МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
МОСКОВСКИЙ ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ
(ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ)

Э. М. Габидулин

ЛЕКЦИИ ПО АЛГЕБРАИЧЕСКОМУ КОДИРОВАНИЮ

Допущено
Учебно-методическим объединением
высших учебных заведений Российской Федерации
по образованию в области прикладных математики и физики
в качестве учебного пособия для студентов вузов по направлению подготовки
«Прикладные математика и физика»

МОСКВА
МФТИ
2015

УДК 621.391(075)
ББК 32.81я73
Г12

Рецензенты:
Кафедра безопасности информационных систем
Санкт-Петербургского государственного университета
аэрокосмического приборостроения
(зав. кафедрой заслуженный деятель науки Российской Федерации
доктор технических наук, профессор *Е.А. Крук*)

Кандидат технических наук, ведущий научный сотрудник *В. Б. Афанасьев*

Габидулин, Э. М.

Г12 **Лекции по алгебраическому кодированию** /
Э.М. Габидулин : учебное пособие – М. : МФТИ, 2015. – 107 с.

ISBN 978-5-7417-0573-5

В учебное пособие включены основные понятия теории конечных полей Галуа, описаны блоковые коды и их корректирующие свойства, определены циклические коды, представлены коды Боуза–Чоудхури–Хоквингема, коды Рида–Соломона и ранговые коды. Новым является включение раздела «Ранговые коды».

Пособие предназначено для студентов технических вузов, начинающих изучать теорию передачи сообщений с использованием алгебраических методов кодирования, а также может оказаться полезным аспирантам, связанным с этой тематикой, и инженерам-связистам.

УДК 621.391(075)
ББК 32.81я73

ISBN 978-5-7417-0573-5

Оглавление

Предисловие **6**

Глава 1. Конечные поля **8**
1.1. Группы 8
1.2. Кольца и поля 10
1.3. Многочлены над простым полем 12
1.4. Деление с остатком для чисел и многочленов . . 13
1.5. Алгоритм Евклида для многочленов 13
1.6. Конечное кольцо многочленов над конечным полем. Расширенные конечные поля 15
1.7. Мультипликативная структура конечного поля . 17
1.8. След и нормальный базис 19
1.9. Некоммутативное кольцо линеаризованных многочленов $R_N[z]$ 19
1.10. Линейное пространство 24

Глава 2. Блоковые коды **27**
2.1. Задача кодирования 28
2.2. Корректирующая способность кода. Скорость передачи 29
2.2.1. Граница Синглтона 30
2.2.2. Граница Плоткина для больших расстояний . . . 30
2.2.3. Верхняя граница Плоткина для двоичных кодов 32
2.2.4. Граница Бассалыго–Элайеса для двоичных равновесных кодов 32
2.2.5. Верхняя граница Хэмминга 33
2.2.6. Нижняя граница Варшамова–Гилберта 33
2.3. Линейные коды 34

2.3.1. Линейные коды. Кодирование 35
2.3.2. Дуальное пространство. Проверочная матрица 35
2.3.3. Систематическое кодирование 36
2.3.4. Другое систематическое кодирование 36
2.3.5. Расстояние в линейных кодах 36
2.3.6. Синдромное декодирование линейного кода 37

Глава 3. Циклические коды **38**
3.1. Представление циклических кодов 38
3.2. Систематическая форма порождающей и проверочной матриц 40

Глава 4. Коды Боуза—Чоудхури—Хоквингема **42**
4.1. Конструкция и параметры кодов БЧХ 42
4.2. Декодирование кодов БЧХ 44
4.2.1. Исправление одиночных ошибок 45
4.2.2. Исправление двойных ошибок 47
4.2.3. Общий случай исправления ошибок 48

Глава 5. Коды Рида—Соломона **52**
5.1. Конструкция кодов Рида—Соломона 52
5.2. Дискретное преобразование Фурье (ДПФ) 53
5.2.1. Циклическая свертка и произведение Адамара 55
5.2.2. Дискретное преобразование Фурье для свертки 55
5.3. Кодирование кодов Рида–Соломона 56
5.4. Декодирование кодов Рида–Соломона 57
5.4.1. Пять шагов декодирования кодов Рида–Соломона 58
5.4.2. Пример: исправление одиночных ошибок 59
5.4.3. Пример: исправление двойных ошибок 59

Глава 6. Ранговые коды **61**
6.1. Ранговая метрика 61
6.2. Коды в ранговой метрике 63
6.2.1. Матричные ранговые коды 63
6.2.2. Векторные ранговые коды 63
6.2.3. Эквивалентность матричных и векторных ранговых кодов 63
6.3. Граница Синглтона для минимального расстояния ранговых кодов 64

6.4. Линейные векторные ранговые коды 64
6.4.1. Проверочная матрица рангового кода 65
6.4.2. Конструкции векторных ранговых МРР-кодов 65
6.4.3. Порождающая матрица МРР-кода 66
6.5. Линеаризованные многочлены 66
6.6. Кодирование МРР-кодов 67
6.7. Декодирование МРР-кодов 68
6.7.1. Пример 1: ошибка ранга 1 69
6.7.2. Пример 2: ошибка ранга 2 70
6.7.3. Общий случай 71

Глава 7. Задачи и упражнения **73**
7.1. Задачи к главе 1 73
7.2. Задачи к главе 2 80
7.3. Задачи к главе 3 84
7.4. Задачи к главе 4 86
7.5. Задачи к главе 5 91
7.6. Задачи к главе 6 97

Литература **106**

Предисловие

Пособие содержит материал лекций, прочитанных автором студентам второго курса факультета радиотехники и кибернетики Московского физико-технического института (государственного университета). Тема «Алгебраическое кодирование» — очень широкая и серьёзная. К настоящему времени на эту тему написано много хороших научных монографий, учебников и учебных пособий, включая недавнее учебное пособие Ю.Л. Сагаловича «Введение в алгебраические коды» выдержавшее несколько изданий с дополнениями.

Необходимость написания ещё одного учебного пособия возникла по двум причинам. Первая причина — очень мало времени (всего 8 лекций) было отведено по программе на изучение этого предмета студентам МФТИ. Поэтому перед автором встала задача дополнить лекционное прослушивание очень кратким и доступным, но в то же время научным изложением материала. Вторая причина — надо было включить материал, которого нет в других учебниках по алгебраическому кодированию, а именно по ранговым кодам. В настоящее время теория кодирования в ранговой метрике успешно развивается и имеет достаточно хорошее применение, например в сетевом кодировании и пространственно-временном кодировании.

В первой главе представлены основные понятия и определения из теории конечных полей Галуа. Проработка этой главы необходима для усвоения остальной части представленного здесь материала.

Во второй главе «Блоковые коды» основное внимание обращено на главное свойство помехоустойчивых кодов — корректирующую способность. Потенциальные свойства определены границами. Приведён вывод известных границ – Синглтона, Плоткина, Хэмминга и Варшамова–Гильберта. Определены линейные коды и рассмотрены основные вопросы кодирования и декодирования.

В третьей главе даны определения и представлены общие свойства циклических кодов.

Четвёртая глава посвящена наиболее известным циклическим кодам — кодам Боуза–Чоудхури–Хоквингема (БЧХ). Здесь приведены конструкциии, основные параметры и характеристики кодов БЧХ, а

также алгоритмы кодирования и декодирования.

В пятой главе представлены коды Рида–Соломона. Приведены конструкции, алгоритмы кодирования и декодирования. В настоящее время эти коды широко используются на практике.

В шестой главе описаны ранговые коды. Введены понятия основного и расширенного полей, приведены алгоритмы кодирования и декодирования.

Отдельную часть пособия составляют задачи. Они разделены на части, соответствующие главам. В каждой части представлены типовые задачи с решениями и несколько задач, где даны условия, но нет решений. Задачи с решениями демонстрируют методы, используемые в теории алгебраического кодирования. Задачи с условиями без решений позволят проверить обучающемуся усвоение этих методов.

В список литературы включены учебные пособия, которые могут дополнить и расширить круг рассматриваемых вопросов, касающихся темы «Алгебраическое кодирование».

Автор благодарит своих рецензентов – Е.А. Крука и В.Б. Афанасьева – за обсуждение вопросов, рассматриваемых в этом пособии, и критические замечания.

Г л а в а 1

Конечные поля, многочлены, векторные пространства

1.1. Группы

Множество объектов F называется группой, если на нем задана *бинарная* операция $*$, при которой двум элементам a и b из этого множества сопоставляется третий элемент $c = a * b$ того же множества. Это свойство называется *замкнутостью* множества F относительно операции $*$. Слово «бинарный» означает, что операция определена на всех парах элементов из F, не обязательно различных. Операция $*$ должна удовлетворять следующим аксиомам.

1. Для любых трех элементов из F выполняется закон ассоциативности $(a * b) * c = a * (b * c)$.

2. Существует *нейтральный элемент* $e \in F$, для которого выполняется соотношение $a * e = e * a = a$ для всех $a \in F$.

3. Для каждого элемента $a \in F$ существует обратный по операции $*$ элемент, обозначаемый a', со свойством $a * a' = a' * a = e$.

Нейтральный элемент e *единственный*. Каждый элемент $a \in F$ имеет *единственный* обратный a'.

Группа F называется *коммутативной* (или *абелевой*), если операция $*$ коммутативна: $a * b = b * a$.

Группа F называется *конечной*, если число элементов в ней конечно. Это число называется *порядком* группы.

Пример 1. ***Сложение по модулю*** 2. *Самая простая группа состоит из двух чисел* $F = \{0, 1\}$. *Бинарная операция на этом множестве обозначается* $\oplus$ *и называется сложением по модулю* 2. *Она определяется таблицей сложения*

$\oplus$	0	1
0	0	1
1	1	0

,

из которой следует, что

$$0 \oplus 0 = 0, \quad 0 \oplus 1 = 1, \quad 1 \oplus 0 = 1, \quad 1 \oplus 1 = 0.$$

Множество $F = \{0, 1\}$ *замкнуто относительно операции* $\oplus$. *Операция* $\oplus$ *коммутативна и ассоциативна, так как для любых трех элементов* $a, b, c \in G$ *легко проверить, что* $(a \oplus b) \oplus c = a \oplus (b \oplus c)$. *Нейтральным элементом является* 0. *Обратным к* 0 *элементом является* 0. *Обратным элементом к* 1 *является* 1.

Пример 2. ***Сложение по модулю m.*** *Пусть* m *— положительное целое число. Рассмотрим множество целых чисел* $F = \{0, 1, \ldots, m - 1\}$. *Пусть знак* $+$ *означает обычное сложение. Для целых чисел* a *и* m *алгоритм Евклида деления с остатком дает:* $a = qm + r$, *где остаток* r *— это неотрицательное целое между* 0 *и* $m - 1$. *Введем на* F *бинарную операцию* $*$, *которую обозначим* $\boxplus$ *и определим следующим образом: если* $a \in F$ *и* $b \in F$, *то*

$$a \boxplus b = r, \tag{1.1}$$

где r *— остаток от деления числа* $a + b$ *на* m. *Так как* $0 \leq r \leq m-1$, *то множество* F *замкнуто относительно бинарной операции* $\boxplus$, *которую называют сложением по модулю* m. *Очевидно, что эта операция коммутативна.*

Нейтральным элементом для этой операции является $e = 0$. *Обратным элементом к элементу* a *в этой операции является элемент* $a' = m - a$, *так как* $a \boxplus a' = a \boxplus (m - a) = 0$. *Легко проверить также, что закон ассоциативности выполняется. Если* $a, b, c \in F$, *то*

$$(a \boxplus b) \boxplus c = a \oplus (b \boxplus c).$$

Таким образом, множество F *с операцией* $\boxplus$ *является группой порядка* m. *Эту группу называют также аддитивной группой.*

Пример 3. ***Умножение по модулю m.*** *Пусть* m *— положительное целое. Пусть знак* $\cdot$ *означает обычное умножение. Обозначим операцию умножения двух целых чисел по модулю* m *как* $\odot$ *и определим ее следующим образом: если* a *и* b *целые, то*

$$a \odot b = r, \tag{1.2}$$

где r *— остаток от деления* $a \cdot b$ *на* m. *Эта операция коммутативна и ассоциативна.*

Построим с ее помощью мультипликативную группу. Рассмотрим сначала случай, когда $m = p$ — простое *число. Рассмотрим множество* $F^* = \{1, 2, \ldots, p-1\}$ *с бинарной операцией* $\odot$. *Все числа в* F^* *взаимно просты с* p. *Для любых* $a, b \in F^*$ *число* $a \cdot b$ *взаимно просто с* p, *поэтому остаток* r *от деления числа* $a \cdot b$ *на* $m = p$ *строго больше* 0 *и меньше* p: $1 \le r \le p-1$. *Для составных чисел* m *остаток может равняться* 0. *Таким образом, множество* F^* *замкнуто относительно операции* $\odot$ *умножения по модулю простого числа* p. *Нейтральным элементом является элемент* 1, *так как* $1 \odot a = a \odot 1 = a$. *Кроме того, каждый элемент* $a \in F^*$ *имеет обратный по умножению элемент* a', *то есть* $a \odot a' = a' \odot a = 1$. *Действительно, в последовательности* $\{a \odot 1, a \odot 2, \ldots, a \odot (p-1)\}$ *все элементы являются различными и принадлежащими* F^*, *так что найдется единственный элемент* a' *такой, что* $a \odot a' = 1$. *Обратный элемент обозначается* $a' = a^{-1}$.

Таким образом, множество F^* *с операцией умножения* $\odot$ *является коммутативной мультипликативной группой порядка* $p - 1$.

1.2. Кольца и поля

Множество F с двумя заданными на нем бинарными операциями $\boxplus$ и $\boxdot$ называется *кольцом*, если выполняются следующие условия:

1. F является аддитивной абелевой группой относительно операции $\boxplus$, называемой сложением в кольце.

2. Операция $\boxdot$, называемая умножением в кольце, ассоциативна: для любых $a, b, c \in F$

$$(a \boxdot b) \boxdot c = a \boxdot (b \boxdot c).$$

3. Выполняются законы дистрибутивности: для любых $a, b, c \in F$

$$a \boxdot (b \boxplus c) = a \boxdot b \boxplus a \boxdot c) \text{ и } (a \boxplus b) \boxdot c = a \boxdot c \boxplus b \boxdot c.$$

Нейтральный элемент аддитивной группы кольца F называется *нулем* кольца F и обозначается 0. Обратный по сложению к элементу $a \in F$ обозначается $-a$.

Для любого элемента $f \in F$ полагаем $0 \boxdot f = f \boxdot 0 = 0$.

Кольцо F называется кольцом *с единицей*, если в нем существует нейтральный элемент e по операции $\boxdot$, называемый мультипликативной единицей такой, что для любого $f \in F$ $e \boxdot f = f \boxdot e = f$.

В кольце с единицей не требуется существование обратных элементов по операции умножения $\boxdot$ для всех ненулевых элементов кольца. Элементы кольца, которые не имеют обратных элементов, называются делителями нуля.

Кольцо называется коммутативным, если операция $\boxdot$ коммутативна.

Пример 4. *Пусть $\boxplus = \oplus$ и $\boxdot = \odot$, то есть сложение и умножение двух целых чисел выполняются по модулю m. Множество $F = \{0, 1, 2, \ldots, m-1\}$ с этими операциями является коммутативным кольцом с единицей. Оно называется кольцом целых чисел по модулю m и обозначается $F = \mathbb{Z}_m$.*

Коммутативное кольцо с единицей называется *полем*, если множество $F^* = F \setminus \{0\}$ всех *ненулевых* элементов кольца образует мультипликативную группу относительно операции $\boxdot$.

Пример 5. *Пусть p — простое число. Очевидно, что множество $F = \{0, 1, 2, \ldots, p-1\}$ с бинарными операциями $\oplus$ (сложение по модулю p) и $\odot$ (умножение по модулю p) является конечным полем порядка p, так как множество F является аддитивной группой относительно операции $\oplus$, а множество $F^* = F \setminus \{0\} = \{1, 2, \ldots, p-1\}$ всех ненулевых элементов является мультипликативной группой относительно операции $\odot$. Такие поля называются простыми порядка p. Их обозначают $\mathbb{Z}_p$ или $GF(p)$.*

Характеристикой поля называют минимальное целое число s такое, что сумма s мультипликативных единиц равна 0:

$$\oplus \sum_{i=1}^{s} 1 = 0.$$

Характеристика любого поля всегда простое число и для поля $GF(p)$ равна p.

Конечные поля порядка q существуют для всех $q = p^m$, являющихся степенью простого, и только для них. Они называются также полями Галуа и обозначаются $\mathbb{F}_q$ или $GF(q)$. Конструкции конечных полей будут описаны позднее. Характеристика этих полей равна p. Более того, верна теорема

Теорема 1. *Для любых элементов a и b из $GF(p^m)$, $m \geq 1$*

$$(a + b)^p = a^p + b^p.$$

1.3. Многочлены над простым полем

Пусть $GF(p)$ — простое поле. *Многочленом* $f(x)$ от переменной x над полем $GF(p)$ называется выражение

$$f(x) = \sum_{i=0}^{n} f_i x^i, \tag{1.3}$$

где коэффициенты $f_i \in GF(p)$.

Степенью многочлена $f(x)$ называют максимальный номер ненулевого коэффициента. Степень многочлена $f(x)$ обозначается символом $\deg(f(x))$. В приведенном выше выражении $\deg(f) = n$, если $f_n \neq 0$. В этом случае коэффициент f_n многочлена называется *старшим коэффициентом*, а f_0 – *постоянным* или *свободным членом*. Если $f_n = 1$, многочлен называют *нормированным* или *приведенным*.

Для удобства многочлену 0 приписывают степень $\deg(0) = -\infty$. Этот многочлен и все многочлены степени 0 – это все элементы поля $GF(p)$. Они называются постоянными многочленами.

Все возможные многочлены конечной степени образуют аддитивную коммутативную группу, в которой *сумма* многочленов $f(x)$ и $g(x)$ определяется формулой

$$h(x) = f(x) + g(x) = \sum_{i=0}^{n} (f_i + g_i) x^i,$$

где $\deg(h) = n \leq \max[\deg f; \deg g]$. Степень суммы равна наибольшему индексу i, для которого $f_i + g_i \neq 0$. Коммутативность сложения следует из коммутативности сложения в $GF(q)$ коэффициентов многочленов. *Нулем* в этой группе является многочлен с нулевыми коэффициентами.

Произведение многочленов $f(x)$ степени s и $g(x)$ степени t определяется как

$$h(x) = f(x)g(x) = \sum_{i=0}^{s} x^i f_i \sum_{k=0}^{t} g_k x^k =$$

$$= \textstyle\sum_{j=0}^{s+t} x^j \sum_{i+k=j} f_i g_k = \sum_{j=0}^{s+t} x^j h_j,$$

где $h_j = \sum_{i=0}^{j} f_i g_{j-i}$. Степень многочлена $h(x)$ равна $s+t$, если $f_s \neq 0$ и $g_t \neq 0$. Коммутативность умножения многочленов следует из коммутативности умножения их коэффициентов.

Множество многочленов над $GF(p)$ конечной степени с введенными операциями сложения и умножения образует бесконечное *коммутативное кольцо* с единичным элементом $e(x) = 1$. Оно обозначается $GF(p)[x]$ или $\mathbb{Z}_p[x]$.

1.4. Деление с остатком для чисел и многочленов

Для чисел и многочленов существуют алгоритмы деления с остатком (алгоритмы Евклида).

Для чисел. Пусть r_0 и r_1 – целые числа. Тогда существуют единственные целые числа — *частное* q_1 и *остаток* r_2 — такие, что

$$r_0 = q_1 r_1 + r_2,$$

причем

$$0 \le r_2 < |r_1|.$$

Для многочленов. Пусть $r_0(x)$ и $r_1(x)$ – многочлены над $GF(p)$. Тогда существуют единственные многочлены — *частное* $q_1(x)$ и *остаток* $r_2(x)$ — такие, что

$$r_0 = q_1(x) r_1(x) + r_2(x),$$

причем либо

$$r_2(x) = 0,$$

либо

$$\deg(r_2(x)) < \deg(r_1(x)).$$

Алгоритмы деления с остатком применяют для нахождения наибольшего общего делителя двух чисел или для наибольшего общего делителя двух многочленов.

Рассмотрим подробнее алгоритм Евклида для многочленов.

1.5. Алгоритм Евклида для многочленов

Для многочленов $r_0(x)$ и $r_1(x)$ над $GF(p)$ существует *нормированный* многочлен $d(x) = \gcd(r_0(x), r_1(x))$, называемый *наибольшим общим делителем*, который делит многочлены $r_0(x)$ и $r_1(x)$ и делится на любой другой общий делитель многочленов $r_0(x)$ и $r_1(x)$. Найти $d(x)$ можно с помощью алгоритма Евклида, применяя многократно алгоритм деления.

В дальнейшем мы будем писать f вместо $f(x)$, если из контекста ясно, что речь идет о многочлене $f(x)$.

Предварительно введем две последовательности вспомогательных многочленов:

$$\begin{array}{l|ll} a_i = -q_{i-1}a_{i-1} + a_{i-2}, & a_0 = 1, & a_1 = 0. \\ b_i = -q_{i-1}b_{i-1} + b_{i-2}, & b_0 = 0, & b_1 = 1. \end{array}$$

Будем предполагать, что степень многочлена $r_0(x)$ больше или равна степени многочлена $r_1(x)$, $\deg(r_0) \geq \deg(r_1)$.

Шаг 1. Делим с остатком многочлен $r_0(x)$ на многочлен $r_1(x)$. Вычисляем также вспомогательные многочлены $a_0(x)$ и $b_0(x)$.

$$1. \mid r_0 = q_1 r_1 + r_2, \mid a_0 = 1, \mid b_0 = 0.$$

Если оказалось, что остаток $r_2(x) = 0$, то алгоритм заканчивает работу. В этом случае наибольший общий делитель равен $d(x) = r_1(x)$ (в приведенной форме).

Если $r_2(x) \neq 0$, то переходим к следующему шагу.

Шаг 2. Делим с остатком многочлен $r_1(x)$ на многочлен $r_2(x)$. Вычисляем также вспомогательные многочлены $a_1(x)$ и $b_1(x)$.

$$\begin{array}{l|l|l} 1. \; r_0 = q_1 r_1 + r_2, & a_0 = 1, & b_0 = 0. \\ 2. \; r_1 = q_2 r_2 + r_3, & a_1 = 0, & b_1 = 1. \end{array}$$

Если оказалось, что остаток $r_3(x) = 0$, то алгоритм заканчивает работу. В этом случае наибольший общий делитель равен $d(x) = r_2(x)$ (в приведенной форме).

Если $r_3(x) \neq 0$, то переходим к следующему шагу.

Шаг 3. Делим с остатком многочлен $r_2(x)$ на многочлен $r_3(x)$. Вычисляем также вспомогательные многочлены $a_2(x)$ и $b_2(x)$.

$$\begin{array}{l|l|l} 1. \; r_0 = q_1 r_1 + r_2, & a_0 = 1, & b_0 = 0. \\ 2. \; r_1 = q_2 r_2 + r_3, & a_1 = 0, & b_1 = 1. \\ 3. \; r_2 = q_3 r_3 + r_4, & a_2 = -q_1 a_1 + a_0, & b_2 = -q_1 b_1 + b_0. \end{array}$$

Если оказалось, что остаток $r_4(x) = 0$, то алгоритм заканчивает работу. В этом случае наибольший общий делитель равен $d(x) = r_3(x)$ (в приведенной форме).

Если $r_4(x) \neq 0$, то переходим к следующему шагу. Продолжаем до тех пор, пока не достигнем шага s такого, что остаток $r_{s+1}(x)$ на предыдущем шаге не равен 0, а остаток $r_{s+2}(x) = 0$.

Шаг *s*. Делим с остатком многочлен $r_s(x)$ на многочлен $r_{s+1}(x)$. Вычисляем также вспомогательные многочлены $a_s(x)$ и $b_s(x)$.

1.	$r_0 = q_1 r_1 + r_2,$	$a_0 = 1,$	$b_0 = 0.$
2.	$r_1 = q_2 r_2 + r_3,$	$a_1 = 0,$	$b_1 = 1.$
3.	$r_2 = q_3 r_3 + r_4,$	$a_2 = -q_1 a_1 + a_0,$	$b_2 = -q_1 b_1 + b_0.$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$s-1.$	$r_{s-1} = q_s r_s + r_{s+1},$	$a_{s-1} = -q_{s-2} a_{s-2} + a_{s-3},$	$b_{s-1} = -q_{s-2} b_{s-2} + b_{s-3}.$
$s.$	$r_s = q_{s+1} r_{s+1},$	$a_s = -q_{s-1} a_{s-1} + a_{s-2},$	$b_s = -q_{s-1} b_{s-1} + b_{s-2}.$

Так как степень $\deg(r_1)$ конечна, то процедура должна закончиться после конечного числа шагов. Если старший коэффициент последнего ненулевого остатка r_{s+1} равен a, то наибольший общий делитель многочленов $r_0(x)$ и $r_1(x)$ равен

$$d(x) = \gcd(r_0(x),\ r_1(x)) = a^{-1} r_{s+1}(x).$$

Попутно можно установить

$$r_i = a_i r_0 + b_i r_1, \qquad i = 0,\ 1,\ \ldots$$

1.6. Конечное кольцо многочленов над конечным полем. Расширенные конечные поля

Многочлены f и g над полем $GF(p)$ называются взаимно простыми, если их наибольший общий делитель равен 1.

Многочлен $f \in GF(p)[x]$ называется *неприводимым* над полем $GF(p)$, если он имеет *положительную* степень и делится только на постоянный многочлен $a \in GF(p)$ либо на многочлен af.

Любой неприводимый над $GF(p)$ многочлен степени m является делителем многочлена $x^{p^m-1} - 1$.

Нормированный неприводимый над $GF(p)$ многочлен $f(x)$ степени m называется *примитивным*, если он делит многочлен $x^{p^m-1} - 1$, но не делит многочлены $x^i - 1$, $i = 1, 2, \ldots, p^m - 2$.

Многочлен $f \in GF(p)[x]$, не являющийся неприводимым над $GF(p)$, называется *приводимым* над $GF(p)$.

Пусть $\varphi(x) = x^m + \varphi_{m-1} x^{m-1} + \cdots + \varphi_1 x + \varphi_0$ — нормированный многочлен над $GF(p)$ степени m. Построим кольцо многочленов по модулю $\varphi(x)$. Рассмотрим множество $F = \{f(x)\}$ всех многочленов $f(x) = f_{m-1} x^{m-1} + f_{m-2} x^{m-2} + \cdots + f_1 x + f_0$ над $GF(p)$ степени $m-1$

или меньше. Это множество содержит в точности $q = p^m$ различных многочленов, включая 0 и 1. Введем на этом множестве операции сложения и умножения.

Сложение $f + g$

$$f + g = \sum_{i=0}^{m-1} f_i\, x^i + \sum_{i=0}^{m-1} g_i\, x^i = \sum_{i=0}^{m-1} (f_i + g_i)\, x^i.$$

Таким образом, множество F замкнуто относительно сложения и является аддитивной группой.

Умножение $f \odot g$ или $fg \mod \varphi(x)$. Если $g = 0$, то полагаем по определению $f \odot 0 = 0 \odot f = 0$. Если $f \neq 0$, $g \neq 0$, то следует вычислить произведение fg как в кольце $GF(p)[x]$ и поделить с остатком на $\varphi(x)$: $fg = qm + r$. Тогда

$$f \odot g = fg \mod \varphi(x) = r.$$

Так как $\deg(r) < \deg(\varphi(x)) = m$, то множество F замкнуто относительно умножения. Законы ассоциативности и дистрибутивности наследуются из кольца $GF(p)[x]$.

Таким образом, множество F является коммутативным кольцом порядка $q = p^m$ с единицей. Оно называется кольцом многочленов над $GF(p)$ по модулю $\varphi(x)$ и обозначается $F = GF(p)[x]/\varphi(x)$.

Пусть $\varphi(x)$ — нормированный *неприводимый* многочлен степени m. Тогда кольцо $GF(p)[x]/\varphi(x)$ содержит элементы 0 и 1 и является *полем* порядка $q = p^m$. Достаточно показать, что все ненулевые элементы кольца образуют мультипликативную группу относительно операции умножения $\odot$. Действительно, в этом случае множество $F^* = GF(p)[x]/\varphi(x) \backslash \{0\}$ состоит из ненулевых многочленов степени не выше $m - 1$, взаимно простых с $\varphi(x)$. Для любого многочлена $f \in F^*$ множество многочленов $f \odot F^* = \{f \odot g,\, g \in F^*\}$ совпадает с F^*. Следовательно, найдется многочлен f' такой, что $f \odot f' = 1$. Другими словами, каждый элемент $f \in F^*$ имеет обратный, так что F^* является мультипликативной группой порядка $q - 1 = p^m - 1$ относительно операции умножения $\odot$.

Поле $GF(p)[x]/\varphi(x)$ называется расширением поля $GF(p)$ степени m и обозначается $GF(q)$.

1.7. Мультипликативная структура конечного поля

Теорема 2. *Каждый элемент поля $a \in GF(q)$ удовлетворяет соотношению $a^q - a = 0$, т.е. является корнем уравнения $x^q - x = 0$.*

Доказательство. Если $a = 0$, то утверждение очевидно.

Пусть a – произвольный ненулевой элемент поля $GF(q)$. Обозначим через $b_1, b_2, \ldots, b_{q-1}$ все ненулевые элементы поля $GF(q)$. Рассмотрим $q-1$ элементов $a \odot b_1, a \odot b_2, \ldots, a \odot b_{q-1}$. Все эти элементы лежат в поле $GF(q)$ и различны, так как если бы для некоторых $i \neq j$ было бы $a \odot b_i = a \odot b_j$, то отсюда следовало бы невозможное равенство $b_i = b_j$. Следовательно, верны равенства

$$\begin{aligned} (a \odot b_1) \odot (a \odot b_2) \odot \cdots \odot (a \odot b_{q-1}) &= b_1 \odot b_2 \odot \cdots \odot b_{q-1}. \\ a^{q-1} \odot (b_1 \odot b_2 \odot \cdots \odot b_{q-1}) &= b_1 \odot b_2 \odot \cdots \odot b_{q-1}. \\ a^{q-1} &= 1. \\ a^q &= a. \end{aligned} \tag{1.4}$$

□

Пусть a – произвольный ненулевой элемент поля $GF(q)$. Вычислим последовательные степени $a, a^2, \ldots, a^n, \ldots$ Так как любые степени a являются элементами поля, то в этом ряду не может быть больше $q-1$ различных ненулевых элементов $GF(q)$. Следовательно, найдется такая пара чисел i и j, что $a^i = a^{i+j}$ или $a^j = 1$. Множество из различных последовательных степеней a^i элемента $a \in GF(q)$ для $i = 1, \ldots, n$ такое, что все $a^i \neq 1$, кроме $a^n = 1$, называется *мультипликативной циклической подгруппой* порядка n поля $GF(q)$. Элемент a называется образующим порядка n или просто элементом порядка n, если n — наименьшее число, при котором $a^n = 1,\ n > 0$.

Теорема 3. *Если элемент поля $a \in GF(q)$ имеет порядок n, то n является делителем $q-1$.*

Доказательство. По определению, порядок n является *наименьшим* целым числом, для которого $a^n = 1$. Пусть n не является делителем $q-1$. Тогда $q - 1 = kn + r$, где $1 \leq r < n$. По теореме 2 имеем $a^{q-1} = a^{kn+r} = a^{kn} \odot a^r = 1$, т. е. $a^r = 1$. Это противоречит условию, что n наименьшее из таких чисел. □

Элементы порядка n являются корнями уравнения $x^n - 1 = 0$.

Элемент порядка $q-1$ называется *примитивным элементом* поля $GF(q)$.

Примем без доказательства следующее утверждение.

Теорема 4. *Поле $GF(q)$ содержит примитивные элементы.*

Если известен один примитивный элемент поля α, то другие примитивные элементы имеют вид $\beta = \alpha^n$ для n взаимно простых с $q-1$.

Степени α^i, $i = 1, \ldots, q-1$, примитивного элемента образуют все ненулевые элементы поля $GF(q)$.

Число примитивных элементов поля $GF(q)$, то есть число взаимно простых с $q-1$ показателей степени, дает функция Эйлера:

$$\phi(q-1) = \prod_{i=1}^{k} p_i^{l_i - 1}(p_i - 1),$$

где $q - 1 = \prod_{i=1}^{k} p_i^{l_i}$.

Для практической реализации поля и алгебраических методов кодирования необходимо найти хотя бы один примитивный элемент. Эту задачу помогает решить следующая

Теорема 5.

$$\alpha^{\frac{(q-1)}{p_i}} \neq 1,\ i = 1, \ldots, k.$$

Элементы $\alpha_1, \alpha_2, \ldots, \alpha_s$ поля $GF(q)$ называются *линейно независимыми* над полем $GF(p)$, если равенство

$$u_1\alpha_1 + u_2\alpha_2 + \cdots + u_s\alpha_s = 0,\ u_i \in GF(p),\ i = 1, 2, \ldots, s,$$

возможно лишь при $u_1 = u_2 = \cdots = u_s = 0$.

При полиномиальном представлении поля $GF(q) = GF(p^m)$ каждый элемент поля представляет собой многочлен над $GF(p)$ степени не выше $m-1$: $f(x) = f_{m-1}x^{m-1} + f_{m-2}x^{m-2} + \cdots + f_1x + f_0$. Это эквивалентно представлению каждого элемента вектором коэффициентов длины m:

$$f(x) \mapsto \begin{pmatrix} f_0 & f_1 & \ldots & f_{m-2} & f_{m-1} \end{pmatrix}. \tag{1.5}$$

Все различные векторы образуют *линейное пространство* размерности m. Таким образом, поле $GF(p^m)$ можно рассматривать как линейное пространство размерности m над полем $GF(p)$. Такое пространство можно задать с помощью базиса из m линейно независимых векторов или, что эквивалентно, с помощью m линейно независимых над $GF(p)$ элементов поля $GF(q)$. В частности, из определения примитивного элемента поля α следует, что элементы $1, \alpha, \ldots, \alpha^{m-1}$ образуют степенной базис поля.

1.8. След и нормальный базис

Следом элемента $a \in GF(p^m)$ из поля $GF(p^m)$ в подполе $GF(p)$ называют сумму $Tr(a) = a + a^p + a^{p^2} + \cdots + a^{p^{m-1}}$. Основные свойства функции след:

1. $Tr(a) \in GF(p)$;

2. $Tr(a+b) = Tr(a) + Tr(b)$;

3. $(Tr(a))^p = Tr(a^p) = Tr(a)$;

4. $Tr(1) = m \mod p$;

5. $Tr(0) = 0$.

Функция след имеет много применений, из которых наиболее важными являются: решение степенных уравнений, построение поля Галуа, построение последовательностей над $GF(p)$ с хорошими корреляционными свойствами.

Базис векторного пространства задается не единственным способом. Чаще всего задают степенные и нормальные базисы.

Нормальным базисом называют базис вида $\gamma, \gamma^p, \gamma^{p^2}, \ldots, \gamma^{p^{m-1}}$, где $\gamma \in GF(p^m)$. Важное свойство нормального базиса состоит в том, что $Tr(\gamma) \neq 0$. В любом поле $GF(p^m)$ существует нормальный базис.

1.9. Некоммутативное кольцо линеаризованных многочленов $R_N[z]$

Рассмотрим расширенное поле $GF(q^N)$, где $q = p^m$ — степень простого числа. Введем обозначение $[i] = q^i$, если $i \geq 0$, и $[i] = q^{N+i}$, если $i < 0$.

Многочлен

$$F(z) = \sum_{i=0}^{n} F_i z^{q^i} = \sum_{i=0}^{n} F_i z^{[i]}, \tag{1.6}$$

где $F_i \in GF(q^N,\ i = 0, 1, \ldots, n)$, называется *линеаризованным* над полем $GF(q^N)$.

Этот термин объясняется следующим свойством таких многочленов. Для любых двух элементов α и β из любого расширения поля $GF(q^N)$ и любых двух коэффициентов a и b из поля $GF(q)$ верно соотношение

$$F(a\alpha + b\beta) = aF(\alpha) + bF(\beta).$$

Многочлены $F(z)$ называют также *q-многочленами.*

Множество всех *q-многочленов* над полем $GF(q^N)$ обозначим $R_N[z]$. Превратим это множество в кольцо, введя операции сложения и умножения.

1. Операция сложения $+$ определяется как для обычных многочленов: если

$$F(z) = \sum_{i=0} F_i z^{[i]},\ G(z) = \sum_{i=0} G_i z^{[i]},$$

то

$$C(z) = F(z) + G(z) = \sum_{i=0} (F_i + G_i) z^{[i]}. \tag{1.7}$$

Таким образом, сумма линеаризованных многочленов также является линеаризованным многочленом.

2. Операция символического умножения, которую обозначим $*$, отличается от умножения обычных многочленов: если

$$F(z) = \sum_{i} F_i z^{[i]},\ G(z) = \sum_{k} G_k z^{[k]},$$

то

$$\begin{aligned} C(z) = F(z) * G(z) = F(G(z)) = \\ = \textstyle\sum_i F_i (G(z))^{[i]} = \sum_i (\sum_{s+k=i} F_s G_k^{[s]}) z^{[i]}. \end{aligned} \tag{1.8}$$

Таким образом, произведение линеаризованных многочленов также является линеаризованным многочленом, причем коэффициенты произведения определяются формулой

$$C_i = \sum_{s+k=i} F_s G_k^{[s]}.$$

В отличие от обычного умножения символическое умножение является некоммутативной операцией: в общем случае

$$F(z) * G(z) \neq G(z) * F(z).$$

Однако символическое умножение ассоциативно:

$$F(z) * (G(z) * H(z)) = (F(z) * G(z)) * H(z).$$

Законы дистрибутивности для введенных операций также выполняются:

$$(F(z) + G(z)) * H(z)) = F(z) * H(z) + G(z) * H(z),$$

$$H(z) * (F(z) + G(z)) = H(z) * F(z) + H(z) * G(z).$$

Следовательно, множество линеаризованных многочленов $R_N[z]$ с операциями сложения и умножения, является *некоммутативным кольцом*.

Кольцо $R_N[z]$ имеет единицу, роль которой играет линеаризованный многочлен $e(z) = z$. Действительно, для любого многочлена $F(z) \in R_N[z]$ верно соотношение $z * F(z) = F(z) * z = F(z)$.

Нормой, или *q-степенью*, многочлена $F(z) = \sum_i F_i z^{[i]}$, обозначаемой $\mathrm{qdeg}(F)$, называется наибольший номер i, для которого $F_i \neq 0$. Соответствующий коэффициент называется старшим. Если $F(z) \neq 0$ и $G(z) \neq 0$, то $\mathrm{qdeg}(F * G) = \mathrm{qdeg}(F) + \mathrm{qdeg}(G)$.

Левый и правый алгоритмы Евклида. В кольце $R_N[z]$ существует алгоритм Евклида левого и правого делений. Сначала опишем алгоритм *левого* деления. Пусть $F_1(z) = \sum_{i=0}^{n} F_{1i} z^{[i]}$ – произвольный многочлен с нормой $\mathrm{qdeg}(F_1) = n$ и пусть $F_0(z) = \sum_{k=0}^{m} F_{0k} z^{[k]}$ – произвольный многочлен с нормой $\mathrm{qdeg}(F_0) = m > n$. Вычтем из многочлена $F_0(z)$ многочлен $F_{0m} F_{1n}^{[m-n]} z^{[m-n]} * F_1(z)$. Тогда норма полученной разности будет строго меньше m. Если она остается большей или равной n, то старший коэффициент разности можно обратить в нуль, вычитая подходящее левое кратное многочлена $F_1(z)$. Продолжая последовательно эту процедуру, в конце концов получим частное $Q_1(z)$ и остаток $F_2(z)$:

$$F_0(z) = Q_1(z) * F_1(z) + F_2(z).$$

Здесь $F_2(z)$ – либо нулевой многочлен, либо многочлен с нормой, строго меньшей n, т.е. $\mathrm{qdeg}(F_2) < \mathrm{qdeg}(F_1)$.

Алгоритм *правого* деления получим, если вычитать правые кратные многочлена $F_1(z)$: $F_0(z) = F_1(z) * Q(z) + f_2(z)$, где либо $f_2(z) = 0$, либо $\mathrm{qdeg}(f_2) < \mathrm{qdeg}(F_1)$.

Рассмотрим более подробно левый алгоритм деления. Запишем цепочку равенств:

$$
\begin{array}{l}
F_0(z) = Q_1(z) * F_1(z) + F_2(z),\ \mathrm{qdeg}(F_2) < \mathrm{qdeg}(F_1);\\
F_1(z) = Q_2(z) * F_2(z) + F_3(z),\ \mathrm{qdeg}(F_3) < \mathrm{qdeg}(F_2);\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
F_{s-1}(z) = Q_s(z) * F_s(z) + F_{s+1}(z),\ \mathrm{qdeg}(F_{s+1}) < \mathrm{qdeg}(F_s);\\
F_s(z) = Q_{s+1}(z) * F_{s+1}(z).
\end{array}
\tag{1.9}
$$

В этой цепочке последний ненулевой остаток $F_{s+1}(z)$ представляет собой правый символический наибольший общий делитель (НОД) многочленов $F_0(z)$ и $F_1(z)$. Если НОД равен cz, то многочлены $F_0(z)$ и $F_1(z)$ называются взаимно простыми.

Пусть

$$
X = \begin{bmatrix} X_1 & X_2 \\ X_3 & X_4 \end{bmatrix}, \qquad Y = \begin{bmatrix} Y_1 & Y_2 \\ Y_3 & Y_4 \end{bmatrix}
$$

– матрицы 2-го порядка с элементами из кольца $R_N(z)$. Произведение матриц определим формулой

$$
X{*}Y = \begin{bmatrix} X_1 & X_2 \\ X_3 & X_4 \end{bmatrix} * \begin{bmatrix} Y_1 & Y_2 \\ Y_3 & Y_4 \end{bmatrix} = \begin{bmatrix} X_1 * Y_1 + X_2 * Y_3 & X_1 * Y_2 + X_2 * Y_4 \\ X_3 * Y_4 + X_4 * Y_3 & X_3 * Y_2 + X_4 * Y_4 \end{bmatrix}.
$$

Порядок сомножителей в элементах последней матрицы существен.

Введем *q-многочлены* $U_i(z)$, $A_i(z)$, $V_i(z)$, $B_i(z)$, определяемые для $i \geq 1$ рекуррентно:

$$
\begin{array}{ll}
U_i(z) = -U_{i-1}(z) * Q_i(z) + U_{i-2}(z), & U_0(z) = z,\ U_{-1}(z) = 0,\\
V_i(z) = -V_{i-1}(z) * Q_i(z) + V_{i-2}(z), & V_0(z) = 0,\ V_{-1}(z) = -z,\\
A_i(z) = -Q_i(z) * A_{i-1}(z) + A_{i-2}(z), & A_0(z) = z,\ A_{-1}(z) = 0,\\
B_i(z) = -Q_i(z) * B_{i-1}(z) + B_{i-2}(z), & B_0(z) = 0,\ B_{-1}(z) = z.
\end{array}
\tag{1.10}
$$

Теорема 6. *Многочлены $U_i(z)$ и $V_i(z)$ позволяют выразить исходные многочлены $F_0(z)$ и $F_1(z)$ через промежуточные остатки $F_i(z)$ и $F_{i+1}(z)$:*

$$
\begin{array}{rcl}
F_0(z) & = & (-1)^i \left\{ U_i(z) * F_i(z) - U_{i-1}(z) * F_{i+1}(z) \right\};\\
F_1(z) & = & (-1)^i \left\{ -V_i(z) * F_i(z) + V_{i-1}(z) * F_{i+1}(z) \right\}.
\end{array}
\tag{1.11}
$$

Доказательство. Из алгоритма Евклида (1.9) можно записать цепочку равенств:

$$
\begin{array}{rl}
\begin{bmatrix} F_0 \\ F_1 \end{bmatrix} & = \begin{bmatrix} Q_1 & z \\ z & 0 \end{bmatrix} * \begin{bmatrix} F_1 \\ F_2 \end{bmatrix} = \begin{bmatrix} Q_1 & z \\ z & 0 \end{bmatrix} * \begin{bmatrix} Q_2 & z \\ z & 0 \end{bmatrix} * \begin{bmatrix} F_2 \\ F_3 \end{bmatrix} = \ldots =\\
& = \begin{bmatrix} Q_1 & z \\ z & 0 \end{bmatrix} * \begin{bmatrix} Q_2 & z \\ z & 0 \end{bmatrix} * \cdots * \begin{bmatrix} Q_i & z \\ z & 0 \end{bmatrix} * \begin{bmatrix} F_i \\ F_{i+1} \end{bmatrix}.
\end{array}
\tag{1.12}
$$

С другой стороны, из первой пары соотношений (1.10) имеем цепочку равенств:

$$\begin{aligned}
&\begin{bmatrix} U_i & -U_{i-1} \\ V_i & -V_{i-1} \end{bmatrix} = \begin{bmatrix} U_{i-1} & -U_{i-2} \\ V_{i-1} & -V_{i-2} \end{bmatrix} * \begin{bmatrix} -Q_i & -z \\ -z & 0 \end{bmatrix} = \\
&= \begin{bmatrix} U_{i-2} & -U_{i-3} \\ V_{i-2} & -V_{i-3} \end{bmatrix} * \begin{bmatrix} -Q_{i-1} & -z \\ -z & 0 \end{bmatrix} * \begin{bmatrix} -Q_i & -z \\ -z & 0 \end{bmatrix} = \\
&= \ldots = \\
&= \begin{bmatrix} U_0 & -U_{-1} \\ V_0 & -V_{-1} \end{bmatrix} * \begin{bmatrix} -Q_1 & -z \\ -z & 0 \end{bmatrix} * \begin{bmatrix} -Q_2 & -z \\ -z & 0 \end{bmatrix} * \ldots * \begin{bmatrix} -Q_i & -z \\ -z & 0 \end{bmatrix} = \\
&= (-1)^i \begin{bmatrix} z & 0 \\ 0 & -z \end{bmatrix} * \begin{bmatrix} Q_1 & z \\ z & 0 \end{bmatrix} * \begin{bmatrix} Q_2 & z \\ z & 0 \end{bmatrix} * \ldots * \begin{bmatrix} Q_i & z \\ z & 0 \end{bmatrix}.
\end{aligned} \tag{1.13}$$

Подставляя (1.13) в (1.12), получим утверждение (1.11) теоремы 6. □

В свою очередь, любой остаток $F_i(z)$ может быть выражен через многочлены $F_0(z)$ и $F_1(z)$ с помощью многочленов $A_{i-1}(z)$ и $B_{i-1}(z)$.

Теорема 7. *Имеем*

$$F_i(z) = B_{i-1}(z) * F_0(z) - A_{i-1}(z) * F_1(z). \tag{1.14}$$

Доказательство. Заметим, что матрица $\left[\begin{smallmatrix} Q(z) & z \\ z & 0 \end{smallmatrix}\right]$ имеет обратную $\left[\begin{smallmatrix} 0 & z \\ z & -Q(z) \end{smallmatrix}\right]$. Следовательно, соотношение (1.12) эквивалентно соотношению

$$\begin{bmatrix} F_i \\ F_{i+1} \end{bmatrix} = \begin{bmatrix} 0 & z \\ z & -Q_i \end{bmatrix} * \begin{bmatrix} 0 & z \\ z & -Q_{i-1} \end{bmatrix} * \cdots * \begin{bmatrix} 0 & z \\ z & -Q_1 \end{bmatrix} * \begin{bmatrix} F_0 \\ F_1 \end{bmatrix}. \tag{1.15}$$

С другой стороны, из второй пары соотношений (1.10) находим:

$$\begin{aligned}
&\begin{bmatrix} B_{i-1} & A_{i-1} \\ B_i & A_i \end{bmatrix} = \begin{bmatrix} 0 & z \\ z & -Q_i \end{bmatrix} * \begin{bmatrix} B_{i-2} & A_{i-2} \\ B_{i-1} & A_{i-1} \end{bmatrix} = \\
&= \cdots = \\
&= \begin{bmatrix} 0 & z \\ z & -Q_i \end{bmatrix} * \begin{bmatrix} 0 & z \\ z & -Q_{i-1} \end{bmatrix} * \cdots * \begin{bmatrix} 0 & z \\ z & -Q_1 \end{bmatrix}.
\end{aligned} \tag{1.16}$$

Подставляя (1.16) в (1.15), получим утверждение теоремы (1.14). □

Наряду с введенным выше кольцом, рассмотрим его фактор-кольцо R_N по модулю многочлена $z^{[N]} - z$, состоящее из правых классов вычетов по этому модулю. Элементы этого кольца можно отождествлять

также с линеаризованными многочленами q-степени не выше $N-1$. Пусть $F(z) = \sum_{i=0}^{N-1} f_i z^{[i]} \in R_N$. Тогда

$$F^{[1]}(z) = f_{N-1}^{[1]} z^{[0]} + f_0^{[1]} z^{[1]} + \ldots + f_{N-2}^{[1]} z^{[N-1]}.$$

Таким образом, возведение в степень q многочлена в кольце R_N эквивалентно возведению в степень q всех его коэффициентов с последующим циклическим сдвигом. Эту операцию будем называть q-циклическим сдвигом. Идеалы в кольце R_N являются главными и порождаются многочленами $G(z)$, которые удовлетворяют соотношению $z^{[N]} - z = H(z) * G(z)$, т.е. являются правыми делителями многочлена $z^{[N]} - z$ (заметим, впрочем, что если старший коэффициент многочлена $G(z)$ равен единице, то многочлены $G(z)$ и $H(z)$ коммутируют). Идеал G инвариантен относительно q-циклического сдвига, т.е. если $g \in G$, то и $g^{[i]} \in G$.

1.10. Линейное пространство

Пусть задано поле $GF(q)$. Его элементы рассматриваются как буквы алфавита из q элементов. Чаще всего используются поля характеристики 2: $GF(2)$ из двух элементов $\{0,1\}$ и $GF(2^m)$ из 2^m элементов. Введем множество векторов длины n с координатами из поля $GF(q)$:

$$X^n = \{\underline{\mathbf{x}} = [x_1, x_2, \ldots, x_n] : x_i \in GF(q)\}.$$

Число различных векторов равно q^n.

Определим на X^n операции *сложения* и *умножения на скаляр*.

Сложение

$$\begin{array}{rcllll} \underline{\mathbf{a}} & = & [a_1 & a_2 & \ldots & a_n] \\ \underline{\mathbf{b}} & = & [b_1 & b_2 & \ldots & b_n] \\ \underline{\mathbf{a}} + \underline{\mathbf{b}} & = & [a_1 + b_1 & a_2 + b_2 & \ldots & a_n + b_n] \end{array}$$

Скаляры это элементы поля $GF(q)$.

Умножение на скаляр. Если $g \in GF(q)$, и $\underline{\mathbf{a}} \in X^n$, то

$$g \cdot \underline{\mathbf{a}} = [ga_1, ga_2, \ldots, ga_n].$$

Множество X^n с введенными операциями является линейным пространством. В нем можно определить *базис*. Например, множество X^n

содержит n векторов:

$$\begin{aligned}
\underline{\mathbf{e}}_1 &= \begin{bmatrix}1 & 0 & \dots & 0 & 0\end{bmatrix},\\
\underline{\mathbf{e}}_2 &= \begin{bmatrix}0 & 1 & \dots & 0 & 0\end{bmatrix},\\
\dots &\quad \dots\\
\underline{\mathbf{e}}_{n-1} &= \begin{bmatrix}0 & 0 & \dots & 1 & 0\end{bmatrix},\\
\underline{\mathbf{e}}_n &= \begin{bmatrix}0 & 0 & \dots & 0 & 1\end{bmatrix}.
\end{aligned}$$

Эти векторы *линейно независимы*. Кроме того, любой вектор $\underline{\mathbf{a}} \in X^n$ можно представить как линейную комбинацию этих векторов:

$$\underline{\mathbf{a}} = [a_1, a_2, \dots, a_n] = a_1\underline{\mathbf{e}}_1 + a_2\underline{\mathbf{e}}_2 + \dots + a_n\underline{\mathbf{e}}_n.$$

Векторы $\{\underline{\mathbf{e}}_1, \underline{\mathbf{e}}_2, \dots, \underline{\mathbf{e}}_n\}$ называются *базисом* линейного пространства, а число n – *размерностью* пространства X^n. Любые $n+1$ векторов пространства X^n линейно зависимы.

Базис линейного пространства можно выбрать многими способами. Любой набор $\{\underline{\mathbf{b}}_i \in X^n,\ i = 1, 2, \dots, n\}$ из n *линейно независимых* векторов пространства X^n является базисом.

Нормированное пространство. Определим на линейном пространстве X^n функцию $\mathcal{N}(\underline{\mathbf{a}})$, называемую *нормой*. Это численная функция, удовлетворяющая аксиомам нормы:

1. $\mathcal{N}(\underline{\mathbf{a}}) \geq 0 \quad \forall \underline{\mathbf{a}} \in X^n$.
2. $\mathcal{N}(\underline{\mathbf{a}}) = 0 \Leftrightarrow \underline{\mathbf{a}} = \underline{\mathbf{0}}$.
3. $\mathcal{N}(g\underline{\mathbf{a}}) = |g|\mathcal{N}(\underline{\mathbf{a}})$.
4. Аксиома треугольника: $\mathcal{N}(\underline{\mathbf{a}} + \underline{\mathbf{b}}) \leq \mathcal{N}(\underline{\mathbf{a}}) + \mathcal{N}(\underline{\mathbf{b}})$.

С помощью нормы определяется *расстояние* между двумя векторами $\underline{\mathbf{a}}$ и $\underline{\mathbf{b}}$ по формуле:

$$d(\underline{\mathbf{a}}, \underline{\mathbf{b}}) = \mathcal{N}(\underline{\mathbf{a}} - \underline{\mathbf{b}}).$$

Метрика Хэмминга. Пусть $\underline{\mathbf{a}} = [a_1, a_2, \dots, a_n] \in X^n$.

Нормой Хэмминга, или *весом Хэмминга*, вектора $\underline{\mathbf{a}}$ называется число $W_H(\underline{\mathbf{a}})$, равное числу *ненулевых* координат вектора.

Проверить, что норма Хэмминга действительно норма!

Расстояние Хэмминга между двумя векторами $\underline{\mathbf{a}}$ и $\underline{\mathbf{b}}$ равно весу их разности, то есть числу несовпадающих координат.

Обозначение: для a и b из поля $GF(q)$

$$|a - b| = \begin{cases} 0, & \text{если } a = b;\\ 1, & \text{если } a \neq b. \end{cases}$$

$$d(\underline{\mathbf{a}}, \underline{\mathbf{b}}) = W_H(\underline{\mathbf{a}} - \underline{\mathbf{b}}) = \sum_{i=1}^{n} |a_i - b_i|.$$

Метрика Хэмминга является покоординатной.

Общие характеристики пространства. Обозначим через w_i число векторов в пространстве X^n, вес которых равен i. Набор чисел $\{w_0, w_1, \ldots, w_n\}$ называется весовым спектром пространства.

Для метрики Хэмминга вектор имеет вес i, если он содержит i ненулевых координат и $n-i$ нулевых координат. Число w_i таких векторов равно

$$w_i = \begin{cases} C_n^i (q-1)^i, & \text{если } q \geq 3; \\ C_n^i, & \text{если } q = 2. \end{cases} \quad i = 0, 1, \ldots, n.$$

$$\sum_{i=0}^{n} w_i = \sum_{i=0}^{n} C_n^i (q-1)^i = q^n. \quad \text{Для } GF(2), \ \sum_{i=0}^{n} w_i = \sum_{i=0}^{n} C_n^i = 2^n.$$

Средний вес вектора, по определению,

$$\overline{w} = \frac{\sum\limits_{i=0}^{n} i \cdot w_i}{\sum\limits_{i=0}^{n} w_i} = n\Big(1 - \frac{1}{q}\Big). \quad \text{Для } GF(2), \ \overline{w} = \frac{n}{2}.$$

Сфера радиуса t с центром в точке $\underline{\mathbf{a}}$ (определение):

$$S_t(\underline{\mathbf{a}}) = \{\underline{\mathbf{b}} : W_H(\underline{\mathbf{b}} - \underline{\mathbf{a}}) = t\}.$$

Мощность сферы (число элементов)

$$|S_t(\underline{\mathbf{a}})| = C_n^t (q-1)^t. \quad \text{Для поля } GF(2) \quad |S_t(\underline{\mathbf{a}})| = C_n^t.$$

Мощность сферы не зависит от центра сферы $\underline{\mathbf{a}}$.

Шар радиуса t с центром в точке $\underline{\mathbf{a}}$ (определение):

$$B_t(\underline{\mathbf{a}}) = \{\underline{\mathbf{b}} : W_H(\underline{\mathbf{b}} - \underline{\mathbf{a}}) \leq t\}.$$

Мощность шара (число элементов)

$$|B_t(\underline{\mathbf{a}})| = \sum_{i=0}^{t} C_n^i (q-1)^i. \quad \text{Для поля } GF(2) \quad |B_t(\underline{\mathbf{a}})| = \sum_{i=0}^{t} C_n^i.$$

Мощность шара не зависит от выбора центра $\underline{\mathbf{a}}$.

Г л а в а 2
Блоковые коды

На рис. 2.1 приведена схема передачи дискретных сообщений.

Рис. 2.1. Дискретный канал

Источник сообщений передает последовательность символов $(U_1, U_2, \dots)$. *Кодер для канала* преобразует эту последовательность в последовательность $(X_1, X_2, \dots)$ и передает ее по *Дискретному каналу*. Выходная последовательность $(Y_1, Y_2, \dots)$ поступает в блок обработки *Декодер канала*, где она преобразуется в последовательность для *Получателя* $(\widetilde{U}_1, \widetilde{U}_2, \dots)$.

Будем считать, что алфавиты всех этих последовательностей одинаковы. В теоретических исследованиях в качестве алфавита чаще всего используется конечное поле $GF(q)$ из q элементов.

Для кодирования могут использоваться различные стратегии. Их можно разбить на два класса — блоковое и неблоковое кодирование. В этом пособии рассматривается только блоковое кодирование.

Блоковое кодирование состоит в том, что последовательность символов источника сообщений $(U_1, U_2, \dots)$ разбивается на блоки, например по k символов в каждом: $\mathbf{U}_1 = (U_1, U_2, \dots, U_k)$, $\mathbf{U}_2 = (U_{k+1}, U_{k+2}, \dots, U_{2k}), \dots$ Эти символы называются информационными. Кодер преобразует каждый входной k-блок информационных символов $\mathbf{U}_i$ в кодовый n-блок

$$\mathbf{X}_i = \mathbf{X}(\mathbf{U}_i) = (X_1(\mathbf{U}_i), X_2(\mathbf{U}_i), \dots, X_n(\mathbf{U}_i)).$$

Кодовые символы передаются по каналу. Канал преобразует кодовый блок в выходной блок $\mathbf{Y} = (Y_1, Y_2, \dots, Y_n)$. Декодер восстанавливает информационные символы источника сообщений (возможно, с ошибками). Восстановленный k-блок $\widetilde{\mathbf{U}} = (\widetilde{U}_1, \widetilde{U}_2, \dots, \widetilde{U}_k)$ передается по-

лучателю. Блоковое кодирование — это отображение информационных k-блоков в кодовые n-блоки.

2.1. Задача кодирования

Пусть задано n-мерное векторное пространство X^n, на котором задана метрика, то есть функция расстояния $d(\underline{\mathbf{a}}, \underline{\mathbf{b}})$ между двумя векторами. Для метрики Хэмминга функция расстояния равна весу Хэмминга разности векторов: $d(\underline{\mathbf{a}}, \underline{\mathbf{b}}) = W_H(\underline{\mathbf{a}} - \underline{\mathbf{b}})$.

Кодом $\mathcal{C}$ называется произвольное подмножество $\mathcal{C} \subseteq X^n$ векторов линейного пространства.

Код $\mathcal{C}$ называется $[n, M, d]$-кодом, если

1. Длина кодовых векторов равна n.

2. Мощность кода (число кодовых слов) равна $|\mathcal{C}| = M$.

3. Кодовое расстояние $d(\mathcal{C})$ равно d, где

$$d(\mathcal{C}) = d = \min\left\{W_H(\underline{\mathbf{a}} - \underline{\mathbf{b}}) : \underline{\mathbf{a}} \neq \underline{\mathbf{b}} \in \mathcal{C}\right\}.$$

Задача кодирования 1: *при заданном расстоянии d выбрать код с максимальной мощностью M.*

Задача кодирования 2: *при заданной мощности M выбрать код с максимальным расстоянием d.*

Большое расстояние нужно, чтобы исправлять ошибки при передаче.

Пусть код $\mathcal{C}$ с расстоянием $d = 2t + 1$ состоит из векторов

$$\underline{\boldsymbol{a}}_{\mathbf{1}} \quad \underline{\boldsymbol{a}}_{\mathbf{2}} \quad \dots \quad \underline{\boldsymbol{a}}_{\boldsymbol{M}}.$$

Пусть по каналу передается кодовый вектор $\underline{\boldsymbol{a}}_1$, а на приемном конце принят вектор

$$\underline{\boldsymbol{y}} = \underline{\boldsymbol{a}}_1 + \underline{\boldsymbol{e}},$$

где вектор ошибки $\underline{\boldsymbol{e}}$ имеет вес $W_H(\underline{\boldsymbol{e}}) = t$. Он исказит t позиций в принятом векторе. Заранее неизвестно, какие и сколько позиций будет искажено.

Как узнать, какой вектор передавался? Другими словами, как декодировать принятое сообщение?

Одним из теоретических методов является *декодирование по минимальному расстоянию.* Суть этого метода состоит в следующем.

Этап 1. На приемном конце считаются известными кодовые векторы $\underline{\boldsymbol{a}}_{\mathbf{1}}, \underline{\boldsymbol{a}}_{\mathbf{2}}, \ldots, \underline{\boldsymbol{a}}_{\boldsymbol{M}}$. Получив вектор $\underline{\boldsymbol{y}}$, приемник (декодер) вычисляет разности и их веса (расстояния до принятого вектора):

$$\underline{\boldsymbol{y}} - \underline{\boldsymbol{a}}_{\mathbf{1}} \qquad \underline{\boldsymbol{y}} - \underline{\boldsymbol{a}}_{\mathbf{2}} \qquad \ldots \qquad \underline{\boldsymbol{y}} - \underline{\boldsymbol{a}}_{\boldsymbol{M}},$$

$$W_H(\underline{\boldsymbol{y}} - \underline{\boldsymbol{a}}_{\mathbf{1}}) \quad W_H(\underline{\boldsymbol{y}} - \underline{\boldsymbol{a}}_{\mathbf{2}}) \quad \ldots \quad W_H(\underline{\boldsymbol{y}} - \underline{\boldsymbol{a}}_{\boldsymbol{M}}).$$

Этап 2. Декодер находит минимальное расстояние и выносит решение, что передавался соответствующий ему вектор.

Доказательство

1. В нашем примере расстояние до передававшегося вектора $\underline{\boldsymbol{a}}_{\mathbf{1}}$ равно

$$d_1 = W_H(\underline{\boldsymbol{y}} - \underline{\boldsymbol{a}}_{\mathbf{1}}) = W_H(\underline{\boldsymbol{e}}) = t.$$

2. Расстояние до любого другого кодового вектора $\underline{\boldsymbol{a}}_{\boldsymbol{i}}$ равно

$$d_i = W_H(\underline{\boldsymbol{y}} - \underline{\boldsymbol{a}}_{\boldsymbol{i}}) =$$

$$= W_H(\underline{\boldsymbol{a}}_1 - \underline{\boldsymbol{a}}_{\boldsymbol{i}} + \underline{\boldsymbol{e}}) \geq |W_H(\underline{\boldsymbol{a}}_1 - \underline{\boldsymbol{a}}_{\boldsymbol{i}}) - W_H(\underline{\boldsymbol{e}})| \geq$$

$$\geq 2t + 1 - t = t + 1.$$

3. Так как наименьшим среди полученных расстояний является только расстояние $d_1 = t$: $(d_1 = t < t+1 \leq d_i,\ i = 2, \ldots, M)$, то выносится (правильное) решение: передавался вектор $\underline{\boldsymbol{a}}_1$. Исправлено t ошибок.

□

2.2. Корректирующая способность кода. Скорость передачи

Код с расстоянием $d = 2t + 1$ позволяет исправлять любые ошибки кратности t или меньше.

Код с расстоянием $d = 2t + 2$ позволяет исправлять любые ошибки кратности t или меньше и *обнаруживать* ошибки кратности $t + 1$. В этом случае если вектор ошибки $\underline{\boldsymbol{e}}$ имеет вес $W_H(\underline{\boldsymbol{e}}) = t + 1$, то при декодировании по минимальному расстоянию на этапе 1 будет найдено несколько *одинаковых минимальных* расстояний, причем минимальное расстояние будет $t + 1$ или больше. Однозначное решение на этапе

2 станет невозможным. Решение в этом случае формулируется так: обнаружена ошибка кратности $t+1$ или больше.

Скорость передачи кода, по определению, равна

$$R = \frac{\log_q M}{n}.$$

2.2.1. Граница Синглтона

Обозначим через $M(n,d)$ максимальную мощность кода при заданных n и d. Легко проверить, что $M(d,d) = q$.

Верно рекуррентное соотношение для максимальных мощностей

$$M(n,d) \le q \cdot M(n-1,d).$$

Так как $M(d,d) = q$, то, применяя рекурсию $n-d$ раз, получим

$$M(n,d) \le q^{n-d} M(d,d) = q^{n-d+1}.$$

Доказательство рекуррентного соотношения. Разобьем код мощности $M(n,d)$ на q подкодов так, что в первом подкоде на первой позиции всех векторов стоит символ поля 0, во втором — символ поля 1 и т.д. Хотя бы один из этих подкодов имеет мощность, не меньшую $\frac{M(n,d)}{q}$. Взяв этот подкод и удалив первую координату, получим код длины $n-1$ с расстоянием d и мощностью

$$\frac{M(n,d)}{q} \le m(n-1,d).$$

Так как $m(n-1,d) \le M(n-1,d)$, то получим рекуррентное соотношение

$$M(n,d) \le qM(n-1,d)$$

2.2.2. Граница Плоткина для больших расстояний

Если $d > n(1-\frac{1}{q}) = \overline{w}$, то

$$M(n,d) \le \frac{d}{d-\overline{w}} = \frac{d}{d-n(1-\frac{1}{q})}.$$

В двоичном случае ($q=2$), если $d > \frac{n}{2} = \overline{w}$, то

$$M(n,d) \le \frac{d}{d-\overline{w}} = \frac{2d}{2d-n}.$$

Вывод границы Плоткина для случая q = 2. Пусть код C с расстоянием d состоит из векторов $\{\underline{\boldsymbol{a}}_{\mathbf{1}}\ \underline{\boldsymbol{a}}_{\mathbf{2}}\ \ldots\ \underline{\boldsymbol{a}}_{\boldsymbol{M}}\}$. Будем оценивать снизу и сверху сумму

$$T = \sum_{i=1}^{M}\sum_{j=1}^{M} W_H(\underline{\boldsymbol{a}}_{\boldsymbol{i}} - \underline{\boldsymbol{a}}_{\boldsymbol{j}}) = \sum_{i=1}^{M}\sum_{j=1}^{M}\sum_{s=1}^{n} |a_{is} - a_{js}|.$$

Оценка снизу. В сумме T содержится M слагаемых равных 0 (те, где $\underline{\boldsymbol{a}}_{\boldsymbol{i}} = \underline{\boldsymbol{a}}_{\boldsymbol{j}}$). Остальные $M^2 - M$ слагаемых имеют величину не меньше d. Отсюда

$$(M^2 - M)d \le T.$$

Оценка сверху. Обозначим через L_s число кодовых векторов, у которых s-я координата равна 1. Следовательно, у остальных $M - L_s$ векторов s-я координата равна 0.

Изменим порядок суммирования:

$$T = \sum_{i=1}^{M}\sum_{j=1}^{M}\sum_{s=1}^{n} |a_{is} - a_{js}| = \sum_{s=1}^{n}\sum_{i=1}^{M}\sum_{j=1}^{M} |a_{is} - a_{js}|.$$

При фиксированном s две внутренние суммы дают

$$\sum_{i=1}^{M}\sum_{j=1}^{M} |a_{is} - a_{js}|.$$

Разность $|a_{is} - a_{js}| = 1$, если либо s-я координата i-го кодового слова равна 1, а s-я координата j-го кодового слова равна 0, либо s-я координата i-го кодового слова равна 0, а s-я координата j-го кодового слова равна 1. Первый случай в указанных выше суммах встретится $L_s(M - L_s)$ раз, а второй — $(M - L_s)L_s$ раз. Таким образом: при фиксированном s две внутренние суммы дают

$$\sum_{i=1}^{M}\sum_{j=1}^{M} |a_{is} - a_{js}| = 2L_s(M - L_s),$$

то есть

$$T = \sum_{s=1}^{n} 2L_s(M - L_s).$$

Объединяя оценки снизу и сверху, получим

$$(M^2 - M)d \le T = \sum_{s=1}^{n} 2L_s(M - L_s). \tag{2.1}$$

Так как $L_s(M - L_s) \leq \frac{M^2}{4}$, то $T \leq \frac{nM^2}{2}$.
Объединим оценки:

$$(M^2 - M)d \leq \frac{nM^2}{2}.$$

Если $d > \frac{n}{2}$, то

$$M \leq \frac{2d}{2d - n}.$$

2.2.3. Верхняя граница Плоткина для двоичных кодов

Из рекуррентного соотношения для мощности оптимальных кодов имеем для двоичных кодов

$$M(n, d) \leq 2^s M(n - s, d).$$

Выберем $s = n - 2d + 1$. Тогда

$$M(n, d) \leq 2^{n-2d+1} M(2d - 1, d).$$

Используя верхнюю границу Плоткина для больших расстояний, получаем: $M(2d - 1, d) \leq 2d$. Следовательно:

$$M(n, d) \leq 2^{n-2d+2} d.$$

Асимптотически верхняя граница Плоткина для скорости передачи имеет вид

$$R = \frac{\log_2 M(n, d)}{n} = 1 - 2\frac{d - 1}{n} + \frac{\log_2 d}{n} = 1 - 2x + \frac{\log_2 d}{n}, \quad x = \frac{d - 1}{n}.$$

2.2.4. Граница Бассалыго–Элайеса для двоичных равновесных кодов

Код $\mathcal{C}$ называется равновесным, если все кодовые векторы имеют одинаковый вес Хэмминга. Обозначим этот вес через r. Расстояние между кодовыми векторами четное. Найдем верхнюю границу для мощности равновесного кода с расстоянием $d = 2\delta$. Обозначим через M число кодовых слов. Сначала получаем неравенства (2.1) как в границе Плоткина:

$$(M^2 - M)d \leq T = \sum_{s=1}^{n} 2L_s(M - L_s).$$

Для равновесных кодов с весом r имеем ограничение $\sum\limits_{s=1}^{n} L_s = Mr$. При этом ограничении имеем

$$\sum_{s=1}^{n} 2L_s(M - L_s) \le 2M^2 r - 2\frac{M^2 r^2}{n}.$$

Из полученных неравенств следует

$$M \le \frac{nd}{nd - 2rn + 2r^2}$$

при условии, что знаменатель в правой части положителен.

2.2.5. Верхняя граница Хэмминга

Пусть код C с расстоянием $d = 2t + 1$ состоит из векторов $\{\underline{\boldsymbol{a}}_{\mathbf{1}}\ \underline{\boldsymbol{a}}_{\mathbf{2}}\ \cdots\ \underline{\boldsymbol{a}}_{\boldsymbol{M}}\}$.

Поместим каждый кодовый вектор в центр шара $B_t(\underline{\boldsymbol{a}}_{\boldsymbol{i}})$ радиуса t. Шары попарно не пересекаются, поэтому

$$M|B_t(\underline{\boldsymbol{a}})| \le 2^n,$$

$$M \le \frac{2^n}{|B_t(\underline{\boldsymbol{a}})|} = \frac{2^n}{\sum\limits_{i=0}^{t} C_n^i}.$$

Скорость передачи асимптотически равна

$$R = \frac{\log_2 M}{n} \le 1 - h\Big(\frac{d-1}{2n}\Big), \quad h(x) = -x\log_2 x - (1-x)\log_2(1-x).$$

2.2.6. Нижняя граница Варшамова–Гилберта

Построим код длины n и с расстоянием d методом исчерпывания.

1. Выберем в качестве первого кодового вектора произвольный вектор $\underline{\boldsymbol{a}}_{\mathbf{1}} \in X^n$. Окружим его шаром $B_{d-1}(\underline{\boldsymbol{a}}_{\mathbf{1}})$ радиуса $d-1$. Удалим этот шар из X^n, получив множество

$$X_2^n = X^n \setminus B_{d-1}(\underline{\boldsymbol{a}}_{\mathbf{1}}).$$

2. Все векторы из X_2^n находятся на расстоянии d или больше от вектора $\underline{\boldsymbol{a}}_{\mathbf{1}} \in X^n$. Выберем в качестве второго кодового вектора любой вектор

$\underline{\boldsymbol{a}}_{\boldsymbol{2}} \in X_2^n$. Окружим его шаром $B_{d-1}(\underline{\boldsymbol{a}}_{\boldsymbol{2}})$ радиуса $d-1$. Удалим этот шар из X_2^n, получив множество

$$X_3^n = X_2^n \setminus B_{d-1}(\underline{\boldsymbol{a}}_{\boldsymbol{2}}).$$

3. Если множество X_3^n не пусто, то процедуру выбора очередного кодового вектора и выбрасывания шара можно продолжить.

Процедура останавливается, если множество

$$X_M^n = X_{M-1}^n \setminus B_{d-1}(\underline{\boldsymbol{a}}_{\boldsymbol{M-1}})$$

не пусто, а множество

$$X_{M+1}^n = X_M^n \setminus B_{d-1}(\underline{\boldsymbol{a}}_{\boldsymbol{M}})$$

пусто. Оценка мощности множеств:

$$\begin{aligned} |X_i^n| &= |X_{i-1}^n \setminus B_{d-1}(\underline{\boldsymbol{a}}_{\boldsymbol{i-1}})| \geq \\ &\geq |X_{i-1}^n| - |B_{d-1}(*)| \geq \\ &\geq \cdots \geq q^n - (i-1)|B_{d-1}(*)|. \end{aligned}$$

Условие остановки процедуры:

$$q^n - (M-1)|B_{d-1}(*)| \geq 1; \qquad q^n - M|B_{d-1}(*)| \leq 0.$$

$$\frac{q^n}{|B_{d-1}(*)|} \leq M \leq \frac{q^n - 1}{|B_{d-1}(*)|} + 1,$$

$$R \approx 1 - \tfrac{d}{n}\log_q(q-1) - h_q\left(\tfrac{d}{n}\right);\ h_q(x) = -x\log_q x - (1-x)\log_q(1-x).$$

2.3. Линейные коды

Линейным (n,k)*-кодом* называется любое k-мерное подпространство пространства X^n.

Число кодовых векторов равно $M = q^k$.

Код можно задать с помощью *порождающей матрицы* размера $k \times n$:

$$G = \begin{bmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ g_{k1} & g_{k2} & \cdots & g_{kn} \end{bmatrix}.$$

Элементы матрицы берутся из поля $GF(q)$. Строки матрицы должны быть линейно независимы над $GF(q)$.

2.3.1. Линейные коды. Кодирование

Для кодирования выбирается k-мерный *информационный вектор*

$$\underline{\mathbf{u}} = \begin{bmatrix} u_1 & u_2 & \dots & u_k \end{bmatrix}$$

с элементами из $GF(q)$.

Соответствующий ему кодовый вектор вычисляется с помощью порождающей матрицы G по формуле

$$\underline{\mathbf{u}}G = \begin{bmatrix} v_1 & v_2 & \dots & v_n \end{bmatrix}.$$

2.3.2. Дуальное пространство. Проверочная матрица

Скалярное произведение двух векторов $\underline{\mathbf{v}}$ и $\underline{\mathbf{h}}$ одинаковой размерности определяется формулой

$$(\underline{\mathbf{v}}, \underline{\mathbf{h}}) = v_1 h_1 + v_2 h_2 + \cdots + v_n h_n.$$

Рассмотрим множество векторов $\mathcal{H}$, *ортогональных всем кодовым векторам*:

$$\mathcal{H} = \{\underline{\mathbf{h}} : (\underline{\mathbf{u}}G, \underline{\mathbf{h}}) = 0 \quad \forall \underline{\mathbf{u}}\}.$$

1. Множество $\mathcal{H}$ является пространством решений однородной системы линейных уравнений $G\underline{\mathbf{h}}^\top = 0$.
2. Размерность пространства равна $n - k$.
3. Пространство называется *дуальным*, или *двойственным*, к кодовому пространству.

Пространство $\mathcal{H}$ порождается матрицей размера $(n-k) \times n$:

$$H = \begin{bmatrix} h_{11} & h_{12} & \cdots & h_{1n} \\ h_{21} & h_{22} & \cdots & h_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ h_{(n-k),1} & h_{(n-k),2} & \cdots & h_{(n-k),n} \end{bmatrix}.$$

Элементы матрицы берутся из поля $GF(q)$. Строки матрицы должны быть линейно независимы над $GF(q)$ и ортогональны порождающей матрице G:

$$GH^\top = 0.$$

Матрица H называется *проверочной*, так как только для кодовых векторов верно равенство

$$\underline{\mathbf{v}}H^\top = \underline{\mathbf{u}}GH^\top = 0. \quad \text{Эквивалентно} \quad H\underline{\mathbf{v}}^\top = 0.$$

2.3.3. Систематическое кодирование

Пусть

$$G = \begin{bmatrix} I_k & P \end{bmatrix},$$

где I_k – единичная матрица порядка k, а P – некоторая матрица размера $k \times (n-k)$. Тогда кодовый вектор имеет вид

$$\underline{\mathbf{u}}G = \begin{bmatrix} \underline{\mathbf{u}} & \underline{\mathbf{u}}P \end{bmatrix}.$$

В кодовом векторе на первых k позициях стоят информационные символы. Символы в части $\underline{\mathbf{u}}P$ называются *проверочными*.

Такая форма порождающей матрицы называется систематической формой, а кодирование – систематическим.

2.3.4. Другое систематическое кодирование

Иногда удобно, чтобы кодовый вектор имел вид

$$\underline{\mathbf{v}}(\underline{\mathbf{u}}) = \begin{bmatrix} \underline{\mathbf{s}} & \underline{\mathbf{u}} \end{bmatrix},$$

где $\underline{\mathbf{s}}$ – проверочные символы. В этом случае порождающая матрица должна иметь вид

$$G = \begin{bmatrix} P & I_k \end{bmatrix}.$$

Тогда

$$\underline{\mathbf{s}} = \underline{\mathbf{u}}P.$$

2.3.5. Расстояние в линейных кодах

Пусть задана проверочная $(n-k) \times n$ матрица H линейного кода.

Кодовое расстояние линейного кода равно d тогда и только тогда, когда в проверочной матрице *любые* $d-1$ столбцов линейно независимы и существуют d линейно зависимых столбцов.

Указание. Если некоторый вектор $\underline{\mathbf{v}}$ имеет вес s, то умножение H на $\underline{\mathbf{v}}^\top$ дает линейную комбинацию каких-то s столбцов матрицы H. Эта комбинация не может равняться 0, если $s \leq d-1$, поэтому такие векторы не могут быть кодовыми.

Коды Хэмминга с расстоянием $d = 3$. Пусть $q = 2$. Построим проверочную матрицу кода с расстоянием $d = 3$. Любые 2 различных ненулевых столбца должны быть линейно независимы, поэтому в $(n-k) \times n$ матрице H все n столбцов должны быть ненулевыми и различными.

Пусть проверочная матрица имеет размер $m \times (2^m - 1)$. В качестве столбцов высоты m выберем все ненулевые двоичные столбцы. Их ровно $2^m - 1$. Построена проверочная матрица оптимального кода Хэмминга с расстоянием $d = 3$.

Коды Хэмминга с расстоянием $d = 4$. Построим проверочную матрицу H размера $m \times (2^{m-1})$ следующим образом. В качестве столбцов матрицы выберем все столбцы нечетного веса. Число таких столбцов равно $C_m^1 + C_m^3 + \cdots = 2^{m-1}$. Очевидно, что любые 3 таких столбца линейно независимы над полем $GF(2)$.

2.3.6. Синдромное декодирование линейного кода

Рассматриваем случай $q = 2$. Задан линейный (n, k)-код с расстоянием $d = 2t + 1$. Обозначим $n - k = m$. Представим пространство X^n виде так называемой стандартной таблицы:

$$\begin{array}{ccccc|l}
v_0 = 0 & v_1 & v_2 & \dots & v_{2^k-1} & S_0 = 0 \\
z_1 & z_1 \oplus v_1 & z_1 \oplus v_2 & \dots & z_1 \oplus v_{2^k-1} & S_1 = z_1 H^\top \\
z_2 & z_2 \oplus v_1 & z_2 \oplus v_2 & \dots & z_2 \oplus v_{2^k-1} & S_2 = z_2 H^\top \\
\dots & \dots & \dots & \dots & \dots & \dots \\
z_{2^m-1} & z_{2^m-1} \oplus v_1 & z_{2^m-1} \oplus v_2 & \dots & z_{2^m-1} \oplus v_{2^k-1} & S_{2^m-1} = z_{2^m-1} H^\top
\end{array}$$

$y = v_j \oplus z_i$; $S = yH^\top = v_j H^\top \oplus z_i H^\top = z_i H^\top = S_i$;
z_i – лидер смежного класса; S – синдром. Если $W_H(z_i) \le t$, то лидер единственный и ошибка будет исправлена правильно.

Г л а в а 3

Циклические коды

3.1. Представление циклических кодов

Пусть $\mathbf{v} = (v_0, v_1, v_2, \ldots, v_{n-1})$ — вектор из пространства X^n. *Правым циклическим сдвигом* этого вектора называется вектор

$$\mathbf{v}^{\mathrm{r}} = (v_{n-1}, v_0, v_1, \ldots, v_{n-2}).$$

Линейный (n, k)-код $\mathcal{C}$ называется *циклическим*, если циклический сдвиг каждого кодового вектора также является кодовым вектором.

Для анализа свойств циклических кодов удобно каждый вектор $\mathbf{v} = (v_0, v_1, v_2, \ldots, v_{n-1})$ линейного пространства X^n представить в виде многочлена над полем $GF(q)$ степени $n-1$ или меньше, используя координаты вектора $\mathbf{v}$ в качестве коэффициентов:

$$\mathbf{v} = (v_0, v_1, \ldots, v_{n-1}) \Leftrightarrow \mathbf{v}(x) = v_0 + v_1 x + \cdots + v_{n-1} x^{n-1}.$$

Многочлены $\mathbf{v}(x)$ можно складывать и умножать на скаляр. Расширим операцию умножения, разрешив перемножать многочлены $\mathbf{v}_1(x)$ и $\mathbf{v}_2(x)$ по модулю $x^n - 1$. С этой целью представим произведение этих многочленов в виде $\mathbf{v}_1(x)\mathbf{v}_2(x) = \mathbf{q}(x)(x^n - 1) + \mathbf{v}(x)$, где $\mathbf{v}(x)$ – многочлен над $GF(q)$ степени не выше $n-1$. Тогда

$$\mathbf{v}_1(x)\mathbf{v}_2(x) \bmod (x^n - 1) = \mathbf{v}(x).$$

Пусть

$$\mathbf{v} = (v_0, v_1, \ldots, v_{n-1}) \Leftrightarrow \mathbf{v}(x) = v_0 + v_1 x + \cdots + v_{n-1} x^{n-1}.$$

Тогда многочлен $x\mathbf{v}(x) \bmod (x^n - 1)$ имеет вид

$$\begin{aligned} x\mathbf{v}(x) \bmod (x^n - 1) &= v_0 x + v_1 x^2 + \cdots + v_{n-1} x^n \bmod (x^n - 1) = \\ &= v_{n-1}(x^n - 1) + v_{n-1} + v_0 x + v_1 x^2 + \cdots + v_{n-2} x^{n-1} \bmod (x^n - 1) = \\ &= v_{n-1} + v_0 x + v_1 x^2 + \cdots + v_{n-2} x^{n-1}. \end{aligned}$$

Таким образом,

$$x\mathbf{v}(x) \bmod (x^n - 1) \Rightarrow \mathbf{v}^{\mathrm{r}} = (v_{n-1}, v_0, \ldots, v_{n-2}),$$

то есть умножение многочлена на x приводит к правому циклическому сдвигу его коэффициентов.

В полиномиальной форме линейный циклический (n, k)-код $\mathcal{C}$ состоит из q^k многочленов. Каждый ненулевой многочлен имеет степень, по крайней мере, $n - k$, но не более $n - 1$. Существует один и только один приведенный многочлен $\mathbf{g}(x)$ степени $n - k$ следующего вида:

$$\mathbf{g}(x) = g_0 + g_1 x + g_2 x^2 + \cdots + g_{n-k-1} x^{n-k-1} + x^{n-k},\ g_0 \neq 0.$$

Этот многочлен имеет минимальную степень. Каждый кодовый многочлен кода $\mathcal{C}$ *делится без остатка* на $\mathbf{g}(x)$. Любой многочлен степени не выше $n-1$, делящийся без остатка на $\mathbf{g}(x)$, лежит в коде $\mathcal{C}$. Следовательно, линейный циклический (n, k)-код $\mathcal{C}$ однозначно определяется единственным многочленом $\mathbf{g}(x)$, который называется *порождающим*. Степень порождающего многочлена равна числу проверочных символов кода.

Каждый кодовый многочлен $\mathbf{v}(x)$ может быть представлен в виде

$$\mathbf{v}(x) = \mathbf{u}(x)\mathbf{g}(x),$$

где многочлен $\mathbf{u}(x) = u_0 + u_1 x + \cdots + u_{k-1} x^{k-1}$ имеет степень $k - 1$ или меньше. Вектор $\mathbf{u} = (u_0, u_1, \ldots, u_{k-1})$ можно интерпретировать как *информационный вектор*, подлежащий передаче. Соответствующий многочлен $\mathbf{u}(x)$ называют *информационным многочленом*, а многочлен $\mathbf{v}(x)$ — кодовым многочленом, полученным в результате кодирования. Порождающая матрица циклического (n, k)-кода для этого метода кодирования имеет вид

$$\mathbf{G} = \begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_{n-k-1} & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k-2} & g_{n-k-1} & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & g_0 & g_1 & g_2 & g_3 & \cdots & g_{n-k-1} & 1 \end{bmatrix}.$$

Первая строка этой матрицы состоит из коэффициентов порождающего полинома $\mathbf{g}(x)$. Остальные $k-1$ строк являются последовательными правыми циклическими сдвигами первой строки. Порождающая матрица $\mathbf{G}$ не имеет систематической формы, но может быть приведена к ней только элементарными преобразованиями строк.

Порождающий многочлен $\mathbf{g}(x)$ циклического (n, k) кода является делителем многочлена $x^n - 1$. Следовательно, многочлен $x^n - 1$ можно представить в виде

$$\mathbf{g}(x)\mathbf{h}(x) = x^n - 1,$$

где $\mathbf{h} = h_0 + h_1 x + \cdots + h_{k-1}x^{k-1} + h_k x^k$.

Многочлен $\mathbf{h}(x)$ называется *проверочным* многочленом кода $\mathcal{C}$. Если преобразовать его в вектор $\mathbf{h} = (1, h_1, \ldots, h_{k-1}, h_k, 0, \ldots, 0)$ из X^n, то проверочную матрицу линейного циклического кода $\mathcal{C}$ можно записать в виде

$$H = \begin{bmatrix} 0 & 0 & \cdots & 0 & h_k & h_{k-1} & \cdots & h_0 \\ 0 & \cdots & 0 & h_k & h_{k-1} & \cdots & h_0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ h_k & h_{k-1} & \cdots & h_0 & 0 & 0 & \cdots & 0 \end{bmatrix}.$$

Коэффициенты многочлена $g(x)h(x) = x^n - 1$ равны нулю, кроме первого и последнего. Вычисляя их в явном виде, находим, что они равны произведению строк матриц G и H. Таким образом, $GH^\top = 0$.

3.2. Систематическая форма порождающей и проверочной матриц

Кодирование с помощью порождающего многочлена $\mathbf{g}(x)$ можно сделать систематическим, если условиться, что информационные символы $\mathbf{u} = (u_0, u_1, \ldots, u_{k-1})$ будут расположены на последних k позициях кодового вектора. С этой целью умножим информационный многочлен $\mathbf{u}(x)$ на x^{n-k}:

$$x^{n-k}\mathbf{u}(x) = u_0 x^{n-k} + u_1 x^{n-k+1} + \cdots + u_{k-1}x^{n-1}.$$

Полученный многочлен степени $n-1$ или меньше разделим с остатком на порождающий многочлен $\mathbf{g}(x)$:

$$x^{n-k}\mathbf{u}(x) = \mathbf{a}(x)\mathbf{g}(x) + \mathbf{b}(x), \tag{3.1}$$

где $\mathbf{a}(x)$ и $\mathbf{b}(x)$ — частное и остаток соответственно. Многочлен $-\mathbf{b}(x)$ можно записать в виде

$$-\mathbf{b}(x) = -b_0 - b_1 x - \cdots - b_{n-k-1}x^{n-k-1}.$$

Этот многочлен называют многочленом *проверочных символов*. Перепишем соотношение (3.1) как

$$-\mathbf{b}(x) + x^{n-k}\mathbf{u}(x) = \mathbf{a}(x)\mathbf{g}(x).$$

Левая часть является кратным многочлена $\mathbf{g}(x)$. Следовательно, она является кодовым многочленом циклического (n,k)-кода $\mathcal{C}$. Представим этот многочлен как вектор из X^n:

$$(-b_0, -b_1, \ldots, -b_{n-k-1}, u_0, u_1, \ldots, u_{k-1}).$$

Этот вектор записан в систематической форме: последние k позиций — это *информационные* символы, а первые $n-k$ — это *проверочные* символы, которые равны взятым со знаком «минус» коэффициентам остатка $\mathbf{b}(x)$. Если информационный многочлен содержит единственный ненулевой коэффициент, то есть $\mathbf{u}(x) = \mathbf{u}_i(x) = x^i$, то многочлен проверочных символов равен

$$-\mathbf{b}(x) = -\mathbf{b}_i(x) = -b_{i,0} - b_{i,1}x - \cdots - b_{i,n-k-1}x^{n-k-1}.$$

Как следствие, порождающая матрица циклического (n,k)-кода $\mathcal{C}$ в систематическом виде примет форму

$$G_{\text{sys}} = \begin{bmatrix} -b_{0,0} & -b_{0,1} & \cdots & -b_{0,n-k-1} & 1 & 0 & 0 & \cdots & 0 \\ -b_{1,0} & -b_{1,1} & \cdots & -b_{1,n-k-1} & 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ -b_{k-1,0} & -b_{k-1,1} & \cdots & -b_{k-1,n-k-1} & 0 & 0 & 0 & \cdots & 1 \end{bmatrix}. \tag{3.2}$$

Соответствующая проверочная матрица циклического (n,k)-кода в систематической форме такова:

$$H_{\text{sys}} = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & b_{0,0} & b_{1,0} & \cdots & b_{k-1,0} \\ 0 & 1 & 0 & \cdots & 0 & b_{0,1} & b_{1,1} & \cdots & b_{k-1,1} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & b_{0,n-k-1} & b_{1,n-k-1} & \cdots & b_{k-1,n-k-1} \end{bmatrix}. \tag{3.3}$$

Г л а в а 4
Коды Боуза—Чоудхури—Хоквингема

Наиболее интересными циклическими кодами являются коды Боуза—Чоудхури—Хоквингема (БЧХ-коды). Далее рассматриваются коды над полями характеристики 2.

4.1. Конструкция и параметры кодов БЧХ

Пусть α примитивный элемент поля $GF(2^m)$ порядка $2^m - 1$.

Двоичным кодом БЧХ называется циклический (n, k)-код длины $n = 2^m - 1$, порождающий многочлен $\mathbf{g}(x)$ которого делит многочлен $x^{2^m-1} - 1$, имеет наименьшую степень и содержит в качестве корней следующие $2t$ последовательных степеней примитивого элемента α:

$$\alpha, \alpha^2, \ldots, \alpha^{2t}.$$

Напомним, что минимальным многочленом элемента $\gamma \in GF(2^m)$ называется многочлен над $GF(2)$ минимальной степени, корнем которого является γ. Степень минимального многочлена не превосходит m.

Обозначим через $\varphi_i(x)$ минимальный многочлен для α^i. Тогда порождающий многочлен $\mathbf{g}(x)$ равен наименьшему общему кратному (LCM — the least common multiple) минимальных многочленов:

$$\mathbf{g}(x) = LCM\left\{\varphi_1(x), \varphi_2(x), \ldots, \varphi_{2t}(x)\right\}.$$

В двоичном случае минимальные многочлены для элементов α и α^2 одинаковы, поэтому в указанном выражении можно опустить все многочлены с четными индексами. В результате порождающий многочлен будет равен

$$\mathbf{g}(x) = LCM\left\{\varphi_1(x), \varphi_3(x), \ldots, \varphi_{2t-1}(x)\right\}.$$

Это выражение содержит только t многочленов. Так как степень минимального многочлена любого элемента γ из поля $GF(2^m)$ не превосходит m, то степень порождающего многочлена $\mathbf{g}(x)$ не превосходит mt.

Следовательно, число проверочных символов циклического $(2^m-1, k)$-кода БЧХ также не превосходит mt, а размерность кода k не меньше $2^m - mt - 1$.

Описанные выше коды БЧХ называются *примитивными* или кодами БЧХ в *узком смысле*, так как для их построения используется примитивный элемент α поля $GF(2^m)$.

Найдем кодовое расстояние кода БЧХ. С этой целью вычислим проверочную матрицу кода.

Проверочная матрица кодов БЧХ. Любой кодовый многочлен циклического кода делится на порождающий многочлен $\mathbf{g}(x)$. Пусть $\mathbf{v}(x) = v_0 + v_1 x + \cdots + v_{2^m-2} x^{2^m-2}$ — какой-нибудь кодовый многочлен циклического кода БЧХ. Тогда он обращается в нуль во всех корнях многочлена $\mathbf{g}(x)$. В частности, для $1 \le i \le 2t$ имеем

$$\mathbf{v}(\alpha^i) = v_0 + v_1\alpha^i + v_2\alpha^{2i} + \cdots + v_{2^m-2}\alpha^{(2^m-2)i} = 0,$$

или в матричном виде

$$\begin{pmatrix} v_0 & v_1 & v_2 & \cdots & v_{2^m-2} \end{pmatrix} \begin{pmatrix} 1 \\ \alpha^i \\ \alpha^{2i} \\ \vdots \\ \alpha^{(2^m-2)i} \end{pmatrix} = 0.$$

Рассматривая вместо кодового многочлена

$$\mathbf{v}(x) = v_0 + v_1 x + \cdots + v_{2^m-2} x^{2^m-2}$$

кодовый вектор $\mathbf{v} = (v_0, v_1, \ldots, v_{2^m-2})$, получаем соотношение

$$\mathbf{v} \cdot H^\top = 0,$$

где

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \ldots & \alpha^{2^m-2} \\ 1 & \alpha^2 & (\alpha^2)^2 & \ldots & (\alpha^2)^{2^m-2} \\ 1 & \alpha^3 & (\alpha^3)^2 & \ldots & (\alpha^3)^{2^m-2} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 1 & \alpha^{2t} & (\alpha^{2t})^2 & \ldots & (\alpha^{2t})^{2^m-2} \end{pmatrix}$$

— проверочная матрица циклического кода БЧХ над расширенным полем $GF(2^m)$. Размер этой матрицы равен $2t \times (2^m - 1)$. Докажем, что любые $2t$ столбцов этой матрицы линейно независимы над полем

$GF(2^m)$, а значит, и над полем $GF(2)$. Отсюда следует, что кодовое расстояние описанных кодов БЧХ не меньше, чем $2t+1$.

Для доказательства напомним, что квадратная $2t \times 2t$ матрица Вандермонда имеет вид

$$V = \begin{pmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{2t-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{2t-1} \\ 1 & x_3 & x_3^2 & \dots & x_3^{2t-1} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 1 & x_{2t} & x_{2t}^2 & \dots & x_{2t}^{2t-1} \end{pmatrix}.$$

Определитель этой матрицы равен

$$\det V = \prod_{1 \le j < i \le 2t} (x_i - x_j).$$

Он не равен нулю ($\det V \neq 0$), если все элементы x_i различны. В этом случае все $2t$ столбцов матрицы $\mathbf{V}$ линейно независимы.

Заметим, что любые $2t$ столбцов матрицы $\mathbf{H}$ могут быть представлены как матрица Вандермонда, что и доказывает линейную независимость любых $2t$ столбцов матрицы $\mathbf{H}$.

Параметры кодов БЧХ

1. Длина двоичного примитивного кода БЧХ равна $n = 2^m - 1$.

2. Число проверочных символов равно степени r многочлена

$$\mathbf{g}(x) = LCM\left\{\varphi_1(x), \varphi_3(x), \dots, \varphi_{2t-1}(x)\right\}.$$

$$\deg(\varphi_i(x)) \le m, \quad r \le tm.$$

3. Число информационных символов $k = n - r \ge 2^m - 1 - tm$.

4. Расстояние примитивного кода БЧХ $d \ge 2t+1$. Код может исправлять t или меньше ошибок.

Число $2t+1$ называется *конструктивным расстоянием* кода БЧХ.

4.2. Декодирование кодов БЧХ

Пусть на передающем конце используется циклический код БЧХ с расстоянием $2t+1$. Пусть по каналу передается кодовый вектор кода БЧХ

$$\mathbf{v} = (v_0, v_1, \dots, v_{2^m-2}).$$

Предположим, что в канале добавляется вектор ошибки

$$\mathbf{e} = (e_0, e_1, \ldots, e_{2^m-2}),$$

так что приемник получает вектор

$$\mathbf{y} = \mathbf{v} + \mathbf{e} = (v_0 + e_0, v_1 + e_1, \ldots, v_{2^m-2} + e_{2^m-2}).$$

Задача декодирования состоит в том, чтобы по принятому вектору $\mathbf{y}$ определить, какой кодовый вектор $\mathbf{v}$ передавался приемником. Эта задача всегда имеет решение, если вес Хэмминга вектора ошибки $\mathbf{e}$ не превосходит корректирующей способности t кода БЧХ. Однако в этом случае декодирование должно быть простым, чтобы его можно было реализовать на практике.

Обычно декодирование начинается с вычисления *синдрома* $\mathbf{S}$ принятого вектора $\mathbf{y}$, определяемого как произведение принятого вектора на транспонированную проверочную матрицу кода БЧХ:

$$\mathbf{S} = \mathbf{y} \cdot \mathbf{H}^\top = (S_1, S_2, \ldots, S_{2t-1}, S_{2t}).$$

Так как $\mathbf{y} = \mathbf{v} + \mathbf{e}$ и $\mathbf{v} \cdot \mathbf{H}^\top = 0$, то синдром

$$\mathbf{S} = (\mathbf{v} + \mathbf{e}) \cdot \mathbf{H}^\top = \mathbf{e} \cdot \mathbf{H}^\top$$

зависит только от вектора ошибки $\mathbf{e}$. Для кодов БЧХ удобно принятый вектор $\mathbf{y}$ преобразовать в многочлен $\mathbf{y}(x)$, равный сумме передававшегося кодового многочлена $\mathbf{v}(x)$ и многочлена ошибки $\mathbf{e}(x)$:

$$\mathbf{y}(x) = \mathbf{v}(x) + \mathbf{e}(x).$$

Так как $\mathbf{v}(\alpha^i) = 0,\ i = 1, 2, \ldots, 2t$, то компоненты синдрома S_i равны

$$\begin{aligned} &S_i = y(\alpha^i) = v(\alpha^i) + e(\alpha^i) = e(\alpha^i) = \\ &= e_0 + e_1(\alpha^i) + \cdots + e_{2^m-3}(\alpha^i)^{2^m-3} + e_{2^m-2}(\alpha^i)^{2^m-2}. \\ &i = 1, 2, \ldots, 2t. \end{aligned} \tag{4.1}$$

Декодирование состоит в решении этой системы относительно неизвестных e_i в предположении, что известны компоненты синдрома S_j и что число ошибок не превосходит t.

4.2.1. Исправление одиночных ошибок

Пусть используется код БЧХ с расстоянием $d = 3$. С его помощью можно исправлять ошибки кратности $t = 1$. Корни порождающего

многочлена $\mathbf{g}(x)$ равны α и α^2. Для примитивного кода БЧХ с длиной $n = 2^m - 1$ в качестве порождающего многочлена $\mathbf{g}(x)$ можно выбрать неприводимый над $GF(2)$ примитивный многочлен степени m. Напомним, что позиции координат вектора нумеруются целыми числами от 0 до $2^m - 2$. Пусть при передаче кодового многочлена произошла ошибка в позиции с номером j. Многочлен ошибки будет равен $\mathbf{e}(x) = x^j$, где позиция j неизвестна декодеру. Однако синдром ошибки $\mathbf{e}(x)$ можно вычислить. Система (4.1) имеет вид

$$S_1 = \mathbf{e}(\alpha) = \alpha^j; \quad S_2 = \mathbf{e}(\alpha^2) = \alpha^{2j}.$$

Так как $S_2 = \mathbf{e}(\alpha^2) = \mathbf{e}(\alpha)^2 = S_1^2$, то второе уравнение излишне. Обозначив $\alpha^j = X$, получим уравнение

$$X = S_1,$$

из которого надо найти j. Так как любой ненулевой элемент поля можно представить как степень элемента α, то по таблице поля находим степень j для элемента S_1. Номером позиции ошибки будет j.

Рассмотрим, например, таблицу поля $GF(2^4)$, заданного примитивным многочленом $\mathbf{p}(x) = 1 + x^3 + x^4$ над $GF(2)$. В первом и третьем столбцах таблицы запишем все элементы поля в естественном базисе $(1, \alpha, \alpha^2, \alpha^3)$, где α — корень многочлена $\mathbf{p}(x)$. Во втором и четвертом столбцах эти же элементы записаны в степенном виде.

Базисный вид	Степенной вид	Базисный вид	Степенной вид
0	0	$\alpha + \alpha^2$	α^7
1	1	$\alpha + \alpha^2 + \alpha^3$	α^8
α	α	$1 + \alpha^2$	α^9
α^2	α^2	$\alpha + \alpha^3$	α^{10}
α^3	α^3	$1 + \alpha^2 + \alpha^3$	α^{11}
$1 + \alpha^3$	α^4	$1 + \alpha$	α^{12}
$1 + \alpha + \alpha^3$	α^5	$\alpha + \alpha^2$	α^{13}
$1 + \alpha + \alpha^2 + \alpha^3$	α^6	$\alpha^2 + \alpha^3$	α^{14}

Порождающий многочлен $\mathbf{g}(x)$ кода БЧХ здесь совпадает с многочленом $\mathbf{p}(x)$. Предположим, что передавался кодовый вектор

$$\mathbf{v} = (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0),$$

а принят вектор

$$\mathbf{y} = ((1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)).$$

Многочлен $\mathbf{y}(x)$ равен

$$\mathbf{y}(x) = 1 + x^3 + x^4 + x^5 + x^6 + x^8 + x^9.$$

С помощью таблицы поля вычисляем компоненту синдрома:

$$S_1 = \mathbf{y}(\alpha) = 1 + \alpha^3 + \alpha^4 + \alpha^5 + \alpha^6 + \alpha^8 + \alpha^9 = 1 + \alpha + \alpha^2 + \alpha^3.$$

Снова по таблице поля находим представление S_1 в степенном виде: $S_1 = 1 + \alpha + \alpha^2 + \alpha^3 = \alpha^6$. Отсюда следует, что ошибка произошла в позиции $j = 6$ (отсчет позиций начинается с 0).

4.2.2. Исправление двойных ошибок

Пусть используется код БЧХ с расстоянием $d = 5$. С его помощью можно исправлять ошибки кратности $t = 2$. Корни порождающего многочлена $\mathbf{g}(x)$ равны $\alpha, \alpha^2, \alpha^3, \alpha^4$. Для примитивного кода БЧХ с длиной $n = 2^m - 1$ в качестве порождающего многочлена $\mathbf{g}(x)$ можно выбрать произведение неприводимого над $GF(2)$ примитивного многочлена степени m, содержащего корни $\alpha, \alpha^2, \alpha^4$, и неприводимого многочлена, содержащего корень α^3. Пусть при передаче кодового многочлена произошла двойная ошибка в позициях с номерами j_1 и j_2. Многочлен ошибки будет равен $\mathbf{e}(x) = x^{j_1} + x^{j_2}$, где позиции j_1, j_2 неизвестны декодеру. Однако синдром ошибки $\mathbf{e}(x)$ можно вычислить. Система (4.1) имеет вид:

$$\begin{aligned}
&S_1 = \mathbf{e}(\alpha) = \alpha^{j_1} + \alpha^{j_2};\\
&S_2 = \mathbf{e}(\alpha^2) = \alpha^{2j_1} + \alpha^{2j_2} = S_1^2;\\
&S_3 = \mathbf{e}(\alpha^3) = \alpha^{3j_1} + \alpha^{3j_2};\\
&S_4 = \mathbf{e}(\alpha^4) = \alpha^{4j_1} + \alpha^{4j_2} = S_1^4.
\end{aligned}$$

Для решения понадобятся только первое и третье уравнения, так как второе и четвертое являются следствием первого. Введем обозначения $\alpha^{j_1} = X_1,\ \alpha^{j_2} = X_2$. Тогда

$$\begin{aligned}
X_1 + X_2 &= S_1\\
X_1^3 + X_2^3 &= S_3.
\end{aligned}$$

Исключив неизвестное X_2, получим уравнение

$$X_1^2 + S_1 X_1 + S_1^2 + \frac{S_3}{S_1} = 0.$$

Находим решение X_1 этого уравнения перебором, используя таблицу поля. Находим $X_2 = X_1 + S_1$. Представим решения в степенном виде: $X_1 = \alpha^{j_1},\ X_2 = \alpha^{j_2}$. Найдем позиции ошибок j_1 и j_2.

Для поля $GF(2^4)$ код БЧХ, исправляющий 2 ошибки, имеет длину 15 и задается порождающим многочленом

$$\mathbf{g}(x) = (1 + x^3 + x^4)(1 + x + x^2 + x^3 + x^4).$$

Первый сомножитель имеет среди корней элементы $\alpha, \alpha^2, \alpha^4$, второй имеет в качестве корня элемент α^3. Предположим, что передавался кодовый вектор

$$\mathbf{v} = (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0),$$

а принят вектор

$$\mathbf{y} = ((1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)).$$

Многочлен $\mathbf{y}(x)$ равен

$$\mathbf{y}(x) = 1 + x^3 + x^4 + x^5 + x^6 + x^8 + x^9 + x^{14}.$$

С помощью таблицы поля вычислим компоненты синдрома:

$$S_1 = \mathbf{y}(\alpha) = 1 + \alpha^3 + \alpha^4 + \alpha^5 + \alpha^6 + \alpha^8 + \alpha^9 + \alpha^{14} = \alpha^{12};$$
$$S_3 = \mathbf{y}(\alpha^3) = 1 + \alpha^9 + \alpha^{12} + \alpha^{15} + \alpha^{18} + \alpha^{24} + \alpha^{27} + \alpha^{42} = \alpha^5.$$

Решаем уравнение $X_1^2 + S_1 X_1 + S_1^2 + S_3/S_1 = X_1^2 + \alpha^{12} X_1 + \alpha^5 = 0$ перебором. Находим $X_1 = \alpha^6$, $X_2 = X_1 + S_1 = \alpha^6 + \alpha^{12} = \alpha^{14}$. Находим позиции, в которых произошли ошибки: $j_1 = 6,\ j_2 = 14$ (отсчет позиций начинается с 0).

4.2.3. Общий случай исправления ошибок

Для описания алгоритма исправления ошибок кодами БЧХ нужны некоторые сведения из теории симметрических многочленов.

Симметрические многочлены. Многочлен $f(X_1, X_2, \ldots, X_t)$ называется *симметрическим*, если он не меняется при любой перестановке неизвестных.

Рассмотрим два типа симметрических многочленов.

Степенные симметрические многочлены от t переменных:

$$S_k = X_1^k + X_2^k + \cdots + X_t^k, \quad k = 1, 2, \ldots$$

Степени k могут быть любыми.

Элементарные симметрические многочлены от t переменных:

$$\begin{aligned}
&\sigma_0 = 1,\\
&\sigma_1 = X_1 + X_2 + \cdots + X_t,\\
&\sigma_2 = \sum_{1\le i_1<i_2\le t} X_{i_1}X_{i_2},\\
&\cdots\cdots\cdots\\
&\sigma_k = \sum_{1\le i_1<i_2<\cdots<i_k\le t} X_{i_1}X_{i_2}\ldots X_{i_k},\\
&\cdots\cdots\cdots\\
&\sigma_t = X_1X_2\ldots X_t,\\
&\sigma_{t+i} = 0, \quad i \ge 1.
\end{aligned}$$

Число элементарных симметрических многочленов от t переменных равно $t+1$: $\sigma_0, \sigma_1, \ldots, \sigma_t$. Для удобства полагаем, что $\sigma_k = 0$ при $k > t$.

Тождества Ньютона. Многочлены S_k и σ_k связаны соотношениями, которые называются тождествами Ньютона:

$$\begin{aligned}
&S_1 - \sigma_1 = 0,\\
&S_2 - S_1\sigma_1 + 2\sigma_2 = 0,\\
&S_3 - S_2\sigma_1 + S_1\sigma_2 - 3\sigma_3 = 0,\\
&\ldots\\
&S_t - S_{t-1}\sigma_1 + S_{t-2}\sigma_2 - \cdots + (-1)^{t-1}\cdot S_1\sigma_{t-1} + (-1)^t\cdot t\sigma_t = 0,\\
&S_{t+1} - S_t\sigma_1 + S_{t-1}\sigma_2 - \cdots + (-1)^t\cdot S_1\sigma_t = 0,\\
&S_{t+2} - S_{t+1}\sigma_1 + S_t\sigma_2 - \cdots + (-1)^t\cdot S_2\sigma_t = 0,\\
&\ldots\\
&S_{2t} - S_{2t-1}\sigma_1 + S_{2t-2}\sigma_2 - \cdots + (-1)^t\cdot S_t\sigma_t = 0.\\
&\ldots
\end{aligned}$$

Уравнение с номером $j = 1, 2, \ldots, t$ содержит j слагаемых, причем последнее слагаемое равно $(-1)^j \cdot j\sigma_j$. Начиная с номера $j = t+1$, число слагаемых остается равным t, причем последнее слагаемое равно $(-1)^t S_{j-t}\sigma_t$. Для примера выше приведены первые $2t$ из тождеств Ньютона.

При заданных S_j это линейная система относительно σ_k. Для двоичных полей $GF(2^m)$ четные числа эквивалентны 0, а нечетные $-$ 1. В дальнейшем понадобится находить решения $\sigma_1, \ldots, \sigma_t$ при заданном числе $j = 2t$ уравнений и заданных значениях элементов $S_1, S_2, \ldots, S_{2t}$. Число уравнений больше числа неизвестных. В случае, когда система имеет решение с заданными свойствами, можно использовать только часть уравнений. В одном из алгоритмов удобно использовать последние t из написанных выше уравнений. Запишем их в матричном виде

для двоичных полей:

$$\begin{pmatrix} S_t & S_{t-1} & S_{t-2} & \dots & S_2 & S_1 \\ S_{t+1} & S_t & S_{t-1} & \dots & S_3 & S_2 \\ S_{t+2} & S_{t+1} & S_t & \dots & S_4 & S_3 \\ \vdots & \vdots & \vdots & \dots & \vdots & \vdots \\ S_{2t-2} & S_{2t-3} & S_{2t-4} & \dots & S_t & S_{t-1} \\ S_{2t-1} & S_{2t-2} & S_{2t-3} & \dots & S_{t+1} & S_t \end{pmatrix} \begin{pmatrix} \sigma_1 \\ \sigma_2 \\ \sigma_3 \\ \vdots \\ \sigma_{t-1} \\ \sigma_t \end{pmatrix} = \begin{pmatrix} S_{t+1} \\ S_{t+2} \\ S_{t+3} \\ \vdots \\ S_{2t-1} \\ S_{2t} \end{pmatrix}. \quad (4.2)$$

Перейдем к декодированию кодов БЧХ. Пусть $d = 2t + 1$. Порождающий многочлен $\mathbf{g}(x)$ кода БЧХ имеет, по определению, корни α, α^2, α^3, $\dots$, α^{2t}.

Пусть произошло t ошибок в позициях j_1, j_2, $\dots$, j_t. Тогда многочлен ошибок равен

$$\mathbf{e}(x) = x^{j_1} + x^{j_2} + \dots + x^{j_t},$$

где позиции $j_1, j_2, \dots, j_t$ неизвестны. Вычисляем синдром:

$$\begin{aligned} &S_1 = \mathbf{e}(\alpha) = \alpha^{j_1} + \alpha^{j_2} + \dots + \alpha^{j_t}, \\ &S_2 = \mathbf{e}(\alpha^2) = \alpha^{2j_1} + \alpha^{2j_2} + \dots + \alpha^{2j_t}, \\ &S_3 = \mathbf{e}(\alpha^3) = \alpha^{3j_1} + \alpha^{3j_2} + \dots + \alpha^{3j_t}, \\ &\dots\dots\dots\dots \\ &S_{2t} = \mathbf{e}(\alpha^{2t}) = \alpha^{2tj_1} + \alpha^{2tj_2} + \dots + \alpha^{2tj_t}. \end{aligned}$$

Обозначим $\alpha^{j_i} = X_i$. Элементы X_i называются *локаторами ошибок*. Запишем систему в виде

$$\begin{aligned} &S_1 = X_1 + X_2 + \dots + X_t, \\ &S_2 = X_1^2 + X_2^2 + \dots + X_t^2, \\ &S_3 = X_1^3 + X_2^3 + \dots + X_t^3, \\ &\dots\dots\dots \\ &S_{2t} = X_1^{2t} + X_2^{2t} + \dots + X_t^{2t}. \end{aligned}$$

Компонента синдрома S_k — это значение степенного симметрического многочлена $X_1^k + X_2^k + \dots + X_t^k$ в точках α^{j_1}, α^{j_2}, $\dots$, α^{j_t}. Введем *многочлен локаторов ошибок*:

$$\sigma(X) = (X - X_1)(X - X_2)\cdots(X - X_t) = X^t - \sigma_1 X^{t-1} + \sigma_2 X^{t-2} - \dots + (-1)^t \sigma_t.$$

Коэффициентами этого многочлена являются элементарные симметрические функции $\sigma_1, \dots, \sigma_t$ от переменных $(X_1, X_2, \dots, X_t)$.

Алгоритм декодирования кодов БЧХ

1. Вычислить синдром $\begin{pmatrix} S_1 & S_2 & \dots & S_{2t} \end{pmatrix}$ принятого вектора $\mathbf{y}$.

2. Предположить, что произошло точно t ошибок и попытаться решить систему (4.2). Это возможно, если матрица коэффициентов в (4.2) невырожденная. В противном случае предположить, что произошло $t-1$ ошибок и рассмотреть систему с меньшим числом переменных.

3. По найденным $\sigma_1, \dots, \sigma_t$ восстановить многочлен локаторов ошибок:

$$\sigma(X) = X^t + \sigma_1 X^{t-1} + \sigma_2 X^{t-2} + \dots + \sigma_t.$$

4. Перебором найти корни $X_1, X_2, \dots, X_t$ этого многочлена. Восстановить по таблицам поля позиции $j_1, j_2, \dots, j_t$ искаженных символов и исправить их значения.

Г л а в а 5

Коды Рида—Соломона

Линейные (n, k)-коды с расстоянием d, для которых

$$k = n - d + 1,$$

называются кодами с *максимально достижимым расстоянием* (кодами МДР).

Наиболее важным классом кодов МДР являются коды Рида–Соломона. Эти коды могут быть определены над любым конечным полем $GF(q)$. На практике наиболее расп5странен случай, когда $q = 2^m$, m — положительное целое число. Далее рассматривается только этот случай.

5.1. Конструкция кодов Рида—Соломона

Пусть α — примитивный элемент поля $GF(2^m)$ порядка $2^m - 1$.

Кодом Рида—Соломона длины $n = 2^m - 1$ и с расстоянием d называется циклический код, порождающий многочлен $\mathbf{g}(x)$ которого равен

$$\mathbf{g}(x) = (x - \alpha)(x - \alpha^2) \cdots (x - \alpha^{d-1}).$$

Кодовые многочлены $\mathbf{V}(x)$ имеют вид $\mathbf{V}(x) = \mathbf{m}(x) \cdot \mathbf{g}(x)$, где $\mathbf{m}(x)$ — многочлен над полем $GF(2^m)$ степени не выше $n-d = k-1$. Параметры кода Рида—Соломона:

1. Длина $n = q - 1 = 2^m - 1$.

2. Число проверочных символов $r = d - 1$.

3. Число информационных символов $k = n - r = n - d + 1$.

4. Кодовое расстояние d.

5. Код Рида—Соломона является кодом МДР.

Для анализа свойств кодов Рида—Соломона удобно использовать методы, связанные с применением дискретного преобразования Фурье, хотя результаты для кодов БЧХ применимы и для кодов Рида–Соломона.

5.2. Дискретное преобразование Фурье (ДПФ)

Рассмотрим n-мерное линейное пространство над полем $GF(q)$ размерности $n = q-1 = 2^m-1$. Пусть α примитивный элемент этого поля. *Дискретное преобразование Фурье* (ДПФ) в линейном пространстве определяется с помощью квадратной $n \times n$ матрицы:

$$\mathbf{F} = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{2(n-1)} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 1 & \alpha^{n-1} & \alpha^{2(n-1)} & \dots & \alpha^{(n-1)(n-1)} \end{bmatrix} = \left[\alpha^{ij}\right]_{i=0,\dots,n-1}^{j=0,\dots,n-1}.$$

Для линейного пространства над полем $GF(8)$ матрица ДПФ имеет вид

$$\mathbf{F}_8 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^8 & \alpha^{10} & \alpha^{12} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & \alpha^{15} & \alpha^{18} \\ 1 & \alpha^4 & \alpha^8 & \alpha^{12} & \alpha^{16} & \alpha^{20} & \alpha^{24} \\ 1 & \alpha^5 & \alpha^{10} & \alpha^{15} & \alpha^{20} & \alpha^{25} & \alpha^{30} \\ 1 & \alpha^6 & \alpha^{12} & \alpha^{18} & \alpha^{24} & \alpha^{30} & \alpha^{36} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha & \alpha^4 \\ 1 & \alpha^4 & \alpha & \alpha^5 & \alpha^2 & \alpha^6 & \alpha^3 \\ 1 & \alpha^5 & \alpha^3 & \alpha & \alpha^6 & \alpha^4 & \alpha^2 \\ 1 & \alpha^6 & \alpha^5 & \alpha^4 & \alpha^3 & \alpha^2 & \alpha \end{bmatrix} \tag{5.1}$$

Прямое дискретное преобразование Фурье (ПДПФ) вектора линейного пространства $\mathbf{v} = [v_0\ v_1\ \dots\ v_{n-1}]$ определяется формулой

$$\mathbf{V} = [v_0\ v_1\ \dots\ v_{n-1}] \cdot \mathbf{F} = [V_0\ V_1\ \dots\ V_{n-1}].$$

Вектор $\mathbf{V}$ называется фурье-образом вектора $\mathbf{v}$, а его координаты V_j фурье-компонентами.

Матрица ДПФ $\mathbf{F}$ имеет обратную:

$$\mathbf{W} = \mathbf{F}^{-1} = \left[\alpha^{-ij}\right]_{i=0,\dots,n-1}^{j=0,\dots,n-1}.$$

Для линейного пространства над полем $GF(8)$ матрица обратного

ДПФ имеет вид

$$\mathbf{W}_8 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha^{-1} & \alpha^{-2} & \alpha^{-3} & \alpha^{-4} & \alpha^{-5} & \alpha^{-6} \\ 1 & \alpha^{-2} & \alpha^{-4} & \alpha^{-6} & \alpha^{-8} & \alpha^{-10} & \alpha^{-12} \\ 1 & \alpha^{-3} & \alpha^{-6} & \alpha^{-9} & \alpha^{-12} & \alpha^{-15} & \alpha^{-18} \\ 1 & \alpha^{-4} & \alpha^{-8} & \alpha^{-12} & \alpha^{-16} & \alpha^{-20} & \alpha^{-24} \\ 1 & \alpha^{-5} & \alpha^{-10} & \alpha^{-15} & \alpha^{-20} & \alpha^{-25} & \alpha^{-30} \\ 1 & \alpha^{-6} & \alpha^{-12} & \alpha^{-18} & \alpha^{-24} & \alpha^{-30} & \alpha^{-36} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha^{6} & \alpha^{5} & \alpha^{4} & \alpha^{3} & \alpha^{2} & \alpha \\ 1 & \alpha^{5} & \alpha^{3} & \alpha & \alpha^{6} & \alpha^{4} & \alpha^{2} \\ 1 & \alpha^{4} & \alpha & \alpha^{5} & \alpha^{2} & \alpha^{6} & \alpha^{3} \\ 1 & \alpha^{3} & \alpha^{6} & \alpha^{2} & \alpha^{5} & \alpha & \alpha^{4} \\ 1 & \alpha^{2} & \alpha^{4} & \alpha^{6} & \alpha & \alpha^{3} & \alpha^{5} \\ 1 & \alpha & \alpha^{2} & \alpha^{3} & \alpha^{4} & \alpha^{5} & \alpha^{6} \end{bmatrix} \tag{5.2}$$

Эта матрица определяет *обратное дискретное преобразование Фурье* (ОДПФ):

$$\mathbf{v} = [V_0\ V_1\ \ldots\ V_{n-1}] \cdot \mathbf{W} = [v_0\ v_1\ \ldots\ v_{n-1}].$$

Множество векторов $\{\mathbf{v}\}$ обычно называют *временно́й* областью.

Множество фурье-образов, то есть векторов $\{\mathbf{V} = \mathbf{v} \cdot \mathbf{F}\}$, называют *частотной* областью.

В координатном виде связь между координатами векторов $\mathbf{v}$ и $\mathbf{V}$ из временно́й и частотной областей (и обратно) описывается следующими формулами:

$$V_j = \sum_{i=0}^{n-1} v_i \alpha^{ij},\ j = 0, 1, \ldots, n-1;$$
$$v_i = \sum_{j=0}^{n-1} V_j \alpha^{-ij},\ i = 0, 1, \ldots, n-1.$$

Представим векторы $\mathbf{v}$ и $\mathbf{V}$ многочленами:

$$\mathbf{v}(x) = v_0 + v_1 x + \cdots + v_{n-1} x^{n-1};$$

$$\mathbf{V}(x) = V_0 + V_1 x + \cdots + V_{n-1} x^{n-1}.$$

Многочлен $\mathbf{V}(x)$ называют фурье-образом многочлена $\mathbf{v}(x)$, если вектор его коэффициентов $\mathbf{V}$ является фурье-образом вектора коэффициентов $\mathbf{v}$. Тогда коэффициенты прямого и обратного ДПФ можно вычислять как значения многочленов:

$$V_j = v_0 + v_1 \alpha^j + \cdots + v_{n-1} (\alpha^j)^{n-1} = \mathbf{v}(\alpha^j),$$

$$v_i = V_0 + V_1 \alpha^{-i} + \cdots + V_{n-1} (\alpha^{-i})^{n-1} = \mathbf{V}(\alpha^{-i}).$$

Из этого представления следует, что j-я фурье-компонента равна нулю, то есть $V_j = 0$, если α^j является корнем временно́го многочлена $\mathbf{v}(x)$, то есть $\mathbf{v}(\alpha^j) = 0$. В свою очередь, i-я временна́я компонента равна нулю, то есть $v_i = 0$, если $\alpha^{-i} = \alpha^{n-i}$ является корнем частотного многочлена $\mathbf{V}(x)$, то есть $\mathbf{V}(\alpha^{-i}) = \mathbf{V}(\alpha^{n-i}) = 0$.

5.2.1. Циклическая свертка и произведение Адамара

Пусть заданы многочлены $\mathbf{u}(x) = \sum\limits_{i=0}^{n-1} u_i x^i$ и $\mathbf{g}(x) = \sum\limits_{i=0}^{n-1} g_i x^i$.

Обозначим $\mathbf{U}(x)$ и $\mathbf{G}(x)$ их фурье-образы.

Циклической сверткой многочленов называется многочлен

$$\mathbf{c}(x) = \mathbf{u}(x)\mathbf{g}(x) \mod (x^n - 1).$$

Произведением Адамара двух многочленов называется многочлен

$$\mathbf{C}(x) = \mathbf{U}(x) \boxtimes \mathbf{G}(x) = \sum_{i=0}^{n-1} U_i G_i x^i.$$

5.2.2. Дискретное преобразование Фурье для свертки

Найдем прямое дискретное преобразование Фурье циклической свертки многочленов $\mathbf{u}(x)$ и $\mathbf{g}(x)$. По определению имеем

$$\mathbf{c}(x) = \mathbf{u}(x)\mathbf{g}(x) \mod (x^n - 1) = \sum_{i=0}^{n-1} c_i x^i,$$

где

$$c_i = \sum_{s=0}^{n-1} u_s g_{i-s};\ i = 0, 1, \ldots, n-1,$$

а отрицательные индексы приводятся по модулю n: $g_{-k} = g_{n-k}$. Для $j = 0, 1, \ldots, n-1$ соответствующие фурье-компоненты C_j равны

$$\begin{aligned} C_j &= \sum_{i=0}^{n-1} c_i \alpha^{ij} = \sum_{i=0}^{n-1} \sum_{s=0}^{n-1} u_s g_{i-s} \alpha^{ij} = \\ &= \sum_{s=0}^{n-1} u_s \sum_{i=0}^{n-1} g_{i-s} \alpha^{ij} = \\ &= \left(\sum_{s=0}^{n-1} u_s \alpha^{sj} \right) \left(\sum_{i=0}^{n-1} g_{i-s} \alpha^{(i-s)j} \right) = \\ &= \left(\sum_{s=0}^{n-1} u_s \alpha^{sj} \right) \left(\sum_{k=0}^{n-1} g_k \alpha^{kj} \right). \end{aligned}$$

Заметим, что $\left(\sum\limits_{s=0}^{n-1} u_s\alpha^{sj}\right) = U_j$ — это j-я компонента U_j фурье-образа $\mathbf{U}(x)$ многочлена $\mathbf{u}(x)$, а $\left(\sum\limits_{k=0}^{n-1} g_k\alpha^{kj}\right)$ — это j-я компонента G_j фурье-образа $\mathbf{G}(x)$ многочлена $\mathbf{g}(x)$.

Таким образом, фурье-компоненты свертки двух многочленов равны произведению фурье-компонент этих многочленов. Другими словами, фурье-образ свертки равен произведению Адамара фурье-образов многочленов. Запишем это соотношение в следующем виде:

$$\mathbf{c}(x) = \mathbf{u}(x)\mathbf{g}(x) \mod x^n - 1 \overset{\text{ПДПФ } F}{\Longrightarrow} \mathbf{C}(x) = \mathbf{U}(x) \boxtimes \mathbf{G}(x).$$

Здесь сокращение ПДПФ означает «Прямое дискретное преобразование Фурье». Аналогично для обратного преобразования (ОДПФ) имеем:

$$\mathbf{C}(x) = \mathbf{U}(x) \boxtimes \mathbf{G}(x) \overset{\text{ОДПФ } W}{\Longrightarrow} \mathbf{c}(x) = \mathbf{u}(x)\mathbf{g}(x) \mod x^n - 1.$$

5.3. Кодирование кодов Рида–Соломона

Пусть $k = n - d + 1,\ n = 2^m - 1$. Рассмотрим множество из $(2^m)^k = 2^{mk}$ векторов вида

$$\mathbf{v} = [v_0\ v_1\ \ldots\ v_{k-1}\ \underbrace{0\ 0\ \ldots\ 0}_{n-k}].$$

Первые k координат вектора можно интерпретировать как информационные символы.

Применим к каждому вектору прямое ДПФ:

$$\mathbf{V} = \mathbf{v} \cdot \mathbf{F} = [V_0,\ V_1,\ \ldots,\ V_{k-1},\ V_k,\ V_{k+1},\ \ldots,\ V_{n-1}].$$

Векторы $\mathbf{V}$ образуют циклический код Рида–Соломона над полем $GF(2^m)$. Действительно, покажем, что любой кодовый многочлен $\mathbf{V}(x)$ имеет корни $\alpha, \alpha^2, \ldots, \alpha^{d-2}, \alpha^{d-1}$. Так как $v_i = \mathbf{V}(\alpha^{-i}) = \mathbf{V}(\alpha^{n-i})$ и для $i = k, k+1 \ldots, n-1$, имеем по определению $v_i = 0$, то

$$\begin{aligned}
&\mathbf{V}(\alpha) = \mathbf{V}(\alpha^{-(n-1)}) = v_{n-1} = 0,\\
&\mathbf{V}(\alpha^2) = \mathbf{V}(\alpha^{-(n-2)}) = v_{n-2} = 0,\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
&\mathbf{V}(\alpha^{(d-2)}) = \mathbf{V}(\alpha^{n-(d-2)}) = v_{n-d+2} = v_{k+1} = 0,\\
&\mathbf{V}(\alpha^{(d-1)}) = \mathbf{V}(\alpha^{n-(d-1)}) = v_{n-d+1} = v_k = 0.
\end{aligned}$$

Параметры этого кода: длина $n = 2^m - 1$, число 2^m-ичных информационных символов k, кодовое расстояние d. Код является кодом МДР и может исправлять вплоть до $t = \lfloor \frac{d-1}{2} \rfloor$ символьных ошибок.

5.4. Декодирование кодов Рида–Соломона

В этом разделе описан алгоритм исправления символьных ошибок. Передается кодовый вектор $\mathbf{V}$. Принят вектор $\mathbf{Y} = \mathbf{V} + \mathbf{E}$, где

$$\mathbf{E} = [E_0,\ E_1,\ \ldots,\ E_{n-1}].$$

Ошибки в количестве s произошли в позициях $j_1, j_2, \ldots, j_s$. Число s и позиции j декодеру *неизвестны*.

Декодер применяет обратное ДПФ к вектору $\mathbf{Y}$, то есть вычисляет $\mathbf{y} = \mathbf{YW}$:

$$\begin{aligned}\mathbf{y} = \mathbf{YW} = (\mathbf{V} + \mathbf{E})\mathbf{W} = \mathbf{v} + \mathbf{e} = \\ = [v_0 + e_0,\ \ldots,\ v_{k-1} + e_{k-1},\ \underbrace{e_k,\ e_{k+1},\ \ldots,\ e_{n-1}}_{n-k}].\end{aligned}$$

Определим во временно́й области многочлен локаторов ошибок:

$$\sigma(x) = (\alpha^{-j_1}x - 1)(\alpha^{-j_2}x - 1)\cdots(\alpha^{-j_s}x - 1) = \sigma_0 + \sigma_1 x + \cdots + \sigma_s x^s.$$

Здесь $\sigma_0 = 1$.

Вектор $\mathbf{S}$ прямого ДПФ от $\sigma(x)$ имеет нулевые значения в позициях $j_1, j_2, \ldots, j_s$. Следовательно,

$$\mathbf{S} \boxtimes \mathbf{E} = [0\ 0\ \ldots\ 0].$$

Применим обратное ДПФ к обеим частям равенства. В левой части получим циклическую свертку $\mathbf{c}(x)$ многочленов $\sigma(x)$ и $\mathbf{e}(x)$, а в правой части — нулевой вектор:

$$\mathbf{c}(x) = \sigma(x)\mathbf{e}(x)\ \mod x^n - 1 = [0,\ 0,\ \ldots,\ 0].$$

Коэффициенты свертки выражаются формулой

$$c_j = \sum_{i=0}^{s} \sigma_i e_{j-i}, \quad j = 0, 1, \ldots, n-1.$$

В многочлене $\mathbf{e}(x)$ декодеру известны $n-k$ старших коэффициентов $e_k, e_{k+1}, \ldots, e_{n-1}$. Предположим, что число s ошибок известно. Выберем коэффициенты $c_{k+s}, c_{k+s+1}, \ldots, c_{n-1}$. Получим систему из $n-k-s$ линейных уравнений относительно s неизвестных $\sigma_1, \sigma_2, \ldots, \sigma_s$:

$$\begin{array}{l} c_{k+s} = \sigma_0 e_{k+s} + \sigma_1 e_{k+s-1} + \sigma_2 e_{k+s-2} + \cdots + \sigma_s e_k = 0; \\ c_{k+s+1} = \sigma_0 e_{k+s+1} + \sigma_1 e_{k+s} + \sigma_2 e_{k+s-1} + \cdots + \sigma_s e_{k+1} = 0; \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ c_{n-1} = \sigma_0 e_{n-1} + \sigma_1 e_{n-2} + \sigma_2 e_{n-3} + \cdots + \sigma_s e_{n-1-s} = 0. \end{array} \tag{5.3}$$

Система имеет единственное решение, если $s \le n-k-s$, то есть если $s \le \frac{n-k}{2} = t$.

Найдя $\sigma_1, \sigma_2, \ldots, \sigma_s$, рекуррентно находим $e_{k-1}, e_{k-2}, \ldots, e_0$, например:

$$c_{k+s-1} = \sigma_0 e_{k+s-1} + \sigma_1 e_{k+s-2} + \sigma_2 e_{k+s-3} + \cdots + \sigma_{s-1} e_k + \sigma_s e_{k-1} = 0.$$

Здесь все величины известны, кроме e_{k-1}. Находим e_{k-1}. Далее:

$$c_{k+s-2} = \sigma_0 e_{k+s-2} + \sigma_1 e_{k+s-3} + \sigma_2 e_{k+s-4} + \cdots + \sigma_{s-1} e_{k-1} + \sigma_s e_{k-2} = 0.$$

Здесь все величины известны, кроме e_{k-2}. Находим e_{k-2}. Продолжаем, пока не найдем все величины $e_{k-1}, e_{k-2}, \ldots, e_0$. Вычитаем их из первых k координат вектора $\mathbf{y}$ и находим информационный вектор:

$$\mathbf{v} = [v_0\ v_1\ \ldots\ v_{k-1}\ 0\ 0\ \ldots\ 0].$$

5.4.1. Пять шагов декодирования кодов Рида–Соломона

Шаг 1. Применить к принятому вектору $\mathbf{Y} = \mathbf{V} + \mathbf{E}$ обратное дискретное преобразование Фурье, получить вектор $\mathbf{y} = \mathbf{v} + \mathbf{e}$, найти из него последние $n-k$ координат $e_k,\ e_{k+1},\ \ldots,\ e_{n-1}$.

Шаг 2. Задавшись числом предполагаемых ошибок $s \le t = \frac{d-1}{2}$, найти из системы (5.3) коэффициенты $\sigma_0 = 1$, σ_1, σ_2, $\ldots$, σ_s.

Шаг 3. С их помощью из рекуррентного по j соотношения

$$c_{k+s-j} = \sigma_0 e_{k+s-j} + \sigma_1 e_{k+s-j-1} + \cdots + \sigma_{s-1} e_{k-j+1} + \sigma_s e_{k-j} = 0.$$

найти координаты e_{k-j}, $j = 1, 2, \ldots, k$. Найти вектор

$$\mathbf{e} = [e_0\ e_1\ e_2\ \ldots\ e_{n-1}].$$

Шаг 4. Вычислить информационный вектор $\mathbf{v} = \mathbf{y} - \mathbf{e}$.

Шаг 5. Контроль правильности декодирования. Вычислить прямое дискретное преобразование Фурье $\mathbf{V}'$ найденного вектора $\mathbf{v}$. Вычесть вектор $\mathbf{V}'$ из принятого вектора $\mathbf{Y}$. Если в разности $\mathbf{Y} - \mathbf{V}'$ число ненулевых координат совпадает с s, то декодирование правильное.

5.4.2. Пример: исправление одиночных ошибок

Предположим, что $s = 1$. Система (5.3) относительно неизвестной σ_1 приобретает вид:

$$\begin{aligned}
&\sigma_1 e_k = e_{k+1}\\
&\sigma_1 e_{k+1} = e_{k+2}\\
&\cdots\cdots\cdots\\
&\sigma_1 e_{n-2} = e_{n-1}.
\end{aligned}$$

Решение существует и будет единственным, если выполняются условия

$$\sigma_1 = \frac{e_{k+1}}{e_k} = \frac{e_{k+2}}{e_{k+1}} = \cdots = \frac{e_{n-1}}{e_{n-2}}.$$

В этом случае неизвестные координаты вектора $\mathbf{e}$ вычисляются рекуррентно:

$$e_{k-1} = \frac{e_k}{\sigma_1},\ e_{k-2} = \frac{e_{k-1}}{\sigma_1} = \frac{e_k}{\sigma_1^2},\ \cdots,\ e_0 = \frac{e_1}{\sigma_1} = \frac{e_k}{\sigma_1^k}.$$

5.4.3. Пример: исправление двойных ошибок

Предположим, что $s = 2$. Система (5.3) относительно неизвестных σ_1 и σ_2 приобретает вид:

$$\begin{aligned}
&\sigma_1 e_{k+1} + \sigma_2 e_k = e_{k+2}\\
&\sigma_1 e_{k+2} + \sigma_2 e_{k+1} = e_{k+3}\\
&\cdots\cdots\cdots\cdots\cdots\\
&\sigma_1 e_{n-2} + \sigma_2 e_{n-3} = e_{n-1}.
\end{aligned}$$

Система имеет единственное решение, если матрицы

$$\begin{bmatrix} e_{k+1} & e_{k+2} & \cdots & e_{n-2} \\ e_k & e_{k+1} & \cdots & e_{n-3} \end{bmatrix} \text{ и } \begin{bmatrix} e_{k+2} & e_{k+3} & \cdots & e_{n-1} \\ e_{k+1} & e_{k+2} & \cdots & e_{n-2} \\ e_k & e_{k+1} & \cdots & e_{n-3} \end{bmatrix} \tag{5.4}$$

имеют одинаковый ранг, равный 2. Найдя решение σ_1 и σ_2, переходим к рекуррентному соотношению

$$\sigma_2 e_{k-j} = -\sigma_1 e_{k+1-j} - e_{k+2-j}, \quad j = 1, 2, \ldots, k,$$

из которого последовательно находим $e_{k-1}, e_{k-2}, \ldots, e_0$.

Если ранги матриц (5.4) различны, то система не имеет решения. Число ошибок больше 2. Выносится решение «отказ от декодирования».

Если ранги одинаковы и равны 1, то произошла одиночная ошибка. Следует перейти к другой системе, соответствующей этому случаю.

Г л а в а 6

Ранговые коды

6.1. Ранговая метрика

Пусть $GF(q)$ — конечное поле из q элементов, называемое *основным полем*.

Выберем неприводимый примитивный многочлен с коэффициентами из $GF(q)$:

$$\varphi(x) = x^m + \varphi_0 x^{m-1} + \cdots + \varphi_1 x + \varphi_0.$$

Обозначим через α корень этого многочлена. Степени этого корня порождают *расширенное поле* $GF(q^m)$, элементами которого являются $\{0, \alpha, \alpha^2, \ldots, \alpha^{q^m-1}\}$. Расширенное поле $GF(q^m)$ можно рассматривать как m-мерное векторное пространство над полем $GF(q)$ (см. гл. 1). Базис расширенного поля состоит из m элементов, линейно независимых над полем $GF(q)$. Например, базисом являются элементы $\{1, \alpha, \ldots, \alpha^{m-1}\}$, линейно независимые над $GF(q)$. Все остальные элементы расширенного поля является их линейными комбинациями с коэффициентами из основного поля $GF(q)$:

$$\alpha^j = v_{0,j} \cdot 1 + v_{1,j} \cdot \alpha + \cdots + v_{m-1,j} \cdot \alpha^{m-1},\ v_{i,j} \in GF(q).$$

Существует взаимно однозначное соответствие между элементами расширенного поля и вектор-столбцами размера m с координатами из основного поля:

$$\alpha^j \Longleftrightarrow \begin{bmatrix} v_{0,j} \\ v_{1,j} \\ \vdots \\ v_{m-1,j} \end{bmatrix}.$$

Существует много различных базисов.

Основное и расширенное поля используют для построения различных пространств и кодов на их основе.

Пространство матриц над основным полем. Линейное пространство матриц над полем $GF(q)$ с размерами $m \times n$ обозначается $GF(q)^{m\times n}$. Оно состоит из матриц

$$M = \begin{bmatrix} v_{0,0} & v_{0,1} & \cdots & v_{0,n-1} \\ v_{1,0} & v_{1,1} & \cdots & v_{1,n-1} \\ \vdots & \vdots & \cdots & \vdots \\ v_{m-1,0} & v_{m-1,1} & \cdots & v_{m-1,n-1} \end{bmatrix}, \quad v_{i,j} \in GF(q).$$

Матрицу можно умножать на скаляр (элемент $GF(q)$). Матрицы одинаковых размеров можно складывать и вычитать.

Ранг матрицы $\mathrm{Rk}(M)$ определяется как максимальное число *линейно независимых* над $GF(q)$ строк (или столбцов).

Пространство можно сделать нормированным, если ввести подходящую функцию нормы.

Ранговая норма матрицы (или *ранговый вес* матрицы) определяется как ее ранг:

$$N(M) = \mathrm{Rk}(M).$$

Эта функция удовлетворяет всем аксиомам нормы
1. $N(M) \geq 0 \quad \forall M \in GF(q)^{m\times n}$.
2. $N(M) = 0 \Leftrightarrow M = 0$.
3. $N(M_1 + M_2) \leq N(A) + N(B)$ неравенство треугольника.

Ранговое расстояние между матрицами M_1 и M_2 определяется как ранг их разности:

$$d(M_1, M_2) = N(M_1 - M_2) = \mathrm{Rk}(M_1 - M_2).$$

Векторное пространство над расширенным полем. Линейное пространство векторов размерности n над расширенным полем $GF(q^m)$ обозначается $GF(q^m)^n$. Оно состоит из векторов с координатами из расширенного поля:

$$\mathbf{v} = \begin{bmatrix} v_0 & v_1 & \ldots & v_{n-1} \end{bmatrix}, \quad v_j \in GF(q^m).$$

Вектор можно умножать на скаляр (элемент $GF(q^m)$). Векторы одинаковых размеров можно складывать и вычитать.

Ранг вектора $\mathbf{v}$ определяется как *максимальное число линейно независимых* над основным полем $GF(q)$ координат вектора.

Отобразим вектор $\mathbf{v}$ в матрицу $M(\mathbf{v}) = [v_{i,j}]$, заменив каждую координату v_j столбцом ее коэффициентов в некотором базисе.

Ранг вектора $\mathbf{v}$ эквивалентно определяется как ранг соответствующей ему матрицы $M(\mathbf{v}) = [v_{i,j}]$.

Ранговая норма вектора (или *ранговый вес* вектора) определяется как его ранг: $N(\mathbf{v}) = \mathrm{Rk}(M(\mathbf{v}))$.

Ранговое расстояние между векторами $\mathbf{v_1}$ и $\mathbf{v_2}$ определяется как ранговый вес их разности:

$$d(\mathbf{a}, \mathbf{b}) = N(\mathbf{a} - \mathbf{b}) = \mathrm{Rk}(A(\mathbf{a}) - B(\mathbf{b})).$$

6.2. Коды в ранговой метрике

6.2.1. Матричные ранговые коды

Матричным ранговым кодом $\mathcal{M}$ называется любой набор матриц из пространства матриц $GF(q)^{m \times n}$.

Ранговым расстоянием d матричного кода $\mathcal{M}$ называется *наименьший ранг* попарных разностей кодовых матриц:

$$d = \min_{M_1 \neq M_2} \mathrm{Rk}(M_1 - M_2), \quad M_1, M_2 \in \mathcal{M}.$$

6.2.2. Векторные ранговые коды

Векторным ранговым кодом $\mathcal{V}$ называется любой набор векторов из векторного пространства $GF(q^m)^n$.

Ранговым расстоянием d векторного кода $\mathcal{V}$ называется *наименьший ранг* попарных разностей кодовых векторов:

$$d = \min_{v_1 \neq v_2} \mathrm{Rk}(v_1 - v_2), \quad v_1, v_2 \in \mathcal{V}.$$

6.2.3. Эквивалентность матричных и векторных ранговых кодов

Любой *матричный код* $\mathcal{M}$ может быть преобразован в *векторный код* $\mathcal{V}$ той же мощности и с тем же кодовым расстоянием d. Для этого каждый столбец кодовой матрицы следует заменить на соответствующий элемент расширенного поля.

Любой *векторный код* $\mathcal{V}$ может быть преобразован в *матричный код* $\mathcal{M}$ той же мощности и с тем же кодовым расстоянием d. Для этого

каждую координату кодового вектора следует заменить на соответствующий столбец из элементов основного поля.

Векторное представление удобнее использовать для описания конструкций ранговых кодов и быстрых алгоритмов их декодирования.

Матричное представление полезно в практических приложениях, например, в теории многоканальной связи, в теории пространственно-временных кодов или в теории сетевого кодирования.

6.3. Граница Синглтона для минимального расстояния ранговых кодов

Вывод границы для матричных кодов $\mathcal{M}$ размера $m \times n$. Пусть задано кодовое расстояние d, размер кодовых матриц $m \times n$, $m \geq n$, число кодовых матриц L. Представим каждую кодовую матрицу C в виде $\begin{bmatrix} A & B \end{bmatrix}$, где A – подматрица размера $m \times (d-1)$, а B – подматрица размера $m \times (n-d+1)$. Выпишем все кодовые матрицы:

$$\mathcal{M} = \left\{ C_1 = \begin{bmatrix} A_1 & B_1 \end{bmatrix}, C_2 = \begin{bmatrix} A_2 & B_2 \end{bmatrix}, \ldots, C_M = \begin{bmatrix} A_L & B_L \end{bmatrix} \right\}.$$

Матрицы B_j должны быть попарно различны. Если $B_1 = B_2$, то

$$d(C_1, C_2) = \mathrm{Rk}(C_1 - C_2) = \mathrm{Rk}([A_1 - A_2 \;\; 0]) = \mathrm{Rk}(A_1 - A_2) \leq d - 1,$$

а должно быть $d(C_1, C_2) \geq d$.

Число *различных* матриц размера $m \times (n-d+1)$ равно $q^{m(n-d+1)}$. Получаем границу Синглтона $L \leq q^{m(n-d+1)}$.

6.4. Линейные векторные ранговые коды

Линейный векторный ранговый $[n, k, d]$-код над $GF(q^m)$ — это k-мерное подпространство пространства векторов $GF(q^m)^n$ с ранговым расстоянием d. Число векторов в k-мерном подпространстве равно q^{mk}.

Из границы Синглтона следует

$$k \leq n - d + 1.$$

Если достигается знак равенства, то код называется кодом с *максимальным ранговым расстоянием* (MRP-кодом).

Линейный код задается порождающей матрицей G размера $k \times n$ и ранга k либо проверочной матрицей H размера $(n-k) \times n$ и ранга $n-k$ такой, что

$$GH^\top = 0.$$

Выясним условия, которым должны удовлетворять элементы проверочной матрицы.

6.4.1. Проверочная матрица рангового кода

Проверочная матрица H задает код с ранговым расстоянием, не меньшим d, если выполняются условия: для любой матрицы Y над основным полем $GF(q)$ размера $(d-1)\times n$ и ранга $d-1$ выполняется условие

$$\mathrm{Rk}(YH^\top) = d-1.$$

По определению, любой вектор $\mathbf{u}$ ранга $d-1$ не может быть кодовым. Вектор $\mathbf{u}$ всегда может быть представлен в виде

$$\mathbf{u} = [u_1\ u_2\ \ldots\ u_{d-1}]Y,$$

где u_i линейно независимы над $GF(q)$, а Y является матрицей над $GF(q)$ размера $(d-1)\times n$ и ранга $d-1$. Произведение

$$\mathbf{u}H^\top = [u_1\ u_2\ \ldots\ u_{d-1}]YH^\top$$

может равняться нулю для ненулевых u_i, только если $\mathrm{Rk}(YH^\top) < d-1$. У нас $\mathrm{Rk}(YH^\top) = d-1$.

6.4.2. Конструкции векторных ранговых МРР-кодов

Рассмотрим матрицу H_{d-1} размера $(d-1)\times n$ следующего вида:

$$H_{d-1} = \begin{bmatrix} h_1 & h_2 & \ldots & h_n \\ h_1^q & h_2^q & \ldots & h_n^q \\ h_1^{q^2} & h_2^{q^2} & \ldots & h_n^{q^2} \\ \ldots & \ldots & \ldots & \ldots \\ h_1^{q^{d-2}} & h_2^{q^{d-2}} & \ldots & h_n^{q^{d-2}} \end{bmatrix},$$

где элементы $h_1, h_2, \ldots, h_n$ из расширенного поля $GF(q^m)$ линейно независимы над $GF(q)$.

Эта матрица удовлетворяет указанным выше условиям:

$$YH_{d-1}^\top = \begin{bmatrix} f_1 & f_1^q & \ldots & f_1^{q^{d-2}} \\ f_2 & f_2^q & \ldots & f_2^{q^{d-2}} \\ f_3 & f_3^q & \ldots & f_3^{q^{d-2}} \\ \ldots & \ldots & \ldots & \ldots \\ f_{d-1} & f_{d-1}^q & \ldots & f_{d-1}^{q^{d-2}} \end{bmatrix},$$

где

$$\begin{bmatrix} f_1 & f_2 & f_3 & \dots & f_{d-1} \end{bmatrix} = \begin{bmatrix} h_1 & h_2 & h_3 & \dots & h_n \end{bmatrix} Y^{\top}.$$

Элементы f_i линейно независимы над $GF(q)$, поэтому матрица невырождена и имеет ранг $d-1$.

6.4.3. Порождающая матрица MPP-кода

Указанной проверочной матрице соответствует порождающая матрица вида

$$G_k = \begin{bmatrix} g_1 & g_2 & \cdots & g_n \\ g_1^q & g_2^q & \cdots & g_n^q \\ g_1^{q^2} & g_2^{q^2} & \cdots & g_n^{q^2} \\ \cdots & \cdots & \cdots & \cdots \\ g_1^{q^{k-1}} & g_2^{q^{k-1}} & \cdots & g_n^{q^{k-1}} \end{bmatrix},$$

где элементы $g_1, g_2, \dots, g_n$ из $GF(q^m)$ линейно независимы над $GF(q)$.

Параметры $[n, k, d]$ MPP-кодов

1. Алфавит — расширенное поле $GF(q^m)$.

2. Длина кодового вектора — n. Размер соответствующей кодовой матрицы – $m \times n$, где $m \geq n$.

3. Число кодовых векторов или кодовых матриц — q^{mk}.

4. Кодовое расстояние $d = n - k + 1$.

5. Код позволяет исправлять ошибки, ранг которых равен или меньше $t = \frac{d-1}{2}$.

6.5. Линеаризованные многочлены

Многочлен

$$F(x) = \sum_{i=0}^{n} F_i x^{q^i}$$

называется линеаризованным многочленом над расширенным полем $GF(q^m)$, если все коэффициенты F_i лежат в этом поле. Если коэффициенты $\alpha, \beta \in GF(q)$, то $(\alpha x_1 + \beta x_2)^q = \alpha x_1^q + \beta x_2^q$, то есть

$$F(\alpha x_1 + \beta x_2) = \alpha F(x_1) + \beta F(x_2).$$

Сложение — обычное.

Умножение — композиция:

$$F(z) \star G(z) = F(G(z)).$$

Результатом умножения двух линеаризованных многочленов является линеаризованный многочлен.

Имеем некоммутативное кольцо с многочленом z в качестве единичного элемента по умножению.

Корни линеаризованных многочленов. Пусть

$$\sigma(x) = \sum_{i=0}^{r} \sigma_i x^{q^i}$$

— линеаризованный многочлен над $GF(q^m)$. Пусть x_1 и x_2 — линейно независимые над $GF(q)$ корни этого многочлена:

$$\sigma(x_1) = 0; \qquad \sigma(x_2) = 0.$$

Тогда для любых $\alpha, \beta \in GF(q)$ линейная комбинация $\alpha x_1 + \beta x_2$ — также корень этого многочлена:

$$\sigma(\alpha x_1 + \beta x_2) = \alpha\sigma(x_1) + \beta\sigma(x_2) = 0.$$

В общем случае, если $\{x_1, x_2, \ldots, x_k\}$ линейно независимые корни $\sigma(x)$, то все линейные комбинации этих корней также являются корнями $\sigma(x)$.

6.6. Кодирование МРР-кодов

Простое несистематическое кодирование. Вектор информационных символов

$$\mathbf{u} = \begin{bmatrix} u_0 & u_1 & \ldots & u_{k-1} \end{bmatrix}, \quad u_i \in GF(q^m),$$

отображается в информационный линеаризованный многочлен

$$\mathbf{U}(x) = \sum_{i=0}^{k-1} u_i x^{q^i}.$$

Кодовый вектор $\mathbf{v}(\mathbf{u})$, соответствующий вектору $\mathbf{u}$, вычисляется как

$$\mathbf{v}(\mathbf{u}) = \mathbf{u}G_k = \begin{bmatrix} \mathbf{U}(g_1) & \mathbf{U}(g_2) & \ldots & \mathbf{U}(g_n) \end{bmatrix} = \begin{bmatrix} v_0 & v_1 & \ldots & v_{n-1} \end{bmatrix}..$$

Кодирование сводится к вычислению значений линеаризованного информационного многочлена $\mathbf{U}(x)$ в заранее заданных точках $\{g_1, g_2, \ldots, g_n\}$.

6.7. Декодирование МРР-кодов

Пусть передавался кодовый вектор $\mathbf{v} = \begin{bmatrix} v_0 & v_1 & \dots & v_{n-1} \end{bmatrix}$. Принят вектор $\mathbf{y} = \mathbf{v} + \mathbf{e}$, где

$$\mathbf{e} = [e_0 \; e_1 \; \dots \; e_{n-1}]$$

— вектор ошибки. По построению кодовый вектор $\mathbf{v}$ удовлетворяет условию $\mathbf{v}H_{d-1}^{\top} = \mathbf{0}$. Декодирование начинается с вычисления вектора синдрома:

$$\mathbf{s} = \mathbf{y}H_{d-1}^{\top} = \mathbf{e}H_{d-1}^{\top} = \begin{bmatrix} s_0 & s_1 & \dots & s_{d-2} \end{bmatrix}.$$

Задача декодера — по известному вектору $\mathbf{s}$ найти вектор ошибки $\mathbf{e}$, а затем — передававшийся вектор $\mathbf{v}$.

Преобразование уравнений. Предположим, что ранговая норма ошибки $\mathbf{e}$ равна r. Тогда вектор ошибки можно представить в виде

$$\mathbf{e} = \begin{bmatrix} e_1 & e_2 & \dots & e_r \end{bmatrix} Y,$$

где элементы $\{e_1, e_2, \dots, e_r\}$ линейно независимы над основным полем $GF(q)$, а Y — $(r \times n)$-матрица с элементами из $GF(q)$ ранга r.

Проведем замену переменных:

$$\mathbf{s}^{\top} = H_{d-1}Y^{\top} \begin{bmatrix} e_1 & e_2 & \dots & e_r \end{bmatrix}^{\top} = X \begin{bmatrix} e_1 & e_2 & \dots & e_r \end{bmatrix}^{\top},$$

где

$$X = \begin{bmatrix} x_1 & x_2 & \dots & x_r \\ x_1^{q^1} & x_2^{q^1} & \dots & x_r^{q^1} \\ \dots & \dots & \dots & \dots \\ x_1^{q^d-2} & x_2^{q^d-2} & \dots & x_r^{q^d-2} \end{bmatrix},$$

$$\mathbf{x} = \begin{bmatrix} x_1 & x_2 & \dots & x_r \end{bmatrix} = \begin{bmatrix} h_1 & h_2 & \dots & h_n \end{bmatrix} Y^{\top}.$$

В координатной записи получена система из $d-1$ нелинейных уравнений

$$\sum_{j=1}^{r} e_j x_j^{q^p} = s_p, \quad p = 0, 1, \dots, d-2,$$

относительно $2r$ неизвестных

$$\{e_1, e_2, \dots, e_r; x_1, x_2, \dots, x_r\}.$$

6.7.1. Пример 1: ошибка ранга 1

Пусть $d = 3$. Пусть

$$H_2 = \begin{bmatrix} h_1 & h_2 & \dots & h_n \\ h_1^q & h_2^q & \dots & h_n^q \end{bmatrix}.$$

Ошибка ранга 1 имеет вид

$$\mathbf{e} = e_1 \begin{bmatrix} y_1 & y_2 & \dots & y_n \end{bmatrix} = e_1 Y,$$

где $e_1 \in GF(q^m)$, $y_i \in GF(q)$. Вычислим синдром

$$\mathbf{s} = \mathbf{e} H_2^\top = e_1 \begin{bmatrix} h_1 y_1 + \dots + h_n y_n & h_1^q y_1 + \dots + h_n^q y_n \end{bmatrix} = e_1 [x_1 \ x_1^q].$$

Получаем систему

$$s_0 = e_1 x_1,$$

$$s_1 = e_1 x_1^q.$$

Дальнейшие преобразования системы уравнений. Система из $d-1$ нелинейных уравнений

$$\sum_{j=1}^{r} e_j x_j^{[p]} = s_p, \quad p = 0, 1, \dots, d-2, \tag{6.1}$$

относительно $2r$ неизвестных $\{e_1, e_2, \dots, e_r\}$ и $\{x_1, x_2, \dots, x_r\}$, где $\{e_i\}$ линейно независимы над $GF(q)$ и $\{x_i\}$ линейно независимы над $GF(q)$.

Идея решения

1. Ввести линеаризованный многочлен над $GF(q^m)$

$$\sigma(x) = \sum_{i=0}^{r} \sigma_i x^{q^i} = \sigma_0 x + \sigma_1 x^q + \dots + \sigma_{r-1} x^{q^{r-1}} + x^{q^r}$$

такой, что $\sigma(x_1) = 0$, $\sigma(x_2) = 0, \dots,$ $\sigma(x_r) = 0$. Коэффициенты σ_i неизвестны.

2. Преобразовать исходную систему в систему относительно σ_i. Решить полученную систему.

3. Найти линейно независимые корни $\{x_1, x_2, \dots, x_r\}$ многочлена $\sigma(x)$.

4. Подставить их в систему (6.1) и найти $\{e_i\}$.

5. Найти $\mathbf{e}$ и $\mathbf{v}$.

6.7.2. Пример 2: ошибка ранга 2

Пусть $d = 5, r = 2$. Система (6.1) имеет вид

$$\begin{aligned} e_1 x_1 + e_2 x_2 &= s_0, \\ e_1 x_1^q + e_2 x_2^q &= s_1, \\ e_1 x_1^{q^2} + e_2 x_2^{q^2} &= s_2, \\ e_1 x_1^{q^3} + e_2 x_2^{q^3} &= s_3. \end{aligned} \tag{6.2}$$

Вводим многочлен $\boldsymbol{\sigma}(x) = \sigma_0 x + \sigma_1 x^q + x^{q^2}$ с неизвестными коэффициентами. Используем условие: $\boldsymbol{\sigma}(x_1) = 0,\ \boldsymbol{\sigma}(x_2) = 0$. Преобразуем систему (6.2) в систему относительно σ_0 и σ_1.

Первый шаг. Умножим 1-е уравнение на σ_0, 2-е — на σ_1, 3-е — на 1 и суммируем:

$$\begin{aligned} e_1(\sigma_0 x_1 + \sigma_1 x_1^q + x_1^{q^2}) + e_2(\sigma_0 x_2 + \sigma_1 x_2^q + x_2^{q^2}) &= s_0\sigma_0 + s_1\sigma_1 + s_2, \\ e_1\boldsymbol{\sigma}(x_1) + e_2\boldsymbol{\sigma}(x_2) &= s_0\sigma_0 + s_1\sigma_1 + s_2, \\ 0 &= s_0\sigma_0 + s_1\sigma_1 + s_2. \end{aligned}$$

Получено уравнение относительно σ_0 и σ_1:

$$s_0\sigma_0 + s_1\sigma_1 = -s_2.$$

Второй шаг. Умножим 2-е уравнение на σ_0^q, 3-е — на σ_1^q, 4-е — на 1 и сложим:

$$\begin{aligned} e_1(\sigma_0^q x_1^q + \sigma_1^q x_1^{q^2} + x_1^{q^3}) + e_2(\sigma_0^q x_2^q + \sigma_1^q x_2^{q^2} + x_2^{q^3}) &= s_1\sigma_0^q + s_2\sigma_1^q + s_3, \\ e_1(\sigma_0 x_1 + \sigma_1 x_1^q + x_1^{q^2})^q + e_2(\sigma_0 x_2 + \sigma_1 x_2^q + x_2^{q^2})^q &= s_1\sigma_0^q + s_2\sigma_1^q + s_3, \\ e_1(\boldsymbol{\sigma}(x_1))^q + e_2(\boldsymbol{\sigma}(x_2))^q &= s_1\sigma_0^q + s_2\sigma_1^q + s_3, \\ 0 &= s_1\sigma_0^q + s_2\sigma_1^q + s_3. \end{aligned}$$

Получено уравнение относительно σ_0^q и σ_1^q:

$$s_1\sigma_0^q + s_2\sigma_1^q = -s_3.$$

Возводим в степень q^{m-1}, учитываем, что $\sigma_0^{q^m} = \sigma_0,\ \sigma_1^{q^m} = \sigma_1$:

$$s_1^{q^{m-1}}\sigma_0 + s_2^{q^{m-1}}\sigma_1 = -s_3^{q^{m-1}}.$$

Собираем оба уравнения, линейных относительно σ_0 и σ_1:

$$s_0\sigma_0 + s_1\sigma_1 = -s_2,$$

$$s_1^{q^{m-1}}\sigma_0 + s_2^{q^{m-1}}\sigma_1 = -s_3^{q^{m-1}}.$$

В матричном виде

$$[\sigma_0\ \sigma_1]\begin{bmatrix} s_0 & s_1^{q^{m-1}} \\ s_1 & s_2^{q^{m-1}} \end{bmatrix} = -[s_2\ s_3^{q^{m-1}}].$$

Находим решение $[\sigma_0\ \sigma_1]$. После этого находим линейно независимые решения x_1 и x_2 уравнения $\boldsymbol{\sigma}(x) = \sigma_0 x + \sigma_1 x^q + x^{q^2} = 0$. Затем из системы (6.2) находим неизвестные e_1 и e_2.

6.7.3. Общий случай

Предполагаем, что ранг ошибки равен $r \le \frac{(d-1)}{2}$. Вводим многочлен $\boldsymbol{\sigma}(x) = \sigma_0 x + \sigma_1 x^q + \cdots + \sigma_{r-1}x^{q^{r-1}} + x^{q^r}$ такой, что

$$\boldsymbol{\sigma}(x_1) = 0,\ \boldsymbol{\sigma}(x_2) = 0, \ldots,\ \boldsymbol{\sigma}(x_r) = 0.$$

Первый шаг. Умножим 1-е уравнение на σ_0, 2-е — на σ_1, ..., r-е — на σ_{r-1}, $(r+1)$-е — на 1 и суммируем. Получаем 1-е линейное уравнение относительно σ_i:

$$\sigma_0 s_0 + \sigma_1 s_1 + \sigma_2 s_2 + \cdots + \sigma_{r-1}s_{r-1} = -s_r.$$

Второй шаг. Умножим 2-е уравнение на σ_0^q, 3-е — на σ_1^q, ..., $(r+1)$-е — на σ_{r-1}^q, $(r+2)$-е — на 1 и суммируем. Возводим полученное уравнение в степень q^{m-1}. Получаем 2-е линейное уравнение относительно σ_i:

$$\sigma_0 s_1^{q^{m-1}} + \sigma_1 s_2^{q^{m-1}} + \sigma_2 s_3^{q^{m-1}} + \cdots + \sigma_{r-1}s_r^{q^{m-1}} = -s_{r+1}^{q^{m-1}}.$$

Третий шаг. Умножим 3-е уравнение на $\sigma_0^{q^2}$, 4-е — на $\sigma_1^{q^2}$, ..., $(r+2)$-е — на $\sigma_{r-1}^{q^2}$, $(r+3)$-е — на 1 и суммируем. Возводим полученное уравнение в степень q^{m-2}. Получаем 3-е линейное уравнение относительно σ_i:

$$\sigma_0 s_2^{q^{m-2}} + \sigma_1 s_3^{q^{m-2}} + \sigma_2 s_4^{q^{m-2}} + \cdots + \sigma_{r-1}s_{r+1}^{q^{m-2}} = -s_{r+2}^{q^{m-2}}.$$

...

Шаг $d-2-r$**.** Умножим $d-2-r$-е уравнение на $\sigma_0^{q^{d-3-r}}$, следующее уравнение — на $\sigma_1^{q^{d-3-r}}$, …, $(d-2)$-е — на $\sigma_{r-1}^{q^{d-3-r}}$, $(d-1)$-е — на 1 и суммируем. Возводим полученное уравнение в степень $q^{m-d+3+r}$. Получаем $(d-2-r)$-е линейное уравнение относительно σ_i:

$$\sigma_0 s_{d-2-r}^{q^{m-d+2+r}} + \sigma_1 s_{d-2-r+1}^{q^{m-d+2+r}} + \cdots + \sigma_{r-1} s_{d-2-r+r-1}^{q^{m-d+2+r}} = -s_{d-2-r+r}^{q^{m-d+2+r}}.$$

Эти уравнения в матричной форме имеют вид

$$\begin{bmatrix}\sigma_0 & \sigma_1 & \dots & \sigma_{r-1}\end{bmatrix} \begin{bmatrix} s_0 & s_1^{q^{m-1}} & \dots & s_{r-1}^{q^{m-r+1}} \\ s_1 & s_2^{q^{m-1}} & \dots & s_r^{q^{m-r+1}} \\ \vdots & \vdots & \vdots & \vdots \\ s_{r-1} & s_r^{q^{m-1}} & \dots & s_{2r-2}^{q^{m-r+1}} \end{bmatrix} =$$
$$= -\begin{bmatrix} s_r & s_{r+1}^{q^{m-1}} & \dots & s_{2r-1}^{q^{m-r+1}} \end{bmatrix}.$$

Решаем эту систему.

Находим линейно независимые корни многочлена

$$\boldsymbol{\sigma}(x) = \sigma_0 x + \sigma_1 x^q + \cdots + \sigma_{r-1} x^{q^{r-1}} + x^{q^r}.$$

Находим величины $e_1, e_2, \dots, e_r$.

Находим вектор ошибки $\mathbf{e}$ и кодовый вектор.

Г л а в а 7

Задачи и упражнения

7.1. Задачи к главе 1

Задача 1

1. Найти все подгруппы аддитивной группы кольца $\mathbb{Z}_{30}$ и указать, какие из них циклические и с каким порождающим элементом.
2. Найти максимальную группу по умножению кольца $\mathbb{Z}_{30}$ и все ее подгруппы.

Решение

1. Операцией *сложения* в аддитивной группе кольца $\mathbb{Z}_{30}$ является сложение по модулю 30. Группа является циклической и состоит из элементов $\{0, 1, 2, \ldots, 28, 29\}$ с порождающим элементом 1. Порядок группы равен 30. Порядки подгрупп равны делителям числа 30, то есть 1, 2, 3, 5, 6, 10, 15, 30. Подгруппа порядка 1 состоит из элемента 0. Подгруппа порядка 2 (циклическая с порождающим элементом 15) состоит из элементов $\{0, 15\}$. Подгруппа порядка 3 (циклическая с порождающим элементом 10) состоит из элементов $\{0, 10, 20\}$. Подгруппа порядка 5 (циклическая с порождающим элементом 6) состоит из элементов $\{0, 6, 12, 18, 24\}$. Подгруппа порядка 6 (циклическая с порождающим элементом 5) состоит из элементов $\{0, 5, 10, 15, 20, 25\}$. Подгруппа порядка 10 (циклическая с порождающим элементом 3) состоит из элементов $\{0, 3, 6, 9, 12, 15, 20, 25\}$. Подгруппа порядка 15 (циклическая с порождающим элементом 2) состоит из элементов $\{0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28\}$.
2. Операцией *умножения* в кольце $\mathbb{Z}_{30}$ является умножение по модулю 30. Максимальную группу по умножению образуют все элементы, взаимно простые с модулем 30. Это числа $\{1, 7, 11, 13, 17, 19, 23, 29\}$. Порядок группы равен 8. Группа не является циклической. Порядки подгрупп являются делителями числа 8, то есть $\{1, 2, 4, 8\}$. Подгруппа порядка 1 состоит из элемента 1. Существуют 3 различные подгруппы порядка 2. Это

циклическая подгруппа $\{1, 11\}$ с порождающим элементом 11; циклическая подгруппа $\{1, 19\}$ с порождающим элементом 19; циклическая подгруппа $\{1, 29\}$ с порождающим элементом 29. Существуют 3 различные подгруппы порядка 4. Это циклическая подгруппа $\{1, 7, 19, 13\}$ с порождающим элементом 7; циклическая подгруппа $\{1, 17, 19, 23\}$ с порождающим элементом 17; подгруппа $\{1, 11, 19, 29\}$ (произведение двух различных подгрупп порядка 2 с порождающими элементами 11 и 19).

Задача 2

1. Найти все подгруппы аддитивной группы кольца $\mathbb{Z}_{19}$ и указать порождающие элементы.
2. Показать, что максимальная группа по умножению кольца $\mathbb{Z}_{19}$ циклическая и найти все порождающие элементы. Перечислить все ее подгруппы.

Решение

1. Операцией *сложения* в аддитивной группе кольца $\mathbb{Z}_{19}$ является сложение по модулю 19. Группа является циклической и состоит из элементов $\{0, 1, 2, \ldots, 17, 18\}$. Порождающим элементом является 1 или любой другой ненулевой элемент. Порядок группы равен 19. Так как 19 — простое число, то подгруппами являются либо сама группа, либо группа, состоящая из одного элемента 0.
2. Операцией *умножения* в кольце $\mathbb{Z}_{19}$ является умножение по модулю 19. Максимальную группу по умножению образуют все элементы, взаимно простые с модулем 19. Это все ненулевыу числа $\{1, 2, 3, \ldots, 17, 18\}$. Порядок группы равен 18. Порядки подгрупп являются делителями числа 18, то есть числа $\{18, 9, 6, 3, 2, 1\}$. Максимальная подгруппа порядка 18 является циклической. Порождающий элемент максимальной группы число 2. Проверкой убеждаемся, что все 18 степеней $2, 2^2, 2^3, \ldots, 2^{17}, 2^{18}$ различны по модулю 18. Другими порождающими элементами являются числа $3, 10, 13, 14, 15$. Подгруппа порядка 9 является циклической с порождающим элементом 4. Подгруппа порядка 6 является циклической с порождающим элементом 8. Подгруппа порядка 3 является циклической с порождающим элементом 7. Подгруппа порядка 2 является циклической и состоит из элементов $\{18, 1\}$. Подгруппа порядка 1 состоит из элемента 1.

Задача 3

1. Найти все подгруппы аддитивной группы кольца $\mathbb{Z}_{16}$ и указать, какие из них циклические и с каким порождающим элементом.

2. Найти максимальную группу по умножению кольца $\mathbb{Z}_{16}$ и все ее подгруппы.

Решение найти.

Задача 4

1. Найти все подгруппы аддитивной группы кольца $\mathbb{Z}_{21}$ и указать, какие из них циклические и с каким порождающим элементом.
2. Найти максимальную группу по умножению кольца $\mathbb{Z}_{21}$ и все ее подгруппы.

Решение найти.

Задача 5

1. Найти все подгруппы аддитивной группы кольца $\mathbb{Z}_{17}$ и указать, какие из них циклические и с каким порождающим элементом.
2. Найти максимальную группу по умножению кольца $\mathbb{Z}_{17}$ и все ее подгруппы.

Решение найти.

Задача 6

1. Используя расширенный алгоритм Евклида, найти наибольший общий делитель $d(x)$ многочленов $r_0(x)$ и $r_1(x)$ в кольце $GF(2)[x]$.
$r_0(x) = x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^6 + x^3 + x + 1$,
$r_1(x) = x^8 + x^3 + x^2 + x + 1$.
2. Записать многочлен $d(x)$ как линейную комбинацию многочленов $r_0(x)$ и $r_1(x)$.

Решение

1. Последовательное применение алгоритма деления Евклида дает следующие шаги:

$$\begin{array}{l|l|l} 1. & r_0 = q_1 r_1 + r_2, & a_0 = 1, \quad b_0 = 0, \\ 2. & r_1 = q_2 r_2 + r_3, & a_1 = 0, \quad b_1 = 1, \\ 3. & r_2 = \cdots, & a_2 = 1, \quad b_2 = -q_1, \end{array}$$

где $q_1(x) = x^5 + x^4 + x^3 + x^2 + x$, $r_2(x) = 1$, $r_3(x) = 0$. Последний ненулевой остаток равен $r_2(x) = 1$, так что наибольший общий делитель равен $d(x) = r_2(x) = 1$. Для нахождения наибольшего общего делителя в этом примере достаточно двух этапов. Третий этап нужен для вычисления многочленов $a_2(x)$ и $b_2(x)$.

2. Многочлен $r_2(x)$ равен $r_2(x) = a_2(x)r_0(x) + b_2(x)r_1(x)$. Многочлены $a_2(x)$ и $b_2(x)$ находятся на дополнительном этапе алгоритма Евклида и равны $a_2(x) = 1. b_2(x) = -q_1(x)$. Имеем равенство

$$d(x) = r_2(x) = 1 = a_2(x)r_0(x) + b_2(x)r_1(x) = r_0(x) - q_1(x)r_1(x) =$$
$$= x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^6 + x^3 + x + 1 +$$
$$+(x^5 + x^4 + x^3 + x^2 + x)(x^8 + x^3 + x^2 + x + 1).$$

Задача 7

1. Используя расширенный алгоритм Евклида, найти наибольший общий делитель $d(x)$ многочленов $r_0(x)$ и $r_1(x)$ в троичном кольце $GF(3)[x]$.
   $r_0(x) = x^5 + 2x^4 + x^3 + x^2 + 2x + 1$,
   $r_1(x) = x^2 + x + 1$.
2. Записать многочлен $d(x)$ как линейную комбинацию многочленов $r_0(x)$ и $r_1(x)$.

Решение

1. Последовательное применение алгоритма деления Евклида дает следующие шаги:

1.	$r_0 = q_1 r_1 + r_2,$	$a_0 = 1,$	$b_0 = 0.$
2.	$r_1 = q_2 r_2 + r_3,$	$a_1 = 0,$	$b_1 = 1$
3.	$r_2 = q_3 r3 + r_4,$	$a_2 = 1,$	$b_2 = -q_1,$
4.	$r_3 = \cdots ,$	$a_3 = -q_2,$	$b_3 = q_1 q_2 + 1,$

   где $q_1(x) = x^3 + x^2 + 2x + 1$, $r_2(x) = 2x$, $r_3(x) = 1$, $r_4(x) = 0$. Последний ненулевой остаток равен $r_3(x) = 1$, так что наибольший общий делитель равен $d(x) = r_3(x) = 1$. Для нахождения наибольшего общего делителя в этом примере достаточно трех этапов. Четвертый этап нужен для вычисления многочленов $a_3(x)$ и $b_3(x)$.
2. Многочлен $r_3(x)$ равен $r_3(x) = a_3(x)r_0(x) + b_3(x)r_1(x)$. Многочлены $a_3(x)$ и $b_3(x)$ находятся на дополнительном этапе алгоритма Евклида и равны $a_3(x) = -q_2(x). b_3(x) = q_1(x)q_2(x)$. Имеем равенство:

$$d(x) = r_3(x) = 1 = a_3(x)r_0(x) + b_3(x)r_1(x) =$$
$$= -q_2(x)r_0(x) + (q_1(x)q_2(x) + 1)r_1(x).$$

Задача 8

1. Показать, что многочлены $r_0(x)$ и $r_1(x)$ взаимно просты в двоичном кольце $GF(2)[x]$.
   $r_0(x) = x^8 + x^4 + x^3 + x^2 + 1$,
   $r_1(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$.
2. Найти многочлен, обратный многочлену $r_1(x)$ по модулю многочлена $r_0(x)$.

Решение

1. Последовательное применение алгоритма деления Евклида дает следующие шаги:

$$\begin{array}{l|l|l|l}
1. & r_0 = q_1 r_1 + r_2, & a_0 = 1, & b_0 = 0, \\
2. & r_1 = q_2 r_2 + r_3, & a_1 = 0, & b_1 = 1, \\
3. & r_2 = q_3 r3 + r_4, & a_2 = 1, & b_2 = -q_1, \\
4. & r_3 = q_4 r_4 + r_5, & a_3 = -q_2, & b_3 = q_1 q_2 + 1, \\
5. & r_4 = \cdots & a_4 = q_2 q_3 + 1, & b_4 = q_1 q_2 q_3 + q_3 - q_1,
\end{array}$$

   где

$$q_1(x) = x^2 + x, r_2(x) = x^4 + x^3 + x^2 + x + 1, q_2(x) = x^2,$$
$$r_3(x) = x + 1, q_3(x) = x^3 + x, r_4(x) = 1, r_5(x) = 0.$$

   Последний ненулевой остаток равен $r_4(x) = 1$, так что наибольший общий делитель равен $d(x) = r_4(x) = 1$. Следовательно, многочлены $r_0(x)$ и $r_1(x)$ взаимно просты. Для нахождения наибольшего общего делителя в этом примере достаточно четырех этапов. Пятый этап нужен для вычисления многочленов $a_4(x)$ и $b_4(x)$.

2. Многочлен $r_4(x)$ равен $r_4(x) = 1 = a_4(x)r_0(x) + b_4(x)r_1(x)$. Приводя обе части по модулю $r_0(x)$, получим $1 = b_4(x)r_1(x) \bmod (r_0(x))$. Следовательно, обратным к многочлену $r_1(x)$ по модулю $r_0(x)$ будет многочлен $b_4(x) \bmod (r_0(x))$. Многочлен $b_4(x)$ равен

$$b_4(x) = q_1(x)q_2(x)q_3(x) + q_3(x) - q_1(x) = x^7 + x^6 + x^5 + x^4 + x^3 + x^2.$$

   Этот многочлен и будет обратным к многочлену $r_1(x)$. Проверяем, что $b_4(x)r_1(x) \bmod (r_0(x)) = 1$.

Задача 9

1. Используя расширенный алгоритм Евклида, найти наибольший общий делитель $d(x)$ многочленов $r_0(x)$ и $r_1(x)$ в кольце $GF(2)[x]$.
   $r_0(x) = x^{14} + x^{12} + x^8 + x^6 + x^5 + x^4 + 1$,
   $r_1(x) = x^7 + x^5 + x^4 + x^3 + x$.
2. Записать многочлен $d(x)$ как линейную комбинацию многочленов $r_0(x)$ и $r_1(x)$.

Решение найти.

Задача 10

1. Используя расширенный алгоритм Евклида, найти наибольший общий делитель $d(x)$ многочленов $r_0(x)$ и $r_1(x)$ в троичном кольце $GF(3)[x]$.
   $r_0(x) = x^7 + x^2 + 2x + 1$,
   $r_1(x) = x^3 + 2x + 1$.
2. Записать многочлен $d(x)$ как линейную комбинацию многочленов $r_0(x)$ и $r_1(x)$.

Решение найти.

Задача 11

1. Показать, что многочлены $r_0(x)$ и $r_1(x)$ взаимно просты в двоичном кольце $GF(2)[x]$.
   $r_0(x) = x^7 + x^3 + 1$,
   $r_1(x) = x^5 + x^4 + x^3 + x^2 + x + 1$.
2. Найти многочлен, обратный многочлену $r_1(x)$ по модулю многочлена $r_0(x)$.

Решение найти.

Задача 12

1. Показать, что многочлены $r_0(x)$ и $r_1(x)$ взаимно просты в двоичном кольце $GF(2)[x]$.
   $r_0(x) = x^8 + x^4 + x^3 + x^2 + 1$,
   $r_1(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$.
2. Найти многочлен, обратный многочлену $r_1(x)$ по модулю многочлена $r_0(x)$.

Решение найти.

Задача 13

1. Показать, что многочлены $r_0(x)$ и $r_1(x)$ взаимно просты в кольце $GF(5)[x]$.
   $r_0(x) = x^6 + 3x + 2$,
   $r_1(x) = 3x^2 + 1$.
2. Найти многочлен, обратный многочлену $r_1(x)$ по модулю многочлена $r_0(x)$.

Решение найти.

Задача 14

1. Показать, что многочлен $r_0(x) = x^8 + x^6 + x^5 + x + 1$ примитивен над $GF(2)$.
2. Найти многочлен, обратный многочлену $r_1(x) = x^2 + x + 1$ по модулю многочлена $r_0(x)$.

Решение найти.

Задача 15

1. Показать, что многочлен $r_0(x) = x^6 + x^5 + x^2 + x + 1$ примитивен над $GF(2)$.
2. Найти многочлен, обратный многочлену $r_1(x) = x^5 + x + 1$ по модулю многочлена $r_0(x)$.

Решение найти.

Задача 16

1. Зная, что $r_0(x) = x^5 + x^2 + 1$ неприводим над $GF(2)$, найти все неприводимые над $GF(2)$ многочлены пятой степени.
2. Найти многочлен, обратный многочлену $r_1(x) = x^2 + 1$ по модулю многочлена $r_0(x)$.

Решение найти.

Задача 17

1. Показать, что многочлен $r_0(x) = x^3 + x^2 + x + 2$ над полем $GF(5)$ является неприводимым.
2. Найти многочлен, обратный многочлену $r_1(x) = x^2 + 3$ по модулю многочлена $r_0(x)$.

Решение найти.

Задача 18

1. Показать, что многочлен $r_0(x) = x^5 - x + 1$ примитивен над $GF(3)$.

2. Найти многочлен, обратный многочлену $r_1(x) = x^4$ по модулю многочлена $r_0(x)$.

Решение найти.

7.2. Задачи к главе 2

Задача 1

Задана следующая порождающая матрица двоичного линейного кода:

$$\mathbf{G} = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

1. Преобразовать эту матрицу к систематическому виду.
2. Выписать все кодовые векторы.
3. Найти проверочную матрицу в систематическом виде.
4. Определить проверочные соотношения.
5. Найти минимальное кодовое расстояние.
6. Найти распределение весов кодовых векторов.

Решение

1. Преобразованиями строк приводим матрицу к систематическому виду:

$$\mathbf{G}_{\text{sys}} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

2. Таблица кодовых векторов. Кодовые векторы — все линейные

комбинации строк порождающей матрицы, включая нулевую.

$$\mathbf{M} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

3. Проверочная матрица в систематическом виде:

$$\mathbf{H}_{\text{sys}} = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

4. Обозначим координаты кодового вектора как

$$\mathbf{v} = \begin{bmatrix} v_0 & v_1 & v_2 & v_3 & v_4 & v_5 & v_6 & v_7 \end{bmatrix}.$$

Координаты $\{v_0, v_1, v_2, v_3\}$ называют информационными, а $\{v_4, v_5, v_6, v_7\}$ — проверочными. Координаты удовлетворяют следующим уравнениям, определяемым строками проверочной матрицы:

$$\begin{array}{llllllllll} 1. & v_0 & +v_1 & +v_2 & & +v_4 & & & & = 0. \\ 2. & & v_1 & +v_2 & +v_3 & & +v_5 & & & = 0. \\ 3. & v_0 & & +v_2 & +v_3 & & & +v_6 & & = 0. \\ 4. & v_0 & +v_1 & & +v_3 & & & & +v_7 & = 0. \end{array}$$

5. Кодовое расстояние равно $d = 4$.
6. Обозначим число кодовых векторов веса i через w_i. Весовое распределение кода имеет вид

$$W = \{w_0{=}1, w_1{=}w_2{=}w_3{=}0, w_4{=}14, w_5{=}w_6{=}w_7{=}0, w_8{=}1\}.$$

Задача 2

1. Для линейного $(6, 2)$-кода с порождающей матрицей

$$\mathbf{G} = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}$$

найти систематический вид порождающей матрицы и весовое распределение.

2. Найти проверочную матрицу $\mathbf{H}$ и множество лидеров смежных классов. Перечислить все исправляемые кодом ошибки.

3. Найти результат декодирования блока $\mathbf{y} = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$.

Решение найти.

Задача 3

1. линейного $(6, 2)$-кода с порождающей матрицей

$$\mathbf{G} = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 \end{bmatrix}$$

найти систематический вид порождающей матрицы и весовое распределение.

2. Найти проверочную матрицу $\mathbf{H}$ и множество лидеров смежных классов. Перечислить все исправляемые и обнаруживаемые кодом ошибки.

3. Найти результат декодирования блока $\mathbf{y} = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$.

Решение найти.

Задача 4

1. Для линейного $(6, 3)$-кода с порождающей матрицей

$$\mathbf{G} = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

найти систематический вид порождающей матрицы и весовое распределение.

2. Найти проверочную матрицу $\mathbf{H}$ и множество лидеров смежных классов. Перечислить все исправляемые кодом ошибки.

3. Найти результат декодирования блока $\mathbf{y} = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 1 \end{bmatrix}$.

Решение найти.

Задача 5

Пусть $\mathcal{C}$ — двоичный линейный код с четными и нечетными весами кодовых слов.

1. Покажите, что число кодовых слов с четными весами равно числу кодовых слов с нечетными весами.
2. Покажите, что кодовые слова с четными весами формируют линейный код.

Решение найти.

Задача 6

Пусть $\mathcal{C}$ — двоичный линейный код без нулевых столбцов в порождающей матрице.

1. Найти средний вес кодового слова.
2. Как изменится средний вес, если в порождающей матрице будет один нулевой столбец?

Решение найти.

Задача 7

Пусть $\mathcal{C}$ — двоичный линейный код длины $n = 7$ без нулевых столбцов в порождающей матрице.

1. Найти кодовое расстояние, если все столбцы проверочной матрицы различны и имеют четный вес.
2. Найти порождающую матрицу кода.

Решение найти.

Задача 8

Пусть $\mathcal{C}$ — двоичный линейный код длины $n = 8$ без нулевых столбцов в порождающей матрице.

1. Найти кодовое расстояние, если все столбцы проверочной матрицы различны и имеют нечетный вес.
2. Найти порождающую матрицу кода.

Решение найти.

Задача 9

Построить двоичный линейный код длины $n = 7$ с кодовым расстоянием $d = 4$, достигающий границы Плоткина.

Решение найти.

Задача 10

1. Построить двоичный линейный код длины $n = 7$ с кодовым расстоянием $d = 3$, достигающий границы Хэмминга.
2. Найти проверочную матрицу кода.
3. Закодировать информационный вектор $\begin{bmatrix}0 & 1 & 1 & 0\end{bmatrix}$.
4. Декодируйте сообщение $\begin{bmatrix}1 & 1 & 1 & 1 & 1 & 0 & 0\end{bmatrix}$.

Решение найти.

Задача 11

1. Построить двоичный линейный $(15, 11)$ код Хэмминга с кодовым расстоянием $d = 3$.
2. Показать, что код достигает границы Хэмминга.
3. Найти проверочную матрицу кода.
4. Декодируйте сообщение $\begin{bmatrix}1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1\end{bmatrix}$.

Решение найти.

7.3. Задачи к главе 3

Задача 1

1. Порождающий многочлен $(15, 5)$ циклического кода над $GF(2)$ имеет вид $g(x) = 1 + x + x^2 + x^4 + x^5 + x^8 + x^{10}$. Записать порождающую матрицу кода в систематическом виде.
2. Найти проверочный многочлен кода.

Решение

1. Находим остатки от деления многочленов

$$\{x^{n-k},\ x^{n-k+1}, \ldots,\ x^{n-1}\} = \{x^{10},\ x^{11},\ x^{12},\ x^{13},\ x^{14}\}.$$

В соответствии с выражением (3.2) порождающая матрица в систематической форме имеет вид

$$\mathbf{G}_{\text{sys}} = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

2. Проверочный многочлен равен

$$h(x) = \frac{x^{15} - 1}{g(x)} = x^5 + x^3 + x + 1.$$

Задача 2

1. Порождающий многочлен циклического кода над $GF(2)$ имеет вид $g(x) = 1 + x^4 + x^6 + x^7 + x^8$. Покажите, что длина этого кода равна $n = 15$.
2. Записать порождающую и проверочную матрицы кода в систематическом виде.

3. Пусть α – корень многочлена $1 + x + x^4$. Показать, что корнями многочлена $g(x)$ будут $\alpha, \alpha^2, \alpha^3, \alpha^4$.

Решение

1. Многочлен $x^{15} - 1$ делится на многочлен $g(x)$ без остатка. Многочлены $x^i - 1, 1 \le i \le 14$ *не делятся* на $g(x)$.
2. В соответствии с уравнением (3.2) находим остатки от деления многочленов $x^9, \ldots, x^{14}$ на многочлен $g(x)$. С их помощью находим порождающую и проверочную матрицы кода.
3. Если α — корень многочлена $1+x+x^4$, то $\alpha, \alpha^2, \alpha^4$ — также корни этого многочлена. Так как порождающий многочлен равен
$$g(x) = 1 + x^4 + x^6 + x^7 + x^8 = (1 + x + x^4)(1 + x + x^2 + x^3 + x^4),$$
то эти величины являются также корнями $g(x)$. Элемент α^3 является корнем второго сомножителя:
$$1 + \alpha^3 + \alpha^6 + \alpha^9 + \alpha^{12} = \frac{\alpha^{15} - 1}{\alpha^3 - 1} = \frac{0}{\alpha^3 - 1} = 0.$$

Задача 3

1. Порождающий многочлен циклического кода над $GF(2)$ имеет вид $g(x) = 1+x^4+x^6+x^7+x^8$. Пусть $g^*(x) = 1+x+x^2+x^4+x^8$ — многочлен, двойственный к многочлену $g(x)$. Показать, что коды, порождаемые этими многочленами, эквивалентны.
2. Записать порождающую матрицу кода в систематическом виде.
3. Найти проверочный многочлен кода.

Решение найти.

Задача 4

1. Задан двоичный циклический код длины n с порождающим полиномом $g(x)$. Покажите, что если n нечетное и $g(x)$ не делится на $x + 1$, то код содержит слово, состоящее из единиц.

Решение найти.

Задача 5

1. Два циклических кода C_1 и C_2 длины n порождены многочленами $g_1(x)$ и $g_2(x)$ соответственно.
2. Покажите, что код C_1 вложен в код C_2, то есть $C_1 \subseteq C_2$, если $g_1(x)$ делится на $g_2(x)$.

Решение найти.

Задача 6

1. Пусть порождающий многочлен двоичного циклического кода равен $g(x) = \dfrac{x^{15} - 1}{h(x)}$, где $h(x) = x^4 + x + 1$.

2. Найти порождающую матрицу кода в систематическом виде.
3. Найти кодовое расстояние d и распределение весов кода.

Решение найти.

Задача 7

1. Порождающий многочлен двоичного циклического кода равен $g(x) = (x^3 + x^2 + 1)^2$.
2. Найти длину кода n и порождающую матрицу.
3. Найти кодовое расстояние d.

Решение найти.

7.4. Задачи к главе 4

Задача 1

1. Построить поле по модулю многочлена $\varphi(x) = 1 + x + x^4$.
2. Задан $(15, 7)$ БЧХ-код в узком смысле, исправляющий 2 ошибки. Найдите порождающий многочлен.
3. Декодируйте вектор $\mathbf{y} = (001100101100000)$.

Решение

1. Пусть α — корень многочлена $\varphi(x)$, то есть $\alpha^4 + \alpha + 1 = 0$. Поле $GF(2^4)$, построенное по модулю многочлена $\varphi(x) = 1 + x + x^4$, состоит из степеней элемента α. Таблица поля имеет вид

Базисный вид	Степенной вид	Базисный вид	Степенной вид
0	0	$1 + \alpha + \alpha^3$	α^7
1	1	$1 + \alpha^2$	α^8
α	α	$\alpha + \alpha^3$	α^9
α^2	α^2	$1 + \alpha + \alpha^2$	α^{10}
α^3	α^3	$\alpha + \alpha^2 + \alpha^3$	α^{11}
$1 + \alpha$	α^4	$1 + \alpha + \alpha^2 + \alpha^3$	α^{12}
$\alpha + \alpha^2$	α^5	$1 + \alpha^2 + \alpha^3$	α^{13}
$\alpha^2 + \alpha^3$	α^6	$1 + \alpha^3$	α^{14}

2. Порождающий многочлен $(15, 7)$ БЧХ-кода должен иметь в качестве корней элементы $\{\alpha, \alpha^2, \alpha^3, \alpha^4\}$. Многочлен $\varphi(x) = 1+x+x^4$ имеет корни $\alpha, \alpha^2, \alpha^4, \alpha^8$. Многочлен $\varphi_1(x) = 1 + x + x^2 + x^3 + x^4$ имеет корни $\{\alpha^3, \alpha^6, \alpha^{12}, \alpha^9\}$. Поэтому нужный набор корней будет иметь многочлен $g(x)$, равный их произведению:

$$g(x)=\varphi(x)\varphi_1(x)=(1+x+x^4)(1+x+x^2+x^3+x^4) = 1+x^4+x^6+x^7+x^8.$$

3. Преобразуем принятый вектор $\mathbf{y}$ в многочлен:

$$\mathbf{y} = (001100101100000) \to \mathbf{y}(x) = x^2 + x^3 + x^6 + x^8 + x^9.$$

Вычислим необходимые синдромы $S_i = \mathbf{y}(\alpha^i)$, $i = 1, 2, 3, 4$. Получим $S_1 = \alpha^{12}$, $S_2 = \alpha^9$, $S_3 = \alpha^7$, $S_4 = \alpha^3$. Предполагаем, что произошло $t = 2$ ошибки. Можно воспользоваться методами гл. 4 для исправления двух ошибок. Решаем перебором уравнение

$$X^2 + S_1 X + S_1^2 + \frac{S_3}{S_1} = 0,$$

то есть

$$X^2 + \alpha^{12} X + \alpha^{13} = 0.$$

Находим 2 решения: $X_1 = \alpha^3$ и $X_2 = \alpha^{10}$. Это означает, что ошибки произошли в позициях 3 и 10, то есть многочлен ошибок имеет вид

$$\mathbf{e}(x) = x^3 + x^{10}.$$

Передавался кодовый многочлен

$$\mathbf{v}(x) = \mathbf{y}(x) + \mathbf{e}(x) = x^2 + x^6 + x^8 + x^9 + x^{10}.$$

Задача 2

1. Построить поле по модулю многочлена $\varphi(x) = 1 + x^3 + x^4$.
2. Задан $(15, 5)$ БЧХ код в узком смысле, исправляющий 3 ошибки. Найдите порождающий многочлен.
3. Декодируйте вектор $\mathbf{y} = (010001110010010)$.

Решение

1. Пусть α — корень многочлена $\varphi(x)$, то есть $\alpha^4 + \alpha^3 + 1 = 0$. Поле $GF(2^4)$, построенное по модулю многочлена $\varphi(x) = 1 + x^3 + x^4$, состоит из степеней элемента α. Таблица поля имеет вид

Базисный вид	Степенной вид	Базисный вид	Степенной вид
0	0	$\alpha + \alpha^2$	α^7
1	1	$\alpha + \alpha^2 + \alpha^3$	α^8
α	α	$1 + \alpha^2$	α^9
α^2	α^2	$\alpha + \alpha^3$	α^{10}
α^3	α^3	$1 + \alpha^2 + \alpha^3$	α^{11}
$1 + \alpha^3$	α^4	$1 + \alpha$	α^{12}
$1 + \alpha + \alpha^3$	α^5	$\alpha + \alpha^2$	α^{13}
$1 + \alpha + \alpha^2 + \alpha^3$	α^6	$\alpha^2 + \alpha^3$	α^{14}

2. Порождающий многочлен $(15, 5)$ БЧХ-кода должен иметь в качестве корней элементы $\{\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$. Неприводимый многочлен $\varphi(x) = 1 + x^3 + x^4$ имеет корни $\alpha, \alpha^2, \alpha^4, \alpha^8$. Многочлен $\varphi_1(x) = 1 + x + x^2 + x^3 + x^4$ имеет корни $\{\alpha^3, \alpha^6, \alpha^{12}, \alpha^9\}$. Многочлен $\varphi_2(x) = 1 + x + x^2$ имеет корни $\{\alpha^5, \alpha^{10}\}$. Поэтому нужный набор корней будет иметь многочлен $g(x)$, равный их произведению:

$$g(x) = \varphi(x)\varphi_1(x)\varphi_2(x) = 1 + x^2 + x^5 + x^6 + x^8 + x^9 + x^{10}.$$

3. Преобразуем принятый вектор $\mathbf{y}$ в многочлен:

$$\mathbf{y} = (010001110010010) \to \mathbf{y}(x) = x + x^5 + x^6 + x^7 + x^{10} + x^{13}.$$

Вычислим синдромы $S_i = \mathbf{y}(\alpha^i)$, $i = 1, 2, 3, 4, 5, 6$. Тогда получим $S_1 = \alpha^{11},\ S_2 = \alpha^7,\ S_3 = \alpha^{10},\ S_4 = \alpha^{14},\ S_5 = \alpha^5,\ S_6 = \alpha^5$. Предполагаем, что произошло $t = 3$ ошибки. Вычисляем определитель системы:

$$\Delta_3 = \begin{vmatrix} S_3 & S_2 & S_1 \\ S_4 & S_3 & S_2 \\ S_5 & S_4 & S_3 \end{vmatrix} = \begin{vmatrix} \alpha^{10} & \alpha^7 & \alpha^{11} \\ \alpha^{14} & \alpha^{10} & \alpha^7 \\ \alpha^5 & \alpha^{14} & \alpha^{10} \end{vmatrix} = 0.$$

Так как $\Delta_3 = 0$, делаем вывод, что произошло меньше ошибок. Предполагаем, что произошли две ошибки, $t = 2$. Определитель системы в этом случае равен

$$\Delta_2 = \begin{vmatrix} S_2 & S_1 \\ S_3 & S_2 \end{vmatrix} = \begin{vmatrix} \alpha^7 & \alpha^{11} \\ \alpha^{10} & \alpha^7 \end{vmatrix} = \alpha^{12}.$$

Так как $\Delta_2 \neq 0$, делаем вывод, что действительное число ошибок равно 2. Можно воспользоваться методами гл. 4 для исправления двух ошибок. Решаем перебором уравнение

$$X^2 + S_1 X + S_1^2 + \frac{S_3}{S_1} = 0,$$

то есть

$$X^2 + \alpha^{11} X + \alpha^5 = 0.$$

Находим 2 решения: $X_1 = \alpha^8$ и $X_2 = \alpha^{12}$. Это означает, что ошибки произошли в позициях 8 и 12, то есть многочлен ошибок имеет вид

$$\mathbf{e}(x) = x^8 + x^{12}.$$

Передавался кодовый многочлен

$$\mathbf{v}(x) = \mathbf{y}(x) + \mathbf{e}(x) = x + x^5 + x^6 + x^7 + x^8 + x^{10} + x^{12} + x^{13}.$$

Задача 3

1. Построить поле по модулю многочлена $\varphi(x) = 1 + x^3 + x^4$.
2. Задан $(15, 5)$ БЧХ-код в узком смысле, исправляющий 3 ошибки. Найдите порождающий многочлен.
3. Декодируйте вектор $\mathbf{y} = (011001001111000)$.

Решение

1. Поле по модулю многочлена $\varphi(x) = 1 + x^3 + x^4$ строим, как в предыдущей задаче.
2. Порождающий многочлен $(15, 5)$ БЧХ-кода находим, как в предыдущей задаче:

$$g(x) = 1 + x^2 + x^5 + x^6 + x^8 + x^9 + x^{10}.$$

3. Преобразуем принятый вектор $\mathbf{y}$ в многочлен:

$$\mathbf{y} = (011001001111000) \to \mathbf{y}(x) = x + x^2x^5 + x^8 + x^9 + x^{10} + x^{11}.$$

Вычислим синдромы $S_i = \mathbf{y}(\alpha^i)$, $i = 1, 2, 3, 4, 5, 6$. Тогда получим $S_1 = 1,\ S_2 = 1,\ S_3 = \alpha^4,\ S_4 = 1,\ S_5 = 1,\ S_6 = \alpha^8$. Предполагаем, что произошло $t = 3$ ошибки. Вычисляем определитель системы:

$$\Delta_3 = \begin{vmatrix} S_3 & S_2 & S_1 \\ S_4 & S_3 & S_2 \\ S_5 & S_4 & S_3 \end{vmatrix} = \begin{vmatrix} \alpha^4 & 1 & 1 \\ 1 & \alpha^4 & 1 \\ 1 & 1 & \alpha^4 \end{vmatrix} = \alpha^{10}.$$

Так как $\Delta_3 \neq 0$, делаем вывод, что действительно произошло 3 ошибки. Решаем уравнение (4.2) для коэффициентов многочлена локаторов ошибки:

$$\begin{pmatrix} S_3 & S_2 & S_1 \\ S_4 & S_3 & S_2 \\ S_5 & S_4 & S_3 \end{pmatrix} \begin{pmatrix} \sigma_1 \\ \sigma_2 \\ \sigma_3 \end{pmatrix} = \begin{pmatrix} S_4 \\ S_5 \\ S_6 \end{pmatrix}.$$

В нашем случае система имеет вид

$$\begin{pmatrix} \alpha^4 & 1 & 1 \\ 1 & \alpha^4 & 1 \\ 1 & 1 & \alpha^4 \end{pmatrix} \begin{pmatrix} \sigma_1 \\ \sigma_2 \\ \sigma_3 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ \alpha^8 \end{pmatrix}.$$

Находим решения: $\sigma_1 = 1$, $\sigma_2 = 1$ и $\sigma_3 = \alpha^4$. Многочлен локаторов ошибок имеет вид

$$\boldsymbol{\sigma}(x) = x^3 + \sigma_1 x^2 + \sigma_2 x + \sigma_3 = x^3 + x^2 + x + \alpha^4.$$

Перебором находим корни этого многочлена: $X_1 = \alpha^8$, $X_2 = \alpha^{12}$, $X_3 = \alpha^{14}$. Это означает, что ошибки произошли в позициях 8, 12 и 14. Многочлен ошибок имеет вид

$$\mathbf{e}(x) = x^8 + x^{12} + x^{14}.$$

Добавив его к принятому многочлену $\mathbf{y}(x)$, найдем передававшийся кодовый многочлен

$$\mathbf{v}(x) = \mathbf{y}(x) + \mathbf{e}(x) = x + x^2 + x^5 + x^9 + x^{10} + x^{11} + x^{12} + x^{14}.$$

Задача 4

1. Построить поле по модулю многочлена $\varphi(x) = 1 + x^3 + x^4$.
2. Задан $(15, 7)$ БЧХ-код в узком смысле, исправляющий 2 ошибки. Найдите порождающий многочлен.
3. Декодируйте вектор $\mathbf{y} = (111110110000001)$.

Решение

1. Пусть α — корень многочлена $\varphi(x)$, то есть $\alpha^4 + \alpha^3 + 1 = 0$. Поле $GF(2^4)$, построенное по модулю многочлена $\varphi(x) = 1 + x^3 + x^4$, состоит из степеней элемента α. Таблица поля имеет вид как в предыдущей задаче.
2. Порождающий многочлен $(15, 7)$ БЧХ-кода имеет в качестве корней элементы $\{\alpha, \alpha^2, \alpha^3, \alpha^4\}$. Многочлен $\varphi(x) = 1 + x^3 + x^4$ имеет корни $\alpha, \alpha^2, \alpha^4, \alpha^8$. Многочлен $\varphi_1(x) = 1 + x + x^2 + x^3 + x^4$ имеет корни $\{\alpha^3, \alpha^6, \alpha^{12}, \alpha^9\}$. Поэтому нужный набор корней будет иметь многочлен $g(x)$, равный их произведению:

$$g(x) = \varphi(x)\varphi_1(x) = (1+x^3+x^4)(1+x+x^2+x^3+x^4) = \\ = 1+x+x^2+x^4+x^8.$$

3. Преобразуем принятый вектор $\mathbf{y}$ в многочлен:

$$\mathbf{y} = (111110110000001) \to \mathbf{y}(x) = 1+x+x^2+x^3+x^4+x^6+x^7+x^{14}.$$

Вычислим синдромы $S_i = \mathbf{y}(\alpha^i)$, $i = 1, 2, 3, 4$.Тогда получим $S_1 = \alpha$, $S_2 = \alpha^2$, $S_3 = \alpha^2$, $S_4 = \alpha^4$. Предполагаем, что произошло $t = 2$ ошибки. Можно воспользоваться методами гл. 4 для исправления двух ошибок. Решаем перебором уравнение

$$X^2 + S_1 X + S_1^2 + \frac{S_3}{S_1} = 0,$$

то есть

$$X^2 + \alpha^{12}X + \alpha^{13} = 0.$$

Находим 2 решения: $X_1 = \alpha^3$ и $X_2 = \alpha^{10}$. Это означает, что ошибки произошли в позициях 3 и 10, то есть многочлен ошибок имеет вид

$$\mathbf{e}(x) = x^3 + x^{10}.$$

Передавался кодовый многочлен

$$\mathbf{v}(x) = \mathbf{y}(x) + \mathbf{e}(x) = 1 + x + x^2 + x^4 + x^6 + x^7 + x^{10} + x^{14}.$$

7.5. Задачи к главе 5

Задача 1

1. Построить поле $GF(2^3)$ по модулю многочлена $\varphi(x) = x^3+x^2+1$.
2. Над полем $GF(2^3)$, порождающий элемент которого является корнем уравнения $\varphi(x) = x^3 + x^2 + 1$, построен $(7, 5)$-код Рида—Соломона, исправляющий одиночные ошибки.
3. При передаче кодового вектора в канале был добавлен вектор ошибки $\mathbf{E}$ с хэмминговой нормой 1, вследствие чего на приёмной стороне получен следующий вектор:

$$\mathbf{Y} = \mathbf{V} + \mathbf{E} = \begin{bmatrix}\alpha^5 & \alpha^2 & \alpha^4 & 0 & 0 & \alpha & \alpha^6\end{bmatrix}.$$

4. Найти параметры кода, исправить ошибку и найти информационный вектор.

Решение

1. Таблица поля по модулю многочлена $\varphi(x) = x^3 + x^2 + 1$ имеет вид

0	$1 = \alpha^0$	α	α^2	α^3	α^4	α^5	α^6
0	1	α	α^2	$1 + \alpha^2$	$1 + \alpha + \alpha^2$	$1 + \alpha$	$\alpha + \alpha^2$

.

2. Код Рида—Соломона имеет следующие параметры:

$$n = 7;\ d = 3;\ k = 5.$$

Информационный вектор имеет вид

$$\mathbf{v} = [v_0\ v_1\ v_2\ v_3\ v_4\ 0\ 0].$$

Кодовый вектор имеет вид $\mathbf{V} = \mathbf{v} \cdot \mathbf{F}_8$.

3. Декодирование. На приемном конце вычислим с помощью таблицы поля обратное преобразование Фурье входного вектора:

$$\mathbf{Y}\mathbf{F}_8^{-1} = \mathbf{Y}\mathbf{W}_8 = \begin{bmatrix}\alpha^2 & 1 & \alpha & \alpha^5 & \alpha^2 & \alpha^6 & \alpha^3\end{bmatrix}.$$

Предполагаем, что произошла только одна ошибка. Тогда уравнение для коэффициентов многочлена локаторов ошибок примет вид

$$\sigma_1 e_5 = e_6, \text{ то есть } \sigma_1 \cdot \alpha^6 = \alpha^3.$$

Отсюда находим $\sigma_1 = \alpha^4$ и далее рекуррентно

$$e_6 = \alpha^3,\ e_5 = \alpha^6,\ e_4 = \tfrac{e_5}{\sigma_1} = \alpha^2,\ e_3 = \tfrac{e_4}{\sigma_1} = \alpha^5,$$
$$e_2 = \tfrac{e_3}{\sigma_1} = \alpha,\ e_1 = \tfrac{e_2}{\sigma_1} = \alpha^4,\ e_0 = \tfrac{e_1}{\sigma_1} = 1.$$

Тем самым найден вектор ошибок во временно́й области:

$$\mathbf{e} = [e_0\ e_1\ e_2\ e_3\ e_4\ e_5\ e_6] = [1\ \alpha^4\ \alpha\ \alpha^5\ \alpha^2\ \alpha^6\ \alpha^3].$$

Далее находим информационный вектор:

$$\widetilde{\mathbf{v}} = \mathbf{Y}\mathbf{W}_8 - \mathbf{e} = [\alpha^3\ \alpha^6\ 0\ 0\ 0\ 0\ 0].$$

4. Проверка. Находим кодовый вектор для информационного вектора $\widetilde{\mathbf{v}}$ и сравниваем с вектором $\mathbf{Y}$.

$$\widetilde{\mathbf{V}} = \widetilde{\mathbf{v}} \cdot \mathbf{F}_8 = [\alpha^5\ \alpha^2\ \alpha^4\ 1\ 0\ \alpha\ \alpha^6].$$

Этот кодовый вектор отличается от вектора $\mathbf{Y}$ в одной позиции.

Задача 2

1. Построить поле $GF(2^3)$ по модулю многочлена $\varphi(x) = x^3 + x^2 + 1$.
2. Над полем $GF(2^3)$, порождающий элемент которого является корнем уравнения $\varphi(x) = x^3 + x^2 + 1$, построен $(7, 5)$-код Рида—Соломона, исправляющий одиночные ошибки.
3. При передаче кодового вектора в канале был добавлен вектор ошибки $\mathbf{E}$ с хэмминговой нормой 1, вследствие чего на приёмной стороне получен следующий вектор:

$$\mathbf{Y} = \mathbf{V} + \mathbf{E} = \begin{bmatrix}\alpha^5 & 0 & \alpha^6 & \alpha & \alpha^4 & \alpha & 1\end{bmatrix}.$$

4. Найти параметры кода, исправить ошибку и найти информационный вектор.

Решение

1. Таблица поля по модулю многочлена $\varphi(x) = x^3 + x + 1$ имеет вид

0	1	α	α^2	α^3	α^4	α^5	α^6
0	1	α	α^2	$1+\alpha$	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$	$1+\alpha^2$

.

2. Код Рида—Соломона имеет следующие параметры:

$$n = 7;\ d = 3;\ k = 5.$$

Информационный вектор имеет вид

$$\mathbf{v} = [v_0\ v_1\ v_2\ v_3\ v_4\ 0\ 0].$$

Кодовый вектор имеет вид $\mathbf{V} = \mathbf{v} \cdot \mathbf{F}_8$.

3. Декодирование. На приемном конце вычислим с помощью таблицы поля обратное преобразование Фурье входного вектора:

$$\mathbf{Y}\mathbf{F}_8^{-1} = \mathbf{Y}\mathbf{W}_8 = \begin{bmatrix}\alpha^6 & \alpha^4 & \alpha^5 & \alpha^2 & \alpha^6 & \alpha^3 & 1\end{bmatrix}.$$

Предполагаем, что произошла только одна ошибка. Тогда уравнение для коэффициентов многочлена локаторов ошибок примет вид

$$\sigma_1 e_5 = e_6,\ \text{то есть}\ \sigma_1 \cdot \alpha^3 = 1.$$

Отсюда находим $\sigma_1 = \alpha^4$ и далее рекуррентно

$$e_6 = 1,\ e_5 = \alpha^3,\ e_4 = \tfrac{e_5}{\sigma_1} = \alpha^6,\ e_3 = \tfrac{e_4}{\sigma_1} = \alpha^2,$$
$$e_2 = \tfrac{e_3}{\sigma_1} = \alpha^5,\ e_1 = \tfrac{e_2}{\sigma_1} = \alpha,\ e_0 = \tfrac{e_1}{\sigma_1} = \alpha^4.$$

Тем самым найден вектор ошибок во временно́й области

$$\mathbf{e} = [e_0\ e_1\ e_2\ e_3\ e_4\ e_5\ e_6] = [\alpha^4\ \alpha\ \alpha^5\ \alpha^2\ \alpha^6\ \alpha^3\ 1].$$

Далее находим информационный вектор:

$$\widetilde{\mathbf{v}} = \mathbf{Y}\mathbf{W}_8 - \mathbf{e} = [\alpha^3\ \alpha^2\ 0\ 0\ 0\ 0\ 0].$$

4. Проверка. Находим кодовый вектор для информационного вектора $\widetilde{\mathbf{v}}$ и сравниваем с вектором $\mathbf{Y}$.

$$\widetilde{\mathbf{V}} = \widetilde{\mathbf{v}} \cdot \mathbf{F}_8 = [\alpha^5\ 0\ \alpha^6\ \alpha^2\ \alpha^4\ \alpha\ 1].$$

Этот кодовый вектор отличается от вектора $\mathbf{Y}$ в одной позиции.

Задача 3

1. Построить поле $GF(2^3)$ по модулю многочлена $\varphi(x) = x^3 + x^2 + 1$.
2. Над полем $GF(2^3)$, порождающий элемент которого является корнем уравнения $\varphi(x) = x^3 + x^2 + 1$, построен $(7, 3)$-код Рида—Соломона, исправляющий двойные ошибки.
3. При передаче кодового вектора в канале был добавлен вектор ошибки $\mathbf{E}$ с хэмминговой нормой 2, вследствие чего на приёмной стороне получен следующий вектор:

$$\mathbf{Y} = \mathbf{V} + \mathbf{E} = \begin{bmatrix} \alpha^4 & \alpha^2 & \alpha^4 & 0 & 0 & \alpha & \alpha^6 \end{bmatrix}.$$

4. Найти параметры кода, исправить ошибку и найти информационный вектор.

Решение

1. Таблица поля по модулю многочлена $\varphi(x) = x^3 + x^2 + 1$ имеет вид

0	$1 = \alpha^0$	α	α^2	α^3	α^4	α^5	α^6
0	1	α	α^2	$1 + \alpha^2$	$1 + \alpha + \alpha^2$	$1 + \alpha$	$\alpha + \alpha^2$

2. Код Рида—Соломона имеет следующие параметры:

$$n = 7;\ d = 5;\ k = 3.$$

Информационный вектор имеет следующую структуру: первые 3 позиции информационные, остальные — нулевые,

$$\mathbf{v} = [v_0\ v_1\ v_2\ 0\ 0\ 0\ 0].$$

Кодовый вектор имеет вид $\mathbf{V} = \mathbf{v} \cdot \mathbf{F}_8$.

3. Декодирование. На приемном конце вычислим с помощью таблицы поля обратное преобразование Фурье входного вектора:

$$\mathbf{Y}\mathbf{F}_8^{-1} = \mathbf{Y}\mathbf{W}_8 = \begin{bmatrix} 0 & \alpha^3 & \alpha^6 & \alpha^4 & 0 & \alpha & 1 \end{bmatrix}.$$

Последние $n - k = 4$ позиции не зависят от информационной части. Обозначим их e_3, e_4, e_5, e_6. Предполагаем, что произошли две ошибки. Тогда уравнение для коэффициентов многочлена локаторов ошибок примет вид

$$\begin{aligned} e_5 &= \sigma_1 e_4 + \sigma_2 e_3, \\ e_6 &= \sigma_1 e_5 + \sigma_2 e_4 \end{aligned}$$

или

$$\begin{aligned} \alpha &= \sigma_1 \cdot 0 + \sigma_2 \alpha^4, \\ 1 &= \sigma_1 \alpha + \sigma_2 \cdot 0. \end{aligned}$$

Отсюда находим $\sigma_1 = \alpha^3$, $\sigma_2 = \alpha^3$ и далее рекуррентно

$$\begin{aligned} \sigma_2 e_2 &= \sigma_1 e_3 + e_4, \\ \sigma_2 e_1 &= \sigma_1 e_2 + e_3, \\ \sigma_2 e_0 &= \sigma_1 e_1 + e_2. \end{aligned}$$

После вычислений получим $\{e_2 = \alpha^6,\ e_1 = \alpha^5,\ e_0 = \alpha^3\}$.

Тем самым найден вектор ошибок во временно́й области:

$$\mathbf{e} = [e_0\ e_1\ e_2\ e_3\ e_4\ e_5\ e_6] = [\alpha^3\ \alpha^5\ 0\ \alpha\ \alpha^4\ \alpha^5\ \alpha^3].$$

Далее находим информационный вектор:

$$\widetilde{\mathbf{v}} = \mathbf{Y}\mathbf{W}_8 - \mathbf{e} = [\alpha^3\ \alpha^6\ 0\ 0\ 0\ 0\ 0].$$

4. Проверка. Находим кодовый вектор для информационного вектора $\widetilde{\mathbf{v}}$ и сравниваем с вектором $\mathbf{Y}$.

$$\widetilde{\mathbf{V}} = \widetilde{\mathbf{v}} \cdot \mathbf{F}_8 = [\alpha^5\ \alpha^2\ \alpha^4\ 1\ 0\ \alpha\ 1].$$

Этот кодовый вектор отличается от вектора $\mathbf{Y}$ в двух позициях.

Задача 4

1. Построить поле $GF(2^3)$ по модулю многочлена $\varphi(x) = x^3 + x + 1$.
2. Над полем $GF(2^3)$, порождающий элемент которого является корнем уравнения $\varphi(x) = x^3 + x + 1$, построен $(7, 3)$-код Рида—Соломона, исправляющий двойные ошибки.
3. При передаче кодового вектора в канале был добавлен вектор ошибки $\mathbf{E}$ с хэмминговой нормой 2, вследствие чего на приёмной стороне получен следующий вектор:

$$\mathbf{Y} = \mathbf{V} + \mathbf{E} = \begin{bmatrix} \alpha^5 & 1 & \alpha^6 & \alpha & \alpha^4 & \alpha & 1 \end{bmatrix}.$$

4. Найти параметры кода, исправить ошибку и найти информационный вектор.

Решение

1. Таблица поля по модулю многочлена $\varphi(x) = x^3 + x + 1$ имеет вид

0	1	α	α^2	α^3	α^4	α^5	α^6
0	1	α	α^2	$1+\alpha$	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$	$1+\alpha^2$

.

2. Код Рида—Соломона имеет следующие параметры:

$$n = 7;\ d = 5;\ k = 3.$$

Информационный вектор имеет следующую структуру: первые 3 позиции информационные, остальные — нулевые,

$$\mathbf{v} = [v_0\ v_1\ v_2\ 0\ 0\ 0\ 0].$$

Кодовый вектор имеет вид $\mathbf{V} = \mathbf{v} \cdot \mathbf{F}_8$.

3. Декодирование. На приемном конце вычислим с помощью таблицы поля обратное преобразование Фурье входного вектора:

$$\mathbf{Y}\mathbf{F}_8^{-1} = \mathbf{Y}\mathbf{W}_8 = \begin{bmatrix}\alpha^2 & \alpha^3 & 0 & \alpha & \alpha^4 & \alpha^5 & \alpha^3\end{bmatrix}.$$

Последние $n - k = 4$ позиции не зависят от информационной части. Обозначим их e_3, e_4, e_5, e_6. Предполагаем, что произошли две ошибки. Тогда уравнение для коэффициентов многочлена локаторов ошибок примет вид

$$\begin{aligned} e_5 &= \sigma_1 e_4 + \sigma_2 e_3, \\ e_6 &= \sigma_1 e_5 + \sigma_2 e_4 \end{aligned}$$

или

$$\begin{aligned} \alpha^5 &= \sigma_1 \alpha^4 + \sigma_2 \alpha, \\ \alpha^3 &= \sigma_1 \alpha^5 + \sigma_2 \alpha^4. \end{aligned}$$

Отсюда находим $\sigma_1 = \alpha^3$, $\sigma_2 = \alpha^3$ и далее рекуррентно

$$\begin{aligned} \sigma_2 e_2 &= \sigma_1 e_3 + e_4, \\ \sigma_2 e_1 &= \sigma_1 e_2 + e_3, \\ \sigma_2 e_0 &= \sigma_1 e_1 + e_2. \end{aligned}$$

После вычислений получим $\{e_2 = 0,\ e_1 = \alpha^5,\ e_0 = \alpha^5\}$. Тем самым найден вектор ошибок во временно́й области:

$$\mathbf{e} = [e_0\ e_1\ e_2\ e_3\ e_4\ e_5\ e_6] = [\alpha^5\ \alpha^5\ 0\ \alpha\ \alpha^4\ \alpha^5\ \alpha^3].$$

Далее находим информационный вектор:

$$\widetilde{\mathbf{v}} = \mathbf{Y}\mathbf{W}_8 - \mathbf{e} = [\alpha^3\ \alpha^2\ 0\ 0\ 0\ 0\ 0].$$

4. Проверка. Находим кодовый вектор для информационного вектора $\widetilde{\mathbf{v}}$ и сравниваем с вектором $\mathbf{Y}$.

$$\widetilde{\mathbf{V}} = \widetilde{\mathbf{v}} \cdot \mathbf{F}_8 = [\alpha^5\ 0\ \alpha^6\ \alpha^2\ \alpha^4\ \alpha\ 1].$$

Этот кодовый вектор отличается от вектора $\mathbf{Y}$ в двух позициях.

Задача 5

1. Построить поле $GF(2^3)$ по модулю многочлена $\varphi(x) = x^3 + x^2 + 1$.
2. Над полем $GF(2^3)$, порождающий элемент которого является корнем уравнения $\varphi(x) = x^3 + x^2 + 1$, построен $(7, 5)$-код Рида—Соломона, исправляющий одиночные ошибки.
3. При передаче кодового вектора в канале был добавлен вектор ошибки $\mathbf{E}$ с хэмминговой нормой 1, вследствие чего на приёмной стороне получен следующий вектор:

$$\mathbf{Y} = \mathbf{V} + \mathbf{E} = \begin{bmatrix} \alpha & 0 & \alpha & 1 & \alpha^6 & \alpha^3 & \alpha^5 \end{bmatrix}.$$

4. Найти параметры кода, исправить ошибку и найти информационный вектор.

Решение найти.

Задача 6

1. Построить поле $GF(2^3)$ по модулю многочлена $\varphi(x) = x^3 + x + 1$.
2. Над полем $GF(2^3)$, порождающий элемент которого является корнем уравнения $\varphi(x) = x^3 + x + 1$, построен $(7, 3)$-код Рида—Соломона, исправляющий двойные ошибки.
3. При передаче кодового вектора в канале был добавлен вектор ошибки $\mathbf{E}$ с хэмминговой нормой 2, вследствие чего на приёмной стороне получен следующий вектор:

$$\mathbf{Y} = \mathbf{V} + \mathbf{E} = \begin{bmatrix} 1 & \alpha^2 & \alpha^4 & 0 & \alpha^5 & \alpha & \alpha^3 \end{bmatrix}.$$

4. Найти параметры кода, исправить ошибку и найти информационный вектор.

Решение найти.

7.6. Задачи к главе 6

Задача 1

1. Проверочная матрица двоичного *рангового* кода длины $n = 3$ с ранговым расстоянием $d = 3$ равна

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 \\ 1 & \alpha^2 & \alpha^4 \end{bmatrix},$$

где α — корень многочлена $\varphi(x) = x^3 + x^2 + 1$. Найти порождающую матрицу.

2. Сообщение передаётся как кодовая матрица V. Декодировать сообщение

$$Y = V + E = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{bmatrix},$$

предполагая, что при передаче добавлена матрица ошибок E ранга 1.

Решение

1. Строим таблицу поля, порожденного многочленом $x^3 + x^2 + 1$:

0	1	α	α^2	α^3	α^4	α^5	α^6
0	1	α	α^2	$1+\alpha^2$	$1+\alpha+\alpha^2$	$1+\alpha$	$\alpha+\alpha^2$

.

2. Находим порождающую матрицу $G = \begin{bmatrix} g_1 & g_2 & g_3 \end{bmatrix}$ из уравнения

$$GH^\top = 0.$$

Можно положить $g_1 = 1$. Тогда $g_2 = \alpha^3,\ g_3 = \alpha^4$.

$$G = \begin{bmatrix} 1 & \alpha^3 & \alpha^4 \end{bmatrix}.$$

3. Преобразуем матрицу Y в вектор:

$$Y = V + E = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{bmatrix} \Rightarrow \mathbf{y} = \mathbf{v} + \mathbf{e} = \begin{bmatrix} \alpha^6 & 1 & \alpha^3 \end{bmatrix}.$$

Так как $d = 3$, то ошибка ранга 1 имеет вид

$$\mathbf{e} = e_1 \begin{bmatrix} u_1 & u_2 & u_3 \end{bmatrix} = e_1 U,$$

где $e_1 \in GF(2^3)$, $u_i \in GF(2)$. Вычислим синдром:

$$\begin{aligned} &\mathbf{y}H^\top = \mathbf{v} + \mathbf{e})H^\top = \mathbf{e}H^\top = \\ &= \begin{bmatrix} s_0 & s_1 \end{bmatrix} = \begin{bmatrix} \alpha^3 & \alpha^6 \end{bmatrix} = \\ &= e_1 \begin{bmatrix} 1 \cdot u_1 + \alpha u_2 + \alpha^2 u_3 & 1^2 \cdot u_1 + \alpha^2 u_2 + \alpha^4 u_3 \end{bmatrix} = \\ &= e_1 [x_1\ x_1^2]. \end{aligned}$$

Получаем систему

$$s_0 = \alpha^3 = e_1 x_1,$$

$$s_1 = \alpha^6 = e_1 x_1^2.$$

В этом случае $x_1 = \dfrac{s_1}{s_0} = \alpha^3$, $e_1 = \dfrac{s_0}{x_1} = 1$.

Находим

$$x_1 = \alpha^3 = 1 \cdot 1 + \alpha \cdot 0 + \alpha^2 \cdot 1 = 1 \cdot u_1 + \alpha \cdot u_2 + \alpha^2 \cdot u_3.$$

Вектор ошибки равен

$$\mathbf{e} = e_1 \begin{bmatrix} u_1 & u_2 & u_3 \end{bmatrix} = 1 \cdot \begin{bmatrix} 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 \end{bmatrix}.$$

Кодовый вектор

$$\mathbf{v} = \mathbf{y} + \mathbf{e} = \begin{bmatrix} \alpha^6 + 1 & 1 + 0 & \alpha^4 + \alpha^3 + 1 \end{bmatrix} = \begin{bmatrix} \alpha^4 & 1 & \alpha \end{bmatrix} = \alpha^4 \cdot G.$$

Задача 2

1. Проверочная матрица двоичного *рангового* кода длины $n = 3$ с ранговым расстоянием $d = 3$ равна

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 \\ 1 & \alpha^2 & \alpha^4 \end{bmatrix},$$

где α — корень многочлена $\varphi(x) = x^3 + x^2 + 1$. Найти порождающую матрицу.

2. Сообщение передаётся как кодовый вектор $\mathbf{v}$. Декодировать сообщение $\mathbf{y} = \mathbf{v} + \mathbf{e} = \begin{bmatrix} \alpha^5 & 0 & \alpha^6 \end{bmatrix}$, предполагая, что при передаче произошла ошибка $\mathbf{e}$ ранга 1.

Решение

1. Строим таблицу поля, порожденного многочленом $x^3 + x^2 + 1$:

0	1	α	α^2	α^3	α^4	α^5	α^6
0	1	α	α^2	$1 + \alpha^2$	$1 + \alpha + \alpha^2$	$1 + \alpha$	$\alpha + \alpha^2$

2. Находим порождающую матрицу $G = \begin{bmatrix} g_1 & g_2 & g_3 \end{bmatrix}$ из уравнения

$$GH^\top = 0.$$

Можно положить $g_1 = 1$. Тогда $g_2 = \alpha^3$, $g_3 = \alpha^4$.

$$G = \begin{bmatrix} 1 & \alpha^3 & \alpha^4 \end{bmatrix}.$$

3. Так как $d = 3$, то ошибка ранга 1 имеет вид

$$\mathbf{e} = e_1 \begin{bmatrix} u_1 & u_2 & u_3 \end{bmatrix} = e_1 U,$$

где $e_1 \in GF(2^3)$, $u_i \in GF(2)$. Вычислим синдром:

$$\begin{aligned} &\mathbf{y}H^\top = \mathbf{v} + \mathbf{e})H^\top = \mathbf{e}H^\top = \\ &= \begin{bmatrix} s_0 & s_1 \end{bmatrix} = \begin{bmatrix} 1 & \alpha^6 \end{bmatrix} = \\ &= e_1 \begin{bmatrix} 1 \cdot u_1 + \alpha u_2 + \alpha^2 u_3 & 1^2 \cdot u_1 + \alpha^2 u_2 + \alpha^4 u_3 \end{bmatrix} = \\ &= e_1 [x_1 \; x_1^2]. \end{aligned}$$

Получаем систему

$$s_0 = 1 = e_1 x_1,$$

$$s_1 = \alpha^6 = e_1 x_1^2.$$

В этом случае $x_1 = \dfrac{s_1}{s_0} = \alpha^6$, $e_1 = \dfrac{s_0}{x_1} = \alpha$.

Находим

$$x_1 = \alpha^6 = 1 \cdot 0 + \alpha \cdot 1 + \alpha^2 \cdot 1 = 1 \cdot u_1 + \alpha \cdot u_2 + \alpha^2 \cdot u_3.$$

Вектор ошибки равен

$$\mathbf{e} = e_1 \begin{bmatrix} u_1 & u_2 & u_3 \end{bmatrix} = \alpha \begin{bmatrix} 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & \alpha & \alpha \end{bmatrix}.$$

Кодовый вектор

$$\mathbf{v} = \mathbf{y} + \mathbf{e} = \begin{bmatrix} \alpha^5 + 0 & 0 + \alpha & \alpha^6 + \alpha \end{bmatrix} = \begin{bmatrix} \alpha^5 & \alpha & \alpha^2 \end{bmatrix} = \alpha^5 \cdot G.$$

Задача 3

1. Проверочная матрица двоичного *рангового* кода длины $n = 3$ с ранговым расстоянием $d = 3$ равна

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 \\ 1 & \alpha^2 & \alpha^4 \end{bmatrix},$$

где α — корень многочлена $\varphi(x) = x^3 + x + 1$. Найти порождающую матрицу.

2. Сообщение передаётся как кодовая матрица V. Декодировать сообщение

$$Y = V + E = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{bmatrix},$$

предполагая, что при передаче добавлена матрица ошибок E ранга 1.

Решение

1. Строим таблицу поля, порожденного многочленом $x^3 + x + 1$:

0	1	α	α^2	α^3	α^4	α^5	α^6
0	1	α	α^2	$1+\alpha$	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$	$1+\alpha^2$

.

2. Находим порождающую матрицу $G = \begin{bmatrix} g_1 & g_2 & g_3 \end{bmatrix}$ из уравнения

$$GH^\top = 0.$$

Можно положить $g_1 = 1$. Тогда $g_2 = \alpha,\ g_3 = \alpha^4$.

$$G = \begin{bmatrix} 1 & \alpha & \alpha^4 \end{bmatrix}.$$

3. Преобразуем матрицу Y в вектор:

$$Y = V + E = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{bmatrix} \Rightarrow \mathbf{y} = \mathbf{v} + \mathbf{e} = \begin{bmatrix} \alpha^5 & 0 & \alpha^2 \end{bmatrix}.$$

Так как $d = 3$, то ошибка ранга 1 имеет вид

$$\mathbf{e} = e_1 \begin{bmatrix} u_1 & u_2 & u_3 \end{bmatrix} = e_1 U,$$

где $e_1 \in GF(2^3)$, $u_i \in GF(2)$. Вычислим синдром:

$$\begin{aligned} &\mathbf{y}H^\top = \mathbf{v} + \mathbf{e})H^\top = \mathbf{e}H^\top = \\ &= \begin{bmatrix} s_0 & s_1 \end{bmatrix} = \begin{bmatrix} 1 & \alpha \end{bmatrix} = \\ &= e_1 \begin{bmatrix} 1 \cdot u_1 + \alpha u_2 + \alpha^2 u_3 & 1^2 \cdot u_1 + \alpha^2 u_2 + \alpha^4 u_3 \end{bmatrix} = \\ &= e_1 [x_1 \ x_1^2]. \end{aligned}$$

Получаем систему

$$s_0 = 1 = e_1 x_1,$$

$$s_1 = \alpha = e_1 x_1^2.$$

В этом случае $x_1 = \dfrac{s_1}{s_0} = \alpha$, $e_1 = \dfrac{s_0}{x_1} = \alpha^6$. Находим

$$x_1 = \alpha = 1 \cdot 0 + \alpha \cdot 1 + \alpha^2 \cdot 0 = 1 \cdot u_1 + \alpha \cdot u_2 + \alpha^2 \cdot u_3.$$

Вектор ошибки равен

$$\mathbf{e} = e_1 \begin{bmatrix} u_1 & u_2 & u_3 \end{bmatrix} = \alpha^6 \cdot \begin{bmatrix} 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & \alpha^6 & 0 \end{bmatrix}.$$

Кодовый вектор

$$\mathbf{v} = \mathbf{y} + \mathbf{e} = \begin{bmatrix} \alpha^5 + 0 & 0 + \alpha^6 & \alpha^2 + 0 \end{bmatrix} = \begin{bmatrix} \alpha^5 & \alpha^6 & \alpha^2 \end{bmatrix} = \alpha^5 \cdot G.$$

Задача 4

1. Проверочная матрица двоичного *рангового* кода длины $n = 3$ с ранговым расстоянием $d = 3$ равна

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 \\ 1 & \alpha^2 & \alpha^4 \end{bmatrix},$$

где α — корень многочлена $\varphi(x) = x^3 + x + 1$. Найти порождающую матрицу.

2. Сообщение передаётся как кодовый вектор $\mathbf{v}$. Декодировать сообщение $\mathbf{y} = \mathbf{v} + \mathbf{e} = \begin{bmatrix} \alpha^3 & 1 & 0 \end{bmatrix}$, предполагая, что при передаче произошла ошибка $\mathbf{e}$ ранга 1.

Решение

1. Строим таблицу поля, порожденного многочленом $x^3 + x + 1$:

0	1	α	α^2	α^3	α^4	α^5	α^6
0	1	α	α^2	$1+\alpha$	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$	$1+\alpha^2$

.

2. Находим порождающую матрицу $G = \begin{bmatrix} g_1 & g_2 & g_3 \end{bmatrix}$ из уравнения

$$GH^\top = 0.$$

Можно положить $g_1 = 1$. Тогда $g_2 = \alpha,\ g_3 = \alpha^4$.

$$G = \begin{bmatrix} 1 & \alpha & \alpha^4 \end{bmatrix}.$$

3. Так как $d = 3$, то ошибка ранга 1 имеет вид

$$\mathbf{e} = e_1 \begin{bmatrix} u_1 & u_2 & u_3 \end{bmatrix} = e_1 U,$$

где $e_1 \in GF(2^3)$, $u_i \in GF(2)$. Вычислим синдром:

$$\begin{aligned} &\mathbf{y}H^\top = \mathbf{v} + \mathbf{e})H^\top = \mathbf{e}H^\top = \\ &= \begin{bmatrix} s_0 & s_1 \end{bmatrix} = \begin{bmatrix} 1 & \alpha^5 \end{bmatrix} = \\ &= e_1 \begin{bmatrix} 1 \cdot u_1 + \alpha u_2 + \alpha^2 u_3 & 1^2 \cdot u_1 + \alpha^2 u_2 + \alpha^4 u_3 \end{bmatrix} = \\ &= e_1 [x_1\ x_1^2]. \end{aligned}$$

Получаем систему

$$\begin{aligned} s_0 = 1 = e_1 x_1, \\ s_1 = \alpha^5 = e_1 x_1^2. \end{aligned}.$$

В этом случае $x_1 = \dfrac{s_1}{s_0} = \alpha^5$, $e_1 = \dfrac{s_0}{x_1} = \alpha^2$. Находим

$$x_1 = \alpha^5 = 1 \cdot 1 + \alpha \cdot 1 + \alpha^2 \cdot 1 = 1 \cdot u_1 + \alpha \cdot u_2 + \alpha^2 \cdot u_3.$$

Вектор ошибки равен
$$\mathbf{e} = e_1 \begin{bmatrix} u_1 & u_2 & u_3 \end{bmatrix} = \alpha^2 \begin{bmatrix} 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} \alpha^2 & \alpha^2 & \alpha^2 \end{bmatrix}.$$

Кодовый вектор
$$\begin{aligned} \mathbf{v} &= \mathbf{y} + \mathbf{e} = \begin{bmatrix} \alpha^3 + \alpha^2 & 1 + \alpha^2 & 0 + \alpha^2 \end{bmatrix} = \\ &= \begin{bmatrix} \alpha^5 & \alpha^6 & \alpha^2 \end{bmatrix} = \alpha^5 \cdot G. \end{aligned}$$

Задача 5

1. Проверочная матрица двоичного рангового кода длины $n = 4$ с ранговым расстоянием $d = 3$ равна
$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 \end{bmatrix},$$
где α — корень многочлена $\varphi(x) = x^4 + x + 1$. Найти порождающую матрицу.
2. Сообщение передаётся как кодовый вектор $\mathbf{v}$. Декодировать сообщение $\mathbf{y} = \mathbf{v} + \mathbf{e} = \begin{bmatrix} 0 & 0 & \alpha^5 & \alpha^{13} \end{bmatrix}$, предполагая, что при передаче произошла ошибка $\mathbf{e}$ ранга 1.

Решение

1. Строим таблицу поля, порожденного многочленом $x^4 + x + 1$:

Базисный вид	Степенной вид	Базисный вид	Степенной вид
0	0	$1 + \alpha + \alpha^3$	α^7
1	1	$1 + \alpha^2$	α^8
α	α	$\alpha + \alpha^3$	α^9
α^2	α^2	$1 + \alpha + \alpha^2$	α^{10}
α^3	α^3	$\alpha + \alpha^2 + \alpha^3$	α^{11}
$1 + \alpha$	α^4	$1 + \alpha + \alpha^2 + \alpha^3$	α^{12}
$\alpha + \alpha^2$	α^5	$1 + \alpha^2 + \alpha^3$	α^{13}
$\alpha^2 + \alpha^3$	α^6	$1 + \alpha^3$	α^{14}

2. Находим порождающую матрицу $G = \begin{bmatrix} g_1 & g_2 & g_3 & g_4 \end{bmatrix}$ из уравнения
$$GH^\top = 0.$$
В первой строке порождающей матрицы можно положить $g_1 = 1$. Тогда $g_2 = \alpha^{12}$, $g_3 = \alpha^8$, $g_4 = \alpha^4$. Вторая строка состоит из квадратов элементов первой строки.
$$G = \begin{bmatrix} 1 & \alpha^{12} & \alpha^8 & \alpha^4 \\ 1 & \alpha^9 & \alpha & \alpha^8 \end{bmatrix}.$$

3. Так как $d = 3$, то ошибка ранга 1 имеет вид

$$\mathbf{e} = e_1 \begin{bmatrix} u_1 & u_2 & u_3 & u_4 \end{bmatrix} = e_1 U,$$

где $e_1 \in GF(2^4)$, $u_i \in GF(2)$. Вычислим синдром:

$$\begin{array}{l} \mathbf{y}H^\top = (\mathbf{v} + \mathbf{e})H^\top = \mathbf{e}H^\top = \\ = \begin{bmatrix} s_0 & s_1 \end{bmatrix} = \begin{bmatrix} \alpha^{14} & \alpha^{14} \end{bmatrix} = \\ = e_1 \begin{bmatrix} 1 \cdot u_1 + \alpha u_2 + \alpha^2 u_3 + \alpha^3 u_4 & 1^2 \cdot u_1 + \alpha^2 u_2 + \alpha^4 u_3 + \alpha^6 u_4 \end{bmatrix} = \\ = e_1 [x_1 \; x_1^2]. \end{array}$$

Получаем систему

$$\begin{aligned} s_0 = \alpha^{14} &= e_1 x_1, \\ s_1 = \alpha^{14} &= e_1 x_1^2. \end{aligned}$$

В этом случае $x_1 = \dfrac{s_1}{s_0} = 1$, $e_1 = \dfrac{s_0}{x_1} = \alpha^{14}$.

Находим неизвестные u_1, u_2, u_3, u_4, представив x_1 как комбинацию элементов первой строки проверочной матрицы:

$$x_1 = 1 = 1 \cdot u_1 + \alpha \cdot u_2 + \alpha^2 \cdot u_3 + \alpha^3 \cdot u_4 = 1 \cdot 1 + \alpha \cdot 0 + \alpha^2 \cdot 0 + \alpha^3 \cdot 0.$$

Вектор ошибки равен

$$\mathbf{e} = e_1 \begin{bmatrix} u_1 & u_2 & u_3 & u_4 \end{bmatrix} = \alpha^{14} \begin{bmatrix} 1 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} \alpha^{14} & 0 & 0 & 0 \end{bmatrix}.$$

Кодовый вектор равен

$$\begin{array}{l} \mathbf{v} = \mathbf{y} + \mathbf{e} = \begin{bmatrix} 0 + \alpha^{14} & 0 + 0 & \alpha^5 + 0 & \alpha^{13} + 0 \end{bmatrix} = \\ = \begin{bmatrix} \alpha^{14} & 0 & \alpha^5 & \alpha^{13} \end{bmatrix} = \begin{bmatrix} 1 & \alpha^3 \end{bmatrix} \cdot G. \end{array}$$

Задача 6

1. Проверочная матрица двоичного *рангового* кода длины $n = 3$ с ранговым расстоянием $d = 3$ равна

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 \\ 1 & \alpha^2 & \alpha^4 \end{bmatrix},$$

где α — корень многочлена $\varphi(x) = x^3 + x + 1$. Найти порождающую матрицу.

2. Сообщение передаётся как кодовый вектор $\mathbf{v}$. Декодировать сообщение $\mathbf{y} = \mathbf{v} + \mathbf{e} = \begin{bmatrix} \alpha^2 & \alpha^4 & \alpha^5 \end{bmatrix}$, предполагая, что при передаче произошла ошибка $\mathbf{e}$ ранга 1.

Решение найти

Задача 7

1. Проверочная матрица двоичного рангового кода длины $n = 4$ с ранговым расстоянием $d = 3$ равна

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 \end{bmatrix},$$

   где α — корень многочлена $\varphi(x) = x^4 + x + 1$. Найти порождающую матрицу.

2. Сообщение передаётся как кодовый вектор $\mathbf{v}$. Декодировать сообщение $\mathbf{y} = \mathbf{v} + \mathbf{e} = \begin{bmatrix} \alpha^{12} & 0 & 0 & \alpha^{13} \end{bmatrix}$, предполагая, что при передаче произошла ошибка $\mathbf{e}$ ранга 1.

Решение найти.

Литература

1. *Сагалович Ю.Л.* Введение в алгебраические коды: учебное пособие. – М.: МФТИ, 2007. – 262 с.

2. *Колесник В.Д.* Кодирование при передаче и хранении информации (Алгебраическая теория блоковых кодов): учеб. пособие для вузов / В.Д. Колесник. – М.: Высш. шк., 2009. – 550 с.: ил.

Учебное издание

Габидулин Эрнст Мухамедович

ЛЕКЦИИ ПО АЛГЕБРАИЧЕСКОМУ КОДИРОВАНИЮ

Редактор *Котова О.П.* Корректор *Себова Л.В.*
Компьютерная вёрстка *Казеннова Е.А.*

Подписано в печать 20.08.2015. Формат 60 × 84 $^{1}/_{16}$. Усл. печ. л. 6,8. Уч.-изд. л. 5,4.
Тираж 300 экз. Заказ № 333.

Федеральное государственное автономное образовательное учреждение
высшего профессионального образования
«Московский физико-технический институт (государственный университет)»
141700, Московская обл., г. Долгопрудный, Институтский пер., 9
Тел. (495) 408-58-22, e-mail: rio@mipt.ru

Отдел оперативной полиграфии «Физтех-полиграф»
141700, Московская обл., г. Долгопрудный, Институтский пер., 9
Тел. (495) 408 84 30, e-mail: polygraph@mipt.ru