УДК 004.056.55

В. А. ЛИПНИЦКИЙ, А. О. ОЛЕКСЮК

ОЦЕНКА МИНИМАЛЬНЫХ РАССТОЯНИЙ НЕ ПРИМИТИВНЫХ КОДОВ ХЕММИНГА

Военная академия Республики Беларусь

(Поступила в редакцию 09.04.2015)

Введение. Помехоустойчивые коды являются необходимым средством борьбы с шумами и помехами для большинства современных телекоммуникационных систем (ТКС). К настоящему времени развита достаточно стройная теория помехоустойчивых кодов, равно как и практика их применения. Коды Хемминга – исторически первый класс кодов, разработанный Р. Хеммингом в конце 40-х годов XX в. [1, 2]. Это класс совершенных линейных кодов, исправляющих лишь одну ошибку на каждый блок передаваемой информации.

В начале 60-х годов XX в. положено начало исследованию свойств и применению кодов Боуза–Чоудхури–Хоквингема (БЧХ-кодов) [2], допускающих исправление многократных ошибок и включающих в себя как частный предельный случай коды Хемминга. Примитивные БЧХ-коды имеют достаточно завершенную и четкую теорию, являются наиболее применимыми на практике.

В отличие от примитивных не примитивные БЧХ-коды обладают стохастически меняющимися свойствами, их параметры приходится скрупулезно получать громоздкими компьютерными вычислениями в каждом случае. Видимо, из-за этих причин не примитивные БЧХ-коды не вызывают большого интереса в теории и практике помехоустойчивого кодирования. Белорусская школа кодирования ведет систематическую работу по исследованию не примитивных БЧХ-кодов [3–5].

Цель данной статьи – доказательство того факта, что минимальное расстояние не примитивных кодов Хемминга может принимать сколь угодно большие значения.

Необходимые сведения о кодах Хемминга. В данной работе мы опираемся на следующее определение

О п р е д е л е н и е 1. [3] *Двоичным кодом Хемминга называется линейный циклический код* C_x^n*, определяемый следующими тремя параметрами:*

1) *длина кода n – любое нечетное число* $n \geq 7$*;*

2) $GF(2^m)$ *– поле определения кода – имеет минимальное значение показателя m, при котором* $2^m - 1$ *делится на n;*

3) *проверочная матрица кода* C_x^n *есть матрица*

$$H = (\beta^i) = (1,\ \beta,\ \beta^2,\ ...,\ \beta^{n-1}), \tag{1}$$

где β *– примитивный корень n-й степени из* 1*, принадлежащий* $GF(2^m)$.

Данное несколько громоздкое определение требует пояснений. Согласно основам теории полей Галуа [6, 7], всякое конечное поле состоит из q^t-элементов, где q – простое число; t – натуральное число, потому и обозначается через $GF(q^t)$; ненулевые элементы этого поля образуют группу относительно операции умножения – мультипликативную группу $GF(q^t)^*$; это циклическая группа порядка $q^t - 1$; образующая α группы $GF(q^t)^*$ называется примитивным элементом поля $GF(2^m)$; поле $GF(q^t)$ содержит в качестве минимального подполя поле $GF(q) = Z / qZ$, является t-мерным векторным пространством над полем $GF(q)$; примитивный

элемент α поля $GF(q^t)$ обязательно является корнем некоторого неприводимого полинома t-й степени $M_\alpha(x)$ с коэффициентами из минимального подполя $GF(q)$; данный полином еще называют примитивным полиномом t-й степени над Z/qZ. Тогда поле $GF(q^t)$ изоморфно факторкольцу $(Z/qZ)[x]/<M_\alpha(x)>$ кольца полиномов $(Z/qZ)[x]$ по максимальному идеалу $<M_\alpha(x)>$, порожденному неприводимым полиномом $M_\alpha(x)$. Поэтому элементы поля $GF(q^t)$ имеют тройную интерпретацию:

1) мультипликативную – как степени примитивного элемента α;

2) полиномиальную – как полиномы от α степени, меньшей t: $c_{t-1}\alpha^{t-1}+...+c_1\alpha+c_0$ для $c_i \in Z/qZ$, $0 \le i < t$;

3) векторную – $(c_{t-1}, c_{t-2}, ..., c_1, c_0)$, получаемую очевидным образом из полиномиальной интерпритации.

Поле $GF(q^t)$ считается идеально заданным, если установлена взаимосвязь между 1-м и 2-м способами его задания, т. е. таблица соответствий между мультипликативным и полиномиальным заданиями этого поля.

В силу теоремы Лагранжа конечная группа $GF(q^t)^*$ состоит из всех возможных корней из 1 порядка q^t-1. Пусть α – примитивный элемент поля $GF(2^t)$. Тогда для всякого делителя n чисел q^t-1 и $s=(q^t-1)/n$ элемент α^s является примитивным корнем n-й степени из 1 в поле $GF(q^t)$. Таким образом, делимость числа q^t-1 на n является необходимым и достаточным условием принадлежности полю $GF(q^t)$ всех корней n-й степени из 1.

Для любого наперед заданного нечетного числа $n>1$ существуют поля $GF(2^t)$, такие, что 2^t-1 делится на n. Одним из них является поле $GF(2^{\varphi(n)})$, где $\varphi(n)$ – количество целых k, $1 \le k < n$, взаимно простых с n [8]. Действительно, в силу теоремы Эйлера $2^{\varphi(n)} \equiv 1 (\mathrm{mod}\, n)$ для любого нечетного n. Тогда $2^{\varphi(n)}-1$ делится на n. Отсюда следует, что минимальное поле $GF(2^m)$ с условием 2^m-1 делится на n, будет подполем поля $GF(2^{\varphi(m)})$, а следовательно, его показатель m будет делителем $\varphi(m)$.

Необходимо также отметить, что минимальность m влечет за собой отсутствие подполей поля $GF(2^m)$, которые могли бы содержать элемент β из определения 1, а из этого факта следует, что минимальный полином $M_\beta(x)$ элемента β, т. е. неприводимый полином с корнем β и с коэффициентами из $Z/2Z$, должен иметь степень, равную m.

Для задания кода Хемминга с заданной нечетной длиной $n>1$ следует вычислить $\varphi(n)$, определить все делители $\varphi(n)$, найти среди них наименьший делитель m с условием: 2^m-1 делится на n. Далее следует найти неприводимый и примитивный полином β степени m из кольца $(Z/2Z)[x]$. С помощью корня α полинома $p(x)$ строится троякое задание поля $GF(2^m)$. Наконец, с помощью элемента $\beta=\alpha^s$ для $s=(2^m-1)/n$ строится по формуле (1) проверочная матрица H кода C_x^n – двоичная матрица порядка $m \times n$, столбцами которой являются векторы $\beta^i=(c_{i(m-1)}, c_{i(m-2)}, ..., c_{i0})^T$, где $\beta^i=c_{i(m-1)}\alpha^{m-1}+...+c_{i1}\alpha+c_{i0}$. В силу отмеченных выше свойств элемента β ранг такой матрицы H обязательно должен равняться m. Следовательно, размерность кода C_x^n есть величина $k=n-m$.

В табл. 1 приведены результаты вычисления параметров m и k кодов Хемминга для длин n в диапазоне от 9 до 309.

Таблица 1. **Поля определения и размерности кодов Хемминга длиной *n* для нечетных длин в диапазоне *n* от 9 до 309**

n	*m*	*k*	*n*	*m*	*k*	*n*	*m*	*k*	*n*	*m*	*k*
9	6	3	91	12	79	167	83	84	243	162	81
15	4	11	93	10	83	169	156	13	245	84	161
17	8	9	95	36	59	171	18	153	247	36	211
21	6	15	97	48	49	175	60	115	249	82	167
23	11	12	99	30	69	177	58	119	251	50	201
25	20	5	103	51	52	183	60	123	253	110	143
27	18	9	105	12	93	185	36	149	255	8	247
31	5	26	109	36	73	187	40	147	257	16	241
33	10	23	111	36	75	189	18	171	259	36	223

Окончание табл. 1

n	*m*	*k*	*n*	*m*	*k*	*n*	*m*	*k*	*n*	*m*	*k*
35	12	23	113	28	85	191	95	96	261	84	177
39	12	27	115	44	71	193	96	97	263	131	132
41	20	21	117	12	105	195	12	183	265	52	213
43	14	29	119	24	95	199	99	100	267	22	245
45	12	33	121	110	11	201	66	135	271	135	136
47	23	24	123	20	103	203	84	119	273	12	261
49	21	28	125	100	25	205	20	185	275	20	255
51	8	43	127	7	120	207	66	141	277	92	185
55	20	35	129	14	115	209	90	119	279	30	249
57	18	39	133	18	115	213	70	143	281	70	211
63	6	57	135	36	99	215	28	187	283	94	189
65	12	53	137	68	69	217	15	202	285	36	249
67	66	1	141	46	95	219	18	201	287	60	227
69	22	47	143	60	83	221	24	197	289	136	153
71	35	36	145	28	117	223	37	186	291	48	243
73	9	64	147	42	105	225	60	165	295	116	179
75	20	55	151	15	136	229	76	153	297	90	207
77	30	47	153	24	129	231	30	201	299	132	167
79	39	40	155	20	135	233	29	204	301	42	259
81	54	27	157	52	105	235	92	143	303	100	203
85	8	77	159	52	107	237	78	159	305	60	245
87	28	59	161	33	128	239	119	120	307	102	205
89	11	78	165	20	145	241	24	217	309	102	207

П р и м е р 1. Построим код Хемминга C_{χ}^{17} длиной 17. Решаем задачу в соответствии с приведенной выше программой действий. Согласно данным табл. 1, этот код определен над полем $GF(2^8)$. В кольце полиномов $Z/2Z[x]$ имеется 16 неприводимых и примитивных полиномов 8-й степени. Зафиксируем один из них – полином $p(x)=x^8+x^4+x^3+x^2+1$. С его помощью построим троякое задание поля $GF(2^8)$, взяв в качестве примитивного элемента α этого поля корень выбранного полинома $p(x)$.

Здесь $2^8-1=255=17\cdot 15$, следовательно, примитивный корень 17-й степени в поле $GF(2^8)$ есть $\beta=\alpha^{255/17}=\alpha^{15}$. При использовании векторного задания поля $GF(2^8)$ строим, согласно формуле (1), проверочную матрицу кода C_{χ}^{17}:

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

Аналогичным образом своей проверочной матрицей H задается код Хемминга любой нечетной длины *n*.

Определение минимального расстояния кода Хемминга. Когда $n=2^m-1$, проверочная матрица кода Хемминга состоит из всех возможных ненулевых столбцов – векторов *n*-мерного пространства над полем $Z/2Z$. Разумеется, любые два столбца в такой матрице отличаются друг от друга, но обязательно найдутся три столбца, сумма которых равна нулю. Например, $(00...001)^T+(00...010)^T+(00...011)^T=(00...000)^T$. Таким образом, каждый примитивный код Хемминга имеет минимальное расстояние 3.

Не примитивный код Хемминга длиной *n*, определенный над полем $GF(2^m)$, можно интерпретировать как код, проверочная матрица которого получается из проверочной матрицы

примитивного кода Хемминга длиной 2^m-1 выбрасыванием s определенных столбцов, где $s=(2^m-1)/n$. Такая процедура может только увеличить минимальное расстояние кода с 3 на большую величину.

Наиболее радикальное увеличение минимального расстояния наблюдается у не примитивных кодов Хемминга $C^n_{\chi,}$ у которых $m=n-1$. Тогда $k=n-m=1$, такой код состоит только из двух кодовых символов: $\overline{0}=(0,0,...,0)$ и $\overline{1}=(1,1,...,1)$. Здесь $d=dist(\overline{0},\overline{1})=n$ – максимально возможное значение. Однако вряд ли такой код может получить непосредственное применение в практике помехоустойчивого кодирования. Ведь такие коды практически передают только два сообщения: «точка» и «тире». В дальнейшем мы их не рассматриваем, имеется 23 таких кода из 150, из них в диапазон от 9 до 99 попадают коды длиной 11, 13, 19, 29, 37, 53, 59, 61, 67, 83.

В [3] описан ряд методов определения минимального расстояния линейного кода: по определению – составлением таблицы весов кодовых слов; по критерию, связанному со столбцами проверочной матрицы кода; синдромным методом; методом орбит. Последний метод требует знания об автоморфизмах кодов, построения орбит ошибок под действием этих автоморфизмов. Код Хемминга, определенный формулой (1), является, очевидно, циклическим кодом. Это означает, что группа автоморфизмов $Aut(C^n_\chi)$ содержит подгруппу Г циклических сдвигов координат векторов. Группа Г циклическая порядка n и порождена автоморфизмом σ, действующим на каждый вектор $\overline{v}=(a_1,\ a_2,\ ...,\ a_n)$ векторного пространства размерности n по правилу: $\sigma(\overline{v})=\sigma(a_1,\ a_2,\ ...,\ a_n)=(a_n,\ a_1,\ a_2,\ ...,\ a_{n-1})$ [3, 9, 10].

Под действием группы Г векторы ошибок линейного кода разбиваются на непересекающиеся классы – Г-орбиты, состоящие из векторов, последовательно переходящих друг в друга под действием σ. Как правило, Г-орбиты являются полными, т. е. содержат по n различных векторов.

Так, все ошибки весом 1 образуют одну Г-орбиту $<(1)>$ для вектора $(1)=(1,\ 0,\ ...,\ 0)$. Все векторы весом 2 в количестве $C^2_n=(n-1)/2n$ делятся на $(n-1)/2$ полных Г-орбит: $<(1,2)>$, $<(1,3)>,...,<(1,\nu+1)>$ для векторов $(1,2)=(1,1,0,...,0)$, $(1,3)=(1,0,1,0,...,0),...,(1,\nu+1)=(1,0,...,0,1,0,...,0)$ – вектор, у которого вторая единица стоит на месте под номером $\nu+1$, где $n=2\nu+1$ [3, 10].

Каждый вектор ошибок $\overline{e}$ в коде C^n_χ имеет свой синдром $S(\overline{e})=H\cdot\overline{e}^T$ – вектор из m-мерного двоичного линейного пространства. В [9] определена формула

$$S(\sigma(\overline{e}))=\beta\cdot S(\overline{e}). \tag{2}$$

Из нее следует, что каждая Г-орбита $<\overline{e}>$ имеет четко очерченный спектр синдромов $S(<\overline{e}>)$, синхронно отражающий действие σ на векторах Г-орбиты:

если

$$<\overline{e}>=\{\overline{e},\sigma(\overline{e}),\sigma^2(\overline{e}),...,\sigma^{n-1}(\overline{e}),\sigma^n(\overline{e})=e\},$$

то

$$S(<\overline{e}>)=\{S(\overline{e}),\beta\cdot S(\overline{e}),\beta^2\cdot S(\overline{e}),...,\beta^{n-1}\cdot S(\overline{e}),\beta^n\cdot S(\overline{e})=S(\overline{e})\}. \tag{3}$$

Иллюстрацией к формуле (3) является

П р и м е р 2. В табл. 2 представлены Г-орбита, порожденная вектором $\overline{e}=(1,9)$ в коде C^{17}_χ из примера 1, а также спектр показателей синдромов этой орбиты.

Т а б л и ц а 2. **Спектр синдромов Г-орбиты, порожденной вектором $\overline{e}=(1,9)$ в коде C^{17}_χ**

Векторы Г-орбиты	$\overline{e}$	$\sigma(\overline{e})$	$\sigma^2(\overline{e})$	$\sigma^3(\overline{e})$	$\sigma^4(\overline{e})$	$\sigma^5(\overline{e})$	$\sigma^6(\overline{e})$	$\sigma^7(\overline{e})$	$\sigma^8(\overline{e})$
$\overline{e}_i=\sigma^{i-1}(\overline{e})$	(1,9)	(2,10)	(3,11)	(4,12)	(5,13)	(6,14)	(7,15)	(8,16)	(9,17)
$\deg S(\overline{e}_i)$	9	24	39	54	69	84	99	114	129
Векторы Г-орбиты	$\sigma^9(\overline{e})$	$\sigma^{10}(\overline{e})$	$\sigma^{11}(\overline{e})$	$\sigma^{12}(\overline{e})$	$\sigma^{13}(\overline{e})$	$\sigma^{14}(\overline{e})$	$\sigma^{15}(\overline{e})$	$\sigma^{16}(\overline{e})$	$\sigma^{17}(\overline{e})$
$\overline{e}_i=\sigma^{i-1}(\overline{e})$	(1,10)	(2,11)	(3,12)	(4,13)	(5,14)	(6,15)	(7,16)	(8,17)	(1,9)
$\deg S(\overline{e}_i)$	144	159	174	189	204	219	234	249	9

Как известно (например, [3, 9]), если минимальное расстояние линейного кода равно $d = 2t + 1$, то все векторы весом $1, 2, ..., t$ имеют попарно различные синдромы. Верно и обратное.

Л е м м а 1. *Если все векторы ошибок весом* $1, 2, ..., t$, $t \geq 1$, *имеют попарно различные синдромы в линейном коде* C, *то минимальное расстояние этого кода* $d \geq 2t + 1$.

Д о к а з а т е л ь с т в о. Пусть в условиях леммы 1 минимальное расстояние d кода C на самом деле удовлетворяет неравенству $d \leq 2t$. Ясно, что $d > 1$, т. е. $d \geq 2$. По свойствам минимального расстояния наименьший вес кодовых слов в коде C равен d. В коде C найдется, по крайней мере, одно кодовое слово $\overline{c} = (i_1, i_2, ..., i_d)$ весом d, у которого координаты с номерами $i_1, i_2, ..., i_d$ равны 1, а остальные равны 0, $d = \delta + \mu$ для некоторых целых δ, μ, $1 \leq \delta < d, 1 \leq \mu < d$. Тогда $\overline{c} = \overline{e}' + \overline{e}''$ для $\overline{e}' = (i_1, i_2, ..., i_\delta)$, $\overline{e}'' = (i_{\delta+1}, i_{\delta+2}, ..., i_d)$ – для векторов весом δ и μ соответственно. $S(\overline{c}) = H \cdot \overline{c}^T = \overline{0} = H \cdot (\overline{e}' + \overline{e}'')^T = H \cdot \overline{e}'^T + H \cdot \overline{e}''^T = S(\overline{e}') + S(\overline{e}'') = 0$.

Следовательно, $S(\overline{e}') = S(\overline{e}'')$, что противоречит условиям леммы. Таким образом, $d \geq 2t + 1$, что и требовалось доказать.

П р и м е р 3. Опираясь на лемму 1, покажем, что минимальное расстояние не примитивного кода Хемминга C_χ^{17}, построенного в примере 1, равно 5.

Действительно, табл. 3 представляет список образующих Г-орбит всех векторов-ошибок весом 1, 2 в коде C_χ^{17}, разделенных на 9 полных Г-орбит, а также показателей синдромов названных векторов-ошибок.

Т а б л и ц а 3. **Образующие $\overline{e}_i$ Г-орбит векторов-ошибок весом 1 и 2, показатели $\deg S(\overline{e}_i)$ их синдромов $S(\overline{e}_i)$ в коде Хемминга C_χ^{17}, а также остатки r_i от деления $\deg S(\overline{e}_i)$ на 15**

№	1	2	3	4	5	6	7	8	9
$\overline{e}_i$	<1>	<1,2>	<1,3>	<1,4>	<1,5>	<1,6>	<1,7>	<1,8>	<1,9>
$\deg S(\overline{e}_i)$	0	33	66	31	132	199	62	248	9
$r_i (\mathrm{mod} 15)$	0	3	6	1	12	4	2	8	9

Поскольку все остатки в табл. 3 попарно не сравнимы друг с другом по модулю 15, то спектры синдромов $S(<\overline{e}_i>)$ всех перечисленных Г-орбит попарно не пересекаются. В соответствии с леммой 2 это означает, что минимальное расстояние d кода C_χ^{17} не менее 5.

Однако в этом коде существуют векторы ошибок весом 3, синдромы которых совпадают с синдромами двойных ошибок. К примеру, пары векторов ошибок <1, 4, 9> и <7, 16> или <1, 5, 11> и <3, 16> имеют одинаковые значения показателя степени синдрома $\deg S_1 = 234$ и $\deg S_2 = 117$. Таким образом, минимальное расстояние d кода C_χ^{17} в точности равно 5.

Оценка сверху минимального расстояния некоторых классов кодов Хемминга. Минимальное расстояние – главный параметр кода, определяющий его практическую ценность: чем больше d, тем больше ошибок данный код способен исправлять.

Наличие делителей у длины и кода Хемминга является автоматическим ограничением сверху на его кодовое расстояние.

Л е м м а 2. *Если длина* n *кода Хемминга* C_χ^n *делится на простое число* p, *то в данном коде имеется кодовое слово весом* p.

Д о к а з а т е л ь с т в о. Пусть $n = p \cdot s$ для некоторого целого $s > 1$. Пусть вектор $\overline{c}$ имеет координаты, равные 1, только на позициях $1, s+1, 2s+1, ..., (p-1)s+1$, а остальные его координаты равны 0. Вес вектора $\overline{c}$ равен p. Этот вектор принадлежит коду C_χ^n потому, что $H_\chi \cdot \overline{c}^T = \overline{0}$.

В самом деле,

$$H_\chi \cdot \overline{c}^T = 1 + \beta^s + \beta^{2s} + ... + \beta^{(p-1)s} = \frac{(1 + \beta^s + ... + \beta^{(p-1)s})(1 + \beta^s)}{1 + \beta^s} = \frac{1 + \beta^{ps}}{1 + \beta^s} = 0.$$

Лемма 2 полностью доказана. Из нее непосредственно вытекает

Т е о р е м а 1. *Минимальное расстояние* d *кода* C_χ *находится в диапазоне* $[3, p_{\min}]$ *для минимального простого делителя* $p_{\min} > 1$ *длины кода* n.

В частности, если n *делится на* 3*, то минимальное расстояние равно* 3*; если* n *делится на* 5*, то* d *принимает одно из* 3 *значений:* 3, 4 *или* 5.

П р и м е р 4. Вычисления, аналогичные проведенным в примерах 1–3, показывают, что код C_χ^{25} имеет минимальное расстояние 5.

Как уже отмечалось выше, примитивные коды Хемминга, в частности, коды C_χ^7, C_χ^{15}, C_χ^{31}, C_χ^{63}, имеют минимальное расстояние $d = 3$. Такое же значение d имеют, согласно теореме 1, коды C_χ^n, у которых длина делится на 3, в частности, коды длиной n, равной 9, 21, 27, 33, 39, 45, 51, 57, 69, 75, 81, 87, 93, 99, 105. Таким образом, 1/3 часть многообразия не примитивных кодов Хемминга обязательно имеет $d = 3$ (для длин $n = 6k + 3 = 3(2k + 1)$).

Реальных вычислительных затрат на определение точного значения d требуют коды Хемминга, длины которых $n = 6k + 1$ и $n = 6k + 5$, $n \neq 2^m - 1$ и $m < n - 1$. Именно для таких длин кодов C_χ^n в диапазоне от 9 до 109 составлена табл. 4 величин d с применением перечисленных выше методов. Как показывает таблица, переход к не примитивным кодам Хемминга может привести к пятикратному увеличению минимального расстояния (код C_χ^{79}), что в свою очередь является не максимальным пределом.

Т а б л и ц а 4. **Точные значения минимального расстояния кодов Хемминга в диапазоне длин от 9 до 109**

n	*m*	*k*	*d*	*n*	*m*	*k*	*d*	*n*	*m*	*k*	*d*
17	8	9	5	55	20	35	5	89	11	78	4
23	11	12	7	57	18	39	3	91	12	79	3
25	20	5	5	65	12	53	5	95	36	59	5
35	12	23	3	71	35	36	11	97	48	49	11
41	20	21	9	73	9	64	3	103	51	52	11
43	14	29	6	77	30	47	3	109	36	73	7
47	23	24	11	79	39	40	15				
49	21	28	3	85	8	77	3				

Некоторые сведения о квадратично-вычетных кодах. Для построения квадратично-вычетных кодов (КВ-кодов) нужны два простых числа p и l, при этом l является квадратичным вычетом по модулю p. В результате получается код, определенный над полем *GF*(*l*). Ограничимся рассмотрением важнейшего для практики случая $l = 2$.

Как известно (например, [6]), число 2 является квадратичным вычетом по простому модулю p тогда и только тогда, когда p имеет вид $8k \pm 1$. Именно такие простые числа p мы и будем рассматривать.

КВ-код определяется минимальным расширением поля $GF(l) = GF(2) -$ полем $GF(2^m)$, содержащим группу C_p корней p-й степени из 1. Как установлено выше, поле $GF(2^m)$ содержит группу C_p тогда и только тогда, когда $2^m - 1$ делится на p. Поскольку $\varphi(p) = p - 1$ в силу простоты p, то одним из таких расширений является поле $GF(2^{p-1})$. Поскольку по условию 2 l является квадратичным вычетом по модулю p, то, согласно теореме Эйлера, $2^{(p-1)/2} \equiv 1 (\mathrm{mod}\, p)$, т. е. $2^{(p-1)/2} - 1$ делится на p. Таким образом, доказано следующее.

П р е д л о ж е н и е 1. *Для простых чисел* p *вида* $8k \pm 1$ *мультипликативная группа поля* $GF(2^{(p-1)/2})$ *содержит подгруппу* C_p *корней порядка* p *из* 1.

С л е д с т в и е. *Минимальное расширение поля* $GF(2)$*, содержащее подгруппу* C_p *корней порядка* p *из* 1*, имеет вид* $GF(2^m)$*, где* m *является натуральным делителем числа* $(p-1)/2$*, в частности, совпадает с* $(p-1)/2$.

Заметим, что простых чисел p вида $8k \pm 1$ бесконечно много [8].

Составим перечень всех простых чисел вида $p = 8k \pm 1$ в диапазоне от 7 до 309 соответствующих им значений $(p-1)/2$, а также минимальных значений m с условием: $2^m - 1$ делится на p (табл. 5).

В табл. 5 представлено 28 значений $p = 8k \pm 1$. Для 17 из них минимальное значение *m* совпадает с $(p-1)/2$, для 10 значений m является делителем $(p-1)/2$: в двух случаях ($p = 113, 281$)

$(p-1)/2=2m$, в одном случае ($p=31$) $(p-1)/2=3m$, в трех случаях ($p=73,89,233$) $(p-1)/2=4m$, в двух случаях ($p=151,241$) $(p-1)/2=5m$, в одном случае ($p=257$) $(p-1)/2=8m$ и в одном случае ($p=127$) $(p-1)/2=9m$.

Согласно определению (например, [2, с. 190]), циклический двоичный код длиной n – это идеал в кольце $R_n=GF(2)[x]/<x^n-1>$, в фактор-кольце кольца $GF(2)[x]$ полиномов с коэффициентами из $GF(2)$ по идеалу $<x^n-1>$, порожденному полиномом x^n-1. Как и в кольце полиномов, всякий идеал J кольца R_n является главным, порожден полиномом $g(x)$ наименьшей степени, принадлежащим идеалу J. Таким образом, $J=<g(x)>$ ([2, с. 191]). С этой точки зрения код Хемминга длиной n есть идеал $J=<M_\beta(x)>$ кольца R_n, где, как уже отмечалось выше, $M_\beta(x)$ – неприводимый на $Z/2Z$ полином с корнем β [2].

Таблица 5. **Простые числа вида $p=8k\pm1$ в диапазоне от 7 до 309 соответствующих величин $(p-1)/2$ при условии, что 2^m-1 делится на p**

p	m	$\frac{p-1}{2}$	p	m	$\frac{p-1}{2}$	p	m	$\frac{p-1}{2}$
7	3	3	97	48	48	223	37	111
17	8	8	103	51	51	233	29	116
23	11	11	113	28	56	239	119	119
31	5	15	127	7	63	241	24	120
41	20	20	137	68	68	257	16	128
47	23	23	151	15	75	263	131	131
71	35	35	167	83	83	271	135	135
73	9	36	191	95	95	281	70	140
79	39	39	193	96	96			
89	11	44	199	99	99			

Двоичные КВ-коды имеют простую длину $n=p=8k\pm1$, являются циклическими, делятся на четыре класса, поскольку порождаются в кольце R_p как идеалы одним из полиномов следующих четырех видов: $q(x),(x-1)q(x),n(x),(x-1)n(x)$ [2, с. 464]. Здесь $q(x)$ и $n(x)$ – специальные полиномы степени $(p-1)/2$ из кольца $GF(2)[x]$: $q(x)=\prod_{i\in Q}(x-\beta^i)$; $n(x)=\prod_{r\in N}(x-\beta^r)$; β – примитивный корень p-й степени из 1; Q – циклическая подгруппа квадратов (квадратичных вычетов по модулю p) мультипликативной группы $GF(p)^*$ поля $GF(p)$; N – множество квадратичных невычетов по модулю p.

Отметим, что подгруппа Q имеет порядок $(p-1)/2$, содержит всю циклическую группу $<2>$, порожденную классом вычетов 2 в $GF(p)=Z/pZ$. Ту же мощность $(p-1)/2$ имеет и множество N квадратичных невычетов. Полиномы $q(x)$ и $n(x)$ имеют степень $(p-1)/2$.

Если какой-то элемент попал в Q, то, очевидно, и вся циклическая подгруппа, им порожденная, принадлежит Q. Отсюда следует, что в полиноме $q(x)=\prod_{i\in Q}(x-\beta^i)$ вместе с каждым множителем $x-\beta^i$ содержатся и множители $x-\beta^j$ со всеми сопряженными элементу β^i элементами β^j поля $GF(2^m)$, содержащего β. Отсюда следует, что коэффициенты полинома $q(x)=\prod_{i\in Q}(x-\beta^i)$ должны принадлежать полю $GF(2)$, при этом $q(x)$ должен делиться на полином $M_\beta(x)$.

О принадлежности КВ-кодов классу кодов Хемминга. Пусть $C_{q(x)}$ – КВ-код – циклический код длиной p, порожденный полиномом $q(x)$ в кольце R_p, причем $m=(p-1)/2$. Тогда $q(x)$ совпадает с неприводимом полином $M_p(x)$ элемента β над $Z/2Z$. Отсюда, и из приведенных выше вычислений вытекает

Теорема 2. *Класс КВ-кодов $C_{q(x)}$, определенных над полем $GF(2^m)$ с $m=(p-1)/2$, принадлежит семейству кодов Хемминга.*

Из свойств КВ-кодов непосредственно вытекает

Следствие. *Коды Хемминга простой длины $p=8k\pm1$ с полем определения $GF(2^{(p-1)/2})$ имеют минимальное расстояние $d\ge\sqrt{p}$.*

Никаких ограничений на величину длины кода Хемминга (кроме требования нечетности) не существует. Отсюда следует в силу сказанного, что реальное минимальное расстояние кодов Хемминга может принимать сколь угодно большие значения.

В табл. 6 приведены первые 9 КВ-кодов, являющихся кодами Хемминга, с указанием их точного минимального расстояния.

Таблица 6. **КВ-коды, являющиеся кодами Хемминга, с указанием их точного минимального расстояния**

$n = p = 8s \pm 1$	17	23	41	47	71	79	97	103	137
$\frac{p-1}{2} = m$	8	11	20	23	35	39	48	51	68
$\sqrt{p} \approx$	4,1	4,8	6,4	6,9	8,4	8,9	9,9	10,1	11,7
Точное d	5	7	9	11	11	15	11	11	13

Заключение. Примитивные коды Хемминга имеют минимальное расстояние три и исправляют только ошибки весом один. Проведенные исследования показывают, что примерно треть не примитивных кодов Хемминга имеют те же параметры. Однако более трети не примитивных кодов Хемминга имеют минимальное расстояние больше трех. Имеется так же бесконечно много кодов Хемминга простой длины, совпадающих с квадратично-вычетными кодами. Отсюда следует, что не примитивные коды Хемминга могут иметь сколь угодно большие минимальные расстояния. Данный факт служит неоспоримым свидетельством в пользу практической применимости не примитивных кодов Хемминга.

Литература

1. *Хемминг Р. В.* Коды с обнаружением и исправлением ошибок. М., 1956.
2. *Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.* Теория кодов, исправляющих ошибки. М., 1979.
3. *Липницкий В. А., Конопелько В. К.* Норменное декодирование помехоустойчивых кодов и алгебраические уравнения. Мн, 2007.
4. *Курилович А. В., Липницкий В. А., Михайловская Л. В.* // Сб. науч. статей. Вып. 2: Технологии информатизации и управления. Мн., 2011. С. 43–49.
5. *Липницкий В. А., Олексюк А. О.* // Докл. БГУИР. 2014. № 8 (86). С 72 – 78.
6. *Липницкий В. А.* Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа: Учеб. пособие. М., 2006.
7. *Лидл Р., Недеррайтер Г.* Конечные поля: В 2 т. Пер. с англ. М., 1988.
8. *Виноградов И. М.* Основы теории чисел. М., 1972.
9. *Конопелько В. К., Липницкий В. А.* Теория норм синдромов и перестановочное декодирование помехоустойчивых кодов. Мн., 2000.
10. *Липницкий В. А.* Теория норм синдромов: Методич. пособие. Мн., 2011.

V. A. LIPNITSKI, A. O. ALIAKSIUK

ASSESSMENT OF MINIMUM DISTANCES OF NON-PRIMITIVE HAMMING CODES

Summary

It is proved that under certain conditions, non-primitive Hamming codes are quadratic residue codes, and can be at arbitrarily large minimum distance. Therefore, unlike primitive Hamming codes without decoding the primitive have unlimited possibilities.