УДК 621.391

А.С. Волков

Украинская государственная академия железнодорожного транспорта, Харьков

МЕТОД ДЕКОДИРОВАНИЯ АЛГЕБРАИЧЕСКИХ КАСКАДНЫХ СВЕРТОЧНЫХ КОДОВ

Предложен алгебраический метод декодирования каскадных сверточных кодов во временной области. Показано, что эффект распространения ошибок устраняется введением операторов задержки на внешней и внутренней ступени декодирования.

Ключевые слова: *помехоустойчивое кодирование, сверточные коды, каскадные сверточные коды, декодирование, алгебраическое декодирование.*

Введение

Постановка проблемы в общем виде и анализ литературы. В настоящее время в телекоммуникационных системах и сетях широко применяются каскадные помехоустойчивые коды с целью повышения достоверности передаваемой информации по каналам связи. Каскадный код представляет собой кодовую конструкцию, основанную на последовательном соединении нескольких компонентных помехоустойчивых кодов [1 – 5]. С практической точки зрения, наибольший интерес вызывают каскадные коды с двумя ступенями кодирования. Одну ступень кодирования называют внешней, а другую внутренней [1 – 3].

В качестве компонентных кодов внешней и внутренней ступени широкое применение нашли блоковые (РС и БЧХ – коды) и сверточные коды [1, 3, 8]. При этом, комбинируя различные компонентные коды в составе каскадного кода, удается получить новые классы кодов [1 – 3]. Следовательно, построение каскадного кода определяется выбором компонентных кодов. В то же время известно, что характеристики сверточных кодов превосходят характеристики блоковых кодов при фиксированных длинах [8].

Декодирование последовательных каскадных сверточных кодов состоит из нескольких этапов. На первом этапе реализуется декодирование компонентного сверточного кода внутренней ступени, а на втором соответственно внешней. Особенностью последовательных каскадных схем декодирования является то, что декодирование компонентных кодов практически происходит независимо друг от друга. Это дает возможность синтезировать различные методы декодирования сверточных и блоковых кодов для реализации методов декодирования каскадных кодов [1, 3, 5].

Важным преимуществом последовательных каскадных кодов (блоковых, сверточных и сверточно-блоковых) является возможность декодирования кодов большой длины при помощи отдельных компонентных сверточных или блоковых кодов [1]. Следовательно, каскадные коды имеют меньшую сложность декодирования по сравнению с одним кодом той же длины [1, 3].

Ниже предлагается решение актуальной научно-технической задачи разработки метода алгебраического декодирования алгебраических каскадных сверточных $(n^{(k)}, k^{(k)})$ – кодов во временной области.

Цель статьи – разработка алгебраического метода декодирования алгебраических каскадных сверточных $(n^{(k)}, k^{(k)})$ – кодов во временной области.

Основной материал

В основе алгебраического метода декодирования во временной области лежит идея использования корней порождающих многочленов внутренней и внешней ступени алгебраических сверточных кодов для вычисления синдромной последовательности по принятой декодером последовательности кодового слова. Затем, на основании найденного синдрома осуществляется поиск многочлена (вектора) ошибок с последующим исправлением кодового слова [6 – 8].

Рассмотрение метода декодирования алгебраических каскадных сверточных кодов начнем с внутренней ступени.Пусть $g^*(x)$ – порождающий многочлен над $GF(q^m)$ алгебраического сверточного (n_0, k_0) – кода, а $f(x) = f_0 + f_1x + f_2x^2 + ...$ – входной многочлен бесконечной длины, коэффициенты которого удовлетворяют условию: $f_i \in Q$, $i = 0, 1, 2, \ldots$; $/Q/ \geq /GF(q)/$, $Q \in GF(q^m)$ [6]. Тогда многочлен $s(x)$ кодового слова бесконечной длины алгебраического каскадного сверточного $(n^{(k)}, k^{(k)})$ – кода внутренней ступени формируется следующим образом [6, 7]:

$$s(x) = f(x) \cdot g^*(x) = s_0 + s_1x + s_2x^2 + ..., \qquad (1)$$

где $s_i \in GF(q^m)$, $i = 0, 1, 2, \ldots$.

Разобьем многочлен $f(x)$ бесконечной длины на множество многочленов $f_i(x)$ степени не более $K_0 - 1$, где $i = 0, 1, 2, \ldots$. Тогда (1) можно переписать в виде [6]:

$$s(x) = f(x) \cdot g^*(x) = \\ = \sum_{i=0}^{\infty} f_i(x) \cdot g^*(x) \cdot x^{i \cdot K_0} = \sum_{i=0}^{\infty} s_i(x) \cdot x^{i \cdot K_0}. \qquad (2)$$

Из выражения (2) видно, что каждый многочлен $s_i(x)$ является кодовым словом циклического блокового (N_0, K_0, D_0) – кода над $GF(q^m)$ ограниченного на подполе, которое определяется в соответствии с множеством Q [6, 7]. Следовательно, многочлен s(x) кодового слова бесконечной длины алгебраического каскадного сверточного $(n^{(k)}, k^{(k)})$ – кода формируется суммированием кодовых слов блокового (N_0, K_0, D_0) – кода над $GF(q^m)$ с учетом оператора задержки $x^{i\cdot K_0}$ [6, 8]. Для того, чтобы избежать перекрытия слагаемых в выражении (2) произведем замену оператора задержки $x^{i\cdot K_0}$ на $x^{i\cdot N_0}$ [6]:

$$s(x)=\sum_{i=0}^{\infty} s_i(x)\cdot x^{i\cdot N_0}\ . \tag{3}$$

Это эквивалентно подачи $(N_0 - K_0)$ нулевых символов на вход внутренней ступени кодера алгебраического каскадного сверточного $(n^{(k)}, k^{(k)})$ – кода после K_0 информационных. Таким образом, удается сформировать многочлен s(x) бесконечной длины путем суммирования кодовых слов блокового (N_0, K_0, D_0) – кода над $GF(q^m)$ без перекрытия [6].

Предположим, что недвоичный циклический блоковый (N_0, K_0, D_0) – код над $GF(q^m)$ является кодом РС, исправляющий t_0 ошибок. Тогда, корнями порождающего многочлена w(x) кода РС являются $2\cdot t_0$ последовательных степеней элемента α, при этом α – примитивный элемент поля $GF(q^m)$ [8]. Порождающий многочлен w(x) алгебраическим способом определяет порождающий многочлен g*(x) сверточного (n_0, k_0) – кода внутренней ступени [6, 7], следовательно, справедливо следующее утверждение.

Утверждение 1. Если порождающий многочлен g*(x) над $GF(q^m)$ алгебраического сверточного (n_0, k_0) – кода внутренней ступени кодирования задан через порождающий многочлен w(x) блокового (N_0, K_0, D_0) – кода РС над $GF(q^m)$, то его корнями являются 2 t_0 последовательных степеней α, где α – примитивный элемент поля $GF(q^m)$. Причем корни порождающих многочленов g*(x) и w(x) равны.

Важным следствием данного утверждения является то, что $2\cdot t_0$ корней порождающего многочлена g*(x) над $GF(q^m)$ сверточного (n_0, k_0) – кода внутренней ступени кодирования являются корнями кодового слова блокового (N_0, K_0, D_0) – кода РС и, следовательно, каждого слагаемого $s^*_i(x)$ (секции) в выражении (3).

Допустим, что на вход внутренней ступени декодера поступило кодовое слово, искаженное ошибками. Пусть многочлен ошибок бесконечной длины, имеет вид: $e(x)=e_0+e_1x+e_2x^2+\ldots$. Тогда принятый декодером многочлен кодового слова искаженный ошибками s*(x), можно представить [6, 8]:

$$s^*(x)=s(x)+e(x). \tag{4}$$

Разобьем многочлен e(x) бесконечной длины на множество многочленов $e_i(x)$ степени не более N_0. Тогда с учетом оператора задержки $x^{i\cdot N_0}$ многочлен ошибок бесконечной длины можно представить [6 – 8]:

$$e(x)=\sum_{i=0}^{\infty} e_i(x)\cdot x^{i\cdot N_0}\ , \tag{5}$$

где коэффициенты многочлена $e_i(x)$ принадлежат $GF(q^m)$, i = 0, 1, 2, ….

Слагаемые в выражении (5) не перекрываются.

Тогда с учетом выражения (3) и (5) выражение (4) можно переписать следующим образом [6 – 8]:

$$\begin{aligned} s^*(x)&=s(x)+e(x)=\sum_{i=0}^{\infty}(s_i(x)+e_i(x))\cdot x^{i\cdot N_0}= \\ &=\sum_{i=0}^{\infty} s^*_i(x)\cdot x^{i\cdot N_0} \end{aligned}\ . \tag{6}$$

Очевидно, что в выражении (6) каждый i – ый многочлен $s^*_i(x)$ является кодовым словом циклического блокового (N_0, K_0, D_0) – кода над $GF(q^m)$, искаженный многочленом ошибок $e_i(x)$ над $GF(q^m)$ [6]:

$$s^*_i(x)=s_i(x)+e_i(x). \tag{7}$$

Многочлен кодового слова бесконечной длины s*(x) искаженный многочленом ошибок e(x), формируется суммированием многочленов $s^*_i(x)$ в соответствии с оператором задержки $x^{i\cdot N_0}$, благодаря которому слагаемые в (6) не перекрываются [6, 8].

Рассмотрим процедуру обнаружения ошибок в принятом кодовом слове s*(x) и формирования синдромного многочлена z(x) бесконечной длины.

Согласно утверждению 1, корнями каждого слагаемого $s_i(x)$ в выражении (3) являются $2\cdot t_0$ корней, входящих в формирование порождающего многочлена g*(x). Следовательно, каждый i-ый многочлен $s_i(x)$ является кратным многочлену g*(x). Предположим, что α^a, α^{a+1}, …, α^{a+2t-1} – корни g*(x), тогда для всех $s_i(x)$ в выражении (3) справедливо: $s_i(\alpha^j)=0$, где $j=a,\ldots,a+2\cdot t-1$; a – целое число.

Пусть $z_1, z_2, z_3, \ldots, z_{2\cdot t_0}$ – синдромная последовательность принятого декодером многочлена $s^*_i(x)$. Компоненты синдромной последовательности определяется как значение кодового многочлена $s^*_i(x)$ в точках, являющихся корнями g*(x). Тогда согласно выражению (7) [6 – 8]:

$$z_j=s^*_i(\alpha^j)=s_i(\alpha^j)+e_i(\alpha^j)=e_i(\alpha^j)\,, \tag{8}$$

где j = 1, … , $2\cdot t_0$; i = 0, 1, 2, ….

Следовательно, если $z_j=0$ для всех j = 1, …, $2\cdot t_0$, то справедливо утверждать, что многочлен $s^*_i(x)$ был принят без искажений и $s^*_i(\alpha^j)=s_i(\alpha^j)=0$. В противном случае каждый i-ый многочлен $s^*_i(x)$ алгебраического каскадного сверточного $(n^{(k)}, k^{(k)})$ – кода на внутренней ступени содержит ошибку.

Представим i–ую синдромную последовательность многочлена $s^*_i(x)$ в виде многочлена:

$$z_i(x) = z_0 + z_1 x + ... + z_{2\cdot t-1} x^{2\cdot t-1}. \quad (9)$$

Тогда согласно выражению (9), формирование синдромного многочлена z(x) бесконечной длины алгебраического каскадного сверточного $(n^{(k)}, k^{(k)})$ – кода на внутренней ступени с учетом оператора задержки $x^{i\cdot 2\cdot t_0}$ можно представить:

$$z(x) = \sum_{i=0}^{\infty} z_i(x) \cdot x^{i\cdot 2\cdot t_0}. \quad (10)$$

Благодаря оператору задержки $x^{i\cdot 2\cdot t_0}$, введенному в выражении (10) слагаемые не перекрываются. Это позволяет предотвратить эффект распространения ошибок, который может возникнуть при вычислении синдромной последовательности бесконечной длины [6, 7].

Таким образом, задачу алгебраического декодирования кодового слова s*(x) бесконечной длины алгебраического сверточного (n_0, k_0) – кода над $GF(q^m)$ внутренней ступени можно рассматривать как задачу декодирования бесконечной последовательности неперекрывающихся кодовых слов циклического блокового (N_0, K_0, D_0) – кода над $GF(q^m)$ [6, 8].

Рассмотрим процедуру декодирования одной секции многочлена кодового слова алгебраического сверточного кода на внутренней ступени [6]. Для упрощения представим данную секцию в виде многочлена:

$$s^*_o(x) = s_0 + s_1 x + ... + s_{N_0-1} x^{N_0-1}. \quad (11)$$

Тогда многочлен ошибок $e_o(x)$ можно представить [8]:

$$e_o(x) = e_0 + e_1 x + ... + e_{N_0-1} x^{N_0-1}. \quad (12)$$

При этом количество ненулевых коэффициентов многочлена $e_o(x)$ не должно превышать корректирующей способности кода t_0. Пусть произошло w ошибок, причем $0 \le w \le t_0$. Тогда [8]:

$$e_o(x) = e_{i_1} + e_{i_2} x^{i_2} + ... + e_{i_w} x^{i_w}, \quad (13)$$

где i_l – позиция l-й ошибки; e_{i_l} – величина l-й ошибки; l = 1, … , w.

Для всех l = 1, …, w обозначим $Y_l = e_{i_l}$ – величины ошибок, а $X_l = \alpha^{i_l}$ – локаторы ошибок $\in GF(q^m)$ [8].

По известным корням g*(x) вычислим 2 t_0 компонент синдрома [3, 8]:

$$z_j = s_o^*(\alpha^j) = s_o(\alpha^j) + e_o(\alpha^j) = e_o(\alpha^j), \quad (14)$$

где j = 1, … , 2 t_0.

Далее формируется система, состоящая из 2 t_0 уравнений [8]:

$$\begin{aligned} z_1 &= Y_1 \cdot X_1 + Y_2 \cdot X_2 + ... + Y_w \cdot X_w; \\ z_2 &= Y_1 \cdot X_1^2 + Y_2 \cdot X_2^2 + ... + Y_w \cdot X_w^2; \\ z_{2\cdot t_0} &= Y_1 \cdot X_1^{2\cdot t} + Y_2 \cdot X_2^{2\cdot t} + ... + Y_w \cdot X_w^{2\cdot t_0}. \end{aligned} \quad (15)$$

Из-за нелинейности системы уравнений вида (15) непосредственное ее решение затруднительно [8]. Зафиксируем многочлен локаторов ошибок λ(x) степени не больше w [5, 8]:

$$\lambda(x) = \lambda_w x^w + ... + \lambda_1 x + 1. \quad (16)$$

Корнями многочлена λ(x) будут являться значения X^{-1}_l при l = 1, …, w, т.е. обратные к локаторам ошибок [1, 3, 5, 8]. Тогда:

$$\begin{aligned} \lambda(x) &= \prod_{l=1}^{w} (1 - x \cdot X_l) = \\ &= (1 - x \cdot X_1) \cdot (1 - x \cdot X_2) \cdot ... \cdot (1 - x \cdot X_w) \end{aligned}. \quad (17)$$

В результате умножения левой и правой части выражения (16) на $Y_l \cdot X_l^{j+w}$ и подстановки вместо x значения X^{-1}_l получим следующую систему уравнений [3, 5, 8]:

$$\begin{aligned} &\lambda_1 \cdot z_{j+w-1} + \lambda_2 \cdot z_{j+w-2} + \\ &+ ... + \lambda_w \cdot z_j = -z_{j+w} \end{aligned}, \quad (18)$$

где j = 1, …, w.

В матричной форме систему уравнений вида (18) перепишем следующим образом [8]:

$$\begin{vmatrix} z_1 & z_2 & z_3 & ... & z_w \\ z_2 & z_3 & z_4 & ... & z_{w+1} \\ z_3 & z_4 & z_5 & ... & z_{w+2} \\ ... & ... & ... & ... & ... \\ z_w & z_{w+1} & z_{w+2} & ... & z_{2w-1} \end{vmatrix} \cdot \begin{vmatrix} \lambda_w \\ \lambda_{w-1} \\ \lambda_{w-2} \\ ... \\ \lambda_1 \end{vmatrix} = \begin{vmatrix} -z_{w+1} \\ -z_{w+2} \\ -z_{w+3} \\ ... \\ -z_{2w} \end{vmatrix}. \quad (19)$$

Таким образом, удается связать компоненты синдромной последовательности одной секции многочлена $s^*_o(x)$ кодового слова алгебраического сверточного кода на внутренней ступени и коэффициенты многочлена локаторов ошибок λ(x). В результате решения системы уравнений вида (19) возможно определить коэффициенты (λ_1, λ_2, λ_3, …, λ_w) многочлена локаторов ошибок λ(x).

Для решения системы уравнений вида (19) воспользуемся итеративным алгоритмом Берлекэмпа – Месси [8]. Перепишем систему (19) таким образом:

$$z_j = -\sum_{i=1}^{w} \lambda_i \cdot z_{j-i}, \quad (20)$$

где j = w + 1, …, 2·w.

Тогда, согласно алгоритму Берлекэмпа – Месси итеративную процедуру нахождения набора коэффициентов (λ_1, λ_2, λ_3, …, λ_w) многочлена локаторов ошибок можно представить [8]:

$$z_j + \sum_{i=1}^{t} z_{j-i} \cdot \lambda_i = 0, \quad (21)$$

где j = t_0 + 1, …, 2·t_0.

Таким образом, по известным компонентам синдрома $(z_1, z_2, z_3, ..., z_{2\cdot t_0})$ из выражения (21) вычисляется набор (вектор) коэффициентов (λ_1, λ_2, λ_3, …, λ_w) минимальной длины. При этом заранее определено, что $\lambda_j = 0$, при j > t_0 [5, 8].

Далее необходимо вычислить корни многочлена локаторов ошибок $\lambda(x)$, которые будут обратными значениями к положениям ошибок [8].

Воспользуемся методом проб и ошибок, подставив поочередно все элементы поля $GF(q^m)$ в многочлен локаторов ошибок $\lambda(x)$. Такой метод называется процедурой Ченя [5, 8].

Вычисление величин ошибок Y_l выполним с использованием алгоритма Форни [8]. Введем многочлен значений ошибок $\omega(x)$, который имеет вид [8]:

$$\omega(x) = z_i(x) \cdot \lambda(x) (\mathrm{mod}\, x^{2 \cdot t}) . \qquad (22)$$

В выражении (3.22) многочлен $z_i(x)$ – синдромный многочлен одной секции $s^*_o(x)$ многочлена кодового слова алгебраического сверточного кода на внутренней ступени, подлежащей декодированию.

Пусть $\lambda'(x)$ – формальная производная по x многочлена локаторов ошибок $\lambda(x)$ имеет вид [3, 8]:

$$\lambda'(x) = \sum_{j=1}^{w} (j \cdot \lambda_j) \cdot x^{j-1} . \qquad (23)$$

Тогда величины ошибок Y_l определяется следующим выражением [3, 8]:

$$Y_l = -\frac{\omega(X_l^{-1})}{\lambda'(X_l^{-1})} \cdot X_l^{(1-a)} , \qquad (24)$$

где $l = 1, \ldots, w$; a – целое число.

Если a = 1, тогда в выражении (24) множитель $X_l^{(1-a)} = 1$, что упрощает вычисление величин ошибок Y_l.

Для нахождения истинного (переданного) многочлена $s_o(x)$ осуществляется исправление многочлена $s^*_o(x)$ путем вычитания из него найденного вектора ошибок $e_o(x)$:

$$s_o(x) = s^*_o(x) + e_o(x). \qquad (25)$$

На этом процедура декодирования одной секции $s^*_o(x)$ закончена. Таким образом, для реализации декодирования на внутренней ступени многочлена кодового слова s(x) бесконечной длины алгебраического сверточного кода необходимо последовательно декодировать все i – тые секции $s^*_i(x)$.

Далее, процедуру алгебраического декодирования кодового слова c*(x) бесконечной длины алгебраического сверточного (n_1, k_1) – кода над $GF(q^p)$ внешней ступени искаженного ошибками, можно рассматривать как процедуру декодирования бесконечной последовательности кодовых слов циклического блокового (N_1, K_1, D_1) – кода над $GF(q^p)$. Следовательно, процедуру декодирования можно реализовать согласно выражениям (11) – (25), с учетом оператора задержки $x^{i \cdot N_1}$.

Выводы

Разработан метод декодирования алгебраических каскадных сверточных кодов во временной области, позволяющий за фиксированное число операций реализовать процедуру алгебраического декодирования. При этом метод допускает декодирование с большими длинами кодового ограничения на каждой из ступени. Эффект размножения ошибок данным методом исключается благодаря введению на каждой из ступени операторов задержки $x^{i \cdot N_0}$ и $x^{i \cdot N_1}$.

Список литературы

1. Форни Д. Каскадные коды / Д. Форни; [пер. с англ. В.В. Зяблова, О.В. Попова]; под ред. С.И. Самойленко. – М.: Мир, 1970. – 207 с.

2. Forney G.D. Generalized minimum distance decoding / G.D Forney // IEEE transactions on information theory. – 1966. – IT – 12. – P. 125-131.

3. Блох Э.Л. Обобщенные каскадные коды / Э.Л. Блох, В.В. Зяблов. – М.: Связь, 1976. – 240 с.

4. Блох Э.Л. Линейные каскадные коды / Э.Л. Блох, В.В. Зяблов. – М.: Наука, 1982. – 229 с.

5. Зяблов В.В. Обобщенные каскадные помехоустойчивые конструкции на базе сверточных кодов / В.В. Зяблов, С.А. Шавгулидзе. – М.: Наука, 1991. – 207 с.

6. Приходько С.И. Метод построения алгебраических каскадных сверточных кодов / С.И. Приходько, А.С. Волков // Системи обробки інформації. – Х.: ХУПС, 2010. – Вип. 6(87). – С. 224-228.

7. Приходько С.И. Метод кодирования алгебраическим каскадным сверточным кодом на базе синтеза процедур вычисления сверток / С.И. Приходько, А.С. Волков // Системи управління, навігації та зв'язку. – Х.: ХУПС. – 2010. – Вип. 4(16). – С. 165-168.

8. 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.

Поступила в редколлегию 18.06.2013

Рецензент: канд. техн. наук, доц. А.В. Северинов, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

МЕТОД ДЕКОДУВАННЯ АЛГЕБРАЇЧНИХ КАСКАДНИХ ЗГОРТКОВИХ КОДІВ

О.С. Волков

Запропоновано алгебраїчний метод декодування каскадних згорткових кодів у часовій області. Показано, що ефект розповсюдження помилок усувається введенням операторів затримки на зовнішній та внутрішній ступені декодування.

***Ключові слова:** завадостійке кодування, згорткові коди, каскадні згорткові коди, декодування, алгебраїчне декодування.*

THE METHOD OF DECODING ALGEBRAIC CONVOLUTIONAL CODES

A.S. Volkov

We propose an algebraic method for decoding concatenated convolutional codes in the time domain. It is shown that the effect of error propagation is eliminated by introducing a delay operators on the outer and the inner decoding stage.

***Keywords:** error correcting coding, convolutional codes, concatenated convolutional codes, decoding, algebraic decoding.*