УДК 512.21:621.391

С.И. Приходько, Д.М. Кузьменко

Харьковская государственная академия железнодорожного транспорта

МЕТОД ДЕКОДИРОВАНИЯ АЛГЕБРАИЧЕСКИХ СВЕРТОЧНЫХ КОДОВ

Рассматриваются сверточные коды, алгебраически заданные совокупностью порождающих многочленов, в том числе, посредством ограничения порождающих многочленов недвоичных циклических кодов на произвольное подполе. Исследуются процедуры декодирования сверточных кодов. Предлагается новый метод декодирования алгебраических сверточных кодов, который основан на последовательном итеративном декодировании конечной суммы кодовых слов циклического кода и реализуется с помощью алгебраических процедур локализации и исправления случайных ошибок полубесконечного кодового слова непрерывных кодов.

сверточные коды, метод декодирования

Постановка проблемы в общем виде и анализ литературы

Для повышения помехоустойчивости передачи дискретных сообщений в телекоммуникационных системах и сетях используют методы помехоустойчивого кодирования [1, 2]. Наиболее эффективными считаются сверточные коды, которые при прочих равных условиях позволяют обеспечить высокую помехоустойчивость и получить бо́льший энергетический выигрыш от кодирования [2 – 4].

В работах [4, 5] предложен алгебраический подход к решению проблемы синтеза сверточных кодов, в [6] исследованы свойства синтезируемых кодовых конструкций по достигаемому свободному кодовому расстоянию алгебраически заданных сверточных кодов. В тоже время научно-техническая задача разработки алгебраических методов построения сверточных кодов в общем виде не решена [1 – 4].

В данной статье предлагается метод декодирования алгебраических сверточных кодов, исследуются особенности его реализации, оценивается временная сложность как функция размера решаемой задачи.

Основная часть

Рассмотрим структуру кодовых слов алгебраически заданных сверточных кодов, исследуем особенности его построения.

Сверточный код по определению состоит из бесконечного числа бесконечно длинных кодовых слов. Он линеен, следовательно, может быть задан бесконечной порождающей матрицей [2, 3].

Предположим, что нерекурсивный сверточный код над GF(q) в несистематическом виде задан порождающими многочленами вида

$$P_1(x) = p_{1,r-1}x^{r-1} + p_{1,r-2}x^{r-2} + \ldots + p_{1,1}x + p_{1,0};$$

$$P_2(x) = p_{2,r-1}x^{r-1} + p_{2,r-2}x^{r-2} + \ldots + p_{2,1}x + p_{2,0};$$

$$P_m(x) = p_{m,r-1}x^{r-1} + p_{m,r-2}x^{r-2} + \ldots + p_{m,1}x + p_{m,0},$$

где коэффициенты при x являются элементами GF(q), $n^0 = m$.

Тогда соответствующая полубесконечная порождающая матрица запишется в виде [2, 3]:

$$G = \begin{vmatrix} G_0 & G_1 & G_2 & \ldots & G_r & 0 & 0 & \ldots & 0 & \ldots \\ 0 & G_0 & G_1 & \ldots & G_{r-1} & G_r & 0 & \ldots & 0 & \ldots \\ 0 & 0 & G_0 & \ldots & G_{r-2} & G_{r-1} & G_r & \ldots & 0 & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & G_0 & G_1 & G_2 & \ldots & G_r & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \end{vmatrix}, \quad (1)$$

где G_i – матрица-строка, состоящая из коэффициентов порождающих многочленов сверточного кода при x:

$$G_i = (p_{1,i}, p_{2,i}, \ldots, p_{m,i}). \quad (2)$$

Символом 0 в (1) обозначена матрица-строка, состоящая из n^0 нулевых символов из GF(q).

В случае систематического сверточного кода

$$G_0 = (1, p_{2,0}, \ldots, p_{m,0}) = (1, P_0)$$

и

$$G_i = (0, p_{2,i}, \ldots, p_{m,i}) = (0, P_i).$$

Тогда матрица (1) перепишется в виде

$$G = \begin{vmatrix} 1 & P_0 & 0 & P_1 & 0 & P_2 & 0 & \ldots & 0 & P_r & 0 & 0 & 0 & \ldots \\ 0 & 0 & 1 & P_0 & 0 & P_1 & 0 & \ldots & 0 & P_{r-1} & 0 & P_r & 0 & \ldots \\ 0 & 0 & 0 & 0 & 1 & P_0 & 0 & \ldots & 0 & P_{r-2} & 0 & P_{r-1} & 0 & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \ldots & 1 & P_0 & 0 & P_1 & 0 & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \end{vmatrix}.$$

Соответствующую полубесконечную проверочную матрицу запишем в виде [2, 3]:

$$H = \begin{vmatrix} P_0^T & -1 & 0 & 0 & 0 & 0 & \ldots & 0 & 0 & 0 & 0 & 0 & 0 & \ldots \\ P_1^T & 0 & P_0^T & -1 & 0 & 0 & \ldots & 0 & 0 & 0 & 0 & 0 & 0 & \ldots \\ P_2^T & 0 & P_1^T & 0 & P_0^T & -1 & \ldots & 0 & 0 & 0 & 0 & 0 & 0 & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ P_r^T & 0 & P_{r-1}^T & 0 & P_{r-2}^T & 0 & \ldots & 0 & P_0^T & -1 & 0 & 0 & 0 & \ldots \\ 0 & 0 & P_r^T & 0 & P_{r-1}^T & 0 & \ldots & 0 & P_1^T & 0 & P_0^T & -1 & 0 & \ldots \\ 0 & 0 & 0 & 0 & P_r^T & 0 & \ldots & 0 & P_2^T & 0 & P_1^T & 0 & P_0^T & \ldots \\ 0 & 0 & 0 & 0 & 0 & 0 & \ldots & 0 & P_3^T & 0 & P_2^T & 0 & P_1^T & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \end{vmatrix}$$

Воспользуемся введенным выше алгебраическим описанием нерекурсивных сверочных кодов. Сопоставим каждую подматрицу G_i элементу поля $\beta_i \in GF(q^m)$, так, например, что

$$\beta_i = p_{1,i} + p_{2,i}x + \ldots + p_{m,i}x^m.$$

Тогда (2) перепишем в виде

$$G_i = (p_{1,i}, p_{2,i}, \ldots, p_{m,i}) = \beta_i,$$

а полубесконечную матрицу (1) представим в виде соответствующей матрицы с элементами из $GF(q^m)$:

$$G = \begin{vmatrix} \beta_0 & \beta_1 & \beta_2 & \ldots & \beta_r & 0 & 0 & \ldots & 0 & \ldots \\ 0 & \beta_0 & \beta_1 & \ldots & \beta_{r-1} & \beta_r & 0 & \ldots & 0 & \ldots \\ 0 & 0 & \beta_0 & \ldots & \beta_{r-2} & \beta_{r-1} & \beta_r & \ldots & 0 & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & \beta_0 & \beta_1 & \beta_2 & \ldots & \beta_r & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \end{vmatrix}. \quad (3)$$

В полиномиально-матричном представлении последнее выражение перепишем в виде матрицы многочленов G(x):

$$G(x) = \begin{vmatrix} P(x) \\ x \cdot P(x) \\ \ldots \\ x^r \cdot P(x) \\ \ldots \end{vmatrix},$$

где многочлен

$$P(x) = \beta_r x^r + \beta_{r-1}x^{r-1} + \ldots + \beta_1 x + \beta_0 -$$

суть порождающий многочлен недвоичного (N, K, D) циклического кода над $GF(q^m)$, который однозначно задает (n, k) несистематический сверточный код над GF(q) с параметрами: $k^0 = 1$, $n^0 = m$, $\nu = r \cdot k^0 = r$, $k = r + 1$, $n = (r + 1) \cdot n^0 = k \cdot m$, $R = 1 / m$, $d_\infty \geq D$, $C(x) = I(x) \cdot P(x)$. Тогда подматрица

$$\|G\|_{K,N} = \begin{vmatrix} \beta_0 & \beta_1 & \beta_2 & \ldots & \beta_r & 0 & 0 & \ldots & 0 \\ 0 & \beta_0 & \beta_1 & \ldots & \beta_{r-1} & \beta_r & 0 & \ldots & 0 \\ 0 & 0 & \beta_0 & \ldots & \beta_{r-2} & \beta_{r-1} & \beta_r & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & \beta_0 & \beta_1 & \beta_2 & \ldots & \beta_r \end{vmatrix} \quad (4)$$

суть порождающая матрица (N, K, D) циклического кода над $GF(q^m)$. В полиномиально-матричном представлении запишем в виде

$$\|G(x)\|_K = \begin{vmatrix} P(x) \\ x \cdot P(x) \\ \ldots \\ x^{K-1} \cdot P(x) \end{vmatrix}.$$

Введенное обобщение (N, K, D) циклического кода на непрерывный случай позволяет использовать свойства колец многочленов при описании соответствующих сверточных кодов.

Пусть $I(x) = i_0 + i_1 x + i_2 x^2 + \ldots$ - информационный многочлен, возможно бесконечной длины, с коэффициентами из GF(q). Предположим что I(x) поступает на вход несистематического кодера нерекурсивного сверточного (n, k, d) кода алгебраически заданного через порождающий многочлен P(x) циклического (N, K, D) кода над $GF(q^m)$. Тогда кодовое слово сверточного кода суть обобщение на непрерывный случай кодового слова циклического кода ограниченного на подполе GF(q). Кодовая последовательность на выходе сверточного кодера будет задаваться выражением:

$$C(x) = I(x) \cdot P(x) = C_0 + C_1 x + C_2 x^2 + \ldots, \quad (5)$$

где C_i – элементы поля $GF(q^m)$, отображаемые в наборы по m символов из подполя GF(q).

В матричной форме последнее выражение примет вид:

$$C = I \cdot G, \quad (5')$$

где $C = (C_0, C_1, C_2, \ldots)$, $I = (i_0, i_1, i_2, \ldots)$ – кодовый и информационный векторы, составленные из коэффициентов соответствующих многочленов.

Рассмотрим правило формирования коэффициентов кодового многочлена (5), аналитически свяжем значение каждого кодового символа с информационными символами, поступающими на вход кодера.

Разобьем информационный вектор I на блоки по K символов из GF(q):

$$I = (i_0, i_1, i_2, \ldots, i_{K-1}) \cup (i_K, i_{K+1}, i_{K+2}, \ldots, i_{2K-1}) \cup (i_{2K}, i_{2K+1}, i_{2K+2}, \ldots, i_{3K-1}) \cup \ldots.$$

Обозначим каждый блок из K символов через I_i:

$$I = I_0 \cup I_1 \cup I_2 \cup \ldots.$$

В полиномиальном виде последнее выражение эквивалентно следующему:

$$I(x) = I_0(x) + x^K I_1(x) + x^{2K} I_2(x) + \ldots, \quad (6)$$

где $I_i(x) = i_{i \cdot K} + i_{i \cdot K+1} x + i_{i \cdot K+2} x^2 + \ldots i_{(i+1) \cdot K-1} x^{K-1}$.

Подставим (6) в (5), получим:

$$C(x) = I(x) \cdot P(x) =$$

$$= \left(I_0(x) + x^K I_1(x) + x^{2K} I_2(x) + \ldots\right) \cdot P(x) =$$

$$I_0(x) \cdot P(x) + x^K I_1(x) \cdot P(x) + x^{2K} I_2(x) \cdot P(x) + \ldots = \quad (7)$$

$$= \sum_{i=0}^{\infty} x^{i \cdot K} I_i(x) \cdot P(x),$$

или в матричном виде

$$C = \sum_{i=0}^{\infty} \|I_i\|_K \cdot \|G\|_{K,N} \cdot \|0, I\|_{N, i \cdot K+N}, \quad (7')$$

где $\|0, I\|_{N, i \cdot K+N}$ – единичная матрица с добавленными слева $i \cdot K$ нулевыми столбцами.

Проанализируем полученное выражение (7). Каждое слагаемое содержит произведение порождающего многочлена циклического (N, K, D) кода на информационный многочлен $I_i(x)$ степени $\deg I_i(x) \leq K - 1$. Однако, произведение $I_i(x) \cdot P(x)$ – суть кодовое слово циклического (N, K, D) кода, которое соответствует информационному вектору

$$I_i = (i_{i \cdot K}, i_{i \cdot K+1}, i_{i \cdot K+2}, \ldots, i_{(i+1) \cdot K-1}),$$

т.е.

$$I_i(x) \cdot P(x) = c_i(x), \quad (8)$$

где $c_i(x) = c_{i,0} + c_{i,1} x + c_{i,2} x^2 + \ldots c_{i,N-1} x^{N-1}$.

Подставим (8) в (7), получим:

$$C(x) = I(x) \cdot P(x) =$$

$$= c_0(x) + x^K c_1(x) + x^{2K} c_2(x) + \ldots = \sum_{i=0}^{\infty} x^{i \cdot K} c_i(x) \quad (9)$$

или, в матричном виде

$$C = \sum_{i=0}^{\infty} \|c_i\|_N \cdot \|0, I\|_{N, i \cdot K+N}. \quad (9')$$

Таким образом, как следует из выражения (9), бесконечное кодовое слово нерекурсивного сверточ-

ного кода алгебраически заданного через порождающий многочлен циклического кода состоит из бесконечной суммы кодовых слов циклического кода, умноженных на соответствующий оператор задержки $x^{i\cdot K}$. Структура бесконечного кодового слова алгебраического сверточного кода представлена на рис. 1.

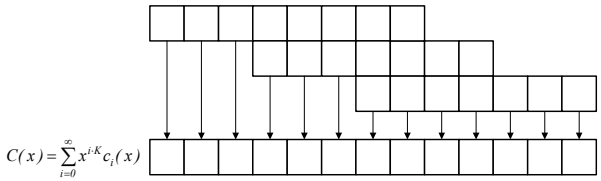

Рис. 1. Структура бесконечного кодового слова алгебраического нерекурсивного сверточного кода

Как видно на рис. 1 бесконечное кодовое слово сверточного кода формируется наложением бесконечного числа кодовых слов циклического кода и суммированием соответствующих элементов $c_{i,j}$.

Предположим теперь, что при передаче бесконечной кодовой последовательности вектор C = (C_0, C_1, …) исказился, т.е. на приемной стороне получено искаженное кодовое слово

$$C^*(x) = C(x) + E(x), \qquad (10)$$

где $E(x) = e_0 + e_1x + \ldots$ – бесконечный вектор ошибок.

По аналогии с информационным вектором разобьем вектор ошибок E = (e_0, e_1, e_2, …), составленный из коэффициентов многочлена ошибок E(x), на блоки по K символов из GF(q):

$$E = (e_0, e_1, e_2, \ldots, e_{K-1}) \cup (e_K, e_{K+1}, e_{K+2}, \ldots, e_{2K-1}) \cup \ldots.$$

Обозначим каждый блок из K символов через E_i:

$$E = E_0 \cup E_1 \cup E_2 \cup \ldots.$$

В полиномиальном виде последнее выражение эквивалентно следующему:

$$E(x) = E_0(x) + x^K E_1(x) + x^{2K} E_2(x) + \ldots, \qquad (11)$$

где $E_i(x) = e_{i\cdot K} + e_{i\cdot K+1}x + e_{i\cdot K+2}x^2 + \ldots e_{(i+1)\cdot K-1}x^{K-1}$.

Подставим (11) в (10), получим:

$$C^*(x) = C(x) + E(x) = \sum_{i=0}^{\infty} x^{i\cdot K}\left(I_i(x)\cdot P(x) + E_i(x)\right).$$

С учетом (9) последнее выражение

$$C^*(x) = C(x) + E(x) = \sum_{i=0}^{\infty} x^{i\cdot K}\left(c_i(x) + E_i(x)\right) \qquad (12)$$

или матричной форме

$$C^* = \sum_{i=0}^{\infty}\left(\|c_i\|_N + \|e_i, 0\|_N\right)\cdot\|0, I\|_{N,i\cdot K+N}, \qquad (12')$$

где $\|e_i, 0\|_N$ – вектор ошибок E_i длины K символов с добавленными справа (N – K) нулями.

Проанализируем полученное выражение. Каждое слагаемое содержит сумму кодового слова $c_i(x)$ циклического (N, K, D) кода и многочлена ошибки $E_i(x)$. Размерность вектора E_i составляет K символов, т.е. сумма $c_i(x)+ E_i(x)$ – суть кодовое слово циклического (N, K, D) кода, искаженное вектором ошибки E_i:

$$c_i^*(x) = c_i(x) + E_i(x). \qquad (13)$$

Тогда, с учетом (13), выражение (12) перепишем в виде:

$$C^*(x) = C(x) + E(x) = \sum_{i=0}^{\infty} x^{i\cdot K} c_i^*(x) \qquad (14)$$

или

$$C^* = \sum_{i=0}^{\infty}\|c^*_i\|_N \cdot \|0, I\|_{N,i\cdot K+N}. \qquad (14')$$

Таким образом, как следует из выражения (14), бесконечное кодовое слово алгебраического нерекурсивного сверточного кода искаженное бесконечным вектором ошибок состоит из бесконечной суммы кодовых слов циклического кода, искаженных вектором ошибок конечной размерности, умноженных на соответствующий оператор задержки $x^{i\cdot K}$.

Представим, для наглядности, структуру искаженного ошибками бесконечного кодового слова алгебраического сверточного кода на рис. 2.

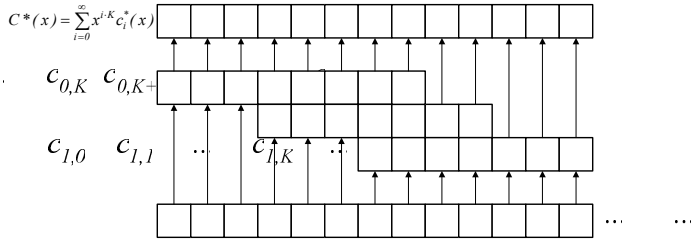

Рис. 2. Структура искаженного ошибками бесконечного кодового слова алгебраического нерекурсивного сверточного кода

Как видно на рис. 2, искаженное ошибками бесконечное кодовое слово сверточного кода формируется наложением бесконечного числа искаженных кодовых слов циклического кода и суммированием соответствующих элементов $c^*_{i,j}$.Введем синдромный многочлен алгебраического сверточного кода:

$$S(x) = s_0 + s_1x + s_2x^2 + \ldots, \qquad (15)$$

как бесконечную сумму синдромных многочленов циклического кода, умноженных на соответствующий оператор задержки $x^{i\cdot K}$, т.е. как бесконечную сумму остатков от деления кодовых слов циклического кода на порождающий многочлен P(x):

$$S(x) = \sum_{i=0}^{\infty} x^{i\cdot(N-K)} R_{P(x)}\left[c_i^*(x)\right]. \qquad (16)$$

В кольце многочленов $GF(q^m)[x]/(x^N - 1)$ существует единственный приведенный ненулевой многочлен h(x)

$$h(x) = \gamma_K x^K + \gamma_{K-1}x^{K-1} + \ldots + \gamma_1 x + \gamma_0$$

наименьшей степени K, который обозначается проверочным многочленом и также однозначно задает (N, K, D) циклический код над $GF(q^m)$ [2 – 4]. Соответствующая проверочная матрица (N, K, D) циклического кода может быть записана в виде

$$\|H\|_{N-K,N} = \begin{vmatrix} \gamma_K & \ldots & \gamma_2 & \gamma_1 & \gamma_0 & \ldots & 0 & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & \gamma_K & \gamma_{K-1} & \gamma_{K-2} & \ldots & \gamma_0 & 0 & 0 \\ 0 & \ldots & 0 & \gamma_K & \gamma_{K-1} & \ldots & \gamma_1 & \gamma_0 & 0 \\ 0 & \ldots & 0 & 0 & \gamma_K & \ldots & \gamma_2 & \gamma_1 & \gamma_0 \end{vmatrix},$$

или в полиномиально-матричном обозначении:

$$H(x)=\begin{vmatrix} h(x) \\ x\cdot h(x) \\ \dots \\ x^{r-1}\cdot h(x) \end{vmatrix},$$

где нумерация коэффициентов многочлена идет в обратном G(x) порядке.

Воспользуемся мультипликативно обратным многочлену P(x) в кольце $GF(q^m)[x]/(x^N-1)$ элементом – проверочным многочленом h(x) циклического (N, K, D) кода, перепишем последнее выражение как

$$S(x)=\sum_{i=0}^{\infty} x^{i\cdot(N-K)} R_{(x^N-1)}\left[c_i^*(x)\cdot h(x)\right], \quad (16')$$

что в матричном виде эквивалентно следующему

$$S=\sum_{i=0}^{\infty} \|c^*_i\|_N \cdot \|H\|^T_{N-K,N} \cdot \|0,I\|_{N-K,i\cdot(N-K)+N-K}. \quad (16'')$$

С учетом (12) последнее выражение перепишется в виде

$$S(x)=\sum_{i=0}^{\infty} x^{i\cdot(N-K)} R_{P(x)}\left[c_i(x)+E_i(x)\right]=$$

$$=\sum_{i=0}^{\infty} x^{i\cdot(N-K)}\left(R_{P(x)}\left[c_i(x)\right]+R_{P(x)}\left[E_i(x)\right]\right)= \quad (17)$$

$$=\sum_{i=0}^{\infty} x^{i\cdot(N-K)} R_{P(x)}\left[E_i(x)\right].$$

Перепишем через проверочный многочлен

$$S(x)=\sum_{i=0}^{\infty} x^{i\cdot(N-K)} R_{(x^N-1)}\left[E_i(x)\cdot h(x)\right], \quad (17')$$

что в матричной форме примет следующий вид

$$S=\sum_{i=0}^{\infty} \|e_i,0\|_N \cdot \|H\|^T_{N-K,N} \cdot \|0,I\|_{N-K,i\cdot(N-K)+N-K}. \quad (17'')$$

Таким образом, как следует из выражения (17), бесконечный синдром принятого с ошибками кодового слова алгебраического нерекурсивного сверточного кода состоит из бесконечной суммы синдромов принятых кодовых слов циклического кода, умноженных на соответствующий оператор задержки $x^{i\cdot(N-K)}$. Следовательно, запишем

$$S(x)=\sum_{i=0}^{\infty} x^{i\cdot(N-K)} S_i(x), \quad (18)$$

или $$S=\sum_{i=0}^{\infty} \|S_i\|_{N-K} \cdot \|0,I\|_{N-K,i\cdot(N-K)+N-K}, \quad (18')$$

где $S_i(x) = s_{i\cdot K} + s_{i\cdot K+1}x + s_{i\cdot K+2}x^2 + \dots\ s_{(i+1)\cdot K-1}x^{K-1}$ – синдромный многочлен циклического (N, K, D) кода, $S_i = (s_{i\cdot K}, s_{i\cdot K+1}, s_{i\cdot K+2}, \dots\ s_{(i+1)\cdot K-1})$ - соответствующий синдромный вектор.

Значение синдромного многочлена (вектора) зависит только от значения ошибок и не зависит от выбранного кодового слова. Представим, для наглядности, структуру и правило формирования синдромного многочлена на рис. 3. Как видно на рис. 3 бесконечный синдром формируется бесконечным суммированием соответствующих синдромов циклического кода $S_i(x)$. Причем синдромы $S_i(x)$ суммируются без наложений, т.е. каждый блок из (N - K) синдромных символов зависит исключительно от блока из K ошибочных символов. Этот факт позволяет реализовать алгебраическое правило декодирования алгебраически заданного сверточного кода.

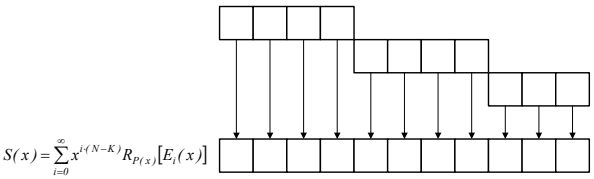

Рис. 3. Структура бесконечного синдромного многочлена алгебраического нерекурсивного сверточного кода

Действительно, декодирование бесконечного кодового слова сверточного кода распадается на бесконечную последовательность декодирований кодовых слов циклического (N, K, D) кода. Причем каждый синдромный вектор S_i соответствует ошибке, произошедшей на блоке из K символов. В случае неправильного декодирования ошибка распространяется только в пределах блока данных из K символов. Следовательно, независимость блоков синдромных символов позволяет избежать распространения ошибок, которое присуще некоторым известным способам декодирования сверточных кодов [2, 3].

Таким образом, в результате проведенных рассуждений удалось свести декодирование бесконечного кодового слова к бесконечной серии декодирований циклического блокового кода. Рассмотрим теперь декодирование одного блока символов бесконечного сверточного кода, а затем обобщим его на случай бесконечных серий.

Проанализируем выражение (17). Оно содержит бесконечную сумму произведений непересекающихся ненулевых векторов ошибок на проверочную $\|H\|_{N-K,N}$ матрицу циклического (N, K, D) кода, заданного через порождающий многочлен P(x). Очевидно, что матрица $\|H\|^T_{N-K,N}$ может быть записана в виде (4), но для декодирования циклических кодов используется другая ее форма, которая отражает структуру колец многочленов и, непосредственно, свойства самого многочлена P(x).

Обозначим через X_l – l-й корень порождающего многочлена P(x), причем $X_l = \alpha^{Jl}$ для некоторого J_l, $X_l \in GF(q^m)$. Если $X_0, X_1, \dots, X_{r-1}$ – все корни многочлена P(x), т.е. $P(x) = (x + X_0)\cdot(x + X_1) \cdot \dots \cdot (x + X_{r-1})$, то справедливо равенство

$$c(X_i) = c_0 + c_1 X_i + c_2 X_i^{\,2} + \dots + c_{N-1} X_i^{\,N-1} = 0,$$

где c(x) – кодовый многочлен.

Перепишем последнее выражение в виде матричного произведения:

$$c(X_i) = (c_0, c_1, c_2, \dots, c_{N-1}) \cdot (1, X_i, X_i^{\,2}, \dots, X_i^{\,N-1})^T = 0,$$

где c кодовое слово циклического (N, K, D) кода как набор коэффициентов многочлена c(x).

Обобщим последнее равенство для всех корней P(x), получим:

$$(c_0, c_1, c_2, ..., c_{N-1}) \cdot \begin{vmatrix} 1 & X_0 & X_0^2 & ... & X_0^{N-1} \\ 1 & X_1 & X_1^2 & ... & X_1^{N-1} \\ 1 & X_2 & X_2^2 & ... & X_2^{N-1} \\ ... & ... & ... & ... & ... \\ 1 & X_{r-1} & X_{r-1}^2 & ... & X_{r-1}^{N-1} \end{vmatrix}^T = 0 \cdot$$

Полученное выражение соответствует условию взаимной ортогональности произвольного кодового слова c =(c_0, c_1, c_2,…, c_{N-1}) и матрицы в правой части произведения. Следовательно, положим

$$\|H\|_{N-K,N} = \begin{vmatrix} 1 & X_0 & X_0^2 & ... & X_0^{N-1} \\ 1 & X_1 & X_1^2 & ... & X_1^{N-1} \\ 1 & X_2 & X_2^2 & ... & X_2^{N-1} \\ ... & ... & ... & ... & ... \\ 1 & X_{r-1} & X_{r-1}^2 & ... & X_{r-1}^{N-1} \end{vmatrix}. \quad (19)$$

Предположим теперь, что кодовое слово с исказилось при передаче. Пусть число ошибок на блоке из N символов не превышает исправляющей способности t = (D – 1)/2 циклического (N, K, D) кода. Обозначим e(x) – многочлен ошибок, так, что

$$e(x) = e_0 + e_1x + e_2x^2 + \ldots + e_{N-1}x^{N-1}$$

c ≤ t ненулевыми коэффициентами.

Пусть $c^*(x) = c^*_0 + c^*_1x + c^*_2x^2 + \ldots + c^*_{N-1}x^{N-1}$ – кодовое слово с ошибками, т.е.

$$c^*(x) = c(x) + e(x) = (c_0 + e_0) + (c_1 + e_1)x + (c_2 + e_2)x^2 + \ldots + (c_{N-1} + e_{N-1})x^{N-1}.$$

Значение вектора синдромов вычислим из выражения

$$(s_0, s_1, ..., s_{r-1}) = (e_0, e_1, e_2, ..., e_{N-1}) \times \begin{vmatrix} 1 & X_0 & X_0^2 & ... & X_0^{N-1} \\ 1 & X_1 & X_1^2 & ... & X_1^{N-1} \\ 1 & X_2 & X_2^2 & ... & X_2^{N-1} \\ ... & ... & ... & ... & ... \\ 1 & X_{r-1} & X_{r-1}^2 & ... & X_{r-1}^{N-1} \end{vmatrix}^T,$$

что эквивалентно следующей системе уравнений:

$$s_0 = e_0 + e_1X_0 + e_2X_0^2 + ... + e_{N-1}X_0^{N-1} = \sum_{i=0}^{N-1} e_iX_0^i;$$

$$s_1 = e_0 + e_1X_1 + e_2X_1^2 + ... + e_{N-1}X_1^{N-1} = \sum_{i=0}^{N-1} e_iX_1^i; \quad (20)$$

$$\ldots s_{r-1} = e_0 + e_1X_{r-1} + e_2X_{r-1}^2 + ... + e_{N-1}X_{r-1}^{N-1} = \sum_{i=0}^{N-1} e_iX_{r-1}^i.$$

Задача декодирования блока данных из N символов состоит в нахождении всех e_i, i = 0,…, N – 1 по известным элементам синдромной последовательности (s_0, s_1, …, s_{r-1}).

Система уравнений (20) нелинейная, прямых методов ее решения не известно. Для нахождения вектора ошибок (e_0, e_1, e_2, …, e_{N-1}) воспользуемся искусственным приемом. Введем многочлен локаторов ошибок Λ(x), корнями которого являются ненулевые элементы вектора ошибок, т.е.

$$\Lambda(x) = \prod_j (x + X_j), \quad (21)$$

где j – индекс ненулевых элементов вектора ошибок, X_j – локатор ошибки, произошедшей в j-ом символе кодового слова.

Раскроем скобки в выражении (21), получим

$$\Lambda(x) = x^w + \lambda_{w-1}x^{w-1} + \ldots + \lambda_1x + \lambda_0, \quad (22)$$

где степень w многочлена Λ(x) задает число произошедших ошибок на блоке из N символов, w ≤ t, т.е. число ненулевых элементов вектора ошибок (e_0, e_1, e_2, …, e_{N-1}).

Набор (λ_0, λ_1, …, λ_{w-1}) коэффициентов многочлена (22) однозначно задает его корни, которые, соответственно, однозначно указывают (локализуют) расположение произошедших ошибок. Умножим многочлен (22) на e_iX^i и вычислим его значение в X_j, получим:

$$e_iX_j^{w+i} + e_i\lambda_{w-1}X_j^{w+i-1} + \ldots + e_i\lambda_1X_j^{i+1} + e_i\lambda_0X_j^i = 0,$$

где $X_j \in GF(q^m)$, т.е. $X_j = \alpha^{Jj}$ для некоторого J_j.

Следовательно, $X_j^{a+b} = \alpha^{a+b+Jj} = X^b_{j+a}$, т.е. справедливо выражение

$$e_iX_{j+w}^i + e_i\lambda_{w-1}X_{j+w-1}^i + \ldots + e_i\lambda_1X_{j+1}^i + e_i\lambda_0X_j^i = 0.$$

Последнее равенство выполняется для любого j и при каждом i. Просуммируем по всем i = 0…N – 1, получим

$$\sum_{i=0}^{N-1} \left(e_iX_{j+w}^i + e_i\lambda_{w-1}X_{j+w-1}^i + \ldots + e_i\lambda_1X_{j+1}^i + e_i\lambda_0X_j^i \right) = 0.$$

Изменив порядок суммирования, вынесем коэффициенты многочлена локаторов ошибок за знак суммирования, получим:

$$\sum_{i=0}^{N-1} e_iX_{j+w}^i + \lambda_{w-1} \cdot \sum_{i=0}^{N-1} e_iX_{j+w-1}^i + \ldots + \lambda_1 \cdot \sum_{i=0}^{N-1} e_iX_{j+1}^i + \lambda_0 \cdot \sum_{i=0}^{N-1} e_iX_j^i = 0.$$

Значение каждого слагаемого в последнем выражении соответствует произведению коэффициентов многочлена локаторов ошибок на соответствующие синдромы в выражении (20), так что запишем

$$s_{j+w} + \lambda_{w-1} \cdot s_{j+w-1} + \ldots + \lambda_1 \cdot s_{j+1} + \lambda_0 \cdot s_j = 0. \quad (23)$$

Перепишем выражение (23) для каждого j = 0…w, получим систему линейных уравнений:

$$\begin{aligned} &s_w + \lambda_{w-1} \cdot s_{w-1} + \ldots + \lambda_1 \cdot s_1 + \lambda_0 \cdot s_0 = 0; \\ &s_{w+1} + \lambda_{w-1} \cdot s_w + \ldots + \lambda_1 \cdot s_2 + \lambda_0 \cdot s_1 = 0, \\ &s_{2\cdot w} + \lambda_{w-1} \cdot s_{2\cdot w-1} + \ldots + \lambda_1 \cdot s_{w+1} + \lambda_0 \cdot s_w = 0. \end{aligned} \quad (24)$$

Система из w линейных уравнений (24) с w неизвестными разрешима, сложность ее решения растет полиномиально от числа неизвестных [1 – 3]. Так, например, для решения системы (24) методом Гаусса необходимо выполнить n^2 сложений и умножений над элементами $GF(q^m)$, или, формально, сложность алгоритма $O(n^2)$.

Решение системы уравнений (24) дает значения коэффициентов многочлена локаторов ошибок (22). Корнями многочлена (22) являются локаторы-элементы $GF(q^m)$, которые однозначно указывают

расположение ошибок. Следовательно, для локализации ошибок необходимо найти корни уравнения (22).

Наиболее простая процедура поиска корней многочлена локаторов ошибок состоит в подстановке всех элементов поля $GF(q^m)$ и выборе тех элементов, которые обращают в нуль многочлен (22). В литературе такой прием получил название процедуры Ченя [1, 3].

После локализации ошибок – нахождении локаторов ошибок X_j, необходимо вычислить значения ошибок в j-ом символе, т.е. вычислить вектор ошибок $(e_0, e_1, e_2, \ldots, e_{N-1})$ и восстановить кодовое слово: $c = c^* - e$.

Для нахождения значений ошибок воспользуемся выражением (20). Подставим значения найденных локаторов X_j и неизвестные значения e_j в систему уравнений. Остальные e_i при $i \neq j$ равны нулю. Следовательно, система уравнений (20) запишется в виде:

$$s_0 = \sum_{i \in J} e_i X_0^i ; \quad s_1 = \sum_{i \in J} e_i X_1^i ; \quad s_{r-1} = \sum_{i \in J} e_i X_{r-1}^i , \qquad (25)$$

где J – множество индексов ненулевых элементов вектора ошибок, т.е. набор номеров локаторов ошибок, причем $|J| = w \le t$.

Система (25) из r линейных уравнений содержит $|J| = w \le t$ неизвестных значений ошибок e_i, причем $t < r$. Следовательно, система (25) разрешима, ее решение дает неизвестные ненулевые значения ошибок вектора $(e_0, e_1, e_2, \ldots, e_{N-1})$. Для восстановления кодового слова длины N кодовых символов достаточно снять действие найденного вектора ошибок:

$$c = c^* - e.$$

Выводы

Таким образом, в результате проведенных исследований предложен метод декодирования алгебраически заданных сверточных кодов. Для реализации предложенного подхода необходимо и достаточно вычислить бесконечную сумму синдромов соответствующих кодовых слов циклического кода, т.е. вычислить все значения S_i в выражении (18).

Для вычисления синдромной последовательности в алгебраической теории блоковых кодов используют умножение кодового слова на проверочную матрицу и/или, что эквивалентно, формируют синдромный многочлен $S_i(x)$ через соответствующие операции в кольце многочленов $GF(q)[x]/(x^n - 1)$.

Эквивалентной операцией для непрерывных кодов будет произведение кодового слова на полубесконечную проверочную матрицу сверточного кода, заданную через корни порождающего многочлена.

Таким образом, **перспективным направлением дальнейших исследований** является разработка процедур формирования бесконечной серии синдромных последовательностей $S_i = (s_{i \cdot K}, s_{i \cdot K+1}, s_{i \cdot K+2}, \ldots s_{(i+1) \cdot K-1})$, выработка практических рекомендаций по реализации предложенного выше подхода алгебраического декодирования сверточных кодов.

Список литературы

1. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. – М.: Вильямс, 2003. – 1104 с.

2. Краснобаев В.А., Приходько С.И., Снисаренко А.Г. Помехоустойчивое кодирование в АСУ. – Х.: ХВВКИУРВ, 1990 – 155 с.

3. Касами Т., Токура Н., Ивадари Е., Инагаки Я. Теория кодирования. – М.: Мир. – 1978. – 576с.

4. Приходько С.И. Алгебраические сверточные коды // Інформаційно-керуючі системи на залізничному транспорті. – Х.: ХарДАЗТ. – 1999. – № 2 (17). – С. 62-64.

5. Приходько С.И., Кузнецов А.А., Гусев С.А., Кужель И.Е. Алгебраический метод сверточного кодирования // Комп'ютерні системи та інформаційні технології. – Х.: ХАИ. – 2005. – № 1 – С. 35-43.

6. Приходько С.И., Кузьменко Д.М. Оценка нижней границы свободного кодового расстояния алгебраически заданных сверточных кодов // Системи обробки інформації. – Х.: ХУ ПС. – 2007. – Вип. 5 (63). – С. 147-149.

Поступила в редколлегию 5.03.2008

Рецензент: канд. техн. наук, ст. научн. сотр. А.А. Кузнецов, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

МЕТОД ДЕКОДУВАННЯ ЗГОРТАЛЬНИХ КОДІВ АЛГЕБРИ

Приходько С.І., Кузьменко Д.М.

Розглядаються загортальні коди, алгебра задані сукупністю багаточленів, що породжують, зокрема, за допомогою обмеження багаточленів недвійкових циклічних кодів, що породжують, на довільне підполе. Досліджуються процедури декодування загортальних кодів. Пропонується новий метод декодування загортальних кодів алгебри, який заснований на послідовному ітеративному декодуванні кінцевої суми кодових слів циклічного коду і реалізується за допомогою процедур алгебри локалізації і виправлення випадкових помилок напівнескінченного кодового слова безперервних кодів.

Ключові слова: *згортальні коди, метод декодування.*

METHOD OF DECODING OF ALGEBRAIC CONVOLUTION CODES

Prihod'ko S.I., Kuz'menko D.M.

Convolution codes, algebraically set the aggregate of originative polynomials, are examined, including, by means of limit of originative polynomials of unbinary cyclic codes on the arbitrary subfield. Procedures of decoding of convolution codes are explored. The new method of decoding of algebraic convolution codes is offered, which is based on the successive umerativном decoding of eventual sum of words of codes of cyclic code and realized by algebraic procedures of localization and correction of random errors of semiendless code word of continuous codes.

Keywords: *convolution codes, method of decoding.*