УДК 004.6

НЕКОТОРЫЕ СВОЙСТВА РЕВЕРСИВНЫХ ПОМЕХОУСТОЙЧИВЫХ КОДОВ

В.А. Липницкий, А.В. Кушнеров

В данной статье приведены наиболее важные свойства реверсивных кодов, изложены некоторые подходы к вычислению их кодового расстояния, исследованы корректирующие возможности этих кодов в диапазоне длин от 7 до 230. Выделены особенности, преимущества и недостатки реверсивных кодов.

Введение

Сегодня, в век информационных технологий остро стоит проблема передачи и хранения информации. Передача информации в современных каналах (за исключением оптоволоконных) сопряжена с разного рода шумами и помехами, что приводит к искажению передаваемой информации. Особенно актуален этот вопрос для беспроводных цифровых каналов передачи информации, популярность которых растет с каждым днем. Основным инструментом противостояния шумам и помехам в цифровых инфокоммуникационных системах (ИКС) является применение предварительного помехоустойчивого кодирования передаваемой информации.

Помехоустойчивое кодирование – раздел прикладной математики, который развивается на протяжении уже более полувека в русле основополагающей идеи К. Шеннона (1948 г.), согласно которой введением избыточности в передаваемый блок цифровой информации можно добиться исправления возникающих в ней ошибок любой сложности. Конкретные методы введения этой избыточности и получили название помехоустойчивого кодирования.

Наибольшую популярность в теории и практике получили линейные помехоустойчивые коды [1]. Эффективность работы линейного кода характеризуется, прежде всего, количеством ошибок, которое код способен исправить в передаваемом сообщении. В свою очередь количество исправляемых ошибок зависит от важного параметра кода – его минимального расстояния [1]. Зависимость эта 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 [1, 2].

Вычисление точного значения кодового расстояния на практике является трудоёмкой вычислительной задачей. Поэтому ее решение сочетает в себе различные методы и подходы [1, 2]. В данной работе подводятся некоторые итоги изучения свойств и корректирующих возможностей реверсивных кодов – одного из слабоизученных классов линейных кодов.

Коды Хемминга и коды-БЧХ

Пожалуй, самый известный пример линейного помехоустойчивого кода – код Хемминга. Данный линейный код длиной n однозначно определяется своей проверочной матрицей

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

где α – примитивный элемент поля Галуа $GF\left(2^m\right)$ [1 – 3]. Это 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.

Лишь в 2012 году в научный обиход было явно введено понятие не примитивных кодов Хемминга [4], хотя изучались они и ранее как крайний случай не примитивных БЧХ-кодов. Формальное определение не примитивных кодов Хемминга получается заменой в формуле (1) параметра α на $\beta=\alpha^z$ где $z=\frac{2^m-1}{n}$ 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 кодов Хемминга (см., к примеру, [5 – 8]). Интерес к ним обусловлен, прежде всего, тем, что их минимальное расстояние может принимать значения, существенно превосходящее значение 3. Об этом свидетельствует, к примеру, код Голея, полностью совпадающий, как доказано в [3], стр. 151 – 152, с БЧХ-кодом длиной 23 и конструктивным расстоянием 3. В табл. 1 приведены из [8] значения минимального расстояния d для ряда не примитивных кодов Хемминга. В этой таблице n - длина кода Хемминга, m – степень расширения поля определения кода над $Z/2Z$, k – размерность кода как векторного пространства над $Z/2Z$

Таблица 1. Некоторые коды Хемминга на длинах от 7 до 100

n	m	k	d	n	m	k	d
23	11	12	7	63	6	57	3
31	5	26	3	71	35	36	11
41	20	21	9	97	48	49	15
47	23	24	11				

В [8] доказано, что коды Хемминга с параметрами $n=p=8t\pm1$ простое, $m=\frac{p-1}{2}$ являются квадратично-вычетными кодами. Из теории КВ-кодов следует, что их минимальное расстояние $d\geq\sqrt{p}$. Отсюда следует, что минимальное расстояние не примитивных кодов Хемминга в общем не ограничено сверху.

В целях увеличения количества исправляемых линейными кодами ошибок, в 60-х годах XX века Боузом, Чоудхури и Хоквингемом на основе кодов Хемминга впервые были разработаны коды, способные конструктивно исправлять, в принципе, любое количество случайных ошибок. Естественно, их называют кодами Боуза-Чоудхури-Хоквингема или БЧХ-кодами. Это наиболее популярный класс линейных кодов как в теории, так и в приложениях [1 - 3]. Как и коды Хемминга, БЧХ-коды делятся на примитивные и не примитивные.

Хорошо изучены примитивные БЧХ-коды, корректирующие возможности которых, как правило, остаются в рамках конструктивных возможностей. Созданная на рубеже XX и XXI веков теория норм синдромов [2, 3] предоставляет перестановочные норменные методы коррекции ошибок, кратность которых существенно выходит за рамки конструктивных возможностей. Это обстоятельство привлекло внимание к не примитивным БЧХ-кодам, минимальное расстояние которых не поддаётся точным теоретическим оценкам и может быть неожиданно большим. В таблице 2 представлены вычисленные основные параметры и точные значения минимального расстояния ряда не примитивных БЧХ-кодов с конструктивным расстоянием $\partial = 5$ в диапазоне длин от 35 до 89.

Таблица 2. Минимальное расстояние некоторых не примитивных БЧХ-кодов с $\partial = 5$

Длина кода	Размерность поля	Размерность кода	Минимальное расстояние
35	10	15	10
43	14	15	13
49	21	7	7
57	18	21	14
89	11	67	7

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

Реверсивные помехоустойчивые коды

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

$$H = \left(\beta^i, \beta^{-i}\right)^T; \qquad (2)$$

$0 \le i \le n-1, 2m < n$, $\beta = \alpha^\tau$ для примитивного элемента α поля Галуа $GF(2^m)$, $\tau = \dfrac{2^m - 1}{n}$. При $n = 2^m - 1$, величина $\beta = \alpha$, и код C_R называется примитивным. В противном случае код называется не примитивным.

В данной работе систематически исследуются свойства реверсивных помехоустойчивых кодов, а также их корректирующие способности на длинах n в пределах от 7 до 230.

В силу теоретико-числовой теоремы Эйлера, для каждого нечётного значения n, существует своё поле определения $GF(2^m)$ с минимальным m, обеспечивающим делимость $2^m - 1$ на n. Размерность реверсивного кода определяется с помощью формулы $k = n - 2m$. Смысл этого параметра в следующем, если код C_R имеет размерность k, то он способен передавать 2^k слов. Следовательно, в случае, когда $2m > n$ рассмотрение кода в принципе не

имеет смысла. Отдельно стоит сказать о кодах с размерностью 1, для них $n-2m=1$. Такие коды существуют только в теории, так как передают лишь два слова, а, следовательно, не применимы на практике. Таким образом, коды C_R с параметрами (n,m), такими, что $n-2m\le 1$, мы исключаем из рассмотрения.

Также следует исключить случаи, когда β и β^{-1} являются корнями одного и того же неприводимого полинома, случая, 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 $M(\beta,x)$, выраженных как степени β с помощью автоморфизма Фробениуса поля Галуа. 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 $C(1)=\{1,2,4,\ldots\}$.

С учётом выше изложенного, в табл. 3 приведен список всех реверсивных кодов в диапазоне длин n от 7 до 230 с параметрами k и m, перспективными для дальнейших исследований.

Таблица 3. Возможные параметры реверсивных помехоустойчивых кодов.

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

Всего в табл. 3 оказалось 52 таких кодов. Для определения их корректирующих возможностей необходимо для каждого из них отыскать их минимальное (кодовое) расстояние.

Непосредственно проверяется, что для каждого натурального делителя s, $s>1$ числа $n-$длины кода C_R в этом коде найдётся кодовое слово веса s. Отсюда немедленно вытекает следующее утверждение.

Предложение 1. 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.

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

В табл. 3 представлены 4 примитивных реверсивных кода с длинами 15, 31, 63 и 127. Два из них имеют $d=3$, как доказано в предложении 1. И это справедливо для всех примитивных кодов C_R с четным $m=2\mu$, ибо в этом случае $2^{2\mu}-1=\left(2^{\mu}-1\right)\left(2^{\mu}+1\right)-$ делится на 3. Коды с длинами 31 и 127 имеют $d=5$. Это общий факт для всех примитивных кодов C_R с нечетным $m=2\mu+1$ (см. [1] или [9]).

Из оставшихся в табл. 3 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.

Табл. 4 содержит параметры (n,m,k) реверсивных кодов из табл. 3, кодовое расстояние которых может быть больше 5.

Таблица 4 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			

Табл. 4 содержит лишь 15 кодов, минимальное расстояние которых имеет перспективу принять значение, больше чем 5. Для них значение этого параметра необходимо устанавливать с привлечением компьютерных вычислений, сочетанием 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 растёт сложность вычислений. На больших (>50) длинах кодов следует прибегнуть к более эффективным методам. В основном, приходилось комбинировать следующие четыре метода: вычисление таблицы весов кода C_R или начального фрагмента этой таблицы; комбинаторный метод, базирующийся на теореме о рангах систем столбцов проверочной матрицы [1]; метод синдромов; норменный метод [3]; метод G-орбит для подгруппы G группы автоморфизмов кода C_R, порождённой циклическими и циклотомическими подстановками [3]. В результате скрупулёзных вычислений были получены точные значения минимальных расстояний, представленные в табл. 5

Таблица 5 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

Выводы

В результате исследования были получены теоретически или вычислены точные значения минимального расстояния для реверсивных помехоустойчивых кодов в диапазоне длин от 7 до 230. Некоторые результаты уже были изложены в [10]. Код на длине 223 имеет расстояние менее чем 22, однако в силу большой длины точное значение получить пока не удалось. Наилучшими корректирующими возможностями обладает код C_R на длине 143, этот представитель реверсивных кодов способен исправлять до 5 ошибок в сообщении. Также стоит отметить код C_R длиной 49, который способен корректировать до 3 ошибок в передаваемом сообщении.

Если сравнивать реверсивные коды с БЧХ-кодами с конструктивным расстоянием 5 на тех же длинах, которые имеют проверочную матрицу $H = \left(\beta^i, \beta^{3i} \right)^T$ (табл. 2), то реверсивные коды заметно уступают. Всплески минимальных расстояний, характерные для не примитивных БЧХ-кодов, в реверсивных кодах проявляются в гораздо меньшей степени.

Список литературы

1. Мак-Вильямс Ф. Дж. Теория кодов, исправляющих ошибки./ Ф. Дж. Мак-Вильямс, Н. Дж. А. Слоэн - М: Радио и связь, 1979. – 744 с.

2. Липницкий В.А. Теория норм синдромов. / В.А.Липницкий – Мн.: БГУИР, 2010. – 108 с.

3. Липницкий В.А. Норменное декодирование помехоустойчивых кодов и алгебраические уравнения. / В.А. Липницкий, В.К. Конопелько. – Мн.: Издательский центр БГУ, 2007. – 214 с.

4. 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.

5. 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.

6. 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, № Д201315.

7. 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.

8. 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.

9. 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.

10. 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.

Кушнеров Александр Викторович, аспирант кафедры дифференциальных уравнений и системного анализа механико-математического факультета Белорусского государственного университета, al.v.kushnerov@gmail.com

Липницкий Валерий Антонович, профессор кафедры дифференциальных уравнений и системного анализа механико-математического факультета Белорусского государственного университета, доктор технических наук, профессор, valipnitski@yandex.ru