УДК 621.391

А.В. Боцул[1], С.И. Приходько[2], А.С. Волков[2], Н.А. Штомпель[2], Билал Хамзе[2]

[1] *Национальный технический университет «ХПИ», Харьков*
[2] *Украинская государственная академия железнодорожного транспорта, Харьков*

ОСОБЕННОСТИ МЕТОДА ДЕКОДИРОВАНИЯ АЛГЕБРАИЧЕСКИХ СВЕРТОЧНЫХ КОДОВ ПЕРЕМЕЖЕНИЯ

Рассмотрен алгебраический способ формирования синдромной последовательности полубесконечной длины алгебраических сверточных кодов перемежения. Показано, что для исключения эффекта распространения ошибок при реализации алгебраической процедуры декодирования алгебраических сверточных кодов перемежения необходимо введение операторов задержки.

Ключевые слова: *помехоустойчивое кодирование, сверточные коды, синдром, декодирование сверточных кодов.*

Введение

Постановка проблемы в общем виде и анализ литературы. В телекоммуникационных системах и сетях широкое применение нашли помехоустойчивые сверточные коды [1, 2, 5]. В настоящее время известны алгебраические сверточные коды, которые допускают сколь угодно большие значения длин кодового ограничения. При этом, обработка символов кодирующими и декодирующими устройствами может быть выполнена как в поле GF(2) так и в поле $GF(q^m)$ [11].

Алгебраические сверточные коды допускают алгебраические методы декодирования, так как обладают специальной алгебраической структурой [10, 11]. Корректирующая способность таких кодов достаточно высокая, что позволяет исправлять большое число случайных ошибок [7 – 9, 11].

Известно, что в реальных каналах связи возникают как случайные, так и группирующиеся ошибки [6, 10]. При этом существующие методы сверточного кодирования и декодирования не ориентированы на исправление группирующихся ошибок, что является их значительным недостатком. Это связано с тем, что в основе данных методов декодирования заложена идея вычисления синдромной последовательности [5, 7, 10] только на длине кодового ограничения [11]. Данный недостаток ограничивает применение эффективных методов кодирования и декодирования сверточных кодов в телекоммуникационных системах и сетях [10, 11].

Таким образом, разработка и усовершенствование методов кодирования и декодирования сверточных кодов, допускающих исправление группирующихся ошибок, кратность которых превышает корректирующую способность кода, является актуальной научно-технической задачей.

Цель статьи – разработка способа формирования синдромной последовательности полубесконечной длины для реализации алгебраического метода декодирования сверточных кодов перемежения, исправляющих группирующиеся ошибки.

Основной материал

Пусть на вход декодера алгебраического сверточного кода перемежения поступает кодовое слово полубесконечной длины, представленное многочленом C(x) [3, 4, 11]:

$$C(x) = C_0 + C_1 x + C_2 x^2 + \ldots = \sum_{i=0}^{\infty} C_i x^i , \qquad (1)$$

где $C_i \in GF(q^m)$.

Разобьем кодовое слово C(x) на подблоки кодовых слов длины $N = q^m - 1$. Тогда M подблоков кодовых слов представляют собой многочлен $C_j(x)$ блока кодовых алгебраического сверточного кода перемежения длины $M \cdot N$ символов над $GF(q^m)$ (допустим M = N). Следовательно, многочлен $C_j(x)$ справедливо записать [3, 4]:

$$\begin{gathered} C_j(x) = [C_{0,j,0,0} + C_{0,j,1,1}x + C_{0,j,2,2}x^2 + \ldots + \\ + C_{0,j,N-1,N-1}x^{N-1}] + x^N \cdot [C_{1,j,0,N} + C_{1,j,1,N+1}x + \\ + C_{1,j,2,N+2}x^2 + \ldots + C_{1,j,N-1,2\cdot N-1}x^{N-1}] + \ldots + \\ + x^{(M-1)\cdot N} \cdot [C_{M-1,j,0,(M-1)\cdot N} + \\ + C_{M-1,j,1,(M-1)\cdot N+1}x + C_{M-1,j,2,(M-1)\cdot N+2}x^2 + \\ + \ldots + C_{M-1,j,N-1,M\cdot N-1}x^{N-1}]. \end{gathered} \qquad (2)$$

В выражении (2) первый индекс коэффициента указывает на номер подблока кодовых слов в одном блоке (l = 0, 1, 2, …, M – 1); второй индекс коэффициента указывает на номер блока кодового слова алгебраического сверточного кода перемежения (j = 0, 1, 2, …); третий индекс коэффициента указывает на номер коэффициента в одном подблоке кодовых слов на длине M ($\mu = 0,\ 1,\ 2,\ ...,\ N-1$); четвертый индекс коэффициента указывает номер коэффициента над GF(q^m) в одном блоке кодового слова алгебраического сверточного кода перемежения на длине $M \cdot N$ ($i = 0,\ 1,\ 2,\ ...,\ M \cdot N - 1$); $x^{l \cdot N}$ – оператор задержки и $C_{l,j,\mu,i} \in GF(q^m)$.

Далее, в процессе декодирования, выполняется алгебраическая процедура деперемежения, как показано в работах [3, 4], после которой выражение (2) возможно записать:

$$\begin{aligned} c^*_j(x) = {} & [c^*_{0,j,0,0} + c^*_{1,j,0,N}\, x + c_{2,j,0,2\cdot N} x^2 + \\ & + ... + c_{N-1,j,0,(M-1)\cdot N} x^{N-1}] + x^N \cdot [c^*_{0,j,1,1} + \\ & + c^*_{1,j,1,N+1}\, x + c_{2,j,1,2\cdot N+1} x^2 + \ ...\ + \\ & + c_{N-1,j,1,(M-1)\cdot N+1} x^{N-1}] + ... + \\ & + x^{N\cdot(M-1)} \cdot [c^*_{0,j,N-1,N-1} + c^*_{1,j,N-1,2\cdot N-1}\, x + \\ & + c_{2,j,N-1,3\cdot N-1} x^2 + \ ...\ + c_{N-1,j,N-1,M\cdot N-1} x^{N-1}], \end{aligned} \tag{3}$$

где $c^*_{l,j,\mu,i} \in GF(q^m)$ – коэффициенты многочлена $c^*_j(x)$, учитывающие влияние ошибки; $l = 0,\ 1,\ 2,\ ...,\ N-1$; j = 0, 1, 2, … ; μ = 0, 1, 2, …, M – 1; $M = N = q^m - 1$; $i = 0,\ 1,\ 2,\ ...,\ M \cdot N - 1$.

В выражении (3) показано, как распределяются поврежденные группирующейся ошибкой символы блока кодовых слов, в случае если ошибка исказила два первых подблока кодовых слов [4].

Последовательность компонент синдрома S (синдромная последовательность) длины $2 \cdot t_0$, соответствующая одному подблоку кодового слова сверточного кода перемежения, представим как:

$$S = (S_1,\ S_2,\ S_3,\ ...,\ S_{2t_0}), \tag{4}$$

где $S_b \in GF(q^m)$; b = 1, 2, …, $2 \cdot t_0$; t_0 – корректирующая способность сверточного кода перемежения на длине одного подблока. Тогда многочлен S(x) синдромной последовательности возможно представить:

$$S(x) = \sum_{b=1}^{2\cdot t_0} S_b x^b. \tag{5}$$

Пусть $(\alpha^1; \alpha^2; \alpha^3;\ ...;\ \alpha^{2\cdot t_0})$ – корни порождающего многочлена $g^*(x)$ сверточного кода перемежения. Тогда вычисление $2 \cdot t_0$ компонент синдромной последовательности выполняется следующим образом [4, 11]:

$$S_b = c^*_{j,0}(\alpha^b) = c_{j,0}(\alpha^b) + e(\alpha^b) = e(\alpha^b), \tag{6}$$

где e – вектор ошибок, $e_i \in GF(q^m)$; $c^*_{j,0}(\alpha^b)$ – нулевой подблок кодового слова поврежденный ошибками.

Каждому подблоку длины $N = q^m - 1$ кодового слова сверточного кода перемежения соответствует синдромная последовательность длины $2 \cdot t_0$ символов над GF(q^m), представленная многочленом S(x) вида (5). Так как блок кодовых слов сверточного кода перемежения, представленный многочленом $c_j(x)$, включает в себя M подблоков, то многочлен синдромной последовательности блока кодовых слов состоит из M многочленов синдромных последовательностей подблоков кодовых слов. Перепишем выражение (5) в соответствии с дополнительными индексами: l, j, μ и i для каждого коэффициента многочлена синдромной последовательности следующим образом:

$$\begin{aligned} S_{j,0}(x) = {} & S_{0,j,0,0} + S_{1,j,0,1} x + S_{2,j,0,2} x^2 + \\ & + ... + S_{2\cdot t_0 - 1,j,0,2\cdot t_0 - 1} x^{2\cdot t_0 - 1}, \end{aligned} \tag{7}$$

где $S_{l,j,\mu,i} \in GF(q^m)$.

В выражении (7) введены следующие обозначения: l – индекс, указывающий номер коэффициента на длине $2 \cdot t_0$ (первый индекс коэффициента), $l = 0,\ 1,\ 2,\ ...,\ 2 \cdot t_0 - 1$; j – индекс, указывающий номер многочлена синдромной последовательности соответствующей блоку кодового слова алгебраического сверточного кода перемежения (второй индекс коэффициента), j = 0, 1, 2, … ; μ – индекс, указывающий номер многочлена синдромной последовательности соответствующей подблоку кодовых слов в одном блоке (третий индекс коэффициента), $\mu = 0,\ 1,\ 2,\ ...,\ M-1$; i – индекс, указывающий номер коэффициента многочлена синдромной последовательности на длине $M \cdot 2 \cdot t_0$ (четвертый индекс коэффициента), $i = 0,\ 1,\ 2,\ ...,\ M \cdot 2 \cdot t_0 - 1$.

Тогда, при $\mu = 1$ многочлен синдромной последовательности, соответствующий подблоку кодового слова сверточного кода, можно записать:

$$\begin{aligned} S_{j,1}(x) = {} & S_{0,j,1,0} + S_{1,j,1,1} x + S_{2,j,1,2} x^2 + \\ & + ... + S_{2\cdot t_0 - 1,j,1,2\cdot t_0 - 1} x^{2\cdot t_0 - 1}, \end{aligned} \tag{8}$$

при $\mu = 2$:

$$\begin{aligned} S_{j,2}(x) = {} & S_{0,j,2,0} + S_{1,j,2,1} x + S_{2,j,2,2} x^2 + \\ & + ... + S_{2\cdot t_0 - 1,j,2,2\cdot t_0 - 1} x^{2\cdot t_0 - 1}, \end{aligned} \tag{9}$$

при $\mu = M - 1$:

$$\begin{aligned} S_{j,M-1}(x) = {} & S_{0,j,M-1,0} + \\ & + S_{1,j,M-1,1} x + S_{2,j,M-1,2} x^2 + \\ & + ... + S_{2\cdot t_0 - 1,j,M-1,2\cdot t_0 - 1} x^{2\cdot t_0 - 1}. \end{aligned} \tag{10}$$

Следовательно, многочлен $S_j(x)$ синдромной последовательности, соответствующий блоку кодовых слов сверточного кода перемежения, можно представить следующим образом:

$$\begin{gathered} S_j(x) = [S_{0,j,0,0} + S_{1,j,0,1}x + S_{2,j,0,2}x^2 + \\ + \ldots + S_{2\cdot t_0-1,j,0,2\cdot t_0-1}x^{2\cdot t_0-1}] + \\ + x^{2\cdot t_0}\cdot[S_{0,j,1,2\cdot t_0} + S_{1,j,1,2\cdot t_0+1}x + \\ + S_{2,j,1,2\cdot t_0+2}x^2 + \ldots + \\ + S_{2\cdot t_0-1,j,1,4\cdot t_0-1}x^{2\cdot t_0-1}] + \\ + x^{4\cdot t_0}\cdot[S_{0,j,2,4\cdot t_0} + S_{1,j,2,4\cdot t_0+1}x + \\ + S_{2,j,2,4\cdot t_0+2}x^2 + \ldots + S_{2\cdot t_0-1,j,2,6\cdot t_0-1}x^{2\cdot t_0-1}] + \\ + \ldots + \\ + x^{2\cdot t_0\cdot(M-1)}\cdot[S_{0,j,M-1,2\cdot t_0\cdot(M-1)} + \\ + S_{1,j,M-1,2\cdot t_0\cdot(M-1)+1}x + \\ + S_{2,j,M-1,2\cdot t_0\cdot(M-1)+2}x^2 + \\ + \ldots + S_{2\cdot t_0-1,j,M-1,2\cdot t_0\cdot M-1}x^{2\cdot t_0-1}], \end{gathered} \qquad (11)$$

где $l = 0, 1, 2, \ldots, 2\cdot t_0 - 1$; $\mu = 0, 1, 2, \ldots, M - 1$; $i = 0, 1, 2, \ldots, M \cdot 2 \cdot t_0 - 1$; $j = 0, 1, 2, \ldots$; $S_{l,j,\mu,i} \in GF(q^m)$.

Следовательно:

$$S_j(x) = \sum_{\mu=0}^{M-1} S_{j,\mu}(x)\cdot x^{\mu\cdot 2\cdot t_0}, \qquad (12)$$

где $S_{j,\mu}(x)$ – многочлен синдромной последовательности, соответствующий μ-му подблоку кодового слова сверточных кодов перемежения степени не выше $2\cdot t_0 - 1$.

Таким образом, выражение (12) является многочленом $S_j(x)$ синдромной последовательности блока кодового слова сверточных кодов перемежения. Степень многочлена $S_j(x)$ не превышает значения $M\cdot 2\cdot t_0 - 1$, а его коэффициенты $S_{l,j,\mu,i}$ принадлежат полю $GF(q^m)$. На основании введения оператора задержки $x^{\mu\cdot 2\cdot t_0}$ многочлены синдромных последовательностей подблоков не перекрываются, следовательно, удается избежать распространения ошибок.

Обобщим на полубесконечный случай синдромную последовательность алгебраического сверточного кода перемежения, тогда многочлен синдромной последовательности можно представить следующим образом:

$$\begin{gathered} S(x) = \sum_{j=0}^{\infty}\left[\sum_{\mu=0}^{M-1} S_{j,\mu}(x)\cdot x^{\mu\cdot 2\cdot t_0}\right]\cdot x^{j\cdot M\cdot 2\cdot t_0} = \\ = \sum_{j=0}^{\infty} S_j(x)\cdot x^{j\cdot M\cdot 2\cdot t_0}. \end{gathered} \qquad (13)$$

Таким образом, μ-й подблок кодового слова сверточных кодов перемежения степени не выше $N-1$ по своей сути является кодовым словом блокового кода Рида-Соломона, ограниченного на подполе [4, 11]. Тогда, множество всех возможных подблоков кодовых слов алгебраического сверточного кода перемежения является подмножеством множества всех кодовых слов блокового кода Рида-Соломона, ограниченных на подполе [4, 11]. Так как для блокового кода Рида-Соломона справедлива граница Синглтона [10, 11], согласно которой минимальное кодовое расстояние $D = 2 \cdot t_0 + 1 = N - K + 1$, то минимальное расстояние d_m алгебраического сверточного кода перемежения на длине N подблока кодового слова тоже удовлетворяет данной границе. Тогда, корректирующая способность алгебраического сверточного кода перемежения на длине N подблока кодового слова составляет t_0 символов над $GF(q^m)$.

В результате перемежения символов M подблоков входящих в блок кодовых слов сверточного кода перемежения удается разбить группирующуюся ошибку на случайные ошибки. При этом, если группирующаяся ошибка имеет длину не превосходящую значение $M\cdot t_0$ и при этом на длине блока кодовых слов не произойдет ни одной случайной ошибки, то можно гарантировать исправление группирующейся ошибки длины $M\cdot t_0$.

Выводы

Алгебраическая процедура декодирования сверточных кодов перемежения предусматривает вычисление по известным $2\cdot t_0$ корням порождающего многочлена синдромной последовательности полубесконечной длины вида (13). Следовательно, алгебраическая процедура декодирования сверточных кодов перемежения имеет фиксированное число операций для декодирования одного блока кодовых слов и позволяет исправлять группирующиеся ошибки.

Введение в многочлен S(x) выражения (13) оператора задержки $x^{j\cdot M\cdot 2\cdot t_0}$ позволяет устранить эффект распространения ошибок при вычислении компонент синдрома.

Следовательно, метод декодирования алгебраических сверточных кодов перемежения предполагает вычисление полубесконечной серии не перекрывающихся синдромных последовательностей вида (13), что позволяет исправлять группирующиеся ошибки длины $M\cdot t_0$ на длине блока кодового слова сверточного кода перемежения.

Список литературы

1. Сопронюк И.И. Метод мониторинга спектра в когнитивных радиосетях на основе использования информационного критерия Акайке / И.И. Сопронюк, В.П. Лысечко, Е.А. Ухова // Системи обробки інформації. – Х.: ХУПС, 2011. – Вип. 5(95). – С. 108-112.

2. Жученко А.С. Оценка влияния перемежителей на эффективность итеративного декодирования турбокодов / А.С. Жученко // Системи обробки інформації. – Х.: ХВУ, 2004. – Вип. 8(36). – С. 157-164.

3. 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.

4. Боцул А.В. Метод декодирования алгебраических сверточных кодов перемежения / А.В. Боцул, А.С. Волков, С.И. Приходько, Н.А. Штомпель // Системи обробки інформації. – Х.: ХУ ПС, 2012. – Вып. 7(105). – С. 175-179.

5. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение / Р. Морелос-Сарагоса; [пер. с англ. В.Б. Афанасьева]. – М.: Техносфера, 2005. – 320 с.

6. Берлекэмп Э. Алгебраическая теория кодирования / Э. Берлекэмп; [пер. с англ. И.И. Грушко]; под ред. С.Д. Бермана. – М.: Мир, 1971. – 477 с.

7. Blahut R. Algebraic codes on lines, planes and curves / R. Blahut. – Cambridge: Cambrige university press, 2008. – 543 p.

8. Blahut R. Algebraic codes for data transmission / R. Blahut. – Cambridge: Cambridge university press, 2003. – 482 p.

9. Блейхут Р. Теория и практика кодов, контролирующих ошибки / Р. Блейхут; [пер. с англ. И.И. Грушко, В.М. Блиновского]; под ред. К.Ш. Зигангирова. – М.: Мир, 1986. – 576 с.

10. 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.

11. Алгебраические сверточные коды: [учебное пособие] / [Н.И. Данько, С.П. Евсеев, А.А. Кузнецов и др.]. – Х.: УкрГАЖТ, 2007. – 238 с.

Поступила в редколлегию 4.02.2013

Рецензент: д-р техн. наук, проф. В.А. Краснобаев, Полтавский национальный технический университет имени Юрия Кондратюка, Полтава.

ОСОБЛИВОСТІ МЕТОДУ ДЕКОДУВАННЯ АЛГЕБРАЇЧНИХ ЗГОРТКОВИХ КОДІВ, ЩО ПЕРЕМЕЖУЮТЬ

А.В. Боцул, С.І. Приходько, О.С. Волков, М.А. Штомпель, Хамзе Білал

Розглянуто алгебраїчний спосіб формування синдромної послідовності напівнескінченної довжини алгебраїчних згорткових кодів, що перемежують. Показано, що для виключення ефекту розповсюдження помилок при реалізації алгебраїчної процедури декодування алгебраїчних згорткових кодів, що перемежують необхідно введення операторів затримок.

Ключові слова: *завадостійке кодування, згорткові коди, синдром, декодування загорткових кодів.*

FEATURE OF THE METHOD OF DECODING ALGEBRAIC CONVOLUTIONAL CODES INTERLEAVING

A.V. Botsul, S.I. Prihodko, A.S. Volkov, N.A. Shtompel, Khamze Bilal

The algebraic method of forming a semi-infinite length syndromic sequence of algebraic convolutional codes interleaving. It is shown that to avoid the effect of the propagation of errors in the implementation of the algebraic decoding procedure algebraic convolutional codes interleaving must be entered by the operators delay.

Keywords: *error correcting coding, convolutional codes, syndrome, decoding of convolutional codes.*