УДК 004.056.55

ТЕОРИЯ НОРМ СИНДРОМОВ И ПЛЮС-ДЕКОДИРОВАНИЕ

В.А. ЛИПНИЦКИЙ, А.О. ОЛЕКСЮК

Военная академия Республики Беларусь
Минск, 220057, Беларусь

Поступила в редакцию 8 октября 2014

Представлены результаты исследования не примитивных БЧХ-кодов, имеющих декодирующий потенциал, многократно превышающий конструктивные возможности. Показана эффективность автоморфизмов кодов, теории норм синдромов при коррекции всех допустимых минимальным расстоянием ошибок в названных кодах.

Ключевые слова: помехоустойчивое кодирование, БЧХ-коды, конструктивное и минимальное расстояния кода, циклические подстановки, теория норм синдромов.

Введение

Помехоустойчивое кодирование призвано вести синхронную борьбу с ошибками при передаче информации в цифровых системах связи, вынужденных функционировать в реальных зашумленных каналах [1, 2]. Реалии информационной эпохи XXI века, всеобщая компьютеризация, стремительный рост широчайших потоков информации предъявляют различные и порой противоречащие друг другу требования к применяемым кодам, создавая ряд проблем в теории и практике помехоустойчивого кодирования. Наиболее острая из них – проблема «селектора» - проблема быстрого и надежного выбора конкретной ошибки среди обширного корректируемого многообразия этих ошибок [3, 4].

Корректирующий потенциал кода обеспечивают спектры ошибок с попарно различными синдромами. Однако прямые развязки типа «синдром - ошибка» эффективны лишь при исправлении одиночных ошибок.

Применяемые на практике коды нередко обладают корректирующим потенциалом, выходящим за рамки конструктивных возможностей. Сказанное наиболее характерно для популярнейшего на практике класса кодов Боуза-Чоудхури-Хоквингема (БЧХ-кодов), особенно не примитивных БЧХ-кодов [2, 5]. Для реализации названного потенциала стандартные средства неприменимы. Здесь требуется разработка принципиально новых подходов, применение новых идей. Круг вопросов, связанных с коррекцией ошибок, выходящих за рамки конструктивных возможностей кодов, предлагаем назвать «плюс-декодированием».

Теория норм синдромов (ТНС) [4, 5], на порядок снизившая влияние проблемы «селектора», предоставляет также и конструктивные подходы к решению проблемы «плюс-декодирования». Их обсуждению, особенно в применении к не примитивным БЧХ-кодам, рассчитанным на коррекцию двукратных ошибок, и посвящена данная работа.

О БЧХ-кодах с конструктивным расстоянием 5

Общее определение и основные свойства БЧХ-кодов приведены в монографии [2]. 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 коды C_{2t+1} с проверочной матрицей

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

Здесь β – элемент мультипликативной группы $GF(2^m)^*$ поля Галуа $GF(2^m)$, имеющий порядок $n=\left(2^m-1\right)/\tau$ для некоторого делителя τ числа $\left|GF(2^m)^*\right|=2^m-1,\ 0\le i\le n-1$. Длина кода C_{2t+1} равна n и всегда является нечетной величиной. Группа $GF(2^m)^*$ циклична. Если α – образующая этой группы – примитивный элемент поля $GF(2^m)$, то в качестве β можно взять $\beta=\alpha^\tau$. При $\tau=1$ длина $n=2^m-1$, элемент $\beta=\alpha$ и потому код C_{2t+1} называется примитивным; если же $\tau>1$, $\beta\ne\alpha$ и потому код C_{2t+1} называют не примитивным [5, 6].

БЧХ-коды C_5 – частный случай кодов с проверочной матрицей (1) – задаются проверочными двоичными $\left(2m\times n\right)$ – матрицами, $2m<n=\left(2^m-1\right)/\tau$,

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

В [2] доказано, что у примитивных кодов C_5 при $m\ge4$ ранг матрицы (2) равен $2m$, циклотомические классы $C^1\ne C^3$, их размерность $k=n-2m$, а минимальное расстояние $d=\delta=5$. У не примитивных кодов C_5 любое из названных соотношений может нарушиться.

Ранг подматрицы β^i равен m [5]. Ранг подматрицы $(\beta^{3i})=\left(1,\beta^3,\beta^6,...,\beta^{3(n-1)}\right)$ матрицы (2) и подматрицы (1) не всегда равен m. Действительно, из каждых трех последовательных нечетных значений n одно делится на 3, а два – не делятся на три. Если НОД$(3,n)=1$, то отображение φ_3 циклической группы $\left\{1,\beta,\beta^2,...,\beta^{n-1}\right\}$ порядка n в себя, действующее по правилу $\varphi_3(x)=x^3$ является автоморфизмом этой группы. Отсюда следует, в частности, что β^3 имеет тот же порядок в мультипликативной группе $GF(2^m)^*$, что и его прообраз β при отображении φ_3. Это означает, что неприводимый полином над $GF(2)$ с корнем β^3 должен иметь степень m, а следовательно, элементы $1,\beta^3,\beta^6,...,\beta^{3(m-1)}$ образуют линейно независимую над $GF(2)$ систему. Следовательно, $rank(\beta^{3i})=m$.

Пусть n делится на три. Здесь возможны два варианта: 1) элемент β^3 поля $GF(2^m)$ не принадлежит никакому подполю этого поля; 2) существует подполе $GF(2^\mu)$ поля $GF(2^m)$, содержащее β^3. В первом случае неприводимый над полем $GF(2)$ полином элемента β^3 должен иметь степень m, а тогда $rank(\beta^{3i})=m$. Во втором случае по тем же причинам $rank(\beta^{3i})=\mu$ для некоторого делителя μ числа m. Второй случай хорошо иллюстрирует следующий пример. БЧХ-код C_5 длиной 219 определен над полем $GF(2^{18})$. $2^{18}-1=7\cdot9\cdot57\cdot73$. В этом случае матрица (2) задается элементом $\beta=\alpha^{57\cdot21}=\alpha^{1197}$, а элемент $\beta^3=\alpha^{57\cdot21\cdot3}=\alpha^{57\cdot7\cdot9}$ имеет порядок 73. Но такой элемент должен принадлежать мультипликативной группе $GF(2^9)^*$, которая имеет порядок $2^9-1=7\cdot73$. В таком случае $rank(\beta^{3i})\le9$.

Элементы β и β^3 в коде C_5 не должны быть сопряженными в поле $GF(2^m)$, что, очевидно, эквивалентно неравенству $C^1\ne C^3$ циклотомических классов. И это свойство не всегда выполняется. К примеру, у БЧХ-кода C_5 длиной 95 имеет место совпадение циклотомических классов: $C^1=C^3$; данный код реально относится к классу кодов Хемминга.

Во всех конкретных случаях проверка каждого параметра не примитивного кода C_5 требует внимания, дополнительных вычислений, а порой и серьезных компьютерных ресурсов.

Потенциал плюс-декодирования для БЧХ-кодов C_5

Ранее проблема декодирования ошибок, выходящих за конструктивные рамки, имела частный характер, поскольку количество таких ошибок было незначительным (см. [7, 8]). В

случае не примитивных БЧХ-кодов картина резко меняется. БЧХ-код C_5 конструктивно рассчитан на исправление одиночных и двойных ошибок в количестве $K_{\text{констр}} = C_n^1 + C_n^2 = n(n+1)/2$. Если у данного кода минимальное расстояние $d = 7$ (в табл. 1 отмечено пять таких кодов), то код должен исправлять и тройные ошибки в количестве $C_n^3 = n(n-1)(n-2)/6$. Данное количество ошибок превосходит почти в $n/3$ раз $K_{\text{констр}}$ и составляет потенциал K^+ плюс-декодирования для рассматриваемых кодов. Если же у кода C_5 реальное значение $d = 9$ (в табл. 1 отмечено пять таких кодов), то $K^+ = C_n^3 + C_n^4 = (n+1)n(n-1)(n-2)/24$, что почти в $n^2/12$ раз превосходит $K_{\text{констр}}$ и т.д. Точные данные приведены ниже в табл. 1. Из нее следует, что на плюс-декодирование приходится в десятки тысяч раз больше векторов-ошибок, чем на конструктивное.

ТНС как средство реализации возможностей плюс-декодирования

Конструктивные подходы к реализации в БЧХ-кодах C_5 потенциала плюс-декодирования предоставляет теория норм синдромов [4, 5]. Данная теория опирается на цикличность БЧХ-кодов с проверочными матрицами (1) и (2). Группам автоморфизмов $Aut(C)$ названных кодов C принадлежит подгруппа Г порядка n (длина кода) циклических сдвигов, которая состоит из степеней линейного преобразования σ двоичного векторного пространства V_n, действующего на каждый вектор $\bar{x} = (x_1, x_2, ..., x_n) \in V_n$ по правилу

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

Под действием группы Г пространство V_n, а с ним и совокупность K_C декодируемых конкретным БЧХ-кодом C векторов-ошибок, разбивается на попарно непересекающиеся классы – Г-орбиты. Каждая Г-орбита состоит из переходящих друг в друга под действием степеней σ векторов. Поэтому каждая Г-орбита J имеет следующую стандартную структуру:

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

для произвольного фиксированного вектора $\bar{e} \in J$. Здесь μ – наименьшее натуральное число с условием: $\sigma^{\mu}(\bar{e}) = \bar{e}$, делитель длины кода n. Чаще всего $\mu = n$. В последнем случае Г-орбита содержит максимально возможное количество векторов и потому называется полной. Равенство (4) служит причиной для следующего, более точного обозначения Г-орбит: $J = <\bar{e}>$.

Отображение φ_H из двоичного пространства V_n в двоичное пространство V_{2m}, действующее по правилу $\bar{y} = \bar{x} \cdot H^T$, есть линейный оператор между названными пространствами. Согласно базовым результатам линейной алгебры, полный образ $\varphi_H(V_n)$ есть подпространство пространства V_{2m} размерностью $n - \dim KerH = n - k = 2m$. Это означает, что $\varphi_H(V_n) = V_{2m}$.

Каждая вектор-ошибка $\bar{e}$ в БЧХ-коде C_5 над полем $GF(2^m)$ имеет в силу формулы (2) синдром $S(\bar{e}) = H \cdot \bar{e}^T = (s_1, s_2)^T$ для некоторых $s_1, s_2 \in GF(2^m)$. Из равенства $\varphi_H(V_n) = V_{2m}$ следует, что для любых $s_1^*, s_2^* \in GF(2^m)$ найдется вектор $\bar{e} \in V_n$, такой, что $S(\bar{e}) = H \cdot \bar{e}^T = (s_1^*, s_2^*)^T$.

Действие оператора σ на каждый вектор $\bar{e}$ однозначно отражается в коде C_5 на синдромах по формуле [4, 5]:

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

Формула (5) определяет структуру спектра синдромов $S(<\bar{e}>)$ каждой Г-орбиты $<\bar{e}>$:

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

Из формул (5), (6) следует, что, если у двух Г-орбит нашлись векторы с одинаковыми синдромами, то спектры синдромов этих орбит совпадают полностью.
Формула (5) послужила отправной точкой для следующего определения.

Нормой синдрома $S(\bar{e})=\left(s_1,s_2\right)^T$ в БЧХ-коде C_5 называется величина

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

Норма синдрома не определена для единственного нулевого значения синдрома: $S(\bar{e})=\left(0,0\right)^T$. Нормы синдромов обладают рядом замечательных свойств. Очевидно, 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. Если две Г-орбиты J_1 и J_2 имеют различные нормы, то спектры синдромов этих орбит не пересекаются, иными словами, данные орбиты не могут содержать векторы с одинаковыми синдромами.

К наиглавнейшим свойствам норм синдромов относится следующее: у всех векторов, принадлежащих каждой 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 $\bar{e}\in J$.

Приведем еще одно достаточно важное свойство норм синдромов – 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. Действительно, если у синдрома $S(\bar{e})=\left(s_1,s_2\right)^T$ компонента $s_1\neq 0$ и $N(S(\bar{e}))=N$, то 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 самое значение нормы. 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 равна $+\infty$. В целом, таким образом мы учли уже $n\left(n+2\right)=(2^m-1)\cdot\left(2^m+1\right)=2^{2m}-1$ синдромов. Добавив к ним нулевой синдром, мы получим весь спектр возможных синдромов в БЧХ-коде C_5, что и завершает доказательство свойства равномерного распределения синдромов по значения норм синдромов.

У примитивных БЧХ-кодов из равномерного свойства вытекает еще одно важное свойство норм синдромов – из равенства $N(J_1)=N(J_2)$ норм синдромов двух полных Г-орбит J_1 и J_2 с полными спектрами синдромов следует и равенство самих синдромов: для каждого 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 не примитивных БЧХ-кодов ситуация сложнее. Полная Г-орбита J с полным спектром синдромов $S(J)$ содержит $n=\left(2^m-1\right)/\tau$ векторов с $n=\left(2^m-1\right)/\tau$ синдромами в $S(J)$. Отсюда и из сформулированного выше равномерного свойства следует, что существует τ различных полных Г-орбит с попарно непересекающимися полными спектрами синдромов и с одинаковой нормой.

Теория норм синдромов дает новый взгляд на коррекцию ошибок. Она предлагает иметь дело не с отдельными векторами ошибок, а с их Г-орбитами. Любую декодируемую кодом C совокупность K_C векторов-ошибок, обязательно имеющих попарно различные синдромы, можно разбить на множество K_C/Γ Г-орбит этих ошибок. Для задания каждой конкретной Г-орбиты J достаточно зафиксировать один из ее представителей $\bar{e}_J$. Остальные векторы орбиты

легко строятся действием группы Г – циклическими сдвигами координат вектора $\bar{e}_J$.

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

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

Алгоритм 1 – математический алгоритм норменного декодирования с помощью Г-орбит

ТКС, получив очередное сообщение $\bar{x}$, в обязательном порядке вычисляет синдром $S(\bar{x}) = S(\bar{e})$. Если $S(\bar{x}) = S(\bar{e}) \neq \bar{0}$, что однозначно свидетельствует о наличии неизвестной и подлежащей определению вектор-ошибки $\bar{e}$, то вычисляем $N^* = N(S(\bar{x}))$. Совпадение N^* с $N(S(\bar{e}_J))$ из списка 3 резко сужает круг Г-орбит декодируемой совокупности, которые могут содержать искомую вектор-ошибку $\bar{e}$ из сообщения $\bar{x}$, до небольшой группы орбит $J_1, J_2, ..., J_\theta$, $1 \le \theta \le \tau$, с одинаковой нормой N^*.

Синдром $S(\bar{x}) = S(\bar{e}) = (s_1, s_2)$ принадлежит спектру синдромов только одной Г-орбиты J_l, $1 \le l \le \theta$. Пусть N^* является элементом поля Галуа $GF(2^m)$. Тогда у всех рассматриваемых синдромов первая компонента отлична от нуля. 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 $i, 0 \le i < n,$ в силу формулы (6), $\alpha^\lambda = \beta^i \cdot \alpha^\nu = \alpha^{\tau \cdot i + \nu}$. Полученное равенство означает, что либо $\lambda - \nu$ (если $\lambda > \nu$), либо $2^m - 1 + \lambda - \nu$ (если $\lambda < \nu$) делится на τ и частное i однозначно определяет искомую вектор-ошибку: $\bar{e} = \sigma^i(\bar{e}_{J_l})$. Величина же l и есть то единственное число из множества целых $\{1, 2, ..., \theta\}$, для которого одна из величин $\lambda - \nu$ или $2^m - 1 + \lambda - \nu$ делится нацело на τ.

Пусть $N^* = +\infty$. Тогда у всех рассматриваемых синдромов первая компонента равна нулю. Пусть синдром образующей $\bar{e}_{J_l}$ Г-орбиты J_l имеет вторую компоненту $s_2^{J_l} = \alpha^\nu$ для некоторого целого ν, $0 \le \nu < n$. Пусть у синдрома $S(\bar{x})$ вторая компонента $s_2 = \alpha^\lambda$, $0 \le \lambda < n$. Тогда для подходящего целого $i, 0 \le i < n,$ в силу формулы (6), $\alpha^\lambda = \beta^{3i} \cdot \alpha^\nu = \alpha^{\tau 3i + \nu}$. Полученное равенство означает, что либо $\lambda - \nu$ (если $\lambda > \nu$), либо $2^m - 1 + \lambda - \nu$ (если $\lambda < \nu$) делится на τ. Величина l и есть то единственное число из множества целых $\{1, 2, ..., \theta\}$, для которого одна из величин $\lambda - \nu$ или $2^m - 1 + \lambda - \nu$ делится нацело на τ. Очевидно, этим целым частным будет число $3i$.

Пусть n не делится на 3. Для взаимно простых чисел n и 3 выполняется соотношение Безу, то есть существуют такие целые числа u и ν, что $3u + n\nu = 1$. Искомую вектор-ошибку $\bar{e}$ определяем формулой: $\bar{e} = \sigma^{3ui}(\bar{e}_{J_l})$.

Действительно, $\sigma^{3ui}(\bar{e}_{J_l}) = \sigma^{3iu + n\nu i}(\bar{e}_{J_l}) = \sigma^{(3u + n\nu)i}(\bar{e}_{J_l}) = \sigma^i(\bar{e}_{J_l}) = \bar{e}$. Ситуация: $N^* = +\infty$ и n делится на 3 – крайне редкая, присуща неполным Г-орбитам и рассматривается в индивидуальном порядке.

Итак, работа норменного декодера достаточно легко реализуется, если созданы списки 1 – 3, характеризующие Г-орбиты декодируемой совокупности векторов-ошибок.

Эффективность работы норменных декодеров особенно ярко наблюдается на примитивных БЧХ-кодах [5, 9]. Отличительным и несколько усложняющим фактором непримитивного случая является возможное наличие отдельных значений $\theta > 1$.

Циклотомические подстановки для норменного декодирования

Следует признать, что при $d>7$ списки 1 – 3 становятся достаточно обширными, а работа с ними – затруднительной – проблема «селектора» начинает проявлять себя на новом уровне. Эффективным в преодолении названных затруднений мог бы быть метод «сжатия» – преобразования исправляемых векторов-ошибок в ошибки с узким спектром значений норм синдромов [10]. Однако имеющиеся подходы рассчитаны на примитивные коды и ошибки конкретного веса, автоматически эти подходы не переносятся на ошибки других весов. Для не примитивных же кодов они попросту не применимы.

Богатство группы автоморфизмов кода остается наиболее реальным и конструктивным средством сжатия обрабатываемой декодерами информации. Группа автоморфизмов любого из кодов C_5 достаточно богата, содержит, к примеру, циклотомические подстановки. Их действие, свойства и применение частично уже рассматривались в [5].

Циклотомические подстановки составляют циклическую группу Ф порядка m с образующей ϕ, такой, что для каждого вектора-ошибки $\bar{e}$ с синдромом $S(\bar{e})=(s_1, s_2)$ синдром $S(\phi(\bar{e}))=(s_1^2, s_2^2)$. Тогда при условии $N(S(\bar{e}))=N\in GF(2^m)$ норма $N(S(\phi(\bar{e})))=N^2$. Вектор $\phi(\bar{e})$ получается 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 соотношением: $\phi\sigma=\sigma^3\phi$ [2, 5]. Вместе они образуют некоммутативную группу G порядка mn, подгруппу группы $Aut(C_5)$. Если $J-$ некоторая Г-орбита векторов-ошибок, то $\phi(J)-$ новая Г-орбита векторов-ошибок [5]. Таким образом, группа Ф действует на множестве Г-орбит K_C/Γ декодируемой кодом $C=C_5$ совокупности K_C векторов-ошибок, разбивая его на Ф-орбиты. Соответственно, множество K_C разбивается на G-орбиты, содержащие, как правило, по mn векторов-ошибок. Зафиксировав одну вектор-ошибку $\bar{e}$, можно восстановить все вектор-ошибки G-орбиты $<\bar{e}>_G$. Таким образом, списки 1–3 можно сократить примерно в m раз, оставив по одной образующей каждой G-орбиты декодируемой совокупности (табл. 1).

Таблица 1. **Оценка количества Г-орбит и *G*-орбит корректируемой совокупности для БЧХ-кодов C_5**

№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
№п/п	7	8	9	10	11	12
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 – математический алгоритм коррекции ошибок с помощью *G*-орбит

Этот алгоритм является некоторой модификацией алгоритма 1. Если для принятого сообщения $\bar{x}$ с синдромом $S(\bar{x}) = S(\bar{e}) = (s_1, s_2)$ норма $N^* = N(S(\bar{x}))$ является элементом поля Галуа $GF(2^m)$, но не принадлежит третьему списку, то 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 декодируемой совокупности. Полученное равенство норм означает, что для искомого вектора-ошибки $\bar{e}$ в сообщении $\bar{x}$ вектор $\phi^i(\bar{e})$ имеет синдром $S(\phi^i(\bar{e})) = (s_1^\lambda, s_2^\lambda)$, принадлежащий спектру синдромов $S(<\bar{e}_J>)$ одной Г-орбиты $<\bar{e}_J>$, порожденной конкретным вектором-ошибкой $\bar{e}_J$ 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, $0 \le s \le n-1$. Далее, вектор $\bar{e}$ однозначно восстанавливается в соответствии с формулой: $\bar{e} = \phi^{m-i}(\sigma^s(\bar{e}_J))$.

Заключение

Примерно треть не примитивных БЧХ-кодов имеют декодирующий потенциал, многократно превышающий конструктивные возможности. Применение автоморфизмов кодов, теория норм синдромов обеспечивают эффективные конструктивные норменные методы коррекции всех допустимых минимальным расстоянием ошибок в названных кодах. Перечисленные факторы обеспечивают перспективность для приложений многих представителей класса не примитивных БЧХ-кодов.

THEORY OF NORMAL SYNDROME AND PLUS-DECODING

V.A. LIPNITSKI, A.O. ALIAKSIUK

Abstract

The results of the study are not primitive BCH codes with decoding the guide, the potential is much greater than the design possibilities. The efficiency of automorphisms of codes, norms theory syndromes in the correction of all admissible-Mykh minimum distances errors in the above code is shown.

Список литературы

1 *Шеннон, К.* Работа по теории информации и кибернетике. М., 1963.
2 *Мак-Вильямс Ф.Дж., Слоэн Н. Дж.А.* Теория кодов, исправляющих ошибки. М., 1979.
3 *Колесник В.Д.*, *Мирончиков Е.Т.* Декодирование циклических кодов. М., 1968.
4 *Конопелько В.К., Липницкий В.А.* Теория норм синдромов и перестановочное декодирование помехоустойчивых кодов. М., 2004.
5 *Липницкий В.А., Конопелько В.К.* Норменное декодирование помехоустойчивых кодов и алгебраические уравнения. Минск, 2007.
6 *Курилович А.В., Липницкий В.А., Михайловская Л.В.* // Технологии информатизации и управления. 2011. Вып. 2. С. 43–49.
7 *Сагалович Ю.Л.* // Тез. докл. IX Симпозиума по проблеме избыточности в информационных системах. Ленинград, 3–8 июня 1986 г. С. 135–138.
8 *Давыдов А.А., Дрожжина-Лабинская А.Ю., Калинчева В.В* // Вопросы кибернетики. Проблемы программного обеспечения супер-ЭВМ. 1990. С. 151–174.
9 *Конопелько В.К.* Устройство декодирования для коррекции двоичных ошибок / Патент СССР SU1833968 A1.
10 *Липницкий В.А., Аль-Хайдар Е.К.* // Докл. БГУИР. 2009. № 5 (43). С. 12–16.