ИССЛЕДОВАНИЕ НЕ ПРИМИТИВНЫХ БЧХ-КОДОВ С МИНИМАЛЬНЫМ КОНСТРУКТИВНЫМ РАССТОЯНИЕМ 7

Олексюк А.О., Липницкий В.А.
Военная академия РБ

Введение. Защита информации от помех, шумов и искажений является одной их важных проблем в современную информационную эпоху. Она актуальна для специалистов занимающихся эксплуатацией и разработкой систем передачи данных.

Основные идеи и направления защиты информации берут свое начало со второй половине 20 века [1 – 3]. Решается эта проблема в рамках научного направления, которое носит название помехоустойчивое кодирование.

Помехоустойчивое кодирование – это преобразование цифровой информации введением дополнительной избыточной информации в нее с целью обеспечения в дальнейшем борьбы с возможными помехами.

На данном этапе развития разработан достаточно широкий спектр таких преобразований. Результатом, каждого из них, является свой специфический помехоустойчивый код. Исторически первыми были коды Хемминга и их модификации. Они получили хорошую теоретическую разработку и массовое применение, в практике создания инфокоммуникационных и телекоммуникационных систем. Однако сказанное выше относится лишь к семейству примитивных кодов Хемминга и кодов Боуза-Чоудхури-Хоквингема (БЧХ-коды), коды на остальных длинах (не примитивные коды) досконально не исследовались.

В статье будут приведены результаты исследования основных параметров не примитивных БЧХ-кодов в диапазоне нечетных длин от 9 до 509 имеющих конструктивное расстояние равное 7. Будут выделены наиболее перспективные коды, которые способны корректировать ошибки, кратность которых превышает их конструктивные значения, в перспективе они могут быть внедрены и найти широчайшее применение в средствах передачи данных, нуждающихся в улучшении их помехоустойчивых характеристик.

Необходимые сведения о строении БЧХ-кодов. Общее определение и основные свойства БЧХ-кодов приведены в монографии [4]. Это линейные (n,k) – коды, то есть k – мерные подпространства в n – мерных двоичных пространствах (над полем $GF(2)=Z/2Z$). Их точное определение напрямую связано с полями Галуа $GF(2^m)$. Среди БЧХ-кодов с конструктивным расстоянием $2t+1$, рассчитанных на исправление t – кратных случайных ошибок, наибольшую размерность и скорость передачи информации, а, следовательно, и наибольший практический интерес имеют циклические коды C_{2t+1} с проверочной матрицей

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

над полем Галуа $GF(2^m)$ из 2^m элементов, где β – элемент мультипликативной группы $GF(2^m)^*$ этого поля порядка $n=\left(2^m-1\right)/\tau$ для некоторого делителя τ числа $\left|GF(2^m)^*\right|=2^m-1$, параметр i принимает целые значения в диапазоне от нуля до $n-1$. Длина кода C_{2t+1} равна n и всегда является нечетной величиной.

Группа $GF(2^m)^*$, как известно, является циклической. Если α – образующая этой группы – примитивный элемент поля $GF(2^m)$, то в качестве β можно взять $\beta=\alpha^\tau$. Тогда, при $\tau=1$, элемент $\beta=\alpha$, $n=2^m-1$ код C_{2t+1}, естественно, называется примитивным; если же $\tau>1$, код C_{2t+1} называют не примитивным.

Матрица (1) – двоичная, каждый элемент β^i в ней представлен вектором-столбцом из координат этого элемента как вектора пространства $GF(2^m)$ над полем $GF(2)$ в базисе $\alpha^{m-1},\alpha^{m-2},...,\alpha^0=1$. Для существования кода C_{2t+1} длиной $n=\left(2^m-1\right)/\tau$ необходимо выполнение условия: $k=\dim C_{2t+1}=n-rankH>0$. Конечно, выполнение условия $k=1$ делает соответствующий код абсолютно не интересным для применений – все богатство передаваемых с помощью такого кода сообщений сводится к двум словам: $\overline{0}=(0,0,...,0)$ и $\overline{1}=(1,1,...,1)$. Поэтому реальный код должен иметь размерность $k>>1$.

Чаще всего $rankH=tm$. Главной причиной наличия неравенства $rankH<tm$ является сопряженность некоторых из элементов $\beta,\beta^3,...,\beta^{2t-1}$. Если элементы β^{2i-1} и β^{2j-1} сопряжены друг с другом для некоторых целых $i, j,\ 1\le i<i\le t,$ то есть являются корнями одного и того же неприводимого над полем $GF(2)=Z/2Z$ полинома, то, как доказано в [4], глава 6, $rank\left(\beta^{2i-1},\beta^{2j-1}\right)^T=rank(\beta^{2i-1})=m$. В таком случае, $rankH\le(t-1)m$.

Сопряженность элементов β^{2i-1} и β^{2j-1} эквивалентна совпадению друг с другом циклотомических классов C^{2i-1} и C^{2j-1} по модулю n [2, 4]. Такие совпадения нередки даже для примитивных БЧХ-кодов. Так по модулю 31 совпадают циклотомические классы C^9 и C^5; по модулю 63: $C^{17}=C^5$; $C^{19}=C^{13}$; по модулю 127: $C^{17}=C^9$; $C^{25}=C^{19}$; $C^{33}=C^5$.

Конструктивное расстояние δ БЧХ-кода C_{2t+1} считается равным t. Точное значение его минимального расстояния $d\ge\delta$. Отмеченная выше сопряженность двух элементов матрицы (1) не только уменьшает на m количество ее линейно независимых строк, но и автоматически увеличивает на 2 его минимальное расстояние по сравнению с конструктивным. Так в силу сказанного, у примитивного кода C_9 длиной 31 $\delta=9$, а $d=11$ [4], у БЧХ-кодов C_{17} с длинами 63 и 127 $\delta=17$, а $d=19$.

Не примитивные коды предоставляют массу подобных примеров [5 – 6]. Глубинная причина существования таких примеров, в общем-то, известна и кроется в следующей базовой теореме помехоустойчивого кодирования:

«Минимальное расстояние кода L равно d тогда и только тогда, когда любые $d-1$ столбцов проверочной матрицы H_L линейно независимы, но найдутся d линейно зависимых столбцов» [2, 4].

Очевидно, все столбцы проверочной $(tm\times n)-$матрицы $H_{непр}$ каждого не примитивного БЧХ-кода над полем $GF(2^m)$ принадлежат $H_{прим}$ – проверочной $\left(tm\times(2^m-1)\right)-$матрице примитивного БЧХ-кода над тем же полем, а матрица $H_{непр}$ получается из $H_{прим}$, по сути дела, выбрасыванием огромного количества столбцов – $(\tau-1)d$. Такая процедура может привести только к увеличению минимального расстояния кода. Истинное же значение величины d приходится вычислять в каждом конкретном случае, применяя один из четырех разработанных в расчете именно на БЧХ-коды подходов [4].

Исследование реальных конструктивных параметров не примитиых БЧХ-кодов C_7**.** БЧХ-коды C_7 – частный случай кодов с проверочной матрицей (1) – задаются проверочными двоичными $(3m\times n)-$матрицами

$$H=\left(\beta^i,\beta^{3i},\beta^{5i}\right)^T \qquad (2)$$

при обязательном выполнении условия: $3m<n=\left(2^m-1\right)/\tau$.

В [2] доказано, что у примитивных кодов C_7 минимальное расстояние $d=\delta=7$, а их размерность $k=n-3m$, а у не примитивных кодов C_7 любое из названных соотношений может нарушиться. Во всех конкретных случаях проверка каждого параметра кода требует внимания, дополнительных вычислений, а порой и серьезных компьютерных ресурсов.

При исследовании не примитивных БЧХ-кодов в диапазоне нечетных длин от 9 до 509 имеется 246 длин кодов из 251 возможных, коды на длинах 15, 31, 63, 127, 255 являются примитивными и хорошо известными. Для 95 значений длин выполняется неравенство: $n<3m$,это означает что для данных значений длины БЧХ-коды C_5 не существуют. Девять БЧХ-кодов C_7 длиною 43, 109, 157, 229, 277, 283, 307, 499 имеют размерность 1, что, в свою очередь, не вызывает никакого интереса в практическим применении данных кодов. Из оставшихся 86 БЧХ-кодов 28 длин имеют $d_{\text{реал.min}}=\delta=7$, где $d_{\text{реал.min}}$ достаточно близкая оценка d. Не имеет особого смысла рассматривать эти 28 кодов, так как соответствующие им примитивные коды имеют те же параметры $d_{\text{реал.min}}=\delta=7$, но существенно большую скорость передачи информации.

Таким образом, в диапазоне длин от 9 до 509 имеется 58 БЧХ-кодов C_7 с размерностью $k>1$ и $d>7$. Результаты вычислений основных параметров этих 58 не примитивных БЧХ-кодов и оценки $d_{\text{реал.min}}$ их минимальных расстояний приведены в таблице 1.

Таблица 1. – Не примитивные БЧХ коды C_7 с $d_{\text{реал.min}} > 7$, $k > 1$, $9 < n < 509$.

n	m	k	$d_{\text{реал.min}}$	n	m	k	$d_{\text{реал.min}}$	n	m	k	$d_{\text{реал.min}}$
33	10	3	9	207	66	9	9	363	110	33	9
39	12	3	9	213	70	3	11	369	60	189	9
51	8	27	9	219	18	165	9	377	84	125	11
57	18	3	9	221	24	149	9	391	88	127	9
69	22	3	13	223	37	112	9	393	130	3	11
73	9	46	9	237	78	3	9	417	138	3	11
87	28	3	13	247	36	139	9	423	138	9	9
89	11	56	9	249	82	3	11	439	73	220	9
99	30	9	9	251	50	101	9	445	44	313	9
111	36	3	13	261	84	9	9	447	148	3	11
113	28	29	9	281	70	71	11	459	72	243	9
123	20	63	9	291	48	147	9	477	156	9	11
141	46	3	15	297	90	27	9	485	48	341	9
153	24	81	9	303	100	3	11	489	162	3	11
159	52	3	13	305	60	125	9	493	56	325	9
177	58	3	11	309	102	3	9	501	166	3	11
183	60	3	11	321	106	3	9	505	100	205	9
185	36	77	9	323	72	107	9	507	156	39	9
187	40	67	11	333	36	225	9				
201	66	3	9	339	28	255	9				

39 из приведенных в таблице 1 кодов имеют $d_{\text{реал.min}} = 9$, 14 - $d_{\text{реал.min}} = 11$, коды на длинах 69, 87, 111, 159 имеют $d_{\text{реал.min}} = 13$, а код на длине 141 – $d_{\text{реал.min}} = 15$. По отношению $k/n \geq 0{,}5$ к высокоскоростным относятся 18 из 58 представленных в таблице 1, это коды с длиной n: 51, 73 89, 123, 153, 219, 221, 223, 247, 291, 333, 339, 369, 439, 445, 459, 485, 493.

Для более зрелещного подтверждения полученных результатов, составим таблицу 2, в которой на практике продемонстрируем реальное колличество исправляемых ошибок K_{real} и во сколько раз эти реальные значения превышают конструктивные $K_{\text{констр.}}$, когда-то ранее дававшиеся нам только в теории.

Таблица 2 Потенциал конструктивного $K_{\text{констр.}}$ и реального K_{real} количества исправляемых ошибок у БЧХ-кодов C_7 в диапазоне длин от 9 до 509, размерность которых $k > 1$ и $d \geq 7$

n	m	$K_{\text{констр.}}$	K_{real}	n	m	$K_{\text{констр.}}$	K_{real}
33	10	6017	46937	261	84	2963481	191902686
39	12	9919	92170	281	70	3698241	14344756917
51	8	22151	272051	291	48	4107271	296771791
57	18	30913	425923	297	90	4366593	322058583
69	22	54809	132035295	303	100	4636607	20937549167
73	9	64897	1153327	305	60	4729025	358247205
87	28	109823	544266954	309	102	4917529	377444530
89	11	117569	2559195	321	106	5512961	439684721
99	30	161799	3926175	323	72	5616647	450762327

111	36	228031	2398624900	333	36	6154617	509322612
113	28	240577	6679317	339	28	6493319	547091195
123	20	310247	9388877	363	110	7972327	719535817
141	46	467321	199221963507	369	60	8374209	768368085
153	24	597057	22544907	377	84	8930753	62633192453
159	52	670079	21219561240	391	88	9963071	968947266
177	58	924353	1407982313	393	130	10116737	77142181565
183	60	1021567	1664856103	417	138	12085633	103830133681
185	36	1055425	48294435	423	138	12614847	1327757802
187	40	1090023	1855990895	439	73	14101119	1540595870
201	66	1353601	67351951	445	44	14687225	1626660120
207	66	1478463	75782148	447	148	14886143	147070676927
213	70	1610777	3569815319	459	72	16117479	1841475105
219	18	1750759	94990885	477	156	18088953	203649107523
221	24	1799161	98516496	485	48	19014425	2296051110
223	37	1848447	102139352	489	162	19488769	230645743117
237	78	2218873	130373068	493	56	19970937	2451493772
247	36	2511743	153859758	501	166	20959001	260432417351
249	82	2573249	7819604549	505	100	21465025	2699291155
251	50	2635751	164091501	507	156	21721063	2742348973

Вычисления предоставленные в таблице демонстрируют явный перекос в декодирующих возможностях БЧХ-кодов C_7 – на плюс-декодирование [7] приходится в десятки тысяч раз больше векторов-ошибок, чем на конструктивное.

Все приведенные 58 БЧХ-кодов C_7 имеют, как правило, более высокие декодирующие возможности, чем коды C_5 на тех же длинах. Разработанные для кодов C_5 перестановочные алгоритмы коррекции ошибок [8, 9] вселяют надежду на разработку подобных алгоритмов для рассмотренных в данной работе кодов C_7.

Заключение. Проведенное циклотомическое исследование и анализ демонстрируют привлекательность для приложений кодов на рассмотренных длинах. Как правило, работы по более детальному и углубленному исследованию каждой из длин не примитивных БЧХ-кодов и кодов Хемминга [7, 8, 10] дают более впечатляющие результаты, что в свою очередь приближает перспективу использования не примитивных кодов.

Литература

1 Шеннон, К. Работа по теории информации и кибернетике / К.Шеннон. – М. : ИЛ, 1963. – 732 с.

2 Мак-Вильямс Ф.Дж., Слоэн Н. Дж.А. Теория кодов, исправляющих ошибки: Пер. с англ. М.: Связь, 1979. – 744с.

3 Колесник В.Д. Декодирование циклических кодов / В.Д. Колесник, Е.Т. Мирончиков. – М.: Связь, 1968. – 252 с.

4 Липницкий В.А., Конопелько В.К. Норменное декодирование помехоустойчивых кодов и алгебраические уравнения/ В.А. Липницкий, В.К. Конопелько –Мн.: Издательский центр БГУ, 2007.- 216 с.

5 Конопелько В.К., Теория норм синдромов и перестановочное декодирование помехоустойчивых кодов / В.К. Конопелько, В.А. Липницкий. – Изд. 2-е. – М: Едиториал, УРСС 2004. – 176 с.

6 Сагалович Ю.Л. Коды, исправляющие одиночные байты ошибок длины 2 // IX Симпозиум по проблеме избыточности в информационных системах: Тез. докл., часть I, Ленинград, 3–8 июня 1986 г. – С. 135–138.

7 Липницкий, В.А. Теория норм синдромов и плюс-декодирование / Липницкий, В.А., Олексюк А.О.// Доклады БГУИР. – 2014. – №8(86). – С.72–79.

8 Патент на изобретение №19822 МПК G11C 29/00. Устройство декодирования для коррекции четырехкратных ошибок / В.А. Липницкий, А.О. Олексюк, Военная академия Республики Беларусь. – №a20130054; заявл. 16.01.2013; опубл. 28.02.2016.

9 Липницкий, В.А. Перестановочный декодер для коррекции многократных ошибок непримитивными БЧХ-кодами / Липницкий, В.А., Олексюк А.О.// Доклады БГУИР. – 2015. – №3(89). – С.117–123.

10 Липницкий, В.А. Оценки минимальных расстояний не примитивных кодов Хемминга/ В.А. Липницкий, А.О. Олексюк // Весці НАН Беларусі. Сер. фіз. тэх. навук. 2015. – № 2. – С. 103 – 110.