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

В. А. Липницкий, Д. Н. Олешкевич, Н. В. Спичекова

ТЕОРИЯ НОРМ СИНДРОМОВ. ПОСОБИЕ ДЛЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Рекомендовано УМО по образованию в области информатики и радиоэлектроники в качестве учебно-методического пособия для специальностей 1-45 01 03 «Сети телекоммуникаций», 1-45 01 05 «Системы распределения мультимедийной информации», 1-98 01 02 «Защита информации в телекоммуникациях»

Минск БГУИР 2013

УДК 512:621.391(076)
ББК 22.132я73+32.811я73
Л61

Р е ц е н з е н т ы:

доцент кафедры дифференциальных уравнений и системного анализа
Белорусского государственного университета,
кандидат физико-математических наук, доцент А. Э. Малевич;

кафедра высшей математики учреждения образования
«Белорусский государственный экономический университет»
(протокол №8 от 05.04.2012 г.)

Липницкий В. А.

Л61 Теория норм синдромов. Пособие для практических занятий : учеб.-метод. пособие / В. А. Липницкий, Д. Н. Олешкевич, Н. В. Спичекова. – Минск : БГУИР, 2013. – 96 с. : ил.

ISBN 978-985-488-873-6.

Учебно-методическое пособие служит цели практического освоения студентами материала специального курса «Теория норм синдромов». Приведен материал для практических, лабораторных и самостоятельных занятий по помехоустойчивому кодированию и собственно теории норм синдромов. Пособие практически знакомит с базовыми помехоустойчивыми кодами, с применением современной алгебры в теории и практике помехоустойчивого кодирования.

УДК 512:621.391(076)
ББК 22.132я73+32.811я73

ISBN 978-985-488-873-6

Введение

Теория и практика помехоустойчивого кодирования в отличие от многих других разделов научного знания имеет чёткую дату своего рождения. Это 1948 год. Именно в этом году американский инженер-исследователь Клод Шеннон получил ряд результатов, на основе которых сделал знаменитый впоследствии секретный доклад Сенату США. Всё это легло в основу его монографии [1]. Данная книга до сих пор служит вдохновляющим источником и надёжной базой для различных исследований по защите информации от помех и несанкционированного доступа, а потому продолжает оставаться источником многократного цитирования, и надо сказать, вполне заслуженно.

В последней четверти XX века вышел ряд монографий по теории кодирования, в частности [2 – 6]. Среди них выделяется своей фундаментальностью и полнотой информации на момент издания монография [2]. Недаром в среде специалистов она носит почётный титул «библии для кодировщиков».

Лишь в начале третьего тысячелетия стали появляться первые учебники и учебные пособия для вузов по данной отрасли знания [7 – 10]. Однако новое не значит лучшее. Возникающая на глазах одного поколения теория помехоустойчивых кодов насыщена идеями из различных областей математики и вообще науки. Новые коды появляются на основе интуитивных прозрений их создателей, и только их обобщения получаются логическим осмыслением образовавшегося прорыва знаний. Но и эта логика насыщена духом научного творческого поиска. Яркими примерами к сказанному служат теория кодов Рида-Соломона, выросшая из идеи кодов Хемминга через промежуточное, но совершенно необходимое звено – коды Боуза-Чоудхури-Хоквингема, а также алгебро-геометрические коды – неотделимые от их первоисточника – кодов Гоппы. Последние явились результатом научной деятельности и творческой жизни российского математика Гоппы В. Д. Любая же монография, а тем более учебник, пытается уложить новую область знания в прокрустово ложе научной логики. Можно смело утверждать, что этот совершенно необходимый этап научного

развития применительно к теории помехоустойчивого кодирования далёк от своего завершения. Предлагаемая ниже работа лишь скромнейший шажок в указанном направлении, во многом отражающий вкусы, интересы, предпочтения и исследовательский путь автора.

На факультетах БГУИР студенты изучают весь спектр вопросов, связанных с обработкой, хранением, передачей и защитой информации от помех и несанкционированного доступа. Соответствующие курсы являются относительно новыми, многие из них находятся в динамике становления или развития в соответствии с технологической революцией или потребностями времени, требуют изучения новых разделов математики, не вошедших в классический курс «Высшая математика» – необходимую базу высшего технического образования. Такие курсы, как «Цифровая обработка сигналов», «Прикладная теория кодирования», «Криптографические методы защиты информации» и ряд других, предполагают основательное знание структур современной алгебры.

Поэтому на кафедре Высшей математики разработан курс «Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа», относящийся к разделу «Специальные главы высшей математики». На протяжении ряда лет этот курс успешно читается студентам БГУИР специальностей «Информатика» и «Системы и сети телекоммуникаций». Издано соответствующее учебно-методическое пособие, где изложен необходимый теоретический материал.

Опыт показывает, что глубокое и надежное усвоение нового материала невозможно без его основательной проработки на практических и лабораторных занятиях. Данное издание является первым учебно-методическим пособием для проведения практических и лабораторных занятий по названному выше курсу. Предлагается рабочая модель восьми практических и лабораторных занятий по основным темам курса. При этом в зависимости от сложившейся традиции лабораторные задания можно рассматривать как домашние – для самостоятельного, индивидуального изучения.

Данное издание будет полезно не только студентам названных специальностей, но и всем, кто изучает проблематику помехоустойчивого кодирования информации, формирования и обработки дискретных сигналов, защиты информации от помех и несанкционированного доступа.

Практическое занятие №1

Линейные коды. Порождающая матрица кода

1. Необходимые теоретические сведения

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

Формальное математическое определение кода выглядит загадочным.

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.

Данное определение явно требует пояснений. В современных цифровых инфокоммуникационных системах (ИКС) принято передаваемую информацию задавать в виде блоков – конечных последовательностей фиксированной длины символов из данного поля P. Другими словами, всякое информационное слово представляет собой k –разрядный вектор – произвольный вектор из k–мерного линейного пространства $P_k = \{(x_1, x_2, ..., x_k) \,|\, x_i \in P\}$ для заданного целого $k > 1$. Поэтому такая форма представления информации кодированием не считается. Главная цель кодирования – обеспечить надежную передачу информации в каналах с шумами, то есть помехами. Малейшее изменение слова-вектора $\bar{x} = (x_1, x_2, ..., x_k)$ приводит к другому информационному вектору $\bar{y} \in P_k$. Согласно базовой идее Шеннона К. успешную борьбу с помехами в каналах с шумами можно осуществлять искусным введением избыточности в передаваемую информацию.

Теорема 1.1 (Шеннон К., 1948 г.). Введением избыточности в передаваемую в зашумлённом канале связи информацию можно добиться исправле-

ния возникающих в процессе передачи этой информации сколь угодно сложных ошибок.

Удачно наделенный избыточностью, каждый вектор-сообщение приобретает настолько специфические индивидуальные свойства, что даже после прохождения в каналах с шумами, после наложения искажений остается возможность этот вектор, то есть исходную передаваемую информацию, однозначно восстановить.

Идея Шеннона получила различные интерпретации и реализации. Наиболее простой и наиболее популярной оказалась реализация идеи Шеннона линейными кодами.

В линейных кодах избыточность достигается введением искусных поразрядных, то есть покоординатных проверок: к каждому информационному слову-сообщению $\bar{x} = (x_1, x_2, ..., x_k)$ добавляются $n-k$ координат-разрядов; координаты $x_{k+1}, ..., x_n$ таковы, что их специально подобранные алгебраические суммы с предыдущими координатами в неискаженном состоянии принимают строго фиксированные (обычно, нулевые) значения.Удлиненные таким образом векторы принято называть кодовыми. Код – совокупность всех кодовых векторов, получаемых при заданном способе кодирования.

С математической точки зрения рассмотренное преобразование есть линейное отображение линейного пространства P_k в пространство большей размерности P_n, $n > k$. Из курса линейной алгебры следует матричное задание линейных отображений векторных пространств. Следовательно, кодирование есть, по сути дела, умножение информационных слов-векторов на некоторую матрицу G порядка $k \times n$ с коэффициентами из поля P.

Поясним этот момент более детальными 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 этому базису пространства P_n. Полученные в результате разложения 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. Применив операцию траспонирования к равенству $A_\varphi(x) = (y)$, 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 общей 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.

Пример 1.1. С середины XX века долгое время в американских системах цифровой связи передача данных осуществлялась в так называемом ASCII-формате. Этот формат требовал передавать данные блоками по 8 двоичных бит, 7 из них были информационными, а 8-й был проверочным, в нём записывался 0 или 1 так, чтобы во всём байте, то есть во всём блоке, сохранялось чётное число единиц. Таким образом, восьмой бит осуществлял проверку на чётность во всём байте – все восемь координат x_i, $1 \le i \le 8$, байта в совокупности удовлетворяли над полем Галуа $Z/2Z$ из двух элементов 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, причём размерность подпространства решений равна $k = n - r$, где r – ранг матрицы H коэффициентов системы. В линейной алгебре данное подпространство называют ядром матрицы H и потому обозначают через $KerH$ (от английского kernel – ядро).

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 Ф.С.Р. – базис пространства L решений данного уравнения – образуют следующие 7 векторов: $\bar{e}_1 = (1000\,0001)$, $\bar{e}_2 = (0100\,0001)$,..., $\bar{e}_7 = (0000\,0011)$. Пусть $G - (7 \times 8)$ – матрица, строки которой состоят из координат векторов $\bar{e}_1, \bar{e}_2, ..., \bar{e}_7$:

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}. \qquad (1.1)$$

Умножением произвольных 7-мерных информационных двоичных векторов на матрицу G мы 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 $(k+1)$ проверочного разряда, в нём записывается 0 или 1 так, чтобы во всём блоке сохранялось чётное число единиц. Здесь $n = k + 1$. Такие коды называ-

ют кодами с проверкой на чётность. Будем их в дальнейшем обозначать символом $C_ч$.

Осмысление примера 1.1, точнее факта реальной послевоенной жизни США Клодом Шенноном, привело к формулировке его знаменитой теоремы 1.1., выражающей главную цель и назначение помехоустойчивых кодов.

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. Это развитие отражено в следующем примере.

Пример 1.3. Пусть $P = GF(2)$ – поле Галуа из двух элементов; $k = 4$, то есть 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 из поля $GF(2)$. Каждый вектор $\bar{x}$ кодируем, присоединив к нему координаты x_5, x_6, x_7 вычисленные по следующим 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:

$$\begin{cases} x_1 + x_2 + x_4 + x_5 = 0, \\ x_1 + x_3 + x_4 + x_6 = 0, \\ x_2 + x_3 + x_4 + x_7 = 0. \end{cases} \qquad (1.2)$$

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 заданном базисе пространства P_n.

Из примера 1.1 следует, что матрица (1.1) является матрицей G, порождающей ASCII-формат.

Построим порождающую матрицу $G_\chi(7, 4)$ – кода Хемминга из примера

1.3. В двоичном четырёхмерном пространстве возьмём 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 следуют следующие свойства.

Свойство 1. Порождающая матрица G линейного (k, n) – кода является прямоугольной (k, n) – матрицей, где $n > k$, ранг которой равен k.

Значение k возникает из требований на соответствие размеров перемножаемых векторов и матриц. Условие $n > k$ обеспечивает избыточность – наличие «дополнительных, проверочных» $n - k$ разрядов. В силу условия $n > k$ ранг матрицы G не может быть больше k. Условие $rank(G) > k$ неизбежно повлекло бы за собой наличие информационых векторов с одинаковыми «кодировками». Только условие $rank(G) = k$ обеспечивает инъективность операции кодирования: различным информационным словам соответствуют различные кодовые слова.

Название порождающей матрицы объясняет свойство 2.

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.

Свойство 3. Порождающая матрица кода определена не однозначно.

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 следующее свойство.

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

$$\bar{b} = \bar{a} \cdot G. \qquad (1.3)$$

Пример 1.4. Закодируем $(7, 4)$ – кодом Хемминга информационное слово $\bar{a} = (1101)$. Согласно формуле (1.3)

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

Корректность перехода, задаваемого формулой (1.3), то есть однозначность восстановления $\bar{a}$ по заданному $\bar{b}$, гарантирует теорема 1.2.

Теорема 1.2. Отображение $g : P_k \to P_n$ по формуле (1.3) с $k \times n$ матрицей G ранга k, $1 \le k < n$, и с коэффициентами из поля P является взаимно-однозначным (биекцией).

Свойство 5. 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 её 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 даёт непосредственный алгоритм восстановления исходной информации.

Пример 1.5. 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 четырёх уравнений, которая однозначно указывает, что $\bar{x} = \bar{a} = (1101)$.

2. Задания для аудиторной работы

Задание 1. Выяснить, может ли двоичная матрица $A = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \end{pmatrix}$ быть порождающей матрицей линейного кода?

Решение. Известно, что у прямоугольной $(k \times n)$ – матрицы G, порождающей линейный (n, k) – код, ранг равен k. В нашем случае матрица A имеет порядок (4×7). Найдём её ранг методом элементарных преобразова-

ний. С помощью элементарных преобразований строк данную матрицу можно привести к следующему квазитреугольному виду: $B = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}$.

Минор порядка 4 матрицы B, состоящий из 1-го, 2-го, 4-го и 5-го столбцов, очевидно равен $1 \neq 0$. Следовательно, $rankA = 4$ и матрицу A можно взять в качестве порождающей матрицы линейного $(n, k)-$кода.

Задание 2. Выяснить тот же вопрос (из задания 1) для матрицы F, где

а) $F = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$; б) $F = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{pmatrix}$.

Задание 3. С помощью матрицы A закодировать информационное слово $\bar{i} = (1101)$.

Решение. Кодовое слово из информационного получается с помощью порождающей матрицы по формуле $\bar{c} = \bar{i} \cdot G$. В данном случае

$$\bar{c} = \bar{i} \cdot A = (1101) \cdot \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \end{pmatrix} = (0000101).$$

Задание 4. С помощью матрицы F закодировать информационное слово а) $\bar{i} = (11010)$; б) $\bar{i} = (01011)$.

Задание 5. В $(7, 4)-$коде C с порождающей матрицей A однозначно ли восстанавливается информационное слово по данному кодовому слову $\bar{c} = (000\ \ 010\ \ 1)$?

Решение. Данное кодовое слово получено умножением неизвестного информационного слова $\bar{x} = (x_1, x_2, x_3, x_4)$ на матрицу $A: \bar{x} \cdot A = \bar{c}$. Это равенство двух семимерных векторов. В координатной форме оно выглядит как сис-

тема линейных алгебраических уравнений (СЛАУ) относительно неизвестных x_1, x_2, x_3, x_4 :

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

В процессе решения задания 1 мы установили, что один из базисных миноров матрицы A расположен в 1-м, 2-м, 4-м и 5-м столбцах этой матрицы. Значит, полученная СЛАУ эквивалентна своей подсистеме из 1-го, 2-го, 4-го и 5-го уравнений. Выпишем эту подсистему в матричной форме: $\left(\begin{array}{cccc|c} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{array}\right)$. Несложные вычисления показывают, что данная подсистема, а с ней и вся система имеют единственное решение: $x_1 = 1; x_2 = 1; x_3 = 0; x_4 = 1.$ Проведенные вычисления показывают, что существует единственный информационный вектор $\bar{i} = (1101),$ порождающий данное кодовое слово $\bar{c} = (0000101)$.

Задание 6. Убедиться, что полученные в задании 4 кодовые слова однозначно восстанавливаются до породивших их информационных слов.

Задание 7. Попытайтесь «усовершенствовать» пример 1.1 проверкой на четность отдельно координат с нечетными номерами и отдельно – с четными номерами. Постройте проверочную матрицу нового кода.

3. Задания для самостоятельной работы

1. Выяснить, может ли заданная матрица (по вариантам) быть порождающей матрицей линейного кода?

2. Закодировать с помощью матрицы из первого задания сообщение

$\overline{i_1} = (110\ 101)$ для нечетных вариантов и задание $\overline{i_2} = (011\ 011)$ для нечетных вариантов.

3. По полученному в задании 2 кодовому слову однозначно восстановить исходное информационное сообщение.

Вариант 1

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

Вариант 2

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

Вариант 3

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

Вариант 4

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

Вариант 5

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

Вариант 6

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

Вариант 7

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

Вариант 8

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

Вариант 9

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

Вариант 10

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

Вариант 11

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

Вариант 12

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

Вариант 13

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

Вариант 14

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

Вариант 15

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

Вариант 16

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

Практическое занятие №2

Проверочная матрица линейного кода. Метрика Хемминга. Синдромы ошибок

1. Необходимые теоретические сведения

Пусть C – линейный (n, k) – код над полем P.

Определение 2.1. Матрица H порядка $m \times n$, $m = n - k$ называется проверочной матрицей кода C, если $KerH = C$.

Отметим некоторые свойства проверочных матриц.

Свойство 1. Проверочная матрица у каждого линейного кода всегда существует.

Данное свойство следует из общего факта линейной алгебры: для всякого собственного подпространства W линейного пространства P_n существует система линейных однородных уравнений, множество решений которой в точности совпадает с множеством векторов подпространства W.

Если известна порождающая матрица $G = (g_{ij})$ кода C, то с помощью строк этой матрицы, а фактически базиса $\bar{g}_1 = (g_{11}, g_{12}, ..., g_{1n})$, $\bar{g}_2 = (g_{21}, g_{22}, ..., g_{2n})$, $\bar{g}_k = (g_{k1}, g_{k2}, ..., g_{kn})$ кода C, можно составить систему линейных однородных уравнений:

$$\begin{cases} g_{11}x_1 + g_{12}x_2 + ... + g_{1n}x_n = 0, \\ g_{21}x_1 + g_{22}x_2 + ... + g_{2n}x_n = 0, \\ ..... \\ g_{k1}x_1 + g_{k2}x_2 + ... + g_{kn}x_n = 0. \end{cases} \qquad (2.1)$$

Множество решений системы (2.1) составляет ядро матрицы G – подпространство пространства P_n размерностью $m = n - r = n - k$. Пусть $\bar{h}_j = (h_{j1}, h_{j2}, ..., h_{jn})$, $1 \le j \le m$, – базис пространства решений системы (2.1). Тогда матрица

$$H = \begin{pmatrix} h_{11} & h_{12} & \dots & h_{1n} \\ h_{21} & h_{22} & \dots & h_{2n} \\ \dots & \dots & \dots & \dots \\ h_{m1} & h_{m2} & \dots & h_{mn} \end{pmatrix} \tag{2.2}$$

есть искомая проверочная матрица кода C. Действительно, в силу соотношений (2.1) должны выполняться равенства $H \cdot \overline{g}_i^T = \overline{0}^T$, $1 \le i \le k$. Они означают, что $C \subseteq KerH$. С другой стороны, $\dim KerH = n - rankH = n - m = k$. Это означает, что $KerH = C$. H – действительно является проверочнай матрицей кода C.

Свойство 2. Координаты базиса ядра матрицы G составляют проверочную $(n-k) \times n$ – матрицу H кода C: только для векторов $\overline{c} \in L$ $H \cdot \overline{c}^T = \overline{0}$ и только для них.

Свойство 3. $H \cdot G^T = 0$; $G \cdot H^T = 0$.

Пример 2.1. Код $C_ч$ с проверкой на чётность из примера 1.2 состоит из векторов-решений единственного уравнения $x_1 + x_2 + \dots + x_n = 0$ над полем $P = GF(2)$. Следовательно, проверочная матрица кода $C_ч$ есть $(1 \times n)$ – матрица и имеет вид: $H = (1\,1 \dots 1)$.

Пример 2.2. В силу сказанного выше, матрица коэффициентов системы линейных уравнений (1.3)

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

есть проверочная матрица $(7,4)$ – кода Хемминга, определенного в примере 1.3. Так как базисный минор матрицы H расположен в последних трех столбцах, то x_1, x_2, x_3, x_4 являются свободными переменными системы линейных уравнений (1). Отсюда легко получаем порождающую матрицу кода Хемминга:

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

Проверочная матрица кода определена не однозначно.

Свойство 4. 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.

Данное свойство дополняет свойство, указанное ниже.

Свойство 5. 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 $AH = H_1$.

Каждая из матриц G или H однозначно определяет код C.

Из свойств 3 и 4 следует критерий для определения, когда две матрицы являются проверочными матрицами одного и того же линейного кода.

Теорема 2.1. 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 $H^* = AH$.

Свойство 6. Количество различных проверочных матриц линейного (n, k) – кода над конечным полем P совпадает с количеством различных невырожденных квадратных матриц порядка m в поле P, то есть с порядком группы $GL_m(P)$ невырожденных квадратных матриц порядка m над полем P.

Свойство 6 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 $2^{10}\left(2^5 - 1\right)\left(2^{4-1} - 1\right)\left(2^3 - 1\right)\left(2^2 - 1\right) = 9999360$. 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.

Определение 2.2. Метрикой или расстоянием на множестве X называется определённая на декартовом квадрате $X \times X$ функция ρ с неотрицательными действительными значениями, удовлетворяющая при любых $x, y \in X$ условиях:

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

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

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

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

Определение 2.3. Расстоянием Хемминга 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 2.1. Расстояние Хэмминга обладает всеми свойствами обычного расстояния:

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.

Определение 2.4. $t-$окрестностью вектора $\overline{x} \in P_n$ назовём совокупность всех векторов $\overline{y} \in P_n$, для которых $dist(\overline{x}, \overline{y}) \le t.$

$t-$окрестности обладают обычным свойством отделимости.

Лемма 2.2. Если $dist(\overline{x}, \overline{z}) > 2t,$ то $t-$окрестности векторов $\overline{x}, \overline{z} \in P_n$ не пересекаются.

Определение 2.5. Минимальным или кодовым расстоянием кода C называется наименьшее из расстояний между попарно различными векторами кода C.

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

Значение кодового расстояния определяет следующая фундаментальная в помехоустойчивом кодировании теорема.

Теорема 2.2. 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.

Следующая теорема служит критерием для определения минимального расстояния кода.

Теорема 2.3. 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 2.3. Пусть $[i]$ это *i*–ый столбец проверочной матрицы H линейного кода C над полем P. Вектор $\overline{c} \in P_n$ 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.

Одним из важнейших понятий теории помехоустойчивых кодов является синдром ошибок. В процессе передачи информации на кодовое слово $\overline{c}$ может

наложиться «шум» вектор-ошибок $\bar{e}$. В результате приемное устройство получает искажённое сообщение $\bar{y} = \bar{c} + \bar{e}$.

Определение 2.6. 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 $S = \mathrm{H} \cdot \bar{y}^T = \mathrm{H} \cdot \left(\bar{c}^T + \bar{e}^T\right) = \mathrm{H} \cdot \bar{c}^T + \mathrm{H} \cdot \bar{e}^T = \mathrm{H} \cdot \bar{e}^T$. Это означает, что S зависит только от вектора ошибок $\bar{e}$ и не зависит от кодовых слов.

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

Предложение 2.1. Если $\bar{e}$ пробегает все векторы пространства E_n, то S пробегает все векторы пространства E_{n-k}.

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.

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 2.2. 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: $S(\bar{e}_1) \neq S(\bar{e}_2)$.

Предложение 2.2 вместе с очевидной уверенностью, что наиболее вероятны ошибки малого веса, создают теоретическую базу для синдромных мето-

дов коррекции ошибок по значениям синдромов ошибок, определяющих соответствующие векторы ошибок из множества $K_{od...t}$. Основные преимущества синдромных методов в следующем:

1) согласно предложению 2.2 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.

2. Задания для аудиторной работы

Задание 1. Дана порождающая $(7, 4)$ – код – матрица $G = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \end{pmatrix}$. Найти проверочную матрицу этого кода. Однозначно ли она определена?

Решение. Проверочная и порождающая матрицы H и G (соответственно) всякого линейного кода связаны соотношениями: $G \cdot H^T = 0$ и $H \cdot G^T = 0$. При этом размерности этих матриц взаимно-дополнительны: если G является $(k \times n)-$матрицей, то H является $((n-k) \times n)-$матрицей. Из этих фактов следует, что строки матрицы H составлены из координат ядра матрицы G. Следовательно, надо найти Ф.С.Р. – базис пространства решений однородной СЛАУ $G \cdot X = O,$ где $X = (x_1, x_2, ..., x_n)^T -$столбец неизвест-

ных, а затем из координаты векторов базиса пространства решений выписать в строки матрицы H. Выпишем систему $G \cdot X = O$ в матричной форме: $\left(\begin{array}{ccccccc|c} 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{array}\right)$. Решим систему методом Гаусса. Элементарные преобразования строк приводят систему к виду

$\left(\begin{array}{ccccccc|c} 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \end{array}\right)$. Система приведена к квазидиагональному виду. В ней, очевидно, базисными переменными являются 1-я, 2-я, 4-я и 5-я, а свободными – 2-я, 6-я и 7-я. При этом $x_1 = x_3 + x_6$; $x_2 = x_3 + x_7$; $x_4 = x_6 + x_7$; $x_5 = x_7$. Значит, размерность пространства решений равна трём. Придавая тройке свободных переменных (x_3, x_6, x_7) последовательно значения (100); (010); (001), получим искомый базис пространства решений СЛАУ: $\bar{h}_1 = (1110000)$; $\bar{h}_2 = (1001010)$; $\bar{h}_3 = (0101101)$. Следовательно, матрица $H = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$. Матрица H определена неоднозначно, поскольку тройка (x_3, x_6, x_7) может принимать достаточно широкий спектр значений: каждая тройка значений должна быть линейно независимой – определитель, составленный из каждой такой тройки должен быть отличным от нуля.

Задание 2. Построить проверочную матрицу кода по заданной порождающей матрице G, если эта матрица имеет вид

а) $G = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$; б) $G = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{pmatrix}$.

Задание 3. Найти расстояние Хемминга между векторами $\bar{x}$ и $\bar{y}$, если

а) $\bar{x} = (110101001)$, $\bar{y} = (011110101)$; б) $\bar{x} = (111101101)$, $\bar{y} = (111000111)$.

Задание 4. Определить декодирующие возможности линейного кода, заданного проверочной матрицей $H = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$.

Решение. Декодирующие возможности линейного кода определяются его минимальным расстоянием – минимальным весом d кодовых слов этого кода: если $d = 2t+1$ или $d = 2t+2,$ то код способен исправлять векторы-ошибки весом $1 \le \varpi \le t.$ Параметр d определяется по проверочной матрице кода: если у проверочной матрицы H данного кода любые $d-1$ столбцов линейно независимы, но найдутся d линейно зависимых столбцов, то минимальное расстояние кода равно d.

В данном случае любые два столбца неодинаковы и, следовательно, линейно независимы над полем $Z/2Z,$ но найдутся три линейно зависимых столбца. Например, сумма второго, третьего и седьмого столбцов данной матрицы H равна нулю, иными словами, линейная комбинация этих столбцов равна нулю. Короче говоря, эти три столбца линейно зависимы. Следовательно, $d = 3,$ данный код способен корректировать одиночные ошибки.

Задание 5. Найти все кодовые слова кода C, заданного матрицей H из задания 4. Составить таблицу распределения весов кодовых слов. Убедиться непосредственно, что минимальное расстояние кода действительно равно 3.

Задание 6.Определить декодирующие возможности линейного кода, заданного проверочной матрицей $H,$ если эта матрица имеет вид

а) $H = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$; б) $H = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{pmatrix}$.

Задание 7. ТКС функционирует на основе линейного кода, заданного

проверочной матрицей $H = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$ (из задания 3). ТКС приняла сообщение $\bar{x} = (1010101)$. Определить наличие ошибок в этом сообщении.

Решение. О наличии или отсутствии ошибок в принятом сообщении свидетельствует синдром ошибок $S(\bar{x}) = H \cdot \bar{x}^T$. Если $S(\bar{x}) = \bar{0}$, то сообщение $\bar{x}$ не содержит ошибок, если же $S(\bar{x}) \neq \bar{0}$, то сообщение $\bar{x}$ содержит ошибки. В данном случае

$$S(\bar{x}) = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

Следовательно, принятое сообщение содержит ошибки.

Задание 8. Что можно сказать о векторе-ошибке в задании 7, если ее вес равен 1? Можно назвать истинное сообщение?

Решение. Как известно, сообщение $\bar{x} = \bar{c} + \bar{e}$, где $\bar{c}$ – передаваемое кодовое слово, $\bar{e}$ – искомый вектор-ошибка. $H \cdot \bar{x}^T = H \cdot \bar{c}^T + H \cdot \bar{e}^T = \bar{0} + S(\bar{x}) = S(\bar{e})$ – сумма столбцов матрицы H, соответствующих ненулевым координатам вектора $\bar{e}$. Если вес вектора-ошибки $\bar{e}$ равен 1, то $S(\bar{e})$ равен столбцу матрицы H, который соответствует ошибочной позиции. В данном случае видим, что ошибка произошла на третьей позиции. Значит, истинное сообщение $\bar{c} = \bar{x} + \bar{e} = (1010101) + (0010000) = (1000101)$.

Задание 9. Содержит ли ошибки сообщение $\bar{x} = (101\,110\,011)$, если оно получено приёмным устройством ТКС на основе линейного кода с проверочной матрицей из задания 6. Что можно сказать о весе ошибки – вес, возможно, равен 1, или же можно утверждать, что вес ошибки больше 1?

3. Задания для самостоятельной работы

1. Взять матрицу A из заданий для самостоятельной работы ПЗ1 (по вариантам) в качестве проверочной матрицы соответствующего линейного кода C_A. Найти порождающую матрицу этого кода.

2. Найти все кодовые слова кода C_A и их веса. Составить таблицу распределения весов кода C_A. Указать минимальное расстояние кода C_A.

3. Найти минимальное расстояние кода C_A, вычисляя ранги систем столбцов проверочной матрицы A этого кода.

4. Среди кодовых слов кода C_A найти вектор $\overline{c}$ весом 5. Из этого вектора получить три вектора-сообщения: $\overline{x} = \overline{c} + (000010000)$; $\overline{y} = \overline{c} + (000110000)$; $\overline{z} = \overline{c} + (000111000)$. Найти синдромы ошибок этих трех сообщений.

5. Имея в наличии матрицу A и синдромы $S(\overline{x})$; $S(\overline{y})$; $S(\overline{z})$, высказать суждение о весах ошибок в принятых сообщениях $\overline{x}$, $\overline{y}$, $\overline{z}$. Можно ли исправить ошибки в принятых сообщениях?

Практическое занятие №3

Неприводимые полиномы. Поля Галуа и коды Хемминга

1. Необходимые теоретические сведения

Аутентичные коды Хемминга появились еще в 40-х годах XX века – в период зарождения помехоустойчивого кодирования. Задаются они достаточно просто. Произвольный код Хемминга – это линейный код C_χ длиной $n = 2^m - 1$ для некоторого целого $m > 1$, имеющий размерность $k = 2^m - m - 1$, который задается проверочной матрицей $H_\chi = (\overline{1}\ \overline{2} \ldots \overline{2^m - 1})$, где $\overline{i}$ – двоичная m – разрядная запись целого числа i в столбец. Такое задание кода называют лексикографическим. Ясно, что все столбцы матрицы H_χ – ненулевые и попарно различные. При этом $\overline{1} + \overline{2} = \overline{3}$. Следовательно, код Хемминга имеет минимальное расстояние 3 и исправляет одиночные ошибки. Предыдущее занятие позволяет нам успешно исправлять их синдромным методом.

Количество синдромов в коде Хемминга в точности равно количеству исправляемых им ошибок. По этому свойству коды Хемминга относят к разряду совершенных кодов. Еще коды Хемминга относят к классу примитивных БЧХ-кодов.

Примитивные коды Хемминга служат основой для построения других классов кодов с минимальным расстоянием $d > 3$, с интересными свойствами и более широкими декодирующими возможностями. Но для реализации таких возможностей необходимо перейти к иной, более современной интерпретации проверочных матриц кодов Хемминга – на языке полей Галуа. А для этого потребуется дальнейшее погружение в современную математику.

Термин «поле» имеет в науке различные толкования. Мы осведомлены о скалярных и векторных полях, физика поставляет нам их материальные интерпретации в виде электромагнитных, гравитационных полей и т. п.

Алгебра дает совершенно иную интерпретацию термину «поле». Здесь имеет место определение 3.1.

Определение 3.1. Полем называется любое ассоциативное и коммутатив-

ное кольцо P с 1, в котором всякий ненулевой элемент имеет обратный относительно умножения.

Данное определение для своего понимания требует усвоения комплекса понятий из теории колец. В силу определения 3.1 всякое поле не имеет делителей нуля (так как они не могут иметь обратных элементов), не имеют собственных идеалов (так как все собственные идеалы порождаются элементами, не имеющими обратных). По-существу, поле – множество, в котором можно осуществлять четыре арифметические действия: сложение, вычитание, умножение, деление.

Мы прекрасно освоились с полями рациональных чисел Q, вещественных чисел R, комплексных чисел C. Сейчас к ним добавились конечные поля Z / pZ – кольца классов вычетов по простому модулю p. Конечные поля не исчерпываются перечисленными. Все остальные конечные поля строятся факторизацией колец полиномов $Z / pZ[x]$ по тем или иным собственным максимальным идеалам. Об этом следует поговорить более подробно.

Определение 3.2. Кольцом называется непустое множество K с двумя бинарными алгебраическими операциями сложения (+) и умножения (·); относительно операции сложения K является абелевой группой, а умножение и сложение связаны законами дистрибутивности: $(a+b)c = ac + bc$; $a(b+c) = ab + ac$ для произвольных $a, b, c \in K$.

Во всяком ассоциативном (относительно умножения) нетривиальном кольце с единицей (нейтральным элементом относительно умножения) $0 \neq 1$, иначе кольцо состоит из элемента 0.

В дальнейшем будем иметь дело с ассоциативными коммутативными (относительно умножения) кольцами с единицей, содержащими более одного элемента. Наиболее популярные примеры таких колец: кольцо целых чисел Z, кольцо классов вычетов Z / nZ, кольцо полиномов $P[x]$ с коэффициентами из произвольного поля P.

Определение 3.3. Подкольцо кольца K – это подгруппа J аддитивной группы $(K,+)$, которая, в свою очередь, является кольцом относительно операций в кольце K, то есть подгруппа, замкнутая относительно умножения, определенного в кольце K. Подкольцо J коммутативного кольца K называется идеалом этого кольца, если для любого $k \in K$ и для каждого $j \in J$ произведение $jk \in J$, то есть $Jk \subseteq J$.

Среди подколец наибольший интерес представляют идеалы. В любом кольце K множества $\{0\}$ и K формально также являются идеалами кольца K. Их называют несобственными или тривиальными в отличие от остальных – собственных идеалов.Отметим основные свойства идеалов.

Теорема 3.1. Пересечение идеалов данного кольца K есть идеал этого же кольца. Произведение $J_1J_2 = \{j_1 \cdot j_2 | j_1 \in J_1;\ j_2 \in J_2\}$ идеалов J_1, J_2 кольца K есть идеал этого же кольца. Для каждого элемента a кольца K множество $< a >= aK = \{ak | k \in K\}$ есть идеал кольца K. Если в кольце K с единицей элемент a обратим относительно умножения, то $< a >= K$; если же a – ненулевой и необратимый элемент кольца K, то $< a >$ – собственный идеал кольца K. Если $a = bc$ для необратимых элементов $a, b, c \in K$, то $< a > \subset < c >$, $< a > \subset < b >$.

Приведенный в теореме 3.1 идеал $< a >$ называется главным идеалом кольца K, порожденным элементом a. Известно, что в кольце целых чисел каждый идеал является главным. То же самое справедливо и для кольца полиномов $P[x]$ с коэффициентами из произвольного поля P.

На множестве идеалов каждого кольца существует отношение частичного порядка по включению их друг в друга как множеств. Особую роль играют максимальные идеалы.

Определение 3.4. Идеал M кольца K называется максимальным, если в K не существует соответствующего собственного идеала J с условием $M \subset J$.

Теория колец даёт чёткое описание максимальных идеалов в кольце целых чисел и в кольце полиномов. В кольце целых чисел Z идеалы $<a>$ и $<b>$ связаны отношением включения $<a>\subset<b>$ тогда и только тогда, когда a делится на b; идеал $<p>$ является максимальным тогда и только тогда, когда p – простое число.

Теорема 3.2. В кольце полиномов $P[x]$ с коэффициентами из поля P идеал $J=<m(x)>$ максимален тогда и только тогда, когда порождающий его полином $m(x)$ неприводим над полем P.

Главное качество максимальных идеалов выражает следующая теорема.

Теорема 3.3. Фактор-кольцо K/M ассоциативного и коммутативного кольца K с единицей по максимальному идеалу M есть поле.

Пример 3.1. Возьмем в кольце полиномов $P[x]$ с коэффициентами из поля P произвольный собственный идеал J. Как отмечалось выше, он является главным идеалом: $J=<f(x)>$ для некоторого полинома $f(x)$ степени $n\geq 1$. Фактор-кольцо $P[x]/J$ состоит из смежных классов по модулю J. В один класс смежности по модулю J попадают те и только те полиномы, разность которых делится на $f(x)$, то есть те, которые имеют один и тот же остаток $r(x)$ от деления на $f(x)$. Отсюда следует, что фактор-кольцо $P[x]/J$ состоит из классов $\overline{r(x)}=r(x)+J=\{r(x)+f(x)q(x);\ q(x)\in P[x]\}$, где степень $r(x)$ меньше степени полинома $f(x)$.

Рассмотрим конкретный пример.

Пример 3.2. Пусть в примере 3.1 $P=Z/pZ$. В кольце $(Z/pZ)[x]$ имеется, как не трудно заметить, в точности p^n различных полиномов степени, меньшей n. Поэтому для полинома $f(x)$ степени $n\geq 1$ фактор-кольцо $(Z/pZ)[x]/<q(x)>$ конечно и состоит из p^n элементов, определяемых всевозможными полиномами степени, меньшей n. Операции сложения и умножения в этом кольце можно задать конкретно в виде таблиц.

Пример 3.3. Кольцо $F = (Z/2Z)[x]/ < x^2 + x + 1 >$ состоит из смежных классов $\bar{0}, \bar{1}, \bar{x}, \overline{x+1}$. Напишем таблицы сложения и умножения в этом кольце.

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	$\bar{x}$
$\bar{x}$	$\bar{x}$	$\overline{x+1}$	$\bar{0}$	$\bar{1}$
$\overline{x+1}$	$\overline{x+1}$	$\bar{x}$	$\bar{1}$	$\bar{0}$

$\otimes$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{1}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{x}$	$\bar{x}$	$\overline{x+1}$	$\bar{1}$
$\overline{x+1}$	$\overline{x+1}$	$\bar{1}$	$\bar{x}$

Из таблицы умножения следует, что в кольце F все ненулевые элементы обратимы относительно умножения, то есть $F^* = F \setminus \{0\}$. Следовательно, F – поле из четырёх элементов.

Итак, фактор-кольца по максимальным идеалам являются источником новых полей, в частности конечных полей. Выясним, насколько общий характер имеют эти примеры в общей теории полей.

Всякое поле имеет либо нулевую, либо ненулевую характеристику.

Определение 3.5. Если в поле P существует такое натуральное n, что равна нулю сумма n единиц (n раз складывается с самим собой 1 – нейтральный элемент относительно умножения): $1 + 1 + ... + 1 = 0$, то наименьшее n с та-

ким свойством называется характеристикой поля P и обозначается через $charP$. Если в поле P любая конечная сумма единиц отлична от нуля, то говорят, что характеристика поля P равна 0.

Теорема 3.4. Если характеристика поля отлична от нуля, то она является числом простым.

Пример 3.4. В поле $P = Z / pZ$, p – простое число, характеристика равна p. Поля Q, R, C имеют, очевидно, характеристику 0.

Определение 3.6. Поле P называется подполем поля P', если все его элементы принадлежат полю P'.

Теорема 3.5. Если подполе поля P имеет характеристику p, то и поле P имеет ту же характеристику. Все подполя поля P имеют ту же характеристику, что и поле P.

Со школьной скамьи мы привыкли к полям характеристики 0. С их точки зрения арифметика полей положительной характеристики весьма экзотична.

Теорема 3.6. Пусть P – произвольное поле положительной характеристики p. Пусть n – произвольное целое число и r – остаток от деления n на p. Тогда для каждого элемента $a \in P$ имеет место равенство $na = ra$. В частности, при $n = pq$ произведение $na = pqa = 0$. Если $p = 2$, то при $n = 2k$ произведение $na = 2ka = 0$, а при $n = 2k + 1$ произведение $na = (2k + 1)a = a$. Для любых $a, b \in P$ $(a + b)^p = a^p + b^p$; $(a - b)^p = a^p - b^p$; а для каждого целого $k \geq 1$ $(a + b)^{p^k} = a^{p^k} + b^{p^k}$; $(a - b)^{p^k} = a^{p^k} - b^{p^k}$.

На многообразии всех подполей данного поля определено отношение частичного порядка по включению, обладающее свойством транзитивности.

Определение 3.7. Минимальным, или простым, называется поле, не содержащее собственных подполей.

Теорема 3.7. Поле рациональных чисел Q – минимальное поле характеристики 0; Z / pZ – минимальное поле характеристики p. Следовательно, в

любом поле P имеется в точности одно минимальное подполе, изоморфное либо Q, либо Z/pZ в зависимости от характеристики поля P.

Определение и основные свойства векторных пространств над полем R переносятся на произвольные поля. При этом векторное пространство над конечным полем имеет свои особенности.

Теорема 3.8. Пусть $V - n-$ мерное линейное пространство над полем $F(q)$ из q элементов. Тогда V состоит из q^n векторов.

Определение 3.8. Если P является подполем поля F, то F называют расширением поля P.

Очевидно, любое расширение произвольного поля P является векторным пространством над P.

Определение 3.9. Расширение F поля P называется конечным степени n, если размерность векторного пространства F над полем P конечна и равна n. Степень расширения принято обозначать через $[F:P]$.

Теорема 3.9 (о башне расширений полей). Если поле F есть расширение поля P степени n, а поле $H-$расширение F степени m, то H есть расширение P степени $[H:P]=mn$.

Следствие. Если степень расширения $[F:P]=q-$число простое, то поле F не содержит подполей, промежуточных между F и P.

Определение 3.10. Элемент $\alpha \in F-$расширения поля P является алгебраическим над полем P, если существует полином $f(x)\in P[x]$, корнем которого является α, то есть $f(\alpha)=0$. В противном случае α называют трансцендентным над P элементом. Поле F называется алгебраическим расширением поля P, если всякий элемент из F является алгебраическим над полем P.

Теорема 3.10. Всякое конечное расширение произвольного поля P является алгебраическим над P.

Теорема 3.11. Пусть α – алгебраический над полем P элемент. Множество J_α полиномов $f(x) \in P[x]$, для которых $f(\alpha) = 0$, есть максимальный идеал кольца $P[x]$.

Следствие. Пусть $f(x)$ – неприводимый полином из $P[x]$ с корнем α из расширения F поля P. Пусть для $g(x) \in P[x]$ $g(\alpha) = 0$. Тогда $g(x)$ делится на $f(x)$.

Определение 3.11. Пусть $\alpha \in F$ – алгебраический над полем P элемент. Минимальным полиномом элемента α над полем P называется неприводимый полином $Irr(\alpha, P, x)$ в кольце $P[x]$, старший коэффициент которого равен 1, а одним из корней является элемент α.

Теорема 3.12. Пусть F – расширение поля P, пусть $\alpha \in F$ – алгебраический над P элемент с минимальным над P полиномом $Irr(\alpha, P, x)$ степени $n > 1$. Пусть $P(\alpha)$ – минимальное подполе поля F, содержащее P и α. Тогда степень расширения $[P(\alpha) : P] = n$, а поле $P(\alpha)$ имеет следующую структуру: $P(\alpha) = \{a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1}; a_i \in P, 0 \le i \le n-1\}$.

Теорема 3.13. В условиях теоремы 3.11 поле $P(\alpha)$ изоморфно факторкольцу $P[x] / < Irr(\alpha, P, x) >$.

Конечные поля были впервые введены в математическую практику в начале XIX в. гениальным французским математиком Эваристом Галуа. Поэтому конечные поля часто называют полями Галуа, а на письме обозначают через $GF(q)$ – поле Галуа из q элементов. Будем использовать и более краткое обозначение этого же поля – $F(q)$. Из вышесказанного мы уже знаем некоторые основные свойства конечных полей.

Теорема 3.14. Любое конечное поле $GF(q)$ имеет конечную характеристику $p > 0$, является конечным расширением поля Z / pZ, содержит $q = p^k$ элементов, при этом k – степень расширения $[GF(q) : Z / pZ]$.

Из теоремы Лагранжа о конечных группах следует, что все элементы мультипликативной группы $GF(q)^*$ удовлетворяют уравнению $x^{q-1}-1=0$. На самом деле имеет место теорема 3.5.

Теорема 3.15 (о существовании и единственности конечного поля). Для каждого простого числа p и для любого натурального $n \geq 1$ существует конечное поле из $q = p^n$ элементов. Это поле единственно с точностью до изоморфизма, состоит из корней уравнения $x^q - x = 0$ и только из них.

Взаимоотношения между подполями поля Галуа выражает теорема 3.16.

Теорема 3.16. Пусть $F(p^n)$ и $F(p^k)$ – конечные поля, расширения поля $Z/pZ = F(p)$, причем $1 < k < n$. Поле $F(p^k)$ является подполем $F(p^n)$ тогда и только тогда, когда k делит n. Для каждого натурального делителя d числа n существует и единственно подполе $F(p^n)$ из p^d элементов.

Ненулевые элементы поля P образуют группу относительно умножения. Ее называют мультипликативной группой поля и обозначают P^*. Теорема 3.15 характеризует ненулевые элементы полей Галуа как корни из 1. Мультипликативные свойства корней из 1 и в полях характеристики 0 и любой характеристики $p > 0$ идентичны.

Теорема 3.17. Мультипликативная группа конечного поля – циклическая.

Определение 3.12. Образующие мультипликативной группы конечного поля называют примитивными элементами этого поля.

Известно, что каждый примитивный элемент поля Галуа $F(p^n)$ является корнем неприводимого полинома степени n из кольца $F(p)[x]$. Если α – примитивный элемент поля $F(p^n)$, корень неприводимого полинома $f(x) \in Z/pZ[x]$, то и остальные корни этого полинома являются примитивными элементами поля $F(p^n)$.

Теорема 3.18. Пусть $\alpha -$ корень неприводимого полинома $f(x) \in Z/pZ[x]$ степени n, принадлежащий полю $F(p^n)$. Тогда остальными корнями полинома $f(x)$ являются элементы $\alpha^p, \alpha^{p^2}, ..., \alpha^{p^{n-1}} \in F(p^n)$.

Определение 3.13. Неприводимый полином $f(x) \in Z/pZ[x]$ степени n называется примитивным полиномом, если его корни – примитивные элементы поля Галуа $F(p^n)$.

Известно, что для каждого натурального $n > 1$ в кольце $Z/pZ[x]$ существуют примитивные полиномы степени n.

Характеризация конечных полей как множеств корней уравнений специального вида позволила доказать единственность таких полей данного порядка. Для организации вычислений в конечных полях требуется явное конструктивное задание полей Галуа, четкая методика формирования элементов этих полей. Данной цели служит теорема 3.19.

Теорема 3.19. Для каждого натурального n и фиксированного простого числа p существует единственное расширение $F(p^n)$ поля Z/pZ, состоящее из p^n элементов, оно изоморфно полю $(Z/pZ)[x]/<p(x)>$ для любого неприводимого полинома $p(x)$ степени n из кольца $Z/pZ[x]$.

Следствие. Всякое конечное поле $F(p^n)$ состоит из всевозможных полиномов степени, меньшей n, с коэффициентами из поля $F(p) = Z/pZ$. Складываются и вычитаются эти полиномы как обычно, умножаются почленно с учетом равенства $x^n = -a_{n-1}x^{n-1} - ... - a_1 x - a_0$ для фиксированного неприводимого полинома степени n из кольца $Z/pZ[x]$.

Заметим, что полиномиальное задание элементов поля $F(p^n)$ легко преобразуется в векторное: полиному $a_{n-1}x^{n-1} + ... + a_1 x + a_0$ однозначно соответствует вектор $(a_{n-1}, ..., a_1, a_0) \in F(p)_n$.

Пример 3.5. Сформируем поле $F(8) = F(2^3)$. Поскольку $2^3 - 1 = 7$ – число простое, то над полем из двух элементов все неприводимые полиномы третьей степени являются примитивными. Зафиксируем неприводимый полином степени 3, например $p(x) = x^3 + x + 1$. Обозначим через α его корень, принадлежащий $F(8)$. Тогда $\alpha^3 = \alpha + 1$ (так как характеристика поля $F(8)$ равна 2, то –1=1). Тогда $\alpha^4=\alpha^2+\alpha$, $\alpha^5=\alpha^3+\alpha^2=\alpha^2+\alpha+1$, $\alpha^6=\alpha^3+\alpha^2+\alpha=\alpha^2+1$, $\alpha^7=\alpha^3+\alpha=\alpha+\alpha+1=1$, $0=\alpha^{-\infty}$. Следовательно, поле $F(8)$ можно задать в виде таблицы из трех столбцов, в левом столбце запишем все различные степени α, в среднем – соответствующие этим степеням суммы вида $a_2\alpha^2 + a_1\alpha + a_0$, в правом – трехмерные векторы с координатами из поля $F(2)$.

Таблица элементов поля $F(8)$

$\alpha^{-\infty}$ | 0 (000)

α^1 | α (010)

α^2 | α^2 (100)

α^3 | α+1 (011)

α^4 | $\alpha^2 + \alpha$ (110)

α^5 | α^2+α+1 (111)

α^6 | α^2+1 (101)

α^7 | 1. (001)

Векторное задание полей Галуа служит для альтернативного задания кодов Хемминга – в качестве проверочной матрицы кода берется матрица $H_\chi^c = (1\alpha\alpha^2...\alpha^{n-1})$ для $n = 2^m - 1$ и примитивного элемента α поля $F(p^m)$. Фактически, такая запись матрицы есть последовательное задание элементов циклической группы $<\alpha>= GF(2^m)^*$.

Определение 3.14. Линейный код называется циклическим, если для каждого кодового вектора-слова $\overline{c} = (c_1, c_2, ..., c_n)$ кодовым словом будет и вектор

$\overline{c}' = (c_n, c_1, c_2, ..., c_{n-1})$, получаемый из вектора $\overline{c}$ циклическим сдвигом его координат.

Известно, что код с проверочной матрицей $H_\chi^c = (1, \alpha, \alpha^2, ...\alpha^{n-1})$ является циклическим. Данная матрица отличается от лексикографического задания кода лишь перестановкой столбцов.

Определение 3.15. Линейные коды, отличающиеся перестановкой отсчетов (столбцов проверочных матриц), называются эквивалентными.

Пример 3.6. На основании приведенного задания поля $F(8)$ построим проверочную матрицу кода Хемминга длиной 7.

$$H_\chi = (1\alpha ... \alpha^6) = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

2. Задания для аудиторной работы

Задание 1. Проверить на неприводимость следующие полиномы.

1.1) $x^4 + 81$, $x^3 + 13x - 14$ над полем вещественных чисел и над полем рациональных чисел.

1.2) $x^3 + x + 1$; $x^4 + x^3 + x + 1$, $x^4 + x + 1$, $x^7 + x^6 + x^2 + x + 1$, $x^7 + x^6 + 1$, $x^8 + x^7 + x^6 + x^5 + x^4 + x^2 + 1$ над полем $Z/2Z$.

1.3) $x^2 + x + 2$, $x^3 + 2x^2 + x + 1$ над полем $Z/3Z$.

Задание 2. Исследовать на примитивность над полем $Z/2Z$ неприводимые полиномы $x^3 + x^2 + 1$; $x^4 + x + 1$; $x^8 + x^7 + x^6 + x^5 + x^4 + x^2 + 1$.

Решение. Неприводимый полином $f(x)$ степени $n > 1$ примитивен, если его корень α является примитивным элементом, то есть образующим циклической группы $GF(p^n)^*$. В первых двух случаях это проверяется непосредственно, по аналогии с решением примера 3.5. В третьем случае $GF(p^n)^* = GF(2^8)^*$ и имеет порядок 255. Поэтому здесь следует воспользоваться программными средствами. Можно также воспользоваться следующим признаком примитивности элемента в циклической группе.

Пусть G – циклическая группа порядка $n = p_1^{r_1} \cdot p_2^{r_2} \cdot \ldots \cdot p_s^{r_s}$. Если элемент $b \in G$ обладает свойствами: для каждого целого $i, 1 \le i \le s,$ и целого $t_i = n / p_i$ степень $b^{t_i} \neq 1$, то $< b >= G$ – элемент b является образующей группы G .

В данном случае $n = 255 = 3 \cdot 5 \cdot 17$, $t_1 = 255/3 = 85$; $t_2 = 255/5 = 51$; $t_3 = 255/17 = 15$. Величина α^{85} есть результат подстановки α в остаток от деления x^{85} на $f(x)$. Вычисления показывают, что $\alpha^{85} = \alpha^6 + \alpha^4 + \alpha^3 + \alpha^2 + 1$. Аналогично, $\alpha^{51} = \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha$; $\alpha^{15} = \alpha^4 + \alpha^2$.

Проведенные вычисления показывают, что неприводимый полином $x^8 + x^7 + x^6 + x^5 + x^4 + x^2 + 1$ является примитивным.

Задание 3. Исследовать на примитивность над полем $Z/3Z$ неприводимые полиномы $x^2 + x + 2.$

Задание 4. На основе полинома $x^3 + x^2 + 1$ построить полиномиальное, мультипликативное и двоичное векторное задание поля Галуа из 8 элементов.

Задание 5. На основе полинома $x^4 + x + 1$ построить полиномиальное, мультипликативное и двоичное векторное задание поля Галуа из 16 элементов.

Задание 6. На основе полинома $x^2 + x + 2$ построить полиномиальное, мультипликативное и двоичное векторное задание поля Галуа из 9 элементов.

Задание 7. Сформировать матрицу $H = (\alpha^i)$ $(7, 4)$ – кода Хемминга, где α – корень полинома $x^3 + x^2 + 1$. Найти порождающую матрицу этого кода.

Задание 8. Содержит ли ошибки сообщение $\bar{x} = (1010101)$, принятое $(7, 4)$ – кодом Хемминга.

Задание 9. Указать ошибку в сообщении $\bar{x} = (1010101)$ и устранить её. Выписать исправленное сообщение.

Задание 10. Сформировать матрицу $H = (\alpha^i)$ $(15, 11)$ – кода Хемминга, где α – корень полинома $x^4 + x + 1$. Содержит ли ошибки сообщение

$\bar{x} = (101\,111\,010\,111\,001)$, принятое этим кодом. Указать ошибку в сообщении $\bar{x} = (1010101)$ и устранить её. Выписать исправленное сообщение.

Задание 11. Сформировать матрицу $H_\chi^c = (\beta^i)$ непримитивного $(17, 9)$ – кода Хемминга, где $\beta = \alpha^{15}$ и α – корень полинома $x^8 + x^7 + x^6 + x^5 + x^4 + x^2 + 1$.

Решение.

$$H_\chi^c = (\beta^i) = (1\beta ... \beta^{16}) = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

3. Задания для самостоятельной работы

Задание 1. Доказать неприводимость полинома $p(x)$ над $Z / 2Z$ (по вариантам).

Задание 2. Проверить полином $p(x)$ на примитивность.

Задание 3. С помощью корня α полинома $p(x)$ построить проверочную матрицу $H_\chi^c = (\beta^i)$ не примитивного (17, 9) – кода Хемминга.

Задание 4. С помощью построенной матрицы H_χ^c найти минимальное расстояние (17, 9) – кода Хемминга.

Вариант 1. $p(x) = x^8 + x^6 + x^5 + x^4 + 1$.

Вариант 2. $p(x) = x^8 + x^7 + x^5 + x^3 + 1$.

Вариант 3. $p(x) = x^8 + x^6 + x^5 + x^3 + 1$.

Вариант 4. $p(x) = x^8 + x^6 + x^5 + x^2 + 1$.

Вариант 5. $p(x) = x^8 + x^7 + x^3 + x^2 + 1$.

Вариант 6. $p(x) = x^8 + x^6 + x^3 + x^2 + 1$.

Вариант 7. $p(x) = x^8 + x^5 + x^3 + x^2 + 1$.

Вариант 8. $p(x) = x^8 + x^4 + x^3 + x^2 + 1$.

Вариант 9. $p(x) = x^8 + x^7 + x^6 + x + 1$.

Вариант 10. $p(x) = x^8 + x^6 + x^5 + x + 1$.

Вариант 11. $p(x) = x^8 + x^5 + x^3 + x + 1$.

Вариант 12. $p(x) = x^8 + x^7 + x^2 + x + 1$.

Вариант 13. $p(x) = x^8 + x^7 + x^6 + x^5 + x^2 + x + 1$.

Вариант 14. $p(x) = x^8 + x^7 + x^6 + x^3 + x^2 + x + 1$.

Вариант 15. $p(x) = x^8 + x^6 + x^4 + x^3 + x^2 + x + 1$.

Практическое занятие №4

Коды Боуза-Чоудхури-Хоквингема, исправляющие двойные ошибки

1. Необходимые теоретические сведения

Циклическое задание кодов Хемминга с помощью проверочной матрицы H_χ^c обеспечило возможности различных преобразований этих матриц. Подобные эксперименты быстро привели к новым кодам с большим минимальным расстоянием и широким декодирующим потенциалом. Первыми и наиболее удачными из них оказались примитивные коды Боуза-Чоудхури-Хоквингема (БЧХ-коды) с минимальным расстоянием 5. Эти коды имеют длину $n = 2^m - 1$, размерность $k = n - 2m$, где m – степень поля $GF(2^m)$ – поля определения кода Хемминга такой же длины, поля определения и данного БЧХ-кода. Будем данные коды обозначать через C_5. Проверочная матрица данного кода имеет вид:

$$H_{BCH} = H = \begin{pmatrix} 1 & \alpha & \dots & \alpha^{n-1} \\ 1 & \alpha^3 & \dots & \alpha^{3(n-1)} \end{pmatrix} = (\alpha^i, \alpha^{3i})^T . \qquad (4.1)$$

Данный код корректирует одиночные и двойные ошибки. Синдром одиночной ошибки совпадает с одним из столбцов проверочной матрицы, который четко указывает на ошибочное место в принятом векторе-сообщении. Для определения координат двойной ошибки следует решать подходящее квадратное уравнение. Напомним некоторые факты о них.

Прежде всего отметим, что стандартные формулы корней квадратного уравнения в полях характеристики 2 не применимы, так как деление на 2 здесь равносильно делению на 0. Однако всякое квадратное уравнение $ax^2 + bx + c = 0$ с коэффициентами $a, b, c \in GF(2^m)$ приводится к каноническому виду, то есть к виду $x^2 + x + \gamma = 0$ для некоторого $\gamma \in GF(2^m)$. Если x_0 – один из корней уравнения $x^2 + x + \gamma = 0,$ то другим корнем этого уравнения является $x_0 + 1 \in GF(2^m)$.

Теорема 4.1 (Берлекемп, Рамсей, Соломон, 1967). Уравнение $x^2 + x + \gamma = 0$ с элементом $\gamma \in GF(2^m)$ имеет корни в этом же поле тогда и только тогда, когда след $Tr\gamma = 0$.

Напомним, что след в полях Галуа $GF(2^m)$ вычисляется по формуле $Trc = c + c^2 + ... + c^{2^{m-1}}$. При этом правильно вычисленный след принимает только одно из двух значений: 0 или 1.

Формула корней квадратного уравнения в полях Галуа характеристики 2 выводится с помощью нормального базиса в векторном пространстве $GF(2^m)$ над полем $GF(2)$. Напомним, что нормальный базис имеет вид: $\beta, \beta^2, ..., \beta^{2^{m-1}}$ для некоторого $\beta \in GF(2^m)$. Дэвенпорт в 1968 г. доказал, что всякое конечное расширение поля Галуа обладает нормальным базисом. Несложное рассуждение показывает, что элемент β из нормального базиса должен быть примитивным элементом поля и иметь след, равный 1. Поэтому для произвольного $\gamma \in GF(2^m)$, заданного в нормальном базисе равенством $\beta = d_0\gamma + d_1\gamma^2 + ... + d_{n-1}\gamma^{2^{n-1}}$, где $d_i \in GF(2)$, след $Tr\beta = d_0 + d_1 + ... + d_{n-1}$. Формула квадратных корней выглядит достаточно экзотично.

Теорема 4.2 (Чэнь, 1982). Пусть у квадратного уравнения $x^2 + x + \gamma = 0$ с элементом $\gamma \in GF(2^m)$ след $Tr\gamma = 0$. Пусть $\beta, \beta^2, ..., \beta^{2^{m-1}}$ – нормальный базис поля $GF(2^m)$ над полем $GF(2)$. Пусть $\gamma = d_0\beta + d_1\beta^2 + ... + d_{n-1}\beta^{2^{n-1}}$ – разложение γ по нормальному базису для $d_i \in GF(2)$. Тогда $x_0 = d_1\beta^2 + (d_1 + d_2)\beta^4 + ... + (d_1 + d_2 + ...d_{n-1})\beta^{2^{n-1}}$ является корнем уравнения $x^2 + x + \gamma = 0$.

Пример 4.1. Решим квадратное уравнение $x^2 + (\alpha^4 + \alpha^3 + \alpha^2 + \alpha)x + (\alpha^2 + 1) = 0$ над полем $GF(2^5)$ с примитивным элементом α – корнем полинома $x^5 + x^2 + 1$ по формулам Чэня из теоремы 4.2. Для этого приведём уравнение к каноническо-

му виду с помощью замены $x=(\alpha^4+\alpha^3+\alpha^2+\alpha)z=\alpha^{24}z$. Получим уравнение $z^2+z+D=0$ с $D=\alpha^{19}=\alpha^2+\alpha$. При этом след $TrD=\alpha^{19}+\alpha^7+\alpha^{14}+\alpha^{28}+\alpha^{25}=0$.

Выясним, образуют ли нормальный базис в поле $GF(2^5)$ степени примитивного элемента $\alpha,\alpha^2,\alpha^4,\alpha^8=\alpha^3+\alpha^2+1,\alpha^{16}=\alpha^4+\alpha^3+\alpha+1$. Ранг данной системы векторов над полем $GF(2)$ равен рангу матрицы $M=\begin{pmatrix}0&0&1&0&1\\0&0&0&1&1\\0&1&0&1&0\\1&0&0&0&1\\0&0&0&1&1\end{pmatrix}$ из координат этих векторов в базисе $\alpha^4,\alpha^3,\alpha^2,\alpha,1$. В этой матрице две одинаковые строки – вторая и пятая, поэтому перечисленные элементы базиса не образуют. Аналогичная проверка показывает, что нормальным базисом здесь является система $\gamma=\alpha^3,\gamma^2=\alpha^6=\alpha^3+\alpha,\gamma^4=\alpha^{12}=\alpha^3+\alpha^2+\alpha,\gamma^8=\alpha^{24}=\alpha^4+\alpha^3+\alpha^2+\alpha,$

$\gamma^{16}=\alpha^{48}=\alpha^{17}=\alpha^4+\alpha+1$. Действительно, матрица $A=\begin{pmatrix}0&0&0&1&1\\1&1&1&1&0\\0&0&1&1&0\\0&1&1&1&1\\0&0&0&0&1\end{pmatrix}$ из координат этих векторов перестановкой строк преобразуется к треугольному виду $\begin{pmatrix}1&1&1&1&0\\0&1&1&1&1\\0&0&1&1&0\\0&0&0&1&1\\0&0&0&0&1\end{pmatrix}$ и, следовательно, имеет ранг 5. Непосредственные вычисления позволяют найти обратную матрицу: $A^{-1}=\begin{pmatrix}0&1&0&1&1\\0&0&1&1&1\\1&0&1&0&1\\1&0&0&0&1\\0&0&0&0&1\end{pmatrix}$.

Как известно из линейной алгебры, координаты d_0,d_1,d_2,d_3,d_4 вектора $D=\alpha^2+\alpha$ в найденном нормальном базисе вычисляются с помощью матрицы

$$A^{-1}:\begin{pmatrix} d_0 \\ d_1 \\ d_2 \\ d_3 \\ d_4 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}.$$

Найдём корни полученного уравнения $z^2 + z + D = 0$ по формулам из теоремы 4.2: $z_0 = 0, z_1 = z_0 + d_1 = 0, z_2 = z_1 + d_2 = 1, z_3 = z_2 + d_3 = 1, z_4 = z_3 + d_4 = 1$. Следовательно, первый корень $z' = \gamma^4 + \gamma^8 + \gamma^{16} = (\alpha^3 + \alpha^2 + \alpha) + (\alpha^4 + \alpha^3 + \alpha^2 + \alpha) + (\alpha^4 + \alpha + 1) = \alpha + 1$, а второй корень $z'' = z' + 1 = \alpha$. Тогда корни исходного уравнения $x_1 = \alpha^{24} \cdot z' = \alpha^{24} \cdot \alpha^{18} = \alpha^{11}; x_2 = \alpha^{24} \cdot z'' = \alpha^{25}.$

Как видим, применение формул Чэня для решения квадратных уравнений требует достаточно много промежуточных громоздких вычислений. Сам автор этих формул предложил решать квадратные уравнения простым перебором – последовательной подстановкой элементов поля в уравнение до получения нуля. Метод этот называют в литературе методом Чэня.

Вернемся к двойным ошибкам в БЧХ-коде C_5. Пусть при передаче вектора-сообщения $\bar{c}$ в цифровой системе связи с данным кодом C_5 на сообщение наложился вектор-ошибка $\bar{e} = (i, j)$ весом 2 с ненулевыми координатами на неизвестных позициях i и j. Это означает, что приёмное 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} являются неизвестными элементами поля Галуа $GF(2^m)$. Обозначим их через x и y соответственно. Эти величины – решения системы уравнений

$$\begin{cases} x + y = s_1; \\ x^3 + y^3 = s_2. \end{cases} \qquad (4.2)$$

Преобразуем второе уравнение системы (4.2):

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

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, найдём $x = \alpha^{i-1}$, $y = \alpha^{j-1}$, а с ними и вектор-ошибку $\bar{e} = (i, j)$.

Пример 4.2. 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. 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: $H \cdot (\bar{c}^T) = \bar{0}$. Если $\bar{S} = H(\bar{x}^T) \neq \bar{0}$, то сообщение $\bar{x}$ явно содержит ошибки. В данном случае $\bar{S} = (s_1, s_2)^T$, 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 $\bar{x}$ содержит ошибки. Данный код исправляет двойные ошибки. Для нахождения такой ошибки имеем следующую конкретную систему $(*)$: $\begin{cases} x + y = \alpha^{11}, \\ x^3 + y^3 = \alpha. \end{cases}$

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 $t_1 = \alpha, \quad t_2 = \alpha + 1 = \alpha^4.$ Тогда $x = \alpha^{11}\alpha = \alpha^{12}; \quad y = \alpha^{12} + \alpha^{11} = \alpha^0 = 1.$ Таким образом, ошибочными в принятом сообщении являются 1-я и 13-я позиции и правильным является сообщение $\overline{c}_0 = (011011110110001).$

К семейству БЧХ-кодов примыкают и реверсивные коды C_R. Они (те же параметры n и k, что и БЧХ-коды C_5) задаются проверочной матрицей $H_R = (\alpha^i, \alpha^{-i})^T$, где $1 \le i \le n-1,$ $n = 2^m - 1,$ $\alpha -$ примитивный элемент поля Галуа $GF(2^m)$. Реверсивные коды имеют $d = 3$ при четных m и $d = 5$ при нечетных значениях m.

Декодирование двойных ошибок реверсивным кодом аналогично той же процедуре в БЧХ-кодах. Только вместо системы (4.2) здесь появляется система

$$\begin{cases} x + y = s_1; \\ x^{-1} + y^{-1} = s_2. \end{cases} \qquad (4.3)$$

Второе уравнение системы (4.3) легко преобразуется к виду $xy = s_1 / s_2$. Дальнейший переход к квадратному уравнению очевиден.

2. Задания для аудиторной работы

Задание 1. Сформировать матрицу $H = (\alpha^i, \alpha^{3i})^T$ БЧХ-кода длиной 7, где $\alpha -$ корень полинома $x^3 + x + 1.$ Найти порождающую матрицу этого кода.

Решение. Проверочная матрица кода имеет вид:

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

Для нахождения порождающей матрицы кода следует вспомнить решение первого задания в ПЗ№2.

Задание 2. ТКС функционирует на основе БЧХ-кода из задания 1. Его приёмное устройство приняло сообщение $\bar{x} = (1101101)$. Содержатся ли ошибки в данном сообщении?

Решение. Синдром ошибок принятого сообщения $S(\bar{x}) = H \cdot \bar{x}^T = (011111) \neq \bar{0}$. Следовательно, принятое сообщение содержит ошибки.

Задание 3. Найти вектор ошибок в принятом сообщении (задание 2) и указать правильное сообщение.

Решение. В силу структуры проверочной матрицы данного кода синдром $S(\bar{x})$ состоит из двух компонент: $S(\bar{x}) = (s_1, s_2) = (\alpha^3, \alpha^5)$. Синдром не совпадает ни с одним из столбцов матрицы H. Поэтому сообщение содержит ошибку кратности, большей 1. Предположим, что в процессе передачи произошла двойная ошибка с неизвестными локаторами x и y. Тогда $\begin{cases} x + y = s_1; \\ x^3 + y^3 = s_2. \end{cases}$

В данном случае эта система имеет вид: $\begin{cases} x + y = \alpha^3; \\ x^3 + y^3 = \alpha^5. \end{cases}$ Сведём систему к квадратному уравнению. $x^3 + y^3 = (x + y)(x^2 + y^2 - xy) = \alpha^5$. С учётом первого уравнения имеем $\alpha^3(\alpha^6 - xy) = \alpha^5$ или $xy = \alpha^6 + \alpha^2 = 1$. Согласно теореме Виета, x и y являются корнями квадратного уравнения $t^2 + \alpha^3 t + 1 = 0$. Приведём уравнение к каноническому виду заменой $t = \alpha^3 z$.

Получим уравнение $z^2 + z + \alpha = 0.$ Критерий разрешимости квадратных уравнений в каноническом виде $z^2 + z + \gamma = 0$ гласит, что такое уравнение имеет решения тогда и только тогда, когда $Tr\gamma = 0.$ В данном случае $Tr\alpha = \alpha + \alpha^2 + \alpha^4 = 0.$ Таким образом, уравнение $z^2 + z + \alpha = 0$ имеет корни в поле Галуа $GF(8).$ Найдём эти корни по формулам Чэня. Чтобы ими воспользоваться, необходимо найти нормальный базис поля $GF(8).$ В данном случае нормальный базис имеет вид $\gamma, \gamma^2, \gamma^4$ для некоторого элемента поля $GF(8).$ При этом след $Tr\gamma = 1.$ Попробуем взять $\gamma = \alpha^3.$ $Tr(\alpha^3) = \alpha^3 + \alpha^6 + \alpha^{12} = (\alpha + 1) + (\alpha^2 + 1) + (\alpha^2 + \alpha + 1) = 1.$ Элементы $\gamma = \alpha^3,$ $\gamma^2 = \alpha^6, \gamma^4 = \alpha^{12} = \alpha^5$ линейно независимы над $Z/2Z.$ Ведь матрица из координат этих элементов как векторов трёхмерного пространства над полем $Z/2Z$ имеет определитель $\begin{vmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{vmatrix} = 1.$ Найдём разложение α по нормальному базису, то есть такие $d_1, d_2, d_3 \in Z/2Z,$ что $d_1\alpha^3 + d_2\alpha^6 + d_3\alpha^5 = \alpha.$ Это равенство в координатной форме приводит к следующей СЛАУ: $\begin{cases} d_2 + d_3 = 0; \\ d_1 + d_3 = 1; \\ d_1 + d_2 + d_3 = 0. \end{cases}$ Легко видеть, что система имеет единственное решение: $d_1 = 0, d_2 = 1, d_3 = 1.$ Согласно формулам Чэня, уравнение $z^2 + z + \alpha = 0$ имеет корни $z_1 = d_2\gamma^2 + (d_2 + d_3)\gamma^4 = \alpha^6; z_2 = z_1 + 1 = \alpha^2.$ Тогда $x = \alpha^3 z_1 = \alpha^2;$ $y = \alpha^3 z_2 = \alpha^5.$

Найденные локаторы однозначно указывают, что в принятом сообщении произошла двойная ошибка на третьей и шестой позициях и правильное сообщение имеет вид $\bar{c} = (1111111).$

Задание 4. Сформировать матрицу $H = (\alpha^i, \alpha^{3i})^T$ кода БЧХ длиной 15, где α – корень полинома $x^4 + x + 1$.

Задание 5. ТКС функционирует на основе БЧХ-кода из задания 4. Его приёмное устройство приняло сообщение $\overline{x} = (111011110110101)$. Выяснить наличие ошибок в этом сообщении.

Решение. 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 $\overline{c} \in C$ (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.

Задание 6. Найти вектор ошибок в принятом сообщении (задание 2) и указать правильное сообщение.

Данный код исправляет двойные ошибки. Для нахождения такой ошибки имеем следующую конкретную систему

$$\begin{cases} x + y = \alpha^{11}, \\ x^3 + y^3 = \alpha. \end{cases} \tag{4.4}$$

Система (4.4) 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 $t_1 = \alpha, \quad t_2 = \alpha + 1 = \alpha^4$. Тогда $x = \alpha^{11}\alpha = \alpha^{12}; \quad y = \alpha^{12} + \alpha^{11} = \alpha^0 = 1$. Таким образом, ошибочными в принятом сообщении являются 1-я и 13-я позиции и правильным является сообщение $\overline{c}_0 = (011011110110001)$.

3. Задания для самостоятельной работы

Задание 1. Проверить на неприводимость и примитивность заданный полином над полем $Z / 2Z$ (по вариантам).

Задание 2. Сформировать с помощью полинома из задания 1 поле Галуа из 32-х элементов.

Задание 3. Сформировать проверочную матрицу (31, 21)-БЧХ-кода (варианты 1–6, 13 –15) или реверсивного кода (варианты 7 – 12) на основании поля Галуа из задания 2.

Задание 4. Выяснить наличие ошибок в принятом сообщении (по вариантам) в ТКС с БЧХ-кодом из задания 3.

Задание 5. Методом квадратных уравнений исправить ошибки в принятом сообщении из задания 4.

Вариант 1: $p(x) = x^5 + x^2 + 1.$

Вариант 2: $p(x) = x^5 + x^3 + 1.$

Вариант 3: $p(x) = x^5 + x^3 + x^2 + x + 1.$

Вариант 4: $p(x) = x^5 + x^4 + x^2 + x + 1.$

Вариант 5: $p(x) = x^5 + x^4 + x^3 + x + 1.$

Вариант 6: $p(x) = x^5 + x^4 + x^3 + x^2 + 1.$

Вариант 7: $p(x) = x^5 + x^2 + 1.$

Вариант 8: $p(x) = x^5 + x^3 + 1.$

Вариант 9: $p(x) = x^5 + x^3 + x^2 + x + 1.$

Вариант 10: $p(x) = x^5 + x^4 + x^2 + x + 1.$

Вариант 11: $p(x) = x^5 + x^4 + x^3 + x + 1.$

Вариант 12: $p(x) = x^5 + x^4 + x^3 + x^2 + 1.$

Вариант 13: $p(x) = x^5 + x^2 + 1.$

Вариант 14: $p(x) = x^5 + x^3 + 1.$

Вариант 15: $p(x) = x^5 + x^3 + x^2 + x + 1.$

Задание 6.

Вариант 1: $\bar{x} = (001\,011\,011\,100\,000\,100\,000\,000\,100\,000\,1).$

Вариант 2: $\bar{x} = (110\,110\,100\,100\,100\,000\,000\,000\,000\,100\,1).$

Вариант 3: $\bar{x} = (101\,101\,101\,100\,000\,000\,100\,000\,100\,100\,0).$

Вариант 4: $\bar{x} = (111\,011\,011\,100\,000\,001\,000\,100\,000\,000\,1).$

Вариант 5: $\bar{x} = (110\,110\,111\,100\,000\,000\,001\,100\,000\,000\,1).$

Вариант 6: $\bar{x} = (110\,110\,110\,100\,010\,000\,000\,001\,000\,100\,0).$

Вариант 7: $\bar{x} = (011\,010\,110\,100\,000100\,001\,000\,000\,00\,1).$

Вариант 8: $\bar{x} = (011\,010\,110\,100\,000\,000\,010\,000\,000\,010\,1).$

Вариант 9: $\bar{x} = (101\,111\,101\,100\,010\,001\,000\,000\,000\,000\,1).$

Вариант 10: $\bar{x} = (001\,110\,001\,000\,000\,010\,000\,000\,100\,001\,0).$

Вариант 11: $\bar{x} = (001\,010\,001\,000\,000\,010\,000\,000\,100\,101\,0).$

Вариант 12: $\bar{x} = (001\,110\,001\,010\,000\,010\,010\,000\,100\,001\,0).$

Вариант 13: $\bar{x} = (001\,100\,001\,000\,110\,010\,000\,000\,100\,001\,0).$

Вариант 14: $\bar{x} = (000\,110\,001\,000\,001\,010\,000\,000\,100\,001\,0).$

Вариант 15: $\bar{x} = (001\,110\,001\,000\,000\,010\,110\,000\,100\,001\,0).$

Практическое занятие №5

Синдромное декодирование произвольных БЧХ-кодов

1. Необходимые теоретические сведения

Для всякого натурального n, делящего $q^m - 1$, в поле Галуа $GF(q^m)$ найдется элемент β порядка n (например, $\beta = \alpha^c$ для примитивного элемента $\alpha \in GF(q^m)$ и $c = (q^m - 1)/n$). Зафиксируем целые числа $b > 0$, не делящиеся на n, и $\delta > 1$, натуральное n, делящее или равное $q^m - 1$, но не делящее $q^s - 1$ для всех целых s, $0 < s < m$. При этом значение δ должно быть таким, что выполняется неравенство $m(\delta - 1) < n$.

Определение 5.1. Линейный код C длиной n с проверочной матрицей

$$H = \left[\begin{array}{cccc} 1 & \beta^b & \beta^{2b} & \beta^{(n-1)b} \\ 1 & \beta^{b+1} & \beta^{2(b+1)} & \beta^{(n-1)(b+1)} \\ \hline 1 & \beta^{b+\delta-2} & \beta^{2(b+\delta-2)} & \beta^{(n-1)(b+\delta-2)} \end{array}\right] = [\beta^{bi}, \beta^{(b+1)i}, \ldots, \beta^{(b+\delta-2)i}]^T \quad (5.1)$$

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 не примитивным, если $n < q^m - 1$.

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 нетривиально и, следовательно, код C существует, являясь линейным пространством размерности, не меньшей, чем $n - m(\delta - 1)$.

Теорема 5.1. 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.

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 5.2. 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 и непримитивного полинома показателя n и степени m над полем $GF(q)$.

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 5.3.

Теорема 5.3. 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 $rank[\beta^{it}, \beta^{itq}] = rank[\beta^{it}]$.

Заметим, что 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 минимума временных затрат. В силу сказанного, матрица H должна быть мини-

мально 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.

Указанная теоремой 5.3 ситуация чаще всего возникает при $b = 1$ (тогда код называют БЧХ-кодом в узком смысле). 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:

$$H = (\beta^i, \beta^{3i}, ..., \beta^{(2t-1)i})^{\mathrm{T}},\ 0 \le i \le n-1. \qquad (5.2)$$

Истинная размерность данного БЧХ-кода C_{2t+1} есть величина $k \le n - tm,$ что существенно больше конструктивной размерности $n - m(\delta - 1)$. Именно такие коды получили наибольшее применение, особенно когда $n = q^m - 1$, то есть при $\beta = \alpha$.

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

$$H = (\alpha^i, \alpha^{3i}, ..., \alpha^{(2t-1)i})^T, \qquad (5.3)$$

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 ко-

да через C_{2t+1}. Как уже отмечалось, реальное кодовое расстояние $d \geq \delta$.

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:

$$\begin{gathered} x_1 + x_2 + ... + x_t = s_1, \\ x_1^3 + x_2^3 + ... + x_t^3 = s_2, \\ ..... \\ x_1^{2t-1} + x_2^{2t-1} + ... + x_t^{2t-1} = s_t. \end{gathered} \tag{5.4}$$

Если систему (5.4) 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 (5.4) легко сводится к квадратному уравнению и решается. При $t \geq 3$ следует воспользоваться теорией симметрических полиномов. Дело в том, что левые части уравнений системы (5.4) можно рассматривать как симметрические многочлены от t неизвестных. Симметрические многочлены – это полиномы, не меняющиеся при любой перестановке местами переменных, то есть 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 5.2. Следующие n симметрических многочленов от n неизвестных называются элементарными симметрическими многочленами:

$$\sigma_1 = x_1 + x_2 + ... + x_n,$$

$$\sigma_2 = x_1x_2 + x_1x_3 + ... + x_{n-1}x_n,$$

.....

$$\sigma_{n-1} = x_1x_2 \cdot ... \cdot x_{n-1} + x_1x_2 \cdot ... \cdot x_{n-2}x_n + ... + x_2x_3 \cdot ... \cdot x_n,$$

$$\sigma_n = x_1x_2 \cdot ... \cdot x_n.$$

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

$$f_k - f_{k-1}\sigma_1 + f_{k-2}\sigma_2 - ... + (-1)^{k-1} f_1\sigma_{k-1} + (-1)^k k\sigma_k = 0, \quad k \le n, \quad (5.5)$$

$$f_k - f_{k-1}\sigma_1 + f_{k-2}\sigma_2 - ... + (-1)^n f_{k-n}\sigma_n = 0, \quad k > n. \quad (5.6)$$

Эти формулы позволяют последовательно выражать степенные суммы через элементарные симметрические полиномы. Очевидно, $f_1 = \sigma_1$. Формула (5.5) 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 (5.5) 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 (5.5), в противном случае – формулу (5.6).

Предположим, что мы применяем БЧХ-код C_7, исправляющий тройные ошибки, то есть код с параметром $t = 3$. Тогда для исправления тройных ошибок необходимо решать следующий более простой аналог системы (5.4):

$$\begin{cases} x_1 + x_2 + x_3 = s_1, \\ x_1^3 + x_2^3 + x_3^3 = s_2, \\ x_1^5 + x_2^5 + x_3^5 = s_3. \end{cases} \quad (5.7)$$

В данном случае для выражения f_5 через элементарные симметрические многочлены следует воспользоваться формулой (5.6). В таком слу-

чае $f_5 = f_4\sigma_1 + f_3\sigma_2 + f_2\sigma_3 = \sigma_1^5 + (\sigma_1^3 + \sigma_1\sigma_2 + \sigma_2)\sigma_2 + \sigma_1^2\sigma_3$. И так далее.

Посмотрим, однако, на соотношения (5.5) – (5.6) в противоположном направлении – как на соотношения для определения элементарных симметрических полиномов. Фактически, уравнения (5.4) и (5.7) определяют значения степенных сумм f_k. Тогда уравнения (5.6) – (5.7) определяют систему линейных уравнений для нахождения σ_k. Так для БЧХ-кода C_7 эта система линейных уравнений имеет вид:

$$\begin{cases} \sigma_1 = f_1 = s_1, \\ f_2\sigma_1 + f_1\sigma_2 + \sigma_3 = f_3 = s_2, \\ f_4\sigma_1 + f_3\sigma_2 + f_2\sigma_3 = f_5 = s_3, \end{cases} \quad \text{или} \quad \begin{cases} \sigma_1 = s_1, \\ s_1^2\sigma_1 + s_1\sigma_2 + \sigma_3 = s_2, \\ s_1^4\sigma_1 + s_2\sigma_2 + s_1^2\sigma_3 = s_3. \end{cases} \tag{5.8}$$

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 классической теореме о связи корней алгебраических уравнений с коэффициентами этих уравнений.

Теорема Виета. Пусть у уравнения

$$x^t + \sigma_1^0 x^{t-1} + ... + \sigma_t^0 = 0 \tag{5.9}$$

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

$$\begin{aligned} &x_1 + x_2 + ... + x_t = -\sigma_1^0, \\ &x_1x_2 + x_1x_3 + ... + x_{t-1}x_t = \sigma_2^0, \\ &\qquad\qquad ..... \\ &x_1x_2 \cdot ... \cdot x_{t-1} + x_1x_2 \cdot ... \cdot x_{n-2}x_t + ... + x_2x_3 \cdot ... \cdot x_t = (-1)^{t-1}\sigma_{t-1}^0, \\ &x_1x_2 \cdot ... \cdot x_t = (-1)^t\sigma_t^0. \end{aligned} \tag{5.10}$$

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 (5.10) составляем уравнение (5.9) , называемое уравнением локаторов ошибок. Алгебраические уравнения над полями Галуа $GF(2^m)$ проще всего решать методом Чэня, то есть 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 5.1. В системе связи, построенной на основе примитивного БЧХ-кода C_7 длиной 63 с проверочной матрицей $H = (\alpha^i, \alpha^{3i}, \alpha^{5i})^T$, $0 \le i \le 62$, 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 (5.8) 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 (5.9): $x^3 + \alpha^{21}x^2 + \alpha^{41}x + \alpha^{60} = 0$. Кропотливые вычисления метода 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-й, 21-й и 31-й позициях.

В заключении заметим, что представленный синдромный метод декодирования не лишён недостатков. В его реализации имеются такие громоздкие этапы как нахождение коэффициентов уравнения (5.9) и его решение перебор-

ным методом Чэня. Обойти все эти сложности синдромного метода позволяет теория норм синдромов.

2. Задания для аудиторной работы

Задание 1. В (15,3)-БЧХ-коде C_7 с проверочной матрицей $H=(\alpha^i, \alpha^{3i}, \alpha^{5i})^T$, где $0 \le i \le 14, \alpha$ – корень полинома $p(x)=x^4+x^3+1$, принято сообщение $\bar{x}=(11011\,00101\,01101)$ с синдромом ошибок $S(\bar{x})=(\alpha, \alpha^7, \alpha^5)$. Найти вектор ошибок в этом сообщении, если известно, что произошла ошибка весом 3.

Решение. Тройная ошибка в сообщении $\bar{x}$ произошла на неизвестных позициях $i, j, k, 1 \le i < j < k \le 15$. В подматрице $\tilde{H}=(\alpha^i)$ матрицы $H=(\alpha^i, \alpha^{3i}, \alpha^{5i})^T$ позициям i, j, k соответствуют столбцы $\alpha^{i-1}=x, \alpha^{j-1}=y, \alpha^{k-1}=z$. Эти столбцы образно называют локаторами ошибочных позиций. Их рассматриваем как элементы поля Галуа $GF(2^4)$, задаваемые с помощью полинома $p(x)=x^4+x^3+1$. Синдром $S(\bar{x})=(\alpha, \alpha^7, \alpha^5)$ получается двоичным сложением столбцов матрицы $H=(\alpha^i, \alpha^{3i}, \alpha^{5i})^T$ с номерами i, j, k. Каждый $\bar{i}$-й столбец матрицы H состоит из трёх частей, интерпретируемых как элементы x, x^3, x^5 поля $GF(2^4)$. Поэтому для определения истинных значений позиций i, j, k искомой тройной ошибки мы с помощью синдрома $S(\bar{x})=(\alpha, \alpha^7, \alpha^5)$ получаем следующую систему уравнений:

$$\begin{cases} x+y+z=s_1=\alpha; \\ x^3+y^3+z^3=s_2=\alpha^7; \\ x^5+y^5+z^5=s_3=\alpha^5. \end{cases} \qquad (*)$$

Левые части уравнений системы $(*)$ есть симметрические степенные полиномы f_1, f_3, f_5 от трёх переменных x, y, z. Здесь $f_k=x^k+y^k+z^k$. У

нас, в условиях двоичной арифметики, $f_2 = f_1^2;\ f_4 = f_1^4$. В теориях симметрических полиномов существуют формулы, принадлежащие перу великого Ньютона, которые связывают степенные симметрические полиномы с элементарными симметрическими полиномами σ_i. Элементарные симметрические полиномы от трёх переменных x, y, z выглядят следующим образом: $\sigma_1 = x + y + z = f_1; \sigma_2 = xy + xz + yz; \sigma_3 = xyz$.

В полях характеристики 2 формулы Ньютона, связывающие $f_1, f_2, ..., f_5$ с $\sigma_1, \sigma_2, \sigma_3$, имеют специальный вид:

$$\begin{cases} \sigma_1 = f_1, \\ f_2\sigma_1 + f_1\sigma_2 + \sigma_3 = f_3, \\ f_4\sigma_1 + f_3\sigma_2 + f_2\sigma_3 = f_5. \end{cases} \qquad (**)$$

Подставим в систему $(**)$ значения f_i из системы $(*)$: $f_1 = s_1; f_2 = s_1^2;$ $f_3 = s_2; f_4 = s_1^4; f_5 = s_3$. Получим следующую систему линейных уравнений относительно неизвестных $\sigma_1, \sigma_2, \sigma_3$:

$$\begin{cases} \sigma_1 = s_1; \\ s_1^2\sigma_1 + s_1\sigma_2 + \sigma_3 = s_2; \\ s_1^4\sigma_1 + s_2\sigma_2 + s_1^2\sigma_3 = s_3. \end{cases} \qquad (***)$$

Подставим в $(***)$ значения $s_1 = s_2 = \alpha,\ s_3 = \alpha^5$. Получим систему

$$\begin{cases} \sigma_1 = \alpha; \\ \alpha^2\sigma_1 + \alpha\sigma_2 + \sigma_3 = \alpha^7; \\ \alpha^4\sigma_1 + \alpha^7\sigma_2 + \alpha^2\sigma_3 = \alpha^5. \end{cases}$$

Отсюда следует $\begin{cases} \alpha\sigma_2 + \sigma_3 = \alpha^7 + \alpha^3 = \alpha^6; \\ \alpha^5\sigma_2 + \sigma_3 = 0. \end{cases}$

Следовательно, $\sigma_3 = \alpha^5\sigma_2; \sigma_2(\alpha^5 + \alpha) = \alpha^6$ или $\sigma_2\alpha^4 = \alpha^6$. Таким образом, $\sigma_2 = \alpha^2; \sigma_3 = \alpha^7$.Полученные значения $\sigma_1, \sigma_2, \sigma_3$ служат, согласно теореме Виета, коэффициентами кубического уравнения

$t^3 + \sigma_1 t^2 + \sigma_2 t + \sigma_3 = 0$, корнями которого и являются искомые в системе (*) неизвестные x, y, z. Итак, решение системы (*) сводится к поиску корней кубического уравнения $t^3 + \alpha \cdot t^2 + \alpha^2 \cdot t + \alpha^7 = 0$ в поле $GF(2^4)$.

Метод Чэня, то есть последовательная подстановка в уравнение элементов поля $GF(2^4)$ вместо t, позволяет найти следующие его корни: $x = 1$; $y = \alpha^9$; $z = \alpha^{13}$. Корни однозначно указывают тройную ошибку на 1-й, 10-й и 14-й позициях в сообщении $\bar{x}$. Следовательно, отправлено было истинное сообщение $\bar{c} = (01011\ 00100\ 01111)$.

Задание 1. Пусть ТКС функционирует на основе БЧХ-кода C_7 длиной 31 с проверочной матрицей $H = (\alpha^i, \alpha^{3i}, \alpha^{5i})^T$ для примитивного элемента α поля $GF(2^5)$, корня полинома $x^5 + x^4 + x^2 + x + 1$. Пусть приёмное устройство ТКС приняло сообщение с синдромом ошибок $S = (\alpha^{28}, \alpha^{29}, \alpha^{28})$. Найти ошибку в данном сообщении.

Решение. Кубическое уравнение получается преобразованием системы уравнений $\begin{cases} x_1 + x_2 + x_3 = \alpha^{28}, \\ x_1^3 + x_2^3 + x_3^3 = \alpha^{29}, \\ x_1^5 + x_2^5 + x_3^5 = \alpha^{28}. \end{cases}$

Требуемое кубическое уравнение имеет вид $t^3 + \sigma_1 t^2 + \sigma_2 t + \sigma_3 = 0$, где $\sigma_1, \sigma_2, \sigma_3$ находятся из СЛАУ: $\begin{cases} \sigma_1 = s_1, \\ s_1^2 \sigma_1 + s_1 \sigma_2 + \sigma_3 = s_2, \\ s_1^4 \sigma_1 + s_2 \sigma_2 + s_1^2 \sigma_3 = s_3. \end{cases}$ В данном случае СЛАУ имеет вид: $\begin{cases} \sigma_1 = \alpha^{28}, \\ \alpha^{25} \sigma_1 + \alpha^{28} \sigma_2 + \sigma_3 = \alpha^{29}, \\ \alpha^{19} \sigma_1 + \alpha^{29} \sigma_2 + \alpha^{25} \sigma_3 = \alpha^{28}. \end{cases}$ Вычисления показывают, что $\sigma_1 = \alpha^{28}$ $\sigma_2 = \alpha^{28}, \sigma_3 = \alpha^{12}$. Таким образом, получаем следующее кубическое уравнение: $t^3 + \alpha^{28} t^2 + \alpha^{28} t + \alpha^{12} = 0$. Применяя достаточно монотонный метод

Чэня, находим корни этого уравнения: $x = \alpha^9$, $y = \alpha^{13}$, $z. = \alpha^{21}$. Вычисленные локаторы однозначно определяют вектор-ошибку $\bar{e} = (10, 14, 22)$.

3. Задания для самостоятельной работы

Задание 1. В $(31, 16)$ БЧХ-коде C_7 с проверочной матрицей $H = (\alpha^i, \alpha^{3i}, \alpha^{5i})^T$, где α – корень примитивного полинома $p(x)$, принято сообщение $\bar{x}$ с синдромом $S = S(\bar{x}) = (s_1, s_2, s_3)$. Найти вектор ошибок в принятом сообщении сведением задачи к кубическому уравнению и решением этого уравнения методом Чэня.

Вариант 1: $p(x) = x^5 + x^2 + 1$. $S = (\alpha^{24}, \alpha^2, \alpha^{16})$.

Вариант 2: $p(x) = x^5 + x^3 + 1$. $S = (\alpha^{20}, \alpha^{23}, \alpha^{13})$.

Вариант 3: $p(x) = x^5 + x^3 + x^2 + x + 1$. $S = (\alpha^{18}, \alpha^{14}, \alpha^{27})$.

Вариант 4: $p(x) = x^5 + x^4 + x^2 + x + 1$. $S = (\alpha^{28}, \alpha^{29}, \alpha^{28})$.

Вариант 5: $p(x) = x^5 + x^4 + x^3 + x + 1$. $S = (\alpha^{25}, \alpha^6, \alpha^{27})$.

Вариант 6: $p(x) = x^5 + x^4 + x^3 + x^2 + 1$. $S = (\alpha^{22}, \alpha^{24}, \alpha^4)$.

Вариант 7: $p(x) = x^5 + x^2 + 1$. $S = (\alpha^{16}, \alpha^8, \alpha^{27})$.

Вариант 8: $p(x) = x^5 + x^3 + 1$. $S = (\alpha^{23}, \alpha^{22}, \alpha^{15})$.

Вариант 9: $p(x) = x^5 + x^3 + x^2 + x + 1$. $S = (\alpha^{15}, \alpha^{25}, \alpha^8)$.

Вариант 10: $p(x) = x^5 + x^4 + x^2 + x + 1$. $S = (\alpha^6, \alpha^6, \alpha^{17})$.

Вариант 11: $p(x) = x^5 + x^4 + x^3 + x + 1$. $S = (\alpha^{27}, \alpha^{12}, \alpha^6)$.

Вариант 12: $p(x) = x^5 + x^4 + x^3 + x^2 + 1$. $S = (\alpha^{24}, \alpha^{30}, \alpha^{14})$.

Вариант 13: $p(x) = x^5 + x^2 + 1$. $S = (\alpha^{26}, \alpha^8, \alpha^{26})$.

Вариант 14: $p(x) = x^5 + x^3 + 1$. $S = (\alpha^{22}, \alpha^{29}, \alpha^{23})$.

Вариант 15: $p(x) = x^5 + x^3 + x^2 + x + 1$. $S = (\alpha^{20}, \alpha^{20}, \alpha^6)$.

Практическое занятие №6

Циклическая и циклотомическая классификация векторов-ошибок

1. Необходимые теоретические сведения

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 на заре возникновения теории и практики помехоустойчивого кодирования, автоморфизмы линейных имеют более узкие рамки.

Определение 6.1. Автоморфизмом кода C называется произвольная перестановка координат кодовых слов, которая преобразует кодовые слова в новые кодовые слова.

Теорема 6.1. Множество $AutC$ линейного кода C длиной n есть подгруппа группы подстановок S_n.

Пусть σ – оператор циклического сдвига координат векторов, действие которого на произвольный вектор $\overline{e} = (e_1, e_2, ..., e_n)$ 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 6.2.

Теорема 6.2. Оператор σ является автоморфизмом кодов Хемминга с проверочной матрицей H_χ^c, БЧХ-кодов с проверочной матрицей (4.1), реверсивных кодов из ПЗ4.

Следствие. У каждого кода C длиной n из теоремы 5.2 группа автоморфизмов $AutC$ содержит циклическую подгруппу $\Gamma = <\sigma> = \{\sigma, \sigma^2, ..., \sigma^n = e\}$ порядка n.

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

Предложение 6.1. Пусть m – наименьшее натуральное число с условием: $2^m - 1$ делится на данное нечётное число n. Циклическая группа Ф, порожденная степенями подстановки φ на множестве $T = \{1, 2, ..., n\}$, конечна и имеет порядок m.

Группа Ф 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 $(n-1)$-ую. 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 Ф – циклотомической.

Теорема 6.3. Циклотомическая группа Ф является подгруппой группы $AutC$ кодов Хемминга, БЧХ-кодов с проверочной матрицей (4.1), реверсивных кодов – кодов, перечисленных в теореме 5.2.

Лемма 6.2. Для произвольного $\bar{e} \in E_n$ $\varphi(\sigma(\bar{e})) = \sigma^2(\varphi(\bar{e}))$.

Теорема 6.4. Группа подстановок G, порождённая циклической подстановкой σ и циклотомической подстановкой φ, некоммутативна и имеет порядок mn.

Определение 6.2. Равенство $\bar{e} = (i_1, i_2, ..., i_k)$ означает, что двоичный вектор $\bar{e}$ имеет ненулевыми и, следовательно, равными 1 только координаты под номерами $i_1, i_2, ..., i_k$.

Важнейшим для дальнейшего является определение 6.3.

Определение 6.3. Совокупность всех попарно различных векторов-ошибок $\sigma^k(\bar{e})$, $0 \le k < n$, называется Г-орбитой вектора-ошибки $\bar{e}$ в 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 6.5.

Теорема 6.5. 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:

$$<\bar{e}> = \left\{ \bar{e}, \sigma(\bar{e}), \ldots, \sigma^{\lambda-1}(\bar{e}) \right\}. \qquad (6.1)$$

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.

Структурная формула (6.1) 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 $<\bar{e}>$, то есть для всяких векторов $\bar{e}_i$, $\bar{e}_j$ из $<\bar{e}>$ найдется $g \in \Gamma$, при котором $g(\bar{e}_i) = \bar{e}_j$. Этот факт дополняет предложение 6.2.

Предложение 6.2. 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.

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

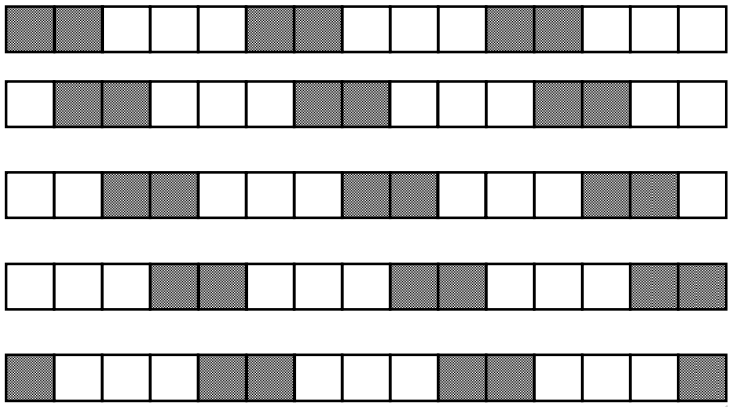

Рис. 6.1. Схематическое изображение вектора $\bar{e}$=(1,2,6,7,11,12) из пространства E_{15} и его циклических сдвигов $\sigma(\bar{e}), \sigma^2(\bar{e}), \sigma^3(\bar{e}), \sigma^4(\bar{e})$

Из теоремы 6.5 и предложения 6.2 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 нём. Множество всех Г-орбит пространства E_n будем обозначать через E_n / Γ.

Пример 6.1. Построим классификацию, то есть 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, порождённые 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 $<\bar{1}>$ – мощности 1, одну – <(1010)> – мощ-

ности 2 и три – <(1000)>, <(1100)>, <(1110)> – мощности 4. Таким образом, множество E_4 / Γ состоит из 6 элементов.

Определение 6.4. (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. 6.2. 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	0	1	0
0	0	0	1	0	1	1	0	0	0	1	0	0	1	0	0	0	1

Рис. 6.2. Пакеты векторов-ошибок длиной 3 в пространстве V_6 над полем $GF(2)$:
а) весом 3; б) весом 2

Определение 6.5. 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 6.2. Вектор-ошибка $\bar{e}$ = (100010) – есть ошибка веса $\omega = 2$ в кодовом слове длиной n = 6, его можно рассматривать как пакет ошибок длиной 5 или пакет длиной 3. Таким образом, диаметр D этого вектора-ошибки равен 3.

Предложение 6.3. Диаметр вектора-ошибки $\bar{e}$ весом ω>1 с ненулевыми координатами на позициях $i_1, i_2 \ldots i_\omega$ вычисляется по формуле

$$D(\bar{e}) = D_{\bar{e}} = \min\{i_\omega - i_1 + 1, n + i_1 - i_2 + 1, n + i_2 - i_3 + 1, \ldots, n + i_{\omega-1} - i_\omega + 1\} \quad (6.2)$$

В частности, при $\omega = 2$

$$D(\bar{e}) = D_{\bar{e}} = \min\{i_2 - i_1 + 1, n + i_1 - i_2 + 1\} \quad (6.3)$$

при $\omega = 3$

$$D(\bar{e}) = D_{\bar{e}} = \min\{i_3 - i_1 + 1, n + i_1 - i_2 + 1, n + i_2 - i_3 + 1\}. \quad (6.4)$$

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

Предложение 6.4. Пусть E_n – двоичное векторное пространство. Одиночные ошибки составляют один класс эквивалентности I_1. Векторы-ошибки веса 2 принадлежат одному классу эквивалентности (Г-орбите) тогда и только тогда, когда их диаметры совпадают. По значениям диаметра множество всех двойных ошибок разбивается на ν непересекающихся классов эквивалентности I_2, $I_3, \ldots, I_{\nu+1}$, где ν = [n/2] – целая часть числа $n/2$, I_k – класс двойных ошибок диаметра k, 2≤k≤ν+1. Для нечетных $n = 2\nu + 1$ каждый из классов I_k состоит из n различных ошибок. При четных $n = 2\nu$ класс I_k, где $2 < k < \nu$, состоит из n векторов-ошибок, а класс $I_{\nu+1}$ – из ν двойных ошибок.

Пример 6.3. В пространстве E_{15} имеется $C_{15}^2 = 105$ векторов-ошибок веса 2, делящихся, согласно предложению 3.7, на 7 полных Г-орбит в соответствии со значением их диаметров. Ниже приведена табл. 6.1 образующих Г-орбит двойных ошибок в 15-мерном пространстве – векторов-ошибок $\bar{e}_{1,i}$ диаметра $D_i = 2, 3, \ldots, 8$.

Таблица 6.1

Г-орбиты двойных ошибок в пространстве E_{15}

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

Определение 6.6. Совокупность всех различных векторов $\varphi^s(\overline{e}),\ 0 \le s \le m-1,$ для данного фиксированного вектора $\overline{e} \in E_n$ называется Ф-орбитой или циклотомической орбитой вектора $\overline{e}$ при действии группы Ф на пространстве E_n и обозначается через $<\overline{e}>_{\Phi}$.

По аналогии с теоремой 5.5 доказывается предложение 6.5.

Предложение 6.5. Для произвольного фиксированного вектора $\overline{e} \in E_n$ его Ф-орбита $<\overline{e}>_{\Phi}$ состоит из μ элементов, где $\mu = m$ или μ делит m. При этом μ – наименьшее натуральное число с условием $\varphi^{\mu}(\overline{e}) = \overline{e},$ а Ф-орбита $<\overline{e}>_{\Phi}$ имеет следующую структуру: $<\overline{e}>_{\Phi} = \{\overline{e}, \varphi(\overline{e}), ..., \varphi^{\mu-1}(\overline{e})\}$. Все векторы из $<\overline{e}>_{\Phi}$ имеют одинаковый вес.

Действие группы Ф на векторы пространства E_7 иллюстрирует рис. 6.3.

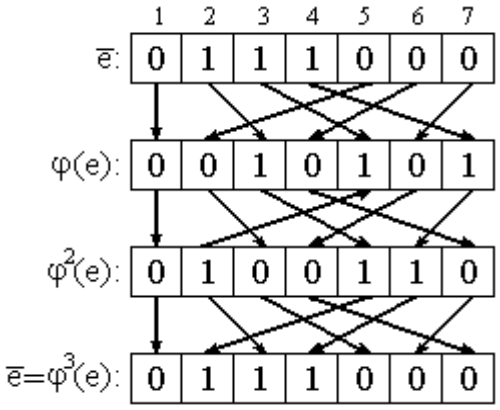

Рис. 6.3. Действие циклотомической подстановки φ и ее степеней на пространстве E_7, в частности на вектор $\bar{e} = (0111000)$

Пример 6.4. 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 6.6. Пусть $J = \{\bar{e}, \sigma(\bar{e}), \ldots, \sigma^{\ell-1}(e)\}$, где $\ell = n$ или ℓ – делитель n, – Г-орбита векторов-ошибок из E_n, а $\varphi(J) = \{\varphi(\bar{e}), \varphi(\sigma(\bar{e})), \ldots, \varphi(\sigma^{\ell-1}(e))\}$. Тогда $\varphi(J)$ – также Г-орбита векторов из E_n.

Определение 6.7. Пусть J – фиксированная Г-орбита векторов-ошибок из E_n. Совокупность всех попарно различных Г-орбит $\varphi^k(J), 0 \le k \le m-1$, называется Ф-орбитой класса J (или циклоклассом Г-орбиты J) при действии Ф на множестве E_n/Γ и обозначается $< J >_{\Phi}$.

Теорема 6.6. 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:

$$< J >_{\Phi} = \{J, \varphi(J), \ldots, \varphi^{\mu-1}(J)\}. \qquad (6.5)$$

Определение 6.8. Два вектора $\bar{f}$ и $\bar{g}$ из E_n называются G-эквивалентными, если найдется такая подстановка $\phi = \varphi^j \sigma^i \in \mathrm{G}$, что $\bar{g} = \phi(\bar{f})$.

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 $m\,n-1$ других векторов, в силу теоремы 3.4. Векторов-ошибок весом 2 имеется $n(n-1)/2 > m \cdot n$ при $n > 2m+1$, то есть при $2^m - 1 > 2m+1$, что выполняется при всех целых $m \geq 4$.

Определение 6.9. 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 6.7. 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 Φ-орбиты $<\bar{e}>_G = \{<\bar{e}>, \varphi<\bar{e}>, \varphi^2<\bar{e}>, \ldots, \varphi^{\mu-1}<\bar{e}>\}$.

Пример 6.5. В двоичном пространстве E_{31} имеется 15 Г-орбит ошибок веса 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.

2. Задания для аудиторной работы

Задание 1. Построить циклическую классификацию двойных векторов-ошибок в коде длиной 8.

Решение. В данном коде имеется $C_8^2 = \frac{8 \cdot 7}{2} = 28$ различных двойных векторов-ошибок, что составляет не более трёх полных Г-орбит (содержащих по восемь векторов-ошибок весом 2). Прямая проверка показывает, что к этим орбитам относятся Г-орбиты $J_1 = <\bar{e}_{12}> = <(1, 2)> = <(1100\,0000)>$; $J_2 = <\bar{e}_{13}> = <(1, 3)> = <(1010\,0000)>$; $J_3 = <\bar{e}_{14}> = <(1, 4)> = <(1001\,0000)>$. Оставшиеся 4 вектора-ошибки содержит неполная Г-орбита $J_4 < \bar{e}_{15} > = <(1, 5)> = <(1000\,1000)>$.

Задание 2. Построить циклическую классификацию двойных векторов-ошибок в коде: а) длиной 15; б) длиной 14.

Задание 3. Построить циклическую классификацию тройных векторов-ошибок в коде длиной 7.

Задание 4. Построить циклическую классификацию тройных векторов-ошибок в коде: а) длиной 8; б) длиной 15.

Задание 5. Построить Ф-орбиты векторов-ошибок $\bar{e}_{12} = (110\,0000)$ и $f = (1000100)$.

Решение. Группа Ф – это циклическая группа, порождённая степенями циклотомической подстановки φ, переставляющего координаты каждого вектора $\bar{e} = (e_1, e_2, ..., e_n) \in E_n$ по правилу: $\varphi(i) = \overline{2i - 1}$, где $1 \le i \le n$, и для каждого целого $j < 2n$ величина $\bar{j} = j$, если $1 \le j \le n$, $\bar{j} = j - n$, если $n + 1 \le j < 2n$.

В соответствии с данным правилом $\varphi(\bar{e}_{12}) = (1010\,000)$; $\varphi^2(\bar{e}_{12}) = (100\,0100) = \bar{f}$; $\varphi^3(\bar{e}_{12}) = (110\,0000) = \bar{e}_{12}$. Следовательно, Ф-орбита $<\bar{e}_{12}>_{\Phi} = \{(1100000), (1010000), (1000100)\}$. Орбиты либо не пересекаются, ли-

бо совпадают. Поэтому из проведенных вычислений следует, что Ф-орбита, порождённая вектором $f = (1000100)$, совпадает с построенной Ф-орбитой $<\bar{e}_{12}>_{\Phi}$.

Задание 6. Пусть $<\bar{e}_{12}>$ – Г-орбита, порождённая вектором $\bar{e}_{12}$. Проверить, является ли Г-орбитой множество $\varphi(<\bar{e}_{12}>)$?

Задание 7. Построить G-орбиту $<\bar{e}_{12}>_G$. Имеются ли ещё другие G-орбиты в пространстве E_7?

Задание 8. Построить все G-орбиты тройных ошибок в пространстве E_7.

3. Задания для самостоятельной работы

Задание 1. Разбить на Г-орбиты и G-орбиты двойные ошибки в двоичном пространстве E_n, где n задано по вариантам.

Задание 2. Разбить на Г-орбиты и G-орбиты тройные ошибки в двоичном пространстве E_n из задания 1.

Задание 3. Разбить на Г-орбиты и G-орбиты 4-кратные ошибки в двоичном пространстве E_n из задания 1.

Задание 1.

Вариант 1: $n = 17$. Вариант 2: $n = 19$.

Вариант 3: $n = 21$. Вариант 4: $n = 23$.

Вариант 5: $n = 25$. Вариант 6: $n = 27$.

Вариант 7: $n = 29$. Вариант 8: $n = 31$.

Вариант 9: $n = 33$. Вариант 10: $n = 35$.

Вариант 11: $n = 37$. Вариант 12: $n = 39$.

Вариант 13: $n = 41$. Вариант 14: $n = 43$.

Вариант 15: $n = 45$.

Практическое занятие №7

Норменное декодирование реверсивных и БЧХ-кодов

1. Необходимые теоретические сведения

Векторы каждой Г-орбиты имеют тесную взаимосвязь – каждый из них можно получить циклическими сдвигами любого фиксированного вектора этой Г-орбиты. Подавляющее большинство Г-орбит принадлежит многообразию полных Г-орбит. Такая же тесная связь существует и между синдромами векторов-ошибок каждой Г-орбиты. Об этом свидетельствуют следующие ниже теоремы.

Теорема 7.1. Пусть $\bar{e}$ – вектор ошибок в БЧХ-коде С с проверочной матрицей (5.1). Пусть $S(\bar{e})=(s_1,s_2,...,s_{\delta-1})$ – синдром ошибок вектора $\bar{e}$. Тогда

$$S(\sigma(\bar{e}))=(\beta^b s_1,\beta^{b+1}s_2,...,\beta^{b+i-1}s_i,...,\beta^{b+\delta-2}s_{\delta-1}); \quad (7.1)$$

а для произвольного целого λ синдром

$$S(\sigma^\lambda(\bar{e}))=(\beta^{\lambda b}\cdot s_1,\beta^{\lambda(b+1)}\cdot s_2,...,\beta^{\lambda(b+i-1)}\cdot s_i,...,\beta^{\lambda(b+\delta-2)}\cdot s_{\delta-1}). \quad (7.2)$$

Если же БЧХ-код задан проверочной матрицей (2.2), то

$$S(\sigma(\bar{e}))=(\beta s_1,\beta^3 s_2,\beta^5 s_3,...,\beta^{2i-1}s_i,...,\beta^{2t-1}s_t). \quad (7.3)$$

Пусть C_R^{2r+1} – реверсивный с проверочной матрицей $H=(\alpha^i,\alpha^{-i})^T$. Тогда $S(\sigma(\bar{e}))=(\alpha\cdot s_1,\alpha^{-1}\cdot s_2)$.

Определение 7.1. Спектром синдромов $S(J)$ в БЧХ-коде С Г-орбиты J называется множество синдромов всех векторов-ошибок из J в этом коде. Спектр $S(J)$ называется полным, если его мощность совпадает с мощностью Г-орбиты J: $|S(J)|=|J|$, в противном случае спектр $S(J)$ будем называть неполным.

Формулы (7.1) – (7.3) определяют структуру спектра синдромов Г-орбит векторов-ошибок, дают синдромные признаки полноты Г-орбит.

Теорема 7.1 утверждает, что, как и векторы каждой Г-орбиты J, спектр синдромов $S(J)$ можно сконструировать по формулам (7.1) – (7.3) из синдрома

$S(\bar{e})$ любого вектора $\bar{e} \in J$. Здесь, при условии полноты $S(J)$, существует полное взаимно-однозначное соответствие между циклическими сдвигами векторов и соответствующими преобразованиями их синдромов.

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

Определение 7.2. Нормой синдрома $S(\bar{e}) = (s_1, s_2, ..., s_{\delta-1})$ вектора ошибок $\bar{e}$ в БЧХ-коде С с проверочной матрицей (5.1) называется вектор $\vec{N}(S(\bar{e})) = (N_{12}, N_{13}, ..., N_{1(\delta-1)}, N_{23}, ..., N_{(\delta-2)(\delta-1)})$ 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 $s_i \neq 0$. (7.4)

В двоичном БЧХ-коде с проверочной матрицей (5.2) синдром имеет меньше координат – t, следовательно, норма синдрома есть вектор $\bar{N} = \bar{N}(S) = (N_{12}, N_{13}, ..., N_{1t}, N_{23}, ..., N_{(t-1)t})$ с C_t^2 координатами, которые для $h_{ij} = НОД(2i-1, 2j-1)$ вычисляются в случае $s_i \neq 0$ по формуле

$$N_{ij} = s_j^{(2i-1)/h_{ij}} \Big/ s_i^{(2j-1)/h_{ij}}. \quad (7.5)$$

Пусть $t = 2$, то есть БЧХ-код C задается проверочной матрицей $H = (\beta^i, \beta^{3i})$, $0 \le i \le n-1$. Тогда норма синдрома состоит из одной компоненты $N = s_2 / s_1^3$. Пусть $t = 3$, то есть БЧХ-код C задается проверочной матрицей $H = (\beta^i, \beta^{3i}, \beta^{5i})$, $0 \le i \le n-1$. Тогда норма синдрома, согласно формуле (7.5), состоит из трех компонент: $N_1 = s_2 / s_1^3$; $N_2 = s_3 / s_1^5$; $N_3 = s_3^3 / s_2^5$. Они соответствуют компонентам N_{13}, N_{15}, N_{35} определения 7.2 при $b = 1$.

Определение 7.3. Нормой синдрома $S(\bar{e}) = (s_1, s_2)$ вектора-ошибки $\bar{e}$ в реверсивном коде C_R^{2r+1} с проверочной матрицей $H = (\alpha^i, \alpha^{-i})^T$ называется ве-

личина $N = N(S(\bar{e})) = s_1 \cdot s_2$.

Основное свойство норм синдромов отражает теорема 7.2

Теорема 7.2. *Для всякого вектора ошибок* $\bar{e}$ *и его синдрома* $S(\bar{e})$ *в БЧХ-коде* C *справедливо равенство* $\overline{N}(S(\sigma(\bar{e}))) = \overline{N}(S(\bar{e}))$. *Это же равенство справедлива и для реверсивных кодов* C_R^{2r+1}.

Из теоремы 7.2 следует, что все векторы каждой Г-орбиты имеют одинаковую норму синдрома, то есть норма синдрома инвариантна относительно группы Γ циклических сдвигов. Это позволяет ввести следующее определение.

Определение 7.4. *Нормой* $N(J)$ *Г-орбиты* J *векторов-ошибок в любом БЧХ-коде, а также и в реверсивном коде, называется норма синдрома любого вектора-ошибки из этой Г-орбиты.*

Норма Γ-орбиты является ее однозначной характеристикой, то есть идентификатором этой орбиты.

Предложение 7.1. Пусть J_1, J_2 – две Г-орбиты векторов-ошибок в БЧХ-коде C (в реверсивном коде C_R^{2r+1}), имеющие различные нормы: $N(J_1) \neq N(J_2)$. Тогда для любых векторов $\bar{g} \in J_1$ и $\bar{f} \in J_2$ их синдромы $S(\bar{f})$ и $S(\bar{g})$ различны. Другими словами, спектры синдромов таких Г-орбит не пересекаются.

Предложение 7.2. Пусть I и J – две Г-орбиты векторов-ошибок с одинаковыми нормами в примитивном двоичном БЧХ-коде C_{2t+1} (в реверсивном коде C_R). 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 $S(\bar{e}) = S(\bar{f})$.

Следствие. *Множество Г-орбит всех векторов-ошибок весом 1–3 имеет в примитивном двоичном БЧХ-коде* C_7 *попарно различные нормы. Множество Г-орбит всех векторов-ошибок весом 1–2 имеет в примитивном двоичном БЧХ-коде* C_5 *попарно различные нормы.*

Построенная теория позволяет предложить норменный метод коррекции

ошибок в БЧХ-кодах. Суть метода. Составляем таблицу всех Г-орбит $<\bar{e}_i>$ корректируемых ошибок, таблицу синдромов $S(\bar{e}_i)$, а также таблицу $\bar{N}(S(\bar{e}_i))$. По принятому вектору-сообщению вычисляем $S(\bar{x}) = S(\bar{e})$ и $\bar{N}(S(\bar{e}))$. В таблице норм находим $\bar{N}(S(\bar{e}_i)) = \bar{N}(S(\bar{e}))$. 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 λ циклического сдвига для получения вектора $\bar{e}$ из вектора $\bar{e}_i$. Тогда $\bar{e} = \sigma^{\lambda}(\bar{e}_i)$ – искомый вектор ошибок.

2. Задания для аудиторной работы

Задание 1. Составить таблицу образующих $\bar{e}_i$ Г-орбит векторов-ошибок весом 2, синдромов $S(\bar{e}_i)$ и норм синдромов в примитивном БЧХ-коде длиной 15 на основе полинома $x^4 + x + 1$.

Задание 2. Норменным методом исправить ошибки в сообщении $\bar{x} = (111011110110101)$, принятом ТКС на основе кода из задания 1.

Задание 3. Составить таблицу образующих $\bar{e}_i$ Г-орбит векторов-ошибок весом 2, синдромов $S(\bar{e}_i)$ и норм синдромов в примитивном БЧХ-коде длиной 31 на основе полинома $x^5 + x^2 + 1$.

Решение. Составим требуемую таблицу 7.1.

Таблица 7.1

Диаметры порождающих векторов, норм и показателей Г-орбит

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
$I5$	$\bar{e}_{1,5}$	10	23	24
$I6$	$\bar{e}_{1,6}$	2	24	18
$I7$	$\bar{e}_{1,7}$	27	1	13
$I8$	$\bar{e}_{1,8}$	22	25	21
$I9$	$\bar{e}_{1,9}$	20	15	17

Окончание таблицы 7.1

Г-орбита	Образующая Вектор-ошибка	Синдром образующей		Норма Г-орбиты
		$\deg S_1$	$\deg S_2$	$\deg N(S)$
I10	$\bar{e}_{1,10}$	16	6	20
I11	$\bar{e}_{1,11}$	4	17	5
I12	$\bar{e}_{1,12}$	19	5	10
I13	$\bar{e}_{1,13}$	23	2	26
I14	$\bar{e}_{1,14}$	14	20	9
I15	$\bar{e}_{1,15}$	13	19	11
I16	$\bar{e}_{1,16}$	24	13	3

Задание 4. Норменным методом исправить ошибки в сообщении $\bar{x} = (001\ 011\ 011\ 100\ 000\ 100\ 000\ 000\ 100\ 000\ 1)$, принятом ТКС на основе кода из задания 3.

Решение. 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 $N(S(\bar{x})) = s_2 / s_1^3 = \alpha^{10}$. Таблица из предыдущего задания показывает, что вектор-ошибка $\bar{e}$ в принятом сообщении $\bar{x} = \bar{c} + \bar{e}$ принадлежит Г-орбите I_{12}, порождённой 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

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

Задание 5. Сформировать матрицу $H = (\alpha^i, \alpha^{-i})^T$ реверсивного кода длиной 31, где α – корень полинома $x^5 + x^2 + 1$. Найти минимальное расстояние этого кода и оценить его декодирующие возможности.

Задание 7. ТКС функционирует на основе реверсивного кода длиной 31 с проверочной матрицей $H = (\alpha^i, \alpha^{-i})^T$, где α – корень полинома $x^5 + x^2 + 1$. Его приёмное устройство приняло сообщение

$\bar{x} = (011\,010\,110\,100\,000100\,001\,000\,000\,00\,1)$. Исправить норменным методом имеющиеся ошибки в данном сообщении.

Решение. Составим таблицу 7.2 порождающих векторов, синдромов и показателей норм Г-орбит одиночных и двойных ошибок в реверсивном коде.

Таблица 7.2

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

Г-орбита	Образующая вектор-ошибка	Синдром образующей		Норма Г-орбиты
		$\deg s_1$	$\deg s_2$	$\deg N(S)$
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
I_9	$\bar{e}_{1,9}$	20	12	1
I_{10}	$\bar{e}_{1,10}$	16	7	23
I_{11}	$\bar{e}_{1,11}$	4	25	29
I_{12}	$\bar{e}_{1,12}$	19	8	27
I_{13}	$\bar{e}_{1,13}$	23	11	3
I_{14}	$\bar{e}_{1,14}$	14	1	15
I_{15}	$\bar{e}_{1,15}$	13	30	12
I_{16}	$\bar{e}_{1,16}$	24	9	2

Вычислим синдром ошибок принятого сообщения. $S(\bar{x}) = (\alpha^{30}, \alpha^{3})$. Вычислим $N(S(\bar{x})) = \alpha^{30} \cdot \alpha^{3} = \alpha^{2}$. Норма указывает в соответствии с таблицей 7.2, 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 $\bar{e} = (7, 22)$.

3. Задания для самостоятельной работы

Задание 1. Взять линейный код из задания №4 раздела «задания для самостоятельной работы» практического занятия №4. Составить таблицу образующих Г-орбит двойных ошибок, синдромов этих образующих и норм вычисленных синдромов.

Задание 2. Задание 5 из раздела «задания для самостоятельной работы» практического занятия №4 решить норменным методом.

Практическое занятие №8

Норменное декодирование тройных ошибок в БЧХ-кодах

1. Необходимые теоретические сведения

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. В [16] установлена формула для числа T_{ω} ошибок с первой компонентой синдрома $s_1 = 0$. Для $\varpi = 3$ эта формула гласит: $T_3 = C_n^2/3 = n(n-1)/6$, 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 $n = 15$, пяти – при $n = 31$, 11 – при $n = 63$ и так далее.

Рассмотрим модификацию норменного метода, предложенную в [17], 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 $S = S(\bar{e}) = (s_1, s_2, s_3)$, причём $s_1 \neq 0$. 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 $\bar{e}^*$ берём 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 8.1. Найдем вектор ошибок $\bar{e}$ модифицированным норменным методом в БЧХ-коде C_7 длиной 63 и проверочной матрицей $H = (\alpha^i, \alpha^{3i}, \alpha^{5i})^T$, где α – примитивный элемент поля Галуа $GF(2^6)$, корень полинома $x^6 + x^5 + x^4 + x + 1$, если принято очередное сообщение с синдромом $S = S(\bar{e}) = (\alpha^{21}, \alpha^{44}, \alpha^{27})$.

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 8.1.

Таблица 8.1

Составим таблицу 11 Г-орбит тройных ошибок в данном коде с $s_1 = 0$.

№ 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)	$(0,\alpha^{3},\alpha^{14})$	$(\infty,\infty,\alpha^{27})$

Окончание таблицы 8.1

№ п/п	Образующая $\bar{e}_i$	Синдром $S(\bar{e}_i)$	Норма $\bar{N}_i = \bar{N}(S(\bar{e}))_i$
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-й, 14-й, 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 $\bar{e}$:

$$x = x^* + s_1 = \alpha^3 + \alpha^{21} = \alpha^{30}; y = y^* + s_1 = \alpha^{13} + \alpha^{21} = \alpha^{10}; \quad z = z^* + s_1 = \alpha^{59} + \alpha^{21} = \alpha^{20}.$$

Следовательно, $\bar{e} = (11, 21, 31)$ – тройная ошибка на 11-й, 21-й и 31-й позициях.

2. Задания для аудиторной работы

Задание 1. Составить таблицу 8.2 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 α – корнем полинома $x^4 + x + 1$.

Решение.

Таблица 8.2

Образующие Г-орбит ошибок веса 1, 2, 3 в пространстве E_{15},

их синдромы и нормы синдромов

№ п/п	Образующая $\bar{e}$ Г-орбиты	Синдром $S(\bar{e})$	Норма $\bar{N}$ Г-орбиты
1	(1)	(1, 1, 1)	(1, 1, 1)
2	(1, 2)	(α^4, α^{14}, α^{10})	(α^2, α^5, α^5)
3	(1, 3)	(α^8, α^{13}, α^5)	(α^4, α^{10}, α^{10})
4	(1, 4)	(α^{14}, α^7, 0)	(α^{10}, 0, 0)

Продолжение таблицы 8.2

№ п/п	Образующая $\bar{e}$ Г-орбиты	Синдром $S(\bar{e})$	Норма $\overline{N}$ Г-орбиты
1	(1)	(1, 1, 1)	(1, 1, 1)
2	(1, 2)	(α^4, α^{14}, α^{10})	(α^2, α^5, α^5)
3	(1, 3)	(α^8, α^{13}, α^5)	(α^4, α^{10}, α^{10})
4	(1, 4)	(α^{14}, α^7, 0)	(α^{10}, 0, 0)
5	(1, 5)	(α, α^{11}, α^{10})	(α^8, α^5, α^5)
6	(1, 6)	(α^{10}, 0, α^5)	(0, 1, ∞)
7	(1, 7)	(α^{13}, α^{14}, 0)	(α^5, 0, 0)
8	(1, 8)	(α^9, α^{13}, α^9)	(α, α^{10}, α^{10})
9	(1, 2, 3)	(α^{10}, α^8, 0)	(α^8, 0, 0)
10	(1, 2, 4)	(α^7, α^4, α^5)	(α^{13}, 1, α^{10})
11	(1, 3, 4)	(α^{13}, α^{10}, α^{10})	(α, α^5, α^{10})
12	(1, 2, 5)	(0, α^5, 1)	(∞, ∞, α^5)
13	(1, 3, 5)	(α^5, α, 0)	(α, 0, 0)
14	(1, 4, 5)	(α^9, α^2, α^5)	(α^5, α^5, α^5)
15	(1, 2, 6)	(α^8, α^3, 0)	(α^9, 0, 0)
16	(1, 3, 6)	(α^4, α^6, 1)	(α^9, α^{10}, 1)
17	(1, 4, 6)	(α^{12}, α^9, α^{10})	(α^3, α^{10}, 1)
18	(1, 5, 6)	(α^2, α^{12}, 0)	(α^6, 0, 0)
19	(1, 2, 7)	(α^{12}, 1, α^5)	(α^9, α^5, 1)
20	(1, 3, 7)	(α^{14}, α^8, α^{10})	(α^{11}, 1, α^5)
21	(1, 4, 7)	(α^8, α^4, 1)	(α^{10}, α^5, α^{10})
22	(1, 5, 7)	(α^{11}, α^5, α^5)	(α^2, α^{10}, α^5)
23	(1, 6, 7)	(α^7, α^3, α^{10})	(α^{12}, α^5, 1)
24	(1, 2, 8)	(α^3, α^8, 1)	(α^{14}, 1, α^5)

Окончание таблицы 8.2

№ п/п	Образующая $\bar{e}$ Г-орбиты	Синдром $S(\bar{e})$	Норма $\overline{N}$ Г-орбиты
25	(1, 3, 8)	$(\alpha^{11}, 1, 0)$	$(\alpha^{12}, 0, 0)$
26	(1, 4, 8)	$(\alpha, \alpha^{10}, \alpha^{5})$	$(\alpha^{7}, 1, \alpha^{10})$
27	(1, 5, 8)	$(\alpha^{14}, \alpha, 1)$	$(\alpha^{4}, \alpha^{5}, \alpha^{10})$
28	(1, 6, 8)	$(\alpha^{6}, \alpha^{6}, 0)$	$(\alpha^{3}, 0, 0)$
29	(1, 7, 8)	$(\alpha^{5}, \alpha^{8}, \alpha^{5})$	$(\alpha^{8}, \alpha^{10}, \alpha^{5})$
30	(1, 2, 9)	$(\alpha^{5}, \alpha^{4}, 0)$	$(\alpha^{4}, 0, 0)$
31	(1, 3, 9)	$(0, \alpha^{10}, 1)$	$(\infty, \infty, \alpha^{10})$
32	(1, 4, 9)	$(\alpha^{6}, 1, \alpha^{10})$	$(\alpha^{12}, \alpha^{10}, 1)$
33	(1, 5, 9)	$(\alpha^{10}, \alpha^{2}, \alpha^{0})$	$(\alpha^{2}, 0, 0)$
34	(1, 6, 9)	$(\alpha, \alpha^{9}, 1)$	$(\alpha^{6}, \alpha^{10}, 1)$
35	(1, 7, 9)	$(\alpha^{3}, \alpha^{4}, \alpha^{10})$	$(\alpha^{10}, \alpha^{10}, \alpha^{10})$
36	(1, 4, 10)	$(\alpha^{4}, \alpha^{2}, 1)$	$(\alpha^{5}, \alpha^{10}, \alpha^{5})$
37	(1, 5, 10)	$(\alpha^{3}, 1, \alpha^{5})$	$(\alpha^{6}, \alpha^{5}, 1)$
38	(1, 6, 10)	$(\alpha^{13}, \alpha^{12}, \alpha^{10})$	$(\alpha^{3}, \alpha^{5}, 1)$
39	(1, 6, 11)	(0, 1, 0)	(∞, —, 0)

Задание 2. ТКС с кодом из задания 1 получило сообщение $\bar{x}$ с синдромом $S(\bar{x}) = (\alpha^{8}, \alpha^{6}, \alpha^{20})$. Найти норменным методом вектор ошибок $\bar{e}$ в этом сообщении.

Задание 3. Взять в ПЗ5 в разделе «задания для аудиторной работы» задание 1 и решить его модифицированным методом.

Решение. В двоичном коде длиной 15 имеется 455 тройных ошибок, которые делятся на 31 орбиту. Прямой норменный метод требует построения таблицы образующих всех орбит тройных ошибок, синдромов этих образующих, а также норм синдромов образующих.

Модифицируем норменный метод, 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 $\bar{e}^*$ берём 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 $S(\bar{e})$:

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

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

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

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

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

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

У нас $S(\bar{e}) = (\alpha, \alpha^7, \alpha^5)$. Следовательно, $s_2^* = \alpha^7 + \alpha^3 = \alpha^6$; $s_3^* = \alpha^5 + \alpha^5 = 0$. Таким образом, $S(\bar{e}^*) = (0, \alpha^6, 0)$. Тогда $\bar{N}(S(\bar{e}^*) = (\infty, -, 0)$.

Поищем в нашем (15, 7)-БЧХ-коде C_7 Г-орбиту с такой экзотической нормой. Единственная неполная Г-орбита J тройных ошибок в этом коде задаётся вектором $\bar{e}_J = (1, 6, 11)$ с ненулевыми координатами на 1-й, 6-й и 11-й позициях. Его синдром $S(\bar{e})$ имеет компоненты $s_1 = 1 + \alpha^5 + \alpha^{10} = 0$; $s_2 = 1 + \alpha^{15} + \alpha^{30} = 1$; $s_3 = 1 + \alpha^{25} + \alpha^{50} = 1 + \alpha^{10} + \alpha^5 = 0$. $\bar{N}(S(\bar{e})) = (\infty, -, 0) = \bar{N}(S(\bar{e}))^*$. Следовательно, $\bar{e}^* \in J$ и получается циклическим сдвигом вектора $\bar{e}_J = (1, 6, 11)$. $S(\sigma(\bar{e}_J)) = (0, \alpha^3, 0)$. $S(\sigma^2(\bar{e}_J)) = (0, \alpha^6, 0) = S(\bar{e}^*)$. Значит,

$\bar{e}^* = \sigma^2(\bar{e}_J) = (3, 8, 13)$ – тройная вектор-ошибка с ненулевыми координатами на 3-й, 8-й, 13-й позициях, локаторы которых $x^* = \alpha^2$, $y^* = \alpha^7$, $z^* = \alpha^{12}$. Отсюда легко находятся локаторы x, y, z ненулевых координат искомого вектора ошибок $\bar{e}$: $x = x^* + s_1 = \alpha^2 + \alpha = \alpha^{13}$; $y = y^* + s_1 = \alpha^7 + \alpha = \alpha^9$; $z = z^* + s_1 = \alpha^{12} + \alpha = 1$. Следовательно, $\bar{e} = (1, 10, 14)$ – тройная ошибка на 1-й, 10-й и 14-й позициях, что полностью совпадает с решением задания 1 практического занятия №5.

Задание 4. Пусть ТКС функционирует на основе БЧХ-кода C_7 длиной 31 с проверочной матрицей $H = (\alpha^i, \alpha^{3i}, \alpha^{5i})^T$ для примитивного элемента α поля $GF(2^5)$, корня полинома $x^5 + x^4 + x^2 + x + 1$. Пусть приёмное устройство ТКС приняло сообщение с синдромом ошибок $S = (\alpha^{28}, \alpha^{29}, \alpha^{28})$. Найти ошибку в данном сообщении.

Решение. Естественно предполагать, что в сообщении произошла тройная ошибка на позициях с неизвестными локаторами x, y, z. В этом случае для их определения имеем систему уравнений:

$$\begin{cases} x_1 + x_2 + x_3 = \alpha^{28}, \\ x_1^3 + x_2^3 + x_3^3 = \alpha^{29}, \\ x_1^5 + x_2^5 + x_3^5 = \alpha^{28}. \end{cases}$$

Сделаем замену $x_1 = x_1^* + \alpha^{28}$, $x_2 = x_2^* + \alpha^{28}$,..., $x_t = x_t^* + \alpha^{28}$. Получим новую систему уравнений: $\begin{cases} x_1^* + x_2^* + x_3^* = 0, \\ x_1^{*3} + x_2^{*3} + x_3^{*3} = \alpha^{24}, \\ x_1^{*5} + x_2^{*5} + x_3^{*5} = \alpha^{29}. \end{cases}$

В данном коде норма синдрома $\bar{N} = (N_1, N_2, N_3)$, где $N_1 = s_2 / s_1^3$; $N_2 = s_3 / s_1^5$; $N_3 = s_3^3 / s_2^5$. Тогда $\bar{N}^* = \bar{N}(S(\bar{e}^*)) = (\infty, \infty, \alpha^{29})$. Известно, что в данном БЧХ-коде имеется лишь пять Г-орбит тройных векторов-ошибок с $s_1 = 0$. Ниже приведен весь список этих Г-орбит (таб. 8.3).

Таблица 8.3

Образующие Г-орбит тройных ошибок, их синдромы и нормы синдромов в (31, 16) – БЧХ-коде C_7 с нормой вида $\bar{N} = (\infty, \infty, \beta)$

№ п/п	Образующая $\bar{e}_i$	Синдром $S(\bar{e}_i)$	Норма $\bar{N}_i = \bar{N}(S(\bar{e}))_i$
1	(1, 2, 20)	$(0, \alpha^{20}, \alpha^{12})$	$(\infty, \infty, \alpha^{29})$
2	(1, 3, 8)	$(0, \alpha^{9}, \alpha^{24})$	$(\infty, \infty, \alpha^{27})$
3	(1, 5, 15)	$(0, \alpha^{18}, \alpha^{17})$	$(\infty, \infty, \alpha^{23})$
4	(1, 4, 12)	$(0, \alpha^{14}, \alpha^{18})$	$(\infty, \infty, \alpha^{15})$
5	(1, 10, 16)	$(0, \alpha^{24}, \alpha^{19})$	$(\infty, \infty, \alpha^{30})$

Из таблицы следует, что вектор $\bar{e}^*$ принадлежит Г-орбите J, порождённой вектором $\bar{e}_{орб} = (1, 2, 20)$ – с ненулевыми координатами на первой, второй и 20-й позициях. Осталось определить величину циклического сдвига вектора $\bar{e}_{орб} = (1, 2, 20)$ для получения $\bar{e}^*$. Конкретное значение этой величины получается сравнением синдромов $S(\bar{e}_{орб}) = (0, \alpha^{20}, \alpha^{12})$ и $S(\bar{e}^*) = (0, \alpha^{24}, \alpha^{29})$. Если в БЧХ-коде C_{2t+1} синдром $S(\bar{e}) = (s_1, s_2, ..., s_t)$, то синдром $S(\sigma(\bar{e})) = (\alpha \cdot s_1, \alpha^3 \cdot s_2, ..., \alpha^{2t-1} \cdot s_t)$. Существует такое натуральное k, что $\sigma^k(\bar{e}_{орб}) = \bar{e}^*$. Следовательно, $20 + 3k = 24 + 31l$ для подходящего целого l или $3k = 4 + 31l$. Подберём наименьшее l, при котором $31l + 4$ делится на 3. Легко видеть, что требуемое $l = 2$. Тогда $31l + 4 = 66 = 3 \cdot 22$, то есть $k = 22$. Следовательно, $\bar{e}^* = (11, 23, 24)$. Поэтому $x_1^* = \alpha^{10}, x_2^* = \alpha^{22}, x_3^* = \alpha^{23}$. Тогда

$$x_1 = x_1^* + \alpha^{28} = \alpha^{10} + \alpha^{28} = \alpha^9, \; x_2 = x_2^* + \alpha^{28} = \alpha^{22} + \alpha^{28} = \alpha^{13},$$
$$x_3 = x_3^* + \alpha^{28} = \alpha^{23} + \alpha^{28} = \alpha^{21}.$$

Вычисленные локаторы однозначно высвечивают искомую вектор-ошибку $\bar{e} = (10, 14, 22)$.

3. Задания для самостоятельной работы

Задания для самостоятельной работы из ПЗ5 решить модифицированным норменным методом.

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, 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. Уэндон. – М. : Мир, 1976. – 574 с.

5. Теория кодирования / Т. Кассами [и др.]. – М. : Мир, 1978. – 576 с.

6. Теория информации и кодирование / Б. Б.Самсонов [и др.]. – Ростов-на-Дону : Феникс, 2002. – 288 с. (Серия «Учебники и учебные пособия»).

7. Конопелько, В. К. Прикладная теория кодирования: учеб. пособие для ВУЗов / В. К. Конопелько, В. А. Липницкий. / Т. 1, 2. – Минск : БГУИР, 2004. – 688 с.

8. Вернер, М. Основы кодирования: учеб. 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. Лиддл, Р. Конечные поля / Р. Лиддл, Г. Нидеррайтер. / Т. 1, 2. – М. : Мир, 1988. – 822 с.

11. Липницкий, В. А. Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа / В. А. Липницкий. – Минск : БГУИР, 2005. – 88 с. ; 2-е изд. – Минск : БГУИР, 2006. – 88 с.

12. Липницкий, В. А. Теория норм синдромов: метод. пособие / В. А. Липницкий. – Минск : БГУИР, 2011. – 96 с.

13. Конопелько, В. К. Теория норм синдромов и перестановочное декодирование помехоустойчивых кодов / В. К. Конопелько, В. А. Липницкий. – Минск : БГУИР, 2000. – 242 с. ; 2-е изд. – М. : УРСС, 2004. – 176 с.

14. Конопелько, В. К. Норменное декодирование помехоустойчивых кодов и алгебраические уравнения / В. К Конопелько, В. А. Липницкий. – Минск : Издательский центр БГУ, 2007. – 240 с.

15. Липницкий, В. А. Норменное декодирование ошибок посредством их модификации / В. А. Липницкий, Е. К. Аль-Хайдар. – Доклады БГУИР, №5(43). – 2009. – С. 12 – 16.

16. Дворников, В. Д. Теория и практика низкоскоростных кодов / В. Д. Дворников, В. К. Конопелько, В. А. Липницкий. – Минск : БГУИР, 2002. – 210 с.

17. Лосев, В. В. Микропроцессорные устройства обработки информации. Алгоритмы цифровой обработки / В. В. Лосев. – Минск : Выш. шк., 1990. – 132 с.

18. Муттер, В. М. Основы помехоустойчивой телепередачи информации / В. М. Муттер. – Л. : Энергоатомиздат, 1990. – 286 с.

Содержание

Св. план 2012, п. 35

Учебное издание

Липницкий Валерий Антонович

Олешкевич Дмитрий Николаевич

Спичекова Наталья Викторовна

ТЕОРИЯ НОРМ СИНДРОМОВ. ПОСОБИЕ ДЛЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

УЧЕБНО-МЕТОДИЧЕСКОЕ ПОСОБИЕ

Редактор *И. П. Острикова*
Корректор *А. В. Бас*

Подписано в печать 05.01.2013. Формат 60x84 1/16. Бумага офсетная. Гарнитура «Таймс».
Отпечатано на ризографе. Усл. печ. л. 5,7. Уч.-изд. л. 4,9. Тираж 200 экз. Заказ 130.

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