \sum_{i=0}^{k} \binom{m}{i}, 2^{m-k}]$.

Данный код может быть представлен как множество *векторов значений* соответствующих функций. *Вектором значений* функции f от m переменных называется вектор длины 2^m, i-ая координата которого равна значению функции на наборе переменных, соответствующему двоичному представлению числа i (координаты нумеруются от 0 до $2^m - 1$). В данной главе мы иногда будем переключаться между данными двумя представлениями — функции и векторы значений функций, — зачастую без явного упоминания. Переменная m в данной главе обозначает количество переменных, от которых зависят функции, в то время как $n := 2^m$ обозначает размерность пространства векторов значений. Веса функций и расстояния между функциями совпадают с весами и расстояниями между соответствующими векторами значений.

В данной главе векторы длины m и квадратные матрицы размера $m \times m$ будут обозначаться буквами римского стиля (напр., x, A), а векторы длины $n = 2^m$ и производные от них, а также связанные с такими векторами матрицы, будут обозначаться полужирными буквами (напр., $\mathbf{v}, \mathbf{B}$).

Порождающей матрицей линейного кода $C \subseteq \mathbb{F}_2^n$ называется матрица $\mathbf{G}$, составленная из векторов произвольного базиса кода C. *Проверочной матрицей* кода C называется такая матрица $\mathbf{H}$ полного ранга, для которой выполняется соотношение $\mathbf{H}\mathbf{x}^\mathbf{T} = \mathbf{0}$ для всех $\mathbf{x} \in C$. *Синдромом* произвольного вектора $\mathbf{x} \in \mathbb{F}_2^n$ называется произведение $\mathbf{s}_\mathbf{x} = \mathbf{H}\mathbf{x}^\mathbf{T}$. Код $C^\perp$, для которого проверочная матрица кода C является порождающей матрицей, называется *двойственным кодом* к C.

Пусть f и g — две булевы функции от m переменных. Обозначим через $L_{\mathrm{A}}^{\mathrm{b}} : \mathbb{F}_2^m \to \mathbb{F}_2^m$ аффинное преобразование переменных с использованием матрицы A и вектора b:

$$(f \circ L_{\mathrm{A}}^{\mathrm{b}})(\mathrm{x}) = f(\mathrm{A}\mathrm{x} + \mathrm{b}).$$

Здесь $\circ$ обозначает операцию композиции двух отображений. В случае, когда вектор b равен нулю, он будет опущен из записи.

Функции f и g называются *линейно эквивалентными*, если одна может быть получена из другой при помощи невырожденного линейного преобразования переменных, т.е. $f = g \circ L_{\mathrm{A}}$, где $\det \mathrm{A} \neq 0$.

При классификации булевых функций более часто встречается *расширенная аффинная (extended affine) эквивалентность*: функции f и g называются EA-*эквивалентными*, если существует невырожденная двоичная матрица A, двоичный вектор b длины m и функция h степени не выше 1 такие, что $f = g \circ L_{\mathrm{A}}^{\mathrm{b}} + h$.

В данной главе используется вариант двух вышеупомянутых эквивалентностей. Назовём функции f и g EL^k-*эквивалентными*, если существует невырожденная двоичная матрица A и функция h степени, не превышающей k, такие, что

$$f = g \circ L_{\mathrm{A}} + h.$$

Легко видеть, что данное отношение действительно является отношением эквивалентности. EL^k-эквивалентность двух функций f и g мы будем обозначать $f \overset{k}{\sim} g$. Мы также будем писать $f \overset{k}{=} g$ в случае, когда степень функции $f + g$ не превышает k. Заметим, что последнее отношение является подмножеством отношения EL^k-эквивалентности.

Произведение всех m переменных, кроме x_i, мы будем обозначать $\overline{x_i}$, а произведение всех m переменных, кроме x_i и x_j, мы будем обозначать $\overline{x_i x_j}$.

Код Рида-Маллера порядка k от m переменных обычно обозначается как $\mathcal{RM}(k,m)$. Поскольку коды данного семейства будут достаточно часто упоминаться в данной главе, мы будем использовать обозначение $\mathcal{R}_{k,m}$ для кода Рида-Маллера порядка k от m переменных. Количество переменных будет опущено, если оно обозначается переменной m.

5.2 Код Рида-Маллера $\mathcal{R}_{1,5}$

Рассмотрим частный случай — код $\mathcal{R}_{1,5}$. Этот код является множеством аффинных функций, однако от нечётного числа переменных, поэтому резуль-

тат Н. Токаревой о метрической регулярности множества бент-функций его не охватывает.

В 1972 году Э. Берлекэмп и Л. Уэлш представили разбиение пространства $\mathbb{F}_2^{32}$ (пространство векторов значений функций от 5 переменных) на 48 классов EA-эквивалентности и вычислили распределения весов векторов для каждого из классов [3]. Код $\mathcal{R}_{1,5}$ является классом функций, EA-эквивалентных нулевой функции. Наибольший из наименьших весов функций класса среди всех классов — т.е. радиус покрытия $\mathcal{R}_{1,5}$ — равен 12, и достигается на четырёх классах (классы 14, 22, 26 и 28 в таблице 1). Эти четыре класса составляют метрическое дополнение кода $\mathcal{R}_{1,5}$. Верна следующая теорема.

Теорема 5.1. *Код $\mathcal{R}_{1,5}$ является метрически регулярным.*

Доказательство. Поскольку код $\mathcal{R}_{1,5}$ линеен, то $\rho(\widehat{\mathcal{R}}_{1,5}) = \rho(\mathcal{R}_{1,5}) = 12$ и $f \in \widehat{\widehat{\mathcal{R}}}_{1,5}$ тогда и только тогда, когда $f + \widehat{\mathcal{R}}_{1,5} = \widehat{\mathcal{R}}_{1,5}$ (см. теорему 4.7 в главе 4). Следовательно, для того, чтобы установить метрическую регулярность кода $\mathcal{R}_{1,5}$, нам необходимо доказать, что для всякой функции $f \notin \mathcal{R}_{1,5}$ имеет место $f + \widehat{\mathcal{R}}_{1,5} \neq \widehat{\mathcal{R}}_{1,5}$.

Поскольку радиус покрытия кода $\mathcal{R}_{1,5}$ чётен, его второе метрическое дополнение может состоять лишь из классов эквивалентности с кодовыми словами чётного веса. Существует 29 таких классов, включая сам код $\mathcal{R}_{1,5}$; они перечислены в таблице 1. Классы, помеченные надстрочным символом, составляют метрическое дополнение $\widehat{\mathcal{R}}_{1,5}$. Данная классификация была получена Э. Берлекэмпом и Л. Уэлшем [3], однако в представленной таблице некоторые представители классов эквивалентности были изменены при помощи простых переименований переменных (найти оригинальные представители читатель может в таблице 5 в приложении A).

Покажем, что только функции из кода $\mathcal{R}_{1,5}$ содержатся во втором метрическом дополнении. Пусть $f_c \notin \mathcal{R}_{1,5}$ — функция из некоторого класса эквивалентности C, отличного от кода $\mathcal{R}_{1,5}$. Предположим, что функция $(f_c + g_c)$ для некоторой $g_c \in \widehat{\mathcal{R}}_{1,5}$ не содержится ни в каком из четырёх классов, составляющих метрическое дополнение $\widehat{\mathcal{R}}_{1,5}$. Это означает, что $f_c + \widehat{\mathcal{R}}_{1,5} \neq \widehat{\mathcal{R}}_{1,5}$, и, следовательно, f_c не содержится во втором метрическом дополнении кода $\mathcal{R}_{1,5}$.

Пусть теперь $f \notin \mathcal{R}_{1,5}$ — произвольная функция из того же класса C, что и f_c, и пусть $(\mathrm{A},\mathrm{b},h)$ — матрица, вектор и аффинная функция такие, что

$$f = f_c \circ L_{\mathrm{A}}^{\mathrm{b}} + h.$$

№	Представитель f	Прибавленная $g \in \widehat{\mathcal{R}}_{1,5}$	$C(g)$	Сумма $h = f + g$	$C(h)$
0	0	—	—	—	—
1	2345	123+14+25	22	2345+123+14+25	12
2	2345+14	123+14+25	22	2345+123+25 ∼ 2345+123+34	8
3	2345+24	2345+123+24+35	14	123+35 ∼ 123+14	21
4	2345+24+35	2345+123+24+35	14	123	19
5	2345+14+25	123+14+25	22	2345+123	6
6	2345+123	123+14+25	22	2345+14+25	5
7	2345+123+12	12+34	28	2345+123+34	8
8	2345+123+34	12+34	28	2345+123+12	7
9	2345+123+14	14+25	28	2345+123+25 ∼ 2345+123+34	8
10	2345+123+45	12+45	28	2345+123+12	7
11	2345+123+12+34	12+34	28	2345+123	6
12	2345+123+14+25	123+14+25	22	2345	1
13	2345+123+12+45	12+45	28	2345+123	6
14^1	2345+123+24+35	2345+123+24+35	14	0	0
15	2345+123+145	123+14+25	22	2345+145+14+25 ∼ 2345+123+12+34	11
16	2345+123+145+45	123+145+45+24+35	26	2345+24+35	4
17	2345+123+145+24+45	2345+123+24+35	14	145+35+45 ∼ 123+14	21
18	2345+123+145+24+35	2345+123+24+35	14	145 ∼ 123	19
19	123	2345+123+24+35	14	2345+24+35	4
20	123+45	2345+123+24+35	14	2345+24+35+45 ∼ 2345+24+35	4
21	123+14	123+14+25	22	25 ∼ 12	27
22^2	123+14+25	123+14+25	22	0	0
23	123+145	123+14+25	22	145+14+25 ∼ 145+25 ∼ 123+14	21
24	123+145+23	23+45	28	123+145+45 ∼ 123+145+23	24
25	123+145+24	123+15+24	22	145+15 ∼ 123	19
26^3	123+145+45+24+35	123+145+45+24+35	26	0	0
27	12	12+34	28	34 ∼ 12	27
28^4	12+34	12+34	28	0	0

Таблица 1 — Таблица классов EA-эквивалентности функций от 5 переменных, которые содержат функции чётного веса, с соответствующими представителями. Классы, помеченные надстрочным символом, составляют $\widehat{\mathcal{R}}_{1,5}$. $C(\cdot)$ обозначает номер класса, к которому принадлежит функция. Функции в таблице представлены в сокращённом виде: число $i_1 i_2 \dots i_k$ обозначает моном $x_{i_1} x_{i_2} \dots x_{i_k}$. Например, представителем класса 14 является функция $x_2x_3x_4x_5 + x_1x_2x_3 + x_2x_4 + x_3x_5$.

Положим

$$g_f = g_c \circ L_{\mathrm{A}}^{\mathrm{b}} + h.$$

Тогда функция $f + g_f$ EA-эквивалентна функции $f_c + g_c$, и, следовательно, она не принадлежит $\widehat{\mathcal{R}}_{1,5}$. По построению, функция g_f принадлежит $\widehat{\mathcal{R}}_{1,5}$. Отсюда следует, что $f + \widehat{\mathcal{R}}_{1,5} \neq \widehat{\mathcal{R}}_{1,5}$ и что $f \notin \widehat{\widehat{\mathcal{R}}}_{1,5}$.

Таким образом, если мы докажем, что $(f + g) \notin \widehat{\mathcal{R}}_{1,5}$ для некоторой функции $f \in C$ и некоторой функции $g \in \widehat{\mathcal{R}}_{1,5}$, то мы докажем, что никакая функция из класса C не содержится во втором метрическом дополнении.

Доказательство данного факта содержится в таблице 1: для представителя f из каждого класса эквивалентности с функциями чётного веса мы находим функцию $g \in \widehat{\mathcal{R}}_{1,5}$ такую, что $(f + g)$ эквивалентна представителю некоторого класса эквивалентности, не содержащегося в $\widehat{\mathcal{R}}_{1,5}$. Следовательно, лишь сам код $\mathcal{R}_{1,5}$ содержится во втором метрическом дополнении $\widehat{\widehat{\mathcal{R}}}_{1,5}$, что доказывает его метрическую регулярность. □

Почти все эквивалентности, представленные в пятом столце таблицы 1, являются переименованиями переменных или простыми заменами вида $x_i \to x_i + 1$, $x_i \to x_i + x_j$ или (для группы 20) $x_i \to x_i + x_j + x_k$ для некоторых i,j,k.

5.3 Коды Рида-Маллера порядков 0, m, $m-1$ и $m-2$

Коды Рида-Маллера порядков 0, m and $m-1$ совпадают с кодом повторений, со всем пространством и с кодом чётных слов соответственно. Очевидно, что все эти коды метрически регулярны.

Радиус покрытия кода Рида-Маллера порядка $m-2$ равен 2 [9]. По определению, этот код состоит из всех булевых функций степени не выше $m-2$. Поскольку функции степени m имеют нечётный вес, а функции меньших степеней имеют чётный вес, функции степени m находятся на расстоянии 1 от $\mathcal{R}_{m-2}$, в то время как функции степени $m-1$ находятся на расстоянии 2. Следовательно,

$$\widehat{\mathcal{R}}_{m-2} = \mathcal{R}_{m-1} \setminus \mathcal{R}_{m-2}.$$

Поскольку код $\mathcal{R}_{m-2}$ линеен, $\rho(\widehat{\mathcal{R}}_{m-2}) = \rho(\mathcal{R}_{m-2}) = 2$, откуда из тех же соображений чётности следует, что функции степени m находятся на расстоянии 1 от $\widehat{\mathcal{R}}_{m-2}$. Следовательно, $\widehat{\widehat{\mathcal{R}}}_{m-2} = \mathcal{R}_{m-2}$ и код $\mathcal{R}_{m-2}$ метрически регулярен.

5.4 Коды Рида-Маллера порядка $m-3$: метод синдромных матриц

Рассмотрим коды Рида-Маллера порядка $m-3$. А. МакЛафлин [30] показал, что

$$\rho(\mathcal{R}_{m-3}) = \begin{cases} m+1, & \text{если } m \text{ нечётно,} \\ m+2, & \text{если } m \text{ чётно.} \end{cases}$$

Мы вновь установим этот результат, следуя книге “Covering codes” Дж. Коэна и др., поскольку полученные в данной главе новые результаты опираются на методы и терминологию, используемые в книге. В частности, мы опишем метод вычисления радиуса покрытия кода $\mathcal{R}_{m-3}$, использующий биективное отображение между синдромами векторов и симметричными матрицами, как он представлен в книге, однако с небольшими изменениями. Затем мы приступим к изучению метрического дополнения кода $\mathcal{R}_{m-3}$. Результаты в разделах 5.4 и 5.5, как и общие результаты, касающиеся радиуса покрытия кода $\mathcal{R}_{m-3}$, принадлежат Коэну и др. [9] (С. 248–250), в то время как все последующие результаты, касающиеся метрического дополнения и метрической регулярности кода, являются новыми.

Найдём сначала радиус покрытия выколотого кода Рида-Маллера $\mathcal{R}^{\circ}_{m-3}$, т.е. кода без нулевой координаты, которая соответствует значению функций на нулевом векторе. Расстояние от произвольного вектора $\mathbf{v} \in \mathbb{F}_2^{n-1}$ до данного кода равно наименьшему из весов векторов, лежащих в смежном классе, который соответствует данному вектору:

$$d(\mathbf{v},\mathcal{R}^{\circ}_{m-3}) = \min_{\mathbf{u}\,:\,\mathbf{u}\in\mathbf{v}+\mathcal{R}^{\circ}_{m-3}} wt(\mathbf{u}).$$

Известно, что два вектора лежат в одном и том же смежном классе кода если и только если синдромы этих векторов совпадают. Следовательно, расстояние от вектора до кода можно записать в следующем виде:

$$d(\mathbf{v},\mathcal{R}^{\circ}_{m-3}) = \min_{\mathbf{u}\,:\,\mathbf{s}_{\mathbf{u}}=\mathbf{s}_{\mathbf{v}}} wt(\mathbf{u}).$$

Поскольку $\mathcal{R}_{m-3}$ является двойственным кодом к $\mathcal{R}_2$, в качестве проверочной матрицы $\mathbf{H}$ кода $\mathcal{R}^{\circ}_{m-3}$ мы можем выбрать матрицу размера $\frac{m(m+1)}{2} \times (n-1)$, состоящую из выколотых векторов значений функций

$$x_1, \ldots, x_m, x_1x_2, x_1x_3, \ldots, x_{m-1}x_m.$$

Представим синдром $\mathbf{s_v} = \mathbf{Hv^T}$ произвольного вектора $\mathbf{v} \in \mathbb{F}_2^{n-1}$ в виде симметричной матрицы $\mathbf{S_v} = (s_{i,j})$ размера $m \times m$. Элемент $s_{i,j}$ данной матрицы положим равным компоненте синдрома $\mathbf{s_v}$, которая соответствует строке функции x_ix_j в проверочной матрице $\mathbf{H}$. Диагональный элемент $s_{i,i}$ положим равным компоненте синдрома, соответствующей строке функции x_i в матрице $\mathbf{H}$. Таким образом, мы построили биекцию между множеством всех синдромов (смежных классов) кода $\mathcal{R}^{\circ}_{m-3}$ и множеством всех симметричных двоичных матриц размера $m \times m$.

Пусть $\mathbf{e_1^{\circ}}, \ldots \mathbf{e_m^{\circ}} \in \mathbb{F}_2^{n-1}$ — выколотые векторы значений функций $x_1, \ldots, x_m$. Заметим, что строка матрицы $\mathbf{H}$, соответствующая функции x_ix_j, равна покомпонентному произведению векторов $\mathbf{e_i^{\circ}} * \mathbf{e_j^{\circ}}$.

Рассмотрим матрицу $\mathbf{B_v}$ размера $m \times (n-1)$, i-ая строка которой равна вектору $\mathbf{e_i^{\circ}} * \mathbf{v}$. Нетрудно видеть, что симметричная матрица $\mathbf{S_v} = \mathbf{B_v B_v^T}$ соответствует синдрому $\mathbf{s_v}$ вектора $\mathbf{v}$ по описанному выше отображению. Заметим также, что количество ненулевых столбцов матрицы $\mathbf{B_v}$ равно весу Хэмминга вектора $\mathbf{v}$.

Используя установленное соответствие между синдромами и симметричными матрицами, мы можем записать расстояние от вектора до кода в следующем виде:

$$d(\mathbf{v}, \mathcal{R}^{\circ}_{m-3}) = \min_{\mathbf{u}:\mathbf{B_u B_u^T} = \mathbf{S_v}} wt(\mathbf{u}) = \min_{\mathbf{u}:\mathbf{B_u B_u^T} = \mathbf{S_v}} Col(\mathbf{B_u}),$$

где $Col(\mathbf{B_u})$ — количество ненулевых столбцов матрицы $\mathbf{B_u}$. Обозначим минимум в правой части равенства через $t(\mathbf{S})$:

$$t(\mathbf{S}) := \min_{\mathbf{u}:\mathbf{B_u B_u^T} = \mathbf{S}} Col(\mathbf{B_u}).$$

Тогда

$$d(\mathbf{v}, \mathcal{R}^{\circ}_{m-3}) = t(\mathbf{S_v}),$$

и, поскольку соответствие между синдромами и симметричными матрицами биективно, мы получаем, что

$$\rho(\mathcal{R}^{\circ}_{m-3}) = \max_{\mathbf{v}} d(\mathbf{v}, \mathcal{R}^{\circ}_{m-3}) = \max_{\mathbf{S}} t(\mathbf{S}).$$

Здесь максимум берётся по всем симметричным $m \times m$ матрицам $\mathbf{S}$. Более того, вектор $\mathbf{v}$ содержится в метрическом дополнении $\widehat{\mathcal{R}}^{\circ}_{m-3}$ тогда и только тогда, когда $t(\mathbf{S_v}) = \rho(\mathcal{R}^{\circ}_{m-3})$.

Будем называть всякую матрицу $\mathbf{B}$ такую, что $\mathbf{BB^T} = \mathbf{S}$, *фактором* матрицы $\mathbf{S}$. Тогда величину $t(\mathbf{S})$ можно описать как наименьшее количество ненулевых столбцов в факторе среди всех факторов матрицы $\mathbf{S}$ вида $\mathbf{B_u}$, где $\mathbf{u} \in \mathbb{F}_2^{n-1}$. Мы будем называть *минимальным фактором* любой фактор, на котором достигается этот минимум.

Расширим теперь определение величины $t(\mathbf{S})$.

Лемма 5.2 (см. [9], С. 250)**.** *Пусть* $\mathbf{S}$ *— симметричная матрица, а* $\mathbf{B}$ *— её фактор (т.е.* $\mathbf{BB^T} = \mathbf{S}$*). Следующие операции над матрицей* $\mathbf{B}$ *оставляют её фактором матрицы* $\mathbf{S}$*:*

1. *удаление нулевого столбца;*
2. *удаление двух одинаковых столбцов;*
3. *перестановка столбцов в матрице;*
4. *добавление произвольного вектора* b *к каждому столбцу некоторого подмножества столбцов матрицы* $\mathbf{B}$ *чётной мощности при условии, что сумма всех столбцов этого подмножества равна нулевому вектору.*

Поскольку среди множеств всех ненулевых столбцов матриц $\mathbf{B_u}$, где $\mathbf{u} \in \mathbb{F}_2^{n-1}$, встречаются в точности все возможные множества ненулевых столбцов длины m, лемма 5.2 позволяет убрать все нулевые столбцы из допустимых факторов и тем самым переформулировать определение величины $t(\mathbf{S})$ следующим образом, допуская использование матриц произвольных размеров:

Определение 2. *Величина* $t(\mathbf{S})$ *равна наименьшему количеству столбцов в факторе матрицы* $\mathbf{S}$ *среди всех возможных факторов. Любой фактор, достигающий этого значения, называется минимальным фактором матрицы* $\mathbf{S}$*.*

Заметим, что всякий фактор $\mathbf{B}$ матрицы $\mathbf{S}$ соответствует в точности одному фактору исходного вида $\mathbf{B_u}$ — такому, множество ненулевых столбцов которого совпадает с множеством ненулевых столбцов матрицы $\mathbf{B}$. Следовательно, предъявление любого минимального фактора симметричной матрицы $\mathbf{S}$ позволяет найти лидера $\mathbf{u}$ смежного класса, для которого $\mathbf{S} = \mathbf{S_u}$.

5.5 Коды Рида-Маллера порядка $m-3$: радиус покрытия

Для того, чтобы определить радиус покрытия кода $\mathcal{R}^{\circ}_{m-3}$, найдём наибольшее возможное значение величины $t(\mathbf{S})$. Очевидно, что

$$t(\mathbf{S}) \geqslant \min_{\mathbf{B}:\mathbf{B}\mathbf{B}^{\mathbf{T}}=\mathbf{S}} \operatorname{rank}(\mathbf{B}) \geqslant \operatorname{rank}(\mathbf{S})$$

для любой матрицы $\mathbf{S}$. Следовательно,

$$\max_{\mathbf{S}} t(\mathbf{S}) \geqslant m.$$

Таким образом, мы получили тривиальную нижнюю оценку. Следующее утверждение позволяет получить оценку сверху:

Лемма 5.3 (см. [9], С. 250)**.** *Пусть* $\mathbf{S}$ *— симметричная матрица, и пусть* $\mathbf{B}$ *— произвольный минимальный фактор матрицы* $\mathbf{S}$*. Тогда все собственные подмножества столбцов матрицы* $\mathbf{B}$ *линейно независимы.*

Доказательство. Предположим, что в факторе $\mathbf{B}$ существует собственное подмножество столбцов, сумма которых равна нулю. Если в этом подмножестве содержится нечётное число векторов, то мы добавим в него (и в матрицу $\mathbf{B}$, при этом оставляя её фактором $\mathbf{S}$ по лемме 5.2) столбец из нулей.

Обозначим за $\bar{\mathbf{B}}$ матрицу, составленную из столбцов данного подмножества. Теперь, при необходимости меняя местами столбцы, матрицу $\mathbf{B}$ можно представить в виде конкатенации двух матриц: $\mathbf{B} = (\bar{\mathbf{B}}, \mathbf{D})$, причём $\bar{\mathbf{B}}$ содержит чётное количество столбцов, сумма которых равна нулю, в то время как $\mathbf{D}$ является матрицей, состоящей из всех оставшихся столбцов матрицы $\mathbf{B}$.

Пусть $\mathbf{b}^1$ и $\mathbf{d}^1$ — первые ненулевые столбцы матриц $\bar{\mathbf{B}}$ и $\mathbf{D}$ соответственно. Добавим столбец $\mathbf{b}^1 + \mathbf{d}^1$ ко всем столбцам матрицы $\bar{\mathbf{B}}$ — по лемме 5.2, такое преобразование не повлияет на свойство матрицы $\mathbf{B}$ быть фактором матрицы $\mathbf{S}$. Теперь первые ненулевые столбцы матриц $\bar{\mathbf{B}}$ и $\mathbf{D}$ совпадают, и мы можем удалить их из матрицы $\mathbf{B}$, вновь используя лемму 5.2.

Таким образом, мы добавили не более одного столбца к фактору $\mathbf{B}$, а затем убрали из него два столбца. В результате мы получили фактор матрицы $\mathbf{S}$, содержащий меньшее количество столбцов, чем исходный фактор $\mathbf{B}$, что противоречит его минимальности. □

Следствие 5.4 (см. [9], С. 250)**.** *Величина* $t(\mathbf{S})$ *не превосходит* $m+1$ *для любой симметричной матрицы* $\mathbf{S}$ *размера* $m \times m$.

Доказательство. Предположим, что для некоторой симметричной матрицы $\mathbf{S}$ выполняется $t(\mathbf{S}) \geqslant m+2$. По определению это означает, что любой минимальный фактор $\mathbf{B}$ матрицы $\mathbf{S}$ содержит как минимум $m+2$ столбца. Следовательно, он содержит собственное линейно зависимое подмножество столбцов, что противоречит лемме 5.3. □

Доказательства леммы 5.3 и следствия 5.4 приведены здесь для полноты результатов, поскольку в книге [9] данные утверждения не сформулированы явно. Из полученных верхней и нижней оценок мы можем заключить, что наибольшее возможное значение величины $t(\mathbf{S})$ может быть равно либо m, либо $m+1$. Следующий результат описывает матрицы, обладающие большим из данных двух значений.

Лемма 5.5 (см. [9], С. 249)**.** *Пусть* $\mathbf{S}$ *— произвольная симметричная матрица. Тогда* $t(\mathbf{S}) = m+1$ *тогда и только тогда, когда* $\operatorname{rank}(\mathbf{S}) = m$ *и диагональ матрицы* $\mathbf{S}$ *состоит из нулей.*

Доказательство. ($\Longleftarrow$) Предположим, что матрица $\mathbf{S}$ невырождена и имеет нулевую диагональ, и пусть $\mathbf{B}$ — произвольный фактор матрицы $\mathbf{S}$. Заметим, что вектор, состоящий из всех диагональных элементов матрицы $\mathbf{S}$, является суммой всех столбцов матрицы $\mathbf{B}$. Следовательно, сумма всех столбцов матрицы $\mathbf{B}$ равна нулю, а значит, множество всех ненулевых столбцов этой матрицы линейно зависимо. Поскольку $\operatorname{rank}(\mathbf{B}) \geqslant \operatorname{rank}(\mathbf{S}) = m$, матрица $\mathbf{B}$ содержит как минимум $m+1$ ненулевых столбцов, и, следовательно, $t(\mathbf{S}) = m+1$.

($\Longrightarrow$) Предположим, что $t(\mathbf{S}) = m+1$. Пусть $\mathbf{B}$ — минимальный фактор матрицы $\mathbf{S}$. Заметим, что все собственные подмножества столбцов матрицы $\mathbf{B}$ линейно независимы (по лемме 5.3), поэтому сумма всех столбцов матрицы $\mathbf{B}$ должна быть равна нулю. Так как вектор, состоящий из диагональных элементов матрицы $\mathbf{S}$, является суммой всех столбцов матрицы $\mathbf{B}$, матрица $\mathbf{S}$ имеет нулевую диагональ.

Предположим, что $\operatorname{rank}(\mathbf{S}) < m$. Тогда существует подмножество строк матрицы $\mathbf{S}$, сумма которых равна $\mathbf{0}$; обозначим эти строки как $\mathbf{S_{i_1}}, \mathbf{S_{i_2}}, \ldots, \mathbf{S_{i_p}}$. Поскольку $\mathbf{S_i} = \mathbf{B_i B^T}$, мы имеем следующее равенство:

$$(\mathbf{B_{i_1}} + \ldots + \mathbf{B_{i_p}})\mathbf{B^T} = \mathbf{0}. \tag{5.1}$$

Рассмотрим вектор $\mathbf{b} := \mathbf{B}_{\mathbf{i}_1} + \ldots + \mathbf{B}_{\mathbf{i}_p}$.

Если вектор $\mathbf{b}$ равен нулю, то $\mathrm{rank}(\mathbf{B}) < m$ и матрица $\mathbf{B}$ содержит линейно зависимое собственное подмножество столбцов, что противоречит лемме 5.3.

Если $\mathbf{b}$ отличен от нуля и от вектора, состоящего из единиц, то по 5.1 сумма всех столбцов матрицы $\mathbf{B}$, соответствующих единицам в векторе $\mathbf{b}$, равна нулю, что вновь противоречит лемме 5.3.

Предположим, что вектор $\mathbf{b}$ состоит из единиц.

Если m чётно, то количество столбцов в матрице $\mathbf{B}$ нечётно, откуда $\mathbf{b}\mathbf{b}^{\mathbf{T}} = 1$. Это противоречит равенству 5.1, поскольку $\mathbf{b}$ является суммой некоторых строк матрицы $\mathbf{B}$.

Если же m нечётно, то количество столбцов в матрице $\mathbf{B}$ чётно, и, в то же время, все строки содержат чётное количество единиц, поскольку сумма всех столбцов равна нулю по 5.1. Тогда, по лемме 5.2, мы можем прибавить произвольный столбец матрицы $\mathbf{B}$ ко всем её столбцам и затем удалить нулевой столбец из получившейся матрицы. Тем самым мы получим новый фактор матрицы $\mathbf{S}$ с меньшим количеством столбцов, чем в исходном факторе $\mathbf{B}$, что противоречит его минимальности.

Таким образом, $\mathrm{rank}(\mathbf{S})$ равен m.

□

Заметим, что матрица $\mathbf{S}$, обладающая свойствами, описанными в условиях леммы (невырожденная с нулевой диагональю), существует тогда и только тогда, когда m чётно (см. [9], С. 249). Это означает, что

$$\max_{\mathbf{S}} t(\mathbf{S}) = \begin{cases} m, & \text{если } m \text{ нечётно,} \\ m+1, & \text{если } m \text{ чётно.} \end{cases}$$

5.6 Коды Рида-Маллера порядка $m-3$: m чётно

Результаты, представленные в данном разделе, являются новыми и опубликованы в работах [58, 59, 63, 64].

5.6.1 Радиус покрытия и метрическое дополнение выколотого кода

Пусть число переменных m чётно. В предыдущем разделе, следуя [9], мы установили, что в этом случае

$$\rho(\mathcal{R}^{\circ}_{m-3}) = \max_{\mathbf{S}} t(\mathbf{S}) = m + 1.$$

Вектор $\mathbf{v} \in \mathbb{F}_2^{m-1}$ содержится в метрическом дополнении кода $\mathcal{R}^{\circ}_{m-3}$ тогда и только тогда, когда $t(\mathbf{S}_{\mathbf{v}}) = m + 1$. Следующее утверждение описывает факторы синдромных матриц таких векторов.

Лемма 5.6 (см. [59]). *Пусть* $\mathbf{S}$ *— симметричная матрица размера* $m \times m$, m *чётно. Тогда* $t(\mathbf{S}) = m + 1$ *тогда и только тогда, когда для матрицы* $\mathbf{S}$ *существует фактор* $\mathbf{B}$ *ранга* m, *состоящий из* $m + 1$ *столбцов, сумма которых равна нулю.*

Доказательство. ($\Longrightarrow$) Предположим, что $t(\mathbf{S}) = m+1$ и пусть $\mathbf{B}$ — произвольный минимальный фактор матрицы $\mathbf{S}$. По лемме 5.5, $\mathrm{rank}(\mathbf{S}) = m$ и диагональ матрицы $\mathbf{S}$ состоит из нулей. Следовательно, $\mathrm{rank}(\mathbf{B}) = m$ и сумма всех столбцов матрицы равна нулю.

($\Longleftarrow$) Пусть $\mathbf{B}$ — фактор матрицы $\mathbf{S}$ ранга m, состоящий из $m+1$ столбцов, сумма которых равна нулю.

Предположим, что $t(\mathbf{S}) = k \leqslant m$ и пусть $\mathbf{D}$ — некоторый минимальный фактор матрицы $\mathbf{S}$, состоящий из k столбцов. Поскольку сумма всех столбцов фактора равна вектору, состоящему из диагональных элементов матрицы $\mathbf{S}$, сумма всех столбцов матрицы $\mathbf{D}$ равна нулю. Отсюда следует, что $\mathrm{rank}(\mathbf{D}) < m$, а значит и $\mathrm{rank}(\mathbf{S}) < m$.

Легко видеть, что всякое собственное подмножество столбцов матрицы $\mathbf{B}$ линейно независимо. Заметим, что существование фактора с данным свойством противоречит предположению “$\mathrm{rank}(\mathbf{S}) < m$”, что было показано в доказательстве леммы 5.5, причём, в случае чётного m, доказательство не опирается на минимальность фактора $\mathbf{B}$.

Следовательно, $\mathrm{rank}(\mathbf{S}) = m$ и $t(\mathbf{S}) = m + 1$, то есть $\mathbf{B}$ является минимальным фактором матрицы $\mathbf{S}$.

□

Легко видеть, что лемма 5.6 описывает в точности все минимальные факторы всех матриц $\mathbf{S}$, для которых $t(\mathbf{S})$ равно $m+1$. Рассмотрим следующее множество векторов:

$$\mathrm{U} = \{\mathbf{u} \in \mathbb{F}_2^{n-1} : \mathbf{B_u} \text{ содержит ровно } m+1 \text{ ненулевых столбцов, среди которых } m \text{ линейно независимы и сумма всех столбцов равна нулю}\}. \quad (5.2)$$

Нетрудно показать, что множество матриц $\{\mathbf{B_u} : \mathbf{u} \in \mathrm{U}\}$ (с точностью до перестановки столбцов и удаления нулевых столбцов) содержит в точности все минимальные факторы, описанные в лемме 5.6.

Иными словами, если $t(\mathbf{S}) = m+1$ для некоторой матрицы $\mathbf{S}$, то существует вектор $\mathbf{u} \in \mathrm{U}$ такой, что $\mathbf{S} = \mathbf{B_u}\mathbf{B_u^T}$. Обратно, для всякого вектора $\mathbf{u} \in \mathrm{U}$ выполняется $t(\mathbf{B_u}\mathbf{B_u^T}) = m+1$. Таким образом, векторы из множества U покрывают все возможные смежные классы кода $\mathcal{R}^{\circ}_{m-3}$, содержащиеся в метрическом дополнении:

$$\widehat{\mathcal{R}}^{\circ}_{m-3} = \bigcup_{\mathbf{u}\in\mathrm{U}} (\mathbf{u} + \mathcal{R}^{\circ}_{m-3}).$$

5.6.2 Радиус покрытия и метрическое дополнение невыколотого кода

Мы нашли радиус покрытия и описали метрическое дополнение выколотого кода. Вернёмся теперь к обычному, невыколотому коду Рида-Маллера $\mathcal{R}_{m-3}$. Поскольку данный код получается из выколотого добавлением проверки на чётность в начало всех кодовых слов, нам пригодится следующий результат:

Лемма 5.7 (см. [59]). *Пусть C — код с радиусом покрытия r и метрическим дополнением $\widehat{C}$. Пусть C_π — код, полученный из C добавлением проверки на чётность ко всем кодовым словам кода C. Тогда $\rho(C_\pi) = r+1$ и $\widehat{C}_\pi$ состоит из всех векторов множества $\widehat{C}$, с добавленной*

1. *проверкой на чётность в случае, если r нечётно;*
2. *проверкой на нечётность в случае, если r чётно.*

Доказательство. Очевидно, что $\rho(C_\pi) \leqslant r+1$.

Докажем случай (2). Предположим, что r чётно. Обозначим

$$C_i = \{c \in C : wt(c) \bmod 2 = i\},\ \widehat{C}_i = \{c \in \widehat{C} : wt(c) \bmod 2 = i\},\ i = 0,1.$$

Поскольку r чётно, векторы из множества $\widehat{C}_0$ находятся на расстоянии r от C_0 и на большем расстоянии от C_1. Аналогично, векторы из $\widehat{C}_1$ находятся на расстоянии r от C_1 и на большем расстоянии от C_0.

Пусть $c' = (\varepsilon, c)$, где $c \notin \widehat{C}$ и $\varepsilon \in \{0,1\}$. Тогда $d(c', C_\pi) \leqslant d(c, C) + 1 \leqslant r$.

Пусть $c \in \widehat{C}_1$. Тогда $d((1,c), C_\pi) = \min(d(c, C_1), d(c, C_0)+1) = r$, в то время как $d((0,c), C_\pi) = \min(d(c, C_1) + 1, d(c, C_0)) > r$.

Если $c \in \widehat{C}_0$, то, аналогично, $d((1,c), C_\pi) = \min(d(c, C_1), d(c, C_0) + 1) > r$, в то время как $d((0,c), C_\pi) = \min(d(c, C_1) + 1, d(c, C_0)) = r$.

Следовательно, векторы из объединения $\{(1,c) \,|\, c \in \widehat{C}_0\} \cup \{(0,c) \,|\, c \in \widehat{C}_1\}$ и только они находятся на расстоянии, превышающем r, от множества C_π. Это расстояние может быть равно только $r + 1$. Случай (2) доказан.

Доказательство случая (1) полностью аналогично и получается из вышеприведённого сменой некоторых множеств C_i,$\widehat{C}_i$ местами.

□

Используя данную лемму, мы можем заключить, что радиус покрытия невыколотого кода Рида-Маллера $\mathcal{R}_{m-3}$ при чётном числе переменных равен $m + 2$, а его метрическое дополнение описывается следующим выражением:

$$\widehat{\mathcal{R}}_{m-3} = \bigcup_{\mathbf{u} \in \mathrm{U}} \left((\pi(\mathbf{u}), \mathbf{u}) + \mathcal{R}_{m-3} \right),$$

где множество U определяется формулой 5.2 из предыдущего подраздела.

Пусть $f_{\mathbf{v}}$ обозначает функцию, соответствующую невыколотому вектору значений $\mathbf{v} \in \mathbb{F}_2^n$. Напомним, что матрица $\mathbf{B}_{\mathbf{v}^\circ}$ размера $m \times (n-1)$ определяется как набор строк $\mathbf{e}_\mathbf{i}^\circ * \mathbf{v}^\circ$, где $\mathbf{e}_\mathbf{i}^\circ$ — выколотый вектор значений функции x_i. Легко показать, что множество всех ненулевых столбцов матрицы $\mathbf{B}_{\mathbf{v}^\circ}$ в точности совпадает с носителем функции $f_{\mathbf{v}}$, за исключением, быть может, нулевого вектора.

Поскольку все векторы множества U имеют нечётный вес, а добавленная проверка на чётность соответствует значению функции на нулевом векторе, мы можем описать метрическое дополнение кода $\mathcal{R}_{m-3}$ в терминах функций, а не векторов значений, следующим образом:

$$\widehat{\mathcal{R}}_{m-3} = \bigcup_{g \in G} \left(g + \mathcal{R}_{m-3} \right),$$

где

$$G = \{f_{(1,\mathbf{u})} : \mathbf{u} \in \mathrm{U}\} = \{g : \mathrm{supp}(g) = \{0,\mathrm{x}_1,\mathrm{x}_2 \ldots,\mathrm{x}_m,\mathrm{x}_1 + \ldots + \mathrm{x}_m\},\ \text{где}$$
$$\{\mathrm{x}_1,\ldots,\mathrm{x}_m\}\ \text{линейно независимы}\}.$$

Все функции множества G образуют замкнутый класс относительно линейной эквивалентности. Напомним, что две функции f и g называются EL^k*-эквивалентными*, если существует невырожденная двоичная матрица A и функция h степени, не превышающей k, такие, что $g = f \circ L_{\mathrm{A}} + h$. Из полученного выше представления следует, что функция g содержится в $\widehat{\mathcal{R}}_{m-3}$ тогда и только тогда, когда она EL^{m-3}-эквивалентна некоторой функции из множества G. Поскольку все функции в метрическом дополнении эквивалентны друг другу, мы можем выбрать из него произвольную функцию в качестве представителя эквивалентности, и в дальнейшем мы будем использовать различных представителей. Будем называть EL^{m-3}-эквивалентность просто “эквивалентностью” для краткости.

Предоставим явное описание (АНФ) некоторой функции из G. Обозначим за g' функцию с носителем $\{0,\mathrm{e}_1,\mathrm{e}_2,\ldots,\mathrm{e}_m,1\}$, где $\mathrm{e}_i \in \mathbb{F}_2^m$ — вектор, имеющий единицу лишь в i-ой координате. Очевидно, что $g' \in G$, и построить алгебраическую нормальную форму данной функции нетрудно: она представляет собой сумму всех мономов, содержащих чётное число переменных, за исключением монома максимальной длины:

$$g'(\mathrm{x}) = 1 + \sum_{k=1}^{\frac{m}{2}-1} \sum_{1 \leqslant i_1 < \ldots < i_{2k} \leqslant m} x_{i_1} x_{i_2} \ldots x_{i_{2k}}.$$

Напомним, что $\overline{x_i}$ обозначает произведение всех m переменных, кроме x_i, а $\overline{x_i x_j}$ обозначает произведение всех m переменных, кроме x_i и x_j. Функция g' эквивалентна сумме всех мономов, содержащих $m-2$ переменных, поэтому в дальнейшем мы будем использовать данную функцию в качестве представителя:

$$g^*(\mathrm{x}) := \sum_{1 \leqslant i < j \leqslant m} \overline{x_i x_j}. \tag{5.3}$$

5.6.3 Метрическая регулярность

В предыдущем подразделе мы установили, что

$$\widehat{\mathcal{R}}_{m-3} = \{g : g \overset{m-3}{\sim} g_0\},$$

где g_0 — произвольная функция из класса G (или всего множества $\widehat{\mathcal{R}}_{m-3}$), и построили определённую функцию-представитель этого класса эквивалентности — функцию g^* (5.3).

Поскольку код $\mathcal{R}_{m-3}$ линеен, $\rho(\widehat{\mathcal{R}}_{m-3}) = \rho(\mathcal{R}_{m-3}) = m+2$ и функция f содержится в $\widehat{\widehat{\mathcal{R}}}_{m-3}$ тогда и только тогда, кода $f + \widehat{\mathcal{R}}_{m-3} = \widehat{\mathcal{R}}_{m-3}$. Докажем метрическую регулярность кода $\mathcal{R}_{m-3}$, показав, что никакая функция, кроме тех, которые содержатся в $\mathcal{R}_{m-3}$, не сохраняет $\widehat{\mathcal{R}}_{m-3}$ на месте при её добавлении ко всех функциям метрического дополнения.

Пусть $f \notin \mathcal{R}_{m-3}$. Поскольку множество $\widehat{\mathcal{R}}_{m-3}$ является классом EL^{m-3}-эквивалентности, то для того, чтобы показать, что $f + \widehat{\mathcal{R}}_{m-3} \neq \widehat{\mathcal{R}}_{m-3}$, достаточно показать, что существует функция f' такая, что $f' \overset{m-3}{\sim} f$ и $f' + \widehat{\mathcal{R}}_{m-3} \neq \widehat{\mathcal{R}}_{m-3}$.

Случай 1. Пусть $\deg(f) > m-2$. Поскольку линейное преобразование переменных сохраняет степень функции, то степень любой функции $g \in \widehat{\mathcal{R}}_{m-3}$ равна $m-2$ (как у функции g^*), в то время как $f+g$ имеет более высокую степень. Следовательно, $f+g$ не может быть эквивалентна функции g^*, то есть прибавление функции f не оставляет никакую функцию из метрического дополнения в нём же. Отсюда следует, что f не содержится в $\widehat{\widehat{\mathcal{R}}}_{m-3}$.

Случай 2. Пусть $\deg(f) = m-2$. Такую функцию можно единственным образом представить в следующем виде:

$$f(\mathrm{x}) = \sum_{(i,j)\in I} \overline{x_i x_j} + h(\mathrm{x}),$$

где $\deg(h) < m-2$, а I — некоторое множество пар индексов. Обозначим через $\tilde{f}$ следующую квадратичную функцию:

$$\tilde{f}(\mathrm{x}) := \sum_{(i,j)\in I} x_i x_j.$$

Будем называть $\tilde{f}$ *квадратичной двойственной* к f функцией.

Для введённых двойственных функций справедливо следующее утверждение:

Лемма 5.8. *Пусть f и g — функции степени $m-2$. Тогда $f \overset{m-3}{\sim} g$ тогда и только тогда, когда их квадратичные двойственные функции* EL^1*-эквивалентны (*EA*-эквивалентны).*

Доказательство. Так как EL^{m-3}-эквивалентность позволяет добавлять функции степени вплоть до $m-3$, то без ограничения общности считаем, что как f, так и g, содержат лишь мономы степени $m-2$. В последующих рассуждениях мы будем отбрасывать члены степени ниже $m-2$ при работе с EL^{m-3}-эквивалентностью, а также отбрасывать члены степени ниже 2 при работе с EL^1-эквивалентностью.

Пусть $f(\mathrm{x}) = \sum\limits_{(i,j)\in I} \overline{x_i x_j}$ — АНФ функции f. Рассмотрим следующее простое невырожденное линейное преобразование переменных L_{ij}:

$$L_{ij} : \begin{cases} x_i \leftarrow x_i + x_j, & \\ x_k \leftarrow x_k & \forall k \neq i. \end{cases}$$

Если мы подействуем данным преобразованием на функцию f, то её мономы изменятся следующим образом:

$$L_{ij} : \begin{cases} \overline{x_i x_k} \leftarrow \overline{x_i x_k} & \forall k \neq i, \\ \overline{x_j x_k} \leftarrow \overline{x_j x_k} + \overline{x_i x_k} & \forall k \neq i,j, \\ \overline{x_k x_l} \leftarrow \overline{x_k x_l} & \forall k,l \neq i,j. \end{cases}$$

Пусть $f_1 = f \circ L_{ij}$. Легко видеть, что двойственная функция $\tilde{f}_1$ получается из функции $\tilde{f}$ при помощи следующего линейного преобразования:

$$L_{ji} : \begin{cases} x_j \leftarrow x_j + x_i, & \\ x_k \leftarrow x_k & \forall k \neq j, \end{cases}$$

которое является транспонированием преобразования L_{ij}.

Предположим теперь, что функция g получается из функции f при помощи линейного преобразования L. Преобразование L нетрудно разложить в последовательность простых преобразований:

$$L = L_{i_1 j_1} \circ L_{i_2 j_2} \circ \ldots \circ L_{i_s j_s}.$$

По вышедоказанному, двойственная функция $\tilde{g}$ получается из $\tilde{f}$ при помощи преобразования $\tilde{L}$:

$$\tilde{L} = L_{j_1 i_1} \circ L_{j_2 i_2} \circ \ldots \circ L_{j_s i_s},$$

являющегося последовательностью транспонированных простых преобразований.

Тем самым мы показали, что, если $f \overset{m-3}{\sim} g$, то $\tilde{f} \overset{1}{\sim} \tilde{g}$. Обратное показывается аналогичными рассуждениями.

□

Вернёмся к произвольно выбранной функции f степени $m-2$. Известно, что всякая квадратичная булева функция EA-эквивалентна функции вида $x_1x_2 + x_3x_4 + \ldots + x_{2k-1}x_{2k}$ для некоторого $k \leqslant \frac{m}{2}$, причём любые две функции такого вида, содержащие разное количество переменных, не являются EA-эквивалентными друг другу. Из данного факта и леммы 5.8 следует, что функция f эквивалентна функции p_k для некоторого k $(0 < k \leqslant \frac{m}{2})$, где

$$p_k(\mathrm{x}) = \overline{x_1x_2} + \overline{x_3x_4} + \ldots + \overline{x_{2k-1}x_{2k}} = \sum_{i=1}^{k} \overline{x_{2i-1}x_{2i}}.$$

Легко показать, что g^* эквивалентна $p_{\frac{m}{2}}$. Тогда $p_k + p_{\frac{m}{2}}$ эквивалентна функции $p_{\frac{m}{2}-k}$, которая, по лемме 5.8, неэквивалентна функции $p_{\frac{m}{2}}$, а следовательно, неэквивалентна и функции g^*. Тем самым, $p_k + \widehat{\mathcal{R}}_{m-3} \neq \widehat{\mathcal{R}}_{m-3}$, а значит и эквивалентная функции p_k функция f не содержится в $\widehat{\widehat{\mathcal{R}}}_{m-3}$.

Поскольку все функции, не лежащие в $\mathcal{R}_{m-3}$, имеют степень $m-2$ или выше, то мы доказали тем самым, что никакая из них не содержится во втором метрическом дополнении, и, следовательно, $\mathcal{R}_{m-3}$ метрически регулярно в случае чётного числа переменных m.

5.7 Коды Рида-Маллера порядка $m-3$: m нечётно

5.7.1 Радиус покрытия и метрическое дополнение выколотого кода

Пусть число переменных m нечётно. Большая часть рассуждений для этого случая похожа или идентична таковым для предыдущего случая, однако доказа-

тельство более трудоёмко. В разделе 5.5 было показано, что в данном случае

$$\rho(\mathcal{R}^{\circ}_{m-3}) = \max_{\mathbf{S}} t(\mathbf{S}) = m.$$

Вектор $\mathbf{v}$ содержится в метрическом дополнении кода $\mathcal{R}^{\circ}_{m-3}$ тогда и только тогда, когда $t(\mathbf{S}_{\mathbf{v}}) = m$. Следующая лемма характеризует матрицы, достигающие этого максимума:

Лемма 5.9. *Пусть $\mathbf{S}$ — симметричная матрица размера $m \times m$, где m нечётно. Тогда $t(\mathbf{S}) = m$ тогда и только тогда, когда $\mathbf{S}$ имеет фактор размера $m \times m$, который является либо невырожденным, либо имеет ранг $m-1$ при том, что сумма всех его столбцов равна нулю.*

Доказательство. ($\Longrightarrow$) Предположим, что $t(\mathbf{S}) = m$ и пусть $\mathbf{B}$ — минимальный фактор матрицы $\mathbf{S}$ с m столбцами. Если ранг матрицы $\mathbf{B}$ меньше $m-1$, то в $\mathbf{B}$ существует собственное линейно зависимое подмножество столбцов, что противоречит его минимальности (по лемме 5.3). Значит, ранг фактора $\mathbf{B}$ не меньше $m-1$. Если ранг равен m, то доказательство завершено.

Предположим, что $\operatorname{rank}(\mathbf{B}) = m-1$. Тогда сумма какого-то подмножества столбцов матрицы $\mathbf{B}$ должна быть равна нулю. Поскольку $\mathbf{B}$ является минимальным фактором, это подмножество не может быть собственным по лемме 5.3. Следовательно, сумма всех столбцов матрицы $\mathbf{B}$ равна нулю.

($\Longleftarrow$) Очевидно, что $t(\mathbf{S}) \geqslant \operatorname{rank}(\mathbf{S})$, поэтому если $\mathbf{S} = \mathbf{B}\mathbf{B}^{\mathbf{T}}$ для некоторой невырожденной $m \times m$-матрицы $\mathbf{B}$, то доказательство завершено.

Пусть $\mathbf{S} = \mathbf{B}\mathbf{B}^{\mathbf{T}}$ для некоторой матрицы $\mathbf{B}$ ранга $m-1$, сумма всех столбцов которой равна нулю.

Предположим, что $t(\mathbf{S}) = k \leqslant m-1$ и пусть $\mathbf{D}$ — некоторый минимальный фактор матрицы $\mathbf{S}$. Поскольку сумма всех столбцов любого фактора равна вектору, составленному из диагональных элементов матрицы $\mathbf{S}$, то сумма всех столбцов матрицы $\mathbf{D}$ равна нулю, как у матрицы $\mathbf{B}$.

Предположим, что $k = m-1$. Тогда $\mathbf{D}$ содержит чётное число столбцов, и в каждой строке матрицы содержится чётное число единиц. По лемме 5.2, мы можем добавить произвольный вектор ко всем столбцам матрицы $\mathbf{D}$, оставляя её фактором $\mathbf{S}$. Добавим первый столбец матрицы $\mathbf{D}$ ко всем её столбцам. Теперь первый столбец матрицы $\mathbf{D}$ равен нулю, и мы можем убрать его по лемме 5.2. Тем самым, мы получили фактор матрицы $\mathbf{S}$ с меньшим количеством столбцов, чем в исходном факторе $\mathbf{D}$, что противоречит его минимальности.

Следовательно, k не может превосходить $m-2$. Поскольку сумма всех столбцов матрицы $\mathbf{D}$ равна нулю, она не может быть матрицей полного ранга. Следовательно, $\mathrm{rank}(\mathbf{D})$ не превосходит $m-3$, а значит, $\mathrm{rank}(\mathbf{S})$ также не превосходит $m-3$.

Поскольку $\mathbf{S}=\mathbf{B}\mathbf{B}^{\mathbf{T}}$, то по неравенству Сильвестра $\mathrm{rank}(\mathbf{S}) \geqslant \mathrm{rank}(\mathbf{B}) + \mathrm{rank}(\mathbf{B}^{\mathbf{T}}) - m = m-2$. Но мы только что показали, что $\mathrm{rank}(\mathbf{S}) \leqslant m-3$, противоречие.

Таким образом, значение $t(\mathbf{S})$ больше, чем $m-1$, и равно m.

□

Лемма 5.9 описывает все минимальные факторы всех матриц $\mathbf{S}$, для которых $t(\mathbf{S})=m$. Рассмотрим следующие множества векторов пространства $\mathbb{F}_2^{n-1}$:

$$\mathrm{U}_1 = \{\mathbf{u} : \mathbf{B}_{\mathbf{u}} \text{ содержит ровно } m \text{ ненулевых столбцов, которые являются линейно независимыми}\}, \quad (5.4)$$

$$\mathrm{U}_2 = \{\mathbf{u} : \mathbf{B}_{\mathbf{u}} \text{ содержит ровно } m \text{ ненулевых столбцов, } m-1 \text{ из которых линейно независимы, и сумма всех столбцов равна нулю}\}. \quad (5.5)$$

Легко видеть, что множество матриц $\{\mathbf{B}_{\mathbf{u}} : \mathbf{u} \in \mathrm{U}_1 \cup \mathrm{U}_2\}$, с точностью до перестановки столбцов и удаления нулевых столбцов, содержит в точности все минимальные факторы, описанные в лемме 5.9.

Иными словами, если $t(\mathbf{S})=m$ для некоторой матрицы $\mathbf{S}$, то существует вектор $\mathbf{u} \in \mathrm{U}_1 \cup \mathrm{U}_2$ такой, что $\mathbf{S} = \mathbf{B}_{\mathbf{u}}\mathbf{B}_{\mathbf{u}}^{\mathbf{T}}$. Обратно, для всякого $\mathbf{u} \in \mathrm{U}_1 \cup \mathrm{U}_2$ выполняется $t(\mathbf{B}_{\mathbf{u}}\mathbf{B}_{\mathbf{u}}^{\mathbf{T}})=m$. Таким образом, векторы из множества $\mathrm{U}_1 \cup \mathrm{U}_2$ покрывают все смежные классы метрического дополнения кода $\mathcal{R}_{m-3}^{\circ}$:

$$\widehat{\mathcal{R}}_{m-3}^{\circ} = \bigcup_{\mathbf{u} \in \mathrm{U}_1 \cup \mathrm{U}_2} (\mathbf{u} + \mathcal{R}_{m-3}^{\circ}).$$

5.7.2 Радиус покрытия и метрическое дополнение невыколотого кода

Вернёмся к невыколотому коду $\mathcal{R}_{m-3}$. Поскольку данный код получается из выколотого кода добавлением проверки на чётность, то, применяя лемму 5.7,

мы получаем, что радиус покрытия $\mathcal{R}_{m-3}$ при нечётных m равен $m+1$, а его метрическое дополнение имеет следующий вид:

$$\widehat{\mathcal{R}}_{m-3} = \bigcup_{\mathbf{u}\in \mathrm{U}_1\cup\mathrm{U}_2} ((\pi(\mathbf{u}),\mathbf{u}) + \mathcal{R}_{m-3}),$$

где множества U_1 и U_2 определены в формулах 5.4, 5.5 предыдущего подраздела.

Напомним снова, что для любого вектора $\mathbf{v} \in \mathbb{F}_2^n$ множество ненулевых столбцов матрицы $\mathbf{B}_{\mathbf{v}^\circ}$ совпадает с носителем функции $f_{\mathbf{v}}$, за исключением, быть может, нулевого вектора. Поскольку все векторы в $\mathrm{U}_1 \cup \mathrm{U}_2$ имеют нечётный вес, а добавленная проверка на чётность соответствует значению функции в нуле, мы можем записать метрическое дополнение кода $\mathcal{R}_{m-3}$ в терминах функций следующим образом:

$$\widehat{\mathcal{R}}_{m-3} = \bigcup_{g\in G_1\cup G_2} (g + \mathcal{R}_{m-3}),$$

где

$$G_1 = \{f_{(1,\mathbf{u})} : \mathbf{u} \in \mathrm{U}_1\} = \\ = \{g : \mathrm{supp}(f) = \{0,\mathrm{x}_1,\mathrm{x}_2 \ldots,\mathrm{x}_m\}, \{\mathrm{x}_1,\ldots,\mathrm{x}_m\} \text{ линейно независимы}\},$$

и

$$G_2 = \{f_{(1,\mathbf{u})} : \mathbf{u} \in \mathrm{U}_2\} = \\ = \{g : \mathrm{supp}(g) = \{0,\mathrm{x}_1,\mathrm{x}_2 \ldots,\mathrm{x}_{m-1},\mathrm{x}_1 + \ldots + \mathrm{x}_{m-1}\}, \\ \{\mathrm{x}_1,\ldots,\mathrm{x}_{m-1}\} \text{ линейно независимы}\}.$$

Легко видеть, что все функции из G_1 образуют класс эквивалентности относительно линейной эквивалентности, как и функции из G_2. Выберем по одной функции $g_1 \in G_1$, $g_2 \in G_2$ из каждого класса. Тогда из определения EL^k-эквивалентности следует, что функция g содержится в $\widehat{\mathcal{R}}_{m-3}$ тогда и только тогда, когда $g \overset{m-3}{\sim} g_1$ или $g \overset{m-3}{\sim} g_2$. В действительности, мы можем выбрать произвольную функцию из класса EL^{m-3}-эквивалентности множества G_1 и из класса EL^{m-3}-эквивалентности множества G_2 соответственно в качестве представителей этих классов.

Опишем явно определённую функцию из G_1. Обозначим через g_1' функцию с носителем $\{0,\mathrm{e}_1,\mathrm{e}_2,\ldots,\mathrm{e}_{m-1},1\}$. Прямыми вычислениями нетрудно получить

АНФ этой функции:

$$g_1'(\mathrm{x}) = \overline{x_m} + (1 + x_m)\left(1 + \sum_{k=1}^{\frac{m-3}{2}} \sum_{1 \leqslant i_1 < \ldots < i_{2k} \leqslant m-1} x_{i_1} x_{i_2} \ldots x_{i_{2k}}\right).$$

Степень этой функции равна $m-1$, и, опуская все слагаемые степени ниже, чем $m-2$, эта функция тривиально EL^{m-3}-эквивалентна следующей функции, которую мы будем использовать в качестве представителя в дальнейшем:

$$g_1^* := \overline{x_m} + x_m g^\dagger, \tag{5.6}$$

где $g^\dagger$ — функция от первых $m-1$ переменных, определяемая равенством

$$g^\dagger(x_1, x_2, \ldots, x_{m-1}) = \left(\sum_{1 \leqslant i < j \leqslant m-1} \overline{x_i x_j}\right).$$

В дальнейшем мы будем обозначать набор из первых $m-1$ переменных как $\bar{\mathrm{x}}$. Мы также будем обозначать аффинные преобразования первых $m-1$ переменных через $\bar{L}_{\mathrm{A}}^{\mathrm{b}}$, где матрица и вектор имеют соответствующие размерности.

Опишем явно теперь определённую функцию из G_2. Обозначим через g_2' функцию с носителем $\{0, \mathrm{e}_1, \mathrm{e}_2, \ldots, \mathrm{e}_{m-1}, \sum_{i=1}^{m-1} \mathrm{e}_i\}$. Прямыми вычислениями нетрудно получить АНФ и для этой функции:

$$g_2'(\mathrm{x}) = (1 + x_m)\left(1 + \sum_{k=1}^{\frac{m-3}{2}} \sum_{1 \leqslant i_1 < \ldots < i_{2k} \leqslant m-1} x_{i_1} x_{i_2} \ldots x_{i_{2k}}\right).$$

Степень этой функции равна $m-2$ и она тривиально EL^{m-3}-эквивалентна следующей функции, которую мы будем использовать в качестве представителя в дальнейшем:

$$g_2^* := x_m g^\dagger. \tag{5.7}$$

Заметим, что $g_1^* = \overline{x_m} + g_2^*$.

Прежде, чем приняться за доказательство метрической регулярности кода $\mathcal{R}_{m-3}$, построим несколько альтернативных представителей для классов эквивалентности множеств G_1 и G_2. Для этого докажем следующую лемму. Напомним, что запись $f \overset{k}{=} g$ означает, что степень функции $f + g$ не превышает k.

Лемма 5.10. *Пусть f — функция степени $m-1$ такая, что $f \overset{m-2}{=} \overline{x_m}$, и пусть* A *— невырожденная матрица размера $m \times m$. Тогда $f \circ L_{\mathrm{A}} \overset{m-2}{=} \overline{x_m}$ тогда и только тогда, когда матрица* A *имеет следующий вид:*

$$\mathrm{A} = \begin{pmatrix} \bar{\mathrm{A}} & 0^{m-1} \\ \mathrm{w} & 1 \end{pmatrix},$$

где 0^{m-1} — нулевой столбец длины $m-1$, $\bar{\mathrm{A}}$ *— невырожденная матрица размера $(m-1) \times (m-1)$, а* w *— произвольная строка длины $m-1$.*

Доказательство. ($\Longleftarrow$) Очевидно, что такое преобразование первых $m-1$ переменных оставляет моном $\overline{x_m}$ единственным мономом степени $m-1$ в функции f, а степень любых других мономов не может возрасти при линейном преобразовании.

($\Longrightarrow$) Предположим, что $f \circ L_{\mathrm{A}} \overset{m-2}{=} \overline{x_m}$. Это означает, что замена переменных оставляет моном $\overline{x_m}$ и не добавляет других мономов степени $m-1$. Ясно, что действие этой замены переменных на мономы степени $m-2$ и ниже не имеет значения, поэтому рассмотрим действие на моном $\overline{x_m}$.

Легко видеть, что коэффициент при мономе $\overline{x_i}$ в функции $f \circ L_{\mathrm{A}}$ равен значению минора размера $(m-1) \times (m-1)$ матрицы A, получаемого удалением m-ой строки и i-го столбца. Следовательно, все такие миноры матрицы A должны быть равны нулю, кроме одного, получаемого удалением последнего столбца.

Пусть $\bar{\mathrm{A}}^1, \bar{\mathrm{A}}^2, \ldots, \bar{\mathrm{A}}^m$ — столбцы матрицы A без последней координаты. Тогда вышеупомянутое условие на миноры можно записать следующим образом: каждое из множеств столбцов $\{\bar{\mathrm{A}}^1, \ldots, \bar{\mathrm{A}}^{i-1}, \bar{\mathrm{A}}^{i+1}, \ldots, \bar{\mathrm{A}}^m\}, i \neq m$, является линейно зависимым, в то время как множество первых $m-1$ столбцов линейно независимо. Это равносильно следующей системе уравнений:

$$\begin{cases} \bar{\mathrm{A}}^m + \sum\limits_{j \leqslant m-1} b_{1,j} \bar{\mathrm{A}}^j = 0, \\ \bar{\mathrm{A}}^m + \sum\limits_{j \leqslant m-1} b_{2,j} \bar{\mathrm{A}}^j = 0, \\ \ldots \\ \bar{\mathrm{A}}^m + \sum\limits_{j \leqslant m-1} b_{m-1,j} \bar{\mathrm{A}}^j = 0, \end{cases}$$

где $\mathrm{B} = (b_{i,j})$ — некоторая матрица коэффициентов — имеет размер $(m-1) \times (m-1)$, а диагональные элементы $b_{i,i}$ равны 0 для всех i.

Если мы обозначим строки матрицы B как B_i, а через $\bar{\mathrm{A}}$ обозначим матрицу размера $(m-1)\times(m-1)$, составленную из первых $m-1$ столбцов $\bar{\mathrm{A}}^1,\ldots,\bar{\mathrm{A}}^{m-1}$, то данную систему можно записать следующим образом:

$$\begin{cases} \bar{\mathrm{A}}\cdot\mathrm{B}_1^T = \bar{\mathrm{A}}^m \\ \bar{\mathrm{A}}\cdot\mathrm{B}_2^T = \bar{\mathrm{A}}^m \\ \ldots \\ \bar{\mathrm{A}}\cdot\mathrm{B}_{m-1}^T = \bar{\mathrm{A}}^m \end{cases}$$

Поскольку множество первых $m-1$ столбцов $\bar{\mathrm{A}}^1,\ldots,\bar{\mathrm{A}}^{m-1}$ линейно независимо, то матрица $\bar{\mathrm{A}}$ невырождена и решение каждого уравнения (которое является системой уравнений в переменных $\{b_{i,j}\}_{j=1}^{m-1}$ для i-ой строки) единственно. Следовательно, $\mathrm{B}_1=\mathrm{B}_2=\ldots=\mathrm{B}_{m-1}=(\bar{\mathrm{A}}^{-1}\bar{\mathrm{A}}^m)^T$. Поскольку $b_{i,i}=0$ для любого i, то матрица B целиком состоит из нулей, откуда следует, что $\bar{\mathrm{A}}^m=0$. Тем самым, последний столбец матрицы A может содержать единицу лишь в последней координате, а поскольку матрица A невырождена, то элемент $a_{n,n}$ с необходимостью равен 1. Таким образом, матрица A имеет описанную в формулировке леммы структуру.

□

Данная лемма показывает, что все линейные преобразования описанного вида, и только они среди всех линейных преобразований, преобразуют функции вида $\overline{x_m}+h$, где $\deg(h)\leqslant m-2$, в функции такого же вида, оставляя $\overline{x_m}$ единственным мономом степени $m-1$. Рассмотрим подробнее действие таких преобразований на мономы степени $m-2$:

Следствие 5.11. *Пусть f — функция степени $m-1$ такая, что $f \overset{m-2}{=} \overline{x_m}$. Данную функцию можно единственным образом представить в виде*

$$f=\overline{x_m}+x_m f_1+f_2,$$

где f_1, f_2 не зависят от x_m, а $\deg(f_1)\leqslant m-3$, $\deg(f_2)\leqslant m-2$. Пусть A — матрица, удовлетворяющая условиям леммы 5.10. Тогда

$$f\circ L_{\mathrm{A}} \overset{m-3}{=} \overline{x_m}+x_m(f_1\circ\bar{L}_{\bar{\mathrm{A}}})+f_3,$$

где f_3 — некоторая функция степени $m-2$, не зависящая от переменной x_m.

Доказательство. Прямо следует из формы матрицы A. □

Построим теперь альтернативных представителей для классов метрического дополнения кода $\mathcal{R}_{m-3}$. Поскольку матрица $\bar{\mathrm{A}}$ в лемме 5.10 может быть любой невырожденной матрицей, выберем $\bar{\mathrm{A}}$ так, что $g^\dagger \circ \bar{L}_{\bar{\mathrm{A}}} \overset{m-3}{=} p_{\frac{m-1}{2}}$ (это возможно в силу леммы 5.8). Заполняя вектор w нулями, мы получаем матрицу A такую, что

$$g_1^{**} := g_1^* \circ L_{\mathrm{A}} \overset{m-3}{=} \overline{x_m} + x_m(g^\dagger \circ \bar{L}_{\bar{\mathrm{A}}}) + h_1 \overset{m-3}{=} \overline{x_m} + x_m p_{\frac{m-1}{2}} + h_1. \tag{5.8}$$

Здесь $p_{\frac{m-1}{2}}, h_1$ не зависят от x_m и степень h_1 не превосходит $m-2$. Более того,

$$g_2^{**} := g_2^* \circ L_{\mathrm{A}} \overset{m-3}{=} x_m(g^\dagger \circ \bar{L}_{\bar{\mathrm{A}}}) \overset{m-3}{=} x_m p_{\frac{m-1}{2}}. \tag{5.9}$$

Мы будем использовать эти функции g_1^{**} и g_2^{**} в качестве представителей классов эквивалентности в некоторых случаях.

5.7.3 Метрическая регулярность

Мы установили, что

$$\widehat{\mathcal{R}}_{m-3} = \{g : g \overset{m-3}{\sim} g_1\} \cup \{g : g \overset{m-3}{\sim} g_2\},$$

где g_1 — произвольный представитель класса EL^{m-3}-эквивалентности множества G_1, а g_2 — произвольный представитель класса EL^{m-3}-эквивалентности множества G_2, и привели несколько вариантов представителей данных классов — функции g_1^*,g_2^*,g_1^{**} и g_2^{**} (уравнения 5.6-5.9).

Поскольку код $\mathcal{R}_{m-3}$ линеен, то $\rho(\widehat{\mathcal{R}}_{m-3}) = \rho(\mathcal{R}_{m-3}) = m+2$ и функция f содержится в $\widehat{\widehat{\mathcal{R}}}_{m-3}$ тогда и только тогда, когда $f + \widehat{\mathcal{R}}_{m-3} = \widehat{\mathcal{R}}_{m-3}$. Докажем метрическую регулярность кода $\mathcal{R}_{m-3}$, показав, что никакая функция, кроме содержащихся в $\mathcal{R}_{m-3}$, не сохраняет $\widehat{\mathcal{R}}_{m-3}$ на месте при её добавлении ко всем функциям метрического дополнения.

Пусть $f \notin \mathcal{R}_{m-3}$ — произвольная функция. Поскольку $\widehat{\mathcal{R}}_{m-3}$ — объединение двух классов EL^{m-3}-эквивалентности, то для того, чтобы показать, что $f + \widehat{\mathcal{R}}_{m-3} \neq \widehat{\mathcal{R}}_{m-3}$, достаточно показать, что существует функция f' такая, что $f' \overset{m-3}{\sim} f$ и $f' + \widehat{\mathcal{R}}_{m-3} \neq \widehat{\mathcal{R}}_{m-3}$.

Случай 1. Пусть степень функции f больше $m-1$. Поскольку линейное преобразование переменных сохраняет степень функции, степень любой функции $g \in \widehat{\mathcal{R}}_{m-3}$ равна либо $m-1$ (как у функции g_1^*), либо $m-2$ (как у функции g_2^*), в то время как $f+g$ имеет более высокую степень. Следовательно, $f+g$ не может быть эквивалентна никакой функции из $\widehat{\mathcal{R}}_{m-3}$, откуда следует, что функция f не может принадлежать $\widehat{\widehat{\mathcal{R}}}_{m-3}$.

Случай 2. Пусть степень функции f равна $m-1$. Всякая функция степени $m-1$ тривиально EL^{m-3}-эквивалентна функции, единственным мономом степени $m-1$ которой является $\overline{x_m}$:

$$f \overset{m-3}{\sim} \overline{x_m} + x_m f_1 + f_2, \tag{5.10}$$

где функции f_1, f_2 не зависят от переменной x_m, f_1 либо равна нулю, либо имеет степень $m-3$, в то время как функция f_2 либо равна нулю, либо имеет степень $m-2$.

Случай 2.1. Предположим, что функция f_1 в 5.10 не равна нулю. Тогда, из леммы 5.10 и леммы 5.8 следует, что

$$f \overset{m-3}{\sim} \overline{x_m} + x_m p_k + f_3 =: f'$$

для некоторого $k > 0$ и некоторой функции f_3 степени не выше $m-2$ (p_k, f_3 не зависят от x_m). Если мы теперь сложим f' и $g_2^{**} \in \widehat{\mathcal{R}}_{m-3}$, мы получим:

$$g_2^{**} + f' \overset{m-3}{=} \overline{x_m} + x_m(p_k + p_{\frac{m-1}{2}}) + f_3 \overset{m-3}{\sim} \overline{x_m} + x_m p_{\frac{m-1}{2}-k} + f_4 =: g',$$

где f_4 — функция степени, не превышающей $m-2$, и не зависящая от переменной x_m, а последняя эквивалентность в уравнении выше получена простым переименованием переменных.

Обозначим функцию в правой части последнего уравнения за g'. Степень этой функции равна $m-1$, следовательно, она не может быть эквивалентна функциям из множества G_2. Она также не может быть эквивалентна функциям из G_1, поскольку по лемме 5.10 любое линейное преобразование переменных с матрицей D, сохраняющее $\overline{x_m}$, будет действовать на g' следующим образом:

$$g' \circ L_{\mathrm{D}} \overset{m-3}{=} \overline{x_m} + x_m(p_{\frac{m-1}{2}-k} \circ \bar{L}_{\bar{\mathrm{D}}}) + f_5,$$

где f_5 — некоторая функция степени $\leqslant m-2$ от первых $m-1$ переменных. Легко видеть, что никакая матрица $\bar{\mathrm{D}}$ не может перевести мономы степени $m-$

2 функции g', содержащие переменную x_m, в таковые функции g_1^{**}, поскольку $p_{\frac{m-1}{2}-k}$ неэквивалентна $p_{\frac{m-1}{2}}$. Таким образом, функция $g' = g_2^{**} + f'$ не содержится в $\widehat{\mathcal{R}}_{m-3}$, следовательно, если f_1 отлична от нуля, то f не содержится в $\widehat{\widehat{\mathcal{R}}}_{m-3}$.

Случай 2.2 Предположим, что как f_1, так и f_2 в равенстве 5.10 равны нулю. Тогда

$$f \overset{m-3}{\sim} \overline{x_m} =: f'.$$

Применяя преобразование $L_{1m} : x_1 \leftarrow x_1 + x_m$ и отбрасывая члены степени меньше $m-2$, функция $g_1^* = \overline{x_m} + x_m g^\dagger$ преобразовывается в $g_1^* \circ L_{1m} \overset{m-3}{=} \overline{x_m} + \overline{x_1} + x_m g^\dagger$.

Если мы теперь сложим функции f' и $g_1^* \circ L_{1m} \in \widehat{\mathcal{R}}_{m-3}$, то получим функцию $g' \overset{m-3}{=} \overline{x_1} + x_m g^\dagger$. Поменяем переменные x_1 и x_m местами в этой функции при помощи ещё одного линейного преобразования и перегруппируем слагаемые:

$$g' \overset{m-3}{\sim} \overline{x_m} + \sum_{2 \leqslant i < j \leqslant m-1} \overline{x_i x_j} + \sum_{i=2}^{m-1} \overline{x_i x_m} \overset{m-3}{\sim} \overline{x_m} + x_m p_{\frac{m-3}{2}} + h,$$

где степень функции h, зависящей от первых $m-1$ переменных, не превосходит $m-2$. По лемме 5.10 и лемме 5.8, эта функция не может быть эквивалентна g_1^{**}, а по сравнению степеней, она не может быть эквивалентна функции g_2^*. Следовательно, g' не содержится в $\widehat{\mathcal{R}}_{m-3}$, а значит функция f не содержится в $\widehat{\widehat{\mathcal{R}}}_{m-3}$.

Случай 2.3 Предположим, что функция f_1 в равенстве 5.10 равна нулю, а функция f_2 отлична от нуля. Тогда

$$f \overset{m-3}{\sim} \overline{x_m} + f_2 =: f'.$$

Поскольку f_2 не содержит переменной x_m, все слагаемые f_2 имеют вид $\overline{x_i x_m}$ для некоторого i. Без ограничения общности (переименовав переменные среди первых $m-1$, если это необходимо), мы можем полагать, что f_2 содержит моном $\overline{x_{m-1} x_m}$. Меняя местами переменные в g_2^{**}, мы можем преобразовать её в следующую функцию:

$$g_2^{**} \overset{m-3}{\sim} \overline{x_2 x_3} + \overline{x_4 x_5} + \ldots + \overline{x_{m-1} x_m}.$$

Если мы теперь сложим f' и функцию из правой части равенства выше (которая содержится в $\widehat{\mathcal{R}}_{m-3}$), мы получим функцию $g' := \overline{x_m} + \sum\limits_{k=1}^{\frac{m-3}{2}} \overline{x_{2k} x_{2k+1}} + \sum\limits_{i \in I} \overline{x_i x_m}$. Эта функция эквивалентна

$$g' \overset{m-3}{\sim} \overline{x_m} + x_m p_{\frac{m-3}{2}} + h$$

для некоторой h степени не выше $m-2$ от первых $m-1$ переменных. По лемме 5.10 и лемме 5.8, эта функция не может быть эквивалентна g_1^{**}, а по сравнению степеней, она не может быть эквивалентна функции g_2^*. Следовательно, g' не содержится в $\widehat{\mathcal{R}}_{m-3}$ и функция f не содержится в $\widehat{\widehat{\mathcal{R}}}_{m-3}$.

Случай 3. Если степень функции f равна $m-2$, то, при помощи рассуждений, аналогичных случаю "m чётно", легко показать, что f эквивалентна функции p_k (от m переменных) для некоторого $k > 0$. Тогда

$$p_k + g_2^{**} \overset{m-3}{\sim} p_{\frac{m-1}{2}-k}.$$

Функция в правой части данного уравнения неэквивалентна ни функции g_2^{**} (поскольку $\frac{m-1}{2} \neq \frac{m-1}{2} - k$), ни функции g_1^* (по сравнению степеней), и, следовательно, $f \notin \widehat{\widehat{\mathcal{R}}}_{m-3}$.

Поскольку все функции, не содержащиеся в $\mathcal{R}_{m-3}$, имеют степень $m-2$ или выше, то мы доказали, что никакая из них не содержится во втором метрическом дополнении, следовательно, код $\mathcal{R}_{m-3}$ метрически регулярен для нечётных значений m.

Прибавляя сюда результаты раздела 5.6, мы получаем следующее утверждение:

Теорема 5.12 (см. [59])**.** *Код $\mathcal{R}_{m-3}$ метрически регулярен для любого $m \geqslant 3$.*

5.8 Код Рида-Маллера $\mathcal{RM}(2,6)$

Рассмотрим ещё один частный случай — код Рида-Маллера $\mathcal{RM}(2,6)$. Если определить порядок в векторе значений функции таким образом, чтобы первая половина вектора соответствовала значениям функции при $x_m = 0$, а вторая — значениям функции при $x_m = 1$, то всякий код Рида-Маллера (при $m > 1$, $r > 0$) можно индуктивно определить следующим образом:

$$\mathcal{R}_{r,m} = \{(\mathbf{u}, \mathbf{u}+\mathbf{v}) : \mathbf{u} \in \mathcal{R}_{r,m-1}, \mathbf{v} \in \mathcal{R}_{r-1,m-1}\}.$$

В частности,

$$\mathcal{R}_{2,6} = \{(\mathbf{u}, \mathbf{u}+\mathbf{v}) : \mathbf{u} \in \mathcal{R}_{2,5}, \mathbf{v} \in \mathcal{R}_{1,5}\}.$$

Поскольку оба кода $\mathcal{R}_{2,5}$, $\mathcal{R}_{1,5}$ метрически регулярны, то данная конструкция оказывается полезной при доказательстве метрической регулярности кода $\mathcal{R}_{2,6}$. В данном разделе полужирные векторы обозначают векторы значений функций от пяти переменных (длины 32), в то время как векторы значений функций от 6 переменных будут представляться в виде пары векторов значений функций от 5 переменных.

Для начала докажем базовое утверждение, используемое в доказательствах данного раздела. Напомним, что $\rho(\mathcal{R}_{2,5}) = 6$ (раздел 5.7), $\rho(\mathcal{R}_{1,5}) = 12$ [3], а $\rho(\mathcal{R}_{2,6}) = 18$ [40].

Лемма 5.13 (см. [59]). *Пусть вектор* $(\mathbf{y},\mathbf{w})$ *содержится в* $\widehat{\mathcal{R}}_{2,6}$. *Тогда* $\mathbf{y} \in \widehat{\mathcal{R}}_{2,5}$ *и для любого* $\mathbf{u} \in \mathcal{R}_{2,5}$ *такого, что* $d(\mathbf{y},\mathbf{u}) = 6$, *выполняется* $d(\mathbf{w}+\mathbf{u}, \mathcal{R}_{1,5}) = 12$, *т.е.* $(\mathbf{w}+\mathbf{u}) \in \widehat{\mathcal{R}}_{1,5}$.

Доказательство. Предположим, что $\mathbf{y} \notin \widehat{\mathcal{R}}_{2,5}$, т.е. что $d(\mathbf{y},\mathcal{R}_{2,5}) < 6$. Тогда существует вектор $\mathbf{u} \in \mathcal{R}_{2,5}$ такой, что $d(\mathbf{y},\mathbf{u}) < 6$. Из индуктивной конструкции кода $\mathcal{R}_{2,6}$ следует, что расстояние от вектора $(\mathbf{y},\mathbf{w})$ до кода $\mathcal{R}_{2,6}$ не превосходит расстояния между векторами $\mathbf{y}$ и $\mathbf{u}$, сложенного с расстоянием от вектора $\mathbf{w}$ до множества $\mathbf{u}+\mathcal{R}_{1,5}$. Последнее расстояние, в свою очередь, равно $d(\mathbf{w}+\mathbf{u},\mathcal{R}_{1,5})$ и следовательно ограничено радиусом покрытия кода $\mathcal{R}_{1,5}$. Таким образом,

$$d((\mathbf{y},\mathbf{w}),\mathcal{R}_{2,6}) \leqslant d(\mathbf{y},\mathbf{u}) + d(\mathbf{w}+\mathbf{u},\mathcal{R}_{1,5}) < 6 + 12 = 18.$$

Это противоречит предположению $(\mathbf{y},\mathbf{w}) \in \widehat{\mathcal{R}}_{2,6}$. Тем самым, $\mathbf{y} \in \widehat{\mathcal{R}}_{2,5}$.

Вторая часть утверждения теперь тривиальна: из рассуждений выше сразу следует, что если вектор $(\mathbf{y},\mathbf{w}) \in \widehat{\mathcal{R}}_{2,6}$ и $\mathbf{u} \in \mathcal{R}_{2,5}$ удовлетворяет равенству $d(\mathbf{y},\mathbf{u}) = 6$, то расстояние $d(\mathbf{w}+\mathbf{u},\mathcal{R}_{1,5})$ обязано достигать максимума, равного 12. □

Пусть вектор $(\tilde{\mathbf{u}},\tilde{\mathbf{u}}+\tilde{\mathbf{v}}) \in \widehat{\widehat{\mathcal{R}}}_{2,6}$. Мы докажем, что $(\tilde{\mathbf{u}},\tilde{\mathbf{u}}+\tilde{\mathbf{v}})$ содержится в $\mathcal{R}_{2,6}$, и тем самым установим метрическую регулярность данного кода, в два шага: сначала мы покажем, что $\tilde{\mathbf{u}}$ содержится в $\mathcal{R}_{2,5}$, а затем покажем, что $\tilde{\mathbf{v}}$ содержится в $\mathcal{R}_{1,5}$.

Вспомним (раздел 5.7), что $\widehat{\mathcal{R}}_{2,5} = \{g : g \overset{2}{\sim} g_1\} \cup \{g : g \overset{2}{\sim} g_2\}$, где g_1 и g_2 — некоторые представители двух классов EL^2-эквивалентности. Обозначим

$$\widehat{\mathcal{R}}^1_{2,5} := \{g : g \overset{2}{\sim} g_1\},\ \widehat{\mathcal{R}}^2_{2,5} := \{g : g \overset{2}{\sim} g_2\}.$$

Следующая лемма пригодится для доказательства первого шага:

Лемма 5.14 (см. [59]). *Для каждого* $i = 1,2$ *выполняется одно из следующих утверждений:*

1. *для любых* $\mathbf{y} \in \widehat{\mathcal{R}}^i_{2,5}, \mathbf{w} \in \mathbb{F}_2^{32}$ *вектор* $(\mathbf{y},\mathbf{w})$ *не содержится в* $\widehat{\mathcal{R}}_{2,6}$;
2. *для любого* $\mathbf{y} \in \widehat{\mathcal{R}}^i_{2,5}$ *существует* $\mathbf{w} \in \mathbb{F}_2^{32}$ *такой, что* $(\mathbf{y},\mathbf{w}) \in \widehat{\mathcal{R}}_{2,6}$;

Доказательство. Предположим, что для какого-то i не выполняется второе утверждение. Обращая это утверждение, мы получаем

$$\exists \mathbf{y}^* \in \widehat{\mathcal{R}}^i_{2,5} : \forall \mathbf{w} \in \mathbb{F}_2^{32} \text{ вектор } (\mathbf{y}^*,\mathbf{w}) \text{ не содержится в } \widehat{\mathcal{R}}_{2,6}.$$

Покажем теперь, что данное утверждение выполняется для любого вектора $\mathbf{y} \in \widehat{\mathcal{R}}^i_{2,5}$, а не только для данного $\mathbf{y}^*$. Во-первых, заметим, что утверждение

$$\forall \mathbf{w} \in \mathbb{F}_2^{32} \text{ вектор } (\mathbf{y}^*,\mathbf{w}) \text{ не содержится в } \widehat{\mathcal{R}}_{2,6}$$

эквивалентно следующему:

$$\forall \mathbf{w} \in \mathbb{F}_2^{32}\ \exists \mathbf{u} \in \mathcal{R}_{2,5} : d(\mathbf{y}^*,\mathbf{u}) + d(\mathbf{w}+\mathbf{u}, \mathcal{R}_{1,5}) < 18. \tag{5.11}$$

Пусть теперь $\mathbf{y}$ — произвольный вектор из $\widehat{\mathcal{R}}^i_{2,5}$. Поскольку все функции из $\widehat{\mathcal{R}}^i_{2,5}$ EL^2-эквивалентны друг другу, то существует невырожденное линейное преобразование переменных L и функция $g \in \mathcal{R}_{2,5}$ такие, что $f_{\mathbf{y}} = f_{\mathbf{y}^*} \circ L + g$. Обозначим через $\mathbf{g}$ вектор значений функции g а через $\mathbf{L}$ — линейное преобразование пространства $\mathbb{F}_2^{32}$, соответствующее преобразованию L на функциях. Тогда $\mathbf{y} = \mathbf{L}\mathbf{y}^* + \mathbf{g}$.

Рассмотрим произвольный вектор $\mathbf{w} \in \mathbb{F}_2^{32}$ и обозначим $\mathbf{w}_{\mathbf{y}} = \mathbf{L}^{-1}(\mathbf{w}+\mathbf{g})$. Тогда из 5.11 следует, что существует вектор $\mathbf{u} \in \mathcal{R}_{2,5}$ такой, что

$$d(\mathbf{y}^*,\mathbf{u}) + d(\mathbf{w}_{\mathbf{y}}+\mathbf{u}, \mathcal{R}_{1,5}) < 18. \tag{5.12}$$

Очевидно, что преобразование $\mathbf{L}$, как и прибавление функции $\mathbf{g}$, являются автоморфизмами пространства $\mathbb{F}_2^{32}$. Применим $\mathbf{L}$ ко всем векторам, сравниваемым в 5.12, и добавим функцию $\mathbf{g}$ к некоторым из них, не нарушая неравенство:

$$d(\mathbf{L}\mathbf{y}^*+\mathbf{g},\mathbf{L}\mathbf{u}+\mathbf{g}) + \min_{\mathbf{v}\in\mathcal{R}_{1,5}} d(\mathbf{L}\mathbf{w}_{\mathbf{y}}+\mathbf{L}\mathbf{u},\mathbf{L}\mathbf{v}) < 18. \tag{5.13}$$

Заметим, что преобразование $\mathbf{L}$ также является автоморфизмом кодов $\mathcal{R}_{1,5}$ и $\mathcal{R}_{2,5}$. Обозначим $\mathbf{u}_{\mathbf{y}} := \mathbf{L}\mathbf{u}+\mathbf{g}$. Тогда $\mathbf{u}_{\mathbf{y}} \in \mathcal{R}_{2,5}$ и 5.13 приводится к виду

$$d(\mathbf{y},\mathbf{u}_{\mathbf{y}}) + \min_{\mathbf{v}\in\mathcal{R}_{1,5}} d(\mathbf{w}+\mathbf{u}_{\mathbf{y}},\mathbf{v}) < 18. \tag{5.14}$$

Таким образом, для произвольного вектора $\mathbf{w} \in \mathbb{F}_2^{32}$ мы нашли вектор $\mathbf{u_y} \in \mathcal{R}_{2,5}$ такой, что выполняется неравенство 5.14. Это означает, что утверждение 5.11 выполняется для вектора $\mathbf{y}$, ранее выбранного из множества $\widehat{\mathcal{R}}^i_{2,5}$. Поскольку выбор был произвольным, мы доказали тем самым, что для множества $\widehat{\mathcal{R}}^i_{2,5}$ выполняется первое утверждение леммы. □

Утверждение 5.15 (см. [59]). *Пусть* $(\tilde{\mathbf{u}},\tilde{\mathbf{u}}+\tilde{\mathbf{v}}) \in \widehat{\widehat{\mathcal{R}}}_{2,6}$. *Тогда* $\tilde{\mathbf{u}} \in \mathcal{R}_{2,5}$.

Доказательство. Рассмотрим множество

$$Y := \{\mathbf{y} \in \mathbb{F}_2^{32} \mid \exists \mathbf{w} \in \mathbb{F}_2^{32} : (\mathbf{y},\mathbf{w}) \in \widehat{\mathcal{R}}_{2,6}\}. \tag{5.15}$$

Из леммы 5.13 следует, что Y непусто и содержится в $\widehat{\mathcal{R}}_{2,5}$. Из леммы 5.14 мы можем заключить, что Y может быть лишь одним из трёх следующих множеств: $\widehat{\mathcal{R}}^1_{2,5}$, $\widehat{\mathcal{R}}^2_{2,5}$ или $\widehat{\mathcal{R}}_{2,5}$.

Пусть $(\tilde{\mathbf{u}},\tilde{\mathbf{u}}+\tilde{\mathbf{v}}) \in \widehat{\widehat{\mathcal{R}}}_{2,6}$. Тогда, как мы знаем, $(\tilde{\mathbf{u}},\tilde{\mathbf{u}}+\tilde{\mathbf{v}}) + \widehat{\mathcal{R}}_{2,6} = \widehat{\mathcal{R}}_{2,6}$. Отсюда следует, что $\tilde{\mathbf{u}} + Y = Y$. Поскольку мы доказали, что код $\mathcal{R}_{2,5}$ метрически регулярен, то известно, что лишь векторы из кода $\mathcal{R}_{2,5}$ сохраняют метрическое дополнение при сложении с ним. Проследив за доказательством метрической регулярности кода $\mathcal{R}_{m-3,m}$ для нечётного m (подраздел 5.7.3), легко видеть, что то же верно и для классов $\widehat{\mathcal{R}}^1_{2,5}$ и $\widehat{\mathcal{R}}^2_{2,5}$, рассматриваемых по отдельности. Следовательно, вне зависимости от содержания множества Y, лишь векторы из кода $\mathcal{R}_{2,5}$ сохраняют его на месте при сложении с ними, откуда следует, что $\tilde{\mathbf{u}} \in \mathcal{R}_{2,5}$. □

Вспомним (раздел 5.2), что код $\widehat{\mathcal{R}}_{1,5}$ состоит из четырёх классов EA-эквивалентности: $\widehat{\mathcal{R}}_{1,5} = \bigcup_{i=1}^{4} \widehat{\mathcal{R}}^i_{1,5}$. Верно следующее утверждение, схожее с леммой 5.14:

Лемма 5.16 (см. [59]). *Для любого* $i = 1,2,3,4$ *выполняется одно из следующих утверждений*

1. *для любых* $\mathbf{w}' \in \widehat{\mathcal{R}}^i_{1,5}, (\mathbf{y},\mathbf{w}) \in \widehat{\mathcal{R}}_{2,6}, \mathbf{u} \in \mathcal{R}_{2,5}$ *если* $d(\mathbf{y},\mathbf{u}) = 6$, *то* $\mathbf{w} + \mathbf{u} \neq \mathbf{w}'$;
2. *для любого* $\mathbf{w}' \in \widehat{\mathcal{R}}^i_{1,5}$ *существуют* $(\mathbf{y},\mathbf{w}) \in \widehat{\mathcal{R}}_{2,6}, \mathbf{u} \in \mathcal{R}_{2,5}$ *такие, что* $d(\mathbf{y},\mathbf{u}) = 6$ *и* $\mathbf{w} + \mathbf{u} = \mathbf{w}'$;

Доказательство. Предположим, что для некоторого i не выполняется второе утверждение. Значит, существует вектор $\mathbf{w}^* \in \widehat{\mathcal{R}}^i_{1,5}$ такой, что

$$\forall (\mathbf{y},\mathbf{w}) \in \widehat{\mathcal{R}}_{2,6}\ \forall \mathbf{u} \in \mathcal{R}_{2,5} \text{ если } d(\mathbf{y},\mathbf{u}) = 6, \text{ то } \mathbf{w} + \mathbf{u} \neq \mathbf{w}^*. \tag{5.16}$$

Покажем, что 5.16 выполняется для любого вектора из данного класса. Пусть $\mathbf{w}'$ — произвольный вектор из $\widehat{\mathcal{R}}_{1,5}^i$. Поскольку все функции в $\widehat{\mathcal{R}}_{1,5}^i$ EA-эквивалентны друг другу, то существует невырожденное аффинное преобразование переменных A и функция $g \in \mathcal{R}_{1,5}$ такие, что $f_{\mathbf{w}'} = f_{\mathbf{w}^*} \circ A + g$. Обозначим через $\mathbf{g}$ вектор значений функции g, а через $\mathbf{A}$ — линейное преобразование пространства $\mathbb{F}_2^{32}$, соответствующее преобразованию A на функциях. Тогда $\mathbf{w}' = \mathbf{A}\mathbf{w}^* + \mathbf{g}$.

Пусть $(\mathbf{y},\mathbf{w})$ — произвольный вектор из $\widehat{\mathcal{R}}_{2,6}$, а $\mathbf{u}$ — произвольный вектор из $\mathcal{R}_{2,5}$. Поскольку $\mathbf{A}$ — автоморфизм кодов $\mathcal{R}_{2,5}$ и $\mathcal{R}_{1,5}$, то вектор $\mathbf{A}^{-1}\mathbf{u}$ содержится в $\mathcal{R}_{2,5}$ и $(\mathbf{A},\mathbf{A}) \cdot \mathcal{R}_{2,6} = \mathcal{R}_{2,6}$. Поскольку добавление вектора $\mathbf{g}$ является автоморфизмом кодов $\mathcal{R}_{2,5}$, $\mathcal{R}_{1,5}$ и пространства $\mathbb{F}_2^{32}$, то вектор $(\mathbf{A}^{-1}\mathbf{y},\mathbf{A}^{-1}(\mathbf{w}+\mathbf{g}))$ содержится в $\widehat{\mathcal{R}}_{2,6}$. Подставляя в 5.16 векторы $(\mathbf{A}^{-1}\mathbf{y},\mathbf{A}^{-1}(\mathbf{w}+\mathbf{g})) \in \widehat{\mathcal{R}}_{2,6}$ и $\mathbf{A}^{-1}\mathbf{u} \in \mathcal{R}_{2,5}$, получаем, что верно следующее утверждение:

$$\text{если } d(\mathbf{A}^{-1}\mathbf{y},\mathbf{A}^{-1}\mathbf{u}) = 6, \text{ то } \mathbf{A}^{-1}(\mathbf{w}+\mathbf{g}) + \mathbf{A}^{-1}\mathbf{u} \neq \mathbf{w}^*. \tag{5.17}$$

Применив преобразование $\mathbf{A}$ к векторам в 5.17, мы видим, что данное утверждение эквивалентно следующему:

$$\text{если } d(\mathbf{y},\mathbf{u}) = 6, \text{ то } \mathbf{w}+\mathbf{u} \neq \mathbf{w}'. \tag{5.18}$$

Следовательно, мы показали, что для произвольного вектора $\mathbf{w}'$ из $\widehat{\mathcal{R}}_{1,5}^i$, произвольного $(\mathbf{y},\mathbf{w})$ из $\widehat{\mathcal{R}}_{2,6}$ и произвольного $\mathbf{u}$ из $\mathcal{R}_{2,5}$ выполняется утверждение 5.18. Это доказывает, что для класса $\widehat{\mathcal{R}}_{1,5}^i$ выполняется первое утверждение леммы.

□

Следующий результат показывает, что любой класс EA-эквивалентности метрического дополнения кода $\mathcal{R}_{1,5}$ является весьма “неустойчивым”, будучи сложенным с неаффинной функцией:

Лемма 5.17 (см. [59]). *Для любого* $\mathbf{v} \notin \mathcal{R}_{1,5}$ *и любого* $i = 1,2,3,4$ *существует вектор* $\mathbf{w} \in \widehat{\mathcal{R}}_{1,5}^i$ *такой, что* $\mathbf{v}+\mathbf{w} \notin \widehat{\mathcal{R}}_{1,5}$.

Доказательство. Как и в разделе 5.2, для того, чтобы доказать данное утверждение, достаточно показать, что для любого $i = 1,2,3,4$ и любого класса EA-эквивалентности C пространства $\mathbb{F}_2^{32}$ чётного веса (за исключением кода $\mathcal{R}_{1,5}$) существует функция $f \in C$ и функция $g \in \widehat{\mathcal{R}}_{1,5}^i$ такие, что $f+g \notin \widehat{\mathcal{R}}_{1,5}$. Данное доказательство можно найти в приложении A в таблицах 2-5. □

Теорема 5.18 (см. [59]). *Код $\mathcal{R}_{2,6}$ метрически регулярен.*

Доказательство. Поскольку любой линейный код является подмножеством своего второго метрического дополнения, нам нужно лишь показать, что $\widehat{\widehat{\mathcal{R}}}_{2,6} \subseteq \mathcal{R}_{2,6}$. Пусть $(\tilde{\mathbf{u}},\tilde{\mathbf{u}}+\tilde{\mathbf{v}})$ — произвольный вектор из $\widehat{\widehat{\mathcal{R}}}_{2,6}$. Мы уже показали, что вектор $\tilde{\mathbf{u}}$ содержится в $\mathcal{R}_{2,5}$, значит вектор $(\mathbf{0},\tilde{\mathbf{v}})$ тоже содержится в $\widehat{\widehat{\mathcal{R}}}_{2,6}$. Докажем, что вектор $\tilde{\mathbf{v}}$ содержится в $\mathcal{R}_{1,5}$.

Предположим, что $\tilde{\mathbf{v}} \notin \mathcal{R}_{1,5}$. Поскольку, по лемме 5.13, для произвольного вектора $(\mathbf{y},\mathbf{w}) \in \widehat{\mathcal{R}}_{2,6}$ существует вектор $\mathbf{u} \in \mathcal{R}_{2,5}$ такой, что $(\mathbf{w}+\mathbf{u}) \in \widehat{\mathcal{R}}_{1,5}$, то для какого-то i должно выполняться второе условие леммы 5.16.

По лемме 5.17, существует вектор $\mathbf{w}^* \in \widehat{\mathcal{R}}^i_{1,5}$ такой, что $(\tilde{\mathbf{v}}+\mathbf{w}^*) \notin \widehat{\mathcal{R}}_{1,5}$.

Из второго утверждения леммы 5.16 следует, что для этого вектора $\mathbf{w}^*$ существует вектор $(\mathbf{y},\mathbf{w}) \in \widehat{\mathcal{R}}_{2,6}$ и вектор $\mathbf{u} \in \mathcal{R}_{2,5}$ такие, что $(d(\mathbf{y},\mathbf{u}) = 6 \wedge \mathbf{w}+\mathbf{u} = \mathbf{w}^*)$. Поскольку $(\mathbf{0},\tilde{\mathbf{v}}) \in \widehat{\widehat{\mathcal{R}}}_{2,6}$, то вектор $(\mathbf{y},\mathbf{w}+\tilde{\mathbf{v}})$ также содержится в $\widehat{\mathcal{R}}_{2,6}$. А так как $d(\mathbf{y},\mathbf{u}) = 6$, то, по лемме 5.13, вектор $\mathbf{w}+\tilde{\mathbf{v}}+\mathbf{u}$ содержится в $\widehat{\mathcal{R}}_{1,5}$. Но $\mathbf{w}+\tilde{\mathbf{v}}+\mathbf{u} = \tilde{\mathbf{v}}+\mathbf{w}^* \notin \widehat{\mathcal{R}}_{1,5}$, противоречие. Следовательно, $\tilde{\mathbf{v}} \in \mathcal{R}_{1,5}$ и вектор $(\tilde{\mathbf{u}},\tilde{\mathbf{u}}+\tilde{\mathbf{v}})$ содержится в $\mathcal{R}_{2,6}$. □

Таким образом, в данной главе мы установили метрическую регулярность кодов $\mathcal{RM}(1,5)$, $\mathcal{RM}(2,6)$ и кодов $\mathcal{RM}(k,m)$ для $k \geqslant m-3$. С учётом результатов Н. Токаревой [47], доказывающих метрическую регулярность кода $\mathcal{RM}(1,m)$ для чётных m, рассмотрены все бесконечные семейства кодов Рида-Маллера с известным радиусом покрытия. Это позволяет нам сформулировать следующую гипотезу:

Гипотеза 5.19 (см. [59]). *Все коды Рида-Маллера $\mathcal{RM}(k,m)$ метрически регулярны.*

Единственными кодами Рида-Маллера с установленным радиусом покрытия, метрическая регулярность которых не была доказана (но и не была опровергнута), остаются коды $\mathcal{RM}(1,7)$ и $\mathcal{RM}(2,7)$.

Заключение

Основные результаты работы заключаются в следующем:

1. Представлены различные конструкции метрически регулярных множеств: доказана сходимость операции взятия метрического дополнения, получены итеративные конструкции строго метрически регулярных множеств и найдено число множеств, полученных при помощи данных конструкций;
2. Показано, что задача поиска наибольшего по мощности метрически регулярного множества сводится к задаче поиска наименьшего покрывающего кода радиуса 1;
3. Получена нижняя оценка суммы мощностей метрически регулярного множества и его метрического дополнения, зависящая от радиуса покрытия множества. Представлены конструкции семейств метрически регулярных множеств большой мощности, получена нижняя оценка мощности наибольшего метрически регулярного множества при заданном радиусе покрытия;
4. Получена общая характеризация первого и второго метрических дополнений линейных кодов;
5. Доказана метрическая регулярность кодов Рида-Маллера $\mathcal{RM}(k,m)$ для $k = 0$, $k \geqslant m - 3$, а также кодов $\mathcal{RM}(1,5)$ и $\mathcal{RM}(2,6)$. Описаны метрические дополнения всех перечисленных кодов, за исключением кода $\mathcal{RM}(2,6)$.

Автор выражает благодарность научному руководителю Токаревой Н. Н. за научное руководство: постановку интересных задач, обсуждение результатов, помощь в подготовке статей и выступлений и поддержку на протяжении всего обучения и работы. Также автор благодарит А. Куценко, А. Городилову, Н. Коломейца и всю команду Криптографического центра (Новосибирск) за поддержку и обсуждение результатов. Автор признателен коллективу исследовательской группы Selmer Center (Норвегия) за предоставленную возможность стажировки и плодотворную работу.

Список литературы

[1] Broué M. Le réseau de Leech et le groupe de Conway // Диссертация — Faculté des Sciences de Paris, 1970.

[2] Боржес Ж., Рифа Д., Зиновьев В. А. О полностью регулярных кодах // Проблемы передачи информации. — 2019. — Т. 55. — №. 1. — С. 3–50.

[3] Berlekamp E., Welch N. Weight distributions of the cosets of the $(32, 6)$ Reed-Muller code // IEEE Transactions on Information Theory. — 1972. — Т. 18. — №. 1. — С. 203–207.

[4] Бассалыго Л. А., Зайцев Г. В., Зиновьев В. А. О равномерно упакованных кодах // Проблемы передачи информации. — 1974. — Т. 10. — №. 1. — С. 9–14.

[5] Cohn H., Kumar A. Optimality and uniqueness of the Leech lattice among lattices // Annals of mathematics. — 2009. — С. 1003–1050.

[6] Cohn H., Kumar A., Miller S. D., Radchenko D., Viazovska M. The sphere packing problem in dimension 24 // Annals of Mathematics. — 2017. — С. 1017–1033.

[7] Carlet C., Mesnager S. Four decades of research on bent functions // Designs, Codes and Cryptography. — 2016. — Т. 78. — №. 1. — С. 5–50.

[8] Cohen G., Lobstein A., Sloane N. Further results on the covering radius of codes // IEEE Transactions on Information Theory. — 1986. — Т. 32. — №. 5. — С. 680–694.

[9] Cohen G., Honkala I., Litsyn S., Lobstein A. Covering codes // Elsevier. — 1997. — Т. 54.

[10] Conway J. H., Parker R. A., Sloane N.J̇, A. The covering radius of the Leech lattice // Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences. — 1982. — Т. 380. — №. 1779. — С. 261–290.

[11] Conway J. H., Sloane N. J. A. Sphere packings, lattices and groups // Springer Science & Business Media. — 2013. — Т. 290.

[12] Delsarte P. An algebraic approach to the association schemes of coding theory // Philips Res. Rep. Suppl. — 1973. — T. 10. — C. vi+–97.

[13] Goethals J. M., Snover S. L. Nearly perfect binary codes // Discrete Mathematics. — 1972. — T. 3. — №. 1-3. — C. 65–88.

[14] van Tilborg H. C. A., Goethals J. M. Uniformly packed codes // Philips Research Reports. — 1975. — T. 30. — C. 9–36.

[15] Henry W. Gould Combinatorial Identities // Morgantown Printing and Binding Co., Morgantown, WV. — 1972.

[16] Golay M. J. E. Notes on digital coding // Proc. IEEE. — 1949. — T. 37. — C. 657.

[17] Gorenstein D., Peterson W. W., Zierler N. Two-error correcting Bose-Chaudhuri codes are quasi-perfect // Information and Control. — 1960. — T. 3. — №. 3. — C. 291–294.

[18] Graham R. L., Sloane N. On the covering radius of codes // IEEE Transactions on Information Theory. — 1985. — T. 31. — №. 3. — C. 385–401.

[19] Hamming R. W. Error detecting and error correcting codes // The Bell system technical journal. — 1950. — T. 29. — №. 2. — C. 147–160.

[20] Hou X. D. Covering Radius of the Reed-Muller code $R(1,7)$ – A Simpler Proof // Journal of Combinatorial Theory, Series A. — 1996. — T. 74. — №. 2. — C. 337–341.

[21] Johnson S. A new upper bound for error-correcting codes // IRE Transactions on Information Theory. — 1962. — T. 8. — №. 3. — C. 203–207.

[22] Коломеец Н. А., Павлов А. В. Свойства бент-функций, находящихся на минимальном расстоянии друг от друга // Прикладная дискретная математика. — 2009. — Т. 6. — №. 2. — С. 5–20.

[23] Kolomeets N. A. Enumeration of the bent functions of least deviation from a quadratic bent function // Journal of Applied and Industrial Mathematics. — 2012. — T. 6. — №. 3. — C. 306–317.

[24] Коломеец Н. А. Верхняя оценка числа бент-функций на расстоянии 2^k от произвольной бент-функции от $2k$ переменных // Прикладная дискретная математика. — 2014. — Т. 25. — №. 3. — С. 28–39.

[25] Kolomeec N. The graph of minimal distances of bent functions and its properties // Designs, Codes and Cryptography. — 2017. — Т. 85. — №. 3. — С. 395–410.

[26] Kutsenko A. Metrical properties of self-dual bent functions // Designs, Codes and Cryptography. — 2020. — Т. 88. — №. 1. — С. 201–222.

[27] Leech J. Notes on sphere packings // Canadian Journal of Mathematics. — 1967. — Т. 19. — С. 251–267.

[28] Lepowsky J., Meurman A. An E8-approach to the Leech lattice and the Conway group // Journal of Algebra. — 1982. — Т. 77. — №. 2. — С. 484–504.

[29] Lindström K. All nearly perfect codes are known // Information and Control. — 1977. — Т. 35. — №. 1. — С. 40–47.

[30] McLoughlin A. M. The Covering Radius of the $(m-3)$-rd Order Reed Muller Codes and a Lower Bound on the $(m-4)$-th Order Reed Muller Codes // SIAM Journal on Applied Mathematics. — 1979. — Т. 37. — №. 2. — С. 419–422.

[31] MacWilliams F. J., Sloane N. J. A. The theory of error correcting codes // Elsevier. — 1977. — Т. 16.

[32] Mesnager S. Bent Functions: Fundamentals and Results // Springer International Publishing. – 2016.

[33] Muller D. E. Application of Boolean algebra to switching circuit design and to error detection // Transactions of the IRE professional group on electronic computers. — 1954. — №. 3. — С. 6–12.

[34] Mykkeltveit J. The covering radius of the $(128, 8)$ Reed-Muller code is 56 // IEEE Transactions on Information Theory. — 1980. — Т. 26. — №. 3. — С. 359–362.

[35] Neumaier A. Completely regular codes // Discrete mathematics. — 1992. — Т. 106. — С. 353–360.

[36] Niemeier H. V. Definite quadratische formen der dimension 24 und diskriminante 1 // Journal of Number Theory. — 1973. — Т. 5. — №. 2. — С. 142–178.

[37] Norton S. A bound for the covering radius of the Leech lattice // Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences. — 1982. — Т. 380. — №. 1779. — С. 259–260.

[38] Odlyzko A. M., Sloane N. J. A. New bounds on the number of unit spheres that can touch a unit sphere in n dimensions // Journal of Combinatorial Theory, Series A. — 1979. — Т. 26. — №. 2. — С. 210–214.

[39] Rothaus O. S. On “bent” functions // Journal of Combinatorial Theory, Series A. — 1976. — Т. 20. — №. 3. — С. 300–305.

[40] Schatz J. The second order Reed-Muller code of length 64 has covering radius 18 // IEEE Transactions on Information Theory. — 1981. — Т. 27. — №. 4. — С. 529–530.

[41] Solé P. Completely regular codes and completely transitive codes // Discrete Mathematics. — 1990. — Т. 81. — №. 2. — С. 193–201.

[42] Stănică P., Sasao T., Butler J. T. Distance duality on some classes of Boolean functions // Journal of Combinatorial Mathematics and Combinatorial Computing. — 2018. — Т. 107. — С. 181–198.

[43] Семаков Н. В., Зиновьев В. А., Зайцев Г. В. Равномерно упакованные коды // Проблемы передачи информации. — 1971. — Т. 7. — №. 1. — С. 38–50.

[44] Shapiro H. S., Slotnick D. L. On the mathematical theory of error-correcting codes // IBM Journal of Research and development. — 1959. — Т. 3. — №. 1. — С. 25–34.

[45] Tietäväinen A. On the nonexistence of perfect codes over finite fields // SIAM Journal on Applied Mathematics. — 1973. — Т. 24. — №. 1. — С. 88–96.

[46] Tits J. Four presentations of Leech’s lattice // Finite simple groups II. — 1980. — С. 303—307.

[47] Tokareva N. N. The group of automorphisms of the set of bent functions // Discrete Mathematics and Applications. — 2010. — Т. 20. — №. 5-6. — С. 655–664.

[48] Tokareva N. Duality between bent functions and affine functions // Discrete mathematics. — 2012. — Т. 312. — №. 3. — С. 666–670.

[49] Tokareva N. Bent functions: results and applications to cryptography // Academic Press. — 2015.

[50] Tokareva N., Gorodilova A., Agievich S., Idrisova V., Kolomeec N., Kutsenko A., Oblaukhov A., Shushuev G. Mathematical methods in solutions of the problems presented at the Third International Students' Olympiad in Cryptography // Прикладная дискретная математика. — 2018. — №. 40. — С. 34–58.

[51] Voskuil H. A special basis for the Leech lattice // Indagationes Mathematicae (Proceedings). — North-Holland, 1987. — Т. 90. — №. 1. — С. 73–86.

[52] Wagner T. J. A search technique for quasi-perfect codes // Information and Control. — 1966. — Т. 9. — №. 1. — С. 94–99.

[53] Wang Q. The covering radius of the Reed-Muller code $RM(2,7)$ is 40 // Discrete Mathematics. — 2019. — Т. 342. — №. 12. — Статья 111625.

[54] Зиновьев В. А., Леонтьев В. К. О совершенных кодах // Проблемы передачи информации. — 1972. — Т. 8. — №. 1. — С. 26–35.

Публикации автора по теме диссертации

[55] Облаухов А. К. О метрическом дополнении подпространств булева куба // Дискретный анализ и исследование операций. — 2016. — Т. 23. — №. 3. — С. 93–106. (Перевод: Oblaukhov A. K. Metric complements to subspaces in the Boolean cube // Journal of Applied and Industrial Mathematics. — 2016. — Т. 10. — №. 3. — С. 397–403.)

[56] Oblaukhov A. K. Maximal metrically regular sets // Сибирские электронные математические известия. — 2018. — Т. 15. — С. 1842–1849.

[57] Oblaukhov A. A lower bound on the size of the largest metrically regular subset of the Boolean cube // Cryptography and Communications. — 2019. — Т. 11. — №. 4. — С. 777–791.

[58] Oblaukhov A. K. On metric complements and metric regularity in finite metric spaces // Прикладная дискретная математика. — 2020. — №. 49. — С. 35–45.

[59] Oblaukhov A. On metric regularity of Reed-Muller codes // Designs, Codes and Cryptography. — 2020. Опубликована онлайн. DOI: 10.1007/s10623-020-00813-z

[60] Облаухов А. К. О некоторых метрических свойствах линейных подпространств булева куба // Прикладная дискретная математика. Приложение. — 2015. — №. 8. — С. 13–15.

[61] Облаухов А. К. О максимальных метрически регулярных множествах // Прикладная дискретная математика. Приложение. — 2017. — №. 10. — С. 23–24.

[62] Облаухов А. К. Нижняя оценка мощности наибольшего метрически регулярного подмножества булева куба // Прикладная дискретная математика. Приложение. — 2018. — №. 11. — С. 14–16.

[63] Oblaukhov A. Metrically regular subsets of the Boolean cube // Тезисы международной конференции “Boolean Functions and their Applications (BFA) 2019”.

[64] Oblaukhov A. Metric regularity of Reed-Muller codes // Тезисы международной конференции “Boolean Functions and their Applications (BFA) 2020”.

Приложение А

Приложение к доказательству леммы 5.17 из раздела 5.8

Таблицы 2-5 показывают, что для любого класса EA-эквивалентности $\widehat{\mathcal{R}}^i_{1,5}$ метрического дополнения $\widehat{\mathcal{R}}_{1,5}$ и для любого класса EA-эквивалентности C пространства $\mathbb{F}_2^{32}$ существует функция $f \in C$ и функция $g \in \widehat{\mathcal{R}}^i_{1,5}$ такие, что $f+g$ не принадлежит $\widehat{\mathcal{R}}_{1,5}$. Заметим, что, если данная функция f не содержится в $\widehat{\mathcal{R}}_{1,5}$, а $f+g$ принадлежит классу C', то нам не нужно искать функцию из класса C', обладающую данными свойствами, поскольку $(f+g)+g = f$ не принадлежит $\widehat{\mathcal{R}}_{1,5}$ — по этой причине некоторые строки нижеследующих таблиц не заполнены.

Обозначения в таблицах 2-5 совпадают с таковыми в таблице 1 (см. раздел 5.2). Второй столбец таблицы 5 содержит “канонические” представители для каждого класса EA-эквивалентности — такие, которые были описаны в работе [3] Э. Берлекэмпом и Л. Уэлшем. В прочих столбцах и таблицах некоторые представители изменены либо при помощи простого переименования переменных, либо с помощью более сложных преобразований. Эти более сложные преобразования помечены звёздочкой и описаны ниже для каждой из таблиц, вместе с другими пояснениями. Здесь и далее “$i \leftarrow i+j$” означает преобразование “$x_i \leftarrow x_i + x_j$”, в то время как двунаправленные стрелки обозначают перемену двух переменных местами.

Таблица 2: Представители f для классов 7, 9, 10 и 22 (столбец 2) получены из “канонических” при помощи следующих преобразований:
$(7)\ 3\leftarrow 3+0;\ (9)\ 4\leftarrow 4+3+0;\ (10)\ 1\leftarrow 1+0;\ (22)\ 4\leftrightarrow 5;\ 1\leftrightarrow 3;$
Функции g из $\widehat{\mathcal{R}}^1_{1,5}$ (третий столбец) получены из “канонических” при помощи следующих преобразований:
$2345{+}123{+}24{+}35 \circ (2\leftarrow 2{+}0) = 2345{+}345{+}123{+}13{+}24{+}35;$
$2345{+}123{+}24{+}35 \circ (5\leftarrow 5{+}0) = 2345{+}234{+}123{+}24{+}35;$
$2345{+}123{+}24{+}35 \circ (1\leftarrow 1{+}0) = 2345{+}123{+}24{+}35{+}23;$

Преобразования, производящие функции в столбце 5 из функций h в столбце 4:
$(1)\ 2\leftarrow 2{+}0;\ 4\leftarrow 4{+}0;\ 1\leftrightarrow 3;\ (2)\ 2\leftarrow 2{+}0;\ 4\leftarrow 4{+}0;\ 1\leftarrow 1{+}4;\ 3\leftarrow 3{+}0;\ 5\leftarrow 5{+}2;\ 1\leftrightarrow 3;$
$2\leftrightarrow 4;\ 3\leftrightarrow 5;\ (3)\ 1\leftrightarrow 3;\ 4\leftrightarrow 5;\ (5)\ 3\leftarrow 3{+}0;\ 1\leftrightarrow 2;\ (6)\ 3\leftarrow 3{+}0;\ 1\leftrightarrow 3;\ 3\leftrightarrow 4;\ 4\leftrightarrow 5;$
$(7)\ 5\leftarrow 5{+}0;\ 1\leftrightarrow 5;\ 3\leftrightarrow 4;\ (8)\ 1\leftrightarrow 3;\ 2\leftrightarrow 5;\ (9)\ 4\leftarrow 4{+}0;\ 1\leftarrow 1{+}2;\ 1\leftrightarrow 4;\ 2\leftrightarrow 5;$

(10) $4{\leftarrow}4{+}3; 2{\leftarrow}2{+}5; 1{\leftrightarrow}4;$ (11) $1{\leftarrow}1{+}4;$ (12) $1{\leftarrow}1{+}2; 2{\leftrightarrow}4;$ (13) $3{\leftarrow}3{+}0; 4{\leftarrow}4{+}0;$
$1{\leftrightarrow}4; 2{\leftrightarrow}5; 4{\leftrightarrow}5;$ (15) $3{\leftarrow}3{+}0; 1{\leftrightarrow}4; 2{\leftrightarrow}3; 4{\leftrightarrow}5;$ (16) $1{\leftarrow}1{+}0; 3{\leftarrow}3{+}0; 1{\leftrightarrow}4; 2{\leftrightarrow}3;$
$4{\leftrightarrow}5;$ (17) $1{\leftarrow}1{+}0; 1{\leftrightarrow}5; 3{\leftrightarrow}4; 2{\leftrightarrow}5;$ (18) $2{\leftrightarrow}4; 3{\leftrightarrow}5;$ (20) $4{\leftarrow}4{+}3{+}0; 5{\leftarrow}5{+}2{+}0;$
(23) $2{\leftrightarrow}4; 3{\leftrightarrow}5; 5{\leftarrow}5{+}2{+}0; 1{\leftarrow}1{+}0; 4{\leftarrow}4{+}3{+}0;$ (24) $2{\leftrightarrow}4; 3{\leftrightarrow}5; 5{\leftarrow}5{+}2{+}0;$
$1{\leftarrow}1{+}0; 4{\leftarrow}4{+}3{+}0;$ (26) $2{\leftrightarrow}4; 3{\leftrightarrow}5;$

Таблица 3: Функции g из $\widehat{\mathcal{R}}^2_{1,5}$ (третий столбец) получены из "канонических" при помощи переименования переменных. Преобразования, производящие функции в столбце 5 из функций h в столбце 4:
(1) $2{\leftrightarrow}3;$ (2) $4{\leftarrow}4{+}2{+}0; 2{\leftrightarrow}3;$ (3) $1{\leftarrow}1{+}0; 2{\leftrightarrow}3;$ (4) $3{\leftarrow}3{+}2{+}0; 1{\leftarrow}1{+}2{+}3;$
(7) $4{\leftarrow}4{+}2{+}0; 2{\leftrightarrow}4; 3{\leftrightarrow}5;$ (8) $2{\leftrightarrow}4;$ (10) $2{\leftarrow}2{+}4{+}0; 2{\leftrightarrow}4; 3{\leftrightarrow}5;$ (11) $2{\leftarrow}2{+}5{+}0;$
(13) $2{\leftarrow}2{+}5{+}0; 5{\leftarrow}5{+}3{+}0; 3{\leftrightarrow}5;$ (15) $2{\leftrightarrow}4; 3{\leftrightarrow}5;$ (16) $1{\leftarrow}1{+}0; 2{\leftrightarrow}4; 3{\leftrightarrow}5;$
(17) $1{\leftarrow}1{+}0; 2{\leftrightarrow}5; 3{\leftrightarrow}4;$ (18) $2{\leftrightarrow}4; 3{\leftrightarrow}5;$ (19) $3{\leftarrow}3{+}0; 1{\leftrightarrow}5;$ (21) $1{\leftrightarrow}5;$
(23) $5{\leftarrow}5{+}0; 1{\leftrightarrow}5; 2{\leftrightarrow}4; 3{\leftrightarrow}5;$ (24) $5{\leftarrow}5{+}0; 3{\leftarrow}3{+}5; 2{\leftrightarrow}4; 3{\leftrightarrow}5;$ (25) $4{\leftarrow}4{+}0; 2{\leftrightarrow}4;$
$3{\leftrightarrow}5;$ (26) $4{\leftarrow}4{+}0; 2{\leftarrow}2{+}5; 2{\leftrightarrow}4; 3{\leftrightarrow}5;$ (27) $1{\leftrightarrow}2; 4{\leftrightarrow}5;$

Таблица 4: Представители f для классов 4 и 9 (столбец 2) получены из "канонических" при помощи следующих преобразований:
(4) $3{\leftarrow}3{+}0;$ (9) $1{\leftarrow}1{+}2;$
Функции g из $\widehat{\mathcal{R}}^3_{1,5}$ (третий столбец) получены из "канонических" при помощи следующих преобразований:
$123{+}145{+}23{+}24{+}35 \circ (1{\leftarrow}1{+}2) = 123{+}145{+}245{+}24{+}35;$
$123{+}145{+}245{+}24{+}35 \circ (3{\leftarrow}3{+}0) = 123{+}145{+}245{+}24{+}35{+}12;$
$123{+}145{+}245{+}24{+}35{+}12 \circ (4{\leftrightarrow}5) = 123{+}145{+}245{+}25{+}34{+}12;$
$123{+}145{+}245{+}24{+}35{+}12 \circ (2{\leftrightarrow}4; 3{\leftrightarrow}5) = 123{+}145{+}234{+}24{+}35{+}14;$
$123{+}145{+}23{+}24{+}35 \circ (2{\leftrightarrow}4; 3{\leftrightarrow}5) = 123{+}145{+}45{+}24{+}35;$

Преобразования, производящие функции в столбце 5 из функций h в столбце 4:
(1) $3{\leftarrow}3{+}0;$ (2) $3{\leftarrow}3{+}0;$ (4) $1{\leftarrow}1{+}0;$ (5) $1{\leftarrow}1{+}2; 1{\leftarrow}1{+}0;$ (6) $2{\leftarrow}2{+}5{+}0;$
$3{\leftarrow}3{+}4{+}0; 1{\leftarrow}1{+}0; 2{\leftrightarrow}4; 3{\leftrightarrow}5;$ (7) $3{\leftarrow}3{+}4; 1{\leftarrow}1{+}4; 2{\leftrightarrow}4; 3{\leftrightarrow}5;$ (8) $2{\leftarrow}2{+}5{+}0;$
$2{\leftrightarrow}4; 3{\leftrightarrow}5;$ (9) $5{\leftarrow}5{+}0; 2{\leftarrow}2{+}5{+}0; 2{\leftrightarrow}4; 3{\leftrightarrow}5;$ (11) $3{\leftarrow}3{+}2; 2{\leftrightarrow}4; 3{\leftrightarrow}5; 2{\leftrightarrow}3;$
(14) $2{\leftrightarrow}4; 3{\leftrightarrow}5;$ (15) $5{\leftarrow}5{+}2{+}0; 3{\leftrightarrow}4;$ (16) $3{\leftrightarrow}4;$ (17) $4{\leftarrow}4{+}3{+}0;$ (19) $1{\leftarrow}1{+}0;$
$3{\leftarrow}3{+}4; 2{\leftarrow}2{+}5; 2{\leftrightarrow}4; 3{\leftrightarrow}5;$ (21) $3{\leftarrow}3{+}0; 1{\leftrightarrow}4; 2{\leftrightarrow}3; 4{\leftrightarrow}5;$ (22) $5{\leftarrow}5{+}0; 2{\leftarrow}2{+}4;$
$2{\leftrightarrow}4; 3{\leftrightarrow}5;$ (23) $5{\leftarrow}5{+}0; 1{\leftrightarrow}5; 3{\leftrightarrow}4;$ (24) $5{\leftarrow}5{+}0; 5{\leftarrow}5{+}2{+}0; 1{\leftrightarrow}5; 3{\leftrightarrow}4;$

(27) $5{\leftarrow}5{+}2;\ 1{\leftarrow}1{+}0;\ 3{\leftarrow}3{+}4;$

Таблица 5: Функции g из $\widehat{\mathcal{R}}^4_{1,5}$ (третий столбец) получены из "канонических" при помощи переименования переменных. Преобразования, производящие функции в столбце 5 из функций h в столбце 4:
(2) $2{\leftrightarrow}4;$ (7) $2{\leftrightarrow}3;$ (9) $2{\leftrightarrow}3;\ 4{\leftrightarrow}5;$ (16) $1{\leftarrow}1{+}0;$ (17) $1{\leftarrow}1{+}0;$ (19) $3{\leftarrow}3{+}0;$
(21) $1{\leftrightarrow}2;\ 4{\leftrightarrow}5;$ (23) $1{\leftarrow}1{+}0;$ (24) $1{\leftarrow}1{+}0;$ (25) $2{\leftrightarrow}3;\ 4{\leftrightarrow}5;$ (27) $1{\leftrightarrow}3;\ 2{\leftrightarrow}4;$

№	Представитель f	g из $\widehat{\mathcal{R}}^1_{1,5}(14)$	Сумма $h=f{+}g$	h эквивалентна	$C(h)$
0	0	—	—	—	—
1	2345	2345+345+123+13+24+35	123+345+13+24+35	123+145+24	25
2	2345+12	2345+345+123+13+24+35	123+345+12+13+24+35	123+145+23	24
3	2345+24	2345+123+24+35	123+35	123+14	21
4	2345+24+35	2345+123+24+35	123	←	19
5	2345+12+35	2345+123+24+35	123+12+24	123+14	21
6	2345+123	2345+234+123+24+35	234+24+35	123+14	21
7	2345+245+123*	2345+123+24+35	245+24+35	123+14	21
8	2345+123+24	2345+123+24+35	35	12	27
9	2345+123+14+13*	2345+345+123+13+24+35	345+14+24+35	123+14	21
10	2345+123+45+23*	2345+123+24+35	23+24+35+45	12	27
11	2345+123+12+35	2345+123+24+35	12+24	12	27
12	2345+123+14+35	2345+123+24+35	14+24	12	27
13	2345+123+13+45	2345+345+123+13+24+35	345+24+35+45	123+14	21
14[1]	2345+123+24+35	2345+123+24+35	0	←	0
15	2345+123+145	2345+234+123+24+35	145+234+24+35	123+145+24	25
16	2345+123+145+45	2345+234+123+24+35	145+234+24+35+45	123+145+24	25
17	2345+123+145+24+45	2345+123+24+35	145+45+35	123+14	21
18	2345+123+145+24+35	2345+123+24+35	145	123	19
19	123	—	—	—	—
20	123+45	2345+123+24+35	2345+24+35+45	2345+23+45	4
21	123+14	—	—	—	—
22[2]	123+24+35*	2345+123+24+35	2345	←	1
23	123+145	2345+123+24+35+23	2345+145+24+35+23	2345+123+45	10
24	123+145+23	2345+123+24+35	2345+145+24+35+23	2345+123+45	10
25	123+145+24	—	—	—	—
26[3]	123+145+23+24+35	2345+123+24+35	2345+145+23	2345+123+45	10
27	12	—	—	—	—
28[4]	24+35	2345+123+24+35	2345+123	←	6

Таблица 2 — Доказательство леммы 5.17 для класса $\widehat{\mathcal{R}}^1_{1,5}$.

№	Представитель f	g из $\widehat{\mathcal{R}}^2_{1,5}(22)$	Сумма $h=f+g$	h эквивалентна	$C(h)$
0	0	—	—	—	—
1	2345	123+14+25	2345+123+14+25	2345+123+14+35	12
2	2345+12	123+14+25	2345+123+12+14+25	2345+123+14+35	12
3	2345+23	123+14+25	2345+123+23+14+25	2345+123+14+35	12
4	2345+25+34	123+14+25	2345+123+14+34	2345+123+14	9
5	2345+14+25	123+14+25	2345+123	←	6
6	2345+123	—	—	—	21
7	2345+123+12	123+14+25	2345+12+14+25	2345+12+34	5
8	2345+123+25	123+14+25	2345+14	2345+12	2
9	2345+123+14	—	—	—	21
10	2345+123+45	123+14+25	2345+14+25+45	2345+12+34	5
11	2345+123+12+34	123+15+34	2345+12+15	2345+12	2
12	2345+123+14+35	—	—	—	27
13	2345+123+12+45	123+15+34	2345+12+15+45+34	2345+12+34	5
14[1]	2345+123+24+35	123+24+35	2345	←	1
15	2345+123+145	123+14+25	2345+145+14+25	2345+12+34	11
16	2345+123+145+45	123+14+25	2345+145+14+25+45	2345+12+34	11
17	2345+123+145+24+45	123+24+35	2345+145+35+45	2345+123+24	8
18	2345+123+145+24+35	123+24+35	2345+145	2345+123	6
19	123+235	123+14+25	235+14+25	123+45	20
20	123+45	—	—	—	—
21	123+14	123+14+25	25	12	27
22[2]	123+14+25	123+14+25	0	←	0
23	123+145	123+14+25	145+14+25	123+14	21
24	123+145+23	123+14+25	145+14+25+23	123+45	20
25	123+145+24	123+15+24	145+15	123	19
26[3]	123+145+23+24+35	123+15+24	145+15+23+35	123+45	20
27	14	123+14+25	123+25	123+14	21
28[4]	14+25	123+14+25	123	←	19

Таблица 3 — Доказательство леммы 5.17 для класса $\widehat{\mathcal{R}}^2_{1,5}$.

№	Представитель f	g из $\widehat{\mathcal{R}}^3_{1,5}(26)$	Сумма $h = f+g$	h эквивалентна	$C(h)$
0	0	—	—	—	—
1	2345	123+145+245+24+35+12	2345+123+145+245+24+35+12	2345+123+145+24+35	18
2	2345+12	123+145+245+24+35	2345+123+145+245+24+35+12	2345+123+145+24+35	18
3	2345+23	123+145+23+24+35	2345+123+145+24+35	←	18
4	2345+245+23+45*	123+145+245+24+35	2345+123+145+23+24+35+45	2345+123+145+24+35	18
5	2345+12+35	123+145+245+24+35+12	2345+123+145+245+24	2345+123+145+24+45	17
6	2345+123	123+145+23+24+35	2345+145+23+24+35	2345+123+45	10
7	2345+123+12	123+145+245+24+35	2345+145+245+24+35+12	2345+123+35+14	12
8	2345+123+24	123+145+23+24+35	2345+145+23+35	2345+123+45	10
9	2345+123+14+23+24*	123+145+234+24+35+14	2345+145+234+23+35	2345+123+12+45	13
10	2345+123+45	—	—	—	—
11	2345+123+12+34	123+145+245+25+34+12	2345+145+245+25	2345+123+24	8
12	2345+123+14+35	—	—	—	—
13	2345+123+12+45	—	—	—	—
14[1]	2345+123+24+35	123+145+23+24+35	2345+145+23	2345+123+45	10
15	2345+123+145	123+145+23+24+35	2345+23+24+35	2345+23+45	4
16	2345+123+145+45	123+145+45+24+35	2345+24+35	2345+23+45	4
17	2345+123+145+24+45	123+145+23+24+35	2345+23+35+45	2345+23+45	4
18	2345+123+145+24+35	—	—	—	—
19	123	123+145+23+24+35	145+23+24+35	123+45	20
20	123+45	—	—	—	—
21	123+14	123+145+234+24+35+14	145+234+24+35	123+145+24	25
22[2]	123+14+25	123+145+23+25+34	145+14+23+34	123+45	20
23	123+145	123+145+245+24+35	245+24+35	123+14	21
24	123+145+23	123+145+245+24+35	245+23+24+35	123+14	21
25	123+145+24	—	—	—	—
26[3]	123+145+23+24+35	123+145+23+24+35	0	←	0
27	35	123+145+45+24+35	123+145+45+24	123+145+23	24
28[4]	24+35	123+145+23+24+35	123+145+23	←	24

Таблица 4 — Доказательство леммы 5.17 для класса $\widehat{\mathcal{R}}^3_{1,5}$.

№	Представитель f	g из $\widehat{\mathcal{R}}^4_{1,5}(28)$	Сумма $h = f+g$	h эквивалентна	$C(h)$
0	0	—	—	—	—
1	2345	12+34	2345+12+34	←	5
2	2345+12	12+34	2345+34	2345+23	3
3	2345+23	—	—	—	—
4	2345+23+45	23+45	2345	←	1
5	2345+12+34	—	—	—	—
6	2345+123	12+34	2345+123+12+34	←	11
7	2345+123+12	12+34	2345+123+34	2345+123+24	8
8	2345+123+24	—	—	—	—
9	2345+123+14	14+35	2345+123+35	2345+123+24	8
10	2345+123+45	12+45	2345+123+12	←	7
11	2345+123+12+34	—	—	—	—
12	2345+123+14+35	14+35	2345+123	←	6
13	2345+123+12+45	12+45	2345+123	←	6
14[1]	2345+123+24+35	24+35	2345+123	←	6
15	2345+123+145	24+35	2345+123+145+24+35	←	18
16	2345+123+145+45	23+45	2345+123+145+23	2345+123+145+45	16
17	2345+123+145+24+45	23+45	2345+123+145+24+23	2345+123+145+24+45	17
18	2345+123+145+24+35	—	—	—	—
19	123	12+45	123+12+45	123+45	20
20	123+45	—	—	—	—
21	123+14	14+25	123+25	123+14	21
22[2]	123+14+25	14+25	123	←	19
23	123+145	23+45	123+145+23+45	123+145	23
24	123+145+23	23+45	123+145+45	123+145+23	24
25	123+145+24	24+35	123+145+35	123+145+24	25
26[3]	123+145+23+24+35	24+35	123+145+23	←	24
27	12	12+34	34	12	27
28[4]	12+34	12+34	0	←	0

Таблица 5 — Доказательство леммы 5.17 для класса $\widehat{\mathcal{R}}^4_{1,5}$.