УДК 512 (075 .8)

НОВЫЕ НЕПРИМИТИВНЫЕ КОДЫ, ОБРАЗОВАННЫЕ ИЗ ПРИМИТИВНЫХ БЧХ-КОДОВ И КОДОВ ХЕММИНГА И ИХ НОРМЕННАЯ ОБРАБОТКА

В.К. КОНОПЕЛЬКО[1], В.А. ЛИПНИЦКИЙ[2]

[1]*Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь*

[2]*Военная академия Республики Беларусь, Республика Беларусь*

Поступила в редакцию 22 марта 2019

Аннотация. В работе проводится интегрированное завершение исследований БЧХ-кодов произвольных длин. Наибольшее внимание уделено кодам, длины которых являются промежуточными между примитивными длинами, которые получаются выбрасыванием специальным образом из проверочных матриц примитивных БЧХ-кодов большого количества столбцов, но с сохранением свойств цикличности, которые предлагается называть непримитивными БЧХ-кодами. Систематически исследуются свойства названного класса кодов. Доказывается, что по разнообразию длин примерно треть непримитивных БЧХ-кодов имеют кодовое расстояние, большее конструктивного, и, следовательно, они способны корректировать случайные ошибки, кратность которых существенно превышает конструктивные рамки. Коррекцию таких ошибок называем плюс-декодированием. Показано, что реализовать плюс-декодирование невозможно известными классическими методами и алгоритмами, а только имеющимися и развивающимися средствами теории норм синдромов. В работе предложены два алгоритма реализации плюс-декодирования перестановочными норменными методами. Непримитивные БЧХ-коды перспективны для приложений в реальных современных инфокоммуникационных системах.

Ключевые слова: минимальное расстояние кода, кратность ошибки, БЧХ-код, синдром ошибок, автоморфизм кода.

Abstract. Integrated studies completion of BCH codes of different lengths is devoted. Most attention is paid to codes whose lengths are intermediate between primitive lengths, which are obtained by throwing in a special way from the check matrices of primitive BCH codes of a large number of columns, but with preservation of cyclical properties, which are proposed to be called non-primitive BCH codes. The properties of the named code class are systematically investigated. It is proved that, according to the variety of lengths, about a third of the non-primitive BCH codes have a code distance greater than constructive, and, therefore, they are able to correct random errors, the multiplicity of which significantly exceeds the constructive frame. Correction of such errors is called plus-decoding. It is shown that it is impossible to implement plus-decoding by known classical methods and algorithms, but only by the available and developing means of the theory of norms syndromes. Two algorithms for the implementation of plus-decoding by permutation normal methods are proposed. Non-primitive BCH-codes are promising for applications in real modern information and communication systems.

Keywords: minimum code distance, error multiplicity, BCH code, error syndrome, code automorphism.

Doklady BGUIR. 2019, Vol. 121, No. 3, pp. 12-24
New non-primitive codes formed from primitive BCH and Hamming codes and their norm evaluation
V.K. Konopelko, V.A. Lipnitski

Введение

Современная информационная эпоха, начавшаяся с 80-х годов XX века, характеризуется экспоненциальным ростом потоков передаваемой и хранимой информации, всеобщей компьютеризацией, технологической революцией. Она сопровождается всеобщей экспансиея цифровых систем передачи информации. Надежность и достоверность передачи и хранения информации в них достигается применением спектра помехоустойчивых кодов. К последним предъявляются различные и порой противоречащие друг другу требования: применение кодов различной длины с высокой корректирующей способностью и высоким быстродействием, масштабируемостью.

Корректирующий потенциал каждого линейного кода обеспечивается объемом его спектра ошибок с попарно различными синдромами. Однако декодирование прямыми развязками типа «синдром–ошибка» эффективны лишь при исправлении одиночных ошибок. Современные же коды рассчитаны на исправление ошибок кратности $\nu > 1$. Как правило, этот потенциал реализуется в декодерах составлением и решением над полями Галуа алгебраических уравнений соответствующей степени. В современном помехоустойчивом кодировании наиболее острой является проблема «селектора». Суть ее – в быстром и надежном нахождении нужного вектора-ошибки среди огромной массы всего корректируемого многообразия ошибок [1, 2].

Белорусская алгебраическая школа и белорусская школа цифровой обработки сигналов хорошо известны в научном мире. Их представителями в начале XXI века проведены широкие исследования использования автоморфизмов помехоустойчивых кодов. Это привело к формированию понятия норм синдромов ошибок в кодах Боуза-Чоудхури-Хоквингема (БЧХ-кодах), устанавлению независимости норм синдромов от циклических сдвигов координат векторов-ошибок, исследованию иных свойств норм синдромов, созданию развитой теории норм синдромов (ТНС) [2, 3]. Теория норм синдромов позволила предложить эффективные перестановочные норменные методы коррекции ошибок, альтернативные методам решения алгебраических уравнений, на порядок снижающие влияние проблемы «селектора». Знакомству с дальнейшими результатами по применению ТНС в помехоустойчивом кодировании и посвящена данная статья.

Краткие сведения о строении БЧХ-кодов

БЧХ-код – это линейный (n, k)-код, то есть k-мерное подпространство в n-мерном двоичном пространстве (над полем $GF(2) = Z / 2Z$). Точное определение БЧХ-кодов напрямую связано с полями Галуа $GF(2^m)$. Наиболее популярны в приложениях циклические коды C_{2t+1}, которые задаются проверочными матрицами вида

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

Здесь β – элемент мультипликативной группы $GF(2^m)^*$ поля $GF(2^m)$ порядка $n = \left(2^m - 1\right)/\tau$ для некоторого делителя τ числа $\left|GF(2^m)^*\right| = 2^m - 1$, в частности $\tau = 1$, $0 \le i \le (n-1)$. Длина кода C_{2t+1} равна n и всегда является нечетной величиной [1]. Такие коды называют БЧХ-кодами с конструктивным расстоянием $2t+1$, поскольку они рассчитаны на исправление t-кратных случайных ошибок, имеют наибольшую размерность среди подобных кодов и скорость передачи информации.

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 $\tau > 1$, то $\beta \ne \alpha$ и код C_{2t+1} называют непримитивным, что также вполне естественно.

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 [3], $rank\left(\beta^{2i-1}, \beta^{2j-1}\right)^T = rank(\beta^{2i-1}) = m$. 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]. 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 $2t+1$. 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 $d = 11$ [2], у БЧХ-кодов C_{17} с длинами 63 и 127 $\delta = 17$, а $d = 19$.

Непримитивные коды предоставляют массу подобных примеров [3, 4]. Глубинная причина существования таких примеров 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, 5]. Очевидно, все столбцы проверочной ($tm \times n$)-матрицы $H_{\text{непр}}$ каждого непримитивного БЧХ-кода над полем $GF(2^m)$ принадлежат $H_{\text{прим}}$-проверочной ($tm \times (2^m - 1)$)-матрице примитивного БЧХ-кода над тем же полем, а матрица $H_{\text{непр}}$ получается из $H_{\text{прим}}$, по сути дела, выбрасыванием большого числа 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, что является сложной задачей, применяя один из четырех подходов, разработанных именно для БЧХ-кодов [2, 3].

В монографиях [2, 3] содержатся различные аспекты ТНС, разработанные в основном для примитивных реверсивных и БЧХ-кодов. Наиболее подробно рассмотрены, вплоть до практических приложений, коды с минимальным расстоянием 5. В [4, 5] для БЧХ-кодов, исправляющих тройные ошибки, разработан оригинальный метод сжатия норм синдромов.

Свойства непримитивных БЧХ-кодов

Систематическое исследование непримитивных БЧХ-кодов и перенос на них ТНС приведено в [3], продолжено в работе [6] и далее в [7–9]. Из [1] известно, что примитивные коды C_5 , которые задаются проверочными матрицами

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

с $\beta = \alpha$, при $m \geq 4$ имеют ранг матрицы (2), равный $2m$, их циклотомические классы $C(1) \neq C(3)$, а размерность $k = n - 2m$, при этом минимальное расстояние $d = \delta = 5$. К сожалению, у непримитивных кодов C_5 любое из перечисленных соотношений может нарушиться. В каждом конкретном случае необходима внимательная проверка каждого параметра кода, что сопровождается дополнительными вычислениями и зачастую требует серьезных компьютерных ресурсов.

Ранг подматрицы $(\beta^{3i}) = \left(1, \beta^3, \beta^6, ..., \beta^{3(n-1)}\right)$ матрицы (2) и матрицы (1) чаще всего также равен m. Очевидно, из трех последовательных нечетных натуральных значений числа n одно делится на три, а два – не делятся на три. Пусть НОД$(3, n) = 1$. Пусть отображение φ_3 циклической группы $\left\{1, \beta, \beta^2, ..., \beta^{n-1}\right\}$ порядка n в себя действует по правилу $\varphi_3(x) = x^3$. Оно является автоморфизмом этой группы (см. [10], теорема 2.12.3). Отсюда, в частности, следует, что β^3 имеет тот же порядок в мультипликативной группе $GF(2^m)^*$, что и его прообраз $\beta = \varphi_3^{-1}(\beta^3)$ при отображении φ_3 . По построению, поле $GF(2^m)$ является минимальным, содержащим β . Это означает, что неприводимый полином над $GF(2)$ с корнем β должен иметь степень m . В силу сказанного то же самое должно иметь место и для β^3 . Отсюда вытекает, что элементы $1, \beta^3, \beta^6, ..., \beta^{3(m-1)}$ образуют линейно независимую над $GF(2)$ систему и, следовательно, $rank(\beta^{3i}) = m$.

Пусть n делится на три. Здесь возможны два варианта:

1) β^3 остается элементом поля $GF(2^m)$ и не принадлежит никакому подполю этого поля;

2) существует подполе $GF(2^\mu)$ поля $GF(2^m)$, содержащее β^3 .

Первый случай, очевидно, означает, что над полем $GF(2)$ неприводимый полином элемента β^3 обязан иметь степень m , а в таком случае $rank(\beta^{3i}) = m$. Второй случай, по тем же причинам, означает, что $rank(\beta^{3i}) = \mu$ для некоторого $\mu < n$, а точнее, для некоторого делителя μ числа m .

Вот пример, иллюстрирующий второй случай. БЧХ-код C_5 длиной 219 определен над полем $GF(2^{18})$. $2^{18} - 1 = 7 \cdot 9 \cdot 57 \cdot 73$. Здесь матрица (2) задается элементом $\beta = \alpha^{57 \cdot 21} = \alpha^{1197}$, а элемент $\beta^3 = \alpha^{57 \cdot 21 \cdot 3} = \alpha^{57 \cdot 7 \cdot 9}$ имеет порядок 73. Но тогда элемент β^3 должен принадлежать мультипликативной группе $GF(2^9)^*$, имеющей порядок $2^9 - 1 = 7 \cdot 73$. Но тогда $rank(\beta^{3i}) \leq 9$.

Элементы β и β^3 не должны быть сопряженными в поле $GF(2^m)$, то есть не должны быть корнями одного и того же неприводимого над полем $GF(2)$ полинома, что, как отмечалось выше, эквивалентно неравенству $C(1) \neq C(3)$ циклотомических классов. Однако это свойство не всегда выполняется. Например, у БЧХ-кода C_5 длиной 95 имеет место совпадение: $C(1) = C(3)$. Поэтому рассматриваемый код C_5 реально относится к классу кодов Хемминга.

Приведем еще некоторые примеры. Имеется 46 нечетных значений возможной длины n БЧХ-кодов в диапазоне от 9 до 99. Для 14 значений длины выполняется неравенство $n < 2m$. Это значения $n = 9$, 11, 13, 19, 25, 27, 29, 37, 53, 59, 61, 67, 81, 83. Для каждого из перечисленных значений длины БЧХ-коды C_5 не существуют. В диапазон от 9 до 99 попадают три значения длины – 15, 31 и 63 – длины примитивных БЧХ-кодов C_5 . Семь БЧХ-кодов C_5 длиною 17, 23, 41, 47, 71, 79, 97 имеют размерность 1. 21 оставшихся в диапазоне длин от 9 до 99 БЧХ-кодов C_5 имеют размерность больше 1 (с длинами 21, 33, 35, 39, 43, 45, 49, 51, 55, 57, 65, 69, 73, 75, 77, 85, 87, 89, 91, 93, 99). Среди них двенадцать (более половины кодов!) имеют $d > 5$. Пять из них имеют $d = 7$ ($n = 49$ (здесь $C(3) = C(5)$), 69, 73, 77 (здесь $C(3) = C(5)$), 91 (здесь $C(3) = C(5)$)), пять имеют $d = 9$ (при $n = 33$, 57, 87, 89 и 99),

один – длиною 39 – имеет $d = 10$ (здесь $C(1) = C(5)$), один – длиною 43 – имеет $d = 13$ (здесь $C(3) = C(5)$). Более подробная информация о названных 21 кодах C_5 сосредоточена в табл. 1.

Таблица 1. **Непримитивные БЧХ-коды C_5 над полями $GF(2^m)$ в диапазоне длин от 9 до 99, размерность которых k**

№ п/п	1	2	3	4	5	6	7	8	9	10	11
n	21	33	35	39	43	45	49	51	55	57	65
m	6	10	12	12	14	12	21	8	20	18	12
k	9	13	11	15	15	21	7	35	15	21	41
d	5	9	5	10	13	5	7	5	5	9	5

№ п/п	12	13	14	15	16	17	18	19	20	21
n	69	73	75	77	85	87	89	91	93	99
m	22	9	20	30	8	28	11	12	10	30
k	25	55	35	17	69	31	67	67	73	39
d	7	7	5	7	5	9	9	7	5	9

Вычисления с непримитивными БЧХ-кодами длиной $n > 99$ подтверждают сохранение отмеченной тенденции – примерно 1/3 всех непримитивных БЧХ-кодов с $\delta = 5$ имеют $d > 5$. Вот некоторые примеры.

Над полем $GF(2^{36})$ определены коды C_5 длиной 109 и 111. У первого равны между собой следующие циклотомические классы: $C(3) = C(5) = C(7)$. Значит, у данного кода минимальное расстояние $d \geq 9$. У второго кода $C(1) = C(5) = C(7)$, $C(3) = C(9)$. Значит, у данного кода минимальное расстояние $d \geq 11$.

Над полем $GF(2^{52})$ определены коды C_5 длиной 157 и 159. У первого равны между собой следующие циклотомические классы: $C(3) = C(5)$, $C(1) = C(7)$. Значит, у данного кода минимальное расстояние $d \geq 9$. У второго кода $C(1) = C(5) = C(7)$; $C(3) = C(9)$. Значит, у данного кода минимальное расстояние $d \geq 11$.

Как уже отмечалось, определение точного значения минимального расстояния для конкретных кодов – достаточно трудоемкая задача, требующая серьезных компьютерных вычислений, индивидуальных подходов и методов в каждом отдельном случае.

Непримитивные коды Хемминга

Всякий примитивный двоичный код Хемминга имеет длину $n = 2^m - 1$, размерность $k = n - m$, задается проверочной матрицей $H = (\alpha^i)$ над полем Галуа $GF(2^m)$, имеет минимальное расстояние $d = 3$, а потому способен исправлять только одиночные ошибки.

Если продолжать терминологию из [1], непримитивные коды Хемминга могут иметь любую нечетную длину $n \neq 2^m - 1$. Задаются они проверочной матрицей (1) при минимальном значении $t = 1$. При таком задании коды Хемминга могут иметь минимальное расстояние $d > 3$, как например, код длиной 17 ($d = 5, k = 8$) или код длиной 23 – двоичный код Голея.

В [8] установлено, что если длина $n = p \cdot s$ делится на простое число p, то код Хемминга длиной n содержит кодовые слова весом p. Отсюда следует, что его минимальное расстояние $d \leq p$. В частности, при n, делящемся на 3, минимальное расстояние кода Хемминга $d = 3$. Таким образом, коды Хемминга простой длины или длины, не имеющей малых делителей, имеют все шансы на большое минимальное расстояние. Проведенные исследования всех кодов Хемминга в диапазоне длин от 9 до 109 показывают, что, как и для БЧХ-кодов, примерно на трети длин коды Хемминга имеют минимальное расстояние, большее трех. Более того, доказана следующая теорема.

Теорема 1. Для любого наперед заданного целого числа $d_0 > 3$ найдется двоичный код Хемминга, минимальное расстояние которого $d \geq d_0$.

Доказательство базируется на том, что бесконечное число квадратично-вычетных кодов (КВ-кодов) принадлежит классу непримитивных кодов Хемминга.

Двоичные КВ-коды имеют простую длину $n = p = 8k \pm 1$, они являются циклическими кодами, порождаются как идеалы в кольце полиномов $R_p = GF(2)[x]/ < x^p - 1 >$ одним из полиномов следующих четырех видов: $q(x), (x-1)q(x), n(x), (x-1)n(x)$ [1]. $q(x)$ и $n(x)-$ специальные полиномы степени $(p-1)/2$ из кольца $GF(2)[x]$: $q(x) = \prod_{i \in Q}(x - \beta^i)$; $n(x) = \prod_{r \in N}(x - \beta^r)$, где $\beta -$ примитивный корень p-й степени из 1 в расширении $GF(2^m)$ поля $GF(2)$ наименьшей степени m; $Q -$ подгруппа квадратов (квадратичных вычетов по модулю p) циклической мультипликативной группы $GF(p)^*$ поля $GF(p)$, являющейся, очевидно, циклической подгруппой; $N -$ множество квадратичных невычетов по модулю p.

Заметим, что имеется бесконечно много простых чисел вида $p = 8k \pm 1$ [11]. Как известно [11], для простых $p = 8k \pm 1$ в поле $GF(p) = Z / pZ$ класс 2 является квадратичным вычетом, то есть $2^{(p-1)/2} \equiv 1 (\mathrm{mod}\, p)$. Поэтому класс 2 принадлежит группе Q, вместе со всей циклической подгруппой $< 2 >$, порожденной классом вычетов 2. Сама же группа Q имеет порядок $(p-1)/2$. Ту же мощность $(p-1)/2$ имеет и множество N квадратичных невычетов.

Как отмечено выше, $2^{(p-1)/2} - 1$ делится на p для рассматриваемых значений p. Поэтому поле $GF(2^m)$ с минимальным m, содержащее корень β, имеет показатель $m = (p-1)/2$ или делящий число $(p-1)/2$. Обозначим через $C_{q(x)}$ квадратично-вычетный код циклический код длиной p, порожденный полиномом $q(x)$ в кольце R_p. При этом предполагаем, что $m = (p-1)/2$. Тогда $q(x)$ совпадает с неприводимом полином $M_\beta(x)$ элемента β над $Z/2Z$, поскольку они имеют одинаковую степень и общий корень β^2. Отсюда следует теорема.

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 квадратично-вычетных кодов [1] непосредственно вытекает следующее.

Следствие. Коды Хемминга, имеющие простую длину $n = p = 8k \pm 1$ и поле определения $GF(2^{(p-1)/2})$, имеют минимальное расстояние $d \geq \sqrt{p}$.

Следовательно, минимальное расстояние непримитивных кодов Хемминга может принимать сколь угодно большие значения.

Проблемы, вопросы и решения, связанные с коррекцией ошибок, выходящих за рамки констуктивных возможностей кодов, предлагается кратко обозначить как «плюс-декодирование».

Теория норм синдромов [2, 3], давшая существенное решение проблемы «селектора», предоставляет и конструктивные подходы к разрешению проблем «плюс-декодирования». Рассматрим их в приложении к непримитивным БЧХ-кодам с малым конструктивным расстоянием.

Возможности плюс-декодирования для БЧХ-кодов C_5

В XX веке проблема коррекции декодирования ошибок, выходящих за рамки конструктивных возможностей, имела частный характер, количество таких ошибок было не очень значительным [2]. В случае непримитивных БЧХ-кодов ситуация значительно меняется. Увеличение кодового расстояния d на два по сравнению с конструктивным влечет увеличение кратности исправляемых ошибок на единицу. Их же количество определяется с помощью биномиальных коэффициентов.

По своему построению БЧХ-код C_5 рассчитан на исправление одиночных и двойных ошибок, количество которых $K_{констр} = C_n^1 + C_n^2 = \frac{n(n+1)}{2}$. Если у данного кода C_5 реальное минимальное расстояние $d = 7$ (в табл. 1 отмечены пять таких кодов), то этот код должен

исправлять и тройные ошибки в количестве $C_n^3 = \frac{n(n-1)(n-2)}{2 \cdot 3}$. Данное количество ошибок и составляет потенциал K^+ плюс-декодирования. Очевидно, здесь K^+ превосходит $K_{\text{констр}}$ почти в $\frac{n}{3}$ раз. Если же код C_5 имеет реальное значение $d = 9$ (в табл. 1 отмечено пять таких кодов), то $K^+ = C_n^3 + C_n^4 = \frac{(n+1)n(n-1)(n-2)}{2 \cdot 3 \cdot 4}$. Это превосходит $K_{констр}$ почти в $\frac{n^2}{12}$ раз (см. табл. 2).

Таблица 2. **Потенциал конструктивного и плюс-декодирования у БЧХ-кодов C_5 в диапазоне длин от 9 до 99, размерность которых $k > 1$ и $d \geq 7$**

№ п/п	1	2	3	4	5	6
N	33	39	43	49	57	69
M	10	12	14	21	18	22
D	9	10	13	7	9	7
$K_{\text{констр}}$	561	780	946	1225	1653	2415
K^+	46376	91390	7194803	18424	424770	52394
N	73	77	87	89	91	99
M	9	30	28	11	12	30
D	7	7	9	7	7	9
$K_{\text{констр}}$	2701	3003	3828	4005	4186	4950
K^+	62196	73150	2331890	2555190	121485	3921225

Данные табл. 2 демонстрируют, что в БЧХ-кодах C_5 на плюс-декодирование приходится в десятки тысяч раз больше векторов-ошибок, чем на конструктивное декодирование.

Реализация возможностей плюс-декодирования с помощью ТНС

Пусть минимальное расстояние кода $d = 2t+1$ или $d = 2t+2$. Тогда в данном коде синдромы всех векторов-ошибок весом ω, $1 \leq \omega \leq t$, попарно различны. Это свойство служит теоретической гарантией возможности коррекции кодом всех ошибок весом ω, $1 \leq \omega \leq t$. Практически же реализация данной возможности зависит от кодов, кратности ошибок и многих иных факторов. При $t = 1$ возможна прямая связь «синдром – ошибка». При $t = 2$ коррекция двойных ошибок в БЧХ-кодах C_5 осуществляется сведением к решению квадратных уравнений в поле определения кода $GF(2^m)$.

Однако стандартных методов коррекции ошибок, выходящих за конструктивные рамки, не существует. Не найти квадратным уравнением координаты тройной ошибки. С другой стороны, слишком слабы структурные возможности синдромов в БЧХ-коде C_5, чтобы составить кубическое уравнение для нахождения координат тройной ошибки. Для плюс-декодирования БЧХ-кодов C_5 явно требуются иные подходы.

Теория норм синдромов опирается на свойство цикличности БЧХ-кодов C с проверочными матрицами (1) и (2). Пусть n – длина кода C и $AutC$ – его группа автоморфизмов. $AutC$ содержит циклическую подгруппу $\Gamma = <\sigma>$ порядка n, состоящую из степеней σ-линейного преобразования двоичного векторного пространства V_n, действующего на каждый вектор $\bar{x} = (x_1, x_2, ..., x_n) \in V_n$ по правилу

$$\sigma(x_1, x_2, ..., x_n) = (x_n, x_1, x_2, ..., x_{n-1}). \quad (3)$$

Пространство V_n, а с ним и совокупность K_C декодируемых БЧХ-кодом C векторов-ошибок, разбиваются под действием группы Γ на попарно непересекающиеся классы –

Г-орбиты. Каждая *Г*-орбита состоит из своеобразного кольца переходящих друг в друга под действием степеней σ векторов и, следовательно, однозначно определяется любым из своих представителей. В силу соотношения (3) всякая Г-орбита J имеет следующее строение:

$$J = \left\{\bar{e}, \sigma(\bar{e}), ..., \sigma^{\mu-1}(\bar{e})\right\} \quad (4)$$

для произвольного фиксированного вектора $\bar{e} \in J$. Здесь $\mu > 1$ – наименьшее натуральное число с условием $\sigma^{\mu}(\bar{e}) = \bar{e}$. Число μ – делитель длины n кода C. Чаще всего $\mu = n$. В последнем случае Г-орбита называется полной. Равенство (4) служит основанием для более точного обозначения Г-орбит: $J = <\bar{e}>$.

Отображение двоичных пространств $\varphi_H : V_n \to V_{2m}$, действующее по правилу $\bar{y} = \bar{x} \cdot H^T$, есть линейный оператор. Согласно основам линейной алгебры, полный образ $\varphi_H(V_n)$ есть подпространство пространства V_{2m} размерностью $n - \dim KerH = n - k = 2m$. Это означает, что $\varphi_H(V_n) = V_{2m}$.

В силу формулы (2) каждая вектор-ошибка $\bar{e}$ в БЧХ-коде C_5, определенном над полем $GF(2^m)$, имеет синдром $S(\bar{e}) = H \cdot \bar{e}^T = \left(s_1, s_2\right)^T$ для $s_1, s_2 \in GF(2^m)$. Равенство $\varphi_H(V_n) = V_{2m}$ влечет, что для произвольных $s_1^*, s_2^* \in GF(2^m)$ существует вектор $\bar{e} \in V_n$ такой, что $S(\bar{e}) = H \cdot \bar{e}^T = \left(s_1^*, s_2^*\right)^T$.

Согласно [2, 3], действие оператора циклического сдвига σ на каждый вектор ошибок $\bar{e}$ однозначно отражается в коде C_5 на компонентах синдрома этого вектора по формуле

$$S(\sigma(\bar{e})) = \left(\beta \cdot s_1, \beta^3 \cdot s_2\right)^T. \quad (5)$$

Из формулы (5) вытекает структура спектра синдромов $S(<\bar{e}>)$ Г-орбиты $<\bar{e}>$:

$$S(<\bar{e}>) = \left\{\beta^i \cdot s_1, \beta^{3i} \cdot s_2\right\}, \quad 0 \le i \le n-1. \quad (6)$$

Формулы (5), (6) означают, что если у двух Г-орбит найдутся векторы с одинаковыми синдромами, то спектры синдромов этих орбит совпадают полностью. Формула (5) послужила основой для следующего определения. Нормой синдрома $S(\bar{e}) = \left(s_1, s_2\right)^T$ в БЧХ-коде C_5 называется величина

$$N = N(S(\bar{e})) = \begin{cases} \dfrac{s_2}{s_1^3};\ s_1 \neq 0; \\ +\infty;\ s_1 = 0,\ s_2 \neq 0. \end{cases} \quad (7)$$

Нормы синдромов обладают рядом важных свойств. Во-первых, норма может быть любым элементом поля $GF(2^m)$, а также имеет одно особое значение: $+\infty$. Всего, таким образом, норма принимает $n + 2 = 2^m + 1$ значений. Во-вторых, у всех векторов, принадлежащих отдельно взятой Г-орбите J, норма синдрома одинакова. Это единственное значение естественно назвать нормой $N(J)$ данной Г-орбиты J. Таким образом, $N(J) = N(S(\bar{e}))$ для произвольного вектора $\bar{e} \in J$.

В третьих, если две *Г*-орбиты J_1 и J_2 имеют различные нормы, то спектры синдромов этих орбит не пересекаются, то есть эти *Г*-орбиты не могут иметь векторов с одинаковыми синдромами.

В четвертых, синдромы равномерно распределены по значениям норм синдромов: для каждого из $n + 2 = 2^m + 1$ значений N норм синдромов найдется в точности $n = 2^m - 1$ различных синдромов, норма которых равна N. В самом деле, пусть у синдрома $S(\bar{e}) = \left(s_1, s_2\right)^T$ компонента $s_1 \neq 0$ и пусть $N(S(\bar{e})) = N$. Тогда для примитивного элемента α поля $GF(2^m)$ различные n синдромов $\left(\alpha^i \cdot s_1, \alpha^{3i} \cdot s_2\right)^T$, $0 \le i \le n-1$, принимают то же значение нормы N. Для всех $n = 2^m - 1$ синдромов вида $\left(0, s_2\right)^T$, где $s_2 \neq 0$, $s_2 \in GF(2^m)$, норма

$N(S)=+\infty$. Таким образом, рассмотрено уже $n(n+2)=(2^m-1)\cdot(2^m+1)=2^{2m}-1$ синдромов. Добавим к ним нулевой синдром. Получим весь спектр синдромов в БЧХ-коде C_5, что и завершает доказательство.

В-пятых, у примитивных БЧХ-кодов из равенства $N(J_1)=N(J_2)$ для двух полных Γ-орбит J_1 и J_2 с полными спектрами синдромов следует также равенство и самих синдромов: для всякого вектора $\bar{f}\in J_1$ найдется вектор $\bar{g}\in J_2$ такой, что их синдромы равны: $S(\bar{f})=S(\bar{g})$.

Для непримитивных БЧХ-кодов ситуация сложнее. Здесь всякая полная Γ-орбита J с полным спектром синдромов $S(J)$ содержит $n=(2^m-1)/\tau$ различных векторов с n попарно-различными синдромами из $S(J)$. Отсюда следует, что может существовать τ различных полных Γ-орбит с попарно непересекающимися полными спектрами синдромов и с одной и той же нормой.

Приведенное рассуждение демонстрирует, как действие автоморфизмов кодов на векторы ошибок взаимно однозначно отображается на числах – на синдромах. Отлаженная веками алгебра чисел позволит, несомненно, найти эффективный алгоритм определения самих векторов-ошибок вычислениями с их синдромами и нормами.

Действительно, теория норм синдромов обеспечивает свой оригинальный взгляд на декодирование ошибок. Она предлагает рассматривать не отдельные векторы ошибок, а их Г-орбиты. Любую декодируемую совокупность K векторов-ошибок с попарно различными синдромами можно распределить на множество K/Γ непересекающихся Γ-орбит этих ошибок. Для идентификации каждой конкретной Γ-орбиты J достаточно зафиксировать один из ее представителей $\bar{e}_J$. Все остальные векторы орбиты легко строятся циклическими сдвигами координат вектора $\bar{e}_J$.

Все Г-орбиты J декодируемой данным кодом C совокупности K_C векторов-ошибок обязательно имеют попарно непересекающиеся спектры синдромов $S(J)$. Спектр $S(J)$ однозначно восстанавливается по формуле (5) из синдрома $S(\bar{e}_J)$, как уже отмечалось выше.

Зафиксируем список 1 образующих $\bar{e}_J$ совокупности K_C/Γ, список 2 синдромов $S(\bar{e}_J)$, а также список 3 норм $N(S(\bar{e}_J))$. Благодаря им можно легко определить «ряд и место» подлежащей определению вектор-ошибки $\bar{e}$ в каждом конкретном сообщении $\bar{x}$, которое принято ТКС на основе кода C.

Алгоритм 1 – норменное декодирование на основе Г-орбит

Инфокоммуникационная система (ИКС), получив очередное сообщение $\bar{x}$, вычисляет его синдром ошибок $S(\bar{x})=S(\bar{e})$. Пусть $S(\bar{x})=S(\bar{e})\neq\bar{0}$. Это свидетельствует о наличии в сообщении неизвестной и подлежащей определению вектор-ошибки $\bar{e}$. Тогда вычисляем норму $N^*=N(S(\bar{x}))$. Совпадение N^* с $N(S(\bar{e}_J))$ из списка 3 сужает круг Г-орбит декодируемой совокупности, которые могут содержать искомую вектор-ошибку $\bar{e}$ в сообщении $\bar{x}$, до небольшой группы орбит $J_1, J_2, ..., J_\theta$, $1\le\theta\le\tau$, имеющих одинаковую норму N^*.

Синдром $S(\bar{x})=S(\bar{e})=(s_1,s_2)$ должен принадлежать спектру синдромов только одной Г-орбиты J_l, $1\le l\le\theta$. Предположим, что N^* является элементом поля Галуа $GF(2^m)$. Тогда у всех рассматриваемых синдромов первая компонента $s_1\neq 0$. Пусть синдром образующей $\bar{e}_{J_l}$ Г-орбиты J_l имеет первую компоненту $s_1^{J_l}=\alpha^\nu$ для некоторого целого ν, $0\le\nu<n$. Пусть у синдрома $S(\bar{x})$ первая компонента $s_1=\alpha^\lambda$, $0\le\lambda<n$. Тогда для подходящего целого i, $0\le i<n$, согласно формуле (6), $\alpha^\lambda=\beta^i\cdot\alpha^\nu=\alpha^{\tau i+\nu}$. Полученное равенство означает, что либо $\lambda-\nu$ (если $\lambda>\nu$), либо $2^m-1+\lambda-\nu$ (если $\lambda<\nu$) делится на τ. Тогда частное i однозначно определяет

искомую вектор-ошибку: $\bar{e} = \sigma^i(\bar{e}_{J_l})$. Величина же l и есть то единственное значение из множества целых $\{1, 2, ..., \theta\}$, для которого только одна из величин $\lambda - \nu$ или $2^m - 1 + \lambda - \nu$ делится нацело на τ.

Возможно, $N^* = +\infty$. Тогда у всех рассматриваемых синдромов первая компонента $s_1 = 0$. Пусть у синдрома образующей $\bar{e}_{J_l}$ Г-орбиты J_l вторая компонента $s_2^{J_l} = \alpha^{\nu}$ для целого ν, $0 \le \nu < n$. Пусть вторая компонента синдрома $S(\bar{x})$ $s_2 = \alpha^{\lambda}$, $0 \le \lambda < n$. Тогда для подходящего целого $i, 0 \le i < n$, согласно формуле (6), $\alpha^{\lambda} = \beta^{3i} \cdot \alpha^{\nu} = \alpha^{\tau 3i + \nu}$. Полученное равенство влечет, что либо $\lambda - \nu$ (если $\lambda > \nu$), либо $2^m - 1 + \lambda - \nu$ (если $\lambda < \nu$) должно делиться на τ . Величина l и есть то единственное число из множества целых чисел $\{1, 2, ..., \theta\}$, для которого одна из величин $\lambda - \nu$ или $2^m - 1 + \lambda - \nu$ делится нацело на τ. Ясно, этим целым частным должно быть число $3i$.

Предположим, что длина кода n не делится на 3. Тогда для взаимно простых чисел n и 3 выполняется соотношение Безу: существуют такие целые числа u и v , что $3u + nv = 1$. Искомую вектор-ошибку $\bar{e}$ находим из формулы $\bar{e} = \sigma^{3ui}(\bar{e}_{J_l})$. В самом деле, $\sigma^{3ui}(\bar{e}_{J_l}) = \sigma^{3iu + nvi}(\bar{e}_{J_l}) = \sigma^{(3u+nv)i}(\bar{e}_{J_l}) = \sigma^i(\bar{e}_{J_l}) = \bar{e}$.

Случай, когда $N^* = +\infty$ и n не делится на 3, встречается весьма редко, он присущ неполным Г-орбитам, а потому рассматривается отдельно.

Таким образом, работа норменного декодера достаточно наглядно реализуется при создании списков 1–3, характеризующих Г-орбиты корректируемой совокупности векторов-ошибок. Эффективность работы норменных декодеров особенно наглядна в работе ИКС на примитивных БЧХ-кодах [3, 6]. Для непримитивных БЧХ-кодов немного усложняющим фактором является возможное наличие отдельных значений $\theta > 1$.

Циклотомические подстановки для норменного декодирования

Следует признать, что при $d > 7$ списки 1–3 становятся достаточно обширными. Работа с ними усложняется. Проблема «селектора» начинает проявлять себя на новом уровне.

Эффективным в преодолении названных затруднений является метод «сжатия» – преобразования исправляемых векторов-ошибок в ошибки с узким спектром значений норм синдромов [5, 6]. Однако разработанные подходы рассчитаны на примитивные коды и на ошибки конкретного веса, автоматически они не переносятся на ошибки большего веса. Для непримитивных же кодов они по-просту не применимы.

Группы автоморфизмов кодов остаются наиболее реальным и наиболее конструктивным средством сжатия обрабатываемой декодерами информации. Группа автоморфизмов любого из кодов C_5 содержит, к примеру, циклотомические подстановки. Их действие, свойства и применение уже рассматривалось в определенной мере в монографии [3].

Циклотомические подстановки составляют циклическую группу Ф порядка m с образующей ϕ, которая действует на каждый вектор-ошибку $\bar{e}$ с синдромом $S(\bar{e}) = (s_1, s_2)$ так, что синдром $S(\phi(\bar{e})) = (s_1^2, s_2^2)$. В таком случае, при условии $N(S(\bar{e})) = N \in GF(2^m)$, норма $N(S(\phi(\bar{e}))) = N^2$. Несложно видеть, что вектор $\phi(\bar{e})$ можно получить из вектора $\bar{e}$ по правилу: для каждого целого i, $1 \le i \le n$, i-я координата вектора $\bar{e}$ становится $(2i–1)$-й координатой вектора $\phi(\bar{e})$, если $2i - 1 \le n$, и $(2i–1–n)$-й координатой вектора $\phi(\bar{e})$, если $2i - 1 > n$.

Циклическая подстановка σ и циклотомическая подстановка ϕ связаны равенством $\phi\sigma = \sigma^3\phi$ [1, 3]. Они образуют некоммутативную группу G порядка mn – подгруппу группы $Aut(C_5)$. Пусть J – некоторая Г-орбита векторов-ошибок. Тогда $\phi(J)$ – новая Г-орбита векторов-ошибок ([3], предложение 2.17). Таким образом, группа Ф действует на множестве Г-орбит K / Γ декодируемой кодом совокупности K векторов-ошибок, разбивает его

на Ф-орбиты. Соответственно, множество K разбивается на укрупненные G-орбиты, содержащие, как правило, по mn векторов-ошибок.

Зафиксировав одну вектор-ошибку $\bar{e}$, мы можем восстановить все вектор-ошибки G-орбиты $<\bar{e}>_G$. Значит, списки 1–3 можно сократить примерно в m раз, оставив в них по одной образующей каждой G-орбиты декодируемой совокупности (см. табл. 3).

Таблица 3. **Количество Г-орбит и *G*-орбит корректируемой совокупности для БЧХ-кодов C_5 из табл. 2**

№ п/п	1	2	3	4	5	6
N	33	39	43	49	57	69
M	10	12	14	21	18	22
D	9	10	13	7	9	7
$K_{\text{констр}}$	561	780	946	1225	1653	2415
K^+	46376	91390	7194803	18424	424770	52394
$\Gamma_{\text{констр}}$	17	20	22	25	29	35
Γ^+	1405	2344	167321	376	7453	760
G^+	141	196	11952	18	415	35
N	73	77	87	89	91	99
M	9	30	28	11	12	30
D	7	7	9	9	7	9
$K_{\text{констр}}$	2701	3003	3828	4005	4186	4950
K^+	62196	73150	2331890	2555190	121485	3921225
$\Gamma_{\text{констр}}$	37	39	44	45	46	50
Γ^+	852	950	2680	28710	1335	39609
G^+	95	32	958	2610	112	1321

Алгоритм 2 – алгоритм декодирования ошибок на основе G-орбит

Пусть принято сообщение $\bar{x}$ с синдромом $S(\bar{x}) = S(\bar{e}) = (s_1, s_2)$, норма которого $N^* = N(S(\bar{x})) \in GF(2^m)$. Предположим, что N^* не принадлежит списку 3. Тогда находим такое наименьшее целое i, $1 \le i \le m$, что для $\lambda = 2^i$ величина $(N^*)^\lambda = N(S(\bar{e}_J))$ для одного или нескольких векторов $\bar{e}_J$ из списка 1 образующих G-орбит корректируемого множества векторов-ошибок. Полученное равенство норм означает, что у искомого вектора-ошибки $\bar{e}$ в сообщении $\bar{x}$ вектор $\phi^i(\bar{e})$ имеет синдром $S(\phi^i(\bar{e})) = (s_1^\lambda, s_2^\lambda)$, который принадлежит спектру синдромов $S(<\bar{e}_J>)$ одной Г-орбиты $<\bar{e}_J>$, порожденной вектором $\bar{e}_J$ из списка 1. Алгоритм 1 однозначно определяет вектор $\bar{e}_J$ и находит выражение вектора $\phi^i(\bar{e})$ через него: $\phi^i(\bar{e}) = \sigma^s(\bar{e}_J)$ для подходящего целого s, $0 \le s \le n-1$. После этого вектор $\bar{e}$ однозначно находится по формуле $\bar{e} = \phi^{m-i}(\sigma^s(\bar{e}_J))$.

Пример. Рассмотрим непримитивный $(33, 13)$ – БЧХ-код C_5. Согласно данным табл. 1–3 данный код имеет минимальное расстояние 9 и способен исправлять все случайные ошибки весом 1–4, всего 46937 векторов-ошибок, делящихся на 1423 Г-орбиты. Из них 1 Г-орбита ошибок весом 1, 16 Г-орбит ошибок весом 2, 165 полных Г-орбит ошибок весом 3 плюс одна неполная Г-орбита из 11 векторов-ошибок, порожденная вектором $\bar{e} = (1, 12, 23)$ с ненулевыми координатами на 1, 11 и 22-й позициях, львиную долю составляют 1240 Г-орбит векторов-ошибок весом 4.

Данный код обладает $2^{20} = 1\,048\,576$ попарно различными синдромами, что примерно в 20 раз превосходит количество корректируемых векторов-ошибок. Однако различных норм

синдромов в данном коде всего может быть $2^{10}+1=1025$, что меньше количества Г-орбит декодируемой совокупности. В списке 3 обязательно найдутся одинаковые нормы.

Для выяснения реальной картины следует задать поле определения данного кода – поле $GF(2^{10})$. Зафиксируем неприводимый над $GF(2)$ и примитивный полином 10-й степени, к примеру, полином $p(x)=x^{10}+x^3+1$. Пусть α – его корень. Тогда $\beta=\alpha^{31}$. Отсюда, в частности, следует, что декодируемая совокупность K может содержать до $\tau=31$ Г-орбит с одинаковым значением нормы. Среди 17 Г-орбит множества $\Gamma_{\text{констр}}$ таких быть не может (доказано в [3] для всех кодов C_5).

Проведенные вычисления приводят к интересным наблюдениям.

1. В списке 3 присутствуют все возможные значения норм синдромов.

2. В рассматриваем коде отсутствуют, за одним исключением, совпадения норм Г-орбит различного веса.

3. Среди 166 Г-орбит ошибок весом 3 имееся 10 пар Г-орбит с одинаковыми нормами, объединяющиеся в две *G*-орбиты. В качестве образующих этих *G*-орбит можно взять векторы: $\bar{e}_1=(1,3,16)$ и $\bar{e}_2=(1,15,19)$; синдромы образующих: $S(\bar{e}_1)=(\alpha^{453},\alpha^{549})$ и $S(\bar{e}_2)=(\alpha^{47},\alpha^{354})$; можно непосредственно проверить, что $N(S(\bar{e}_1))=N(S(\bar{e}_2)=\alpha^{213}$.

4. Среди ошибок весом 4 картина сложнее. Имеется 265 пар Г-орбит с одинаковыми нормами в каждой паре, имеется 70 троек Г-орбит с одинаковыми нормами в каждой тройке, имеется 45 четверок Г-орбит с одинаковыми нормами внутри каждой четверки. Имеется 15 Г-орбит с нормой 0, совпадающей с нормой $N(S(1,12,23))$. Наконец, имеется 5 Г-орбит с нормой 1, совпадающей с нормой Г-орбиты ошибок весом 1.

5. Норму $N=+\infty$ имеет в точности одна Г-орбита – единственная неполная Г-орбита, порожденная вектором-ошибкой $\bar{e}=(1,12,23)$.

6. Таким образом, 392 значения норм принимают по две и более Г-орбит, оставшиеся 633 из 1025 норм принимают в точности по одной Г-орбите декодируемого множества K/Γ.

Заключение

Новые непримитивные коды, получаемые из примитивных БЧХ-кодов и кодов Хемминга специальными процедурами, имеют различные нечетные длины и, во многих случаях, имеют корректирующий потенциал, многократно превышающий их конструктивные возможности. Последовательное применение свойств автоморфизмов кодов и построенной на их основе теории норм синдромов обеспечивает построение эффективных перестановочных норменных методов декодирования всех допустимых минимальным расстоянием ошибок в рассматриваемых линейных кодах. Тем самым обеспечивается реальная перспектива для применения на практике многих представителей построенного класса непримитивных БЧХ-кодов.

Список итературы

1. Мак-Вильямс Ф.Дж., Слоэн Н. Дж.А. Теория кодов, исправляющих ошибки. М.: Связь, 1979. 744 с.
2. Конопелько В.К., Липницкий В.А. Теория норм синдромов и перестановочное декодирование помехоустойчивых кодов. М: Едиториал, УРСС 2004. 176 с.
3. Липницкий В.А., Конопелько В.К. Норменное декодирование помехоустойчивых кодов и алгебраические уравнения. Минск: Издательский центр БГУ, 2007. 216 с.
4. Липницкий В.А., Аль-Хайдар Е.К. Норменное декодирование ошибок посредством их модификации // Докл. БГУИР. 2009. № 5 (43). С. 12–16.
5. Липницкий В.А. Теория норм синдромов. Минск: БГУИР, 2011. 96 с.
6. Курилович А.В., Липницкий В.А., Михайловская Л.В. Непримитивные коды Боуза-Чоудхури-Хоквингема и их основные параметры // Сб. науч. ст. «Технологии информатизации и управления». 2011. Вып. 2. С. 43–49.
7. Липницкий В.А., Олексюк А.О. Теория норм синдромов и плюс-декодирование // Докл. БГУИР. 2014. № 8 (86). С. 72–78.

8. Липницкий В.А., Олексюк А.О. Оценка минимальных расстояний непримитивных кодов Хемминга // Весці НАН Беларусі. 2015. № 2. С. 103–110.
9. Липницкий В.А., Олексюк А.О. Перестановочный декодер для коррекции многократных ошибок непримитивными БЧХ-кодами // Докл. БГУИР. 2015. № 3 (89). С. 117–123.
10. Липницкий В.А. Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа. Минск: БГУИР, 2006. 88 с.
11. Виноградов И.М. Основы теории чисел. М.: Наука, 1976. 168 с.

References

1. Mak-Vil'jams F.Dzh., Slojen N. Dzh.A. Teorija kodov, ispravljajushhih oshibki. M.: Svjaz', 1979. 744 s. (in Russ.)
2. Konopel'ko V.K., Lipnickij V.A. Teorija norm sindromov i perestanovochnoe dekodirovanie pomehoustojchivyh kodov. M: Editorial, URSS 2004. 176 s. (in Russ.)
3. Lipnickij V.A., Konopel'ko V.K. Normennoe dekodirovanie pomehoustojchivyh kodov i algebraicheskie uravnenija. Minsk: Izdatel'skij centr BGU, 2007. 216 s. (in Russ.)
4. Lipnickij V.A., Al'-Hajdar E.K. Normennoe dekodirovanie oshibok posredstvom ih modifikacii // Dokl. BGUIR. 2009. № 5 (43). S. 12–16. (in Russ.)
5. Lipnickij V.A. Teorija norm sindromov. Minsk: BGUIR, 2011. 96 s. (in Russ.)
6. Kurilovich A.V., Lipnickij V.A., Mihajlovskaja L.V. Neprimitivnye kody Bouza-Choudhuri-Hokvingema i ih osnovnye parametry // Sb. nauch. st. «Tehnologii informatizacii i upravlenija». 2011. Vyp. 2. S. 43–49. (in Russ.)
7. Lipnickij V.A., Oleksjuk A.O. Teorija norm sindromov i pljus-dekodirovanie // Dokl. BGUIR. 2014. № 8 (86). S. 72–78. (in Russ.)
8. Lipnickij V.A., Oleksjuk A.O. Ocenka minimal'nyh rasstojanij neprimitivnyh kodov Hemminga // Vesci NAN Belarusi. 2015. № 2. S. 103–110. (in Russ.)
9. Lipnickij V.A., Oleksjuk A.O. Perestanovochnyj dekoder dlja korrekcii mnogokratnyh oshibok neprimitivnymi BChH-kodami // Dokl. BGUIR. 2015. № 3 (89). S. 117–123. (in Russ.)
10. Lipnickij V.A. Sovremennaja prikladnaja algebra. Matematicheskie osnovy zashhity informacii ot pomeh i nesankcionirovannogo dostupa. Minsk: BGUIR, 2006. 88 s. (in Russ.)
11. Vinogradov I.M. Osnovy teorii chisel. M.: Nauka, 1976. 168 s. (in Russ.)

Сведения об авторах

Конопелько В.К., д.т.н., профессор, профессор кафедры инфокоммуникационных технологий Белорусского государственного университета информатики и радиоэлектроники.

Липницкий В.А., д.т.н., профессор, заведующий кафедрой высшей математики Военной академии Республики Беларусь.

Адрес для корреспонденции

220013, Республика Беларусь,
г. Минск, ул. Бровки, 6
Белорусский государственный университет
информатики и радиоэлектроники
тел. 375-17-293-23-86;
e-mail: volos@bsuir.by
Конопелько Валерий Константинович

Information about the authors

Konopelko V.K., D.Sci, professor, professor of infocommunication technologies department of Belarusian state university of informatics and radioelectronics.

Lipnicki V.A., D.Sci, professor, head of the department of higher mathematics of Military academy of Republic of Belarus.

Address for correspondence

220013, Republic of Belarus,
Minsk, Brovki, 6,
Belarusian state university
of informatics and radioelectronics
tel. 375-17-293-23-86;
e-mail: volos@bsuir.by
Konopelko Valerii Konstantinovich