Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Кафедра высшей математики

В. А. Липницкий

ТЕОРИЯ НОРМ СИНДРОМОВ

Методическое пособие
для студентов специальностей
1-45 01 03 «Сети телекоммуникаций»,
1-45 01 05 «Системы распределения мультимедийной информации»,
1-98 01 02 «Защита информации в телекоммуникациях»
всех форм обучения

Минск БГУИР 2011

УДК 621.391.037.3(076)
ББК 32.811.4я73
Л61

Рецензент:
заведующий кафедрой информатики учреждения образования «Белорусский государственный университет информатики и радиоэлектроники, доктор физико-математических наук, профессор Л. И. Минченко

Липницкий, В. А.

Л61 Теория норм синдромов : метод. пособие для студ. спец. 1-45 01 05 «Сети телекоммуникаций», 1-45 01 03 «Системы распределения мультимедийной информации», 1-98 01 02 «Защита информации в телекоммуникациях» всех форм обуч. / В. А. Липницкий. – Минск : БГУИР, 2011. – 96 с.

ISBN 978-985-488-570-4.

В доступной форме излагаются новейшие результаты белорусской школы помехоустойчивого кодирования, полученные на рубеже XX и XXI вв. Приводятся необходимые сведения о помехоустойчивых кодах, о строении семейства кодов Боуза – Чоудхури – Хоквингема, в частности, реверсивных кодов. Исследуется группа автоморфизмов названных кодов, порожденная циклотомическим и циклическим автоморфизмами, действие этих автоморфизмов на векторы ошибок и их синдромы. Вводится новый параметр в помехоустойчивом кодировании – норма синдрома – инвариант группы циклических сдвигов. Исследуются свойства норм синдромов, предлагаются норменные методы декодирования, отличающиеся высокой скоростью работы декодеров, на порядок снижающие влияние проблемы селектора, принципиальной возможностью исчерпания декодирующих возможностей кодов.

УДК 512(075.8)
ББК 22.144.2я73

ISBN 978-985-488-570-4

Введение

Теория норм синдромов по своему содержанию является новым научным направлением в теории и практике помехоустойчивого кодирования. Основные результаты данной теории получены в конце XX и начале XXI в. усилиями белорусской научной школы. Теория норм синдромов ориентирована на линейные коды с богатой группой автоморфизмов, в первую очередь – на циклические коды. Непосредственное изложение теории норм синдромов (ТНС) проведено для семейства кодов БЧХ (Боуза – Чоудхури – Хоквингема). Теория БЧХ-кодов хорошо разработана, а сами коды имеют широчайшие приложения от сотовой до космической связи.

В пособии в доступной форме излагаются основы построенной теории. Пособие состоит из пяти глав. В целях замкнутости изложения и с учётом ориентации на студентов второго курса в первой главе приводятся необходимые классические сведения о помехоустойчивых кодах. Вторая глава посвящена строению семейства кодов Боуза – Чоудхури – Хоквингема, описанию основных параметров этих кодов. Рассматриваются синдромные методы коррекции кратных ошибок БЧХ-кодами и реверсивными кодами, математическая суть которых сводится к решению алгебраических уравнений в полях Галуа.

Способ коррекции ошибок помехоустойчивыми кодами посредством решения уравнений над полями Галуа общепринят и кажется вполне естественным. Однако этот подход обладает рядом недостатков. Прежде всего выяснилось, что теория уравнений здесь имеет ряд лакун, особенно в наиболее важном случае полей характеристики два. Даже стандартные формулы корней квадратных уравнений здесь абсолютно не применимы. Интеллектуальный штурм возникшей проблемы был осуществлён во второй половине XX в. Громоздкие формулы для корней квадратных уравнений с использованием нормальных базисов были в конце концов получены американским математиком Чэнем. Сам Чэнь предложил решать уравнения над полями Галуа прямой последовательной подстановкой элементов поля Галуа в уравнения. Как ни странно, самый плохой – переборный метод – достаточно широко применяется и из уважения к трудам учёного носит название метода Чэня. Альтернативой ему является лишь метод Берлекемпа – Фаддеева, основанный на факторизации полинома в произведение линейных множителей. Аппаратная реализация обоих методов в любом декодере является наиболее громоздкой частью.

Другой недостаток названных синдромных методов коррекции ошибок – отсутствие подходов к решению проблемы избыточности: лишь малая часть спектра синдромов реально применяется для коррекции ошибок.

Названный комплекс проблем и послужил отправной точкой к созданию теории норм синдромов. Собственно изложение этой теории начинается с третьей главы. Здесь исследуется группа автоморфизмов реверсивных и БЧХ-кодов, рассматривается группа Г циклотомических и циклических сдвигов координат векторов, группа Ф циклотомических

автоморфизмов и объединяющая их группа G, изучается действие этих автоморфизмов на векторы ошибок. Исследуется строение Г-орбит и G-орбит векторов-ошибок.

В четвертой главе изучается действие циклических и циклотомических подстановок на синдромы ошибок, приводится описание спектров Г-орбит и G-орбит векторов-ошибок в реверсивных и БЧХ-кодов, показывается чёткая взаимосвязь между синдромами векторов-ошибок, однозначно соответствующая связи самих векторов-ошибок внутри Г-орбит и G-орбит посредством автоморфизмов соответствующих групп.

Пятая глава начинается определением нормы синдрома в произвольном БЧХ-коде. Это новый параметр в помехоустойчивом кодировании. Показывается специфика норм синдромов в зависимости от значений параметров кодов, устанавливается главное свойство норм синдромов – их независимость от действия группы циклических сдвигов. Тем самым норма синдрома становится меткой – характерным параметром соответствующей Г-орбиты. Доказательство ряда теорем обосновывает базовые свойства норм синдромов, фактически формирует контуры самой теории норм синдромов. Формулируется основной результат теории норм синдромов о декодируемости векторов-ошибок из любой совокупности Г-орбит с попарно различными нормами, формулируется обобщённый норменный метод коррекции ошибок. Главные его особенности – отказ от решения уравнений в полях Галуа, высокий уровень распараллеливания вычислений, реализуемость на ПЛИС, принципиальная возможность исчерпания проблемы избыточности применяемых кодов.

Построенная теория далека от завершения, открыта для дальнейших исследований и приложений. Пятая глава заканчивается изложением одного из возможных направлений дальнейших исследований – метода сжатия норм синдромов. Другое направление – разработка норменных методов решения уравнений в полях Галуа – находится в стадии разработки и выходит за рамки курса.

Таким образом, ТНС, с одной стороны, является прямым приложением курса «Прикладная математика», с другой стороны, выводит читателя на передовые рубежи теории и практики помехоустойчивого кодирования.

1. Линейные помехоустойчивые коды

1.1. Понятие линейного кода

Понятие линейного кода – одно из первичных, базовых понятий теории и практики помехоустойчивого кодирования. Сформировалось в теории информации к середине XX в. Аккумулирует в себе достаточно широкую научно-философскую концепцию.

Предполагается, что исходная информация записывается в виде блоков – конечных последовательностей фиксированной длины k символов из данного поля P. Другими словами, всякое информационное слово представляет собой k-разрядный вектор – произвольный вектор из линейного пространства $P_k = \{(x_1, x_2, ..., x_k) \,|\, x_i \in P\}$. Такая форма представления информации кодированием не считается. Главная цель кодирования – обеспечить надежную передачу информации в каналах с шумами, т. е. помехами. В линейных кодах цель эта достигается введением искусных поразрядных, т. е. покоординатных проверок. С математической точки зрения – это линейное отображение линейного пространства P_k в пространство большей размерности P_n, $n > k$. Все мы привыкли к матричному заданию линейных отображений векторных пространств. Следовательно, кодирование есть по сути умножение информационных слов-векторов на некоторую матрицу G порядка $k \times n$ с коэффициентами из поля P.

Поясним этот момент сведениями из линейной алгебры. Если оговорено или из контекста ясно, с какими базисами этих пространств мы имеем дело, то линейный оператор $\varphi : P_k \to P_n$ однозначно определяется матрицей A_φ этого оператора в данных базисах. Пусть $\bar{u}_1, \bar{u}_2, ..., \bar{u}_k$ – базис пространства P_k, а $\bar{v}_1, \bar{v}_2, ..., \bar{v}_n$ – базис пространства P_n. Векторы $\varphi(\bar{u}_1), \varphi(\bar{u}_2), ..., \varphi(\bar{u}_k)$ разложим по базису пространства P_n. Полученные координаты векторов $\varphi(\bar{u}_1), \varphi(\bar{u}_2), ..., \varphi(\bar{u}_k)$ составляют столбцы матрицы A_φ. Как известно, для всякого вектора $\bar{x} = (x_1, x_2, ..., x_k) \in P_k$ вектор-столбец $A_\varphi(x) = (y)$, где (x) – столбец из координат вектора $\bar{x}$, состоит из координат вектора $\varphi(\bar{x})$ в базисе $\bar{v}_1, \bar{v}_2, ..., \bar{v}_n$ пространства P_n. Протранспонировав равенство $A_\varphi(x) = (y)$, получим более точное соотношение $\varphi(\bar{x}) = \bar{x} \cdot A_\varphi^T$. Таким образом, из сказанного выше следует, что матрица $G = A_\varphi^T$.

Получаемые в результате умножения векторов пространства P_k на матрицу G n-разрядные векторы – векторы из пространства P_n – называются кодовыми словами. В совокупности они образуют k-мерное подпространство L в линейном пространстве P_n. Таким образом, получен линейный (n, k)-код L над полем P. Здесь n – длина, а k – размерность кода L. Изложенную концепцию неявно и предполагает следующее формально-математическое

Определение 1.1. Линейным (n, k)-кодом над полем P называется произвольное k-мерное подпространство линейного пространства P_n. Параметр n называется длиной кода, а k – размерностью кода. Линейный (n, k)-код называется высокоскоростным, если отношение k/n близко к 1, и низкоскоростным, если отношение $k/n << 1$ – близко к нулю.

Пример 1.1. С середины XX в. долгое время в американских системах цифровой связи передача данных осуществлялась в так называемом ASCII-формате. Этот формат требовал передавать данные блоками по восемь двоичных бит, семь из них были информационными, а восьмой – был проверочным, в нем записывался 0 или 1 так, чтобы во всем байте, т. е. во всем блоке сохранялось четное число единиц. Таким образом, восьмой бит осуществлял проверку на четность во всем байте – все восемь координат x_i, $1 \le i \le 8$, байта в совокупности удовлетворяли линейному однородному уравнению:

$$x_1 + x_2 + ... + x_8 = 0.$$

Согласно одному из фундаментальных результатов линейной алгебры множество решений любой однородной системы уравнений от n неизвестных с коэффициентами из поля P образует подпространство в пространстве P_n, причем размерность подпространства решений равна $k = n - r$, где r – ранг матрицы H коэффициентов системы. Часто в линейной алгебре данное подпространство называют ядром матрицы H и потому обозначают через $KerH$.

Множество решений данного однородного уравнения представляет весь спектр векторов-слов ASCII-формата. В соответствии с отмеченным выше результатом эти решения – двоичные векторы 8-мерного пространства P_8 над полем Галуа $P = GF(2)$ из двух элементов – образуют в P_8 7-мерное подпространство L – $(8, 7)$-линейный код над полем из двух элементов. Легко видеть, что фундаментальную систему решений – базис пространства L решений данного уравнения образуют следующие семь векторов: $\bar{e}_1 = (1000\ 0001)$, $\bar{e}_2 = (01000001),..., \bar{e}_7 = (00000011)$. Пусть G – (7×8)-матрица, строки которой состоят из координат векторов $\bar{e}_1, \bar{e}_2, ..., \bar{e}_7$. Умножением произвольных 7-мерных информационных двоичных векторов на матрицу G преобразуем их в ASCII-формат.

Пример 1.2. Очевидно, пример 1.1 имеет прозрачное обобщение на коды любой длины. Это двоичные, как и в примере 1.1, коды. Каждое кодовое слово получается добавлением к информационным блокам длиной k единственного $k+1$-го проверочного разряда, в нем записывается 0 или 1 так, чтобы во всем блоке сохранялось четное число единиц. Здесь $n = k + 1$. Такие коды называют кодами с проверкой на четность. Будем их в дальнейшем обозначать символом $C_{\text{ч}}$.

Замечание. Осмысление этого примера, точнее, факта реальной послевоенной жизни США Клодом Шенноном привело к формулировке его знаменитой теоремы [1], выражающей главную цель и назначение помехоустойчивых кодов.

Теорема 1.1 (К. Шеннон, 1948 г.). Введением избыточности в передаваемую в зашумленном канале связи информацию можно добиться исправления возникающих в процессе передачи этой информации сколь угодно сложных ошибок.

Этот же пример привел Роберта Хемминга – современника и соотечественника К. Шеннона – к созданию конкретных основ помехоустойчивого кодирования. Первым шагом в этом направлении было развитие примера 1.2, т. е.

Пример 1.3. Пусть $P = GF(2)$ – поле Галуа из двух элементов; $k = 4$, т. е. передаваемая информация состоит из 4-мерных векторов $\bar{x} = (x_1, x_2, x_3, x_4)$ с координатами x_i, $1 \le i \le 4$, со значениями $0,1 \in GF(2)$. Каждый вектор $\bar{x}$ кодируем, присоединив к нему координаты x_5, x_6, x_7, вычисленные по правилам $x_5 = x_1 + x_2 + x_4$, $x_6 = x_1 + x_3 + x_4$, $x_7 = x_2 + x_3 + x_4$. Тем самым получим линейный код C, состоящий из векторов $\bar{z} = (x_1, x_2, \ldots, x_7) \in P_7$, удовлетворяющих проверочным соотношениям:

$$\begin{cases} x_1 + x_2 \quad + x_4 + x_5 \quad = 0, \\ x_1 \quad + x_3 + x_4 \quad + x_6 \quad = 0, \\ \quad x_2 + x_3 + x_4 \quad + x_7 = 0. \end{cases} \tag{1.1}$$

Это известный совершенный систематический линейный $(7, 4)$-код, принадлежащий семейству кодов Хэмминга.

1.2. Порождающая матрица линейного кода

Пусть C – линейный (n, k)-код над полем P. Пусть $\bar{g}_1, \bar{g}_2, \ldots, \bar{g}_k$ – базис кода C.

Определение 1.2. Порождающей матрицей кода C называется (k, n)-матрица G, строки которой состоят из координат базисных векторов $\bar{g}_1, \bar{g}_2, \ldots, \bar{g}_k$ кода C в каком-нибудь заданном базисе пространства P_n.

Пример 1.4. Из примера 1.1 следует, что матрица

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

является матрицей, порождающей ASCII-формат.

Исходя из примера 1.3 построим порождающую матрицу G_χ $(7, 4)$-кода Хемминга. В двоичном четырехмерном пространстве возьмем стандартный базис $\bar{e}_1 = (1000)$; $\bar{e}_2 = (0100)$; $\bar{e}_3 = (0010)$; $\bar{e}_4 = (0001)$; В соответствии с

формулами $x_5 = x_1 + x_2 + x_4$, $x_6 = x_1 + x_3 + x_4$, $x_7 = x_2 + x_3 + x_4$ из этого базиса получаем базис $(7, 4)$-кода Хемминга: $\bar{g}_1 = (1000110)$; $\bar{g}_2 = (0100101)$; $\bar{g}_3 = (0010011)$; $\bar{g}_4 = (0001111)$. Следовательно,

$$G_\chi = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Отметим основные свойства проверочных матриц. Из определения 1.2 непосредственно следует

Свойство 1. Порождающая матрица линейного (k, n)-кода является прямоугольной (k, n)-матрицей, ранг которой равен k.

Название порождающей матрицы объясняет

Свойство 2. Любое кодовое слово линейного кода является линейной комбинацией строк матрицы G.

Здесь следует вспомнить, что базисов в любом нетривиальном пространстве достаточно много. Поэтому из определения 1.2 вытекает

Свойство 3. Порождающая матрица кода определена неоднозначно.

Любая телекоммуникационная система (ТКС), функционирующая на основе конкретного помехоустойчивого линейного кода C, на своей передающей части должна иметь фиксированную порождающую матрицу G этого кода. Данные, поступающие в ТКС от источника данных, обрабатываются кодером источника – разбиваются на компактные блоки, которые преобразуются в стандартные последовательности символов – кодовые слова источника. Это информационные слова – векторы из k-мерного пространства P_k. Каждое информационное кодовое слово $\bar{a}$ источника преобразуется кодером канала в другую, более длинную последовательность символов $\bar{b}$, содержащую в себе некоторую избыточность, называемую кодовым словом канала. В линейных кодах этот переход определяет

Свойство 4. Всякое информационное слово $\bar{a} \in P_k$ и порождаемое им кодовое слово $\bar{b} \in C$ связаны соотношением

$$\bar{b} = \bar{a} \cdot G. \qquad (1.2)$$

Пример 1.5. Закодируем $(7, 4)$-кодом Хемминга информационное слово $\bar{a} = (1101)$. Согласно формуле (1.2)

$$\bar{b} = \bar{a} \cdot G_\chi = (1101) \cdot \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} = (1101100).$$

Корректность перехода, задаваемого формулой (1.2), т. е. однозначность восстановления $\bar{a}$ по заданному $\bar{b}$ гарантирует

Теорема 1.2. Отображение $g: P_k \to P_n$ по формуле (1.2) с $k \times n$-матрицей G ранга k, $1 \le k < n$, и с коэффициентами из поля P является взаимно однозначным (биекцией).

Доказательство с точки зрения линейной алгебры практически очевидно: полный образ пространства P_k есть подпространство C размерностью k в пространстве P_n, а пространства одинаковой размерности изоморфны, т. е. между ними всегда существует взаимно однозначное соответствие.

Следствие. По известному кодовому вектору $\bar{b}$ при заданной матрице G исходный информационный вектор $\bar{a}$ однозначно восстанавливается.

Доказательство. Пусть $\bar{x} \cdot G = \bar{b}$ для неизвестного вектора $\bar{x} = (x_1, x_2, ..., x_k) \in P_k$. Векторно-матричное равенство $\bar{x} \cdot G = \bar{b}$ есть система из n линейных уравнений от k неизвестных $x_1, x_2, ..., x_k$. По построению матрицы G ранг ее равен k. Это говорит о наличии в матрице G ненулевого минора M порядка k. Согласно общей теории линейных уравнений рассматриваемая система эквивалентна подсистеме из тех уравнений, коэффициенты которых вошли в минор M. А это крамеровская подсистема, определитель которой $\Delta = M \neq 0$. Такая система, согласно правилу Крамера, имеет единственное решение.

Замечание. Доказательство следствия конструктивно – дает непосредственный алгоритм восстановления исходной информации.

Пример 1.6. В $(7, 4)$-коде Хемминга по принятому кодовому слову $\bar{b} = (1101100)$ из примера 1.5 восстановим исходное информационное слово. Для этого выпишем явно систему линейных уравнений $\bar{x} \cdot G = \bar{b}$:

$$\begin{cases} x_1 = 1 \\ x_2 = 1 \\ x_3 = 0 \\ x_4 = 1 \\ x_1 + x_2 + x_4 = 1 \\ x_1 + x_3 + x_4 = 0 \\ x_2 + x_3 + x_4 = 0. \end{cases}$$

Данная система эквивалентна своей подсистеме из первых четырех уравнений, которая однозначно указывает, что $\bar{x} = \bar{a} = (1101)$.

1.3. Проверочная матрица линейного кода

Определение 1.3. Матрица H порядка $m \times n$, $m = n - k$, называется проверочной матрицей кода C, если $KerH = C$.

Предложение 1.1. Для каждого линейного (n, k)-кода C над полем P

существует проверочная матрица. Это матрица из координат базиса пространства решений однородной системы линейных уравнений

$$GX = 0. \qquad (1.3)$$

Доказательство. Рассмотрим систему линейных однородных уравнений (1.3), где $X = (x_1, x_2, ..., x_n)^T$ – столбец неизвестных, $0 = (0,0,...,0)^T$ – нулевой столбец, G – порождающая матрица кода C. Матрица коэффициентов системы линейных уравнений (1.3) совпадает с матрицей G и потому имеет ранг k; это означает, что базис пространства решений содержит $m = n - k$ векторов. Обозначим их через $\overline{h}_1, \overline{h}_2, ..., \overline{h}_m$. Пусть H – матрица порядка $(n-k)\times n$, строками которой являются координаты $h_{ij} \in P, 1 \le i \le m, 1 \le j \le n$, векторов $\overline{h}_1, \overline{h}_2, ..., \overline{h}_m$. Из равенства (1.3) следует, что $HG^T = 0$. Следовательно, $KerH = C$ и предложение доказано.

Пример 1.7. Код $C_{\div}$ с проверкой на четность из примера 1.3 состоит из векторов-решений единственного уравнения $x_1 + x_2 + ... + x_n = 0$ над полем $P = GF(2)$. Следовательно, проверочная матрица кода $C_{\div}$ есть $(1\times n)$-матрица и имеет вид $H = (11...1)$.

Пример 1.8. Согласно определению 1.3 матрица коэффициентов приведенной выше системы линейных уравнений (1.1)

$$H = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

есть проверочная матрица $(7,4)$-кода Хэмминга из примера 1.3.

Координаты базиса ядра матрицы G составляют проверочную $(n-k)\times n$-матрицу H кода L: только для векторов $\overline{c} \in L$ $H \cdot \overline{c}^T = \overline{0}$ и только для них. Каждая из матриц G или H однозначно определяет код L.

Предложение 1.2. Пусть H – матрица порядка $(m\times n)$, $m < n$, и ранга m – проверочная матрица линейного (n, k)-кода C, где $k = n - m$. Тогда для всякой невырожденной квадратной матрицы A порядка $m = n - k$ матрица $A \cdot H$ также является проверочной для кода C.

Доказательство. Ранг матрицы AH равен m. Следовательно, $\dim\ker(AH) = n - m = k$. Для каждого вектора $\overline{c} \in C$ произведение $Hc^T = \overline{0}^T$ по определению проверочной матрицы кода. В силу ассоциативности векторно-матричных произведений $(AH)(\overline{c}^T) = A(H\overline{c}^T) = A\overline{0}^T = \overline{0}^T$. Это означает, что $\ker(AH) \supseteq \ker H = C$. Поскольку $\dim\ker(AH) = \dim\ker H$, то отсюда следует, что $\ker(AH) = C$, т. е. AH – проверочная матрица кода C, что и требовалось доказать.

Предложение 1.3. Пусть H и H_1 – две проверочные матрицы линейного

$(n,\ k)$-кода C. Тогда существует квадратная $m \times m$-матрица A для $m = n - k$, такая, что $AH = H_1$.

Доказательство. Согласно предложению 1.1 матрицы H и H_1 состоят из координат базисов пространства решений системы уравнений (1.3). Пусть $[\overline{h}] = [\overline{h}_1, \overline{h}_2, ..., \overline{h}_m]$ и $[\overline{h}'] = [\overline{h}_1', \overline{h}_2', ..., \overline{h}_m']$ – строки из векторов этих базисов. Пусть T – матрица перехода от базиса $\overline{h}_1, \overline{h}_2, ..., \overline{h}_m$ к базису $\overline{h}_1', \overline{h}_2', ..., \overline{h}_m'$. Тогда $[\overline{h}'] = [\overline{h}]T$. Оба базиса заданы своими координатами в некотором базисе $\overline{e}_1, \overline{e}_2, ..., \overline{e}_m$ пространства P_m. Пусть A и B – матрицы со столбцами – координатами векторов систем $\overline{h}_1, \overline{h}_2, ..., \overline{h}_m$ и $\overline{h}_1, \overline{h}_2, ..., \overline{h}_m$ соответственно в базисе $\overline{e}_1, \overline{e}_2, ..., \overline{e}_m$. Тогда

$$[\overline{h}] = [\overline{e}]A = [\overline{e}_1, \overline{e}_2, \ldots, \overline{e}_m]A\ ; A = H^{\mathrm{T}};\ \ B = H_1^{\mathrm{T}}.\ [\overline{h}'] = [\overline{e}]B = [\overline{h}]T = [\overline{e}]AT.$$

Следовательно, $B = A \cdot T$ или $T^{\mathrm{T}} A^T = B^T$, т. е. $H_1 = A \cdot T$ для невырожденной квадратной $m \times m$-матрицы $A = T^{\mathrm{T}}$. Предложение доказано.

Из предложений 1.2 и 1.3 следует критерий для определения, когда две матрицы являются проверочными матрицами одного и того же линейного кода.

Теорема 1.3. Пусть H – проверочная $m \times n$-матрица линейного (n, k)-кода C. Матрица H^* порядка $m \times n$ является проверочной матрицей этого же кода тогда и только тогда, когда найдется такая невырожденная $m \times m$-матрица A, что $H^* = AH$.

Следствие 1. Если у проверочной матрицы H кода C столбцы $h_{i1}, h_{i2}, \ldots, h_{im}$ образуют ненулевой (нулевой) минор, то и все остальные проверочные матрицы кода C обладают тем же свойством.

Следствие 2. Количество различных проверочных матриц линейного (n, k)-кода над конечным полем P совпадает с количеством различных невырожденных квадратных матриц порядка m в поле P, т. е. с порядком группы $GL_m(P)$ невырожденных квадратных матриц порядка m над полем P.

Следствие 2 позволяет определить количество проверочных матриц у данного линейного кода над конечным полем P. Так, над полем $GF(2)$ из двух элементов по теореме 4.11 [11] группа матриц $GL_m(GF(2))$ имеет порядок $\left|GL_m(GF(2))\right| = (2^m - 1)(2^m - 2) \cdot \ldots \cdot (2^m - 2^{m-1}) = 2^{0,5m(m-1)}(2^m - 1)(2^{m-1} - 1) \cdot \ldots \cdot (2^2 - 1).$

В частности, при $m = 5$ этот порядок равен

$$2^{10}\left(2^5 - 1\right)\left(2^{4-1} - 1\right)\left(2^3 - 1\right)\left(2^2 - 1\right) = 9999360.$$

Это означает, в частности, что у $(31, 26)$-кода Хемминга над полем $GF(2)$ имеется 9999360 различных проверочных матриц. При $m = 3$ искомый порядок равен $2^3\left(2^3 - 1\right)\left(2^{2-1} - 1\right) = 168$. Это означает, что у $(7,4)$-кода Хемминга над полем $GF(2)$ имеется 168 различных проверочных матриц.

1.4. Эквивалентные коды

Определение 1.4. Коды, отличающиеся перестановкой отсчетов, т. е. координат, называются эквивалентными.

Из определения следует существование перестановочной матрицы Π, такой, что для каждого кодового слова $\bar{c}$ кода C, вектор $\bar{c} \cdot \Pi = \bar{c}'$ есть кодовое слово эквивалентного (коду C) кода C' (определение и основные свойства перестановочных матриц см. в прил. 1).

Из этого наблюдения следует

Предложение 1.4. Пусть Π – перестановочная матрица, преобразующая код C в код C'. Если H_C – проверочная матрица кода C, то $H_{C'} = H_C \Pi^{-1}$ – проверочная матрица кода C'.

Доказательство. Для каждого $\bar{c}' \in C'$ существует вектор $\bar{c} \in C$, такой, что $\bar{c}' = \Pi \cdot c'$. Тогда $H_C \cdot \Pi^{-1} \cdot \bar{c}' = H_C \cdot \bar{c} = \bar{0}$, т. е. $H_C \cdot \Pi^{-1}$ – проверочная матрица кода C' в соответствии с определением 1.3.

Теорема 1.4. Матрицы H и H' являются проверочными матрицами эквивалентных линейных (n, k)-кодов C и C' соответственно тогда и только тогда, когда существуют невырожденная квадратная матрица A порядка $m = n - k$ и перестановочная матрица Π, такие, что $H' = A \cdot H \cdot \Pi^{-1}$ (или $H' = A \cdot H \cdot \Pi$).

Доказательство следует из теоремы 1.3 и предложения 1.4.

Пример 1.8. Для кода Хэмминга используют различные задания. Одним из наиболее известных является лексикографическое – когда i-й столбец проверочной матрицы есть двоичная запись числа i. Значит, лексикографически заданный $(7,4)$-код Хэмминга имеет проверочную матрицу

$$H_{\text{лекс}} \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

Общепринятым является интерпретация столбцов проверочной матрицы как элементов поля $GF(2^m)$, являющихся векторами из P_n в базисе $1, \alpha, \alpha^2, ..., \alpha^n$ для примитивного элемента α поля $GF(2^m)$. Если в качестве α взять корень неприводимого полинома $x^3 + x + 1$, то матрица

$$\widetilde{H} = \left[1, \alpha, \alpha^2, ..., \alpha^{2^m - 2}\right] = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

есть матрица линейного $(7,4)$-кода. Непосредственными вычислениями можно

убедиться, что $A \cdot H_{\text{лекс}} \cdot B = H$ и $C \cdot \widetilde{H} \cdot D = H$ для $A = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$; $C = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}$; H – проверочной матрицы из примера 1.3 кода Хэмминга и перестановочных матриц порядка 7

$$B = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \quad D = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Таким образом, $H, \widetilde{H}$ и $H_{\text{лекс}}$ являются проверочными матрицами различных эквивалентных друг другу $(7,4)$-кодов Хэмминга.

1.5. Систематические коды

Определение 1.5. Линейный (n, k)-код называется систематическим, если он задается проверочной матрицей вида $H = (H' \mid E)$, где E – единичная $m \times m$-матрица для $m = n - k$.

Пример 1.9. Сопоставляя определение 1.5 и матрицу H из примера 1.8, убеждаемся, что ранее рассмотренный в вышеназванном примере $(7,4)$-код Хэмминга действительно является систематическим двоичным линейным кодом.

Теорема 1.5 (критерий систематичности линейного кода). Линейный (n, k)-код C является систематическим тогда и только тогда, когда у любой его проверочной $m \times k$-матрицы последние m столбцов образуют невырожденную подматрицу.

Доказательство. Необходимость утверждения очевидна, так как единичная матрица невырожденна.

Достаточность. Пусть $H = (K \mid L)$, где L – квадратная $m \times m$-подматрица, невырожденная по условию. Тогда для матрицы $A = L^{-1}$ матрица $H' = AH = (K \mid E)$, где $K' = A \cdot K$, является проверочной матрицей кода C согласно предложению 1.3. С другой стороны, из вида матрицы H' следует, что код C – систематический. Теорема доказана.

Из теоремы 1.5 с учетом теоремы 1.4 получаем

Следствие. Всякий линейный код эквивалентен систематическому.

Теорема 1.6. Матрица $H = (K|E_m)$ порядка $m \times n$ для $m = n - k$ является проверочной матрицей систематического (n, k)-кода тогда и только тогда, когда $(k \times n)$-матрица $G = (E_k | K^T)$ является порождающей матрицей этого кода.

Доказательство непосредственным перемножением матриц G и H.

1.6. Метрика Хэмминга

Определение 1.6. Метрикой, или расстоянием на множестве X называется определенная на декартовом квадрате $X \times X$ функция ρ с неотрицательными действительными значениями, удовлетворяющая при любых $x, y \in X$ условиям:

1) $\rho(x, y) = 0$ тогда и только тогда, когда $x = y$ (аксиома тождества);

2) $\rho(x, y) + \rho(y, z) + \rho(x, z)$ (аксиома треугольника);

3) $\rho(x, y) = \rho(y, x)$ (аксиома симметрии).

Замечание 1. Часто в данное определение добавляют еще аксиому неотрицательности. Но она является следствиями перечисленных аксиом. Действительно, при $z = y$ аксиома треугольника приобретает вид

$$\rho(x, y) + \rho(y, x) \geq \rho(x, x),$$

а с учетом первой и третьей аксиом имеем $2\rho(x, y) \geq 0$, что в силу отсутствия делителей нуля в поле вещественных чисел означает неравенство $\rho(x, y) \geq 0$.

Замечание 2. Нам привычна метрика в пространстве R_n, задаваемая формулой $\rho(x, y) = \sqrt{\sum (x_i - y_i)^2}$. Но на этом пространстве возможны и другие метрики, например, задаваемые формулами

$$\sigma(x, y) = \sum_{i=1}^{n} |x_i - y_i| \text{ или } \mu(x, y) = \max |x_i - y_i|.$$

Хэмминг весьма удачно предложил свою метрику на векторных пространствах с координатами в полях Галуа. В дальнейшем будем предполагать, что $P = GF(q)$ – конечное поле из q элементов, P_n – векторное n-мерное пространство над полем P, содержащее линейный (n, k)-код C.

Определение 1.7. Расстоянием Хэмминга между векторами $\bar{x}, \bar{y} \in P_n$ называется количество $dist(\bar{x}, \bar{y})$ несовпадающих координат этих векторов.

Весом $w(\bar{x})$ вектора $\bar{x} \in P_n$ называется количество ненулевых координат этого вектора.

Несложно видеть, что расстояние Хэмминга между векторами $\bar{x}, \bar{y} \in P_n$ равно весу вектора $\bar{x} - \bar{y}$. Очевидно, $wt(\bar{x} + \bar{y}) \leq wt(\bar{x}) + wt(\bar{y})$.

Лемма 1.1. Расстояние Хэмминга обладает всеми свойствами обычного расстояния (из определения 1.6):

1) $dist(\bar{y}, \bar{x}) = dist(\bar{x}, \bar{y})$ – свойство симметричности;

2) $dist(\bar{x}, \bar{y}) = 0$ тогда и только тогда, когда $\bar{x} = \bar{y}$;

3) $dist(\bar{x}, \bar{z}) + dist(\bar{z}, \bar{y}) \geq dist(\bar{x}, \bar{y})$ – неравенство треугольника.

Доказательство. Первые два свойства непосредственно следуют из отмеченного выше соотношения: $dist(\bar{x}, \bar{y}) = wt(\bar{x} - \bar{y}) = wt(\bar{y} - \bar{x})$. Аналогично $dist(\bar{x}, \bar{z}) + dist(\bar{z}, \bar{y}) = wt(\bar{x} - \bar{z}) + wt(\bar{z} - \bar{y}) \geq wt((\bar{x} - \bar{z}) + (\bar{z} - \bar{y})) = wt(\bar{x} - \bar{y}) = dist(\bar{x}, \bar{y})$.

Таким образом, доказано и третье свойство расстояния.

Определение 1.8. t-окрестностью вектора $\bar{x} \in P_n$ назовем совокупность всех векторов $\bar{y} \in P_n$, для которых $dist(\bar{x}, \bar{y}) \leq t$. t-окрестности обладают обычным свойством отделимости.

Лемма 1.2. Если $dist(\bar{x}, \bar{z}) > 2t$, то t-окрестности векторов $\bar{x}, \bar{z} \in P_n$ не пересекаются.

Доказательство методом от противного. Предположим, что в пространстве P_n найдутся векторы $\bar{x}, \bar{z}$ на расстоянии $dist(\bar{x}, \bar{z}) \geq 2t + 1$ друг от друга и с вектором $\bar{y} \in P_n$, одновременно принадлежащим обеим t-окрестностям векторов $\bar{x}, \bar{z} \in P_n$. Тогда по аксиоме треугольника

$$dist(\bar{x}, \bar{z}) \leq dist(\bar{x}, \bar{y}) + dist(\bar{y}, \bar{z}) \leq t + t = 2t < 2t + 1,$$

что противоречит условию $dist(\bar{x}, \bar{z}) \geq 2t + 1$. Следовательно, предположение о пересекаемости окрестностей невозможно и лемма доказана.

1.7. Минимальное расстояние кода

Определение 1.9. Минимальным, или кодовым расстоянием кода C называется наименьшее из расстояний между попарно различными векторами кода C.

Из равенства $dist(\bar{x}, \bar{y}) = wt(\bar{x} - \bar{y})$ следует, что минимальное расстояние линейного кода равно наименьшему из весов ненулевых векторов этого кода.

Значение кодового расстояния определяет следующая – фундаментальная в помехоустойчивом кодировании

Теорема 1.7. Если минимальное расстояние кода C равно $d = 2t + 1$ или $d = 2t + 2$, то код C может обнаружить до $d - 1$ ошибок и исправить до t ошибок в каждом принятом векторе-слове длиной n.

Доказательство. Возможность обнаружения до $d - 1$ ошибок. Если к кодовому слову $\bar{c} \in C$ прибавить любой вектор $\bar{e} \in P_n$, у которого менее d ненулевых координат, то полученный вектор $\bar{x} = \bar{c} + \bar{e}$ не принадлежит, очевидно, подпространству C (в противном случае $\bar{x} - \bar{c} = \bar{e} \in C$, что противоречит минимальности d). Как мы уже знаем, принадлежность и не принадлежность данного вектора коду C определяется результатом умножения на проверочную матрицу H_C этого кода. Результат $\bar{x} \cdot H_C^T \neq \bar{0}$ означает, что принятое сообщение $\bar{x} \notin C$ и, следовательно, в отличие от переданного слова $\bar{c}$ содержит ошибки.

Докажем возможность декодирования до t ошибок. Если к кодовому слову $\bar{c} \in C$ прибавить любой вектор $\bar{e} \in P_n$, у которого $\tau \le t$ ненулевых координат, то полученный вектор $\bar{x} = \bar{c} + \bar{e}$ находится на расстоянии τ от вектора $\bar{c} \in C$. Если $\bar{c}_i$ – другой вектор подпространства C, то в силу леммы 1.2 $dist(\bar{x}, \bar{c}_i) > t$. Предположение о противоположном неравенстве приводит к противоречию: если предположить, что найдется вектор $\bar{c}_j \in C$, для которого $dist(\bar{x}, \bar{c}_j) \le t$, то в силу неравенства треугольника

$$d \le dist(\bar{c}, \bar{c}_j) \le dist(\bar{c}, \bar{x}) + dist(\bar{x}, \bar{c}_j) \le 2t < d.$$

Таким образом, существует единственный вектор $\bar{c} \in C$, находящийся на расстоянии $\rho \le t$ от принятого вектора-сообщения $\bar{x}$. Этот однозначно определенный вектор $\bar{c}$ естественно взять в качестве правильного, неискаженного переданного сообщения. Теорема полностью доказана.

Замечание 1. Если вектор ошибок $\bar{e}$ содержит $\tau \ge d$ ненулевых координат, то он может оказаться кодовым словом, т. е. принадлежать подпространству C. Тогда в силу замкнутости C относительно операции сложения вектор $\bar{x} = \bar{c} + \bar{e} \in C$. В таком случае мы не сможем заметить ошибки в принятом сообщении $\bar{x} = \bar{c} + \bar{e}$.

Замечание 2. Предложенный в доказательстве теоремы метод декодирования носит название «декодирования в ближайшее кодовое слово», или «декодирование по максимуму правдоподобия» [6, с. 26].

При оптимистичном определении 1.1 далеко не каждое k-мерное подпространство линейного пространства P_n относят к реальным линейным кодам. На практике применяются коды с попарно удаленными друг от друга кодовыми словами в смысле метрики Хемминга – с достаточно большим кодовым расстоянием d. Ведь согласно фундаментальной в помехоустойчивом кодировании теореме 1.6 только такие коды могут исправлять возникающие в процессе передачи информации ошибки. Со схемотехнической точки зрения полезны в практическом применении и иные свойства линейных кодов – систематичность, цикличность, реверсивность и т. д. Все эти свойства определяются соответствующими свойствами проверочной матрицы H.

Следующая теорема служит критерием для определения минимального расстояния кода.

Теорема 1.8. Пусть H – проверочная матрица двоичного кода C. Минимальное расстояние этого кода равно d тогда и только тогда, когда любые $d-1$ столбцов матрицы H линейно независимы, но найдутся d линейно зависимых столбцов.

Доказательство теоремы обеспечивает

Лемма 1.3. Пусть $[i]$ – i-й столбец проверочной матрицы H линейного кода C над полем P. Вектор $\bar{c} \in P_n$ весом ϖ с ненулевыми координатами на позициях $i_1, i_2, ..., i_\varpi$ принадлежит коду C тогда и только тогда, когда система столбцов $[i_1], [i_2], ..., [i_\varpi]$ линейно зависима.

Доказательство. По условию $\bar{c} = (0, ..., 0, c_{i_1}, 0, c_{i_\varpi}, 0, ..., 0)$ с единственными ненулевыми координатами $c_{i_j} \in P,\ 1 \le j \le \varpi$. Вектор $\bar{c}$ принадлежит коду C тогда и только тогда, когда $H \cdot \bar{c}^T = \bar{0}$. По свойствам матричного умножения

$$H \cdot \bar{c}^T = c_{i_1}[i_1] + c_{i_2}[i_2] + ... + c_{i_\varpi}[i_\varpi].$$

Равенство $c_{i_1}[i_1] + c_{i_2}[i_2] + ... + c_{i_\varpi}[i_\varpi] = \bar{0} = [0]$ означает линейную зависимость столбцов $[i_1], [i_2], ..., [i_\varpi]$. Лемма полностью доказана.

1.8. Коды Хемминга

Определение 1.10. Кодом Хемминга называется линейный код C_χ с проверочной матрицей $H_\chi = (1, \alpha, ..., \alpha^{2m-2})$. Здесь α^i – двоичный вектор-столбец над полем $GF(2)$ в базисе $1, \alpha, ..., \alpha^{m-1}$ для примитивного элемента α поля $GF\left(2^m\right)$.

Из определения следует, что столбцами матрицы H_χ являются все возможные ненулевые векторы двоичного пространства P_n. Поэтому произвольный код Хэмминга имеет параметры $n = 2^m - 1$, $k = n - m$: $(7, 4); (15, 11); (31, 26); (63, 57); (127, 120); (255, 247); (511, 502); (1023, 1013)$ и т. д.

Теорема 1.9. У кода Хэмминга минимальное расстояние $d = 3$.

Доказательство. Из задания проверочной матрицы $H_\chi = (1, \alpha, ..., \alpha^{2m-2})$ непосредственно видно, что в ней любые два столбца попарно различны и, следовательно, линейно независимы. Однако в этой матрице обязательно найдется тройка линейно зависимых столбцов, например, столбцы $1, \alpha, \alpha + 1$.

Следствие. Код Хэмминга исправляет одиночные ошибки.

Следует отметить, что коды Хемминга – это исторически первый и удачный класс линейных помехоустойчивых кодов, нашедших приложения и в теории и на практике.

Отметим, что все коды, эквивалентные коду C_χ, также называются кодами Хэмминга. Все они имеют то же кодовое расстояние и также исправляют одиночные ошибки.

Почти одновременно с кодами Хемминга в руках исследователей как результат «народного творчества» появился код C_{ASC} на основе ASCII-формата, также исправляющий одиночные ошибки. Это двоичный $(64, 49)$-код. Его кодовые слова лучше представлять в виде двоичных квадратных матриц

порядка 8. В этих матрицах координаты c_{ij}, $1 \le i, j \le 7$, являются информационными, а остальные – проверочными. Восьмой элемент каждой строки – проверочный. Как и в ASCII-формате, $c_{i8} = 1$ или $c_{i8} = 0$, причем выбирается такое значение, чтобы сумма всех элементов $i-$й строки равнялась нулю. Аналогичным рассуждением со столбцами определяются элементы c_{8j} восьмой строки матрицы с тем, чтобы сумма единиц в каждом столбце была четной. 64-й разряд каждого кодового слова – элемент c_{88} – проверяет на четность суммарное количество единиц в проверочных разрядах строк.

Если при передаче кодового слова произошла одиночная ошибка в информационном поле, то нарушение четности в конкретных проверочных разрядах строк и столбцов однозначно укажет на ошибочную позицию. Если же возникает нарушение четности в 64-м разряде, то этот факт можно проигнорировать, поскольку ошибка произошла в каком-то из проверочных разрядов и не затронула информационные разряды.

Сравнивая данный код с кодом Хемминга, можно утверждать, что код Хемминга лучше, поскольку при примерно равных длинах (63 и 64) имеет почти на порядок меньше проверочных разрядов (6 и 15 соответственно).

Тем не менее код C_{ASC} послужил прообразом целого направления в помехоустойчивом кодировании – разработки так называемых кодов-произведений, кодов-перемежений, каскадных кодов. Этот код подсказал кодировщикам метод конструирования из слабых кодов более мощных по корректирующим возможностям.

1.9. Декодирование по таблицам смежных классов

Пусть C – линейный (n, k)-код над конечным полем $P = GF(q)$ из q элементов. Векторное пространство P_n состоит из q^n элементов, а его подпространство C – из $\tau = q^k$ векторов. Для каждого $\bar{a} \in P_n$, $\bar{a} \notin C$ множество $\bar{a} + C = \{\bar{a} + \bar{c}_i \mid \bar{c}_i \in C\}$ в теории групп называется смежным классом аддитивной группы P_n по подгруппе C. Видимый приоритет вектора $\bar{a}$ в смежном классе иллюзорен – этот вектор можно заменить любым другим вектором этого же смежного класса ввиду легко проверяемого равенства $\bar{b} + C = \bar{a} + C$ для каждого вектора $\bar{b} \in \bar{a} + C$ и наоборот.

Как аддитивная группа, P_n распадается в объединение $s = q^{n-k}$ непересекающихся смежных классов по своей подгруппе C, также содержащих по q^k векторов $P_n = (\bar{0} + C) \bigcup (\bar{a}_1 + C) \bigcup \ldots \bigcup (\bar{a}_{s-1} + C)$ для подходящих векторов $\bar{a}_i \in P_n$, $1 \le i \le s-1$.

Если в результате передачи неизвестного на приемном конце кодового слова $\bar{c} \in C$ получен вектор $\bar{y} \neq \bar{c}$, то все возможные значения вектора ошибок $\bar{e} = \bar{y} - \bar{c}$ лежат в одном смежном классе с вектором $\bar{y}$. Наиболее вероятным вектором ошибок из них является, очевидно, тот вектор смежного класса, который в этом классе имеет наименьший вес. Определив такой вектор $\bar{e}$, мы декодируем $\bar{y}$, заменяя его кодовым словом $\bar{c} = \bar{y} - \bar{e}$.

Определение 1.11. Лидером смежного класса $U = \bar{a}_i + C$ называется вектор $\bar{e}_i$ наименьшего веса в этом смежном классе.

В силу отмеченных свойств смежных классов $U = \bar{a}_i + C = \bar{e}_i + C$. Предложенный выше метод коррекции ошибок кодом C называется методом декодирования по лидерам смежных классов. Реализуется он выписыванием таблицы смежных классов:

$$\begin{array}{cccc} \bar{0} & \bar{c}_1 & \dots & \bar{c}_{\tau-1} \\ \bar{e}_1 & \bar{e}_1 + \bar{c}_1 & \dots & \bar{e}_1 + \bar{c}_{\tau-1} \\ \dots & \dots & \dots & \dots \\ \bar{e}_{s-1} & \bar{e}_{s-1} + \bar{c}_1 & \dots & \bar{e}_{s-1} + \bar{c}_{\tau-1} \end{array}$$

Первый столбец этой таблицы состоит из лидеров смежных классов. Если $\bar{y} = \bar{e}_i + \bar{c}_j$ – элемент i-й строки и j-го столбца выписанной таблицы смежных классов, то лидер этой строки $\bar{e}_i$ есть вектор-ошибка в принятом сообщении $\bar{y}$, а истинное передаваемое сообщение есть вектор $\bar{c}_j$ – первый элемент j-го столбца.

Пример 1.10. Рассмотрим линейный $(6,3)$-код $\ddot{\ddot{C}}$ с порождающей матрицей

$$G_{\ddot{\ddot{C}}} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} = (E_3 \mid K^T)$$

над полем Галуа из двух элементов. Легко видеть, что определитель матрицы $K^T = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$ не равен нулю. Поэтому согласно теореме 1.4 код $\ddot{\ddot{C}}$ является систематическим, а по теореме 1.5 его проверочная матрица

$$H_{\ddot{\ddot{C}}} = (K \mid E_3) = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Также легко видно, что любые два столбца матрицы $H_{\ddot{\ddot{C}}}$ образуют линейно независимую систему. Тогда в силу теоремы 1.7 минимальное расстояние кода $\ddot{\ddot{C}}$ есть величина $d = 3$. Следовательно, код $\ddot{\ddot{C}}$ способен корректировать одиноч-

ные ошибки. Ясно, что $|P_6| = 2^6 = 64$, а $|\ddot{\ddot{C}}| = 8$. Код $\ddot{\ddot{C}}$, как известно, составляют нулевой вектор, векторы-строки матрицы $G_{\ddot{\ddot{C}}}$, суммы этих строк по две – векторы (110101), (101001), (011100), а также сумма всех трех сток – вектор (111010). Выпишем таблицу смежных классов с лидерами векторного пространства P_6 над полем $P = GF(2)$ по коду $\ddot{\ddot{C}}$.

000000	100110	010011	110101	001111	101001	011100	111010
100000	000110	110011	010101	101111	001001	111100	011010
010000	110110	000011	001100	011111	111001	100101	101010
001000	101110	011011	010100	000111	100001	111101	110010
000100	100010	010111	011000	001011	101101	110001	111110
000010	100100	010001	011110	001101	111011	110110	111000
000001	100111	010010	011101	001110	101000	110100	111011
000101	100011	010110	011001	001010	101100	110000	111111

Первая строка этой таблицы – строка всех кодовых слов из кода $\ddot{\ddot{C}}$, а первый столбец состоит из лидеров строк – смежных классов. Если принято слово 110011, которое находится во второй строке и третьем столбце таблицы, то истинным передаваемым сообщением следует считать кодовое слово 010011. Если принято слово 100101, которое находится в третьей строке и седьмом столбце таблицы, то истинным передаваемым сообщением следует считать кодовое слово 110101.

Данный метод позволяет в рассмотренном примере корректировать все одиночные ошибки и даже одну двойную ошибку – лидера восьмого смежного класса.

1.10. Весовой спектр кода

Метод декодирования по таблицам смежных классов хорош и удобен, но применим лишь для кодов с не очень большими по размерам таблицами этих классов. Во многих важных для практики случаях такой метод неприемлем, поскольку не всегда известен или практически не обозрим список кодовых слов. В таких случаях ценную информацию о коде может дать весовой спектр кода – таблица или гистограмма значений веса кодовых слов.

В любом коде в точности один вектор – нулевой – имеет вес 0, определенное количество кодовых слов имеют минимальный вес d. Весовые значения остальных кодовых слов находятся в диапазоне от $d+1$ до n. Однако распределение весов в этом диапазоне имеет определенные закономерности и достаточно причудливую специфику. Одну из таких закономерностей отражает

Лемма 1.4. В любом двоичном линейном коде C либо все кодовые слова имеют четный вес, либо ровно половина кодовых слов имеет четный вес, а половина – нечетный вес.

Доказательство. Любой двоичный линейный код C является группой относительно операции сложения. Нетрудно видеть, что кодовые слова четного веса образуют подгруппу D в группе C. Если в коде C имеются и кодовые слова нечетного веса, то они образуют отдельный смежный класс по подгруппе D. Мощность любого смежного класса совпадает с мощностью подгруппы D. Поскольку любое кодовое слово либо принадлежит D, либо указанному смежному классу, то тем самым лемма полностью доказана.

Аналогично доказывается

Лемма 1.5. В любом двоичном линейном коде C либо все кодовые слова имеют данную *i*-ю координату, равную нулю, либо ровно у половины кодовых слов *i*-я координата равна 0, а у другой половины – равна 1.

Без труда строится таблица весов кода $\overset{\cdots}{C}$ из примера 1.10. Наглядной иллюстрацией к доказанной лемме 1.4 является

Пример 1.11. Код Хемминга над полем $GF(2^{11})$ имеет параметры $(n, k, d) = (2047, 2036, 3)$. Следовательно, проверочная матрица этого кода есть (11×2047)-матрица $H_\chi = (1, \alpha, \alpha^2, ..., \alpha^{2046})$ для примитивного элемента α поля $GF(2^{11})$ – корня неприводимого и примитивного полинома 11-й степени над полем из двух элементов, например, полинома $x^{11} + x^2 + 1$ – одного из 176 двоичных примитивных полиномов 11-й степени. Отметим, что длина этого кода $n = 2047 = 23 \cdot 89$ – составная. Пусть $\beta = \alpha^{89}$. Выделим в матрице H_χ подматрицу $H_{\tilde{A}} = (1, \beta, \beta^2, ..., \beta^{22})$. Это (11×23)-матрица. Векторы ядра матрицы $H_{\tilde{A}}$ образуют линейный $(23,12)$-код Γ. На рис. 1.1 представлена диаграмма весов кода Γ, данные для которой получены компьютерными расчетами – решением системы линейных уравнений $H_{\tilde{A}} \cdot \bar{x}^T = \bar{0}$ и анализом весов полученных векторов-решений.

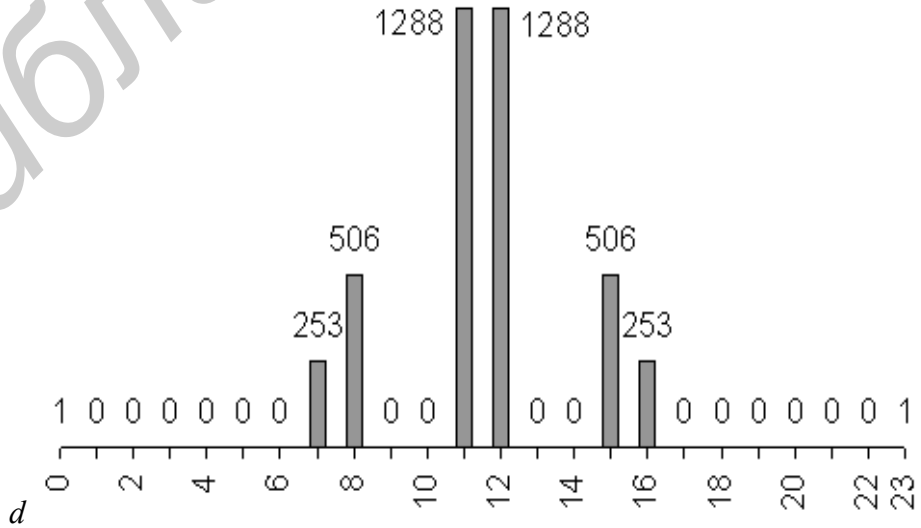

Рис. 1.1. Диаграмма весов кодовых слов $(23,12)$-кода Γ

Из приведенной на рис. 1.1 диаграммы видим, что полностью подтверждается вторая часть альтернативы доказанной леммы 1.4. Также видим, что минимальное расстояние данного кода равно 7. Следовательно, код Γ способен корректировать векторы-ошибки весом 1 – 3.

Оказалось, что найденный спектр весов полностью совпадает с весовым спектром $(23,12,7)$-кода Голея – знаменитого своими уникальными свойствами кода, тщательного изученного в [2]. Иных кодов с такими параметрами не существует. Об этом свидетельствуют многочисленные аналитические и компьютерные исследования, проведенные в различных уголках земного шара. Поэтому можно с уверенностью утверждать, что линейный код с проверочной матрицей $H_{\tilde{A}} = (1, \beta, \beta^2, ..., \beta^{22})$ есть код Голея, во всяком случае эквивалентен коду Голея.

Подобная выше рассмотренной процедура получения нового кода называется укорочением. Как видим, она позволяет в отдельных случаях добиться существенного увеличения кодового расстояния, несмотря на уменьшение длины и размерности кода.

1.11. Синдромы ошибок

Одним из важнейших понятий теории помехоустойчивых кодов является синдром ошибок. В процессе передачи информации на кодовое слово $\bar{c}$ может наложиться «шум» – вектор-ошибка $\bar{e}$. В результате приемное устройство получает искаженное сообщение $\bar{y} = \bar{c} + \bar{e}$.

Определение 1.12. Синдромом ошибок принятого слова $\bar{y}$ в коде C с проверочной матрицей H называется вектор $S = H \cdot \bar{y}^T$.

Если $S = \bar{0}$, то $\bar{y}$ – кодовое слово. Следовательно, условие $S \neq \bar{0}$ служит признаком наличия ошибочных символов в принятом слове $\bar{y}$. В силу ассоциативности операций сложения и умножения матриц синдром

$$S = H \cdot \bar{y}^T = H \cdot (\bar{c}^T + \bar{e}^T) = H \cdot \bar{c}^T + H \cdot \bar{e}^T = H \cdot \bar{e}^T .$$

Это означает, что S зависит только от вектора ошибок $\bar{e}$ и не зависит от кодовых слов.

Предложение 1.5. Пусть H и H_1 проверочные матрицы кода C. Пусть $\bar{e}_1$ и $\bar{e}_2$ – различные векторы ошибок, синдромы которых относительно матрицы H совпадают (различны). Тогда и относительно матрицы H_1 их синдромы также совпадают (различны).

Доказательство. Пусть по условию $H \cdot \bar{e}_1^T = H \cdot \bar{e}_2^T = S$. Докажем, что $H_1 \cdot \bar{e}_1^T = H_2 \cdot \bar{e}_2^T$. Согласно теореме 1.2 $H_1 = A \cdot H$ для подходящей невырожденной матрицы A порядка m. Тогда синдромы векторов ошибок $\bar{e}_1$ и $\bar{e}_2$ от-

носительно матрицы H_1 соответственно равны $H_1 \cdot \bar{e}_1^T = A \cdot H \cdot \bar{e}_1^T = A \cdot S$; $H_1\left(\bar{e}_2^T\right) = A \cdot H\left(\bar{e}_2^T\right) = A \cdot S$. Названные синдромы совпадают. Предложение доказано.

Пусть H – фиксированная проверочная матрица данного линейного (n,k)-кода L над полем P. Пусть $E_n = P_n$ – пространство всех векторов размерностью n над полем P – пространство возможных ошибок кода L, содержащее L в качестве своего подпространства.

Предложение 1.6. Если $\bar{e}$ пробегает все векторы пространства E_n, то S пробегает все векторы пространства E_{n-k}.

Доказательство. Отображение φ_H, ставящее каждому вектору $\bar{e} \in E_n$ в соответствие его синдром $S = S(\bar{e})$, есть линейный оператор из пространства E_n в пространство E_{n-k}. Образ пространства E_n при этом отображении (множество всех синдромов) есть подпространство в E_{n-k} размерностью $n - \dim KerH = n - k$ и, следовательно, совпадает с E_{n-k} Таким образом, вектор S может быть любым вектором. Предложение доказано.

Следствие. Пусть C – линейный (n,k)-код над конечным полем из q элементов. Тогда каждое значение синдрома $S = S(\bar{e})$ принимают в точности q^k различных векторов-ошибок, а именно, векторы $\bar{a} + \bar{e}$ для всех $\bar{a} \in C$ и только они.

Доказательство. Пусть S – синдром вектора-ошибки $\bar{e}$ в коде C. Тогда для каждого вектора $\bar{a} \in C$ в силу линейности оператора $\varphi_H : \bar{e} \to S(\bar{e})$ синдром $S(\bar{a} + \bar{e}) = S(\bar{a}) + S(\bar{e}) = \bar{0} + S(\bar{e}) = S(\bar{e})$. Следовательно, не менее q^k векторов-ошибок имеет синдром $\bar{e}$.

С другой стороны, если для векторов-ошибок $\bar{f}$ и $\bar{e}$ $S\left(\bar{f}\right) = S(\bar{e})$, то $S\left(\bar{f} - \bar{e}\right) = 0$. Следовательно, $\bar{f} - \bar{e} = \bar{a} \in C$. Таким образом, $\bar{f} = \bar{a} + \bar{e}$, что и требовалось доказать.

Пусть d – минимальное расстояние кода C. Пусть $t = [d/2]$, если d нечетно, и $t = (d/2) - 1$, если d четно. Пусть $K_{od...t}$ – множество всех векторов весом $1, 2, ..., t$ в пространстве E_n.

Предложение 1.7. Если $\bar{x} \neq \bar{e}$ для $\bar{e} \in K_{od...t}$, но $S(\bar{e}) = S(\bar{x})$, то $w(\bar{x}) \geq d$. Следовательно, для произвольных $\bar{e}_1, \bar{e}_2 \in K_{od...t}$, $\bar{e}_1 \neq \bar{e}_2$, их синдромы попарно различны: $S(\bar{e}_1) \neq S(\bar{e}_2)$.

Доказательство. Пусть $\bar{e} \in K_{od...t}$, а $\bar{x}$ – произвольный вектор ошибок, но $S(\bar{e}) = S(\bar{x})$. Тогда $S(\bar{x} - \bar{e}) = \bar{0}$. Это означает, что вектор $\bar{y} = \bar{x} - \bar{e} \in C$. Согласно пятому свойству расстояния Хэмминга

$$w(\bar{x}) = w(\bar{y} + \bar{e}) \geq w(\bar{y}) - w(\bar{e}) \geq w(\bar{y}) \geq d\ .$$

Предложение 1.7 вместе с очевидной уверенностью, что наиболее вероятны ошибки малого веса, создает теоретическую базу для синдромных методов коррекции ошибок по значениям синдромов ошибок, определяющих соответствующие векторы ошибок из множества $K_{od...t}$.

Выше были рассмотрены два метода коррекции ошибок – метод максимального правдоподобия и табличный. Основные преимущества синдромных методов в следующем:

1) согласно предложению 1.7 синдромы однозначно соответствуют ошибкам декодируемого многообразия;

2) синдромы имеют существенно меньшие размеры по сравнению с кодовыми словами и векторами ошибок (что особенно наглядно для высокоскоростных кодов, например, для кодов Хемминга);

3) для нахождения синдромов не требуется специальных вычислений, кроме обусловленных необходимостью индикации наличия или отсутствия ошибок в принятом блоке-сообщении;

4) синдром совершенно не связан с передаваемой информацией, а исключительно только с произошедшей ошибкой.

В качестве примера рассмотрим синдромное декодирование кодов Хэмминга. Пусть $H = (1, \alpha, ..., \alpha^{2m-2})$ – проверочная матрица кода Хэмминга. Как установлено выше, код Хэмминга имеет минимальное расстояние 3 и может декодировать только одиночные ошибки. Пусть $\bar{e}_i$ – двоичный вектор-ошибка весом 1 с единственной ненулевой i-й координатой. Ясно, что $S(\bar{e}_i) = H \cdot \bar{e}_i^T = \alpha^{i-1}$ – i-й столбец матрицы H, однозначно указывающий на ошибочную координату – единственную ненулевую координату вектора $\bar{e}_i$.

Определение 1.13. Код называется совершенным, если множество его ненулевых синдромов совпадает по мощности с множеством декодируемых ошибок.

Название объясняется тем, что у совершенных кодов синдромная информация об ошибках на 100 % используется для их коррекции. Большинство кодов, конечно же, совершенными не являются. Но примеры таких кодов есть. Очевидно, код Хэмминга относится к разряду совершенных кодов. Другим примером совершенного кода является код Голея. Как установлено выше, он корректирует все ошибки весом 1 – 3, их общее количество равно $C_{23}^1 + C_{23}^2 + C_{23}^3 = 23 + 23 \cdot 11 + 23 \cdot 11 \cdot 7 = 23 \cdot 89 = 2047 = 2^{11} - 1$, что совпадает с общим количеством ненулевых синдромов ошибок в коде Голея.

2. Основы теории БЧХ-кодов

2.1. Необходимые предварительные сведения

К разряду наиболее популярных в теории и практике помехоустойчивого кодирования относятся коды Боуза – Чоудхури – Хоквингема (БЧХ-коды), открытые в начале 60-х гг. XX в.

Общая теория БЧХ-кодов строится над полем $P = GF(q)$ – конечным полем (полем Галуа) из q элементов, где q – произвольное, но фиксированное простое число. Следует, однако, отметить, что реальное (и широчайшее) воплощение в конкретных телекоммуникационных системах получили БЧХ-коды над двоичным полем – полем Галуа $GF(2)$. Для задания конкретного БЧХ-кода C следует зафиксировать значения ряда параметров, характеризующих этот код. В частности, следует определить заранее желательную длину n кода C. Она взаимосвязана с третьим параметром – полем $GF(q^m)$ – конечным полем из q^m элементов: длина n должна быть делителем числа $q^m - 1$ или совпадать с ним.

Хотя поле $GF(q^m)$ единственно, задание элементов поля $GF(q^m)$ при $m > 1$ неоднозначно, требует определенных договоренностей. Известно, что мультипликативная группа $GF(q^m)^*$ поля $GF(q^m)$ циклична, но образующие этой группы – примитивные элементы поля $GF(q^m)$ – определяются неоднозначно, как корни примитивных неприводимых над $GF(q)$ полиномов степени m. Зафиксируем один из таких полиномов – полином

$$p(x) = x^m + a_{m-1}x^{m-1} + ... + a_0,$$

а также корень α этого полинома. Тогда все ненулевые элементы поля $GF(q^m)$ исчерпываются степенями элемента α. Такое задание удобно при умножении – делении в конечном поле. Для сложения – вычитания в поле удобно работать с полиномиальным заданием элементов поля Галуа – как полиномов степени, меньшей m, или алгебраических сумм $b_0 + b_1\alpha + ... + b_{m-1}\alpha^{m-1}$, $b_i \in GF(q)$. Это представление является следствием того факта, что $GF(q)$ можно рассматривать как фактор-кольцо кольца полиномов $(GF(q))[x]$ по максимальному идеалу, порожденному полиномом $p(x)$. Связь между обоими представлениями определяется фундаментальным соотношением

$$\alpha^m = -a_0 - a_1x - ... - a_{m-1}x^{m-1}. \qquad (2.1)$$

Полиномиальное представление убедительно подтверждает, что $GF(q^m)$ действительно является расширением степени m поля $GF(q)$ – векторным пространством над полем $GF(q)$ размерностью m. Полиномиальное представление легко инвертируется в векторное $(b_{m-1}, b_{m-2}, ..., b_0)$ в базисе $\alpha^{m-1}, \alpha^{m-2}, ..., \alpha, 1$.

2.2. Общее определение БЧХ-кодов

Для всякого натурального n, делящего $q^m - 1$, в поле $GF(q^m)$ найдется элемент β порядка n (например, $\beta = \alpha^c$ для $c = (q^m - 1)/n$). Зафиксируем три целых числа: натуральное n, делящее или равное $q^m - 1$, но не делящее $q^s - 1$ для всех целых s, $0 < s < m$, $b > 0$, не делящееся на n, и $\delta > 1$; значение δ должно быть таким, чтобы выполнялось неравенство $m(\delta - 1) < n$.

Определение 2.1. Линейный код C длиной n с проверочной матрицей

$$H = \begin{bmatrix} 1 & \beta^b & \beta^{2b} & \vdots & \beta^{(n-1)b} \\ 1 & \beta^{b+1} & \beta^{2(b+1)} & \vdots & \beta^{(n-1)(b+1)} \\ \hline 1 & \beta^{b+\delta-2} & \beta^{2(b+\delta-2)} & \vdots & \beta^{(n-1)(b+\delta-2)} \end{bmatrix} = [\beta^{bi}, \beta^{(b+1)i}, \ldots, \beta^{(b+\delta-2)i}]^T \quad (2.2)$$

над полем $GF(q)$ называется кодом Боуза – Чоудхури – Хоквингема (БЧХ-кодом) с конструктивным расстоянием δ. При $n = q^m - 1$ БЧХ-код называют примитивным и непримитивным, если $n < q^m - 1$. При $b = 1$ код C называют БЧХ-кодом в узком смысле [2].

В определении не говорится, но подразумевается (как это было и в определении кода Хемминга), что в матрице H каждый элемент $\beta^i = \alpha^{ci}$ заменен на соответствующий вектор-столбец $(b_{m-1}, b_{m-2}, \ldots, b_0)^T$, поэтому код действительно определен над полем $GF(q)$, а матрица H имеет конструктивные размеры $m(\delta - 1) \times n$. Неравенство $m(\delta - 1) < n$ гарантирует, что ядро этой матрицы не тривиально и, следовательно, код C существует, являясь линейным пространством размерностью, не меньшей чем $n - m(\delta - 1)$.

2.3. Спектр значений длин БЧХ-кодов

Отмеченная выше связь длины n БЧХ-кода с порядком мультипликативной группы поля Галуа $GF(q^m)$ ограничивает значения n. Особенно это наглядно при $q = 2$. Среди чисел вида $2^m - 1$ с простым m (называемых числами Мерсенна) особенно много простых, в частности, рекордно больших простых чисел [12, 13]. Тем не менее имеет место следующая

Теорема 2.1. *Для всякого целого числа n, не делящегося на q, над полем $GF(q)$ существует БЧХ-код длиной n. Для всякого нечетного $n \geq 3$ существует двоичный БЧХ-код длиной n.*

Доказательство вытекает из теоремы Эйлера, согласно которой в условиях сформулированной теоремы $q^{\varphi(n)} \equiv 1 (\mathrm{mod}\, n)$. Сравнение означает, что

$q^{\varphi(n)}-1$ делится на n. При этом по свойствам функции Эйлера всегда имеет место неравенство $\varphi(n)<n$. Поэтому по крайней мере для $\delta=1$ БЧХ-код C существует. Теорема доказана.

Замечание. Может оказаться, что найдется такое целое m, удовлетворяющее неравенству $1<m<\varphi(n)$ и для которого q^m-1 делится на n. Тогда спектр значений δ БЧХ-кодов и количество различных БЧХ-кодов длиной n существенно увеличивается.

Пример 2.1. Оценим многообразие двоичных БЧХ-кодов длиной $n=21$. Здесь $\varphi(n)=\varphi(3)\cdot\varphi(7)=12$. Существует $m<12$, а именно, $m=6$, для которого число $2^m-1=2^6-1=63=21\cdot 3$ делится на 21. Таким образом, двоичные БЧХ-коды длиной 21 определены над полем $GF(2^6)$. При этом параметр δ может принимать 3 различных значения – 1, 2 или 3.

Итак, для каждого допустимого значения n существует БЧХ-код длиной n. Но многообразие БЧХ-кодов длиной n, их свойства целиком определяются однозначно связанным с n полем $GF(q^m)$.

Если исходить из поля Галуа, то для $q>2$ и $m>1$ поле $GF(q^m)$ определяет как примитивные, так и непримитивные БЧХ-коды над полем $GF(q)$. Этот факт следует из формул сокращенного умножения [4]:

$a^k-b^k=(a-b)(a^{k-1}+a^{k-2}b+\ldots+ab^{k-2}+b^{k-1})$ для любого натурального k;

$a^k-b^k=(a+b)(a^{k-1}-a^{k-2}b+\ldots+ab^{k-2}-b^{k-1})$ для четных натуральных k.

Приведенные формулы позволяют также обосновать наличие непримитивных двоичных кодов, определяемых полем $GF(2^m)$ с составным m. В силу второй из приведенных формул число 2^m-1 делится на 3 для всех четных натуральных $m=2l$, делится на 5 (и следовательно на 15) для всех $m=4l$, в силу обеих формул – делится на 7 и на 9 (и следовательно делится на 63) для всех натуральных значений $m=6l$. Лишь для простых пар чисел m и 2^m-1 (в частности, 2 и 3, 3 и 7, 5 и 31, 7 и 127, 13 и 8191, 17 и 131071, 19 и 524287, 31 и $2^{31}-1=2\,147\,483\,647$, и т. д.) поле $GF(2^m)$ определяет только примитивные двоичные БЧХ-коды.

2.4. Образующие БЧХ-кодов

Здесь изучим некоторые свойства элементов $\beta\in GF(q^m)$, играющих неотъемлемую роль в определении БЧХ-кодов – в формировании проверочных матриц этих кодов. Они возникают несколько затененно, как степени примитивных элементов. В принципе это естественно, так как мультипликативная

группа $GF(q^m)^*$ циклична. Но такой подход не позволяет сказать что-либо об аддитивных свойствах β.

Теорема 2.2. *Для всякого натурального* n, *являющегося делителем* q^m-1, *но не делящего* q^s-1 *для всех целых* s, $0<s<m$, *элемент* $\beta \in GF(q^m)^*$ *порядка* n *существует. Он является корнем неприводимого непримитивного полинома показателя* n *и степени* m *над полем* $GF(q)$.

Доказательство. Существование β вытекает из факта справедливости обращения теоремы Лагранжа для конечных циклических групп. Поскольку порядок n элемента $\beta \in GF(q^m)^*$ не делит ни одно из чисел q^s-1 для всех целых s, $0<s<m$, то β не может принадлежать ни одному из подполей поля $GF(q^m)$. А это означает, что минимальный полином элемента β – неприводимый полином с корнем β – имеет степень m. По построению элемента показатель этого полинома должен быть не чем иным, как величиной n. Существование таких неприводимых полиномов независимо гарантирует теорема 3.5 из [12]. Теорема доказана.

Пример 2.2. В поле $GF(2^4)$ мультипликативная группа имеет порядок $15=3\cdot 5$. Одним из примитивных элементов этого поля является корень α неприводимого и примитивного над полем $GF(2)$ полинома x^4+x+1.

Элемент $\beta=\alpha^3$ имеет, очевидно, порядок 5 и, следовательно, будет корнем полинома $x^5+1=(x+1)(x^4+x^3+x^2+x+1)$. Но тогда $\beta=\alpha^3$ является корнем полинома $x^4+x^3+x^2+x+1$. Хорошо известно и легко проверяется непосредственно, что последний является неприводимым над $GF(2)$ и непримитивным полиномом с показателем 5.

Пример 2.3. В поле $GF(2^6)$ мультипликативная группа имеет порядок $63=3^2\cdot 7$. Одним из примитивных элементов этого поля является корень α неприводимого и примитивного над полем $GF(2)$ полинома x^6+x+1. Элемент $\beta=\alpha^3$ имеет, очевидно, порядок 21. Непосредственная проверка показывает, $\beta=\alpha^3$ будет корнем неприводимого над $GF(2)$, но не примитивного полинома $x^6+x^4+x^2+x+1$.

Хорошо известно и легко проверяется непосредственно, что над полем $GF(2)$ всего имеется 9 неприводимых полиномов 6-й степени, из них 6 – примитивные и 3 – непримитивные: x^6+x^3+1 – показателя 9, $x^6+x^5+x^4+x^2+1$ и $x^4+x^3+x^2+x+1$ – показателя 21.

Скрытым, но определяющим параметром БЧХ-кодов является неприводимый полином над минимальным полем Галуа $GF(q)$. Если зафиксировать

такой полином $p(x)$, то его степень m определяет промежуточное поле $GF(q^m)$, а показатель полинома n определяет длину кода. Если $p(x)$ примитивен, то и БЧХ-код примитивен, если $p(x)$ непримитивен, то и БЧХ-код непримитивен. Если n существенно больше m, то есть простор для выбора параметров δ и b. Если же $n-m<m$, то имеет смысл работать только с БЧХ-кодами в узком смысле. В любом случае в качестве образующей β берется любой из корней полинома $p(x)$.

2.5. Размерность БЧХ-кода

Размерность линейного кода L длиной n как векторного пространства над полем P при задании этого кода с помощью проверочной матрицы H определяется формулой $k=\dim L=\dim KerH=n-rankH$.

Ранг проверочной матрицы H БЧХ-кода C чаще всего совпадает с числом ее строк $m(\delta-1)$. Но иногда возникают ситуации, когда этот ранг меньше $m(\delta-1)$. Наиболее типичную из таких ситуаций описывает

Теорема 2.3. *Пусть для некоторого целого t, не делящегося на q^m-1, проверочная матрица H БЧХ-кода C содержит с точностью до перестановки строк, подматрицу* $[\beta^{it}, \beta^{itq}]$. *Тогда* $rank\ [\beta^{it}, \beta^{itq}] = rank\ [\beta^{it}]$.

Доказательство. По определению подматрица $[\beta^{it}]$ состоит из векторов-столбцов $(b_0^{it}, b_1^{it}, ..., b_{m-1}^{it})^T$, $b_j^i \in GF(q)$, $0 \le j \le m-1$, $0 \le i \le n-1$, соответствующих отмеченному выше полиномиальному заданию степеней $\beta^l = \alpha^{cl} = b_0^l + b_1^l\alpha + ... + b_{m-1}^l\alpha^{m-1}$. Возведем обе части этого равенства при $l=it$ в q-ю степень. В соответствии со свойствами поля Галуа $GF(q^m)$ получим

$$\beta^{itq} = \alpha^{citq} = (b_0^{it} + b_1^{it}\alpha + ... + b_{m-1}^{it}\alpha^{m-1})^q = b_0^{it} + b_1^{it}\alpha^q + ... + b_{m-1}^{it}\alpha^{(m-1)q}.$$

По тем же полиномиальным соотношениям заменим в правой части полученного равенства степени α, показатели которых превосходят $m-1$. Априори возможно неравенство $p \ge m$. Поэтому в общем случае необходимо сделать подстановку $\alpha^q = \sum_{j=0}^{m-1} b_j^q\alpha^j; ..., \alpha^{(m-1)q} = \sum_{j=0}^{m-1} b_j^{(m-1)q}\alpha^j$. В итоге после приведения подобных членов получим следующее равенство:

$$\beta^{itq} = (b_0^{it} + b_1^{it}b_0^q + ... + b_{m-1}^{it}b_0^{(m-1)q}) + (b_1^{it}b_1^q + ... + b_{m-1}^{it}b_1^{(m-1)q})\alpha +$$

$$... + (b_1^{it}b_{m-1}^q + ... + b_{m-1}^{it}b_{m-1}^{(m-1)q})\alpha^{m-1}.$$

Таким образом, подматрица

$$[\beta^{itq}] = (b_0^{it} + b_1^{it}b_0^q + ... + b_{m-1}^{it}b_0^{(m-1)q}, b_1^{it}b_1^q + ... + b_{m-1}^{it}b_1^{(m-1)q}, b_1^{it}b_{m-1}^q + ... + b_{m-1}^{it}b_{m-1}^{(m-1)q})^T,$$

где $0 \le i \le n-1$. Как видим, каждая из строк этой подматрицы есть линейная комбинация строк подматрицы $[\beta^{it}]$. Это и означает, что имеет место равенство рангов $rank\ [\beta^{it}, \beta^{itq}] = rank\ [\beta^{it}]$. Теорема доказана.

Замечание. Теорема остается справедливой, если в подматрице $[\beta^{it}, \beta^{itq}]$ степень itq заменить на $f(s) = itq^s$ для целых s, $1 \le s \le m-1$.

Выяснением равенства $H \cdot \bar{x}^T = \bar{0}$ устанавливается принадлежность $\bar{x}$ данному коду. Все декодеры телекоммуникационных цифровых систем реализуют проверку этого соотношения. Вычисления происходят быстро, синхронно с поступлением информации. Поэтому эти вычисления должны требовать минимум временных затрат. В силу сказанного матрица H должна быть минимально сложной, в частности, не содержать линейно зависимых строк – такие из матрицы H следует удалять. Из указанного обстоятельства и возникло условие: ранг проверочной матрицы кода равен числу ее строк.

Ситуация, указанная теоремой 2.3, чаще всего возникает при $b = 1$. Наиболее типична она для двоичных кодов, когда $q = 2$. Поэтому после удаления линейно зависимых строк проверочная матрица БЧХ-кода в узком смысле в данном случае и для $\delta = 2t$, и для $\delta = 2t+1$ имеет один и тот же вид:

$$H = (\beta^i, \beta^{3i}, ..., \beta^{(2t-1)i})^{\mathrm{T}},\ 0 \le i \le n-1. \qquad (2.3)$$

Истинная размерность данного БЧХ-кода $k \le n - tm$, что существенно больше конструктивной размерности $n - m(\delta - 1)$.

В отличие от примитивных у непримитивных БЧХ-кодов наличие условий теоремы 2.3, точнее, условий из замечания 2, не всегда наглядно, требует определенных вычислений. Следует помнить, что элементы $\beta^{it}, \beta^{itq}, \beta^{f(s)}$ являются сопряженными в поле Галуа $GF(q^m)$, а их показатели it, itq, itq^s принадлежат одному циклотомическому классу по модулю n. Поэтому для оценки размерности БЧХ-кода C, задаваемого формулой (2.2), необходимо выписать циклотомические классы по модулю n, порождаемые числами $b, b+1, ..., b+\delta-2$, и найти совпадающие классы. Наличие совпадающих циклотомических классов означает, что истинный ранг матрицы H меньше конструктивного ранга и мы можем уменьшить число строк матрицы (2.2).

Пример 2.4. Поле $GF(2^9)$ порождает как примитивные БЧХ-коды, так и непримитивные коды длиной 73, поскольку $2^9 - 1 = 511 = 7 \cdot 73$. Причем у последних параметр δ может меняться в довольно широком диапазоне от 1 до 9, а для БЧХ-кодов в узком смысле – в диапазоне от 1 до 17 (тогда в силу формулы (2.3) параметр t меняет свои значения от 1 до 8). Оценим с помощью теоремы 2.2 и замечания к нему размерность двоичного БЧХ-кода в узком смысле длиной 73 и с $\delta = 9 = 2 \cdot 4 + 1$, т. е. кода с проверочной матрицей $H = (\beta^i, \beta^{3i}, \beta^{5i}, \beta^{7i})^T$ для $\beta = \alpha^7$ и примитивного элемента α поля $GF(2^9)$. Как указано выше, выпишем

циклотомические классы по модулю 73 чисел 1, 3, 5, 7:

$$C_1 = \{1, 2, 4, 8, 16, 32, 64, 55, 37\};\ \ C_3 = \{3, 6, 12, 24, 48, 23, 46, 19, 38\};$$
$$C_5 = \{5, 10, 20, 40, 7, 14, 28, 56, 39\} = C_7.$$

Из построенных классов видим, что $\beta^7 = (\beta^5)^{16}$. Согласно теореме 2.2 $rankH \le 3 \cdot 9 = 27$ вместо конструктивного ранга 36.

Пример 2.5. Над полем $GF(2^{14})$ имеются непримитивные БЧХ-коды длиной 43, поскольку $2^{14} - 1 = 16\,383 = 3 \cdot 43 \cdot 127$. Из них БЧХ-коды в узком смысле могут иметь значения параметра t от 1 до 3. Такой код с параметром $t = 3$ задается проверочной матрицей $H = (\beta^i, \beta^{3i}, \beta^{5i})^T$ для примитивного элемента α поля $GF(2^{14})$ и $\beta = \alpha^{381}$. Выпишем циклотомические классы по модулю 43 чисел 1, 3, 5:

$$C_1 = \{1, 2, 4, 8, 16, 32, 21, 42, 41, 39, 35, 27, 11, 22\};$$
$$C_3 = \{3, 6, 12, 24, 5, 10, 20, 40, 37, 31, 19, 38, 33, 23\} = C_5.$$

Матрица H содержит 42 строки. Проведенные вычисления показывают, что $rankH \le 2 \cdot 14 = 28$.

Пожалуй, наиболее эффектным здесь является пример следующего кода, свойства которого исследовались в [1, 6].

Пример 2.6. Над полем $GF(2^{11})$ имеются непримитивные БЧХ-коды длиной 23, поскольку $2^{11} - 1 = 2047 = 23 \cdot 89$. Из них БЧХ-коды в узком смысле могут иметь значения параметра t от 1 до 2. Такой код с параметром $t = 2$ задается проверочной матрицей $H = (\beta^i, \beta^{3i})^T$ для примитивного элемента α поля $GF(2^{11})$ и $\beta = \alpha^{89}$. Выпишем циклотомические классы по модулю 23 чисел 1 и 3: $C_1 = \{1, 2, 4, 8, 16, 9, 18, 13, 3, 6, 12\} = C_3$. Следовательно, матрица $H = (\beta^i, \beta^{3i})^T$ эквивалентна матрице $(\beta^i)^T$ и ранг ее меньше или равен 11. На самом деле $rankH = 11$. Это гарантирует

Теорема 2.4. *У проверочной матрицы (2.3) БЧХ-кода C над полем $GF(q^m)$ длиной n ранг подматрицы $[\beta^i]$ равен m. Если целые числа $b + j$ или s взаимно просты с n, то ранги подматриц $[\beta^{(b+j)i}]$ в матрице (2.2) или $[\beta^{si}]$ в матрице (2.3) также равны m.*

Доказательство. Поскольку элемент $\beta \in GF(q^m)$ является корнем неприводимого полинома степени m, то его степени $1, \beta, ..., \beta^{m-1}$ образуют линейно независимую систему векторов над полем $GF(q)$. Следовательно, соответствующие столбцы подматрицы $[\beta^i]$ матрицы (2.3) или (2.2) также образуют линейно независимую систему. Поэтому $rank[\beta^i] = m$. Если целое число s взаимно просто с n, то возведение в s-ю степень элементов циклической группы

$< \beta >$, порожденной элементом β, есть автоморфизм этой группы, поскольку $\text{НОД}(s, n) = 1$ (теорема 2.12.3 [7]). Это означает, что подматрицы $[\beta^{(b+j)i}]$ и $[\beta^{si}]$ представляют собой перестановки элементов (т. е. столбцов) подматрицы $[\beta^{i}]$. Перестановка столбцов матрицы относится к разряду ее элементарных преобразований и, разумеется, ранга не меняет. Теорема доказана.

Замечание. Установление точных значений размерности БЧХ-кодов или, по-другому, количества информационных разрядов – это открытая нерешенная проблема теории помехоустойчивого кодирования. В каждом конкретном случае она решается непосредственными вычислениями с привлечением компьютера.

2.6. Минимальное расстояние БЧХ-кода

Истинное кодовое расстояние БЧХ-кода C есть величина $d \geq \delta$ [1, гл. 9, т. 1]. Для определения кодового расстояния линейного кода имеется ряд подходов. Один из них приведен в теореме 1.6. Конечно, реальная проверка условий этой теоремы, за исключением наглядных случаев, представляет громоздкую комбинаторную процедуру.

Другой метод определения минимального расстояния обеспечивает таблица или диаграмма весов кодовых слов данного линейного кода (см. подразд. 1.9). Конечно, построение таблицы весов кодовых слов – также достаточно трудоемкая задача, требующая серьезных компьютерных ресурсов. Для определения кодового расстояния достаточно построить лишь ее фрагмент, содержащий слова наименьшего веса. Но и этого добиться в реальных кодах не просто.

Третий подход к определению минимального расстояния линейного кода предоставляет теория синдромов (см. подразд. 1.10). Из доказанных в подразд. 1.10 предложений и следствий вытекает синдромный метод определения кодового расстояния данного линейного кода L над полем P.

Вычисляются синдромы векторов-ошибок, последовательно наращивая их вес от 1 до такого значения t, что все векторы-ошибки весом t и меньше имеют попарно различные синдромы, но существуют векторы весом t и $t+1$ с одинаковыми синдромами, тогда минимальное расстояние кода L равно $d = 2t+1$. Если все векторы весом t и $t-1$, а также меньших весов имеют попарно различные синдромы, но существуют по меньшей мере 2 вектора весом t с одинаковыми синдромами, то тогда минимальное расстояние кода L равно $d = 2t$.

Синдромный метод существенно проще предыдущего, так как задача генерировать векторы данного веса не является проблемой в отличие от проблемы формирования кодовых слов. Тем не менее для кодов с большим минимальным расстоянием он приводит к достаточно громоздкой переборной процедуре.

Для БЧХ-кодов можно предложить четвертый – норменный метод определения кодового расстояния. Его основу составляет теория норм синдромов [8, 9], наиболее полно разработанная для БЧХ-кодов.

2.7. Синдромное декодирование примитивных БЧХ-кодов с минимальным расстоянием 5

Здесь рассматривается классический примитивный БЧХ-код C с проверочной матрицей $H = (\alpha^i, \alpha^{3i})^T$, $0 \le i \le n-1$, α – примитивный элемент поля Галуа $GF(2^m)$, $n = 2^m - 1$. Его кодовое расстояние равно 5, $k = n - 2m$. Следовательно, этот код корректирует одиночные и двойные ошибки.

Пусть при передаче вектора-сообщения $\bar{c}$ в цифровой системе связи с данным кодом C на сообщение наложился вектор-ошибка $\bar{e} = (i, j)$ весом 2 с ненулевыми координатами на неизвестных позициях i и j. Это означает, что приемное устройство связи приняло сообщение $\bar{x} = \bar{c} + \bar{e}$. В соответствии со свойствами и структурой матрицы H синдром $S(\bar{x}) = S(\bar{e}) = (s_1, s_2)$, где $s_1 = \alpha^{i-1} + \alpha^{j-1}$; $s_2 = \alpha^{3(i-1)} + \alpha^{3(j-1)}$. Величины α^{i-1} и α^{j-1} пока неизвестные элементы поля Галуа $GF(2^m)$. Обозначим их через x и y соответственно. Эти величины – решения системы уравнений

$$\begin{cases} x + y = s_1, \\ x^3 + y^3 = s_2. \end{cases} \qquad (2.4)$$

Преобразуем второе уравнение этой системы.

$$x^3 + y^3 = (x + y)(x^2 + xy + y^2) = s_1(s_1^2 + xy) = s_2.$$

Следовательно, $xy = s_2 s_1^{-1} + s_1^2$. Правую часть полученного равенства обозначим через a. Таким образом, система преобразована к виду $\begin{cases} x + y = s_1, \\ xy = a. \end{cases}$

Согласно теореме Виета корни x, y системы являются корнями квадратного уравнения $t^2 + s_1 t + a = 0$. Решив уравнение, найдем $x = \alpha^{i-1}, y = \alpha^{j-1}$, а с ними и вектор-ошибку $\bar{e} = (i, j)$.

Конечные поля имеют многочисленные приложения. Без них немыслимо функционирование практически всех цифровых систем связи.

Пример 2.7. В системе связи, построенной на основе БЧХ-кода C с проверочной матрицей $H = (\alpha^i, \alpha^{3i})^T$, $0 \le i \le 14$, α – примитивный элемент поля Галуа $F(16)$, корень полинома $x^4 + x + 1$, принято сообщение $\bar{x} = (111011110110101)$. Выяснить наличие ошибок в этом сообщении и попытаться их исправить.

Решение задачи. Для проведения вычислений необходимо иметь под рукой сформированное поле Галуа из 16 элементов, а именно, таблицу степеней α – корня полинома $x^4 + x + 1$, и их полиномиальных эквивалентов. Все кодовые слова $\bar{c} \in C$ (и только они) составляют ядро проверочной матрицы

$H \cdot (\overline{c}^T) = \overline{0}$. Если $\overline{S} = H(\overline{x}^T) \neq \overline{0}$, то сообщение $\overline{x}$ явно содержит ошибки. В данном случае $\overline{S} = (s_1, s_2)^T$, где

$$s_1 = 1 + \alpha + \alpha^2 + \alpha^4 + \alpha^5 + \alpha^6 + \alpha^7 + \alpha^9 + \alpha^{10} + \alpha^{12} + \alpha^{14} = \alpha^{11};$$

$$s_2 = 1 + \alpha^3 + \alpha^6 + \alpha^{12} + \alpha^{15} + \alpha^{18} + \alpha^{21} + \alpha^{27} + \alpha^{30} + \alpha^{36} + \alpha^{42} = \alpha.$$

Таким образом, полученное сообщение $\overline{x}$ содержит ошибки.

Данный код исправляет двойные ошибки. Для нахождения такой ошибки имеем следующую систему уравнений: $\begin{cases} x + y = \alpha^{11}, \\ x^3 + y^3 = \alpha. \end{cases}$

Данная система сводится к квадратному уравнению. Действительно, $x^3 + y^3 = (x + y)(x^2 + xy + y^2) = \alpha^{11}(\alpha^{22} + xy) = \alpha$. Отсюда получаем $xy = \alpha^{22} + \alpha / \alpha^{11} = \alpha^7 + \alpha^5 = \alpha^{13}$. Замена $y = x + \alpha^{11}$ приводит это уравнение к следующему квадратному уравнению $x^2 + \alpha^{11}x + \alpha^{13} = 0$. После замены $x = \alpha^{11}t$ данное квадратное уравнение приводим к каноническому виду $t^2 + t + \alpha^5 = 0$. Нетрудно проверить, что след $Tr(\alpha^5) = 0$ и, следовательно, уравнение имеет решения в поле $F(16)$. Непосредственным подбором (методом Чэня) можно убедиться, что корнями являются $t_1 = \alpha$, $t_2 = \alpha + 1 = \alpha^4$. Тогда $y = \alpha^{11}\alpha = \alpha^{12}$; $y = \alpha^{12} + \alpha^{11} = \alpha^0 = 1$. Таким образом, ошибочными в принятом сообщении являются 1-я и 13-я позиции и правильным является сообщение $\overline{c}_0 = (011011110110001)$.

2.8. Реверсивные коды

Реверсивные коды относятся к разряду модифицированных БЧХ-кодов.

Определение 2.2. Реверсивным называется код C_R^m, который задается проверочной матрицей $H = (H_1, H_2)^T = (\alpha^i, \alpha^{-i})^T$, где α – примитивный элемент поля $GF(2^m)$, $m \geq 3$; $0 \leq i \leq n-1$ для $n = 2^m - 1$.

Как и в определении БЧХ-кода, каждый элемент матрицы H есть двоичный m-разрядный вектор. Таким образом, H – это двоичная $(2m \times n)$-матрица, ранг которой, очевидно, равен $2m$.

В проверочной матрице $H = (H_1, H_2)^T = (\alpha^i, \alpha^{-i})^T$, реверсивного кода C_R^m подматрица H_1 совпадает с такой же подматрицей проверочной матрицы БЧХ-кода из подразд. 2.7, а вторая подматрица H_2 представляет собой запись элементов первой строки, но в обратном порядке. Поэтому такой код и называют реверсивным.

В соответствии со структурой матрицы H двоичные координаты вектора-синдрома $\overline{S}$ произвольной ошибки в реверсивном коде сгруппируем после-

довательно в две группы по m координат в каждой. Тогда вектор $\overline{S}$ можно записать в виде $\overline{S} = (s_1, s_2)^T$, где s_1 и s_2 – элементы поля $GF(2^m)$. Следовательно, $s_1 = \alpha^i$, $s_2 = \alpha^j$ для подходящих i, j из множества $T = \{-\infty, 0, 1, 2, ..., n-1\}$. Таким образом, вектор $\overline{S}$ может принимать $(n+1)^2 = 2^{2m}$ различных значений.

По построению проверочной матрицы код C_R^m должен иметь конструктивное расстояние 5 и, следовательно, исправлять двойные ошибки. Для определения координат двойной ошибки здесь аналог системы (2.4) имеет следующий вид:

$$\begin{cases} x + y = s_1, \\ 1/x + 1/y = s_2. \end{cases} \tag{2.5}$$

Левую часть второго уравнения приведем к общему знаменателю, т. е. к виду $(x+y)/xy = s_2$. Легко видеть, что здесь синдром любой двойной ошибки имеет ненулевые компоненты s_1, s_2. Поэтому с учетом первого уравнения имеем $xy = s_1/s_2 = b.$ Становится ясным, что компоненты решения системы (2.5) по теореме Виета совпадают с корнями квадратного уравнения:

$$x^2 + s_1 x + b = 0. \tag{2.6}$$

В отличие от БЧХ-кодов здесь ситуация несколько хуже.

Теорема 2.5. *При четных значениях $m = 2\mu$ реверсивный код C_R^m имеет минимальное расстояние 3.*

Доказательство. В системе (2.5) переменные x и y принимают любые значения из мультипликативной группы $GF(2^m)^*$. В частности, может получиться случай $y = 1/x.$ Тогда система (2.5) приобретает вид

$$\begin{cases} x + 1/x = s_1, \\ 1/x + x = s_2. \end{cases} \tag{2.7}$$

В силу симметричности система (2.7) может иметь решение только в случае, когда $s_2 = s_1 \neq 0.$ Однако при $s_2 = s_1 = 1$ оба уравнения системы (2.7) преобразуются в уравнение $x^2 + x + 1 = 0.$ В полях Галуа $GF(2^m)$ с нечетным m след $Tr1 = 1.$ По критерию разрешимости квадратных уравнений в полях Галуа характеристики 2 [2, 13] такое значение следа означает, что уравнение $x^2 + x + 1 = 0$ в поле $GF(2^m)$ решений не имеет. Это означает, что в кодах C_R^m с нечетным m отсутствует двойная ошибка с синдромом $S = (s_1, s_2) = (1, 1)$. Во всех кодах C_R^m имеется одиночная вектор-ошибка с таким синдромом – это вектор $\bar{e}_1 = (1, 0, ..., 0)$, однако в кодах C_R^m с четным m след $Tr1 = 0$ и уравнение $x^2 + x + 1 = 0$ в поле $GF(2^m)$ имеет решения. Их легко найти. Действительно, умножив рассматриваемое уравнение на $x - 1$, получим уравнение $x^3 - 1 = 0.$

Его корни – кубические корни из 1 – в полях $GF(2^{2r})$ имеются. Ведь порядок циклической группы $GF(2^m)^*$ поля $GF(2^m)$ делится на 3 $\left|GF(2^{2r})^*\right| = 2^{2r} - 1 = (2^r - 1)\cdot(2^r + 1)$, а среди трех последовательных натуральных чисел $(2^r - 1), 2^r, (2^r + 1)$ непременно найдется делящееся на три, этим числом заведомо не является 2^r, следовательно, или $2^r - 1$ или $2^r + 1$ обязательно поделится на 3. Таким образом, $2^{2r} - 1 = 3q$ для подходящего натурального q. Отсюда следует, что α^q, α^{2q} – различные и не равные 1 кубические корни из 1 поля $GF(2^{2r})$, а следовательно, искомые корни уравнения $x^2 + x + 1 = 0$. Отсюда следует: в коде C_R^{2r} и одиночная ошибка $\overline{e}_1 = (1, 0, ..., 0)$, и двойная ошибка $\overline{e}_{q,2q}$ на позициях q и $2q$ имеют одинаковый синдром, код C_R^{2r} их различить и откорректировать не может, другими словами, код C_R^{2r} исправляет только одиночные ошибки, т. е. имеет минимальное расстояние 3. Теорема доказана.

Из теоремы следует, что перспективным для приложений является реверсивный код C_R^{2r+1}, который может исправлять двойные ошибки, в общей сложности $C_n^1 + C_n^2 = \dfrac{n(n+1)}{2}$ различных ошибок.

Пример 2.8. Пусть в реверсивном коде C_R^5, проверочная матрица которого построена с помощью примитивного элемента α – корня неприводимого полинома $x^5 + x^3 + x^2 + x + 1$, получено сообщение

$$\overline{x} = (101\,101\,101\,100\,000\,000\,100\,000\,100\,1000).$$

Показать наличие в этом сообщении ошибок и устранить их.

Решение. Вычислим $\overline{S} = H \cdot \overline{x}^T$. Получим $\overline{S} = (\alpha^3, \alpha^6)^T \neq \overline{0}$. Следовательно, сообщение $\overline{x}$ содержит ошибки. Для их определения имеем следующее уравнение (2.6): $x^2 + \alpha^3 x + \alpha^{28} = 0$. Заменой $x = \alpha^3 t$ приведем его к каноническому виду $t^2 + t + \alpha^{22} = 0$. Вычисления показывают, что след $Tr(\alpha^{22}) = 0$. Значит, уравнение имеет корни в поле $GF(2^5)$. Найдем их по формулам Чэня. Для этого необходимо α^{22} задать в нормальном базисе. Несложно убедиться в том, что $Tr(\alpha^7) = 1$ и что система элементов $\alpha^7, \alpha^{14}, \alpha^{28}, \alpha^{25}, \alpha^{19}$ образует нормальный базис. Следовательно, существуют такие $d_1, d_2, d_3, d_4, d_5 \in GF(2) = Z/2Z$, что выполняется равенство $d_1\alpha^7 + d_2\alpha^{14} + d_3\alpha^{28} + d_4\alpha^{25} + d_5\alpha^{19} = \alpha^{22}$. Данное соотношение превращается в крамеровскую систему линейных уравнений с двоичными коэффициентами. В матричной форме эта система уравнений имеет вид

$$\left(\begin{array}{ccccc|c} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \end{array}\right).$$

Данная система имеет единственное решение:

$$d_1 = 1; d_2 = 0; d_3 = 1; d_4 = d_5 = 0.$$

Тогда согласно формулам Чэня

$$t_1 = d_2\alpha^{14} + (d_2 + d_3)\alpha^{28} + (d_2 + d_3 + d_4)\alpha^{25} + (d_2 + d_3 + d_4 + d_5)\alpha^{19} = \alpha^6;$$

$$t_2 = t_1 + 1 = \alpha^{16}.$$

Следовательно, $x_1 = \alpha^3 \cdot \alpha^6 = \alpha^9$; $x_2 = \alpha^3 \cdot \alpha^{16} = \alpha^{19}$. Таким образом, принятое сообщение $\bar{x}$ содержит двойную ошибку на 10-й и 20-й позициях, а правильным является сообщение

$$\bar{c} = (101\,101\,101\,000\,000\,000\,110\,000\,100\,1000).$$

2.9. Синдромное декодирование произвольных примитивных БЧХ-кодов

Примитивный двоичный БЧХ-код C_{2t+1}, исправляющий $t \geq 1$ случайных ошибок, задается над полем Галуа $GF(2^m)$ проверочной матрицей

$$H = (\alpha^i, \alpha^{3i}, ..., \alpha^{(2t-1)i})^T, \qquad (2.8)$$

где α – фиксированный примитивный элемент поля $GF(2^m)$, параметр i принимает целые значения в пределах от 0 до $n-2$ для $n = 2^m - 1$. Предполагается, что каждый элемент матрицы H есть двоичный столбец из m элементов 0 или 1 – координат соответствующей степени α^j как вектора пространства $GF(2^m)$ над полем $GF(2)$ в базисе $1, \alpha, ..., \alpha^{m-1}$. Поскольку ядром матрицы H является весь код C – ненулевое k-мерное подпространство в двоичном n-мерном пространстве, то ранг матрицы H, по построению равный tm, должен быть существенно меньше n. Таким образом, при задании кода автоматически должно выполняться строгое неравенство $tm < n$. Конструктивное кодовое расстояние такого БЧХ-кода $\delta = 2t + 1$, отсюда следует мотивация обозначения данного кода через C_{2t+1}. Как уже отмечалось, реальное кодовое расстояние $d \geq \delta$.

Проверочная матрица кода по своему названию проверяет наличие ошибок в принятом блоке-сообщении $\bar{x}$ – двоичном векторе длиной n, т. е. с n координатами, принимающими значения 0 или 1. Проверка эта осуществляется вычислением вектора $S = H \cdot \bar{x}^T$. Это также двоичный вектор, но с tm координатами, известный в теории помехоустойчивых кодов под названием синдрома

ошибок. В соответствии со структурой матрицы H эти координаты можно последовательно сгруппировать в t групп по m последовательных координат в каждой. Таким образом, $S=(s_1,s_2,...,s_t)$, где каждую координату s_i можно интерпретировать как элемент поля $GF(2^m)$. Как уже отмечалось, $S=\bar{0}$ тогда и только тогда, когда $\bar{x}$ является кодовым словом. Следовательно, неравенство $S\neq\bar{0}$ означает наличие ошибки в принятом сообщении $\bar{x}$. Точнее, означает, что $\bar{x}=\bar{c}+\bar{e}$, где $\bar{c}$ – истинное кодовое слово, $\bar{e}$ – вектор ошибок – результат влияния на $\bar{c}$ в канале передачи информации разного рода шумов и помех. В соответствии с декодирующими возможностями данного БЧХ-кода вектор $\bar{e}$ может содержать до t ненулевых и, следовательно, равных единице координат.

Пусть $x_1,x_2,...,x_t$ – локаторы ошибочных позиций принятого сообщения $\bar{x}$. Это элементы первой строки матрицы H как матрицы с элементами из поля $GF(2^m)$, соответствующие ошибочным позициям. Покоординатная запись векторного равенства $S=H\cdot\bar{x}^T$ приводит к следующей системе уравнений:

$$\begin{cases} x_1+x_2+...+x_t=s_1, \\ x_1^3+x_2^3+...+x_t^3=s_2, \\ ..... \\ x_1^{2t-1}+x_2^{2t-1}+...+x_t^{2t-1}=s_t \end{cases} \tag{2.9}$$

Если систему (2.8) удастся решить относительно неизвестных $x_1,x_2,...,x_t$, то координаты вектора ошибок $\bar{e}$ будут однозначно определены и будет найдено истинное сообщение $\bar{c}=\bar{x}+\bar{e}$. При $t=2$ система (2.8) легко сводится к квадратному уравнению и решается. При $t\geq 3$ следует воспользоваться теорией симметрических полиномов. Дело в том, что левые части уравнений системы (2.5) можно рассматривать как симметрические многочлены от t неизвестных. Симметрические многочлены – это полиномы, не меняющиеся при любой перестановке местами переменных [2], т. е. инвариантные относительно группы подстановок – симметрической группы. В высшей алгебре построена специальная теория симметрических полиномов. Фундаментальный результат этой теории гласит, что любой симметрический полином можно выразить единственным образом в виде полинома от элементарных симметрических полиномов.

Определение 2.3. Следующие n симметрических многочленов от n неизвестных называются элементарными симметрическими многочленами:

$$\begin{cases} \sigma_1=x_1+x_2+...+x_n, \\ \sigma_2=x_1x_2+x_1x_3+...+x_{n-1}x_n, \\ ..... \\ \sigma_{n-1}=x_1x_2\cdot...\cdot x_{n-1}+x_1x_2\cdot...\cdot x_{n-2}x_n+...+x_2x_3\cdot...\cdot x_n, \\ \sigma_n=x_1x_2\cdot...\cdot x_n. \end{cases}$$

Для степенных сумм $f_k = x_1^k + x_2^k + ... + x_n^k,\ k = 1, 2, ...,$ еще Ньютоном установлены следующие рекуррентные формулы:

$$f_k - f_{k-1}\sigma_1 + f_{k-2}\sigma_2 - ... + (-1)^{k-1} f_1\sigma_{k-1} + (-1)^k k\sigma_k = 0, \quad k \le n, \qquad (2.10)$$

$$f_k - f_{k-1}\sigma_1 + f_{k-2}\sigma_2 - ... + (-1)^n f_{k-n}\sigma_n = 0, \quad k > n. \qquad (2.11)$$

Эти формулы позволяют последовательно выражать степенные суммы через элементарные симметрические полиномы. Очевидно, $f_1 = \sigma_1$. Формула (2.10) при $k = 2 \le n$ имеет вид $f_2 - f_1\sigma_1 + 2\sigma_2 = 0$. Следовательно, $f_2 = \sigma_1^2 - 2\sigma_2$. Формула (2.10) при $k = 3 \le n$ имеет более сложный вид: $f_3 - f_2\sigma_1 + f_1\sigma_2 - 3\sigma_3 = 0$. Подстановкой в это уравнение найденных значений для f_1 и f_2 получаем $f_3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3$. Продолжая аналогичным образом, можно получить выражение через элементарные симметрические полиномы любой конкретной степенной суммы f_k.

Для обработки БЧХ-кодов все эти вычисления необходимо проводить в поле $GF(2^m)$ – поле характеристики 2. Здесь $1+1=0$. Поэтому формулы несколько меняются. Здесь $f_2 = \sigma_1^2;\quad f_3 = \sigma_1^3 + \sigma_1\sigma_2 + \sigma_3;\quad f_4 = \sigma_1^4$. Выражение для f_5 зависит от $t = n$, если $n > 5$, то для выражения f_5 через элементарные симметрические многочлены применяем формулу (2.10), в противном случае – формулу (2.11).

Предположим, что мы применяем БЧХ-код C_7, исправляющий тройные ошибки, т. е. код с параметром $t = 3$. Тогда для исправления тройных ошибок необходимо решать следующий более простой аналог системы (2.9):

$$\begin{cases} x_1 + x_2 + x_3 = s_1, \\ x_1^3 + x_2^3 + x_3^3 = s_2, \\ x_1^5 + x_2^5 + x_3^5 = s_3. \end{cases} \qquad (2.12)$$

В данном случае для выражения f_5 через элементарные симметрические многочлены следует воспользоваться формулой (2.11). В таком случае $f_5 = f_4\sigma_1 + f_3\sigma_2 + f_2\sigma_3 = \sigma_1^5 + (\sigma_1^3 + \sigma_1\sigma_2 + \sigma_2)\sigma_2 + \sigma_1^2\sigma_3$. И так далее.

Посмотрим, однако, на соотношения (2.10) – (2.11) в противоположном направлении – как на соотношения для определения элементарных симметрических полиномов. Фактически уравнения (2.9) и (2.12) определяют значения степенных сумм f_k. Тогда уравнения (2.10) – (2.11) определяют систему линейных уравнений для нахождения σ_k. Так, для БЧХ-кода C_7 эта система линейных уравнений имеет вид

$$\begin{cases} \sigma_1 = f_1 = s_1, \\ f_2\sigma_1 + f_1\sigma_2 + \sigma_3 = f_3 = s_2, \\ f_4\sigma_1 + f_3\sigma_2 + f_2\sigma_3 = f_5 = s_3 \end{cases} \quad \text{или} \quad \begin{cases} \sigma_1 = s_1, \\ s_1^2\sigma_1 + s_1\sigma_2 + \sigma_3 = s_2, \\ s_1^4\sigma_1 + s_2\sigma_2 + s_1^2\sigma_3 = s_3. \end{cases} \tag{2.13}$$

В работах [3, 4] систему (2.9) предлагается решать по правилу Крамера. Она настолько проста, что можно применить прямой путь исключения неизвестных.

Аналог системы (2.9) можно выписать для любого $t \geq 3$ с помощью тех же формул (2.6) – (2.7) и системы (2.5). Для решения получаемых систем линейных алгебраических уравнений (СЛАУ) разработан ряд методов, как классических, так и специальных – над полями Галуа. Такие специальные методы решения СЛАУ рассматриваются, например, в последней, одиннадцатой главе монографии [5].

Предположим, мы решили такую систему уравнений и нашли значения элементарных симметрических многочленов $\sigma_1 = \sigma_1^0, \sigma_2 = \sigma_2^0, ..., \sigma_t = \sigma_t^0$. Этой информацией мы можем воспользоваться для нахождения координат ошибочных позиций принятого с помощью БЧХ-кода C_{2t+1} сообщения $\bar{x}$. Идея эта базируется на следующей знаменитой классической теореме о связи корней алгебраических уравнений с коэффициентами этих уравнений.

Теорема 2.6 (теорема Виета). *Пусть в уравнении*

$$x^t + \sigma_1^0 x^{t-1} + ... + \sigma_t^0 = 0 \tag{2.14}$$

коэффициенты принадлежат полю F. Элементы $x_1, x_2, ..., x_t$ поля F являются корнями данного уравнения тогда и только тогда, когда

$$\begin{cases} x_1 + x_2 + ... + x_t = -\sigma_1^0, \\ x_1x_2 + x_1x_3 + ... + x_{t-1}x_t = \sigma_2^0, \\ ..... \\ x_1x_2 \cdot ... \cdot x_{t-1} + x_1x_2 \cdot ... \cdot x_{n-2}x_t + ... + x_2x_3 \cdot ... \cdot x_t = (-1)^{t-1}\sigma_{t-1}^0, \\ x_1x_2 \cdot ... \cdot x_t = (-1)^t\sigma_t^0. \end{cases} \tag{2.15}$$

Теорему Виета будем применять следующим образом. По найденным $\sigma_1 = \sigma_1^0, \sigma_2 = \sigma_2^0, ..., \sigma_t = \sigma_t^0$ в силу соотношений (2.11) составляем уравнение (2.10), называемое уравнением локаторов ошибок. Алгебраические уравнения над полями Галуа $GF(2^m)$, как отмечено в [6, 7], проще всего решать методом Чэня, т. е. последовательной подстановкой в уравнение элементов данного поля. Найдя корни $x_1 = x_1^0$, $x_2 = x_2^0, ..., x_t = x_t^0$, мы однозначно определяем вектор $\bar{e}$ и, следовательно, исправляем принятое сообщение.

Пример 2.9. В системе связи, построенной на основе примитивного БЧХ-кода C_7 длиной 63 с проверочной матрицей $H = (\alpha^i, \alpha^{3i}, \alpha^{5i})^T$, $0 \leq i \leq 62$,

α – примитивный элемент поля Галуа $F(16)$, корень неприводимого полинома $x^6 + x^5 + x^4 + x + 1$, принято сообщение $\bar{x}$ с синдромом $\bar{S} = \bar{S}(\bar{x}) = (\alpha^{21}, \alpha^{44}, \alpha^{27})^T$. Выяснить наличие ошибок в этом сообщении и попытаться их исправить.

Решение. Система линейных уравнений (2.13) здесь имеет вид

$$\begin{cases} \sigma_1 = s_1 = \alpha^{21}, \\ \alpha^{42} \cdot \alpha^{21} + \alpha^{21} \cdot \sigma_2 + \sigma_3 = \alpha^{44}, \\ \alpha^{84} \cdot \alpha^{21} + \alpha^{44}\sigma_2 + \alpha^{42}\sigma_3 = \alpha^{27} \end{cases} \quad \text{или} \quad \begin{cases} \sigma_1 = \alpha^{21}, \\ \alpha^{21}\sigma_2 + \sigma_3 = \alpha^{12}, \\ \alpha^{44}\sigma_2 + \alpha^{42}\sigma_3 = \alpha^{29}. \end{cases}$$

Несложные вычисления показывают, что здесь $\sigma_2 = \alpha^{41}$; $\sigma_3 = \alpha^{60}$. Теперь можно составить уравнение (2.10): $x^3 + \alpha^{21}x^2 + \alpha^{41}x + \alpha^{60} = 0$. Кропотливые вычисления методом Чэня позволяют найти следующие корни этого уравнения: $x_1 = \alpha^{10}$; $x_2 = \alpha^{20}$; $x_3 = \alpha^{30}$. Следовательно, в принятом сообщении имеется тройная ошибка на 11, 21 и 31-й позициях.

В заключение заметим, что представленный синдромный метод декодирования не лишен недостатков. В его реализации имеются такие громоздкие этапы, как нахождение коэффициентов уравнения (2.10) и его решение переборным методом Чэня. Обойти все эти сложности синдромного метода позволяет теория норм синдромов.

3. Автоморфизмы кодов и орбиты векторов-ошибок

Современные телекоммуникационные системы (ТКС) по типу каналов передачи информации можно разделить на три больших класса. К первому следует отнести волоконно-оптические системы. Здесь ошибки происходят крайне редко – в среднем один испорченный бит приходится на два часа непрерывной работы канала. Следовательно, такие ТКС можно считать идеальными. Недостатки их – в стационарности и дороговизне. Ко второму классу относятся каналы с повторением – здесь на приемном конце по специальным процедурам принятые блоки информации проверяются на наличие ошибок, а в случае их обнаружения соответствующий блок просят повторно передать. В этом классе находятся всевозможные почтовые службы. К третьему типу относятся каналы с синхронным исправлением возникающих в процессе передачи информации ошибок. Это все виды мобильной и космической связи, диспетчерские службы, цифровые телефон и телевидение и т. д.

Синхронное исправление ошибок реализуется только применением помехоустойчивых кодов. При этом наиболее применимы синдромные методы – по вычисленному ненулевому синдрому тем или иным образом определяется произошедшая ошибка. В большинстве случаев ошибка находится посредством решения уравнений в полях Галуа. А это, как мы убедились, – громоздкая и трудно алгоритмизуемая процедура.

Теория норм синдромов – новейший синдромный метод, который позволяет обойти названные трудности. Метод этот опирается на свойства автоморфизмов кодов. Нормы синдромов появились как синдромные инварианты автоморфизмов кодов.

3.1. Автоморфизмы кодов

Согласно формальному определению, приведенному в разд. 1, линейный (n, k)-код над полем P – это k-мерное подпространство в n-мерном пространстве P_n строк с n координатами из поля P. Поэтому ТКС с конкретным помехоустойчивым линейным (n, k)-кодом C передает информацию блоками-векторами из подпространства C пространства P_n, называемыми также кодовыми словами. В процессе передачи в каналах с шумами конкретного блока-сообщения $\bar{c} \in C \subset P_n$ на это сообщение может наложиться вектор-ошибка $\bar{e} \in P_n$. В результате на приемном конце ТКС получают вектор $\bar{x} = \bar{c} + \bar{e}$. В принципе вектор $\bar{e}$ может быть любым вектором из пространства P_n. Поэтому в линейном коде C пространство ошибок $E_n = P_n$.

На первом курсе мы хорошо изучили конечномерные векторные пространства и их линейные операторы на этих пространствах. Установили, что

всевозможные линейные преобразования пространства P_n составляют матричное кольцо $M_n(P)$. Автоморфизмами пространства P_n являются невырожденные квадратные матрицы из $M_n(P)$, они образуют группу $GL_n(P)$. Поэтому естественно было бы считать группой автоморфизмов кода C группу $GL_k(P)$. Однако по традиции, сложившейся в начале возникновения теории и практики помехоустойчивого кодирования, автоморфизмы линейных имеют более узкие рамки.

Определение 3.1. Автоморфизмом кода C называются произвольная перестановка координат кодовых слов, которая преобразует кодовые слова в новые кодовые слова.

Данное определение означает, что всякий автоморфизм кода C можно отождествить с конкретной подстановкой из группы S_n. Очевидно, множество $AutC$ всех автоморфизмов кода C содержит тождественную подстановку. Кроме того, легко заметить, что множество $AutC$ замкнуто относительно операции композиции автоморфизмов, т. е. операции их последовательного применения. Следовательно, если $AutC$ содержит некоторую подстановку $\tau \in S_n$, то $AutC$ содержит и всевозможные ее степени, в частности, и обратную подстановку $\tau^{-1} \in S_n$. Отсюда вытекает

Теорема 3.1. *Множество $AutC$ есть подгруппа группы S_n.*

Полное описание группы $AutC$ конкретного кода – достаточно сложная и специальная задача теории помехоустойчивых кодов. Но определенные подгруппы группы автоморфизмов для многих конкретных кодов указать можно.

3.2. Группа циклических сдвигов

Пусть σ – оператор циклического сдвига координат векторов, действие которого на произвольный вектор $\bar{e} = (e_1, e_2, ..., e_n)$ пространства $E_n = P_n$ осуществляется по следующему простому правилу:

$$\sigma(e_1, e_2, ..., e_n) = (e_n, e_1, e_2, ..., e_{n-1}).$$

Оператор σ является одним из наиболее естественных примеров нетривиальных автоморфизмов линейных кодов. Об этом свидетельствует

Теорема 3.2. *Оператор σ является автоморфизмом кодов Хемминга из подразд. 1.7, БЧХ-кодов с проверочной матрицей* (*2.2*), *реверсивных кодов из подразд. 2.8.*

Доказательство проведем для БЧХ-кодов с проверочной матрицей (2.2). Пусть вектор $\bar{c} = (c_{i_1}, c_{i_2}, ..., c_{i_w})$, т. е. имеет отличными от нуля только координаты $c_{i_1}, c_{i_2} ..., c_{i_w}$ с номерами $i_1 < i_2 < ... < i_w$ соответственно, $1 \le w \le n$. Тогда по определению синдрома

$$S(\bar{c}) = \bar{c} \cdot H^T = (c_{i_1} \cdot \beta^{(i_1-1)b} + ... + c_{i_w} \cdot \beta^{(i_w-1)b}, ..., c_{i_1} \cdot \beta^{(i_1-1)(b+\delta-2)} + ... + c_{i_w} \cdot \beta^{(i_w-1)(b+\delta-2)}) =$$

$$= (s_1, s_2, ..., s_{\delta-1}).$$

Если $\bar{c} \in C$, то $S(\bar{c}) = (s_1, s_2, ..., s_{\delta-1}) = (0, 0, ..., 0)$.

Если $i_w < n$, то $\sigma(\bar{c})$ имеет на позициях (и только на них) $i_1 + 1, ..., i_w + 1$ ненулевые координаты, равные соответственно $c_{i_1}, c_{i_2}, ..., c_{i_w}$. Поэтому

$$S(\sigma(\bar{c})) = (s_1^1, ..., s_{\delta-1}^1) = (c_{i_1} \cdot \beta^{i_1 b} + ... + c_{i_w} \cdot \beta^{i_w b}, ..., c_{i_1} \cdot \beta^{i_1(b+\delta-2)} + ... + c_{i_w} \cdot \beta^{i_w(b+\delta-2)}) =$$

$$= (\beta^b \cdot s_1, ..., \beta^{b+\delta-2} \cdot s_{\delta-1}).$$

Поскольку $(s_1, s_2, ..., s_{\delta-1}) = (0, 0, ..., 0)$, то из полученной формулы следует, что $S(\sigma(\bar{c})) = \bar{0}$. А это означает, что $\bar{c}$ и $\sigma(\bar{c})$ являются кодовыми словами. Мы не рассмотрели лишь случай, когда $i_w = n$. Тогда $\beta^{bn} = 1$ и у вектора $\sigma(\bar{c})$ отличны от нуля 1-я, $(i_1 + 1), \ldots, (i_{w-1} + 1)$-я координаты (и только они), равные соответственно $c_{i_w}, c_{i_1}, ..., c_{i_w - 1}$. Тогда

$$S(\sigma(\bar{c})) = (s_1^1, s_2^1, ..., s_{\delta-1}^1) = (c_{i_1} \cdot \beta^{i_1 b} + ... + c_{i_w - 1} \cdot \beta^{i_{[w-i]} b} + c_n \cdot \beta^b, ..., c_{i_1} \cdot \beta^{i_1(b+\delta-2)} + ...$$

$$... + c_{i_{[w-i]}} \cdot \beta^{i_{[w-i]}(b+\delta-2)}) = (c_{i_1} \cdot \beta^{i_1 b} + ... + c_{i_{[w-i]}} \cdot \beta^{i_{[w-i]} b} + c_n \cdot \beta^{(1+n)b}, ..., c_{i_1} \cdot \beta^{i_1(b+\delta-2)} + ...$$

$$... + c_{i_{[w-i]}} \cdot \beta^{(i_{[w-i]})(b+\delta-2)} + c_n \cdot \beta^{(1+n)(b+\delta-2)}) = (\beta^b \cdot s_1, ..., \beta^{(b+\delta-2)} \cdot s_{\delta-1}) = \bar{0},$$

что и требовалось доказать.

Следствие. У каждого кода C длиной n из теоремы 3.2 группа автоморфизмов $AutC$ содержит циклическую подгруппу

$$\Gamma = < \sigma > = \{\sigma, \sigma^2, ..., \sigma^n = e\} \text{ порядка } n.$$

Определение 3.2. Код C называется циклическим, если $\Gamma \subset AutC$.

Циклические коды популярны в теории и практике помехоустойчивого кодирования. Следствие из теоремы 3.2 обеспечивает первые содержательные примеры циклических кодов.

3.3. Группа циклотомических подстановок

Определим на множестве $T = \{1, 2, ..., n\}$ преобразование φ по следующему правилу: для каждого $i \in T$ $\varphi(i) = \overline{2i - 1}$ – элемент множества T, равный $2i - 1$, если $2i - 1 \le n$, и равный $2i - 1 - n$, если $2i - 1 > n$.

Лемма 3.1. Отображение φ является биекцией множества T тогда и только тогда, когда n нечетно.

Доказательство. Отметим, что $\varphi(1) = 1$. Пусть $n = 2l$ – четно. Тогда $\varphi(l + 1) = \overline{2(l + 1) - 1} = \overline{2l + 1} = 1 = \varphi(1)$. Следовательно, для четных n отображение φ не может быть биекцией. Пусть $n = 2l + 1$ – нечетно. Для различных целых $i, j \in T, i < j$, значения $\varphi(i)$ и $\varphi(j)$ различны, когда $j \le l$ или же

$i > l+1$. Пусть $i \le l+1, i < j, j \ge l$. Предположим, что $\varphi(i) = \varphi(j)$. Это означает, что $2i-1 = 2j-1-n$. Но тогда $n = 2(j-i)$ – четное число в противоречие с выбором n. Следовательно, φ – инъективное отображение и является биекцией в силу конечности множества T. Лемма доказана.

В силу доказанной леммы далее в данном разделе будем предполагать, что $n = 2l+1$ – нечетно. Найдем порядок циклической подгруппы $<\varphi>$, порожденной степенями подстановки φ в симметрической группе S_n. Из определения действия φ следует, что для всякого целого $k \ge 1$ $\varphi^k(1) = 1$, а для каждого $i \in T, i > 1$, справедливы следующие соотношения:

$$\begin{cases} \varphi^2(i) = \overline{2(2i-1)-1} = \overline{2^2 i - 2 - 1}; \\ \varphi^3(i) = \overline{2(2^2 i - 2 - 1)-1} = \overline{2^3 i - 2^2 - 2 - 1}; \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \varphi^k(i) = \overline{2^k i - 2^{k-1} - 1} = \overline{2^k i - (2^k - 1)} = \overline{(2^k - 1)(i-1) + i}. \end{cases} \quad (3.1)$$

Здесь $\overline{a} \in T$, т. е. $\overline{a} = a - nq$ для подходящего целого q. Согласно теореме Эйлера [11] $2^{\phi(n)} \equiv 1 (\mathrm{mod}\, n)$, где $\phi(n)$ – количество натуральных чисел, меньших n и взаимно простых с n. Следовательно, существует наименьшее натуральное m с условием $2^m - 1 = nq$, т. е. n делит $2^m - 1$. Тогда из формулы (3.1) вытекает, что $\varphi^m(i) = i$ и, следовательно, $|<\varphi>| \le m$.

Предложение 3.1. Пусть m – наименьшее натуральное число с условием: $2^m - 1$ делится на данное нечетное число n. Циклическая группа Φ, порожденная степенями подстановки φ на множестве $T = \{1, 2, ..., n\}$, конечна и имеет порядок m.

Доказательство. Покажем, что $2, \varphi(2), ..., \varphi^{m-1}(2)$ – попарно различные элементы множества T (тогда $|<\varphi>| \ge m$). При $i = 2$ $i = 2$ основная из формул (3.1) преобразуется к виду $\varphi^k(2) = \overline{(2^k - 1)(2-1) + 2} = \overline{2^k + 1}$. Если бы $\varphi^k(2) = \varphi^r(2)$ для некоторых целых $k, r, 0 \le r < k < m$, то отсюда следовало бы, что $\varphi^s(2) = 2$ для $s = k - r, 1 < s < m$, или $2^s + 1 = 2 + np$ для подходящего целого p. Но тогда $2^s - 1 = np$ делится на n для $s < m$ в противоречие с выбором m. Таким образом, $|<\varphi>| = m$, что и требовалось доказать.

Группа Φ действует на пространстве ошибок E_n любого двоичного линейного кода, переставляя координаты векторов-ошибок в соответствии с действием на их номера, образующие множество T. Вообще говоря здесь уместно было бы нумеровать координаты не с 1-й по n-ю, а с 0-й по $n-1$-ю. Тогда правила действия φ и ее степеней на i-ю координату, $0 \le i \le n-1$, выглядят

проще: $\varphi(i) = \overline{2i}$, где $\overline{2i}$ – вычет целого числа $2i$ по модулю n. Соответственно $\varphi^k(i) = \overline{i2^k}$ – остаток от деления $i2^k$ на n, $0 \le i \le n-1$, $1 \le k \le m$. При этом заметим, что числа $i, 2i, 2^2 i, \cdots, 2^{m-1} i$ образуют циклотомический класс по модулю n [3]. Поэтому подстановки $\varphi, \varphi^2, \cdots, \varphi^m = id$ – называются циклотомическими и соответственно группа Φ – циклотомической.

В дальнейшем, однако, будем использовать первоначальную нумерацию координат – с 1-й по n-ю, а выражение $\overline{a}$ понимать в смысле комментария к формуле (3.1) как элемент из T.

Теорема 3.3. *Циклотомическая группа* Φ *является подгруппой группы* $AutC$ *кодов Хемминга из подразд. 1.7, БЧХ-кодов с проверочной матрицей* (*2.2*)*, реверсивных кодов из подразд. 2.8.*

Доказательство проведем для БЧХ-кодов с проверочной матрицей (2.2). Сохраним обозначения из доказательства теоремы 3.2. Пусть кодовое слово $\overline{c} = (i_1, i_2, \ldots, i_s)$, где $1 \le i_1 < i_2 < \ldots < i_s \le n$. По определению действия циклотомической подстановки $\varphi(\overline{e}) = \left(\overline{2i_1 - 1}, \overline{2i_2 - 1}, \ldots, \overline{2i_s - 1}\right)$. Синдром

$$S(\overline{c}) = \overline{c} \cdot H^T = (\beta^{b(i_1-1)} + \beta^{b(i_2-1)} + \ldots + \beta^{b(i_s-1)}; \beta^{(b+1)(i_1-1)} + \beta^{(b+1)(i_2-1)} + \ldots$$

$$\ldots + \beta^{(b+1)(i_s-1)}; \ldots; \beta^{(b+\delta-2)(i_1-1)} + \beta^{(b+\delta-2)(i_2-1)} + \ldots$$

$$\ldots + \beta^{(b+\delta-2)(i_s-1)}) = (s_1, s_2, \ldots, s_n).$$

Поскольку $\overline{c}$ – кодовое слово, то $S(\overline{c}) = (s_1, s_2, \ldots, s_{\delta-1}) = (0, 0, \ldots, 0)$. С учетом равенства $\beta^n = 1$ и, следовательно, $\beta^{bn} = 1$, синдром

$$S(\varphi(\overline{c})) = (\beta^{b(2i_1-2)} + \beta^{b(2i_2-2)} + \ldots + \beta^{b(2i_s-2)}; \beta^{(b+1)(2i_1-2)} + \beta^{(b+1)(2i_2-2)} + \ldots$$

$$\ldots + \beta^{(b+1)(2i_s-2)}; \ldots; \quad \beta^{(b+\delta-2)(2i_1-2)} + \beta^{(b+\delta-2)(2i_2-2)} + \ldots + \beta^{(b+\delta-2)(2i_s-2)}) =$$

$$= (s_1^2, s_2^2, \ldots, s_{\delta-1}^2).$$

Таким образом, $S(\varphi(\overline{c})) \in \overline{0}$, откуда следует, что $\varphi(\overline{c}) \in C$. Теорема полностью доказана.

Лемма 3.2. *Для произвольного* $\overline{e} \in E_n$ $\varphi(\sigma(\overline{e})) = \sigma^2(\varphi(\overline{e}))$.

Доказательство.

$$\sigma((i)) = (\overline{i+1}) = \begin{cases} (i+1), 1 \le i < n, \\ 1, i = n. \end{cases}$$

Тогда для целых $i, 1 \le i < n$, $\varphi(\sigma(i)) = \left(\overline{2(i+1)-1}\right) = \left(\overline{2i+1}\right)$, а для $i = n$ $\varphi(\sigma(n)) = \varphi(1) = (1)$. С другой стороны, для всех $i, 1 \le i < n$,

$$\sigma^2(\varphi(i)) = \sigma^2\left(\overline{2i-1}\right) = \left(\overline{2i+1}\right) = \varphi(\sigma(i)),$$

а для $i = n$ $\sigma^2(\varphi(n)) = \sigma^2\left(\overline{2n-1}\right) = \sigma^2(n-1) = (1)$. Таким образом, для каждого $\bar{e} \in E_n$ $\sigma^2(\varphi(\bar{e})) = \varphi(\sigma(\bar{e}))$. Лемма полностью доказана.

Теорема 3.4. *Группа подстановок G, порожденная циклической подстановкой σ и циклотомической подстановкой φ, некоммутативна и имеет порядок mn.*

Доказательство следует из леммы 3.2.

Из теорем 3.2 и 3.3 следует, что группа G принадлежит группе автоморфизмов названных в этих теоремах кодов.

3.4. Г-орбиты векторов ошибок

Здесь рассматриваем двоичные пространства P_n, где $P = Z/2Z$. Другими словами, все рассматриваемые векторы имеют координаты 0 и 1. Векторы-ошибки имеют, как правило, немного ненулевых координат. Поэтому часто будем пользоваться следующим определением.

Определение 3.3. Равенство $\bar{e} = (i_1, i_2, ..., i_k)$ означает, что двоичный вектор $\bar{e}$ имеет ненулевыми и, следовательно, равными единице только координаты под номерами $i_1, i_2, ..., i_k$.

Важным для дальнейшего является

Определение 3.4. Совокупность всех попарно различных векторов-ошибок $\sigma^k(\bar{e})$, $0 \le k < n$, называется Г-орбитой вектора-ошибки $\bar{e}$ пространстве ошибок E_n и обозначается через $<\bar{e}>$. Г-орбита называется полной, если она содержит n различных векторов, в противном случае Г-орбиту называют неполной.

Г-орбиты имеют четкую структуру, которую описывает

Теорема 3.5. *Для произвольного фиксированного вектора $\bar{e} \in P_n$ из пространства ошибок $E_n = P_n$ его Г-орбита $<\bar{e}>$ состоит из λ элементов, где $\lambda = n$ или λ делит n. При этом λ – наименьшее натуральное число с условием $\sigma^\lambda(\bar{e}) = \bar{e}$ и Г-орбита $<\bar{e}>$ имеет следующую структуру*:

$$<\bar{e}> = \left\{\bar{e}, \sigma(\bar{e}), \ldots, \sigma^{\lambda-1}(\bar{e})\right\}. \qquad (3.2)$$

Для любых двух векторов-ошибок $\bar{e}$ и $\bar{e}'$ из E_n их Г-орбиты $<\bar{e}>$ и $<\bar{e}'>$ либо совпадают, либо не имеют одинаковых элементов.

Доказательство. Пусть λ – наименьшее натуральное число, такое, что $\sigma^\lambda(\bar{e}) = \bar{e}$. Тогда для любого целого μ согласно теореме о делении с остатком $\mu = \lambda q + r$, где $0 \le r < \lambda$ и $\sigma^\mu(\bar{e}) = \sigma^r(\sigma^{\lambda q}(\bar{e})) = \sigma^r(\bar{e})$ (по определению $\sigma^0(\bar{e}) = (\bar{e})$. Это означает, что $\sigma^\mu(\bar{e})$ принадлежит множеству (3.2). Предположим, что $\sigma^k(\bar{e}) = \sigma^l(\bar{e})$ для некоторых целых $0 < k < l < \lambda$. Тогда

$0 < l - k < \lambda$ и $\sigma^{lk}(\bar{e}) = \bar{e}$, что противоречит минимальности λ. Следовательно, векторы $\bar{e}, \sigma(\bar{e}), ..., \sigma^{\lambda-1}(\bar{e})$ попарно различны. Это означает, что мощность Г-орбиты $< \bar{e} >$ (т.е. число ее элементов) равна λ и справедлива формула (3.2).

Осталось доказать, что λ делит n. Предположим противное, что n не делится на λ. Тогда наибольший общий делитель $\text{НОД}(n, \lambda) = d$, где $1 \le d < \lambda$. Расширенный алгоритм Евклида находит такие целые u, v, что $nu + \lambda v = d$. Тогда $\sigma^d(\bar{e}) = \sigma^{nu+\lambda v}(\bar{e}) = \bar{e}$, что противоречит минимальности λ. Следовательно, λ делит n или $\lambda = n$. Теорема 3.5 полностью доказана.

Структурная формула (3.2) произвольной Г-орбиты $< \bar{e} >$ показывает, что действие Г на элементы из $< \bar{e} >$ не выводит за пределы Г-орбиты и что Г действует транзитивно внутри $< \bar{e} >$, т. е. для всяких векторов $\bar{e}_i$, $\bar{e}_j$, из $< \bar{e} >$ найдется $g \in \Gamma$, что $g(\bar{e}_i) = \bar{e}_j$.

Предложение 3.2. Для любых двух векторов-ошибок $\bar{e}$ и $\bar{e}'$ из E_n их Г-орбиты $< \bar{e} >$ и $< \bar{e}' >$ либо совпадают, либо не имеют одинаковых элементов.

Доказательство. Пусть $\bar{e}''$ – общий элемент Г-орбит $< \bar{e} >$ и $< \bar{e}' >$. Так как $\bar{e}'' \in < \bar{e}' >$, то в силу отмеченной выше транзитивности Г на $< \bar{e}' >$ Г-орбиты $< \bar{e}' >$ и $< \bar{e}'' >$ совпадают. Следовательно, $< \bar{e}' >$ является частью $< \bar{e} >$. Но точно так же верно и обратное включение $< \bar{e} > \subset < \bar{e}' >$. Следовательно, $< \bar{e} >$ и $< \bar{e}' >$ совпадают. Предложение доказано.

На рис. 3.1 изображены все элементы Г-орбиты в пространстве E_{15}, порожденной вектором-ошибкой весом 6. Это Г-орбита состоит из $\lambda = 5 = 15/3$ векторов. Непосредственно из рисунка видно, что $\sigma^5(\bar{e}) = \bar{e}$.

Из теоремы 3.5 и предложения 3.2 следует, что под действием группы Г циклических сдвигов пространство E_n разбивается на непересекающиеся классы – Г-орбиты. Всякое разбиение множества на непересекающиеся классы определяет отношение эквивалентности на нем. Множество всех Г-орбит пространства E_n будем обозначать через E_n / Γ.

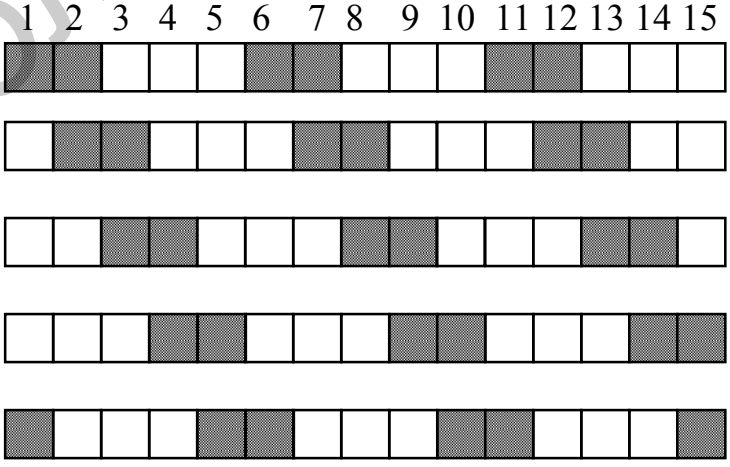

Рис. 3.1. Схематическое изображение вектора $\bar{e}$=(1,2,6,7,11,12) из пространства E_{15} и его циклических сдвигов $\sigma(\bar{e}), \sigma^2(\bar{e}), \sigma^3(\bar{e}), \sigma^4(\bar{e})$

Пример 2.1. Построим классификацию, т. е. систему Г-орбит в двоичном 4-мерном пространстве векторов-ошибок E_4. Здесь $C_4^2 = 6$; $C_4^3 = 4$; и $|E_4| = 2^4 = 16$.

Пусть $\bar{e}_1$ = (1000). Тогда $<\bar{e}_1>$ = {(1000),(0100),(0010),(0001)}.

Пусть $\bar{e}_2$ = (1100). Тогда $<\bar{e}_2>$ = {(1100),(0110),(0011),(1001)}.

Пусть $\bar{e}_3$ = (1010). Тогда $<\bar{e}_3>$ = {(1010),(0101)}.

Пусть $\bar{e}_4$ = (1110). Тогда $<\bar{e}_4>$ = {(1110),(0111),(1011),(1101)}.

Очевидно, Г-орбиты, порожденные векторами $\bar{0}$ = (0000) и $\bar{1}$ = (1111), имеют мощность, равную 1.

Таким образом, пространство E_4, состоящее из 16 векторов-ошибок, разбивается на 6 Г-орбит: две – $<\bar{0}>$ и $<\bar{1}>$ – мощностью 1, одну – <(1010)> – мощностью 2 и три – <(1000)>, <(1100)>, <(1110)> – мощностью 4. Таким образом, множество E_4 / Γ состоит из 6 элементов.

3.5. Признаки полноты Г-орбит

Предложение 3.3. В любом двоичном пространстве E_n имеются лишь две Г-орбиты мощностью 1 – это <0> и <1>. Если $n = p$ число простое, то все остальные Г-орбиты являются полными (т. е. содержат по n векторов). Всего в пространстве E_p имеется $\Pi_p = \dfrac{2^P - 2}{p}$ полных Г-орбит.

Заметим, что согласно малой теореме Ферма число 2^{p-1} сравнимо с 1 по модулю p для простого числа $p > 2$, поэтому величина $\dfrac{2(2^{P-1} - 1)}{p} = \Pi_p$ есть число целое.

В дальнейшем для данного натурального n и произвольного натурального числа k через $\bar{k}$ обозначаем число $k - sn$, принадлежащее множеству $T = \{1, 2, ..., n\}$ целых чисел, для подходящего целого $s \geq 0$.

В любом векторном пространстве большинство векторов-ошибок группируется в полные Г-орбиты. Основанием для этого утверждения служат следующие два предложения.

Предложение 3.4. Пусть $\bar{e} = (i_1, i_2, ..., i_k)$, где $1 \leq i_1 < i_2 < ... < i_k$, причем $i_k \leq [n/2]$, – вектор-ошибка весом k, $1 \leq k \leq [n/2]$. Тогда Г-орбита $<\bar{e}>$ – полная.

Доказательство. Достаточно убедиться, что $\sigma^{\lambda}(\bar{e}) = \bar{e}$ при наименьшем $\lambda = n$. Утверждение очевидно при $k = 1$. Пусть $k \geq 2$. Для всех целых λ, $1 \leq \lambda \leq [n/2]$, вектор $\sigma^{\lambda}(\bar{e}) = (i_1 + \lambda, i_2 + \lambda, ..., i_k + \lambda) \neq \bar{e}$, так как $i_k < i_k + \lambda \leq n$,

а на позиции $i_k+\lambda$ вектора $\bar{e}$ присутствует 0. Для всех целых λ, $[n/2]+1 \le \lambda \le n-i_1$, вектор $\sigma^{\lambda}(\bar{e}) \ne \bar{e}$, так как у вектора $\sigma^{\lambda}(\bar{e})$ координата с номером $i_1+\lambda$ равна 1 и номер этой координаты удовлетворяет неравенствам $i_1+[n/2]+1 \le i_1+\lambda \le n$, а все координаты вектора $\bar{e}$ с такими номерами равны 0. Если $i_1=1$, то предложение доказано. Пусть $i_1>1$. Тогда для λ, $n-i_1<\lambda<n$, $\sigma^{\lambda}(\bar{e}) \ne \bar{e}$, поскольку у вектора $\sigma^{\lambda}(\bar{e}) \ne \bar{e}$ координата с номером $i_1+\lambda = i_1+\lambda$, удовлетворяющим неравенствам: $1 \le \overline{i_1+\lambda} < \overline{i_1+n} = i_1$ и отлична от нуля, а у вектора $\bar{e}$ эта координата равна 0. Таким образом, векторы-ошибки $\bar{e}$, $\sigma(\bar{e}),\ldots,\sigma^{n-1}(\bar{e})$ попарно различны и, следовательно, образуют полную Г-орбиту $<\bar{e}>$. Предложение доказано.

Замечание. Границы изменения i_k в предложении 3.4 нельзя увеличить в общем случае, поскольку могут появиться Г-орбиты мощностью, меньшей *n*. Например, при $n=2l$ Г-орбита $<(1, \ell+1)>$ имеет мощность ℓ в двоичном пространстве E_n,.

Предложение 3.5. Всякая Г-орбита, порожденная в двоичном пространстве E_n вектором-ошибкой (i,j,k) весом 3, где $1 \le i < j < k \le 2[n/3]$, является полной.

Доказательство. Предположим, что $i>1$. Тогда циклически сдвинутый вектор-ошибка $\bar{e}=\sigma^{(i-1)}(i,j,k)=\sigma^{n-i+1}(i,j,k)=(1,\ j-i+1,\ k-i+1)$ имеет первую координату, отличную от нуля. Ясно, что $<\bar{e}>=<(i,j,k)>$. Достаточно доказать, что $|<\bar{e}>|=n$. Пусть $j-i+1=\alpha$, $k-i+1=\beta$. Тогда $\bar{e}=(1,\alpha,\beta)$, где $\beta \le 2[n/3]$.

Предположим, что $|<e>|<n$. Тогда найдется такое число $\lambda, 1<\lambda<n$, что $\sigma^{\lambda}(\bar{e})=\bar{e}$.Это возможно только в двух случаях.

1. Под действием σ^{λ} первая координата перешла в координату с номером α, e_α – в координату e_β, e_β – в 1-ю координату. Следовательно,

$$\beta-\alpha=\alpha-1=n-\beta+1.$$

Отсюда следует, что $\beta=2\alpha-1$ и $\alpha=n-2\alpha+2$ или $3\alpha=n+2$, т. е. $\alpha=\dfrac{n+2}{3}$. Тогда $\beta=2\dfrac{n+2}{3}-1=\dfrac{2n+4-3}{3}=\dfrac{2n+1}{3}$. Поскольку $\alpha-$ целое, то n должно быть числом вида $3k+1$. Следовательно,

$$\beta=\frac{2(3k+1)+1}{3}=\frac{6k+3}{3}=2k+1,$$

что противоречит условию $\beta=2k+1 \le 2[n/3]=2k$.

2. Под действием σ^{λ} происходит преобразование координат следующим образом: $1 \to \beta, \alpha \to 1, \beta \to \alpha$. Тогда $\beta-1=n-\alpha+1-n-\beta+\alpha$. Отсюда сле-

дует: $2\alpha - \beta - 1 = 0$, или $\beta = 2\alpha - 1, 2\beta = n + \alpha + 1$, или $\beta = 2\ell - 1; 2\beta = n + \ell + 1$, или $4\ell - 2 = n + \ell + 1$, что эквивалентно соотношению $3\ell = n + 3$ или $\ell = \frac{n+3}{3}$. Следовательно,

$$n = 3k; [n/3] = k; \beta = 2\frac{n+3}{3} - 1 = \frac{2n+6-3}{3} = \frac{6k+3}{3} = 2k+1 = 2[n/3]+1,$$

что противоречит условию. Следовательно, $\bar{e}$, $\sigma(\bar{e})$, …, $\sigma^{n-1}(\bar{e})$ – попарно различные векторы и $|<\bar{e}>| = n$, что и требовалось доказать.

Замечание. Границы изменения k в предложении 3.5 в общем случае нельзя увеличить. При $n = 3l$ вектор-ошибка $\bar{f} = (1, \ell+1, 2\ell+1)$ порождает Г-орбиту мощностью, меньшей n, так как $\sigma^l(\bar{f}) = \bar{f}$.

3.6. Пакетная длина и диаметр вектора-ошибки

Определение 3.4. Циклическим пакетом ошибок длиной b называется вектор $\bar{e}$, все ненулевые координаты которого расположены среди b последовательных (по циклу) координат, первая и последняя из которых отличны от нуля. Пакет ошибок называется сплошным, если вес ошибки совпадает с длиной пакета.

На рис. 3.2. приведены все возможные пакеты ошибок длиной 3 в пространстве P_6, где $P = GF(2)-$ поле Галуа из двух элементов 1 и 0.

а

1	1	1	0	0	0	0	1	1	1	0	0	0	0	1	1	1	0
0	0	0	1	1	1	1	0	0	0	1	1	1	1	0	0	0	1

б

1	0	1	0	0	0	0	1	0	1	0	0	0	0	1	1	1	0
0	0	0	1	0	1	1	0	0	0	1	0	0	1	0	0	0	1

Рис. 3.2. Пакеты векторов-ошибок длиной 3 в пространстве V_6 над полем $GF(2)$: а – весом 3; б – весом 2

Определение 3.5. Всякую вектор-ошибку $\bar{e}$ весом $\omega > 1$ можно интерпретировать различным образом как пакетную ошибку с соответствующими значениями длины b. Наименьшую из длин b при всех таких интерпретациях вектора-ошибки $\bar{e}$ назовем диаметром D этого вектора-ошибки.

Пример 3.2. Вектор-ошибка $\bar{e} =$ (100010) – есть ошибка весом $\omega = 2$ в ко-

довом слове длиной $n = 6$, его можно рассматривать как пакет ошибок длиной 5 или пакет длиной 3. Таким образом, диаметр D этого вектора-ошибки равен трем.

Предложение 3.6. Диаметр вектора-ошибки $\bar{e}$ весом $\omega > 1$ с ненулевыми координатами на позициях $i_1, i_2, ..., i_\omega$ вычисляется по формуле

$$D(\bar{e}) = D_{\bar{e}} = \min\{ i_\omega - i_1 + 1, n + i_1 - i_2 + 1, n + i_2 - i_3 + 1, \ldots, n + i_{\omega-1} - i_\omega + 1\} \qquad (3.3)$$

В частности, при $\omega = 2$

$$D(\bar{e}) = D_{\bar{e}} = \min\{ i_2 - i_1 + 1, n + i_1 - i_2 + 1\}; \qquad (3.4)$$

при $\omega = 3$

$$D(\bar{e}) = D_{\bar{e}} = \min\{i_3 - i_1 + 1, n + i_1 - i_2 + 1, n + i_3 + 1\}. \qquad (3.5)$$

Доказательство. Вектор-ошибку $\bar{e}$ можно ω способами интерпретировать как пакетную циклическую последовательно, меняя первую и последнюю ненулевые координаты пакета: 1) первая координата – i_1, последняя – i_n, тогда пакетная длина $b_1 = i_\omega - i_1 + 1$; 2) первая координата – i_2, последняя – i_1, тогда пакетная длина $b_2 = n - i_2 + i_1 + 1$; ω) первая координата – i_ω, последняя – $i_{\omega-1}$; тогда пакетная длина $b_\omega = n + i_{\omega-1} - i_\omega + 1$. Следовательно, диаметр $D_{\bar{e}} = \min\{ b_1, b_2, \ldots, b_\omega\} = \min\{ i_\omega = i_1 + 1, n + i_1, i_2 + 1, \ldots, n + i_{\omega-1} + 1\}$.
Предложение доказано.

Через [b] обозначаем целую часть вещественного числа b.

Следствие 1. Диаметры векторов-ошибок весом 2 в точности принадлежат отрезку [2; [n/2]+1].

Доказательство. Пусть $\bar{e}$ произвольный вектор ошибок весом 2 с ненулевыми координатами на позициях i_1 и i_2. Пусть $n = 2k + 1$ – нечетно. Тогда $\lfloor n/2 \rfloor = k$. Пусть $i_2 - i_1 + 1 > k + 1$. Тогда $i_2 - i_1 > k$ и

$$n + i_1 - i_2 + 1 = n - (i_2 - i_1) + 1 < 2k + 1 - k + 1 = k + 2,$$

т. е. $n + i_1 - i_2 + 1 \le k + 1$. Пусть $i_2 - i_1 + 1 \le k + 1$, тогда $i_2 - i_1 \le k$ и

$$n + i_1 - i_2 + 1 = n - (i_2 - i_1) + 1 > 2k + 1 - k + 1 = k + 2$$

и, следовательно, $D_{\bar{e}} = i_2 - i_1 + 1 \le k + 1 = [n/2] + 1$.

Пусть $n = 2k$ – четно, тогда $[n/2] = k$. Если у вектора-ошибки $\bar{e}$ величина $i_2 - i_1 + 1 > k + 1$, т.е. $i_2 - i_1 > k$, то $n - i_2 - i_1 + 1 = n - (i_2 - i_1) + 1 < 2k - k + 1$. Следовательно, $D(\bar{e}) = n - i_2 + i_1 + 1 < k + 1$. Пусть $i_2 - i_1 + 1 \le k + 1$ или $i_2 - i_1 \le k$, тогда $n - i_2 + i_1 + 1 = n - (i_2 - i_1) + 1 \ge 2k - k + 1 = k + 1$ и, значит, согласно формуле (2.2) диаметр $D(\bar{e}) = i_2 - i_1 + 1 \le k + 1$.

Векторы (1, 2) и $(1, k + 1)$, как несложно видеть, имеют диаметр соответственно 2 и $k + 1$ и для $n = 2k$ и для $n = 2k + 1$. Тогда диаметры всех двоичных ошибок находятся в диапазоне [2; [$n/2$] + 1] с достижимыми, не уменьшаемыми границами, что и требовалось доказать.

Следствие 2. Диаметры ошибок весом 3 находятся в диапазоне $[3;\ 2k + 1]$

для $n = 3k$ и $n = 3k+1$, а для $n = 3k+2$ – в диапазоне $[3;\ 2k+2]$.

Доказательство. Нижняя граница диаметра очевидна. Что касается верхней границы, то вектор-ошибка $(1, k+1, 2k+1)$ имеет диаметр $2k+1$ для $n = 3k$ и для $n = 3k+1$. Для $n = 3k+2$ вектор-ошибка $(1, k+2, 2k+2)$ имеет согласно формуле (2.3) диаметр

$$D = \min\{2k+2-1+1, 3k+2+1-k-2+1, 3k+2+k+2-2k-2+1\} =$$

$$= \min\{2k, 2k+2, 2k+3\} = 2k+2.$$

Осталось показать, что диаметр любого вектора-ошибки весом 3 не может быть выше отмеченных границ. Пусть $n = 3k$ и у вектора-ошибки (i_1, i_2, i_3) величина $i_3 - i_1 + 1 > 2k+1$, т. е. $i_3 - i_1 > 2k$. Тогда $i_3 - i_1 \geq 2k$, либо $i_2 - i_1 < 2k$. В первом случае $n + i_1 - i_2 + 1 = n - (i_2 - i_1) + 1 \leq 3k - 2k + 1 = k + 1$ и согласно формуле (2.3) $D_{\bar{e}} \leq k+1$. Во втором случае либо $i_2 - i_1 \leq k$, либо $k < i_2 - i_1 < 2k$. Пусть $i_3 - i_1 > 2k$ и $i_2 - i_1 \leq k$, тогда $i_3 - i_2 = (i_3 - i_1) - (i_2 - i_1) >$
$> 2k - (i_2 - i_1) \geq 2k - k = k$, а число $n + i_2 - i_3 + 1 = n - (i_3 - i_2) + 1 \leq 3k - k + 1 = 2k + 1$; следовательно, по формуле (2.3) диаметр $D_{\bar{e}} \leq k+1$. Пусть $i_3 - i_1 > 2k$ и $k < i_2 - i_1 < 2k$, тогда $n + i_1 - i_2 + 1 = 3k - (i_2 - i_1) + 1 < 3k - k + 1 = 2k + 1$ и, тогда в силу формулы (2.3) $D_{\bar{e}} \leq k+1$. Таким образом, в случае $n = 3k$ следствие 2 полностью доказано. Точно так же обосновывается утверждение при $n = 3k+1$ и $n = 3k+2$.

3.7. Классификация Г-орбит ошибок весом 2

Лемма 3.3. Биномиальный коэффициент C_n^2 делится на n тогда и только тогда, когда n нечетно. Биномиальный коэффициент C_n^3 делится на n тогда и только тогда, когда $n = 3k+1$ или $n = 3k+2$ для произвольного натурального k.

Доказательство. Пусть $n = 2l$ – четно, $l \geq 1$, тогда

$$C_n^2 = n(n-1)/2 = l \cdot (2l-1)$$

есть число, делящееся на l, но не делящееся на $2l$, поскольку $2l-1$ нечетно. Пусть $n = 2l+1$ – нечетное натуральное число, где $l > 1$. Тогда $C_n^2 = (2l+1)l$ делится на n.

Биномиальный коэффициент C_n^3 определен для всех натуральных чисел $n \geq 3$ формулой $C_n^3 = \dfrac{n(n-1)(n-2)}{6}$. Это целое число, поскольку числитель является четным и делящимся на 3 числом. Из формулы, определяющей C_n^3, следует, что C_n^3 делится на n тогда и только тогда, когда $M = (n-1)(n-2)$ делится на 6.

Делимость на 3 определяет отношение эквивалентности на множестве натуральных чисел N, которое разбивает N на 3 непересекающиеся класса чисел вида $3k, 3k+1, 3k+2$, где k – произвольное натуральное число.

Если у коэффициента C_n^3 величина $n = 3k$, то число $M = (3k-1)(3k-2)$ не делится на 6, так как оно, очевидно, не делится на 3. Следовательно, C_{3k}^3 не делится на $3k = n$.

Пусть $n = 3k+1,\ k \geq 1$. Тогда $M = 3k(3k-1)$ делится на 3 и на 2 как произведение двух последовательных натуральных чисел. Таким образом, M делится на 6, а C_{3k+1}^3 делится на $3k+1 = n$.

Пусть $n = 3k+2$. Тогда $M = (3k-1)3k$ делится на 6 по тем же причинам и, следовательно, в данном случае C_n^3 / n является целым числом.

Лемма полностью доказана.

Предложение 3.7. Пусть E_n – двоичное векторное пространство. Одиночные ошибки составляют один класс эквивалентности I_1. Векторы-ошибки весом 2 принадлежат одному классу эквивалентности (Г-орбите) тогда и только тогда, когда их диаметры совпадают. По значениям диаметра множество всех двойных ошибок разбивается на v непересекающихся классов эквивалентности $I_2, I_3, ..., I_{v+1}$, где $v = [n/2]$ – целая часть числа $n/2$, I_k – класс двойных ошибок диаметром k, $2 \leq k \leq v+1$. Для нечетных $n = 2\nu + 1$ каждый из классов I_k состоит из n различных ошибок. При четных $n = 2н$ класс I_k, где $2 < k < \nu$, состоит и n векторов-ошибок, а класс I_{v+1} – из $н$ двойных ошибок.

Доказательство. Утверждение об ошибках весом 1 очевидно. Согласно следствию 1 из предложения 3.6 диаметры $Д$ векторов-ошибок весом 2 удовлетворяют точному неравенству: $2 \leq Д \leq [n/2]+1$. Для каждого числа $Д$, $2 \leq Д \leq [n/2]$ вектор $\bar{e}_{1,Д} = (1, Д)$ имеет диаметр $Д$. Согласно предложению 3.4 Г-орбита $< \bar{e}_{1,Д} >$ является полной.

Вектор-ошибка $\bar{e}_{1,k+1} = (1, k+1)$ для $k = [n/2]$ имеет диаметр $Д = k+1$, как отмечено в доказательстве следствия 1 из предложения 3.6. Если $n = 2k$ – четно, то тогда по лемме 3.3 C_n^2 не делится на n и, следовательно, должны существовать неполные Г-орбиты ошибок весом 2. В самом деле $\bar{e}_{1,k+1}$ является периодическим вектором-ошибкой и, следовательно, $|< \bar{e}_{1,k+1} >| = k = n/2$. Таким образом, при $n = 2k$ имеется $k-1$ полных Г-орбит $<(1, Д)>$, $2 < Д \leq k$, и одна Г-орбита $< (1, k+1) >$ имеет мощность k. Все они попарно различны в силу предложения 3.2. Вместе они содержат $(k-1)2k + k = 2k^2 - k = k(2k+1) = = \dfrac{n(n-1)}{2} = C_n^2$ – векторов-ошибок – все множество ошибок весом 2. Следовательно, для других Г-орбит нет места. При $n = 2k+1$ Г-орбита $<\bar{e}_{1,\ k+1}>$ не является периодической: она могла

быть только $n/2$ – периодической, а число $n/2$ – не целое. Таким образом, при $n = 2k+1$ мы имеем k различных полных Г-орбит $<\bar{e}_{1,Д}>$, $2 \le Д \le k+1$, – ошибок весом 2. Они содержат $k\,n = \dfrac{n(n-1)}{2}$ векторов и, следовательно, исчерпывают весь спектр двойных ошибок. Предложение 3.7 полностью доказано.

Пример 3.3. В пространстве E_{15} имеется $C_{15}^2 = 105$ векторов-ошибок весом 2, делящихся согласно предложению 3.7 на 7 полных Г-орбит в соответствии со значением их диаметров. Ниже приведена табл. 3.1 образующих Г-орбит двойных ошибок в 15-мерном пространстве – векторов-ошибок $\bar{e}_{1,i}$ диаметром $D_i = 2, 3, \ldots, 8$.

Таблица 3.1

Г-орбиты двойных ошибок в пространстве E_{15}

D_i	$\bar{e}_{1,i}$	Координаты порождающего вектора $\bar{e}_{1,i}$														
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	$\bar{e}_{1,2}$	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0
3	$\bar{e}_{1,3}$	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0
4	$\bar{e}_{1,4}$	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0
5	$\bar{e}_{1,5}$	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0
6	$\bar{e}_{1,6}$	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0
7	$\bar{e}_{1,7}$	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0
8	$\bar{e}_{1,8}$	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0

3.8. Классификация Г-орбит ошибок весом 3

Скрупулезное исследование тройных ошибок приводит к следующей классификации их Г-орбит.

Теорема 3.6. *В двоичных кодах длиной n все C_n^3 векторов-ошибок весом 3 под действием группы Г циклических сдвигов разбиваются на C_n^3/n полных Г-орбит для $n = 3k+1$, и $n = 3k+2$. Для $n = 3k$ все векторы-ошибки весом 3 разбиваются на $[C_n^3/n]$ Г-орбит мощностью n плюс одна Г-орбита мощностью k, порожденная вектором-ошибкой $(1, k+1, 2k+1)$.*

Диаметры тройных ошибок находятся в диапазоне $[3; 2k+1]$ для $n = 3k$ и $n = 3k+1$, а для $n = 3k+2$ – в диапазоне $[3; 2k+2]$.

Для каждого значения диаметра Д, $3 \le Д \le \nu+1$, где $\nu = [n/2]$, имеется $Д-2$ различных Г-орбит тройных ошибок. Это классы $<(1, j, Д)>$, где $1 < j < Д$. Если $n = 2\nu+1$ – нечетно, то имеется $\nu-1$ полных Г-орбит векторов-ошибок весом 3 и диаметром $Д = \nu+2$. Это классы

$$<(1, 2, \nu+2)> = <(1, \nu+1, \nu+2)>, <(1, 3, \nu+2)>, \ldots, (1, \nu, \nu+2)>.$$

Если $n = 2\nu$, *то имеется* $\nu - 3$ *полных Г-орбит тройных ошибок диаметром* $Д = \nu + 2$. *Это Г-орбиты* $< (1, 3, \nu + 2) > = < (1, \nu, \nu + 2) >$, $< (1, 4, \nu + 2) >, ..., < (1, \nu - 1, \nu + 2) >$ (*векторы-ошибки из классов* $< (1, 2, \nu + 2) >$ *и* $< (1, \nu + 1, \nu + 2) >$ *имеют диаметр* $\nu + 1$). *Для каждого следующего значения* $Д > \nu + 2$ *количество Г-орбит тройных ошибок диаметром Д уменьшается на 3 по отношению к предыдущему.*

Пример 3.4. Составим таблицу Г-орбит векторов-ошибок весом 3 по значениям диаметров в пространстве E_{15}. Поскольку $15 = 6 \cdot 2 + 3$, то согласно предложению 2.13 здесь имеется $6 \cdot 2^2 + 3 \cdot 2 = 30$ полных Г-орбит диаметрами от 3 до 10 рассматриваемых векторов-ошибок плюс одна Г-орбита мощностью 5 и максимального диаметра $Д = 4 \cdot 2 + 3 = 11$.

Таблица 3.2

Таблица Г-орбит векторов-ошибок весом 3 в пространстве E_{15}

Значение диаметра $Д_i$	Кол-во n_i Г-орбит диаметром $Д_i$	Список образующих Г-орбит векторов-ошибок весом 3 и диаметром $Д_i$
1	2	3
3	1	(1, 2, 3)
4	2	(1, 2, 4); (1, 3, 4)
5	3	(1, 2, 5); (1, 3, 5); (1, 4, 5)
6	4	(1, 2, 6); (1, 3, 6); (1, 4, 6); (1, 5, 6)
7	5	(1, 2, 7); (1, 3, 7); (1, 4, 7); (1, 5, 7); (1, 6, 7)
8	6	(1, 2, 8); (1, 3, 8); (1, 4, 8); (1, 5, 8); (1, 6, 8); (1, 7, 8)
9	6	(1, 2, 9); (1, 3, 9); (1, 4, 9); (1, 5, 9); (1, 6, 9); (1, 7, 9)
10	3	(1, 4, 10); (1, 5, 10); (1, 6, 10)
11	1	(1, 6, 11)

Пример 3.5. Составим аналогичную таблицу в пространстве E_{31}. Здесь $31 = 6 \cdot 5 + 1$. Согласно предложению 2.10 здесь векторы-ошибки весом 3 имеют диаметры в диапазоне от 3 до 21, делятся на 145 полных Г-орбит.

Таблица 3.3

Таблица Г-орбит векторов-ошибок весом 3 в пространстве E_{31}

Значение диаметра $Д_i$	Кол-во n_i Г-орбит диаметром $Д_i$	Список образующих Г-орбит векторов-ошибок весом 3 и диаметром $Д_i$
1	2	3
3	1	(1, 2, 3)
4	2	(1, 2, 4); (1, 3, 4)
5	3	(1, 2, 5); (1, 3, 5); (1, 4, 5)
6	4	(1, 2, 6); (1, 3, 6); (1, 4, 6); (1, 5, 6)
7	5	(1, 2, 7); (1, 3, 7); (1, 4, 7); (1, 5, 7); (1, 6, 7)

Окончание табл. 3.3

1	2	3
8	6	(1, 2, 8); (1, 3, 8); (1, 4, 8); (1, 5, 8); (1, 6, 8); (1, 7, 8)
9	7	(1, 2, 9); (1, 3, 9); (1, 4, 9); (1, 5, 9); (1, 6, 9); (1, 7, 9); (1, 8, 9)
10	8	(1, 2, 10); (1, 3, 10),…,(1, 9, 10)
11	9	(1, 2, 11); (1, 3, 11),…,(1, 10, 11)
12	10	(1, 2, 12); (1, 3, 12),…,(1, 11, 12)
13	11	(1, 2, 13); (1, 3, 13),…,(1, 12, 13)
14	12	(1, 2, 14); (1, 3, 14),…,(1, 13, 14)
15	13	(1, 2, 15); (1, 3, 15),…,(1, 14, 15)
16	14	(1, 2, 16); (1, 3, 16),…,(1, 15, 16)
17	14	(1, 2, 17); (1, 3, 17),…,(1, 16, 17)
18	11	(1, 2, 18); (1, 3, 18),…,(1, 17, 18)
19	8	(1, 6, 19); (1, 7, 19); (1, 8, 19); (1, 9, 19); (1, 10, 19); (1, 11, 19); (1, 12, 19); (1, 13, 19)
20	5	(1, 8, 20); (1, 9, 20); (1, 10, 20); (1, 11, 20); (1, 12, 20)
21	2	(1, 10, 21); (1 ,11, 21)

Ниже приведена табл. 3.4, отражающая количество Г-орбит ошибок весом 2 – 4 на различных длинах в диапазоне 15 – 255.

Таблица 3.4

Количество Г-орбит ошибок весом 2 – 4 на различных длинах

Размерность *n*		7	15	31	63	127	255
Ошибки весом 2. Количество	Ошибок	21	105	465	1953	8001	32385
	Г-орбит	3	7	15	31	63	127
Ошибки весом 3. Количество	Ошибок	35	455	4495	39711	333375	2731135
	Г-орбит	5	31	145	631	2625	10711
	В т.ч. неполных	–	1	–	1	–	1
Ошибки весом 4. Количество	Ошибок	35	1365	14465	595665	10334625	182061175
	Г-орбит	5	91	1015	9455	81375	674751

3.9. Действие циклотомических подстановок на пространствах ошибок двоичных кодов

Действие группы Φ на векторы пространства E_7 иллюстрирует рис. 3.3.

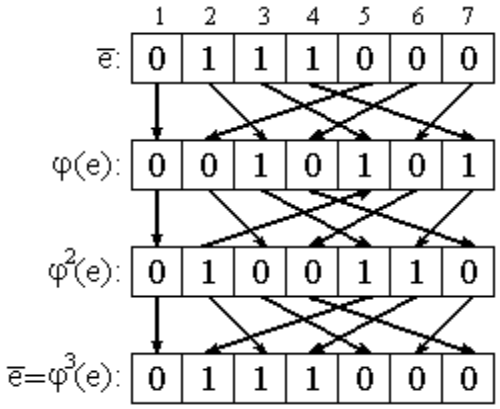

Рис. 3.3. Действие циклотомической подстановки φ и ее степеней на пространстве E_7, в частности, на вектор $\bar{e} = (0111000)$

Определение 3.6. Совокупность всех различных векторов $\varphi^s(\bar{e})$, $0 \le s \le m-1$, для данного фиксированного вектора $\bar{e} \in E_n$ называется Ф-орбитой, или циклотомической орбитой вектора $\bar{e}$ при действии группы Ф на пространстве E_n и обозначается через $<\bar{e}>_\Phi$.

По аналогии с теоремой 3.5 доказывается

Предложение 3.8. Для произвольного фиксированного вектора $\bar{e} \in E_n$ его Ф-орбита $<\bar{e}>_\Phi$ состоит из μ элементов, где $\mu = m$ или μ делит m. При этом μ – наименьшее натуральное число с условием $\varphi^\mu(\bar{e}) = \bar{e}$, а Ф-орбита $<\bar{e}>_\Phi$ имеет следующую структуру: $<\bar{e}>_\Phi = \{\bar{e}, \varphi(\bar{e}), ..., \varphi^{\mu-1}(\bar{e})\}$. Все векторы из $<\bar{e}>_\Phi$ имеют одинаковый вес.

Естественно Ф-орбиты пространства E_n называть полными, если они содержат по m элементов, а остальные – неполными. Так, в любом пространстве E_n (n – нечетно) Ф-орбита $<(1)>_\Phi$ состоит из одного вектора $(1) = (100...0)$, а Ф-орбита $<(2)>_\Phi$ состоит из m элементов для вектора $(2) = (010...0)$, и следовательно, является полной.

Пример 3.6. Выпишем Ф-орбиты векторов весом 1 в пространстве E_{15}.

$$<(1)>_\Phi = \{(1)\}; <(2)>_\Phi = \{(2); (3); (5); (9)\}; <(6)>_\Phi = \{(6); (11)\};$$
$$<(8)>_\Phi = \{(8); (15); (14); (12)\}.$$

Таким образом, 15 векторов-ошибок весом 1 делятся на 5 Ф-орбит; 3 из них – полные, содержат по 4 вектора, 1 имеет мощность 2, 1 – мощность 1.

Предложение 3.9. *Пусть* $J = \left\{\bar{e}, \sigma(\bar{e}), \ldots, \sigma^{\ell-1}(e)\right\}$, *где* $\ell = n$ *или* ℓ –

делитель n, *– Г-орбита векторов-ошибок из* E_n, *а*

$$\varphi(J) = \left\{ \varphi(\bar{e}), \varphi(\sigma(\bar{e})), \ldots, \varphi\left(\sigma^{\ell-1}(e)\right) \right\}.$$

Тогда $\varphi(J)$ *– также Г-орбита векторов из* E_n.

Доказательство. Поскольку φ – биекция на E_n, то $\varphi(J)$ содержит ℓ различных элементов. По лемме 3.2 $\varphi(J) = \left\{\varphi(\bar{e}), \sigma^2(\varphi(\bar{e})), \ldots, \sigma^{2\ell-2}(\varphi(\bar{e})\right\}$ – часть Г-орбиты $<\varphi(\bar{e})>$, содержащая ℓ элементов этой орбиты. Если $\ell = n$, то $\varphi(J)$ – полная Г-орбита. Пусть $\ell < n$, т. е. $\ell = n/\tau$ для подходящего натурального τ $\sigma^n(\bar{g}) = \bar{g}$ для всякого $\bar{g} \in E_n$, в частности, $\sigma^n(\varphi(\bar{e})) = \varphi(\bar{e})$ или $\sigma^{\tau\ell}(\varphi(\bar{e})) = \varphi(\bar{e})$. Подействуем на обе части последнего равенства подстановкой σ^{ℓ}. Получим $\sigma^{\ell+\tau\ell}(\varphi(\bar{e})) = \sigma^{\ell}(\varphi(\bar{e}))$. Поскольку τ нечетно, то $\tau = 2s+1$ для подходящего целого $s \geq 1$. Тогда

$$\sigma^{\ell+\tau\ell}(\varphi(\bar{e})) = \sigma^{(2+2s)\ell}(\varphi(\bar{e})) = \sigma^{2\ell(s+1)}(\varphi(\bar{e})) = \varphi(\bar{e}),$$

поскольку $\sigma^{2\ell}(\varphi(\bar{e})) = \varphi(\sigma^{l}(\bar{e})) = \varphi(\bar{e})$. Таким образом, $\sigma^{\ell}(\varphi(\bar{e})) = \varphi(\bar{e})$. Следовательно, *Г*-орбита $<\varphi(\bar{e})>$ содержит не более ℓ элементов и поэлементно совпадает с $\varphi(J)$. Другими словами, $\varphi(J)$ – *Г*-орбита мощностью ℓ. Предложение полностью доказано.

Следствие. Группа $\Phi = \left\{\varphi, \varphi^2, \ldots, \varphi^m = e\right\}$ *является группой подстановок на множестве* E_n/Γ *всех Г-орбит пространства* E_n.

Доказательство. По свойствам Г-орбит (предложение 3.2) Г-орбиты $<\bar{e}>$ и $\varphi(<\bar{e}>) = <\varphi(\bar{e})>$ либо совпадают, либо не пересекаются. Отсюда и вытекает утверждение.

Определение 3.7. Пусть J *– фиксированная Г-орбита векторов-ошибок из* E_n. *Совокупность всех попарно различных Г-орбит* $\varphi^k(J), 0 \leq k \leq m-1$, *называется* Φ*-орбитой класса* J *(или циклоклассом Г-орбиты* J*) при действии* Φ *на множестве* E_n/Γ *и обозначается* $<J>_{\Phi}$.

Теорема 3.7. *Для произвольного класса* $J \in E_n/\Gamma$ *его Ф-орбита* $<J>_{\Phi}$ *состоит из* μ *классов, где* $\mu = m$ *или* μ *делит* m. *При этом* μ *– наименьшее натуральное число с условием* $\varphi^{\mu}(J) = J$, *а* $<J>_{\Phi}$ *имеет следующую структуру*:

$$<J>_{\Phi} = \left\{J, \varphi(J), \ldots, \varphi^{\mu-1}(J)\right\}. \qquad (3.6)$$

Доказательство аналогично доказательству теоремы 3.5.

Из теоремы 3.7 следует, что действие Φ на классы из $<J>_{\Phi}$ не выводит за пределы $<J>_{\Phi}$ и что Φ действует транзитивно внутри $<J>_{\Phi}$: для любых J и I из $<J>_{\Phi}$ найдется в силу формулы (3.6) такая подстановка $g \in \Phi$, что $g(I) = J$.

3.10. G-орбиты векторов-ошибок

Определение 3.8. Два вектора $\bar{f}$ и $\bar{g}$ из E_n называются G-эквивалентными, если найдется такая подстановка $\tau = \varphi^j \sigma^i \in G$, что $\bar{g} = \tau(\bar{f})$.

Очевидно, G-эквивалентные векторы-ошибки должны иметь одинаковый вес. Заметим, что не все векторы-ошибки весом 2 попарно G-эквивалентны. Ведь одному вектору может быть G-эквивалентно не более $mn-1$ других векторов в силу теоремы 3.4. Векторов-ошибок весом 2 имеется $n(n-1)/2 > m \cdot n$ при $n > 2m+1$, т. е. при $2^m - 1 > 2m+1$, что выполняется при всех целых $m \geq 4$.

Определение 3.9. G-орбитой называется совокупность всех попарно G-эквивалентных между собой векторов-ошибок из E_n.

Пусть $\bar{e}$ – фиксированный вектор из данной G-орбиты. В силу транзитивности свойства G-эквивалентности эта орбита состоит из векторов пространства E_n, G-эквивалентных вектору $\bar{e}$. Поэтому G-орбиту с вектором $\bar{e}$ будем иногда обозначать через $<\bar{e}>_G$.

Предложение 3.10. Пусть $<\bar{e}>$ – Г-орбита, порожденная вектором $\bar{e} \in E_n$. Тогда G-орбита $<\bar{e}>_G$ состоит из всех векторов, принадлежащих всем Г-орбитам из Ф-орбиты $<\bar{e}>_G = \{<\bar{e}>, \varphi<\bar{e}>, \varphi^2<\bar{e}>, \ldots, \varphi^{\mu-1}<\bar{e}>\}$.

Доказательство следует из определения G-орбиты, формулы (3.6), а также теоремы 3.5.

Пример 3.7. 31 Г-орбита векторов-ошибок весом 1, 2, 3 из пространства E_{15} (пример 3.4) делится на следующие G-орбиты:

$J_1^{\mathrm{G}} = I_1 = <(1)>$ – множество векторов весом 1;

$J_{21}^{\mathrm{G}} = <(1,2)>_{\mathrm{G}} = \{<(1,2)>; <(1,3)>; <(1,5)>; <(1,8)>\}$;

$J_{22}^{\mathrm{G}} = <(1,4)>_{\mathrm{G}} = \{<(1,4)>; <(1,7)>\}$; $J_{23}^{\mathrm{G}} = <(1,6)>_{\mathrm{G}} = \{<(1,6)>\}$;

$J_{31}^{\mathrm{G}} = <(1,2,3)>_{\mathrm{G}} = \{<(1,2,3)>; <(1,3,5)>; <(1,5,9)>; <(1,2,9)>\}$;

$J_{32}^{\mathrm{G}} = <(1,2,4)>_{\mathrm{G}} = \{<(1,2,4)>; <(1,3,7)>; <(1,4,8)>; <(1,2,8)>\}$;

$J_{33}^{\mathrm{G}} = <(1,3,4)>_{\mathrm{G}} = \{<(1,3,4)>; <(1,5,7)>; <(1,5,8)>; <(1,7,8)>\}$;

$J_{34}^{\mathrm{G}} = <(1,2,5)>_{\mathrm{G}} = \{<(1,2,5)>; <(1,3,9)>\}$;

$J_{35}^{\mathrm{G}} = <(1,4,5)>_{\mathrm{G}} = \{<(1,4,5)>; <(1,7,9)>\}$;

$J_{36}^{\mathrm{G}} = <(1,2,6)>_{\mathrm{G}} = \{<(1,2,6)>; <(1,6,8)>; <(1,5,6)>; <(1,3,8)>\}$;

$J_{37}^{\mathrm{G}} = <(1,3,6)>_{\mathrm{G}} = \{<(1,3,6)>; <(1,6,10)>; <(1,6,9)>; <(1,6,7)>\}$;

$J_{38}^{\mathrm{G}} = <(1,4,6)>_{\mathrm{G}} = \{<(1,4,6)>; <(1,5,10)>; <(1,4,9)>; <(1,2,7)>\}$;

$J_{39}^{\mathrm{G}} =< (1, 4, 7) >_{\mathrm{G}} = \{< (1, 4, 7) >; < (1, 4, 10) >\};$

$J_{3\,10}^{\mathrm{G}} =< (1, 6, 11) >_{\mathrm{G}} = \{< (1, 6, 11) >\}$ – единственная неполная Г-орбита.

Таким образом, 39 Г-орбит ошибок весом 1 – 3 из пространства E_{15} разбиваются на 14 G-орбит, причем 3 из них совпадают с соответствующими Г-орбитами, 4 G-орбиты содержат по 2 Г-орбиты и 7 G-орбит содержат по 4 Г-орбиты.

Пример 3.8. В двоичном пространстве E_{31} имеется 15 Г-орбит ошибок весом 2, которые делятся на 3 G-орбиты по 5 Г-орбит в каждой:

$J_{21}^{\mathrm{G}} =< (1, 2) >_{\mathrm{G}} = \{< (1, 2) >; < (1, 3) >; < (1, 5) >; < (1, 9) >; < (1, 16) >\};$

$J_{22}^{\mathrm{G}} =< (1, 4) >_{\mathrm{G}} = \{< (1, 4) >; < (1, 7) >; < (1, 13) >; < (1, 8) >; < (1, 15) >\};$

$J_{23}^{\mathrm{G}} =< (1, 6) >_{\mathrm{G}} = \{< (1, 6) >; < (1, 11) >; < (1, 12) >; < (1, 10) >; < (1, 14) >\},$

145 Γ-орбит векторов-ошибок весом 3 (пример 3.5), в свою очередь делящихся на 29 циклоклассов.

Таким образом, проведенные исследования показали, что циклотомические подстановки переводят друг в друга Г-орбиты ошибок одинакового веса. Кроме того, описана взаимосвязь циклотомических и циклических подстановок, а также некоммутативная группа G, порожденная этими подстановками. Построена классификация векторов-ошибок посредством группы G и установлено, что G-орбиты состоят из циклотомически связанных Г-орбит ошибок.

4. Спектры синдромов орбит векторов-ошибок

4.1. Влияние группы циклических сдвигов на синдромы ошибок в БЧХ-кодах

Выше установлено, что векторы-ошибки под действием группы Г циклических сдвигов координат векторов делятся на непересекающиеся классы – Г-орбиты. Векторы каждой Г-орбиты имеют тесную взаимосвязь – каждый из них можно получить циклическими сдвигами какого-нибудь фиксированного вектора Г-орбиты. Такая же тесная связь существует и между синдромами векторов-ошибок каждой Г-орбиты. Ее описанию и посвящен данный раздел.

Теорема 4.1. *Пусть* $\bar{e}$ *– произвольный вектор ошибок в БЧХ-коде С с проверочной матрицей* (*2.2*). *Пусть* $S(\bar{e}) = (s_1, s_2, ..., s_{\delta-1})$ *– синдром вектора-ошибки* $\bar{e}$. *Тогда*

$$S(\sigma(\bar{e})) = (\beta^b s_1, \beta^{b+1} s_2, ..., \beta^{b+i-1} s_i, ..., \beta^{b+\delta-2} s_{\delta-1}). \qquad (4.1)$$

Доказательство. Пусть вектор ошибок $\bar{e} = (e_{i_1}, e_{i_2}, ..., e_{i_w})$, т. е. имеет отличными от нуля только координаты $e_{i_1}, e_{i_2} ..., e_{i_w}$ с номерами $i_1 < i_2 < ... < i_w$ соответственно, $1 \le w \le n$. Тогда по определению синдрома

$$S(\bar{e}) = \bar{e}H^T = (e_{i_1} \cdot \beta^{(i_1-1)b} + ... + e_{i_w} \cdot \beta^{(i_w-1)b}, ..., e_{i_1} \cdot \beta^{(i_1-1)(b+\delta-2)} + ... + e_{i_w} \cdot \beta^{(i_w-1)(b+\delta-2)}).$$

Если $i_w < n$, то $\sigma(\bar{e})$ имеет на позициях (и только на них) $i_1 + 1, ..., i_w + 1$ ненулевые координаты, равные соответственно $e_{i_1}, e_{i_2}, ..., e_{i_w}$. Поэтому $S(\sigma(\bar{e})) = (s_1^1, ..., s_{\delta-1}^1) = (e_{i_1} \cdot \beta^{i_1 b} + ... + e_{i_w} \cdot \beta^{i_w b}, ..., e_{i_1} \cdot \beta^{i_1(b+\delta-2)} + ... + e_{i_w} \cdot \beta^{i_w(b+\delta-2)}) =$ $= (\beta^b \cdot s_1, ..., \beta^{b+\delta-2} \cdot s_{\delta-1})$, что доказывает формулу (3.7). Пусть $i_w = n$, тогда $\beta^{bn} = 1$ и у вектора $\sigma(\bar{e})$ отличны от нуля 1-я, $(i_1 + 1)$,…, $(i_{w-1} + 1)$-я координаты (и только они), равные соответственно $e_{i_w}, e_{i_1}, ..., e_{i_w - 1}$. Тогда

$$S(\sigma(\bar{e})) = (s_1^1, s_2^1, ..., s_{\delta-1}^1) =$$

$$= (e_{i_1} \cdot \beta^{i_1 b} + ... + e_{i_w - 1} \cdot \beta^{i_{[w-i]} b} + e_n \cdot \beta^b, ..., e_{i_1} \cdot \beta^{i_1(b+\delta-2)} + ... + e_{i_{[w-i]}} \cdot \beta^{i_{[w-i]}(b+\delta-2)}) =$$

$$= (e_{i_1} \cdot \beta^{i_1 b} + ... + e_{i_{[w-i]}} \cdot \beta^{i_{[w-i]} b} + e_n \cdot \beta^{(1+n)b}, ..., e_{i_1} \cdot \beta^{i_1(b+\delta-2)} + ...$$

$$+ e_{i_{[w-i]}} \cdot \beta^{(i_{[w-i]})(b+\delta-2)} + e_n \cdot \beta^{(1+n)(b+\delta-2)}) = (\beta^b \cdot s_1, ..., \beta^{(b+\delta-2)} \cdot s_{\delta-1}),$$

что и требовалось доказать.

Следствие 1. В условиях теоремы 4.1 для произвольного целого λ синдром

$$S(\sigma^\lambda(\bar{e})) = (\beta^{\lambda b} \cdot s_1, \beta^{\lambda(b+1)} \cdot s_2, ..., \beta^{\lambda(b+i-1)} \cdot s_i, ..., \beta^{\lambda(b+\delta-2)} \cdot s_{\delta-1}). \qquad (4.2)$$

Доказательство получается кратным применением формулы (4.1).

Следствие 2. Если компонента s_i, $1 \le i \le \delta - 1$, синдрома $S(\bar{f})$ равна 0 (отлична от нуля), то и у всех векторов-ошибок из Г-орбиты $< \bar{f} >$ соответст-

вующая компонента синдрома равна нулю (отлична от нуля).

Следствие 3. Если БЧХ-код задан проверочной матрицей (2.3), то

$$S(\sigma(\bar{e})) = (\beta s_1, \beta^3 s_2, \beta^5 s_3, ..., \beta^{2i-1} s_i, ..., \beta^{2t-1} s_t). \qquad (4.3)$$

Пример 4.1. Приведем список (табл. 4.1) всех векторов Г-орбиты $<\bar{e}>=<(1, 2, 5)>$ в 7-мерном пространстве и их синдромов в примитивном БЧХ-коде C над полем $GF(2^3)$, проверочная матрица $H = (\alpha^i, \alpha^{3i})^T$ которого порождена элементом α – корнем полинома $x^3 + x + 1$.

Таблица 4.1

Векторы Г-орбиты $<(1, 2, 5)>$ *и их синдромы*

$\bar{e}$	1	1	0	0	1	0	0	(α^6, α^6)
$\sigma(\bar{e})$	0	1	1	0	0	1	0	$(1, \alpha^2)$
$\sigma^2(\bar{e})$	0	0	1	1	0	0	1	(α, α^5)
$\sigma^3(\bar{e})$	1	0	0	1	1	0	0	(α^2, α)
$\sigma^4(\bar{e})$	0	1	0	0	1	1	0	(α^3, α^4)
$\sigma^5(\bar{e})$	0	0	1	0	0	1	1	$(\alpha^4, 1)$
$\sigma^6(\bar{e})$	1	0	0	1	0	0	1	(α^5, α^3)

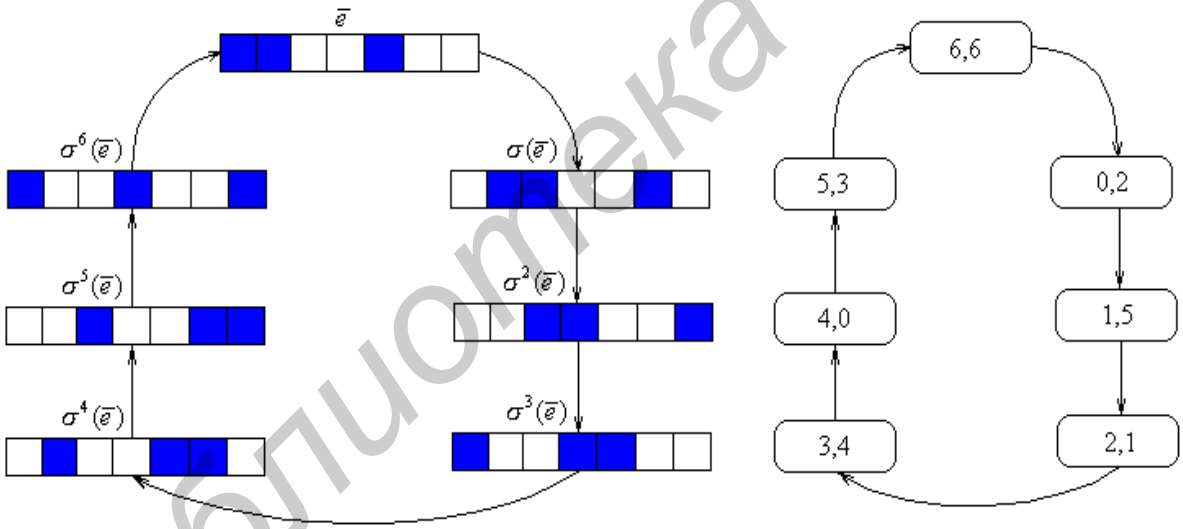

Рис. 4.1. Взаимно однозначная зависимость между циклическими сдвигами векторов Г-орбиты $<\bar{e}>=<(1,2,5)>$ в 7-мерном пространстве и соответствующими преобразованиями показателей компонент синдромов в БЧХ-коде C

Из табл. 4.1 видно, как при переходе от данного вектора $\bar{g}$ к вектору $\sigma(\bar{g})$ первая координата синдрома $S(\bar{g}) = (s_1, s_2)$ умножается на α, а вторая – на α^3 в полном соответствии с формулой (4.3), т. е. к показателю $\deg s_1$ прибавляется целое число 1 по модулю 7, а к показателю $\deg s_2$ – число 3 по модулю 7. Эта закономерность представлена на рис. 4.1.

Определение 4.1. Спектром синдромов в коде C Г-орбиты J назовем множе-

ство синдромов всех векторов-ошибок из J в этом коде и обозначим через $S(J)$. Спектр $S(J)$ будем называть полным, если его мощность совпадает с мощностью Г-орбиты J : $|S(J)| = |J|$, в противном случае $S(J)$ будем называть неполным.

Теорема 4.2. Пусть в БЧХ-коде C с проверочной матрицей (2.2) вектор-ошибка $\bar{e}$ имеет синдром $S(\bar{e}) = (s_1, s_2, ..., s_{\delta-2})$. Спектр синдромов Г-орбиты $J =< \bar{e} >$ состоит из всех попарно различных векторов вида

$$(\beta^{\lambda b} s_1, \beta^{\lambda(b+1)} s_2, ..., \beta^{\lambda(b+j-1)} s_j, ..., \beta^{\lambda(b+\sigma-2)} s_{\sigma-1}), \ 0 \le \lambda \le n-1. \qquad (4.4)$$

Пусть синдром $S(\bar{e})$ имеет компоненту $s_j \neq 0$ для такого целого j, $1 \le j \le \delta - 1$, что НОД $(b + j - 1, n) = 1$. Тогда $S(J)$ содержит n попарно различных синдромов и, следовательно, $|S(J)| = |J| = n$.

Доказательство. Первая часть утверждения следует из теоремы 3.5 о структуре Г-орбит, формулы (4.1) и того факта, что $\beta^n = 1$. Пусть НОД $(b + j - 1, n) = 1$. Тогда β^{b+j-1} является примитивным корнем n-й степени из 1 в поле $GF(q^m)$. Так как $s_j \neq 0$, то элементы

$$s_j, \beta^{b+j-1} \cdot s_j, \beta^{2(b+j-1)} \cdot s_j, ..., \beta^{(n-1)b+j-1} \cdot s_j$$

попарно различны и в силу формулы (4.1) являются j-ми компонентами синдромов из $S(J)$. Их количество равно n. Следовательно, $|S(J)| = n$. Но тогда $|J| = n$, что и требовалось доказать.

Следствие. В двоичном примитивном БЧХ-коде C с проверочной матрицей (2.3) для каждого вектора $\bar{e}$ с синдромом $S(\bar{e}) = (s_1, s_2, ..., s_t)$ спектр синдромов $S(< \bar{e} >)$ состоит из всех попарно различных векторов:

$$(\alpha^i s_i, \alpha^{3i} s_2, ..., \alpha^{(2t-1)i} s_t), \ 0 \le i \le 2^m - 2. \qquad (4.5)$$

Замечание. Теорема 4.2 утверждает, что, как и векторы каждой Г-орбиты J, синдромы спектра $S(J)$ произвольной Г-орбиты J векторов-ошибок можно сконструировать по формуле (4.4) из синдрома $S(\bar{e})$ любого вектора $\bar{e} \in J$. Этот факт можно выразить кратко следующим равенством: $S(< \bar{e} >) =< S(\bar{e}) >$. При условии полноты $S(J)$ существует полное взаимно-однозначное соответствие между циклическими сдвигами векторов и соответствующими преобразованиями их синдромов.

4.2. Влияние циклотомических подстановок на синдромы ошибок в БЧХ-кодах

Выше определено и исследовано действие степеней циклотомической подстановки φ на векторы пространства E_n нечетной размерности n. Это пространство является пространством ошибок двоичного БЧХ-кода C длиной n с проверочной

матрицей H, определяемой формулой (2.2) над полем $GF(2^m)$ для наименьшего натурального m с условием: $2^m - 1$ делится на n или же $n = 2^m - 1$. Исследуем действие группы Φ, порожденной подстановкой φ, на синдромы ошибок в этом коде.

Теорема 4.3. *Пусть* $S(\bar{e}) = (s_1, s_2, ..., s_{\delta-1})$ *– синдром вектора-ошибки* $\bar{e}$ *в БЧХ-коде C с проверочной матрицей* (*2.2*). *Тогда синдром*

$$S(\varphi(\bar{e})) = (s_1^2, s_2^2, ..., s_{\delta-1}^2).$$

Доказательство. Пусть $\bar{e} = (i_1, i_2, \ldots, i_s)$, где $1 \le i_1 < i_2 < \ldots < i_s \le n$. По определению действия циклотомической подстановки

$$\varphi(\bar{e}) = (\overline{2i_1 - 1}, \overline{2i_2 - 1}, \ldots, \overline{2i_s - 1}).$$

Синдром

$$S(\bar{e}) = \bar{e}H^T = (\beta^{b(i_1-1)} + \beta^{b(i_2-1)} + ... + \beta^{b(i_s-1)}; \beta^{(b+1)(i_1-1)} + \beta^{(b+1)(i_2-1)} + ... +$$

$$+ \beta^{(b+1)(i_s-1)}; ...; \beta^{(b+\delta-2)(i_1-1)} + \beta^{(b+\delta-2)(i_2-1)} + ... + \beta^{(b+\delta-2)(i_s-1)}).$$

С учетом равенства $\beta^n = 1$ и, следовательно, $\beta^{bn} = 1$, синдром

$$S(\varphi(\bar{e})) = (\beta^{b(2i_1-2)} + \beta^{b(2i_2-2)} + ... + \beta^{b(2i_s-2)}; \beta^{(b+1)(2i_1-2)} + \beta^{(b+1)(2i_2-2)} + ... +$$

$$+ \beta^{(b+1)(2i_s-2)}; ...; \beta^{(b+\delta-2)(2i_1-2)} + \beta^{(b+\delta-2)(2i_2-2)} + ... + \beta^{(b+\delta-2)(2i_s-2)}) =$$

$$= (s_1^2, s_2^2, ..., s_{\delta-1}^2).$$

Предложение полностью доказано.

Следствие 1. Если одна из компонент s_i, $1 \le i \le \delta - 1$, синдрома $S(\bar{e})$ равна 0 (отлична от нуля, равна 1), то и у синдрома $S(\varphi(\bar{e}))$ соответствующая компонента равна 0 (отлична от нуля, равна 1).

Естественным является следующее

Определение 4.2. Синдромным спектром Φ-орбиты $<\bar{e}>_\Phi$ в БЧХ-коде C называется множество синдромов всех векторов данной Φ-орбиты и обозначается через $S(<\bar{e}>_\Phi)$.

Следствие 2. В условия теоремы 4.3 всякого целого $k, 1 \le k < m$, синдром

$$S(\varphi^k(\bar{e})) = (s_1^{2^k}, s_2^{2^k}, ..., s_{\delta-1}^{2^k}). \qquad (4.6)$$

Поскольку мультипликативная группа поля $GF(2^m)$ имеет порядок $2^m - 1$, то $s_i^{2^m} = s_i$. Поэтому синдромный спектр произвольной Φ-орбиты имеет не более, чем m различных синдромов, выражаемых формулой (4.6).

Следствие 3. Пусть $<\bar{e}>_\Phi$ – полная Ф-орбита векторов-ошибок в коде C, порожденная вектором $\bar{e}$. Пусть i-я компонента $s_i, 1 \le i \le \delta - 1$, синдрома $S(\bar{e})$ отлична от нуля и единицы и, следовательно, $s_i = \alpha^j$ для некоторого целого $j, 0 < j < n$. Тогда показатели i-й компоненты спектра синдромов $S(<\bar{e}>_\Phi)$ образуют циклотомический класс по модулю m $j, \overline{2j}, \overline{2^2 j}, ..., \overline{2^{m-1} j}$.

4.3. Спектры синдромов циклоклассов векторов-ошибок в БЧХ-кодах

Теорема 4.4. *В БЧХ-коде* C *с проверочной матрицей* (*2.2*) *спектр синдромов* $S(<\bar{e}>_G)$ *циклокласса* $<\bar{e}>_G$ *состоит из всевозможных попарно различных векторов*:

$$\beta^{bi}s_1^{2^j}, \beta^{(b+1)i}s_2^{2^j}, ..., \beta^{(b+\delta-2)i}s_{\delta-1}^{2^j}, \text{ где } 0 \le i \le n-2,\ 0 \le j < m. \qquad (4.7)$$

Доказательство следует из теорем 4.1 и 5.3.

Следствие 1. Пусть в условиях теоремы 4.4 у синдрома $S(\bar{e}) = (s_1, s_2, ..., s_{\delta-1})$ вектора $\bar{e} \in E_n$ какая-нибудь из компонент $s_i = 0$ ($s_i \neq 0, s_i = 1$), $i = 1, 2, ..., \delta - 1$. Тогда у всех векторов G-орбиты $<\bar{e}>_G$ соответствующая компонента синдрома также равна нулю (отлична от нуля, равна 1).

Следствие 2. Если $\varphi(J)$ – образ Γ-орбиты J под действием циклотомической подстановки φ, то спектр $S(\varphi(J))$ получается возведением в квадрат компонент всех синдромов спектра $S(J)$ Если спектр $S(J)$ – полный, то спектр $S(\varphi(J))$ – также полный.

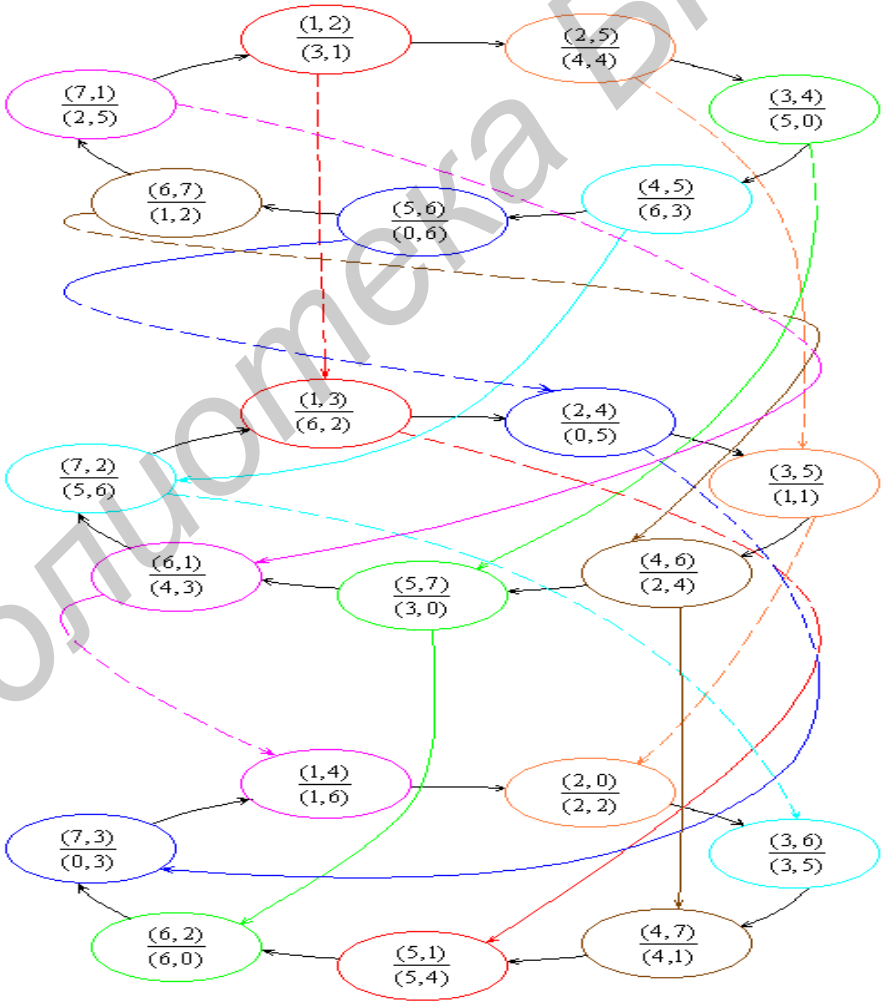

Рис. 4.2. Конструктивное представление *G*-орбиты ошибок весом 2 в БЧХ-коде длиной 7 с помощью циклических и циклотомических подстановок с адекватным преобразованием показателей компонент синдромов

Пример 4.2. Составим список циклоклассов в пространстве E_{15}, составляющих их Γ-орбит, образующих Γ-орбит, синдромов образующих в БЧХ-коде C_7 над полем $GF(2^4)$ с примитивным элементом (α-корнем) полинома $x^4 + x + 1$ для всех векторов весом 1–3.

Таблица 4.2

Структура G-орбит ошибок весом 1–3 и синдромов составляющих их Г-орбит

№ п/п	G-орбита $< \bar{e} >_G$	Γ-орбита $< \bar{e}' >$	Синдром $S(\bar{e}')$
1	2	3	4
1	$<(1)>_G$	$<(1)>$	$(1, 1, 1)$
2	$<(1, 2)>_G$	$<(1, 2)>$	$(\alpha^4, \alpha^{14}, \alpha^{10})$
		$<(1, 3)>$	$(\alpha^8, \alpha^{13}, \alpha^5)$
		$<(1, 5)>$	$(\alpha, \alpha^{11}, \alpha^{10})$
		$<(1, 9)>$	$(\alpha^2, \alpha^7, \alpha^5)$
3	$<(1, 4)>_G$	$<(1, 4)>$	$(\alpha^{14}, \alpha^7, 0)$
		$<(1, 7)>$	$(\alpha^{13}, \alpha^{14}, 0)$
4	$<(1, 6)>_G$	$<(1, 6)>$	$(\alpha^{10}, 0, \alpha^5)$
5	$<(1, 2, 3)>_G$	$<(1, 2, 3)>$	$(\alpha^{10}, \alpha^8, 0)$
		$<(1, 3, 5)>$	$(\alpha^5, \alpha, 0)$
		$<(1, 5, 9)>$	$(\alpha^{10}, \alpha^2, 0)$
		$<(1, 2, 9)>$	$(\alpha^5, \alpha^4, 0)$
6	$<(1, 2, 4)>_G$	$<(1, 2, 4)>$	$(\alpha^7, \alpha^4, \alpha^5)$
		$<(1, 3, 7)>$	$(\alpha^{14}, \alpha^8, \alpha^{10})$
		$<(1, 5, 13)>$	$(\alpha^{13}, \alpha^1, \alpha^5)$
		$<(1, 9, 10)>$	$(\alpha^{11}, \alpha^2, \alpha^{10})$
7	$<(1, 3, 4)>_G$	$<(1, 3, 4)>$	$(\alpha^{13}, \alpha^{10}, \alpha^{10})$
		$<(1, 5, 7)>$	$(\alpha^{11}, \alpha^5, \alpha^5)$
		$<(1, 9, 13)>$	$(\alpha^7, \alpha^{10}, \alpha^{10})$
		$<(1, 2, 10)>$	$(\alpha^{14}, \alpha^5, \alpha^5)$
8	$<(1, 2, 5)>_G$	$<(1, 2, 5)>$	$(0, \alpha^5, 1)$
		$<(1, 3, 9)>$	$(0, \alpha^{10}, 1)$
9	$<(1, 4, 5)>_G$	$<(1, 4, 5)>$	$(\alpha^9, \alpha^2, \alpha^5)$
		$<(1, 7, 9)>$	$(\alpha^3, \alpha^4, \alpha^{10})$
10	$<(1, 2, 6)>_G$	$<(1, 2, 6)>$	$(\alpha^8, \alpha^3, 0)$
		$<(1, 3, 11)>$	$(\alpha^1, \alpha^6, 0)$
		$<(1, 5, 6)>$	$(\alpha^2, \alpha^{12}, 0)$

Окончание табл. 4.2

1	2	3	4
11	$<(1, 3, 6)>_G$	$<(1, 3, 6)>$	$(\alpha^4, \alpha^6, 1)$
		$<(1, 5, 11)>$	$(\alpha^8, \alpha^{12}, 1)$
		$<(1, 6, 9)>$	$(\alpha, \alpha^9, 1)$
		$<(1, 9, 11)>$	$(\alpha^2, \alpha^3, 1)$
12	$<(1, 4, 6)>_G$	$<(1, 4, 6)>$	$(\alpha^{12}, \alpha^9, \alpha^{10})$
		$<(1, 7, 11)>$	$(\alpha^9, \alpha^3, \alpha^5)$
		$<(1, 6, 13)>$	$(\alpha^3, \alpha^6, \alpha^{10})$
		$<(1, 10, 11)>$	$(\alpha^6, \alpha^{12}, \alpha^5)$
13	$<(1, 4, 7)>_G$	$<(1, 4, 7)>$	$(\alpha^8, \alpha^4, 1)$
		$<(1, 7, 13)>$	$(\alpha^1, \alpha^8, 1)$
14	$<(1, 6, 11)>_G$	$<(1, 6, 11)>$	$(0, 1, 0)$

Каждая G-орбита в данной таблице построена из Γ-орбит по циклу: следующая Γ-орбита есть образ предыдущей под действием φ, последняя при этом переходит в первую. Аналогично выбраны и образующие Γ-орбит. Поэтому компоненты синдрома каждой следующей образующей являются квадратами соответствующих компонент синдрома предыдущей образующей в полном соответствии со следствием 2 из предложения 4.3. При этом в полном соответствии со следствием 4 из предложения 4.3 показатели каждой компоненты спектра синдромов $S(<\bar{e}_i>_\Phi)$ для образующей $\bar{e}_i$ полной G-орбиты $<\bar{e}_i>_G$ образуют циклотомический класс по модулю 4. Например, для второй G-орбиты и для первой компоненты синдрома – это класс {4,8,1,2}, а для второй компоненты – это класс {14,13,11,7}, для третьей – это класс {10,5}.

Таким образом, зная образующую G-орбиты, а также ее синдром, можно однозначно восстановить элементы всей G-орбиты, синдромы всех векторов этого циклокласса (формула (4.7)).

Предложение 4.1. Пусть M – множество векторов в БЧХ-коде C с попарно различными синдромами. Тогда все векторы множества $\varphi(M)$ также имеют попарно различные синдромы.

Доказательство. Возьмем произвольные различные векторы $\bar{e}, \bar{f} \in M$ с синдромами $S(\bar{e}) = (s_1, s_2, ..., s_{\delta-1})$ и $S(\bar{f}) = (s_1^f, s_2^f, ..., s_{\delta-1}^f)$ соответственно. По условию $S(\bar{e}) \neq S(\bar{f})$. Это означает, что по крайней мере для одного из номеров $i, 1 \le i \le \delta - 1$, $s_i \neq s_i^f$. По теореме 4.3 у синдромов $S(\varphi(\bar{e}))$ и $S(\varphi(\bar{f}))$ i-я компонента равна s_i^2 и $(s_i^f)^2$ соответственно. Предположим, что

эти компоненты равны между собой. Это означает, что $s_i^2 + (s_i^f)^2 = 0$ или $(s_i + s_i^f)^2 = 0$. Поскольку в поле нет делителей нуля, то отсюда следует, что $s_i + s_i^f = 0$, т. е. $s_i = s_i^f$, что противоречит условию $s_i \neq s_i^f$. Следовательно, $S(\varphi(\bar{e})) \neq S(\varphi(\bar{f}))$. Предложение полностью доказано.

4.4. Влияние циклических подстановок на синдромы ошибок в реверсивных кодах

Исследуем действие группы Γ на синдромы ошибок реверсивных кодов (см. подразд. 2.8). Напомним, что реверсивный код C_R^m задается проверочной матрицей $H_R = (H_1, H_2)^T = (\alpha^i, \alpha^{-i})^T$, где α – примитивный элемент поля $GF(2^m)$, $m \geq 3$; $0 \leq i \leq n-1$ для $n = 2^m - 1$.

В соответствии со структурой матрицы H координаты вектора S сгруппируем последовательно в две группы по m координат в каждой. Тогда вектор S можно записать в виде $S = (s_1, s_2)$, где s_1 и s_2 – элементы поля $GF(2^m)$. Следовательно, $s_1 = \alpha^i, s_2 = \alpha^j$ для подходящих i, j из множества $T = \{-\infty, 0, 1, 2, ..., n-1\}$. Таким образом, вектор S может принимать $(n+1)^2 = 2^{2m}$ различных значений.

Теорема 4.5. *Пусть* $n = 2^m - 1$, $m \geq 3$. *Пусть* σ *– циклическая подстановка на координатах пространства* E_n:

$$\sigma(e_1, e_2, ..., e_n) = (e_n, e_1, e_2, ..., e_{n-1}).$$

Пусть $S(\bar{e}) = S = (s_1, s_2)$ *– синдром в реверсивном коде* C_R^m *вектора-ошибки* $\bar{e}$ *из* E_n. *Тогда для произвольного целого* λ *синдром в реверсивном коде* C_R^m *вектора-ошибки* $\sigma^\lambda(\bar{e})$ *равен* $S(\sigma^\lambda(\bar{e})) = (\alpha^\lambda s_1, \alpha^{-\lambda} s_2)$.

Доказательство. Пусть у вектора-ошибки $\bar{e}$ лишь координаты $i_1, i_2, ..., i_s$ равны 1, а остальные равны 0. Тогда синдром ошибок этого вектора $S(\bar{e}) = (s_1, s_2) = (\alpha^{i_1 - 1} + \alpha^{i_2 - 1} + ... + \alpha^{i_s - 1}, \alpha^{1-i_1} + \alpha^{1-i_2} + ... + \alpha^{1-i_s})$.

У вектора-ошибки $\sigma^\lambda(\bar{e})$ отличными от нуля будут координаты с номерами $\overline{i_1 + \lambda}$, $\overline{i_2 + \lambda}$, ..., $\overline{i_s + \lambda}$. Здесь $\overline{i_\mu + \lambda}$ – вычет по модулю n натурального числа $i_\mu + \lambda$, $\mu = 1, 2, ..., s$. Поскольку $\alpha^n = 1$, то $\alpha^{i_\mu + \lambda} = \alpha^{\overline{i_\mu + \lambda}}$. Поэтому

$$S(\sigma^\lambda(\bar{e})) = (\alpha^{i_1 + \lambda - 1} + \alpha^{i_2 + \lambda - 1} + ... + \alpha^{i_s + \lambda - 1}, \alpha^{1 - i_1 - \lambda} + \alpha^{1 - i_2 - \lambda} + ... + \alpha^{1 - i_s - \lambda}) =$$

$$= (\alpha^\lambda s_1, \alpha^{-\lambda} s_2),$$

что и требовалось доказать.

Предложение 4.2. Пусть в реверсивном коде C_R^m у синдромов векторов-ошибок из Г-орбиты J по крайней мере одна из координат s_1 или s_2 отлична от нуля. Тогда все синдромы векторов-ошибок из J попарно различны. При этом $|J| = |S(J)| = n$, т. е. Г-орбита J – полная с полным спектром синдромов.

Доказательство. При $s_1 \neq 0$ доказательство утверждения совпадает с доказательством предложения 3.10. В силу предложения 3.18 это доказательство переносится лишь с изменением знаков и на случай $s_2 \neq 0$.

Следствие (необходимое условие неполноты Г*-орбиты ошибок). Если* Г*-орбита J-неполная, то в реверсивном коде* C_R^m *ее спектр синдромов* $S(J) = \{(0,0)\}$.

Доказательство проводится методом от противного с учетом предложения 4.2.

Предложение 4.3. Синдромы $S = (s_1, s_2)$ векторов-ошибок весом 1, 2 в реверсивном коде C_R^m попарно различны, причем обе их координаты $s_1 \neq 0$ и $s_2 \neq 0$. Каждая Г-орбита векторов-ошибок весом 1, 2 является полной с полным спектром синдромов.

Доказательство. Тот факт, что у синдромов названных векторов-ошибок $s_1 \neq 0$ и $s_2 \neq 0$ очевиден, поскольку попарно различны столбцы у подматриц $H_1 = (\alpha^i)$ и $H_2 = (\alpha^{-i})$ проверочной матрицы H_R реверсивного кода. Полнота Г-орбит одиночных и двойных ошибок доказана ранее, а полнота их спектров гарантируется следствием из теоремы 4.5. Таким образом, предложение 4.3 полностью доказано.

5. Теория норм синдромов

5.1. Определение норм синдромов векторов-ошибок в произвольных БЧХ-кодах

Норма синдрома – это векторная характеристика векторов-ошибок, вычисляемая через координаты синдрома.

Определение 5.1. Нормой синдрома $S(\bar{e}) = (s_1, s_2, ..., s_{\delta-1})$ вектора ошибок $\bar{e}$ в БЧХ-коде C с проверочной матрицей (2.2) называется вектор

$$N(S(\bar{e})) = (N_{12}, N_{13}, ..., N_{1(\delta-1)}, N_{23}, ..., N_{(\delta-2)(\delta-1)})$$

с $C_{\delta-1}^2$ координатами N_{ij}, $1 \le i < j \le \delta - 1$, которые вычисляются по формулам:

а) $N_{ij} = \infty$, если $s_j \neq 0$, $s_i = 0$; $N_{ij} =$ (не существует), если $s_i = s_j = 0$;

б) $N_{ij} = s_j^{(b+i-1)/h_{ij}} / s_i^{(b+j-1)/h_{ij}}$, если $s_i \neq 0$. (5.1)

Пример 5.1. У БЧХ-кода C с параметрами $b = \delta = 4$ проверочная матрица имеет вид $H = (\beta^{4i}, \beta^{5i}, \beta^{6i})^T$. Для каждого вектора ошибок $\bar{e}$ его синдром $S(\bar{e}) = (s_1, s_2, s_3)$ в коде C. Здесь $h_{12} = h_{23} = 1$, $h_{13} = 2$. Тогда по определению норма $\vec{N}(S(\bar{e})) = (N_{12}, N_{13}, N_{23})$ – вектор, координаты которого вычисляются по формуле (5.1) $N_{12} = s_2^4 / s_1^5$; $N_{13} = s_3^2 / s_1^3$; $N_{23} = s_3^5 / s_2^6$.

Из определения 5.1 следует, что координаты N_{ij} нормы $\bar{N}(S)$ могут принимать $q^m + 2$ значения: либо какой-нибудь из q^m элементов поля $GF(q^m)$, либо ∞, либо – (не существует).

Пусть у исходного БЧХ-кода C параметр $b = 1$. Тогда $h_{ij} = \text{НОД}(i, j)$, в частности, $h_{1j} = 1$ для всех целых i, j $1 \le i < j \le \delta - 1$. Тогда формула (5.1) приобретает вид

$$N_{ij} = s_j^{i/h_{ij}} \Big/ s_i^{i/h_{ij}} \text{ в частности, } N_{1j} = s_j / s_1^j. \quad (5.1^*)$$

Пусть $C = C_{2t+1}$ – является двоичным БЧХ-кодом с кодовым расстоянием $\delta = 2t + 1$ и с проверочной матрицей (2.3). Синдром любого вектора ошибок $\bar{e}$ в этом коде есть вектор $S = S(\bar{e}) = (s_1, s_2, ..., s_t)$, где $s_i \in GF(2^m)$, $1 \le i \le t$.

Пусть 0 и $c \neq 0$ – элементы $GF(2^m)$. Введем обозначения для следующих частных: $\frac{c}{0} = \infty$; $\frac{0}{0} =$ – (не существует, не определено). С учетом специфики кода C_{2t+1} из определения 5.1 вытекает

Определение 5.2. Нормой синдрома $S = (s_1, s_2, ...s_t)$ в коде C_{2t+1} назовем вектор $\vec{N} = \vec{N}(S) = (N_{12}, N_{13}, ..., N_{1t}, N_{23}, ..., N_{(t-1)t})$ с C_t^2 координатами $N_{ij}, 1 \le i < j \le t$, которые вычисляются по формуле

$$N_{ij} = s_j^{(2i-1)/h_{ij}} \Big/ s_i^{(2j-1)/h_{ij}} . \qquad (5.2)$$

Для $h_{ij} = \text{НОД}(2i-1, 2j-1)$.

Пример 5.2. Пусть C_5 есть БЧХ-код C_{2t+1} с $t=2$, т. е. задается проверочной матрицей $H = (\beta^i, \beta^{3i})$, $0 \le i \le n-1$. Тогда норма синдрома состоит из одной компоненты, задаваемой при $s_1 \neq 0$ формулой $N = s_2 / s_1^3$. Чаще всего норма принимает значения в поле $GF(2^m)$. Если $N = \alpha^{\mu} \in GF(2^m)$, то μ называют показателем нормы и обозначают через $\deg N$.

Пример 5.3. Пусть C_7 есть БЧХ-код C_{2t+1} с $t=3$, т. е. задается проверочной матрицей $H = (\beta^i, \beta^{3i}, \beta^{5i})$, $0 \le i \le n-1$. Тогда норма синдрома согласно формулам (5.2) состоит из трех компонент:

$$N_1 = s_2 / s_1^3; \;\; N_2 = s_3 / s_1^5; \;\; N_3 = s_3^3 / s_2^5. \qquad (5.3)$$

Эти координаты соответствуют компонентам N_{13}, N_{15}, N_{35} определения 5.1 при $b=1$.

Замечание. Согласно формуле (5.2) первые $t-1$ координат нормы синдрома имеют вид $N_{12} = s_2 / s_1^3$; $N_{13} = s_3 / s_1^5$; ...; $N_{1t} = s_t / s_1^{2t-1}$. Они имеют вполне определенный «физический» смысл – являются соответственно второй, третьей, и т. д. t-й координатами синдрома $S(\bar{f})$ единственного вектора $\bar{f}$ из Г-орбиты $< \bar{e} >$, первая координата синдрома которого равна 1.

5.2. Основные свойства норм синдромов в БЧХ-кодах

Прежде всего покажем, что между координатами нормы $\bar{N}$ существует определенная зависимость. При $s_1 \neq 0$ первые координаты являются определяющими для нормы синдрома, что подтверждает

Предложение 5.1. Пусть у БЧХ-кода C_δ параметр $b=1$, а синдром $S = (s_1, s_2, ..., s_{\delta-1})$ имеет компоненту $s_1 \neq 0$. Тогда все координаты нормы $\bar{N}(S)$, начиная с N_{23}, однозначно определяются первыми $\delta - 2$ координатами этой нормы по формулам

$$N_{ij} = N_{1j}^{i/h_{ij}} \Big/ N_{1i}^{j/h_{ij}} , \;\; 2 \le i < j \le \delta - 1. \qquad (5.4)$$

Доказательство. В силу формулы (5.1*)

$$\frac{\left(N_{1j}\right)^{\frac{i}{h_{ij}}}}{\left(N_{1i}\right)^{\frac{j}{h_{ij}}}} = \left(\frac{s_j}{s_1^j}\right)^{\frac{i}{h_{ij}}} \Bigg/ \left(\frac{s_i}{s_1^i}\right)^{\frac{j}{h_{ij}}} = \left(s_j\right)^{\frac{i}{h_{ij}}} \Big/ \left(s_i\right)^{\frac{j}{h_{ij}}} = N_{ij},$$

что и требовалось доказать.

Следствие. У двоичного БЧХ-кода C_{2t+1} с проверочной матрицей (2.3) все координаты нормы $\overline{N}(S(\overline{e}))$ синдрома $S(\overline{e}) = (s_1, s_2, ..., s_t)$ с $s_1 \neq 0$, начиная с N_{23}, определяются первыми $t-1$ координатами по формуле

$$N_{ij} = \left(N_{1j}\right)^{\frac{2i-1}{h_{ij}}} \Big/ \left(N_{1i}\right)^{\frac{2j-1}{h_{ij}}}. \qquad (5.4^*)$$

Фундаментальное свойство норм синдромов отражает

Теорема 5.1. *В БЧХ-коде C с проверочной матрицей (2.2) норма синдрома не зависит от циклических сдвигов координат векторов-ошибок: для всякого вектора ошибок $\overline{e}$ и его синдрома $S(\overline{e})$ справедливо равенство* $N(S(\sigma(\overline{e}))) = N(S(\overline{e}))$.

Доказательство. Пусть $S(\overline{e}) = (s_1, s_2, ..., s_{\delta-1})$. Пусть $s_i \neq 0$, $1 \le i < \delta - 1$. Тогда *i*-я компонента синдрома $S(\sigma(\overline{e}))$ равна $s_i' = \beta^{b+i-1} \cdot s_i$ согласно формуле (4.2) и, следовательно, $s_i' \neq 0$. Тогда для каждого целого j, $i < j \le \delta - 1$, координаты N_{ij}' нормы $\overline{N}(S(\sigma(\overline{e})))$ вычисляются по формуле (5.1):

$$N_{ij}' = \frac{s_j'^{(b+i-1)/h_{ij}}}{s_i'^{(b+j-1)/h_{ij}}} = \frac{(\beta^{b+j-1} s_j)^{(b+i-1)/h_{ij}}}{(\beta^{b+i-1} s_i)^{(b+j-1)/h_{ij}}} = \frac{s_j^{(b+i-1)/h_{ij}}}{s_i^{(b+j-1)/h_{ij}}} = N_{ij}.$$

Пусть $s_i = 0$, тогда и $s_i' = 0$. Если $s_j \neq 0$, то и $s_j' \neq 0$. Тогда $N_{ij} = \infty$ и $N_{ij}' = \infty$. Если же $s_j = 0$, то и $s_j' = 0$ и, следовательно, N_{ij} и N_{ij}' одновременно не существуют. Теорема 5.1 полностью доказана.

Следствие 1. Все векторы каждой Г-орбиты векторов-ошибок имеют одинаковую норму синдрома. Норма синдрома инвариантна относительно группы Γ-циклических сдвигов.

Фундаментальное свойство нормы синдрома оттеняет

Следствие 2. Если нормы двух векторов-ошибок в коде C_δ различны, то данные векторы принадлежат различным Г-орбитам.

Следствие 1 из теоремы 5.1 позволяет ввести следующее

Определение 5.3. Нормой $N(J)$ Г-орбиты J в БЧХ-коде называется норма синдрома любого вектора-ошибки из этой Г-орбиты.

Норма каждой Γ-орбиты является ее однозначной характеристикой, т. е. указателем, идентификатором этой орбиты. Это подтверждает и следующее, третье свойство норм синдромов.

Предложение 5.2. Пусть J_1, J_2 – две Г-орбиты векторов-ошибок в БЧХ-коде C, имеющие различные нормы: $N(J_1) \neq N(J_2)$. Тогда для любых векторов $\overline{g} \in J_1$ и $\overline{f} \in J_2$ их синдромы $S(\overline{f})$ и $S(\overline{g})$ различны. Другими словами, спектры синдромов таких Г-орбит не пересекаются.

Доказательство легко получается методом от противного.

Пример 5.4. Рассмотрим двоичный в узком смысле C_5 БЧХ-код с проверочной матрицей $H = (\beta^i, \beta^{3i}), 0 \le i \le n-1$. Как уже отмечалось выше, здесь норма синдрома является скалярной величиной, имеет единственную компоненту $N = s_2 / s_1^3$. Легко видеть, что в этом коде класс I_1 одиночных ошибок, т. е. векторов-ошибок весом 1 имеет норму $N(I_1) = 1$. Представителем класса двойных ошибок I_D диаметром D, $2 \le D \le \nu + 1$, можно взять вектор-ошибку $\bar{e}_{1,D}$. Ее синдром $S(\bar{e}_{1,D}) = (1 + \beta^{D-1}, 1 + \beta^{3D-3})$. Следовательно,

$$N(I_D) = \frac{1+\beta^{3D-3}}{(1+\beta^{D-1})^3} = \frac{1+\beta^{D-1}+\beta^{2D-2}}{(1+\beta^{D-1})^2} = 1 + \frac{\beta^{D-1}}{\beta^{2D-2}}.$$

Ясно, что $N(I_D) \ne 1$ для всех D, $2 \le D \le \nu + 1$.

Теорема 5.2. *В двоичном БЧХ-коде C_5 с проверочной матрицей $H = (\beta^i, \beta^{3i})^T$ классы всех одиночных и двойных ошибок содержат по n векторов-ошибок и имеют попарно различные нормы* (*показатели*).

Доказательство. В коде C_5 длина кодовых слов n делит $2^m - 1$ и, следовательно, нечетная. Поэтому из гл. 3 следует, что все классы одиночных и двойных ошибок имеют одинаковую мощность, равную n. Согласно 1-й части предложения 3.7 векторы-ошибки весом 2 делятся на $v = 0{,}5 \cdot (n-1)$ Г-орбит.

Пусть I_j, I_t два различных класса эквивалентности двойных ошибок. В силу примера 5.1 их нормы равны тогда и только тогда, когда $\frac{\beta^{j-1}}{1+\beta^{2j-2}} = \frac{\beta^{t-1}}{1+\beta^{2t-2}}$, т. е. когда $\beta^{2t-3} + \beta^{2j+t-3} + \beta^{t-1} + \beta^{j-1} = 0$. Пусть для определенности $2 \le j < t \le \nu + 1$. Тогда последнее соотношение преобразуется к виду $\beta^{j-1} \cdot (\beta^{t+j-2} + 1) \cdot (\beta^{t-j} + 1) = 0$. Поскольку в поле нет делителей нуля, это означает, что $\beta^{t+j-2} = 1$ или $\beta^{t-j} = 1$. Но $1 < t - j < n$ и в силу примитивности β равенство $\beta^{t-j} = 1$ невозможно. $t + j < 2(\nu+1) = 2(2^{m-1} - 1) = 2^m - 2 < 2^m - 1$ и равенство $\beta^{t+j-2} = 1$ также невозможно по тем же причинам. Следовательно, $N(I_j) \ne N(I_t)$. Отличие $N(I_D)$, $2 \le D \le \nu + 1$, от нормы $N(I_1)$ отмечено в примере 5.1. Теорема 5.2 полностью доказана.

Пример 5.5. В условиях теоремы 5.2 проверочная матрица H БЧХ-кода C_5 длиной 31 над полем $GF(2^5)$ для α – корня полинома $x^5 + x^2 + 1$ – имеет следующий вид:

1	0	0	0	0	1	0	0	1	0	1	1	0	0	1	1	1	1	1	0	0	0	1	1	0	1	1	1	0	1	0
0	1	0	0	0	0	1	0	0	1	0	1	1	0	0	1	1	1	1	1	0	0	0	1	1	0	1	1	1	0	1
0	0	1	0	0	1	0	1	1	0	0	1	1	1	1	1	0	0	0	1	1	0	1	1	1	0	1	0	1	0	0
0	0	0	1	0	0	1	0	1	1	0	0	1	1	1	1	1	0	0	0	1	1	0	1	1	1	0	1	0	1	0
0	0	0	0	1	0	0	1	0	1	1	0	0	1	1	1	1	1	0	0	0	1	1	0	1	1	1	0	1	0	1
	0	0					0	0		0																				
1	0	0	0	0	1	1	0	0	1	0	0	1	1	1	1	1	0	1	1	1	0	0	0	1	0	1	0	1	1	0
0	0	1	1	1	1	1	0	1	1	1	0	0	0	1	0	1	0	1	1	0	1	0	0	0	0	1	1	0	0	1
0	0	0	0	1	1	0	0	1	0	0	1	1	1	1	1	0	1	1	1	0	0	0	1	0	1	0	1	1	0	1
0	1	1	1	1	1	0	1	1	1	0	0	0	1	0	1	0	1	1	0	1	0	0	0	0	1	1	0	0	1	0
0	0	0	1	0	1	0	1	1	0	1	0	0	0	0	1	1	0	0	1	0	0	1	1	1	1	1	0	1	1	1

Ниже представлена табл. 5.1 диаметров порождающих векторов, норм и показателей Г-орбит одиночных и двойных ошибок в примитивном БЧХ-коде длиной 31 с проверочной матрицей $H = \left(\alpha^i, \alpha^{3i}\right)^T$, где α – корень полинома $x^5 + x^2 + 1$.

Таблица 5.1

Диаметры порождающих векторов Г*-орбит ошибок весом 1–2, показателей их синдромов и норм синдромов*

Г-орбита	Образующая вектор-ошибка	Синдром образующей		Норма Г-орбиты
		degS_1	degS_2	deg$N(S)$
I_1	$\bar{e}_1$	0	0	0
I_2	$\bar{e}_{1,2}$	18	29	6
I_3	$\bar{e}_{1,3}$	5	27	12
I_4	$\bar{e}_{1,4}$	29	16	22
I_5	$\bar{e}_{1,5}$	10	23	24
I_6	$\bar{e}_{1,6}$	2	24	18
I_7	$\bar{e}_{1,7}$	27	1	13
I_8	$\bar{e}_{1,8}$	22	25	21
I_9	$\bar{e}_{1,9}$	20	15	17
I_{10}	$\bar{e}_{1,10}$	16	6	20
I_{11}	$\bar{e}_{1,11}$	4	17	5
I_{12}	$\bar{e}_{1,12}$	19	5	10
I_{13}	$\bar{e}_{1,13}$	23	2	26
I_{14}	$\bar{e}_{1,14}$	14	20	9
I_{15}	$\bar{e}_{1,15}$	13	19	11
I_{16}	$\bar{e}_{1,16}$	24	13	3

Из табл. 5.1 непосредственно видно, что перечисленные Г-орбиты имеют попарно различные нормы.

К сожалению, число возможных ошибок в кодовых словах намного больше, чем самих кодовых слов. При реальных длинах кодовых слов обязательно найдутся классы ошибок, нормы которых совпадают с той или иной нормой $N(I_t)$, $1 \le t \le v+1$. Однако ошибки малой кратностью имеют вероятность существенно большую, чем многократные. Поэтому, если $N(I) = N(I_t)$, $1 \le t \le v+1$, то с уверенностью, равной этой вероятности, можно утверждать, что $I = I_t$.

Итак, все векторы Г-орбиты имеют одинаковую норму, которую называем нормой Г-орбиты. Г-орбиты с различными нормами имеют непересекающиеся спектры синдромов.

Четвертое свойство норм синдромов говорит об их количестве.

Предложение 4.6. В двоичном БЧХ- коде C_{2t+1} с проверочной матрицей (2.3) количество K_t различных векторов $\overline{N}$ – норм синдромов, выражается формулой

$$K_t = (n+1)^{t-1} + (n+1)^{t-2} + \ldots + (n+1)^2 + (n+1) + 2 = K_{t-1} + (n+1)^{t-1}. \qquad (5.5)$$

В частности, при $t = 3$ $K_3 = (n+1)^2 + n + 3$.

Доказательство достаточно технично и потому опускается.

Пятое свойство норм синдромов заключается в равномерном распределение синдромов по значениям норм. Точным выражением этого свойства является

Предложение 5.3. В примитивном двоичном БЧХ-коде C_{2t+1} каждое значение нормы синдрома, кроме $N = (-,-,-,-)$, принимают в точности n различных синдромов $N(S) = (-,-,-,-)$ для единственного синдрома $S = (0,0,...,0)$. Тем самым все $(n+1)^t - 1$ синдромов векторов-ошибок равномерно (по n значений) распределяются по значениям нормы синдрома.

Следствие 1. Пусть I и J – две Г-орбиты векторов-ошибок с одинаковыми нормами в примитивном двоичном БЧХ-коде C_{2t+1}. Пусть I – полная Г-орбита с полным спектром синдромов. Тогда для всякого вектора $\bar{f} \in J$ найдется вектор $\bar{e} \in I$, такой, что $S(\bar{e}) = S(\bar{f})$.

Шестое свойство норм синдромов четко выражает

Следствие 2. Если в примитивном двоичном БЧХ-коде C_{2t+1} две полные Г-орбиты с полными спектрами синдромов имеют одинаковые нормы, то у них и спектры синдромов одинаковы.

5.3. Норменное декодирование двойных ошибок в БЧХ-кодах

Коррекция ошибок кратностью $t \ge 2$ связана, как уже отмечалось в гл. 2, с определенными трудностями. Классические подходы к декодированию

ошибок кратностью $t \geq 2$ приводят к решению алгебраических уравнений степени t в полях Галуа, что трудно реализуется алгоритмически.

Использование норм синдромов позволяет предложить метод коррекции ошибок в двоичных кодах, требующий меньших вычислительных затрат по сравнению с известными алгебраическими методами обработки кодов.

Сущность норменного метода декодирования в двоичных кодах вытекает непосредственно из построенной выше теории: вычисляется синдром ошибок $S(\bar{x}) = S(\bar{e})$ принятого сообщения $\bar{x} = \bar{e} + \bar{y}$, где $\bar{y}$ – истинное кодовое слово, $\bar{e}$ – вектор ошибок; далее вычисляется норма синдрома $\overline{N}(S(\bar{x})) = \overline{N}$. Норма указывает Г орбиту *J*, которой принадлежит вектор $\bar{e}$. Элементы любой Г-орбиты являются звеньями замкнутого кольца, переходящими друг в друга под действием циклических сдвигов. Если в Г-орбите *J* зафиксировать один элемент $\bar{e}_j$ в качестве образующего то, сравнив синдромы $S(\bar{e})$ и $S(\bar{e}_j)$, можно определить величину циклического сдвига, переводящего $\bar{e}_j$ в $\bar{e}$. Тем самым вектор ошибок $\bar{e}$ может быть однозначно определен.

Теорема 5.2 обеспечивает корректность норменного метода для декодирования двойных ошибок – она гарантирует, что Г-орбиты ошибок весом 1 – 2 имеют попарно различные нормы синдромов. Конечно, при конкретной реализации норменного метода следует составить таблицу образующих $\bar{e}_j$ Г-орбит $J_j = <\bar{e}_j>$ корректируемого множества векторов-ошибок, синдромов $S(\bar{e}_j)$ и норм синдромов $N(S(\bar{e}_j))$.

Пример 5.6. В продолжение примера 5.5 рассмотрим ТКС на основе БЧХ-кода C_5 длиной 31 над полем $GF(2^5)$ с фиксированным примитивным элементом α – корнем полинома $x^5 + x^2 + 1$. Требуемая табл. 5.1 уже построена выше. Пусть приемное устройство приняло следующее сообщение: $\bar{x} = (001\ \ 011\ \ 011\ \ 100\ \ 000\ \ 100\ \ 000\ \ 000\ \ 100\ \ 0001)$. Вычислим синдром ошибок этого сообщения $S(\bar{x}) = \bar{x} \cdot H^T = \bar{x} \cdot (\alpha^i, \alpha^{3i}) = (1, \alpha^{10})$. Тогда норма синдрома $N(S(\bar{x})) = s_2 / s_1^3 = \alpha^{10}$. Табл. 5.1 показывает, что вектор-ошибка $\bar{e}$ в принятом сообщении $\bar{x} = \bar{c} + \bar{e}$ принадлежит Г-орбите I_{12}, порожденной вектором $\bar{e}_{12} = (1, 12)$ с синдромом $S(\bar{e}_{12}) = (\alpha^{18}, \alpha^5)$. Таким образом, вектор $\bar{e}$ получается циклическим сдвигом координат вектора $\bar{e}_{12} = (1, 12)$ на $\deg(1/\alpha^{19}) = 31 - 19 = 12$ позиций вправо. Следовательно, $\bar{e} = (13, 24)$ и истинное сообщение

$$\bar{c} = \bar{x} + \bar{e} = (001\ \ 011\ \ 011\ \ 100\ \ 100\ \ 100\ \ 000\ \ 001\ \ 100\ \ 0001).$$

5.4. Норменное декодирование тройных ошибок в БЧХ-кодах

Важным для данного раздела является

Предложение 5.4. Множество Г-орбит всех векторов-ошибок весом $1-3$ имеет в примитивном двоичном БЧХ-коде C_7 попарно различные нормы.

Доказательство. Все Г-орбиты векторов-ошибок весом $1-3$, за исключением, может быть, одной, являются полными. Если бы две из них имели одинаковые нормы, то согласно следствию 1 из предложения 4.3 они содержали бы векторы с одинаковыми синдромами. Это противоречит свойствам кода C_7.

Пример 5.7. Составим табл. 5.2 образующих всех Г-орбит 15-мерных векторов-ошибок весом 1 – 3, их синдромов и норм синдромов в БЧХ-коде C_7 над полем $GF(2^4)$ с примитивным элементом $\alpha-$ корнем полинома x^4+x+1.

Таблица 5.2

Образующие Г*-орбит ошибок весом 1, 2, 3 в пространстве* E_{15}*, их диаметры, синдромы и нормы синдромов*

№ п/п	Диаметр D	Образующая $\bar{e}$ Г-орбиты	Синдром S($\bar{e}$)	Норма $\overline{N}$ Г-орбиты
1	2	3	4	5
1	1	(1)	(1, 1, 1)	(1, 1, 1)
2	2	(1, 2)	(α^4, α^{14}, α^{10})	(α^2, α^5, α^5)
3	3	(1, 3)	(α^8, α^{13}, α^5)	(α^4, α^{10}, α^{10})
4	4	(1, 4)	(α^{14}, α^7, 0)	(α^{10}, 0, 0)
5	5	(1, 5)	(α, α^{11}, α^{10})	(α^8, α^5, α^5)
6	6	(1, 6)	(α^{10}, 0, α^5)	(0, 1, ∞)
7	7	(1, 7)	(α^{13}, α^{14}, 0)	(α^5, 0, 0)
8	8	(1, 8)	(α^9, α^{13}, α^9)	(α, α^{10}, α^{10})
9	3	(1, 2, 3)	(α^{10}, α^8, 0)	(α^8, 0, 0)
10	4	(1, 2, 4)	(α^7, α^4, α^5)	(α^{13}, 1, α^{10})
11	4	(1, 3, 4)	(α^{13}, α^{10}, α^{10})	(α, α^5, α^{10})
12	5	(1, 2, 5)	(0, α^5, 1)	(∞, ∞, α^5)
13	5	(1, 3, 5)	(α^5, α, 0)	(α, 0, 0)
14	5	(1, 4, 5)	(α^9, α^2, α^5)	(α^5, α^5, α^5)
15	6	(1, 2, 6)	(α^8, α^3, 0)	(α^9, 0, 0)
16	6	(1, 3, 6)	(α^4, α^6, 1)	(α^9, α^{10}, 1)
17	6	(1, 4, 6)	(α^{12}, α^9, α^{10})	(α^3, α^{10}, 1)
18	6	(1, 5, 6)	(α^2, α^{12}, 0)	(α^6, 0, 0)
19	7	(1, 2, 7)	(α^{12}, 1, α^5)	(α^9, α^5, 1)
20	7	(1, 3, 7)	(α^{14}, α^8, α^{10})	(α^{11}, 1, α^5)

Окончание табл. 5.2

1	2	3	4	5
21	7	(1, 4, 7)	(α^8, α^4, 1)	(α^{10}, α^5, α^{10})
22	7	(1, 5, 7)	(α^{11}, α^5, α^5)	(α^2, α^{10}, α^5)
23	7	(1, 6, 7)	(α^7, α^3, α^{10})	(α^{12}, α^5, 1)
24	8	(1, 2, 8)	(α^3, α^8, 1)	(α^{14}, 1, α^5)
25	8	(1, 3, 8)	(α^{11}, 1, 0)	(α^{12}, 0, 0)
26	8	(1, 4, 8)	(α, α^{10}, α^5)	(α^7, 1, α^{10})
27	8	(1, 5, 8)	(α^{14}, α, 1)	(α^4, α^5, α^{10})
28	8	(1, 6, 8)	(α^6, α^6, 0)	(α^3, 0, 0)
29	8	(1, 7, 8)	(α^5, α^8, α^5)	(α^8, α^{10}, α^5)
30	9	(1, 2, 9)	(α^5, α^4, 0)	(α^4, 0, 0)
31	9	(1, 3, 9)	(0, α^{10}, 1)	(∞, ∞, α^{10})
32	9	(1, 4, 9)	(α^6, 1, α^{10})	(α^{12}, α^{10}, 1)
33	9	(1, 5, 9)	(α^{10}, α^2, α^0)	(α^2, 0, 0)
34	9	(1, 6, 9)	(α, α^9, 1)	(α^6, α^{10}, 1)
35	9	(1, 7, 9)	(α^3, α^4, α^{10})	(α^{10}, α^{10}, α^{10})
36	10	(1, 4, 10)	(α^4, α^2, 1)	(α^5, α^{10}, α^5)
37	10	(1, 5, 10)	(α^3, 1, α^5)	(α^6, α^5, 1)
38	10	(1, 6, 10)	(α^{13}, α^{12}, α^{10})	(α^3, α^5, 1)
39	11	(1, 6, 11)	(0, 1, 0)	(∞, —, 0)

Из табл. 5.2 непосредственно видно, что все выписанные в ней нормы попарно различны в полном соответствии с предложением 5.4.

Предложение 5.5. В примитивном двоичном БЧХ-коде C_7 спектр норм синдромов $\overline{N} = (N_1, N_2, N_3)$ векторов-ошибок весом 1 – 3 составляют:

1) нормы $\overline{N}$ с координатами $N_1, N_2, N_3 \in GF(2^m)$ (кроме (0, 0, 0));

2) (∞, ∞, N_3), где N_3 – ненулевой элемент поля $GF(2^m)$;

3) (∞, –, 0), если $n = 2^{2m} - 1$ для единственной неполной Г-орбиты ошибок весом $3 < (1, l+1, 2l+1) >$, где $l = n/3$.

4) (0, 0, –) при $m = 3l$ для единственной Г-орбиты с синдромами $(s_1, 0, 0), s_1 \neq 0$.

Доказательство следует из определения нормы и описания синдромов указанных ошибок.

Замечание. Если код C_{2t+1} непримитивен, то следствие из предложения 5.3 перестает быть справедливым. Причина в том, что у полной Г-орбиты с полным спектром синдромов некоторые из координат, как правило, принимают практически все ненулевые значения из поля Галуа, над которым определяется код. У непримитивного же кода длина кода и, следовательно, мощность

множества значений той или иной координаты спектра синдромов Г-орбиты является делителем $\left|GF(2^m)^*\right|$. Следовательно, может существовать до $\nu = \left|GF(2^m)\right|/n$ Г-орбит с одинаковой нормой и попарно различными спектрами синдромов.

Пример 5.8. Рассмотрим двоичный БЧХ-код код C_5 длиной 21 с проверочной матрицей $H = (\beta^i, \beta^{3i})^T, 0 \le i \le n-1,$ где $\beta = \alpha^3$ для примитивного элемента поля Галуа $GF(2^6)$. Пусть α – корень полинома $x^6 + x + 1$. Здесь Г-орбиты <(1,8)>, <(1,2,6)>, <(1,3,4)> имеют спектры синдромов соответственно

$$\{\beta^i\alpha^{42}, 0\}, \{\beta^i\alpha^{62}, 0\}, \{\beta^i\alpha^{49}, 0\} \text{ или } \{\alpha^{42+3i}, 0\}, \{\alpha^{62+3i}, 0\}, \{\alpha^{49+3i}, 0\}.$$

Все три *Г*-орбиты имеют одинаковую норму 0. Однако, как нетрудно видеть, их спектры синдромов не пересекаются.

Построенная теория позволяет предложить норменный метод и для коррекции тройных ошибок в БЧХ-кодах. По сути, принципиальных отличий метода от рассмотренного в подразд. 5.3 метода нет. Отличие лишь в росте таблицы Г-орбит корректируемого множества ошибок, а также в том, что норма становится векторной величиной – содержит три координаты.

Пример 5.9. Пусть ТКС функционирует на основе БЧХ-кода из примера 5.7. Предположим, что приемное устройство ТКС приняло сообщение $\bar{x}$ с синдромом $S(\bar{x}) = (1, \alpha^8, 0)$. Вычисляем норму синдрома $\overline{N}(S(\bar{x})) = (\alpha^8, 0, 0)$. Из табл. 5.2 узнаем, что содержащаяся в сообщении $\bar{x}$ вектор-ошибка $\bar{e}$ принадлежит Г-орбите $I_9 = <\bar{e}_9> = <(1, 2, 3)>$ с синдромом образующей $S(\bar{e}_9) = (\alpha^{10}, \alpha^8, 0)$. Значит, $\bar{e} = \sigma^k(\bar{e}_8)$, где $k = \deg(1/\alpha^{10}) = 5$. Таким образом, $\bar{e} = (6, 7, 8)$.

5.5. Нормы синдромов циклотомически связанных векторов ошибок

В подразд. 3.5. изучено действие группы Ф циклотомических подстановок на пространстве двоичных векторов любой нечетной размерности, а в подразд. 3.7 – их влияние на синдромы ошибок в произвольном БЧХ-коде. Здесь рассмотрим действие групп Ф и G на нормы синдромов.

Предложение 5.6. Пусть $\overline{N} = (N_1, N_2, N_3)$ – норма синдрома вектора-ошибки $\bar{e}$ в примитивном двоичном БЧХ-коде C_7 и пусть $\overline{N}^{\varphi} = \left(N_1^{\varphi}, N_2^{\varphi}, N_3^{\varphi}\right)$ – норма синдрома $S(\varphi(\bar{e}))$. Тогда

1) если $N_i \in GF(2^m)$, то $N_i^{\varphi} = N_i^2$ для любого $i = 1, 2, 3$;
2) если $N_i = 0$, то и $N_i^{\varphi} = 0$;
3) если $N_i = \infty$, то и $N_i^{\varphi} = \infty$;
4) если N_i – не существует, то и N_i^{φ} – не существует.

Доказательство. Пусть $S(\bar{e}) = (s_1, s_2, s_3)$. Тогда согласно предложению 4.7 $S(\varphi(\bar{e})) = (s_1^2, s_2^2, s_3^2)$. Пусть $s_1, s_2, s_3 \in GF(2^m)$. Тогда по определению 5.1 норма $\overline{N}(S(\bar{e}))$ имеет координаты, выражаемые формулой (5.1). Аналогично вычисляются координаты вектора $\overline{N}^{\varphi}$: $N_1^{\varphi} = \dfrac{s_j^{2(b+i-1)/h_{ij}}}{s_i^{2(b+j-1)/h_{ij}}} = N_{ij}^2;\ 1 \le i < j \le \delta - 1.$ Остальные утверждения проверяются аналогично.

Пусть $< \bar{e} >_G$ – G-орбита вектора-ошибки $\bar{e} \in E_n$, n – делитель $2^m - 1$, $m > 1$. Согласно теореме 3.4 существует целое $\mu, 1 \le \mu \le n$, такое, что $< \bar{e} >_G = \{ < \bar{e} >, < \varphi(\bar{e}) >, \ldots, < \varphi^{\mu-1}(\bar{e}) > \}$. Пусть $\overline{N}_i$ – норма в БЧХ-коде C Г-орбиты $< \varphi^{i-1}(\bar{e}) >$ для каждого значения $i = 1, 2, \ldots, \mu$.

Определение 5.4. Спектром норм G-орбиты $< \bar{e} >_G$ называется множество $\{\overline{N}_1,\ \overline{N}_2,\ \ldots\ ,\ \overline{N}_\mu\}$ – норм составляющих ее Г-орбит и обозначается через $\overline{N}(< \bar{e} >_G)$. Спектр норм G-орбиты называется полным, если его мощность совпадает с количеством составляющих Г-орбит.

Каждая G-орбита представляет собой согласно теореме 3.4 цепочку переходящих друг в друга под действием φ Г-орбит. Соответственно преобразуются нормы Г-орбит: их компоненты возводятся в квадрат согласно предложению 4.9. При условии полноты спектра норм G-орбиты названные преобразования становятся взаимно однозначными и, следовательно, определяющими друг друга, что наглядно видно из рис. 5.1. Здесь дана структурная схема G-орбиты $<(1,2)>_G$ в 31-мерном пространстве как цепочка Г-орбит (рис. 5.1) и соответствующая цепочка переходящих друг в друга посредством удвоения по модулю 31 показателей норм Г-орбит в БЧХ-коде C_5 (по данным из табл. 5.1).

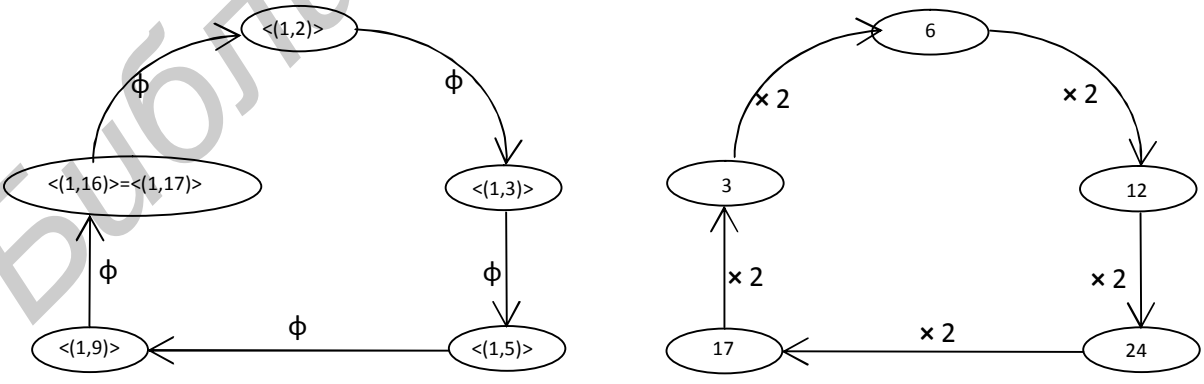

Рис. 5.1. Конструктивное изображение G-орбиты $<(1,2)>_G$ и ее спектр в показателе норм в (31,21)-БЧХ-коде C_5

Предложение 5.7. Пусть $\overline{N}(<\bar{e}>_G)$ – спектр норм G-орбиты $<\bar{e}>_G$. Тогда множество $\{N_i\}$ значений i-й координаты, $i=1, 2, 3$, в спектре норм $\overline{N}(<\bar{e}>_G)$ либо совпадает с одним из одноэлементных множеств $\{0\}$, $\{\infty\}$, $\{-\}$, либо множество показателей $\deg N_i$, $i=1, 2, \ldots, \mu$, составляет один циклотомический класс по модулю $n=2^m-1$.

Доказательство вытекает из предложения 5.6.

Пример 5.10. С помощью табл. 5.2 составим список циклоклассов в пространстве E_{15}, составляющих их Г-орбит, их образующих, синдромов образующих в БЧХ-коде C_7 над полем $GF(2^n)$ с примитивным элементом α – корнем полинома x^4+x+1, а также норм соответствующих Г-орбит для всех векторов весом 1 – 3.

Таблица 5.3

Структура G-орбит ошибок весом 1, 2 и норм составляющих их Г*-орбит*

№ п/п	G-орбита $<\bar{e}>_G$	Г-орбита $<\bar{e}'>$	Синдром $S(\bar{e}')$	Норма Г-орбиты
1	2	3	4	5
1	$<(1)>_G$	$<(1)>$	(1, 1, 1)	(1, 1, 1)
2	$<(1,2)>_G$	$<(1,2)>$	(α^4, α^{14}, α^{10})	(α^2, α^5, α^5)
		$<(1,3)>$	(α^8, α^{13}, α^5)	(α^4, α^{10},
		$<(1,5)>$	(α, α^{11}, α^{10})	(α^8, α^5, α^5)
		$<(1,8)>$	(α^9, α^{13}, α^9)	(α, α^{10},
3	$<(1,4)>_G$	$<(1,4)>$	(α^{14}, α^7, 0)	(α^{10}, 0, 0)
		$<(1,7)>$	(α^{13}, α^{14}, 0)	(α^5, 0, 0)
4	$<(1,6)>_G$	$<(1,6)>$	(α^{10}, 0, α^5)	(0, 1, ∞)
5	$<(1,2,3)>_G$	$<(1,2,3)>$	(α^{10}, α^8, 0)	(α^8, 0, 0)
		$<(1,3,5)>$	(α^5, α, 0)	(α, 0, 0)
		$<(1,5,9)>$	(α^{10}, α^2, α^0)	(α^2, 0, 0)
		$<(1,2,9)>$	(α^5, α^4, 0)	(α^4, 0, 0)
6	$<(1,2,4)>_G$	$<(1,2,4)>$	(α^7, α^4, α^5)	(α^{13}, 1, α^{10})
		$<(1,3,7)>$	(α^{14}, α^8, α^{10})	(α^{11}, 1, α^5)
		$<(1,4,8)>$	(α, α^{10}, α^5)	(α^7, 1, α^{10})
		$<(1,2,8)>$	(α^3, α^8, 1)	(α^{14}, 1, α^5)
7	$<(1,3,4)>_G$	$<(1,3,4)>$	(α^{13}, α^{10}, α^{10})	(α, α^5, α^{10})
		$<(1,5,7)>$	(α^{11}, α^5, α^5)	(α^2, α^{10},
		$<(1,5,8)>$	(α^{14}, α, 1)	(α^4, α^5,
		$<(1,7,8)>$	(α^{14}, α, 1)	(α^4, α^5,
8	$<(1,2,5)>_G$	$<(1,2,5)>$	(0, α^5, 1)	(∞, ∞, α^5)
		$<(1,3,9)>$	(0, α^{10}, 1)	(∞, ∞, α^{10})
9	$<(1,4,5)>_G$	$<(1,4,5)>$	(α^9, α^2, α^5)	(α^5, α^5, α^5)

		$<(1, 7, 9)>$	$(\alpha^3, \alpha^4, \alpha^{10})$	$(\alpha^{10},\alpha^{10},\alpha^{10})$

Окончание табл. 5.3

1	2	3	4	5
10	$<(1, 2, 6)>_G$	$<(1, 2, 6)>$	$(\alpha^8, \alpha^3, 0)$	$(\alpha^9, 0, 0)$
		$<(1, 6, 8)>$	$(\alpha^6, \alpha^6, 0)$	$(\alpha^3, 0, 0)$
		$<(1, 5, 6)>$	$(\alpha^2, \alpha^{12}, 0)$	$(\alpha^6, 0, 0)$
		$<(1, 3, 8)>$	$(\alpha^{11}, 1, 0)$	$(\alpha^{12}, 0, 0)$
11	$<(1, 3, 6)>_G$	$<(1, 3, 6)>$	$(\alpha^4, \alpha^6, 1)$	$(\alpha^9, \alpha^{10}, 1)$
		$<(1, 6, 10)>$	$(\alpha^{13}, \alpha^{12}, \alpha^{10})$	$(\alpha^3, \alpha^5, 1)$
		$<(1, 6, 9)>$	$(\alpha, \alpha^9, 1)$	$(\alpha^6, \alpha^{10}, 1)$
		$<(1, 6, 7)>$	$(\alpha^7, \alpha^3, \alpha^{10})$	$(\alpha^{12}, \alpha^5, 1)$
12	$<(1, 4, 6)>_G$	$<(1, 4, 6)>$	$(\alpha^{12}, \alpha^9, \alpha^{10})$	$(\alpha^3, \alpha^{10}, 1)$
		$<(1, 5, 10)>$	$(\alpha^3, 1, \alpha^5)$	$(\alpha^6, \alpha^5, 1)$
		$<(1, 4, 9)>$	$(\alpha^6, 1, \alpha^{10})$	$(\alpha^{12}, \alpha^{10}, 1)$
		$<(1, 2, 7)>$	$(\alpha^{12}, 1, \alpha^5)$	$(\alpha^9, \alpha^5, 1)$
13	$<(1, 4, 7)>_G$	$<(1, 4, 7)>$	$(\alpha^8, \alpha^4, 1)$	$(\alpha^{10}, \alpha^5,$
		$<(1, 4, 10)>$	$(\alpha^4, \alpha^2, 1)$	$(\alpha^5, \alpha^{10},$
14	$<(1, 6, 11)>_G$	$<(1, 6, 11)>$	$(0, 1, 0)$	$(\infty, -, 0)$

Анализируя таблицу, можно заметить, что в каждом циклоклассе координаты нормы составляющих его Г-орбит являются квадратами соответствующих координат нормы предыдущей Г-орбиты (по циклу), что полностью соответствует утверждению 5.7.

Таким образом, зная образующую *G*-орбиты, ее синдром и норму, можно однозначно восстановить элементы всей *G*-орбиты, синдромы и нормы синдромов всех векторов и Г-орбит этого циклокласса.

5.6. Основная теорема теории норм синдромов

Теорема 5.3. *Пусть K – произвольная, но фиксированная совокупность* Г-*орбит двоичных векторов-ошибок с полными спектрами синдромов в БЧХ-коде C_{2t+1} над полем Галуа $GF(2^m)$ и с попарно различными нормами. Если известно, что принятое слово $\bar{x}$ содержит вектор-ошибку из совокупности K, то код C ее однозначно корректирует.*

Доказательство. Пусть принято сообщение $\bar{x}$ с неизвестным вектором ошибок $\bar{e}$, т. е. $\bar{x} = \bar{y} + \bar{e}$, где $\bar{y}$ – истинное сообщение. Вычисляем $S(\bar{x}) = S(\bar{e})$ и норму $\bar{N}(S(\bar{e}_j))$. В силу условий теоремы $\bar{N}(S(\bar{e}_j)) = \bar{N}(J)$ для некоторой Г-орбиты $J \subset K. J =< \bar{f} >$ для произвольного фиксированного вектора $\bar{f} \in J$ с синдромом $S(\bar{f})$. Вектор $\bar{e}$ может принадлежать только

Г-орбите $< \bar{f} >$, поскольку K не содержит других Г-орбит с такой же нормой. Найдется целое λ, $1 \le \lambda < \left| < \bar{f} > \right|$, такое, что $S(\sigma^{\lambda}(\bar{f})) = S(\bar{e})$. В силу полноты спектра $S(J)$, $\bar{e} = \sigma^{\lambda}(\bar{f})$ – однозначно определенный вектор ошибок. Теорема доказана.

Наиболее естественный пример совокупности K для кода C_5 дает теорема 4.2 – это множество $K_{од}$ всех одиночных и двойных ошибок. Оно содержит $\frac{n+1}{2} = 2^{m-1}$ полных Г-орбит и, следовательно, $\frac{n(n+1)}{2}$ векторов-ошибок. Это составляет примерно половину спектра синдромов и, следовательно, использует лишь половину декодирующих возможностей БЧХ-кода C_5. Действительно, норма синдрома в коде C может принимать не более $n+2$ различных значений. Следовательно, по теореме 5.3 код C_5 может корректировать до $(n+2)n = n^2 + 2n$ векторов-ошибок. Этот практический предел синдромных методов декодирования, так как в коде C_5 имеется не более $(n+1)^2 = n^2 + 2n + 1$ различных синдромов.

Пример 5.11. БЧХ-код минимальной длины. Рассмотрим БЧХ-код C_5 минимальной длины $n = 7$ над полем $GF(2^3)$. В качестве примитивного элемента α возьмем корень неприводимого полинома $x^3 + x + 1$. Тогда проверочная матрица кода C имеет вид

$$H = \left[\alpha^i, \alpha^{3i}\right]^T = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}.$$

Пространство ошибок E_7 этого кода содержит $C_7^2 = 21$ двойных ошибок, которые согласно предложению 2 делятся на 3 полных класса эквивалентности I_D, $D = 2, 3, 4$. Г-орбита I_D состоит из циклических сдвигов вектора-ошибки $\bar{e}_{1D}$, у которого 1-я и D-я координаты равны 1, а остальные равны 0. Г-орбита I_1 состоит из одиночных ошибок и имеет норму, равную 1. В пространстве E_7 имеется $C_7^3 = 35$ векторов-ошибок весом 3, делящихся на 5 полных Г-орбит J_K, $K = 1, 2, ..., 5$. Каждая из них состоит из циклических сдвигов соответствующего вектора $\bar{e}_{1ij}$, у которого 1, i-я и j-я координаты равны 1, а остальные равны 0.

Табл. 5.4 содержит список Г-орбит I_j, $i=1,2,3,4$ и J_K, $k=1,2,...,5$, порождающих их векторов-ошибок, их синдромов и норм этих классов.

Таблица 5.4

Г-*орбиты векторов ошибок весом 1–3, их образующие, синдромы образующих и их нормы в (7,1) БЧХ-коде* C_5

Г-орбита	I_1	I_2	I_3	I_4	J_1	J_2	J_3	J_4	J_5
Образующий вектор-ошибка	$\bar{e}_1$	$\bar{e}_{12}$	$\bar{e}_{13}$	$\bar{e}_{14}$	$\bar{e}_{123}$	$\bar{e}_{124}$	$\bar{e}_{134}$	$\bar{e}_{125}$	$\bar{e}_{135}$
Синдром образующего вектора-ошибки	$(1;1)$	$(\alpha^3;\alpha)$	$(\alpha^6;\alpha^2)$	$(\alpha;\alpha^6)$	$(\alpha^5;\alpha^5)$	$(0;\alpha^4)$	$(\alpha^4;0)^T$	$(\alpha^6;\alpha^6)$	$(\alpha^3;\alpha^3)$
Норма Г-орбиты	1	α^6	α^5	α^3	α^4	∞	0	α^2	α

Из табл. 5.4 видно, что перечисленные Г-орбиты имеют попарно различные нормы. Согласно теореме 5.3 рассматриваемый БЧХ-код C_5 способен корректировать не только 28 векторов-ошибок весом 1 и 2, но и еще 35 векторов-ошибок весом 3, всего 63 векторов-ошибок. Код имеет 64 различных синдрома ошибок. Следовательно, в рассматриваемом примере норменный метод достигает предела синдромных методов коррекции ошибок.

К сожалению, у БЧХ-кодов C_5 длиной $n>7$ декодирующие возможности не столь эффектны. Уже при $n=15$ количество одиночных, двойных и тройных ошибок равно $C_{15}^1+C_{15}^2+C_{15}^3=15+105+455=575>256$ – больше количества различных синдромов. Следовательно, совместная коррекция всех случайных ошибок весом 1–3 БЧХ-кодами C_5 длиной $n>7$ невозможна. Тем не менее определенные классы ошибок весом 3 код C_5 может корректировать совместно с двойными.

Теорема 5.5. *Пусть* C_5 *– БЧХ-код с проверочной матрицей* $H=(\beta^i,\beta^{3i})^T, 0\le i\le n-1$, *где* $n>7$ *и* n *– делитель числа* 2^m-1, β *– примитивный корень* n*-й степени из 1. Если* β *не является корнем полиномов* $x^6+x^5+x^2+x+1$, $x^6+x^5+x^4+x+1$, $x^4+x^3+x^2+x+1$, $x^{12}+x^{10}+x^9+x^8+x^6+x^5+x^4+x+1$, $x^{12}+x^{11}+x^8+x^7+x^6+x^4+x^3+x^2+1$, *а следы элементов*

$$\gamma_1=\frac{(\beta+1)^4\beta}{(\beta^2+\beta+1)^3};\quad \gamma_2=\frac{(\beta+1)^4\beta(\beta^2+\beta+1)}{(\beta^3+\beta^2+1)^2};\quad \gamma_3=\frac{(\beta+1)^4\beta^2(\beta^2+\beta+1)}{(\beta^3+\beta^2+1)^3};$$

$$\gamma_4=\frac{(\beta+1)^2\beta(\beta^5+1)}{(\beta^3+\beta^2+\beta+1)^3}$$

равны 1, то код C_5 корректирует наряду с двойными ошибками любой циклический пакет ошибок длиной четыре.

Подчеркнем еще раз – построенная теория позволяет предложить норменный метод коррекции ошибок в БЧХ-кодах. Суть метода заключается в следующем. Составляем таблицу всех Г-орбит $< \bar{e}_i >$ корректируемых ошибок, таблицу синдромов $S(\bar{e}_i)$, а также таблицу $\overline{N}(S(\bar{e}_i))$. По принятому вектору-сообщению вычисляем $S(\bar{x}) = S(\bar{e})$ и $\overline{N}(S(\bar{e}))$. В таблице норм находим $\overline{N}(S(\bar{e}_i)) = \overline{N}(S(\bar{e}))$. Тогда вектор $\bar{e} \in < \bar{e}_i >$. Сравнивая первые компоненты синдромов $S(\bar{e}_i)$ и $S(\bar{x}) = S(\bar{e})$, определяем величину циклического сдвига для получения вектора $\bar{e}$ из вектора $\bar{e}_i$.

5.7. Теория норм синдромов для реверсивных кодов

Построим теорию норм синдромов для реверсивных кодов C_R.

Определение 5.5. В реверсивном коде C_R нормой синдрома $S = (s_1, s_2) = \left(\alpha^i, \alpha^j\right)$ назовем произведением компонент этого синдрома в поле Галуа $GF(2^m)$:

$$N(S) = s_1 \cdot s_2 \ . \tag{5.3}$$

$N(S) = \alpha^{i+j} = \alpha^{\mu}$ для подходящего $\mu \in T = \{-\infty, 0, 1, 2, ..., n-1\}$. Степень μ назовем показателем нормы синдрома S и будем обозначать через $\deg N\ (S)$ или $\deg N_S$.

Очевидно, $\mu = \begin{cases} i + j, \text{если } i + j < n, \\ i + j - n, \text{если } i + j \geq n, \\ -\infty, \text{если } s_1 \cdot s_2 = 0. \end{cases}$

Предложение 5.8. Нормы синдромов $N(S)$ в реверсивном коде C_R над полем $GF(2^m)$ принимают только значения из $GF(2^m)$, причем каждое из $n+1$ значений этого поля, а показатель $\mu = \deg N(S)$ – принимает каждое значение из множества T.

Доказательство. Тот факт, что $N(S)$ всегда принадлежит $GF(2^m)$, вытекает из (5.3). Компоненты s_1 и s_2 синдрома $S = (s_1, s_2)$ могут быть любыми элементами поля $GF(2^m)$. Если $s_2 = 1$ и s_2 пробегает все значения из $GF(2^m)$, то $N(S) = s_1 \cdot s_2 = s_1$ пробегает $n+1$ значений из $GF(2^m)$. Предложение полностью доказано.

Предложение 5.9. Пусть векторы-ошибки $\bar{e}_1$ и $\bar{e}_2$ в коде C_R принадлежат одной Г-орбите. Тогда нормы их синдромов и показатели этих норм совпадают.

Доказательство. По определению Г-орбиты найдется подстановка $\sigma^{\lambda} \in \Gamma$, $1 \leq \lambda \leq n$, такая, что $\sigma^{\lambda}(\bar{e}_1) = \bar{e}_2$. Пусть $S(\bar{e}) = (s_1, s_2)^T$. Тогда согласно теореме

4.5 $S(\sigma^{\lambda}(\bar{e})) = (\alpha^{\lambda} \cdot s_1; \alpha^{-\lambda} \cdot s_2)^T$. Следовательно,

$$N(S(\bar{e}_2)) = (\alpha^{\lambda} s_1) \cdot (\alpha^{-\lambda} s_2) = s_1 \cdot s_2 = N(S(\bar{e}_1)).$$

Утверждение доказано.

Следствие 1. Если нормы (показатели норм) синдромов двух векторов-ошибок различны, то данные ошибки принадлежат различным классам эквивалентности.

Следствие 2. Норма синдрома ошибок в реверсном коде является инвариантной относительно циклических сдвигов характеристикой векторов-ошибок.

Данное свойство позволяет ввести следующее

Определение 5.6. Нормой (показателем) класса эквивалентности I векторов-ошибок в коде G называется норма (показатель нормы) синдрома любого вектора-ошибки этого класса и обозначается через $N(I)$ (через $\deg I$).

Теорема 5.6. *В реверсивном коде C_R классы эквивалентности ошибок весом 1 и 2 содержат по n ошибок и имеют попарно различные нормы (показатели).*

Доказательство. Согласно предложению 3.7 классы эквивалентности ошибок весом 1 и 2 содержат по n векторов-ошибок в силу нечетности n.

Норма синдрома любой одиночной ошибки, очевидно, равна 1. Класс I_D двойных ошибок диаметром D содержит двойную ошибку на позициях с номерами 1 и D, т. е. вектор-ошибку $\bar{e}_{i,D} = (1, 0, ..., 1, 0, ..., 0)$, у которой только 1-я и D-я координаты равны 1. Следовательно,

$$N(I_D) = N(\overline{e_{i,D}}) = (\alpha^0 + \alpha^{D-1})(\alpha^0 + D^{1-D}) = \alpha^{D-1} + \alpha^{1-D} = \frac{\alpha^{2D-2} + 1}{\alpha^{D-1}}. \quad (5.5)$$

Поэтому равенство $N(I_D) = N(I_1)$ равносильно соотношению $\frac{\alpha^{2D-2} + 1}{\alpha^{D-1}} = 1$ или $(\alpha^{D-1})^2 + \alpha^{D-1} + 1 = 0$. Это означает, что $\alpha^{D\text{-}1}$ является корнем квадратного уравнения $x^2 + x + 1 = 0$. Но в полях Галуа $GF(2^m)$ с нечетным m это уравнение корней не имеет, поскольку абсолютный след $Tr1 = 1$. Следовательно, $N(I_D) \neq N(I_1)$. Пусть $I_i, I_j, 2 \le i < j \le v+1$ – два различных класса двойных ошибок. В силу формулы (5.5) равенство $N(I_i) \neq N(I_j)$ эквивалентно соотношению $\frac{\alpha^{2i-2} + 1}{\alpha^{i-1}} = \frac{\alpha^{2j-2} + 1}{\alpha^{j-1}}$ или $\alpha^{2j+i-3} + \alpha^{2i+j-3} + \alpha^{j-1} + \alpha^{i-1} = 0$, которое преобразуется к виду $\alpha^{i-1}(\alpha^{j+i-2} + 1) \times (\alpha^{j-i} + 1) = 0$. Следовательно, $\alpha^{j-i} = 1$ или $\alpha^{j+i-2} = 1^2$. Однако $0 < j - i < v$ и α – примитивный элемент поля. Поэтому $\alpha^{j-i} \neq 1$. Далее, $1 < i < j \le v + 1 = 2^{m\text{-}1}$. Поэтому $j + i - 2 < 2^m - 2$ и $\alpha^{j+i\text{-}2} \neq 1$ по тем же причинам. Отсюда нормы классов эквивалентности двойных ошибок попарно различны, что завершает доказательство теоремы.

Пример 5.12. Проверочная матрица H_R реверсивного кода C_R длиной 31 над полем $GF(2^5)$ для примитивного элемента α – корня полинома $x^5 + x^2 + 1$ – имеет следующий вид:

$$\begin{vmatrix}
0&0&0&0&1&0&0&1&0&1&1&0&0&1&1&1&1&1&0&0&0&1&1&0&1&1&1&0&1&0&1\\
0&0&0&1&0&0&1&0&1&1&0&0&1&1&1&1&1&0&0&0&1&1&0&1&1&1&0&1&0&1&0\\
0&0&1&0&0&1&0&1&1&0&0&1&1&1&1&1&0&0&0&1&1&0&1&1&1&0&1&0&1&0&0\\
0&1&0&0&0&0&1&0&0&1&0&1&1&0&0&1&1&1&1&1&0&0&0&1&1&0&1&1&1&0&1\\
1&0&0&0&0&1&0&0&1&0&1&1&0&0&1&1&1&1&1&0&0&0&1&1&0&1&1&1&0&1&0\\
0&1&0&1&0&0&1&1&0&1&1&0&0&0&1&1&1&1&1&0&0&1&1&0&1&0&0&1&0&0&0\\
0&0&1&0&1&1&1&1&1&0&1&1&0&0&0&1&1&1&1&1&0&0&1&1&0&1&0&0&1&0&0\\
0&0&0&1&0&0&0&1&1&1&0&1&1&0&0&0&1&1&1&1&1&0&0&1&1&0&1&0&0&1&0\\
0&1&0&1&1&1&0&1&1&0&0&0&1&1&1&1&1&0&0&1&1&0&1&0&0&1&0&0&0&0&1\\
1&0&1&0&1&1&1&0&1&1&0&0&0&1&1&1&1&1&0&0&1&1&0&1&0&0&1&0&0&0&0
\end{vmatrix}$$

Ниже представлена таблица диаметров, порождающих векторов, норм и их показателей Г-орбит одиночных и двойных ошибок в реверсивном коде G длиной 31 с проверочной матрицей $H_R = \left(\alpha^i, \alpha^{-i}\right)^T$, где α – корень полинома $x^5 + x^2 + 1$.

Таблица 5.5

Показатели норм Г*-орбит векторов-ошибок весом 1–2 в реверсивном коде длиной* $n = 31$

Г-орбита	Образующая вектор-ошибка	Синдром образующей		Норма Г-орбиты
		degs_1	degs_2	deg$N(S)$
I_1	$\bar{e}_1$	0	0	0
I_2	$\bar{e}_{1,2}$	18	17	4
I_3	$\bar{e}_{1,3}$	5	3	8
I_4	$\bar{e}_{1,4}$	29	26	24
I_5	$\bar{e}_{1,5}$	10	6	16
I_6	$\bar{e}_{1,6}$	2	28	30
I_7	$\bar{e}_{1,7}$	27	21	17
I_8	$\bar{e}_{1,8}$	22	15	7
I9	$\bar{e}_{1,9}$	20	12	1
I10	$\bar{e}_{1,10}$	16	7	23
I11	$\bar{e}_{1,11}$	4	25	29
I12	$\bar{e}_{1,12}$	19	8	27
I13	$\bar{e}_{1,13}$	23	11	3
I14	$\bar{e}_{1,14}$	14	1	15
I15	$\bar{e}_{1,15}$	13	30	12

I16	$\bar{e}_{1,16}$	24	9	2

Из табл. 5.5 непосредственно видно, что перечисленные Г-орбиты имеют попарно различные нормы.

Предложение 5. 10 (о распределении синдромов по нормам). В реверсивном коде каждое ненулевое значение нормы принимает в точности n различных синдромов. Значение $N(S)=0$ принимают в точности $2n+1$ различных синдромов, а именно, синдромы $(s_1, 0), (0, s_2), (0, 0), s_1 \neq 0, s_2 \neq 0$.

Следствие 1. Если $N(J)=0$, то J – полная Г-орбита с полным спектром синдромов.

Следствие 2. Пусть две Г-орбиты $<\bar{e}>$ и $<\bar{f}>$ имеют одинаковую и ненулевую норму. Тогда их спектры синдромов совпадают.

В любой тройке полных Г-орбит с полными спектрами синдромов и общей нулевой нормой по крайней мере две Г-орбиты имеют общий спектр синдромов.

Синдромы ошибок в коде C_R могут принимать $(n+1)^2$ различных значений. Код G декодирует n одиночных и $C_n^2 = \dfrac{n^2-n}{2}$ двойных случайных ошибок, всего $\dfrac{n^2+n}{2}$ ошибок. Это составляет примерно половину возможностей синдромных методов декодирования. На более широкие возможности кода C_R указывает следующее утверждение.

Теорема 5.7. *Пусть K – произвольная, но фиксированная совокупность* Г*-орбит векторов-ошибок (не являющихся кодовыми словами) с попарно различными нормами в реверсивном коде C_R. Если известно, что принятое слово $\bar{x}$ содержит вектор-ошибку из совокупности K, то код C_R ее однозначно корректирует.*

Замечание. Теорему 5.7 можно усилить, добавив в совокупность K две Г-орбиты с нулевой нормой, но с различными и полными спектрами синдромов.

Норма синдрома в коде C_R может принимать не более $n+1$ различных значений. Следовательно, по замечанию к теореме 5.7 код C_R может корректировать до $(n+2)\,n = n^2+2n$ ошибок. Этот практический предел синдромных методов декодирования, так как в коде C_R имеется не более $(n+1)^2 = n^2+2n+1$ (различных синдромов).

Пример 5.13. Имеем реверсивный код минимальной длины. Это код C_R над полем $GF(2^3)$ длиной $n = 2^3-1 = 7$. В качестве примитивного элемента

α поля $GF(2^3)$ возьмем корень полинома $x^3 + x + 1$. Тогда проверочная матрица кода C_R имеет вид

$$H = (\alpha^i, \alpha^{-i})^T = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

Составим таблицу Г-орбит векторов-ошибок весом 1–3, их образующих, синдромов образующих и норм этих орбит в коде G.

Таблица 5.6

Г-*орбиты векторов ошибок весом 1–3, их образующие, синдромы образующих и их нормы в реверсивном коде* G *длиной 7*

Г-орбита	I_1	I_2	I_3	I_4	J_1	J_2	J_3	J_4	J_5
Образующий вектор $\bar{e}$	$\bar{e}_1$	$\bar{e}_{12}$	$\bar{e}_{13}$	$\bar{e}_{14}$	$\bar{e}_{123}$	$\bar{e}_{124}$	$\bar{e}_{134}$	$\bar{e}_{125}$	$\bar{e}_{135}$
$S(\bar{e})$	$(1;1)$	$(\alpha^3;\alpha^2)$	$(\alpha^6;\alpha^4)$	$(\alpha;\alpha^5)$	$(\alpha^5;\alpha^3)$	$(0;\alpha)$	$(\alpha^4;0)$	$(\alpha^6;\alpha^6)$	$(\alpha^3;\alpha^3)$
$N(S(\bar{e}))$	1	α^5	α^3	α^6	α	0	0	α^4	α^2

Из табл. 5.6 следует, что из перечисленных в ней Г-орбит только J_2 и J_3 имеют одинаковые нормы, равные 0. Но их спектры синдромов, очевидно, не пересекаются, т. е. для любых $\bar{g} \in J_2$ и $\bar{f} \in J_3$ $S(\bar{g}) \neq S(\bar{f})$. Поэтому согласно теореме 5.7 и замечанию к нему рассматриваемый код C_R способен корректировать все ошибки весом 1–3, т. е. $7 \cdot 9 = 63$ векторы-ошибки – практический предел синдромных методов декодирования.

Построенная теория норм синдромов для реверсивных кодов предоставляет норменный метод коррекции ошибок и к данным кодам. Схема работы метода остается прежней. Продемонстрируем работу норменного метода на следующем примере.

Пример 5.14. Пусть ТКС работает на основе реверсивного кода из примера 5.12. Предположим, что приемное устройство ТКС приняло сообщение $\bar{x}$ с синдромом ошибок $S(\bar{x}) = (\alpha^{30}, \alpha^3)$. Вычислим $N(S(\bar{x})) = \alpha^{30} \cdot \alpha^3 = \alpha^2$. Норма указывает в соответствии с табл. 5.5, что вектор-ошибка $\bar{e}$ в сообщении $\bar{x}$ принадлежит Г-орбите $I_{16} = <(\bar{e}_{16})> = <(1,16)>$ с синдромом $S(\bar{e}_{16}) = (\alpha^{24}, \alpha^9)$.

Значит, $\bar{e} = \sigma^k(1, 16)$, где $k = \deg(\alpha^{30} / \alpha^{24}) = 6$. Таким образом, искомый вектор ошибок $\bar{e} = (7, 22)$.

5.8. Метод сжатия норм синдромов

На пути эффективной реализации норменного метода в БЧХ-кодах при коррекции многократных ошибок весом $\omega > 2$ стоит препятствие – достаточно большое количество Г-орбит этих ошибок, оцениваемое числом C_n^ω / n (см. разд. 3). В [14] установлена формула для числа T_ω ошибок с первой компонентой синдрома $s_1 = 0$. Для $\varpi = 3$ эта формула имеет вид: $T_3 = C_n^2 / 3 = n(n-1)/6$, где $n = 2^m - 1$ – длина примитивного БЧХ-кода. Отсюда следует, что количество Г-орбит таких тройных ошибок оценивается числом

$$T / n = (n-1)/6 = (2^m - 2)/6 = (2^{m-1} - 1)/3.$$

Это число равно 3 при $n = 15$, 5 – при $n = 31$, 11 – при $n = 63$ и т. д.

Рассмотрим модификацию норменного метода, предложенную в [15], которая преобразует векторы ошибок в векторы с $s_1 = 0$, на примере коррекции тройных ошибок.

Исходим из примитивного БЧХ-кода C_7 длиной $n = 2^m - 1$, $m > 3$, с проверочной матрицей $H = (\alpha^i, \alpha^{3i}, \alpha^{5i})^T$, где α – примитивный элемент поля Галуа $GF(2^m)$. Пусть принято сообщение $\bar{x}$ с синдромом ошибок $S = S(\bar{e}) = (s_1, s_2, s_3)$, причем $s_1 \neq 0$. Требуется найти тройную ошибку $\bar{e}$ в принятом сообщении $\bar{x}$.

Преобразуем искомую вектор-ошибку $\bar{e}$ в другую тройную ошибку $\bar{e}^*$, синдром которой имеет первую компоненту $s_1^* = 0$. Пусть x, y, z – локаторы ошибочных позиций вектора $\bar{x}$, ненулевых координат вектора $\bar{e}$. В качестве $\bar{e}^*$ берем вектор-ошибку весом 3 с локаторами ненулевых позиций $x^* = x + s_1$; $y^* = y + s_1$; $z^* = z + s_1$. Тогда компоненты синдрома $S(\bar{e}^*) = (s_1^*, s_2^*, s_3^*)$ выражаются следующим образом через компоненты синдрома $S(\bar{e})$:

$$s_1^* = x^* + y^* + z^* = (x + s_1) + (y + s_1) + (z + s_1) = (x + y + z) + s_1 = s_1 + s_1 = 0;$$

$$s_2^* = (x^*)^3 + (y^*)^3 + (z^*)^3 = (x + s_1)^3 + (y + s_1)^3 + (z + s_1)^3 =$$

$$= x^3 + y^3 + z^3 + s_1(x^2 + y^2 + z^2) + s_1^2(x + y + z) + s_1^3 + s_1^3 + s_1^3 = s_2 + s_1^3;$$

$$s_3^* = (x^*)^5 + (y^*)^5 + (z^*)^5 = (x + s_1)^5 + (y + s_1)^5 + (z + s_1)^5 =$$

$$= (x + s_1)^4 (x + s_1) + (y + s_1)^4 (y + s_1) + (z + s_1)^4 (z + s_1) =$$

$$= x^5 + y^5 + z^5 + s_1(x^4 + y^4 + z^4) + s_1^4(x + y + z) + s_1^5 + s_1^5 + s_1^5 = s_2 + s_1^5 = s_3 + s_1^5.$$

Для нахождения вектора-ошибки $\bar{e}^*$ норменным методом достаточно иметь лишь фрагмент таблицы Г-орбит тройных ошибок, содержащий только

Г-орбиты тройных ошибок с $s_1 \neq 0$.

Пример 5.15. Решим пример 2.9 модифицированным норменным методом. В этом примере $n = 63$, α – корень полинома $x^6 + x^5 + x^4 + x + 1$, синдром $S = S(\bar{e}) = (\alpha^{21}, \alpha^{44}, \alpha^{27})$.

Решение. У нас $s = \alpha^{21} \neq 0$. От искомой ошибки $\bar{e}$ переходим к $\bar{e}^*$, у которой компоненты синдрома $s_1^* = s_1 + s_1 = 0$, $s_2^* = s_2 + s_1^3 = \alpha^{44} + \alpha^{63} = \alpha^{12}$, $s_3^* = s_3 + s_1^5 = \alpha^{27} + \alpha^{105} = \alpha^{29}$. Таким образом, $S(\bar{e}^*) = (0, \alpha^{12}, \alpha^{29})$. Тогда $\bar{N}(S(\bar{e}^*) = (\infty, \infty, \alpha^{27})$.

Составим таблицу Г-орбит тройных ошибок в данном коде с $s_1 = 0$, табл. 5.7.

Таблица 5.7

Список всех Г*-орбит тройных ошибок с* $s_1 = 0$, *их образующих, синдромов образующих и норм этих орбит в* (*63, 45, 7*)*-БЧХ-коде*

№ п/п	Образующая $\bar{e}_i$	Синдром $S(\bar{e}_i)$	Норма $\bar{N}_i = \bar{N}(S(\bar{e}))_i$
1	(1,2,40)	$(0,\alpha^{40},\alpha^{12})$	$(\infty, \infty, \alpha^{25})$
2	(1,3,16)	$(0,\alpha^{17},\alpha^{24})$	$(\infty,\infty,\alpha^{50})$
3	(1,5,31)	$(0,\alpha^{34},\alpha^{48})$	$(\infty, \infty, \alpha^{37})$
4	(1,9,61)	$(0,\alpha^{5},\alpha^{33})$	$(\infty,\infty,\alpha^{11})$
5	(1,17,58)	$(0,\alpha^{24},\alpha^{19})$	$(\infty,\infty,\alpha^{22})$
6	(1,33,52)	$(0,\alpha^{20},\alpha^{6})$	$(\infty,\infty,\alpha^{44})$
7	(1,6,29)	$(0,\alpha^{33},\alpha^{7})$	$(\infty,\infty,\alpha^{45})$
8	(1,11,57)	$(0,\alpha^{3},\alpha^{14})$	$(\infty,\infty,\alpha^{27})$
9	(1,21,50)	$(0,\alpha^{6},\alpha^{28})$	$(\infty,\infty,\alpha^{54})$
10	(1,22,43)	(0,1,0)	$(\infty,-,0)$
11	(1,10,46)	$(0,\alpha^{54},\alpha^{27})$	$(\infty,\infty,1)$

Сравнивая $\bar{N}(S(\bar{e}^*) = (\infty, \infty, \alpha^{27})$ с данными таблицы, приходим к выводу, что $\bar{e}^* \in J_8$ и получается циклическим сдвигом вектора $\bar{e}_8 = (1, 11, 57)$. $S(\sigma(\bar{e}_8)) = (0, \alpha^6, \alpha^{19})$. $S(\sigma^2(\bar{e}_J)) = (0, \alpha^9, \alpha^{24})$. $S(\sigma^3(\bar{e}_J)) = (0, \alpha^{12}, \alpha^{29}) = S(\bar{e}^*)$. Значит, $\bar{e}^* = \sigma^3(\bar{e}_8) = (4, 14, 60)$ – тройная вектор-ошибка с ненулевыми координатами на 4, 14, 60-й позициях, локаторы которых $x^* = \alpha^3$, $y^* = \alpha^{13}$, $z^* = \alpha^{59}$. Отсюда легко находятся локаторы x, y, z ненулевых координат искомого вектора ошибок $\bar{e}$ $x = x^* + s_1 = \alpha^3 + \alpha^{21} = \alpha^{30}$; $y = y^* + s_1 = \alpha^{13} + \alpha^{21} = \alpha^{10}$; $z = z^* + s_1 = \alpha^{59} + \alpha^{21} = \alpha^{20}$. Следовательно,

$\bar{e} = (11, 21, 31)$ – тройная ошибка на 11, 21 и 31-й позициях, что полностью совпадает с решением задания 2.9.

Литература

1. Шеннон, К. Работы по теории информации и кибернетике / К. Шеннон. – М. : ИЛ, 1963. – 732 с.

2. Мак-Вильямс, Ф. Дж. Теория кодов, исправляющих ошибки / Ф. Дж. Мак-Вильямс, Н. Дж. А. Слоэн. – М. : Связь, 1979. – 744 с.

3. Блейхут, Р. Теория и практика кодов, контролирующих ошибки / Р. Блейхут. – М. : Мир, 1986. – 576 с.

4. Питерсон, У. Коды, исправляющие ошибки / У. Питерсон, Э. Уэлдон. – М. : Мир, 1976. – 574 с.

5. Теория кодирования / Т. Кассами [и др.]. – М. : Мир, 1978. – 576 с.

6. Теория информации и кодирование: учеб. пособие / Б. Б. Самсонов [и др.]. – Ростов н/Д. : Феникс, 2002. – 288 с.

7. Прикладная теория кодирования: учеб. пособие для вузов. Т. 1 – 2 / В. К. Конопелько [и др.]. – Минск : БГУИР, 2004. – 688 с.

8. Вернер, М. Основы кодирования: учеб. пособие для вузов / М. Вернер. – М. : Техносфера, 2006. – 288 с.

9. Морелос-Сарагоса, Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение: учеб. пособие для вузов / Р. Морелос-Сарагоса. – М.: Техносфера, 2006. – 320 с.

10. Артин, Э. Геометрическая алгебра / Э. Артин. – М.: Наука, 1969. – 284 с.

11. Лиддл, Р. Конечные поля. Т. 1 – 2 / Р. Лиддл, Г. Нидеррайтер. – М.: Мир, 1988. – 822 с.

12. Липницкий, В. А. Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа / В. А. Липницкий. – Минск : БГУИР, 2005. – 88 с.

13. Липницкий, В. А. Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа / В. А. Липницкий. – Минск : БГУИР, 2006. – 88 с.

14. Конопелько, В. К. Теория норм синдромов и перестановочное декодирование помехоустойчивых кодов / В. К. Конопелько, В. А. Липницкий. – Минск : БГУИР, 2000. – 242 с.

15. Конопелько, В. К. Теория норм синдромов и перестановочное декодирование помехоустойчивых кодов / В. К. Конопелько, В. А. Липницкий. – 2-е изд. – М.УРСС, 2004. – 176 с.

16. Липницкий, В. А. Норменное декодирование помехоустойчивых кодов и алгебраические уравнения / В. К. Конопелько, В. А. Липницкий. – Минск : Изд. центр БГУ, 2007. – 240 с.

17. Липницкий, В. А. Норменное декодирование ошибок посредством их модификации / В. А. Липницкий, Е. К. Аль-Хайдар. – Доклады БГУИР. №5(43). – 2009. – С. 12 – 16.

18. Дворников, В. Д. Теория и практика низкоскоростных кодов / В. Д. Дворников, В. К. Конопелько, В. А. Липницкий. – Минск : БГУИР, 2002. – 210 с.

19. Лосев, В. В. Микропроцессорные устройства обработки информации. Алгоритмы цифровой обработки / В. В. Лосев. – Минск : Выш. шк. 1990. – 132 с.

20. Муттер, В. М. Основы помехоустойчивой телепередачи информации / В. М. Муттер. – Л.: Энергоатомиздат, 1990. – 286 с.

СОДЕРЖАНИЕ

Св. план 2010, поз. 62

Учебное издание

Липницкий Валерий Антонович

ТЕОРИЯ НОРМ СИНДРОМОВ

Методическое пособие
для студентов специальностей
1-45 01 03 «Сети телекоммуникаций»,
1-45 01 05 «Системы распределения мультимедийной информации»,
1-98 01 02 «Защита информации в телекоммуникациях»
всех форм обучения

Редактор Е. Н. Батурчик
Компьютерная верстка Г. М. Кореневская

Подписано в печать 01.12.2010. Формат 60×84 1/16 Бумага офсетная.
Гарнитура «Таймс» Отпечатано на ризографе. Усл. печ. л. 5,81.
Уч.-изд. л. 5,6. Тираж 150 экз. Заказ 304.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»
ЛИ № 02330/0494371 от 16.03.2009. ЛП № 02330/0494175 от 03.04.2009.
220013, Минск, П. Бровки, 6