ТЕЛЕКОМУНІКАЦІЙНІ СИСТЕМИ ТА УПРАВЛІННЯ НИМИ

УДК 621.391

Д-р техн. наук С.И. Приходько,
кандидати техн. наук А.С. Волков,
Н.А. Штомпель,
асп. А.В. Боцул,

МЕТОД ПОСТРОЕНИЯ АЛГЕБРАИЧЕСКИХ СВЕРТОЧНЫХ КОДОВ ПЕРЕМЕЖЕНИЯ

Постановка проблемы и анализ литературы. Сверточные коды широко применяются в современных цифровых телекоммуникационных системах для повышения достоверности передаваемой информации по различным каналам связи [1]. Эффективным методом исправления пакетов ошибок, возникающих в каналах с памятью, является использование сверточных кодов перемежения [2]. В работах [3, 4] на основе введения обобщенного порождающего многочлена предложен метод построения алгебраических сверточных кодов с заданными параметрами, исправляющих случайные ошибки. С другой стороны, в работе [5] получен модифицированный обобщенный порождающий многочлен, позволяющий алгебраически задавать параметры несистематических сверточных кодов перемежения, которые можно использовать в каналах с памятью для исправления пакетов ошибок за счет разнесения во времени искаженных кодовых символов.

В работе [3] показано, что сверточные коды алгебраически заданные порождающим многочленом кода Рида-Соломона, обеспечивают наилучшие характеристики, поэтому актуальной задачей является построение алгебраических несистематических сверточных кодов перемежения на основе модифицированных порождающих многочленов данных блоковых кодов с глубиной перемежения *M*.

Целью статьи является разработка метода построения алгебраических сверточных кодов перемежения на основе модифицированных порождающих многочленов кода Рида-Соломона.

Основная часть. Пусть код Рида-Соломона (N,K,D) над полем $GF(q^m)$ задан порождающим многочленом

$$G(x)=(x-\alpha^b)(x-\alpha^{b+1})\ldots(x-\alpha^{b+D-2}), \quad (1)$$

где $\alpha^b,\alpha^{b+1},\ldots,\alpha^{b+D-2}$ – корни многочлена $G(x)$, принадлежащие полю $GF(q^m)$;

b – целое число;

D – минимальное кодовое расстояние.

Тогда степень порождающего многочлена (1) $\deg(G(x)) = D - 1$ и данный код имеет следующие параметры: длина кодового слова $N = q^m - 1$, длина информационного слова $K = N - D + 1$, число проверочных символов $r = D - 1 = \deg(G(x))$, $D = N - K + 1$.

Следовательно, коды Рида-Соломона (N, K, D) являются кодами максимальной длины, т.е. для заданной длины кодового слова *N* и длины информационной части *K* обеспечивают максимально достижимое минимальное кодовое расстояние $D = N - K + 1$.

Группируя по строкам M кодовых слов кода Рида-Соломона (N, K, D) длины N в матрицу размерности $M \times N$, получим линейный код со следующими параметрами: длина кодового слова $N' = M \cdot N$, длина информационного слова $K' = M \cdot K$, минимальное кодовое расстояние, как и у исходного кода Рида-Соломона, $D = N - K + 1$.

Тогда код перемежения Рида-Соломона (N, K, D, M) со степенью (глубиной) перемежения M представим как набор матриц размерности $M \times N$, каждая из которых является кодовым словом данного кода следующего вида [6]:

$$C = \begin{pmatrix} C^1 \\ C^2 \\ \dots \\ C^M \end{pmatrix} = \begin{pmatrix} C_0^1 & C_1^1 & \dots & C_{N-1}^1 \\ C_0^2 & C_1^2 & \dots & C_{N-1}^2 \\ \dots & \dots & \dots & \dots \\ C_{N-1}^M & C_{N-1}^M & \dots & C_{N-1}^M \end{pmatrix}, \quad (2)$$

где C^i – $i-$е кодовое слово исходного кода Рида-Соломона (N, K, D), $i = 1,2,...,M$.

Однако эффективность данных кодов при передаче непрерывных сообщений по каналам с памятью недостаточна, поэтому рассмотрим принципы построения алгебраических сверточных кодов перемежения для снятия данного ограничения.

После проведения вычислений порождающий многочлен (1) представим следующим образом:

$$G(x) = \alpha_0 + \alpha_1 x + \dots + \alpha_{r-1} x^{r-1} + \alpha_r x^r, \quad (3)$$

где $\alpha_0, \alpha_1, \dots, \alpha_r$ – корни многочлена $G(x)$, принадлежащие полю $GF(q^m)$.

Тогда согласно работам [3, 4] несистематический сверточный код (n_0, k_0, v) над полем $GF(q)$ можно алгебраически задать обобщенным порождающим многочленом суть порождающим многочленом кода Рида-Соломона (N, K, D) вида (3), при этом полученный код будет иметь следующие параметры: длина информационного кадра $k_0 = 1$, кадр кодового слова $n_0 = m$, скорость кода $R = k_0 / n_0 = 1/m$, длина кодового ограничения $v = r \cdot k_0 = r$, информационная длина слова $k = r + 1$, кодовая длина блока $n = k \cdot m$, свободное расстояние $d_\infty \geq D$.

Далее на основе работы [5] представим порождающий многочлен (3)

кода Рида-Соломона (N,K,D) в виде модифицированного обобщенного порождающего многочлена, полностью определяющего параметры несистематического сверточного кода перемежения (n_0,k_0,v,M) над полем $GF(q)$, следующим образом:

$$G'(x)=G(x^M)=\alpha_0+\alpha_1 x^M+\alpha_2 x^{2M}+\ldots+\alpha_r x^{rM}. \quad (4)$$

Тогда согласно работе [5] ограниченный кодовый многочлен несистематического сверточного кода перемежения (n_0,k_0,v,M) над полем $GF(q^m)$ можно представить как

$$C(x)=i(x)G'(x)=\sum_{i=0}^{M-1}C_i(x)\cdot x^{iN}, \quad (5)$$

где $C_i(x)$ – $i-$й частичный кодовый многочлен, соответствующий блоку ограниченного информационного многочлена $i(x)$.

Производя вычисления в формуле (5), записывая по строкам полученные коэффициенты при формальной переменной x в виде матрицы аналогичной (2) и осуществляя отображение элементов поля $GF(q^m)$ в наборы элементов поля $GF(q)$, получим одно из ограниченных кодовых слов алгебраического несистематического сверточного кода перемежения:

$$c=\begin{pmatrix} c^{1,0},c^{1,1},\ldots,c^{1,m-1} \\ c^{2,0},c^{2,0}\ldots,c^{2,m-1} \\ \ldots \\ c^{M,0},c^{M,0}\ldots,c^{M,m-1} \end{pmatrix}=\begin{pmatrix} c_0^{1,0},\ldots,c_0^{1,m-1} & \ldots & c_{N-1}^{1,0},\ldots,c_{N-1}^{1,m-1} \\ c_0^{2,0},\ldots,c_0^{2,m-1} & \ldots & c_{N-1}^{2,0},\ldots,c_{N-1}^{2,m-1} \\ \ldots & \ldots & \ldots \\ c_{N-1}^{M,0},\ldots,c_{N-1}^{M,m-1} & \ldots & c_{N-1}^{M,0},\ldots,c_{N-1}^{M,m-1} \end{pmatrix}.$$

Выводы. Показана возможность построения алгебраических сверточных кодов перемежения на основе модифицированных порождающих многочленов кода Рида-Соломона.

Список литературы

1. Вернер, М. Основы кодирования [Текст]: учеб. для вузов / М. Вернер. – М.: Техносфера, 2004. – 288 с.

2. Питерсон, У. Коды, исправляющие ошибки [Текст] / У. Питерсон, Э. Уэлдон: пер. с англ. – М.: Мир, 1976. – 596 с.

3. Приходько, С.И. Построение сверточных кодов с использованием кодов РС [Текст] / С.И. Приходько, Г.Е. Березняков // Тематический научно-технический сборник. – 1986. – №330. – С. 103-107.

4. Приходько, С.И. Алгебраические сверточные коды [Текст] / С.И. Приходько // Информационно-управляющие системы на железнодорожном транспорте. – 1999. – № 2 (17). – С. 62-63.

5. Приходько, С.И. Метод модификации обобщенного порождающего многочлена алгебраических сверточных кодов [Текст] / С.И. Приходько, А.С. Волков, Н.А. Штомпель, А.В. Боцул // Інформаційно-керуючі системи на залізничному транспорті. – 2012. – № 6. – С. 15 – 19.

6. Wachter-Zeh, A. Decoding Interleaved Reed–Solomon Codes Beyond their Joint Error–Correcting Capability [Text] / A. Wachter-Zeh, A. Zeh, M. Bossert // Designs, Codes and Cryptography. – 24 July 2012. – P. 1-21.

Ключевые слова: сверточные коды, коды Рида-Соломона, перемежение, обобщенный порождающий многочлен.

Аннотации

Запропоновано метод побудови алгебраїчних згорткових кодів перемежування на основі модифікованих породжуючих багаточленів коду Рида-Соломона для захисту неперервних інформаційних повідомлень від пакетів помилок, що виникають у каналах з пам’яттю.

Предложен метод построения алгебраических сверточных кодов перемежения на основе модифицированных порождающих многочленов кода Рида-Соломона для защиты непрерывных информационных сообщений от пакетов ошибок, возникающих в каналах с памятью.

Proposed the method of constructing of algebraic interleaved convolutional codes on the basis of modified generator polynomials of the Reed-Solomon code to protect the continuous information messages of burst errors occurring in channels with memory.