УДК 004.6

СВОЙСТВА И ДЕКОДИРОВАНИЕ РЕВЕРСИВНЫХ КОДОВ С КОНСТРУКТИВНЫМ РАССТОЯНИЕМ 5

В. А. Липницкий
доктор технических наук, профессор
Военная Академия Республики Беларусь
А. В. Кушнеров
аспирант
Белорусский государственный университет

В работе исследованы наиболее важные свойства реверсивных кодов и некоторые подходы к вычислению их кодового расстояния, особенности теории норм синдромов для не примитивных реверсивных кодов, корректирующие возможности этих кодов в диапазоне длин от 7 до 230. Коррекция ошибок норменным методом продемонстрирована на примере реверсивного кода длиной 49.

Ключевые слова: помехоустойчивые коды, минимальное расстояние кода, реверсивные коды, коды-БЧХ, норменный метод декодирования.

Введение

Защита информации от помех – важнейшая задача при ее передаче и хранении, которые неизбежны в условиях агрессивно воздействующей среды. С каждым шагом вперед в развитии цифровых технологий эта задача приобретает все большую актуальность. Для решения проблемы зашумления информации в цифровых инфокоммуникационных системах (ИКС) существует надежный метод, который называют помехоустойчивым кодированием. С теоретической точки зрения – это область прикладной математики, которая развивается на протяжении более полувека, давая миру все новые и более мощные средства для противостояния помехам в каналах передачи информации.

В основе помехоустойчивого кодирования лежит теорема К. Шеннона (1948 г.), о том, что введением избыточности в передаваемый блок цифровой информации можно добиться исправления возникающих в ней ошибок любой сложности.

Исторически первые конкретные методы введения этой избыточности были предложены Робертом Хеммингом в начале 50-х гг. XX в. Им же заложены и основы теории линейных помехоустойчивых кодов [1]. В дальнейшем они приобрели наибольшую популярность как в теории, так и на практике, благодаря опоре на язык линейной алгебры.

Линейный двоичный код есть k-мерное подпространство в n-мерном пространстве векторов с коэффициентами из $Z/2Z$. Величину n называют длиной

кода. Весь спектр кодовых слов получается умножением информационных k-мерных векторов на порождающую $k \times n$-матрицу G.

Эффективность работы линейного кода определяется, в первую очередь, количеством ошибок, которое он способен исправить в каждом передаваемом блоке-сообщении. Количество исправляемых ошибок зависит от его минимального расстояния d – наименьшего из расстояний между векторами кода в смысле метрики Хемминга. Зависимость проста: если код длиной n имеет минимальное расстояние $d = 2t+1$ или $d = 2t+2$, то этот код способен исправить до t ошибок в каждом передаваемом блоке-сообщении длиной n [2].

К XXI в. разработан широкий спектр различных помехоустойчивых кодов (см., к примеру, [2]). Наибольшее применение, особенно в высокоскоростных ИКС, приобрело семейство кодов Боуза-Чоудхури-Хоквингема (БЧХ-кодов). Разработанная белорусской школой помехоустойчивого кодирования теория норм синдромов (ТНС) [3, 4] на порядок ускоряет синдромные методы коррекции ошибок, предоставляет норменные методы коррекции ошибок, вес которых выходит за рамки конструктивных ограничений. Эта возможность открыла путь к изучению не примитивных кодов Хемминга, БЧХ-кодов, реверсивных кодов, для которых как раз и имеют место неожиданные всплески минимального расстояния за конструктивные пределы (см. [5–9]).

В данной работе с единых позиций строится теория реверсивных кодов с конструктивным расстоянием 5, систематизируются разрозненные сведения о них, развивается для них теория норм синдромов, норменный метод коррекции ошибок не примитивными реверсивными кодами.

Коды Хемминга и коды БЧХ

Пожалуй, самый известный пример линейного помехоустойчивого кода – код Хемминга. Являясь составным кирпичиком многих иных линейных кодов, в наши дни линейный код Хемминга длиной n однозначно определяется своей проверочной матрицей

$$H = \left(1,\ \alpha,\ \alpha^2,\ \ldots\ ,\ \alpha^{n-1}\right), \qquad (1)$$

где α – примитивный элемент поля Галуа $GF(2^m)$ [1–3]. В этой матрице $n = 2^m-1$, каждый элемент α^i представляет собой столбец из m двоичных элементов – координат вектора α^i в базисе $\alpha^{m-1}, \alpha^{m-2},\ldots, \alpha, 1$. Здесь $k = n - m$. Заданный таким образом код, вообще говоря, отличается от кода Хемминга [1], но лишь перестановкой координат, и следовательно, эквивалентен ему, но приобретает при этом весьма важное свойство цикличности [2].

Коды Хемминга – совершенные коды с минимальным расстоянием 3, а потому исправляющие лишь одну ошибку на передаваемый блок-сообщение. Метод исправления этой ошибки действительно совершенен: синдром ошибки совпадает с тем столбцом матрицы H, номер которого совпадает с номером ошибочной координаты блока-сообщения.

В поисках подходов к увеличению количества исправляемых ошибок, в начале 60-х гг. XX в. Р. Боузом, Д. Чоудхури и А. Хоквингемом на основе кодов

Хемминга впервые были разработаны линейные коды, конструктивно способные исправлять, в принципе, любое количество случайных ошибок. Наиболее популярные как в теории, так и в приложениях примитивные циклические БЧХ-коды, длиной $n = 2^m - 1$ и с конструктивным расстоянием $\delta = 2t + 1$ задаются, по аналогии с (1), проверочными матрицами

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

при условии, что $tm < n$ [2-4]. Реальное минимальное расстояние этих кодов $d \geq \delta$. Примитивные БЧХ-коды хорошо изучены, их корректирующие возможности, как правило, остаются в рамках конструктивных ограничений.

Формальное определение не примитивных БЧХ-кодов получается заменой в формуле (2) параметра α на $\beta = \alpha^z$, где $z = \dfrac{2^m - 1}{n}$ для делителя n числа $2^m - 1$. При этом число m – наименьшее из всех натуральных k с условием: $2^k - 1$ делится на k.

Белорусская школа помехоустойчивого кодирования проводит интенсивное исследование свойств не примитивных БЧХ-кодов и кодов Хемминга (см., к примеру, [5–9]). Интерес к ним обусловлен, прежде всего, тем, что их минимальное расстояние может принимать значения, существенно превосходящее конструктивные значения. Об этом свидетельствует, к примеру, код Голея, полностью совпадающий, как доказано в [4], стр. 151–152, с БЧХ-кодом длиной 23 и конструктивным расстоянием 3. Также следует упомянуть о не примитивных кодах Хемминга длиной 47 (его минимальное расстояние $d = 11$ и длиной 79, кодовое расстояние которого $d = 15$.

В [9] доказано, что коды Хемминга с параметрами $n = p = 8t \pm 1$ – простое число, $m = \dfrac{p-1}{2}$, относятся к одному из четырех классов квадратично-вычетных кодов. Один из основных результатов теории КВ-кодов [2] гласит, что их минимальное расстояние $d \geq \sqrt{p}$. Отсюда следует, что минимальное расстояние не примитивных кодов Хемминга в общем не ограничено сверху

Реверсивные коды

Реверсивные помехоустойчивые коды конструктивно относятся к классу БЧХ-кодов. Они были незаслуженно обделены вниманием исследователей – пробел, в некоторой степени ликвидируемый данной работой.

Всякий двоичный реверсивный код C_R определен над своим полем Галуа $GF(2^m)$ из 2^m элементов, $m > 2$, имеет нечетную длину n, являющуюся делителем числа $2^m - 1$, и размерность, равную $k = n - 2m$. На выбор m накладываются те же ограничения, что и в кодах Хемминга. Код C_R однозначно задается своей проверочной матрицей

$$H_R = \left(\beta^i, \beta^{-i}\right)^T; \qquad (3)$$

$0 \le i \le n-1$, $2m < n$, $\beta = \alpha^z$ для примитивного элемента α поля Галуа $GF(2^m)$, $z = \frac{2^m - 1}{n}$. При $n = 2^m - 1$, величина $\beta = \alpha$, и код C_R называется примитивным. В противном случае код называется не примитивным. Код получил название реверсивного потому, что во второй строке проверочной матрицы стоят элементы первой, но в обратном порядке.

Априори, реверсивный код может существовать на любой нечетной длине. Но из рассмотрения следует исключить случаи, когда $2m > n$. В дальнейшем исключаем из рассмотрения также коды размерностью 1, для них $n - 2m = 1$. Такие коды существуют только в теории, так как передают лишь два слова, а, следовательно, не применяются на практике.

Также следует исключить из рассмотрения случаи, когда β и β^{-1} являются корнями одного и того же неприводимого полинома, случаи, когда ранг матрицы (2) равен m в силу теоремы 6.3 [3], и, следовательно, реверсивный код сводится к коду Хемминга. Подобные случаи удобно отслеживать с помощью циклотомических классов. Циклотомический класс $C(i) = \{i, 2i, 4i, \ldots\}$ – это совокупность степеней всех корней неприводимого полинома $M(\beta^i, x)$, выраженных как степени β^i с помощью автоморфизма Фробениуса поля Галуа $GF(2^m)$. Таким образом, β и β^{-1} принадлежат одному неприводимому полиному тогда и только тогда, когда 1 и $n-1$ лежат в одном циклотомическом классе. Построив циклотомические классы для каждой длины $n > 2m$, оставляем для дальнейшего рассмотрения те, на которых реверсивный код действительно существует, то есть для которых $n > 2m$ и $n - 1$ не принадлежит циклотомическому классу $C(1) = \{1, 2, 4, \ldots\}$.

Сформулируем и докажем одно интересное утверждение о циклотомических классах.

Теорема 1. Для значений $n = 2^m - 1$, $m \ge 3$ (для примитивных кодов), степени 1 и 3, а также 1 и –1 (или $n-1$) лежат в разных циклотомических классах.

Доказательство: Очевидно, что 1 всегда принадлежит классу C(1) по определению. Рассмотрим структуру класса $C(1)$: $C(1) = \{1, 2, \ldots 2^i\}$, иными словами, класс состоит из степеней числа 2, взятых по модулю n. Покажем, что $2^i \ne 3 \left(\mathrm{mod}\left(2^m - 1\right)\right)$, $\forall i : 0 \le i \le 2^m - 2$, $m \ge 3$. Запишем следующее тождество: $2^m = 1*(2^m - 1)+1$; далее переходим к сравнению по модулю $2^m - 1$: $2^m \equiv 1 \left(\mathrm{mod}\left(2^m - 1\right)\right)$. Получаем, что в мультипликативной группе кольца вычетов $Z/(2^m-1)Z$ порядок 2 равен m, следовательно, $C(1) = \{1, 2, \ldots 2^i\}, 0 \le i \le m-1$ будет циклической подгруппой порядка m относительно умножения в $\left(Z / \left(2^m - 1\right) Z\right)^*$. Значит, в циклотомическом классе $C(1)$ будут лишь элементы, которые являются степенями 2, число 3 не представимо в таком виде, и не будет принадлежать тому же классу, что и степень 1.

То же можно сказать и о степени n–1 = 2^m–2 = 2(2^{m-1}–1). Как видно, для $m \geq 3$ n–1 не является степенью числа 2, а значит, не может лежать в одном классе с 1. Теорема доказана.

Заметим, что на не примитивных длинах теорема 1 не справедлива – существуют $n \neq 2^m - 1$, для которых $C(n-1) = C(1)$. Вот их список в диапазоне от 7 до 500: 17, 41, 43, 97, 109, 113, 137, 157, 193, 229, 241, 251, 257, 277, 281, 283, 307, 313, 331, 353, 397, 401, 409, 433, 449, 457, 499. Все реверсивные коды на перечисленных длинах не существуют, они совпадают с кодами Хемминга на тех же длинах.

Отдельно стоит сказать, что для некоторых значений n, величины n–1 и 3 лежат в одном циклотомическом классе, откуда следует, что реверсивный код на этих длинах совпадает с кодом семейства БЧХ, который задается проверочной матрицей $H = \left(\beta^i,\ \beta^3\right)^T$. Список этих длин n в диапазоне от 7 до 500: 35, 49, 55, 77, 175, 203, 245, 247, 259, 295, 319, 343, 371, 385, 395, 413, 415, 439. Исследование реверсивных кодов на указанных длинах адресуется к соответствующим БЧХ-кодам.

Итогом вышеизложенного можно считать табл. 1, где приведен список всех реверсивных кодов в диапазоне длин n от 7 до 230 с параметрами k и m, перспективными для дальнейших исследований. Их оказалось 51.

Таблица 1. Параметры всех реверсивных кодов длиной n, $7 \leq n < 230$

n	m	k	n	m	k
15	4	7	129	14	101
21	6	9	133	18	97
31	5	21	135	36	63
35	12	11	141	46	49
39	12	15	143	60	23
45	12	21	147	42	63
49	21	7	151	15	121
51	8	35	153	24	105
55	20	15	155	20	115
63	6	51	159	52	55
69	22	25	161	33	95
73	9	55	165	20	125
75	20	35	175	60	55
77	30	17	183	60	63
85	8	69	187	40	107
87	28	31	189	18	153
89	11	67	195	12	171
91	12	67	203	84	35
93	10	73	207	66	75
95	36	23	213	70	73
105	12	81	215	28	159
111	36	39	217	15	187
115	44	27	219	18	183
117	12	93	221	24	173

Окончание табл. 1

n	m	k	n	m	k
119	24	71	223	37	149
123	20	83	225	60	105
127	7	113			

Далее следует оценить корректирующие возможности найденных реверсивных кодов – необходимо для каждого кода отыскать его минимальное расстояние. Здесь имеют место некоторые теоретические результаты.

Теорема 2. Минимальное расстояние d кода C_R находится в диапазоне $3 \le d \le s$, где s – наименьший натуральный делитель длины кода n. Если длина кода C_R кратна 3, то код имеет минимальное расстояние 3.

Доказательство следует из того факта, что элементы $1, \beta, \beta^2, \ldots, \beta^{n-1}$ образуют циклическую подгруппу $<\beta>$ порядка n в мультипликативной группе $GF\left(2^m\right)^*$ поля Галуа $GF(2^m)$. Для каждого делителя s числа n и числа $\mu = n/s$ элемент β^μ образует циклическую подгруппу $<\beta^\mu>$ порядка s в группе $<\beta>$. Сумма всех элементов этой подгруппы в поле $GF(2^m)$ равна нулю, как несложно видеть. Рассмотрим двоичный вектор $\bar{x}$ с n координатами, из которых s координат равны 1, а именно координаты, номера которых совпадают с номерами элементов $\beta^{\mu i}$ в матрице (3), а остальные равны 0. Легко видеть, что $H_R \cdot \bar{x}^T = \bar{0}$. Из этого равенства следует, что вектор $\bar{x}$ весом s принадлежит коду C_R. Отсюда и вытекает доказательство теоремы 2.

Следствие. Примитивный реверсивный код C_R длиной $n = 2^{2\mu} - 1$ имеет минимальное расстояние 3.

Доказательство. Пусть $m = 2\mu$ – четно. Тогда $n = 2^{2\mu} - 1 = (2^\mu - 1) \cdot (2^\mu + 1)$. Среди трех последовательных натуральных чисел $(2^\mu - 1), 2^\mu, (2^\mu + 1)$ непременно найдется делящееся на три. Этим числом заведомо не является 2^μ. Следовательно, или $2^\mu - 1$, или $2^\mu + 1$ обязательно поделится на 3. Таким образом, $2^{2\mu} - 1 = 3q$ для подходящего натурального q. Остальное непосредственно вытекает из теоремы 2.

Отметим, что данное следствие иным путем было доказано ранее Дзенгом и Хартманом [10]. Им же принадлежит и ослабленный вариант следующего утверждения.

Теорема 3. При нечетных значениях $m = 2\mu + 1$ примитивный реверсивный код C_R длиной $n = 2^m - 1$ имеет минимальное расстояние 5.

Доказательство. Пусть $m = 2\mu + 1$ – нечетно. Среди трех последовательных натуральных чисел $(2^{2\mu+1} - 1), 2^{2\mu+1}, (2^{2\mu+1} + 1)$ одно и только одно делится на три. В силу формулы сокращенного умножения: $(2^{2\mu+1} + 1) = (2 + 1)(2^{2\mu} - 2^{2\mu-1} + \ldots - 1)$, таковым является третье из названных. Значит, $2^{2\mu+1} - 1$ на 3 не делится.

Любые два столбца матрицы (3) попарно различны. Поэтому предположим, что в коде C_R длиной $n = 2^{2\mu+1} - 1$ найдутся три столбца с нулевой двоичной сум-

мой. Это означает наличие трех ненулевых и попарно различных элементов $x, y, z \in GF(2^{2\mu+1})$, таких, что

$$\begin{cases} x+y+z=0; \\ \dfrac{1}{x}+\dfrac{1}{y}+\dfrac{1}{z}=0. \end{cases} \tag{4}$$

Из (4) следует, что $\begin{cases} x+y=z; \\ \dfrac{y+x}{xy}+\dfrac{1}{z}=0; \end{cases}$ или $\begin{cases} z=x+y; \\ z^2=xy. \end{cases}$

Из последней системы следует, что $(x+y)^2 = xy$ или $x^2 + y^2 = xy$, что равносильно равенству $t^2+t+1=0$ для $t=\dfrac{x}{y}\neq 1$, поскольку $x \neq y$. Умножим обе части уравнения $t^2+t+1=0$ на $t-1$. Получим уравнение $t^3-1=0$. Так как t является ненулевым элементом поля $GF(2^{2\mu+1})$, то $t=\alpha^s$ для примитивного элемента $\alpha \in GF(2^{2\mu+1})$ и некоторого целого $s, 1 \le s < 2^{2\mu+1}-1=n$. Тогда $t^3=\alpha^{3s}=1$. Минимальная степень α, равная 1, есть степень $n=2^{2\mu+1}-1$. Отсюда следует, что $3s=n=2^{2\mu+1}-1$ или $3s=2n=2(2^{2\mu+1}-1)$, чего быть не может, поскольку $n=2^{2\mu+1}-1$ не может делиться на 3 в силу леммы 1.

Лемма 1. Длина $n=2^m-1$ примитивного реверсивного кода делится на 3 тогда и только тогда, когда $m=2\mu$ – четно.

Следовательно, система (4) не может иметь решений, а, следовательно, минимальное расстояние кода C_R длиной $n=2^{2\mu+1}-1$ больше или равно 4.

Предположим, что в проверочной матрице кода C_R длиной $n=2^{2\mu+1}-1$ найдутся четыре столбца с нулевой двоичной суммой. Это означает наличие четырех ненулевых и попарно различных элементов $x, y, z, t \in GF(2^{2\mu+1})$, таких, что

$$\begin{cases} x+y+z+t=0; \\ \dfrac{1}{x}+\dfrac{1}{y}+\dfrac{1}{z}+\dfrac{1}{t}=0. \end{cases} \tag{5}$$

Из (5) следует, что $\begin{cases} x+y=z+t; \\ \dfrac{y+x}{xy}=\dfrac{z+t}{zt}; \end{cases}$ или $\begin{cases} z+t=x+y=a; \\ zt=xy=b \end{cases}$ для некоторых ненулевых $a, b \in GF(2^{2\mu+1})$. Отсюда следует, что 4 различных элемента $x, y, z, t \in GF(2^{2\mu+1})$ являются корнями одного квадратного уравнения $u^2+au+b=0$, чего, разумеется, быть не может. Следовательно, минимальное расстояние кода C_R длиной $n=2^{2\mu+1}-1$ больше или равно 5.

Предположим, что в проверочной матрице в коде C_R длиной $n=2^{2\mu+1}-1$ найдутся пять столбцов с нулевой двоичной суммой. Это означает наличие пяти ненулевых и попарно различных элементов $x, y, z, t, u \in GF(2^{2\mu+1})$, таких, что

$$\begin{cases} x+y+z+t+u=0; \\ \frac{1}{x}+\frac{1}{y}+\frac{1}{z}+\frac{1}{t}+\frac{1}{u}=0 \end{cases} \quad \text{или} \quad \begin{cases} x+y+z+t+u=0; \\ yztu+xztu+xytu+xyzu+xyzt=0. \end{cases} \qquad (3)$$

В силу следствия 1 из теоремы 3 [12] система (3) имеет нетривиальные решения, то есть хотя бы с одной ненулевой координатой. Однако наличие решения с хотя бы одной нулевой или двумя одинаковыми координатами, привело бы к решению предыдущей системы, но с меньшим числом переменных. Вышеприведенные рассуждения показывают, что этого быть не может. Следовательно, гарантированное решение системы (3) должно иметь все отличные от нуля и попарно различные координаты. Все сказанное в совокупности означает, что в проверочной матрице реверсивного кода действительно имеются пять различных столбцов с нулевой двоичной суммой. Отсюда следует, что искомое минимальное расстояние кода равно 5.

Теорема 3 полностью доказана.

Таким образом, реверсивные коды с длинами, делящимися на 3, не представляют практического интереса, их следует удалить из дальнейшего рассмотрения.

Из оставшихся в табл. 1 кодов удалим также и коды с длинами, делящимися на 5, поскольку у них $d \le 5$. Для кодов C_R с $d = 5$ методики декодирования хорошо разработаны и уже не представляют научного интереса.

Таблица 2 содержит параметры (n, m, k) реверсивных кодов из табл. 1, кодовое расстояние которых может быть больше 5.

Таблица 2. Перспективные реверсивные коды с длинами в диапазоне от 31 до 230

n	m	k	N	m	k
49	21	7	151	15	121
73	9	55	161	33	95
77	30	17	187	40	107
89	11	67	203	84	35
91	12	67	217	15	187
119	24	71	221	24	173
133	18	97	223	37	149
143	60	23			

Таблица 2 содержит лишь 15 кодов, минимальное расстояние которых имеет перспективу принять значение, больше 5. Для них значение этого параметра необходимо устанавливать с привлечением компьютерных вычислений при сочетании нескольких методов.

Одним из базовых является метод вычисления минимального расстояния по определению. Находя ядро проверочной матрицы кода C_R, мы получим базис кода из $n - 2m$ векторов, далее непосредственным перебором кодовых слов необходимо отыскать кодовое слово минимального веса. Метод перебора не слишком эффективен, так как с увеличением значений параметров n, m экспоненциально растет сложность вычислений. Однако метод нашел применение при вычислении кодового расстояния на длинах 45, 149, 203. На диапазоне длин

от 73 до 119 неплохо работает синдромный метод вычисления минимального расстояния, базирующийся на теореме о рангах систем столбцов проверочной матрицы [2]. Для длин, превышающих 119, целесообразно применять норменный метод [3], а также метод G-орбит для подгруппы G группы автоморфизмов кода C_R, порожденной циклическими и циклотомическими подстановками [4]. В результате скрупулезных вычислений были получены точные значения минимальных расстояний, представленные в табл. 3

Таблица 3. Корректирующие возможности наиболее перспективных реверсивных кодов

Длина кода	Размерность поля определения	Размерность кода	Минимальное расстояние кода Хемминга на заданной длине	Минимальное расстояние реверсивного кода
49	21	7	3	7
73	9	55	3	6
77	30	17	3	7
89	11	67	4	7
91	12	67	3	6
119	24	71	3	5
133	18	97	3	8
143	60	23	11	11
151	15	121	5	8
161	33	95	3	7
187	40	107	5	5
203	84	35	3	7
217	15	187	3	5
221	24	173	3	5
223	37	149	9	<=21

Норменное декодирование реверсивных кодов

Теория норм синдромов и норменный метод декодирования [3–4] эффективно работают с примитивными БЧХ-кодами и реверсивными кодами. Рассмотрим специфику применения данного метода при декодировании ошибок не примитивными реверсивными кодами.

Вектора ошибок для кода длиной n имеют вид $\bar{e} = (i_1, i_2, \ldots, i_k)$. Данная запись означает, что в векторе ошибки $\bar{e}$ длиной n на позициях $i_1, i_2, \ldots, i_k$ находятся 1, а на остальных 0. На данном множестве векторов-ошибок рассматривается операция циклического сдвига σ. Пусть $\bar{e} = (e_1, e_2, \ldots, e_n)$, тогда $\sigma(\bar{e}) = \sigma(e_1, e_2, \ldots, e_n) = (e_n, e_1, e_2, \ldots, e_{n-1})$. Введем понятие Г-орбиты вектора ошибки [3].

Определение 1: 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-орбиты имеют четкую структуру, которую описывает

Теорема 4 [3. 4]. 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

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

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.

Синдром $S(\bar{e})$ вектора-ошибки $\bar{e}$ есть произведение проверочной матрицы кода на вектор ошибки: $S = H\bar{e}^T$. Синдромы векторов-ошибок в коде C_R в силу структуры их проверочной матрицы состоят из двух компонент: $S(\bar{e}) = (s_1, s_2)$; $s_1, s_2 \in GF(2^m)$. Известно, что синдромы векторов-ошибок весом 1, 2,..., t в коде с минимальным расстоянием $d = 2t+1$ попарно различны. Этот факт служит основой синдромных методов коррекции ошибок.

В реверсивном коде синдромы каждой Г-орбиты имеют четко очерченную структуру (см. [3, 4]).

Теорема 5. Если в коде C_R синдром $S(\bar{e}) = (s_1, s_2)$, то $S(\sigma(\bar{e})) = \left(\beta s_1, \beta^{-1} s_2\right)$,

Теорема 5 подсказывает следующее определение нормы синдрома ошибки для реверсивного кода.

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

$$N(S) = s_1 \cdot s_2.$$

Из определения 2 и теоремы 5 вытекает

Теорема 6. В реверсивном коде C_R с проверочной матрицей (3) норма синдрома не зависит от циклических сдвигов координат векторов-ошибок: для всякого вектора ошибок $\bar{e}$ и его синдрома $S(\bar{e})$ справедливо равенство

$$N(S(\sigma(\bar{e}))) = N(S(\bar{e})).$$

Это означает, что в рамках одной орбиты норма будет одинакова, а следовательно, нормой Г-орбиты можно назвать норму синдрома любого вектора ошибки, в нее входящего.

Теорема 7. Нормы Г-орбит всех векторов-ошибок весом 1, 2,..., t в примитивном коде C_R с минимальным расстоянием $d = 2t+1$ или $d = 2t+2$ попарно различны. В не примитивном коде C_R с теми же условиями может существовать до z различных Г-орбит векторов-ошибок весом 1, 2,..., t с одинаковыми нормами.

Пример 1. Рассмотрим реверсивный код C_R с проверочной матрицей (3) длиной 49. Он определен над полем $GF(2^{21})$. Здесь $z = 42799$. Из табл. 3 следует, что данный код имеет минимальное расстояние 7 и, следовательно, корректирует все случайные ошибки весом 1 – 3. Из них одиночные образуют одну

Г-орбиту, двойные – 24 Г-орбиты, тройные – 376, всего 401 полная Г-орбита.

Как уже отмечалось выше, синдромы всех перечисленных ошибок попарно различны. Компьютерные расчеты показали, что нормы 401 Г-орбиты составляют спектр из 225 значений. Значит, в приведенном списке из 401 Г-орбиты имеются орбиты с одинаковыми значениями их норм. Особенность данного примера в том, что из 225 значений нормы 176 повторяются, причем по одному разу. Иными словами, 176 пар Г-орбит имеют по одинаковой норме, оставшиеся 49 орбит имеют уникальные значения норм. Еще одна специфическая особенность данного примера в том, что совпадения значений норм наблюдаются лишь в классе тройных ошибок. Следовательно, из 49 Г-орбит с уникальными нормами 25 одинарных и двойных и 24 тройных.

Для декодирования ошибок норменным методом следует иметь 3 списка: список 1 образующих $\bar{e}_i$ Г-орбит декодируемой совокупности, список 2 синдромов $S(\bar{e}_i)=(s_{1,i},s_{2,i})$ образующих и список 3 норм $N_i = N(S(\bar{e}_i))$ Г-орбит этой же совокупности. Если ИКС с данным кодом C_R приняла блок-сообщение $\bar{x}$, то она автоматически вычисляет синдром ошибок этого сообщения по формуле $S(\bar{x}) = H.\bar{x}^T = (s_1, s_2) = (\alpha^i, \alpha^j)$ для фиксированного примитивного элемента α поля $GF(2^m)$. Если $S(\bar{x}) \neq \bar{0}$, то вычисляем норму синдрома $N^* = N\left(S\left(\bar{x}\right)\right) = s_1 * s_2 = \alpha^{i+j}$. Вычисленная норма N^* сравнивается со списком 3. Пусть эта норма совпадает с нормой N_l списка 3. Далее возможны два варианта действий в зависимости от уникальности нормы N_l. Предположим, что норма N_l уникальна (что характерно для всех примитивных реверсивных кодов). Вычисляем целое число $\tau = (i - \deg(s_{1,l}))/z$. Тогда сообщение $\bar{x} = \bar{c} + \bar{e}$, где $\bar{e} = \sigma^{(\tau) \bmod n}(e_l)$ и истинное сообщение вычисляется по формуле: $\bar{c} = \bar{x} + \bar{e}$.

Пусть норма N_l не уникальна, то есть $N^* = N_{l[1]} = N_{l[2]} = \ldots = N_{l[h]}$. Тогда вычисляем h значений $\tau(l[\mu]) = (i - \deg(s_{1,l[\mu]}))/z$. В силу теоремы 5 только для одного из значений $l[\mu]$ эта величина будет целым числом. Пусть для определенности это значение совпадает с $l[1]$. Искомая ошибка $\bar{e}$ в принятом сообщении $\bar{x}$ вычисляется по формуле $\bar{e} = \sigma^{(\tau(l[1])) \bmod n}(e_{l[1]})$.

Пример 2. Продемонстрируем работу норменного декодера на примере не примитивного реверсивного кода C_R длиной 49, исследованного в примере 1.

Пусть ИКС с кодом C_R приняла следующее сообщение:

$\bar{x}$ = (0,0,0,1,1,0,0,0,0,1,0,1,0,0,0,0,1,0,1,0,0,0,0,0,0,1,0,0,0,0,0,0,1,0,0,0,0,0,0,1,0,0,0,0,0,0,1,0,0,0,0,0,0,1,0,0).

Вычислим синдром ошибки в принятом сообщении по формуле $S(\bar{x}) = H.\bar{x}^T$. Имеем: $S(\bar{x}) = (\alpha^{929465}, \alpha^{1668303})$. Вычисляем норму синдрома $N(S(\bar{x})) = \alpha^{500617}$. Далее определяем согласно списку норм соответствующие Г-орбиты. Данному значению нормы соответствуют две различные Г-орбиты с образующими: $\bar{e}_1 = (1,7,14)$ и $\bar{e}_2 = (1,7,43)$. Синдромы образующих равны соответственно:

$$S(\bar{e}_1) = (\alpha^{801068}, \alpha^{1796700}) \text{ и } S(\bar{e}_2) = (\alpha^{2053494}, \alpha^{544274}).$$

Вычисляем $\tau(1) = \frac{929465 - 801068}{42799} = 3$; $\tau(2) = \frac{929465 - 2053494}{42799} = -26{,}263$ – величина дробная. Искомый вектор-ошибку находим по формуле $\bar{e} = \sigma^3(e_1) = (4,10,17)$. В двоичном виде получаем искомый вектор-ошибку длиной 49 и весом три

$\bar{e} = (0,0,0,1,0,0,0,0,0,1,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)$.

Прибавив полученный вектор ошибки к принятому сообщению, получим верное кодовое слово:

$w = (0,0,0,0,1,0,0,0,0,0,0,1,0,0,0,0,0,0,1,0,0,0,0,0,0,1,0,0,0,0,0,0,1,0,0,0,0,0,0,1,0,0,0,0,0,0,1,0,0,0,0,0,0,1,0,0)$.

В принятом сообщении исправлена тройная ошибка.

Заключение

Разработаны основы теории и общий подход к исследованию реверсивных кодов с конструктивным расстоянием 5, как примитивных, так и не примитивных. Установлены общие свойства и различия между двумя названными классами кодов. Получены теоретически или вычислены точные значения минимального расстояния для реверсивных помехоустойчивых кодов в диапазоне длин от 7 до 230. Некоторые результаты были изложены ранее в [11]. Наилучшими корректирующими возможностями обладает код C_R на длине 143, этот представитель реверсивных кодов способен исправлять до 5 ошибок в сообщении. Также следует отметить код C_R длиной 49, который способен корректировать до 3 ошибок в передаваемом сообщении.

Норменный метод коррекции ошибок развит на не примитивные реверсивные коды. Представлен пример исправления тройной ошибки норменным методом с помощью реверсивного кода с минимальным расстоянием 7.

Если сравнивать реверсивные коды с БЧХ-кодами с конструктивным расстоянием 5 на тех же длинах, которые имеют проверочную матрицу $H = \left(\beta^i, \beta^{3i}\right)^T$, то реверсивные коды ведут себя заметно мягче. Всплески минимальных расстояний, характерные для не примитивных БЧХ-кодов, в реверсивных кодах проявляются в гораздо меньшей степени.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. ***Хемминг, Р. В.*** Коды с обнаружением и исправлением ошибок / Р. В. Хемминг. – М. : ИЛ, 1956. – 356 с.
2. ***Мак-Вильямс, Ф. Дж.*** Теория кодов, исправляющих ошибки./ Ф. Дж. Мак-Вильямс, Н. Дж. А. Слоэн. – М. : Радио и связь, 1979. – 744 с.
3. ***Липницкий, В. А.*** Теория норм синдромов. / В. А. Липницкий – Минск : БГУИР, 2010. – 108 с.
4. ***Липницкий, В. А.*** Норменное декодирование помехоустойчивых кодов и алгебраические уравнения / В. А. Липницкий, В. К. Конопелько. – Минск : Издательский центр БГУ, 2007. – 214 с.
5. ***Lipnitski, V.*** Non-primitive Hamming Codes, p. 73–75. Modeling and Simulation: MS'2012; Proc. of the Intern. Conf., 2–4 May 2012, Minsk, Belarus. – Minsk : Publ. Center of BSU, 2012. – 178 p.
6. ***Липницкий В. А., Михайловский Е. Б.*** Определение реальных корректирующих возможностей не примитивных кодов Хемминга. – 17-я МНТК "Современные средства связи", Минск, 16–18 октября 2012 г. Материалы МНТК, Минск : УО "Высший государственный колледж связи", 2012. – С. 173.
7. ***Липницкий В. А., Олексюк А. О.*** Реализация декодера не примитивного кода Хемминга с помощью метода сжатия орбит. / "Современные информационные компьютерные технологии mcIT-2013" : материалы III Международной научно-практической конференции [Электронный ресурс] / УО "Гр. ун-т им. Я. Купалы". – Гродно, 2013. – 1 электр. компакт диск (CD-R). – 792 с. – Рус. – Деп. в ГУ "БелИСА" 19.09.13, № Д 201315.
8. ***Липницкий В. А., Олексюк А. О.*** О коррекции кратных ошибок не примитивными кодами Хемминга / Международная научно-практическая конференция "Молодежь в науке – 2013" г. Минск, 19–22 ноября 2013 г. Материалы международной научно-практической конференции. – Минск : НАН РБ, 2013. – С. 616–619.
9. ***Липницкий В. А., Олексюк А. О.*** Оценка минимальных расстояний не примитивных кодов Хемминга / Весці НАН Беларусі, серыя фізіка-тэхнічных навук. – 2015. – № 2. – С. 103–110.
10. ***Tzeng K. K., Hartman C.R.P.*** On the minimum distance of certain reversible cyclic codes / IEEE Trans. on Info. Theory. – 1970. – Vol. IT-16, № 5. – P. 644–646.
11. ***Липницкий В. А., Кушнеров А. В.*** Свойства непримитивных реверсивных кодов: материалы международной научной конференции ITS – 2014, Минск, 29 октября 2014 / БГУИР ; под ред. Д. П. Кукин [и др.]. – Минск, 2014. – С. 276–277.
12. ***Серр, Ж.-П.*** Курс арифметики / Ж.-П. Серр. – М. : Мир, 1972. – 184 с.

Поступила в редакцию 01.06.2016 г.

Контакты: valipnitski@yandex.ru (Липницкий Валерий Антонович)
al.v.kushnerov@gmail.com (Кушнеров Александр Викторович)

Lipnitsky V. A., Kushnerov A. V. REVERSE CODES WITH CONSTRUCTIONAL DISTANCE 5 AND DECODING.

In the article the most important properties of reverse codes and some ways to assess their minimal distance are displayed. Some features of the theory of syndrome norms for non-

primitive reverse codes and correction possibilities of these codes in length from 7 to 230 are represented. The norm correction method is exemplified by means of the code with length 49.

Key words: error correcting codes, code minimal distance, reverse codes, bch codes, norm method of error correction.