УДК 621.391

БОЦУЛ А.В., аспирант (НТУ «ХПИ»),
ЗУБЕНКО В.А., к.т.н., ст. преподаватель (Кировоградский национальный технический университет),
ВОЛКОВ А.С., к.т.н., ст. преподаватель (УкрГАЖТ),
ШТОМПЕЛЬ Н.А., к.т.н., доцент (УкрГАЖТ)

Свойства алгебраических сверточных кодов перемежения

Проведен анализ и исследование основных свойств алгебраических сверточных кодов перемежения, исправляющих группирующиеся ошибки, возникающих в каналах связи. Получены выражения, позволяющие алгебраическим способом представить группирующиеся ошибки, искажающие кодовые слова алгебраических сверточных кодов перемежения.

Ключевые слова: *сверточный код, помехоустойчивое кодирование, перемежение, декодирование.*

Анализ литературы и постановка проблемы

При передаче дискретных сообщений по реальным каналам связи возникают различные конфигурации случайных ошибок и группирующиеся ошибки произвольно большой длины [1, 3, 4]. В то же время к современным системам передачи информации предъявляются требования по обеспечению высокой достоверности [2, 4]. Эффективным способом обеспечения или повышения достоверности передаваемых дискретных сообщений по реальным каналам связи является применение методов помехоустойчивого кодирования и декодирования [1 - 5].

Известно, что высокой эффективностью обладают сверточные коды с большой длиной кодового ограничения [1 - 4]. Однако практическую реализацию сверточных кодов с большой длиной кодового ограничения допускают не все методы их декодирования. При этом классические методы декодирования обладают ограниченными возможностями в случае возникновения группирующихся ошибок, возникающих в каналах связи. Данное явление имеет случайный характер и приводит к распространению ошибок декодирующими устройствами сверточных кодов. В тоже время, для борьбы с группирующимися ошибками используют дополнительные устройства – перемежитель/ деперемежитель. Но их применение требует согласования параметров кодера и перемежителя, а также декодера и деперемежителя, что усложняет разработку системы передачи информации в целом [1 - 5].

Другим эффективным способом борьбы с группирующимися ошибками является применение методов кодирования и декодирования сверточных кодов, обладающих специальной структурой, которые позволяют исправлять случайные и группирующиеся ошибки. Однако, известные сверточные коды, исправляющие группирующиеся ошибки, обладают низкой корректирующей способностью [2 - 4].

С появлением алгебраических сверточных кодов появилась возможность борьбы с группирующимися ошибками. При этом алгебраические методы их декодирования допускают практическую реализацию с большими длинами кодового ограничения. Недостатком данных методов является способность алгебрических сверточных кодов исправлять группирующиеся ошибки только на длине кодового ограничения.

Следовательно, актуальной научно-технической задачей является разработка и усовершенствование методов и алгоритмов кодирования и декодирования сверточных кодов, позволяющих исправлять группирующиеся ошибки большой длинны и достигать высоких значений энергетического выигрыша от помехоустойчивого кодирования.

В работах [6, 7] предложены алгебраические сверточные коды перемежения, которые позволяют исправлять группирующиеся ошибки, возникающие в реальных каналах связи.

Но в работах [6, 7] не показаны конфигурации ошибок, которые могут исправлять алгебраические сверточные коды перемежения.

Цель статьи

Исследование основных свойств алгебраических сверточных кодов перемежения, исправляющих группирующиеся ошибки, возникающих в каналах связи.

Основная часть

Исследование свойств помехоустойчивых кодов исправляющих группирующиеся ошибки

В настоящее время в теории помехоустойчивого кодирования известны блоковые и сверточные коды, которые позволяют исправлять группирующиеся ошибки. Рассмотрим блоковые коды, исправляющие группирующиеся ошибки [2,4].

Эффективным методом борьбы с группирующимися ошибками в телекоммуникационных системах и сетях является применение недвоичных блоковых (N, K) – кодов Рида-Соломона над $GF(q^p)$ [2]. При этом недвоичный циклический (N, K) – код Рида-Соломона над $GF(q^p)$ представляют кодом над $GF(q)$, в котором информационные и кодовые слова заданы q – ичными p – последовательностями (символами). Тогда полученный код будет линейным ($p{\cdot}N$, $p{\cdot}K$) – кодом над $GF(q)$. Следовательно, представленный таким образом блоковый код над $GF(q)$ можно переписать так: ($p{\cdot}(q^p - 1)$, $p{\cdot}(q^p - 1 - 2{\cdot}t)$) [2,4]. При этом удается исправлять все группирующиеся ошибки, длина которых не превышает величину $p{\cdot}(t - 1) + 1$ и все конфигурации ошибок кратности t и меньше. По определению недвоичный блоковый (N, K) – код Рида-Соломона над $GF(q^p)$ является циклическим, а сформированный ($p{\cdot}(q^p - 1)$, $p{\cdot}(q^p - 1 - 2{\cdot}t)$) – код над $GF(q)$, может не являться циклическим, что затрудняет их декодирование [2].

В то же время популярными блоковыми кодами, исправляющими группирующиеся ошибки, являются коды над $GF(2)$, найденные переборными методами с применением ЭВМ [1 - 2]. В работах [2 - 5] предложен ряд таких помехоустойчивых двоичных блоковых кодов относительно небольшой длины.

Недостатком переборных методов построения блоковых кодов, исправляющих группирующиеся ошибки, является ограничения по длине кода, т. к. число перебираемых вариантов порождающих многочленов, которые полностью (однозначно) определяют код, возрастает экспоненциально. При этом для переборных методов отсутствует возможность алгебраического декодирования блоковых кодов из-за отсутствия алгебраической структуры кодов [1 - 3].

Для построения блоковых кодов большой длины, исправляющих группирующиеся ошибки, применяют методы перемежения символов [2, 4]. В теории помехоустойчивого кодирования такие коды получили название блоковые коды - перемежения [2 - 4].

Многочлен $g(x^j)$ блокового ($j{\cdot}N$, $j{\cdot}K$) – кода - перемежения формируется путем модификации порождающего многочлена $g(x)$ блокового (N, K) – кода. Если блоковый (N, K) – код обладает корректирующей способностью равной t ошибок, то полученный методом перемежения блоковый ($j{\cdot}N$, $j{\cdot}K$) – код способен исправлять все группирующиеся ошибки, длина которых не превышает величину $j{\cdot}t$ [2].

Если модификации подвергается порождающий многочлен $g(x)$ циклического блокового (N, K) – кода, то результирующий блоковый ($j{\cdot}N$, $j{\cdot}K$) – код сохраняет свойство цикличности [2-4].

Тогда, алгебраически процедуру кодирования ($j{\cdot}N$, $j{\cdot}K$) – кодом-перемежения можно представить следующим образом [2]:

$$\begin{aligned} c(x) &= c_1(x) + x\cdot c_2(x) + \ldots + x^{j-1}\cdot c_j(x^j) = \\ &= i_1(x^j)\cdot g(x^j) + x\cdot i_2(x^j)\cdot g(x^j) + \ldots + \\ &+ x^{j-1}\cdot i_j(x^j)\cdot g(x^j) = [i_1(x^j) + x\cdot i_2(x^j) + \\ &+ \ldots + x^{j-1}\cdot i_j(x^j)]\cdot g(x^j). \end{aligned} \qquad (1)$$

В выражении (1) даны следующие обозначения: $c(x)$ – кодовое слово ($j{\cdot}N$, $j{\cdot}K$) – кода-перемежения, которое получается задержкой и сложением j кодовых слов блокового кода, каждое из которых содержит вставку между всеми символами, состоящую из j – 1 нулей; $g(x)$ – порождающий многочлен блокового (N, K) – кода; $g(x^j)$ – порождающий многочлен ($j{\cdot}N$, $j{\cdot}K$) – кода – перемежения; $i_j(x^j)$ – информационное слово ($j{\cdot}N$, $j{\cdot}K$) – кода-перемежения.

Выражение (1) позволяет сделать вывод, что процедура кодирования ($j{\cdot}N$, $j{\cdot}K$) – кодом - перемежения с порождающим многочленом $g(x^j)$ эквивалентна перестановке (перемежению) некоторого числа кодовых слов (а именно j их копий), порождаемых многочленом $g(x)$ [2 - 4].

В настоящее время известны коды Файра [1 - 5]. Это помехоустойчивые блоковые коды, которые исправляют группирующиеся ошибки. Блоковые коды Файра допускают аналитические методы построения.

Порождающий многочлен циклического блокового кода Файра над $GF(q)$ имеет следующий вид [2]:

$$g(x) = (x^{2\cdot T-1} - 1)\cdot A(x), \qquad (2)$$

где T – длина исправляемой группирующиеся ошибки.

В выражении (2) многочлен $A(x)$ представляет собой примитивный многочлен над $GF(q)$, который представляется следующим образом [2]:

$$A(x) = 1 + A_1 x + A_2 x^2 + \ldots + A_w x^w. \qquad (3)$$

Многочлен $A(x)$ не должен делить $x^{2\cdot T-1} - 1$, при этом его степень w должна быть не меньше длины исправляемой группирующиеся ошибки T.

Важным параметром циклического блокового кода Файра над $GF(q)$ является длина блока кодового слова n_f. Величина n_f удовлетворяет следующему выражению [2]:

$$n_f = B \cdot (2 \cdot T - 1), \tag{4}$$

где B – наименьшее целое число, при котором выполняется деление примитивного многочлена $A(x)$ на $x^B - 1$.

Тогда справедливо, что циклический блоковый код (n_f, k_f) – Файра над $GF(q)$ имеет следующие параметры [2 - 4]:

$$\begin{aligned}(n_f, k_f) = ((q^A - 1)\cdot(2\cdot T - 1),\\ (q^A - 1)\cdot(2\cdot T - 1) - A - 2\cdot T + 1)\end{aligned}. \tag{5}$$

Таким образом, циклический блоковый код (n_f, k_f) – Файра над $GF(q)$ гарантированно исправляет все группирующиеся ошибки длины T и меньше [2, 4].

В то же время, в работах [2, 4] доказано, что циклический блоковый код (n_f, k_f) – Файра над $GF(q)$ удовлетворяет границе Рейгера [2, 4], суть которой заключается в следующем: если циклический блоковый код исправляет группирующиеся ошибки длины T, то число проверочных символов в блоке кодовых слов должно быть не меньше значения $2\cdot T$ [2 - 4].

Рассмотрим методы построения и кодирования сверточных кодов, исправляющих группирующиеся ошибки.

В этом направлении работали и получили важные научные результаты следующие ученые [2 - 5]: Хегельбергер, Вайнер, Эш, Препарата, Берлекэмп, Месси, Коленбург, Тонг и Ивадари.

По аналогии с методами кодирования блоковыми кодами - перемежения, в настоящее время известны методы кодирования сверточных кодов-перемежения. В основе методов кодирования сверточных кодов - перемежения заложена идея чередования j одинаковых выходных кадров, генерируемых j одинаковыми кодерами сверточных кодов [2 - 4].

Для данных методов кодирования справедливо утверждение [1 - 5]. Если сверточный (n, k) – код исправляет все конфигурации ошибок и группирующиеся ошибки, кратность которых не превышает значение t, то полученный сверточный $(j\cdot n, j\cdot k)$ – код - перемежения исправляет все конфигурации ошибок и группирующиеся ошибки, кратность которых не превышает значение $j\cdot t$.

Порождающий многочлен $g(x^j)$ сверточных $(j\cdot n, j\cdot k)$ – кодов - перемежения формируется подобным способом, как и в блоковых кодах, – модификацией порождающего многочлена $g(x)$ сверточного (n, k) – кода.

В результате можно построить достаточно большое число сверточных $(j\cdot n, j\cdot k)$ – кодов-перемежения, исправляющих все конфигурации ошибок и группирующиеся ошибки [2].

Однако если необходимо корректировать только группирующиеся ошибки, то можно воспользоваться известными сверточными кодами Ивадаре [2 - 5], при этом удается добиться лучших характеристик [2 - 4].

Сверточный (n, k)– код Ивадаре в систематическом виде возможно однозначно определить матрицей $G(x)$ из многочленов, которая имеет размерность $(n-1\times n)$ [2]. Представим данную матрицу $G(x)$ из многочленов следующим образом [2 - 4]:

$$G(x) = \begin{bmatrix} 1 & 0 & 0 & 0 & g_1(x) \\ 0 & 1 & 0 & 0 & g_2(x) \\ 0 & 0 & \ddots & 0 & \\ 0 & 0 & 0 & 1 & g_{(n-1)}(x) \end{bmatrix}. \tag{6}$$

В матрице $G(x)$ из многочленов каждый $g_i(x)$ порождающий многочлен представляется следующим образом [2]:

$$g_i(x) = x^{(j+1)\cdot(2\cdot n - i) + i - 3} + x^{(j+1)\cdot(n-i)-1}, \tag{7}$$

где j и n – любые целые числа (положительные), $i = 1, \ldots, n-1$.

В матрице $G(x)$ из многочленов вида (6) максимальную степень имеет порождающий многочлен $g_1(x)$. Тогда [2]

$$\deg[g_1(x)] = (j+1)\cdot(2\cdot n - 1) - 2. \tag{8}$$

Тогда проверочная матрица $H(x)$ из многочленов (n, k) – код Ивадаре в систематическом виде имеет следующий вид [2]:

$$H(x) = [g_1(x) \quad g_2(x) \quad g_{(n-1)}(x) \quad 1]. \tag{9}$$

Параметры (n, k) – кода Ивадаре можно представить следующим образом [2, 4]:

$$(n, k) = ((r+1)\cdot n, (r+1)\cdot(n-1)), \tag{10}$$

где r – число кадров (n, k) – кода Ивадаре; $r = (j+1)\cdot(2\cdot n - 1) - 2$.

При декодировании (n, k) – кодов Ивадаре, по принятой из канала связи последовательности, декодер вычисляет синдром s. Данный синдром удобно представлять в виде многочлена $s(x)$ [2]

$$\begin{aligned} s(x) = e_n(x) + \\ + \sum_{i=0}^{n-1}\left[x^{(j+1)\cdot(n-i)-1} + x^{(j+1)\cdot(2\cdot n - i)+i-3}\right]\cdot e_i(x)\end{aligned}, \tag{11}$$

где $e_i(x)$ – многочлен ошибок.

Важным преимуществом сверточных (n, k) – кодов Ивадаре является возможность уменьшения так называемого защитного интервала [2]. В работе под защитным интервалом будем понимать последовательность не искаженных символов, следующую за группирующейся ошибкой [2, 4].

Сверточный $((r+1)\cdot n,(r+1)\cdot(n-1))$ – код Ивадаре в систематическом виде позволяет исправлять все группирующиеся ошибки, длина которых не превышает значение $j\cdot n$ [2].

В тоже время сверточные (n, k) – коды Ивадаре удовлетворяют нижней границе для длины защитного интервала [2], обладая при этом низкой сложностью декодирования [4].

Недостатком сверточных (n, k) – кодов Ивадаре является отсутствие возможности декодирования и случайных конфигураций ошибок и группирующихся ошибок одновременно [4]. При этом коды не обладают алгебраической структурой как, например, коды Рида-Соломона, что не позволяет применять алгебраические методы их декодирования, основанные на корнях порождающих многочленов [5].

Для исправления конфигураций ошибок и группирующихся ошибок Коленбург [4] и Месси [2, 4] предложили диффузные сверточные (n, k) – коды коды, которые далее были усовершенствованы Тонгом [4] для произвольных значений скорости кода и числа составных проверок. Диффузные сверточные (n, k) – коды, как и сверточные (n, k) – коды Ивадаре, допускают пороговые методы декодирования [4].

С появлением алгебраических сверточных (n, k) – кодов [1], применяя математический аппарат высшей алгебры, появилась возможность исправлять все группирующиеся ошибки, кратность которых не превышает корректирующей способности сверточного кода на некоторой фиксированной длине.

Исследование основных свойств алгебраических сверточных кодов перемежения

В настоящее время в теории помехоустойчивого сверточного кодирования известно несколько типов [4] группирующихся ошибок. Рассмотрим алгебраический способ представления группирующихся ошибок, которые принадлежат к типу В1 и типу В2 [4].

Пусть на вход декодера сверточного (n, k) – кода поступает непрерывная последовательность кадров кодовых слов, которая подлежит декодированию. Предположим, что последовательность не содержит ошибочных символов. Представим данную последовательность кадров кодовых слов в виде вектора C полубесконечной длины. Тогда справедливо следующее выражение [4]:

$$C=(O_{0,0},O_{0,1},O_{0,2},...,O_{0,(n-1)},O_{1,0},O_{1,1},\\ O_{1,2},...,O_{1,(n-1)},O_{2,0},O_{2,1},O_{2,2},...,O_{2,(n-1)},...), \qquad (12)$$

где $O_{i,j}$ – один символ кадра кодового слова без воздействия на него ошибок; i – индекс, указывающий номер кадра кодового слова в принятой последовательности C, i = 0, 1, 2, 3, … ; j – индекс, указывающий номер символа в одном кадре кодового слова, j = 0, 1, 2, …, n – 1.

Перепишем выражение (12) при наличии группирующейся ошибки следующим образом:

$$C=(O_{0,0},O_{0,1},O_{0,2},...,O_{0,(n-1)},E_{1,0},E_{1,1},\\ O_{1,2},...,O_{1,(n-1)},O_{2,0},O_{2,1},O_{2,2},...,O_{2,(n-1)},...), \qquad (13)$$

где $E_{i,j}$ – один символ кадра кодового слова поврежденный ошибкой; i – индекс, указывающий номер кадра кодового слова, i = 0, 1, 2, 3, … ; j – индекс, указывающий номер символа в одном кадре кодового слова, j = 0, 1, 2, …, n – 1.

Анализ выражения (13) позволяет сделать вывод, что кодовое слово сверточного (n, k) – кода содержит ошибку в первом кадре кодовых слов. При этом повреждены символы, которые находятся на нулевой ($E_{1,0}$) и первой ($E_{1,1}$) позиции кадра кодового слова сверточного (n, k) – кода. Следовательно, кодовое слово сверточного (n, k) – кода содержит группирующуюся ошибку типа В1 длины два символа. В тоже время, можно утверждать, что кодовое слово сверточного (n, k) – кода содержит группирующуюся ошибку типа В2 длины один кадр [4].

Рассмотрим случай, когда группирующаяся ошибка содержится на всей длине кадра кодового слова n. Тогда выражение (13) перепишем следующим образом [4]:

$$C=(O_{0,0},O_{0,1},O_{0,2},...,O_{0,(n-1)},E_{1,0},E_{1,1},\\ E_{1,2},...,E_{1,(n-1)},O_{2,0},O_{2,1},O_{2,2},...,O_{2,(n-1)},...). \qquad (14)$$

Из выражения (14) видно, что символы $E_{i,j}$ группирующейся ошибки расположены при i = 1 и j = 0, 1, 2, …. n – 1. Следовательно, кодовое слово сверточного (n, k) – кода содержит группирующуюся ошибку типа В1 длины n символов или содержит группирующуюся ошибку типа В2 длины один кадр [4].

Возможны ситуации, когда группирующаяся ошибка возникает в смежных кадрах кодового слова сверточного (n, k) – кода. Тогда выражение (12) представим следующим образом:

$$C=(O_{0,0},O_{0,1},O_{0,2},...,E_{0,(n-1)},E_{1,0},O_{1,1},\\ O_{1,2},...,O_{1,(n-1)},O_{2,0},O_{2,1},O_{2,2},...,O_{2,(n-1)},...). \qquad (15)$$

В выражении (15) показано, что символы $E_{i,j}$ группирующейся ошибки расположены при i = 0 и

$j = n - 1$ и при $i = 1$ и $j = 0$ соответственно. Тогда кодовое слово сверточного (n, k) – кода содержит группирующуюся ошибку типа B1 длины два символа или, что тоже самое, содержит группирующуюся ошибку типа B2 длины два кадра [4].

На основании проведенного анализа выражений (12) – (15) можно сделать вывод, что группирующуюся ошибку типа B1 длины t символов $E_{i,j}$ можно представить группирующейся ошибкой типа B2 длины $]t/n[$ или $]t/n[+1$ кадров [2 - 4]. В то же время группирующуюся ошибку типа B2 длины T кадров можно представить группирующейся ошибкой типа B длины t символов $E_{i,j}$, где $T \cdot n \le t \le (T+1) \cdot n$ [4].

С появлением алгебраических сверточных (n, k) – кодов появилась необходимость представления группирующихся ошибок с учетом параметров недвоичных циклических блоковых (N, K) – кодов над $GF(q^p)$. Множество порождающих многочленов алгебраических сверточных (n, k) – кодов формируется модификацией порождающего многочлена недвоичного циклического блокового (N, K) – кода над $GF(q^p)$ [1]. При этом декодирование выполняется на длине N, которая является длиной блока кодового слова блокового кода. В соответствии с выражением (12) алгебраическое представление группирующихся ошибок на длине N кадров кодовых слов алгебраических сверточных (n, k) – кодов можно представить следующим образом [6]:

$$\begin{aligned} C = (&E_{0,0}, E_{0,1}, E_{0,2}, ..., E_{0,(n-1)}, E_{1,0}, E_{1,1}, \\ &E_{1,2}, ..., E_{1,(n-1)}, E_{2,0}, E_{2,1}, E_{2,2}, ..., E_{2,(n-1)}, \\ &O_{3,0}, O_{3,1}, O_{3,2}, ..., O_{3,(n-1)}, ..., O_{N-1,0}, O_{N-1,1}, \\ &O_{N-1,2}, ..., O_{N-1,(n-1)}, O_{N,0}, O_{N,1}, O_{N,2}, ..., \\ &O_{,(n-1)}, O_{N+1,0}, O_{N+1,1}, O_{N+1,2}, ..., O_{N+1,(n-1)}, ...) \end{aligned}, \qquad (16)$$

где N – длина блока кодовых слов недвоичных циклических блоковых (N, K) – кодов над $GF(q^p)$; $N = q^p - 1$.

В выражении (16) $E_{i,j}$ представляет собой один элемент поля $GF(q)$ и является одним символом кадра кодового слова поврежденного ошибкой алгебраического сверточного (n, k) – кода над $GF(q)$.

Если обработка символов кодирующим и декодирующим устройством алгебраических сверточных (n, k) – кодов выполняется в поле $GF(q^p)$, где $N = q^p - 1$, то выражение (16) можно представить следующим образом:

$$\begin{aligned} C = (&E_0, E_1, E_2, O_3, ..., O_{N-2}, O_{N-1}, \\ &O_N, O_{N+1}, O_{N+2}, ..., O_{2 \cdot N-2}, O_{2 \cdot N-1}, ...) \end{aligned}, \qquad (17)$$

где E_i – один кадр кодового слова алгебраического сверточного (n, k) – кода искаженного ошибкой; O_i – один кадра кодового слова без воздействия на него ошибок; $i = 0, 1, 2, \ldots$.

В выражении (17) один кадр кодового слова алгебраического сверточного (n, k) – кода является элементом поля $GF(q^p)$. При этом выполняется равенство: $p = n$ [6].

Из анализа выражений (16) и (17) можно сделать вывод, что алгебраические сверточные (n, k) – коды позволяют гарантированно исправлять на длине N группирующиеся ошибки длины $T \le (N - K)/2$, где $N = q^p - 1$; $K = N - \deg\, g(x)$; $g(x)$ – порождающий многочлен максимальной степени алгебраического сверточного (n, k) – кода.

На практике возможно возникновение группирующихся ошибок длины $T > (N - K)/2$, которые можно представить в виде следующего выражения (частный случай $T = N$) [6, 7]:

$$\begin{aligned} C = (&E_0, E_1, E_2, E_3, ..., E_{N-2}, E_{N-1}, \\ &O_N, O_{N+1}, O_{N+2}, ..., O_{2 \cdot N-2}, O_{2 \cdot N-1}, ...) \end{aligned}. \qquad (18)$$

Следовательно, корректирующей способности алгебраических сверточных (n, k) – кодов недостаточно для исправления группирующейся ошибки при $T > (N - K)/2$.

Рассмотрим алгебраический сверточный код перемежения [6, 7] над $GF(q^m)$. Пусть на вход декодера алгебраического сверточного кода перемежения над $GF(q^m)$ поступает кодовое слово, представленное многочленом $C(x)$. И предположим, что в результате помехи в реальном канале связи, кодовое слово искажено ошибками. Тогда искаженное ошибками кодовое слово обозначим многочленом $C^*(x)$ и запишем следующим образом [1, 6]:

$$C^*(x) = C(x) + E(x), \qquad (19)$$

где $C(x)$ – кодовое слово сверточных кодов перемежения; $E(x) = E_0 + E_1 x + E_2 x^2 + ...$ – многочлен ошибок полубесконечной длины, $E_i \in GF(q^m)$.

Тогда вектор ошибок E полубесконечной длины с компонентами над $GF(q^m)$ имеет вид $E = (E_0, E_1, E_2, ...)$.

Разобьем вектор E над $GF(q^m)$ на подблоки длины N

$$\begin{aligned} E = ((&E_0, E_1, E_2, ..., E_{N-1}), (E_N, E_{N+1}, E_{N+2}, ..., \\ &E_{2 \cdot N-1}), (E_{2 \cdot N}, E_{2 \cdot N+1}, E_{2 \cdot N+2}, ..., E_{3 \cdot N-1}) ...), \end{aligned} \qquad (20)$$

где E_i – вектор i – го подблока ошибок; $i = 0, 1, 2, \ldots$.

Следовательно

$$E_i = (E_{i\cdot N}, E_{i\cdot N+1}, E_{i\cdot N+2}, ..., E_{(i+1)\cdot N-1}) . \quad (21)$$

Тогда, многочлен $E(x)$ над $GF(q^m)$ представим последовательностью многочленов $E_i(x)$ степени N-1

$$E(x) = (E_0 + E_1 x + E_2 x^2 + ... + \\ + E_{N-1}x^{N-1}) + x^N \cdot (E_N + E_{N+1}x + \\ + E_{N+2}x^2 + ... + E_{2\cdot N-1}x^{N-1}) + x^{2\cdot N} \cdot (E_{2\cdot N} + \\ + E_{2\cdot N+1}x + E_{2\cdot N+2}x^2 + ... + E_{3\cdot N-1}x^{N-1}) + ... , \quad (22)$$

где $E_i(x) = E_{i\cdot N} + E_{i\cdot N+1}x + ... + E_{(i+1)\cdot N-1}x^{N-1}$;

$E_i(x)$ – i – ый многочлен подблока ошибок;

$x^{i\cdot N}$ – оператор задержки; $i = 0, 1, 2, ...$.

Представим многочлен $E_j(x)$ блока ошибок над $GF(q^m)$ с коэффициентами $E_{l,j,\mu,i}$ последовательностью из M многочленов подблоков $E_i(x)$ вида (22) следующим образом:

$$E_j(x) = [E_{0,j,0,0} + E_{0,j,1,1}x + E_{0,j,2,2}x^2 + ... + \\ + E_{0,j,N-1,N-1}x^{N-1}] + x^N \cdot [E_{1,j,0,N} + E_{1,j,1,N+1}x + \\ + E_{1,j,2,N+2}x^2 + ... + E_{1,j,N-1,2\cdot N-1}x^{N-1}] + x^{2\cdot N} \cdot \\ \cdot [E_{2,j,0,2\cdot N} + E_{2,j,1,2\cdot N+1}x + E_{2,j,2,2\cdot N+2}x^2 + \\ + ... + E_{2,j,N-1,3\cdot N-1}x^{N-1}] + ... + x^{(M-1)\cdot N} \cdot \\ \cdot [E_{M-1,j,0,(M-1)\cdot N} + E_{M-1,j,1,(M-1)\cdot N+1}x + \\ + E_{M-1,j,2,(M-1)\cdot N+2}x^2 + ... + E_{M-1,j,N-1,M\cdot N-1}x^{N-1}] , \quad (23)$$

где l – индекс, указывающий номер подблока ошибок в одном блоке (первый индекс коэффициента), l = 0, 1, 2, …, M – 1; j – индекс, указывающий номер блока ошибок (второй индекс коэффициента), $j = 0, 1, 2, ...$; μ – индекс, указывающий номер коэффициента многочлена ошибок в одном подблоке (третий индекс коэффициента), $\mu = 0, 1, 2, ..., N-1$; i – индекс, указывающий номер коэффициента многочлена ошибок в одном блоке на длине $M \cdot N$ (четвертый индекс коэффициента), $i = 0, 1, 2, ..., M\cdot N-1$; $E_{l,j,\mu,i} \in GF(q^m)$; $x^{l\cdot N}$ – оператор задержки [6,7].

Из выражения (23) при $l = 0$ многочлен подблока ошибок $E_{j,0}(x)$ представим

$$E_{j,0}(x) = E_{0,j,0,0} + E_{0,j,1,1}x + \\ + E_{0,j,2,2}x^2 + ... + E_{0,j,N-1,N-1}x^{N-1}; \quad (24)$$

при $l = 1$ $E_{j,1}(x)$ запишем

$$E_{j,1}(x) = E_{1,j,0,N} + E_{1,j,1,N+1}x + \\ + E_{1,j,2,N+2}x^2 + ... + E_{1,j,N-1,2\cdot N-1}x^{N-1}; \quad (25)$$

при $l = M-1$:

$$E_{j,M-1}(x) = E_{M-1,j,0,(M-1)\cdot N} + \\ + E_{M-1,j,1,(M-1)\cdot N+1}x + E_{M-1,j,2,(M-1)\cdot N+2}x^2 + \cdot \\ + ... + E_{M-1,j,N-1,M\cdot N-1}x^{N-1} \quad (26)$$

Таким образом, многочлен $E_j(x)$ блока ошибок с коэффициентами $E_{l,j,\mu,i}$ над $GF(q^m)$ запишем

$$E_j(x) = \sum_{l=0}^{M-1} E_{j,l}(x) \cdot x^{l\cdot N} . \quad (27)$$

На основе выражений (22) и (27) многочлен $E(x)$ ошибок над $GF(q^m)$ имеет вид

$$E(x) = \sum_{j=0}^{\infty}\left[\sum_{l=0}^{M-1} E_{j,l}(x)\cdot x^{l\cdot N}\right]\cdot x^{j\cdot M\cdot N} = \\ = \sum_{j=0}^{\infty} E_j(x)\cdot x^{j\cdot M\cdot N} . \quad (28)$$

Таким образом, выражение (28) является алгебраическим представлением последовательности ошибок, которые могут возникать в последовательностях кодовых слов алгебраических сверточных кодов перемежения из-за наличия помех в реальных каналах связи.

Выводы

Анализ известных методов помехоустойчивого кодирования, позволяющих исправлять группирующиеся ошибки, показал, что известные методы обладают рядом недостатков, при этом отсутствует алгебраическая процедура их построения или отсутствуют алгебраические методы их декодирования.

Предложены выражения (20) – (28), позволяющие алгебраическим способом представить группирующиеся ошибки в последовательностях кодовых слов алгебраических сверточных кодов перемежения.

На основании алгебраического представления группирующихся ошибок, удается учесть их при разработке и модернизации новых методов алгебраического сверточного декодирования [6].

Литература

1. Данько Н.И. Алгебраические сверточные коды: учеб. пособие/ Н.И. Данько, С.П. Евсеев, А.А. Кузнецов, П.Ф. Поляков, С.И. Приходько. – Х.: УкрГАЖТ, 2007. – 238 с.
2. Блейхут Р. Теория и практика кодов, контролирующих ошибки: пер. с англ./ Р. Блейхут. – М.: Мир, 1986. – 576 с.
3. Кларк Дж. Кодирование с исправлением ошибок в системах цифровой связи / Дж. Кларк, мл., Дж. Кейн; пер. с англ. С.И. Гельфанда; под ред. Б.С. Цибакова. – М.: Радио и связь, 1987. – 392 с.
4. Теория кодирования / Т. Касами, Н. Токура, Е. Ивадари, Я. Инагаки; пер. с япон. А.В. Кузнецова; под ред. Б.С. Цыбакова, С.И. Гельфанда. – М.: Мир, 1978. – 576 с.
5. Скляр Б. Цифровая связь. Теоретические основы и практическое применение / Б. Скляр; [пер. с англ. Е.Г. Грозы, В.В. Марченко, А.В. Назаренко]; под ред. А.В. Назаренко. – М.: Издат. дом «Вильямс», 2003. – 1104 с.
6. Боцул А.В. Метод декодирования алгебраических сверточных кодов перемежения / А.В. Боцул., А.С. Волков, С.И. Приходько, Н.А. Штомпель // Системы обработки информации. – 2012. – Вып. 7(105). – С. 175 – 179.
7. Приходько С.И. Метод модификации обобщенного порождающего многочлена алгебраических сверточных кодов / С.И. Приходько, А.С. Волков, Н.А. Штомпель, А.В. Боцул // Інформаційно-керуючі системи на залізничному транспорті. – Х.: УкрДАЗТ, – 2012. – №6. – С. 15 – 19.

Боцул А.В., Зубенко В.О., Волков О.С., Штомпель М.А. Властивості алгебраїчних згорткових кодів перемеження. Проведено аналіз та дослідження основних властивостей алгебраїчних згорткових кодів перемеження, які виправляють груповані помилки, що виникають у каналах зв'язку. Отримано вирази, які дозволяють алгебраїчним способом представити груповані помилки, що спотворюють кодові слова алгебраїчних загорткових кодів перемеження.
Ключові слова: згортковий код, завадостійке кодування, перемеження, декодування.

Botsul Andrey Vladimirovich, Zubenko Valentina Alexandrovna, Volkov Alexey Stanislavovych, Shtompel Nikolay Anatolevych. Properties of algebraic convolutional interleaving codes . The analysis and study of basic properties of algebraic convolutional interleaving codes correcting packing errors that occur in the communication channels have been conducted. Expressions allowing us to introduce packing errors distorting the code words of algebraic convolutional interleaving codes algebraically have been obtained.
Key words: convolutional code, antinoise coding, interleaving, decoding.

Рецензент д.т.н., профессор Краснобаев В.А. (Полтавский национальный технический университет им. Ю.Кондратюка)

Поступила 16.09.2013 г.