УДК 621.391

С.И. Приходько, А.С. Волков

*Украинская государственная академия железнодорожного транспорта, Харьков*

# МЕТОД ПОСТРОЕНИЯ АЛГЕБРАИЧЕСКИХ КАСКАДНЫХ СВЕРТОЧНЫХ КОДОВ

*Предложен метод построения алгебраического каскадного сверточного кода для определения сверточных кодов внешней и внутренней ступени кодирования, основанный на использовании порождающих многочленов недвоичных циклических блоковых кодов над различными конечными полями. Показано, что метод позволяет алгебраически определять каскадные сверточные коды с большой длиной кодового ограничения, с заранее заданными параметрами и согласованными скоростями кодов внешней и внутренней ступени кодирования.*

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

## Введение

**Постановка проблемы в общем виде и анализ литературы.** В современных телекоммуникационных системах и сетях наблюдается увеличение объема и скорости передаваемой информации. При этом возникает проблема обеспечения достоверности передаваемых дискретных сообщений.

Эффективным решением данной проблемы является использование помехоустойчивых кодов для исправления случайных и группирующихся ошибок, возникающих в результате передачи дискретных сообщений по каналам связи.

В последнее время широкое применение приобрели сверточные коды и кодовые конструкции на их основе. Общим недостатком существующих методов поиска сверточных кодов является то, что их построение основано на переборных методах. Такие методы достаточно эффективны при небольших длинах кодового ограничения ($v \le 10$) [5]. При значениях $v > 10$ метод малоэффективен, так как не имеет практической реализации.

Из теоремы Шеннона [1] известно, что высокой эффективностью обладают помехоустойчивые коды большой длины. Одним из перспективных способов построения длинных кодов является метод последовательного каскадирования (каскадный код), предложенный Д. Форни [1]. Метод позволяет последовательно комбинировать несколько кодов, при этом удается построить каскадный код с высокими корректирующими способностями, с большой длиной блока или длиной кодового ограничения и с относительно простыми методами декодирования.

В теории помехоустойчивого кодирования известны так называемые обобщенные каскадные коды, введенные Э.Л. Блохом и В.В. Зябловым [2, 3, 4]. Такие коды имеют более двух ступеней кодирования и являются общим классом каскадных кодов. Наибольшую значимость с точки зрения теории и практики приобрели каскадные коды с двумя ступенями кодирования [1].

При построении каскадного кода в качестве кодов внутренней и внешней ступени кодирования целесообразно выбирать сверточные коды над большими полями и большой длиной кодового ограничения, при этом внешняя и внутренняя ступень каскадного кода должны быть согласованы по скорости [1, 5, 6].

Отсутствие алгебраического метода построения каскадного кода существенно сужает спектр его применения и не позволяет задавать такой код над большими полями и с заранее заданными параметрами.

Таким образом, возникает противоречие между требованиями, предъявляемыми телекоммуникационными системами к достоверности передаваемых дискретных сообщений и возможностями существующих методов построения каскадных кодов с использованием сверточных кодов с большой длиной кодового ограничения для обеспечения требуемой достоверности.

Для разрешения данного противоречия необходимо решить научно-техническую задачу, которая заключается в разработке метода построения алгебраического каскадного сверточного кода. Метод построения алгебраического каскадного сверточного кода основан на использовании сверточных кодов на внешней и внутренней ступени кодирования, заданных алгебраическим способом через порождающие многочлены недвоичных блоковых циклических кодов.

**Цель статьи.** Разработка метода построения алгебраического каскадного сверточного кода, обеспечивающего повышение достоверности передаваемых дискретных сообщений.

## Основной материал

Пусть на внешней ступени алгебраического каскадного сверточного $(n_k, k_k)$-кода задан нерекурсивный сверточный $(n^{(1)}, k^{(1)})$-код над $GF(q^p)$ в несистематическом виде со следующими параметрами: кадр информационных символов $k_1 = \log_q |M|$, кадр кодового слова $n_1 = p$, скорость кодирования $R_1 = k_1/p$, информационная длина слова $k^{(1)} = (r + 1) k_1$ и кодовая длина слова $n^{(1)} = k^{(1)} \cdot n_1/k_1$ [7].

Общий принцип построения алгебраического каскадного сверточного кода с двумя ступенями кодирования представлен на рис. 1.

Допустим порождающий многочлен $g(x)$ сверточного $(n^{(1)}, k^{(1)})$-кода задан над полем $GF(q^p)$ (где $p$ – степень расширения примитивного поля $GF(q)$).

В полиномиальном представлении запишем:

$$g(x) = g_{r-1}x^{r-1} + g_{r-2}x^{r-2} + \ldots + g_1 x + g_0, \qquad (1)$$

где $g_i \in GF(q^p)$.

Пусть порождающий многочлен $u(x)$ степени $r$ циклического блокового $(N_1, K_1, D_1)$-кода над $GF(q^p)$ имеет вид:

$$u(x) = u_{r-1}x^{r-1} + u_{r-2}x^{r-2} + \ldots + u_1 x + u_0, \qquad (2)$$

где $u_i \in GF(q^p)$.

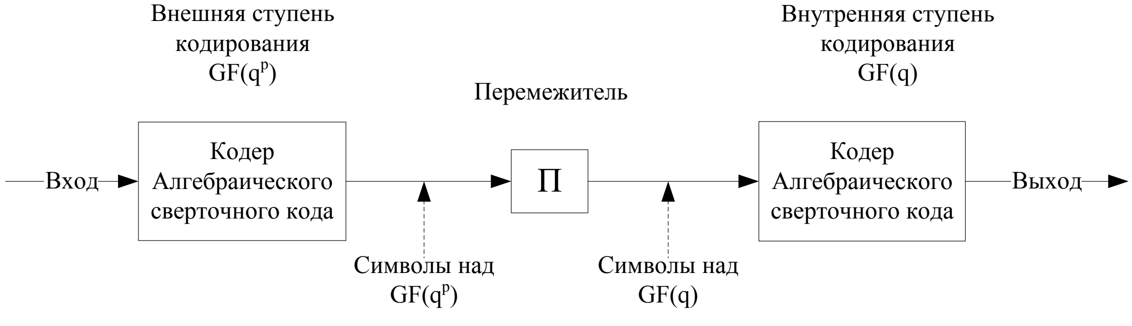


Рис. 1. Общий принцип построения алгебраического каскадного сверточного кода

Сопоставим коэффициентам $g_i$ многочлена $g(x)$ при соответствующих формальных переменных $x^i$ коэффициенты $u_i$ при соответствующих формальных переменных $x^i$ порождающего многочлена $u(x)$ циклического блокового $(N_1, K_1, D_1)$-кода над $GF(q^p)$ для всех $i = 0, \ldots, r–1$. Тогда нерекурсивный сверточный $(n^{(1)}, k^{(1)})$-код над $GF(q^p)$ в несистематическом виде на внешней ступени алгебраического каскадного сверточного $(n_k, k_k)$-кода полностью определяется порождающим многочленом $u(x)$ вида (2) циклического блокового $(N_1, K_1, D_1)$-кода над $GF(q^p)$.

Порождающий многочлен $g(x)$ определяет схему кодера на внешней ступени кодирования каскадного $(n_k, k_k)$-кода в виде регистра сдвига без обратной связи, в отводах которого стоят весовые множители над полем $GF(q^p)$. Весовые множители регистра сдвига равны коэффициентам $g_i$ порождающего многочлена $g(x)$ над $GF(q^p)$, при $i = 0, \ldots, r–1$. Длина регистра сдвига определяется степенью $\deg u(x)$ порождающего многочлена недвоичного блокового $(N_1, K_1, D_1)$-кода над $GF(q^p)$ [7].

Рассмотрим процедуру кодирования на внешней ступени каскадного $(n_k, k_k)$-кода.

Пусть на вход кодера поступает информационная последовательность над $GF(q)$ (в общем случае ее принято считать бесконечной длины). Разобьем информационную последовательность на кадры информационных символов по $k_1$ символов над $GF(q)$, при этом каждый кадр является одним элементом множества $M \in GF(q^p)$, где $p \ge k_1$, при условии, что $|M| \ge |GF(q)|$.

В полиномиальном виде информационная последовательность может быть представлена так:

$$b(x) = b_{r-1}x^{r-1} + b_{r-2}x^{r-2} + \ldots + b_1x + b_0, \qquad (3)$$

где $b_i \in M$, $i = 0, \ldots, r–1$; $\log_q |M| = k_1$.

Следовательно, кодер внешней ступени алгебраического каскадного сверточного $(n_k, k_k)$-кода реализует алгебраическое правило кодирования, представляющее собой умножение информационной последовательности $b(x)$ вида (3) на порождающий многочлен $g(x)$ алгебраического сверточного $(n^{(1)}, k^{(1)})$-кода над $GF(q^p)$. При этом формируется многочлен $c(x)$ кодового слова:

$$\begin{aligned} c(x) &= b(x)\cdot g(x) = \\ &= c_{2r-2}x^{2r-2} + c_{2r-3}x^{2r-3} + \ldots + c_1x + c_0, \end{aligned} \qquad (4)$$

где $c_i \in GF(q^p)$.

В общем случае многочлен $c(x)$ кодового слова имеет бесконечную степень, т.е. кодовое слово является бесконечно длинным. Следовательно, кодер на внешней ступени реализует обработку символов в поле $GF(q^p)$.

Рассмотрим процедуру построения внутренней ступени алгебраического каскадного сверточного $(n_k, k_k)$-кода. Предположим, что на внутренней ступени задан нерекурсивный сверточный $(n^{(0)}, k^{(0)})$-код над $GF(q)$ в несистематическом виде со следующими параметрами: $k_0 \ge 1$, $n_0 = m$, $k^{(0)} = h + 1$, $n^{(0)} = k^{(0)} \cdot m$ и скоростью кодирования $R_0 = k_0/m$.

Алгебраический сверточный код с такими параметрами отличается от алгебраического сверточного кода внешней ступени способом обработки символов и скоростью кодирования $R_0$ [7].

Зафиксируем порождающий многочлен $w(x)$ степени $h$ циклического недвоичного блокового $(N_0, K_0, D_0)$-кода над $GF(q^m)$, где $m$ – степень расширения примитивного поля $GF(q)$:

$$w(x) = w_{h-1}x^{h-1} + w_{h-2}x^{h-2} + \ldots + w_1x + w_0, \qquad (5)$$

где $w_i \in GF(q^m)$.

Тогда сверточный код внутренней ступени алгебраического каскадного сверточного кода над $GF(q)$ полностью определяется набором порождающих многочленов:

$$g_z{}^*(x) = \beta_{z,h-1}x^{h-1} + \beta_{z,h-2}x^{h-2} + \ldots + \beta_1x + \beta_0, \qquad (6)$$

где $z = 1, \ldots, m$; $\beta \in GF(q)$.

Набор порождающих многочленов вида (6) над $GF(q)$ определяется порождающим многочленом $w(x)$ циклического недвоичного блокового $(N_0, K_0, D_0)$-кода над $GF(q^m)$ вида (5), а их количество – числом $m$ [7].

Формирование коэффициентов порождающих многочленов $g_z{}^*(x)$ сверточного кода над $GF(q)$ происходит по следующему правилу.

Каждый коэффициент порождающего многочлена $w(x)$ над $GF(q^m)$ можно представить в виде вектора $W_i$ [6], содержащего $m$ компонент, являющихся элементами из поля $GF(q)$:$(\beta_{1,i}\ \beta_{2,i}\ \ldots\ \beta_{m,i})$. После такого изоморфного отображения элементов поля $GF(q^m)$ в векторы $W_i$ с $m$ компонентами над $GF(q)$ порождающий многочлен $w(x)$ можно записать в виде:

$$\begin{aligned} w^*(x) &= (\beta_{1,h-1}\beta_{2,h-1}\ldots\beta_{m,h-1})x^{h-1} + \\ &+\ldots + (\beta_{1,h-2}\beta_{2,h-2}\ldots\beta_{m,h-2})x^{h-2} + \ldots + \\ &+(\beta_{1,1}\beta_{2,1}\ldots\beta_{m,1})x + (\beta_{1,0}\beta_{2,0}\ldots\beta_{m,0}). \end{aligned} \qquad (7)$$

В качестве коэффициентов при формальной переменной $x^i$ $(i = 0, \ldots, h – 1)$ для каждого многочлена $g_z{}^*(x)$ выбирается компонента $\beta_{z,i}$. Полученные таким образом $m$ многочленов над $GF(q)$ являются порождающими многочленами алгебраического каскадного сверточного $(n_k, k_k)$-кода на внутренней ступени кодирования.

Набор порождающих многочленов $g_z{}^*(x)$ однозначно определяет схему кодера, а степень $\deg w(x)$ порождающего многочлена недвоичного блокового $(N_0, K_0, D_0)$-кода над $GF(q^m)$ определяет длину регистра сдвига сверточного кодера с обработкой символов над GF(q) на внутренней ступени кодирования алгебраического каскадного сверточного кода.

Рассмотрим процесс кодирования на внутренней ступени.

Представим каждый коэффициент $c_i$ над $GF(q^p)$ многочлена c(x) вида (4) кодового слова сверточного кода внешней ступени вектором $C_i$, состоящим из p компонент, принадлежащих полю GF(q): ($\beta_{1,i}$ $\beta_{2,i}$ … $\beta_{p,i}$). Тогда многочлен c(x) можно представить в следующем виде:

$$\begin{aligned} c^*(x) &= (\beta_{1,2r-2}\beta_{2,2r-2}\cdots\beta_{p,2r-2})x^{2r-2} + \\ &+\ldots+(\beta_{1,2r-3}\beta_{2,2r-3}\cdots\beta_{p,2r-3})x^{2r-3}+\ldots+ \\ &+(\beta_{1,1}\beta_{2,1}\cdots\beta_{p,1})x+(\beta_{1,0}\beta_{2,0}\cdots\beta_{p,0}). \end{aligned} \tag{8}$$

Входную последовательность сверточного ($n^{(0)}$, $k^{(0)}$)-кода внутренней ступени разобьем на кадры по $k_0 = \log_q |Q| \geq 1$ символов над полем GF(q), где множество $Q \in GF(q^m)$, $|Q| \geq |GF(q)|$, $m \geq k_0$. Тогда, в полиномиальном виде входную последовательность внутренней ступени представим:

$$f(x) = f_{h-1}x^{h-1} + f_{h-2}x^{h-2} + \ldots + f_1x + f_0, \tag{9}$$

где $f_i \in |Q|$, i = 0, … , h – 1.

Следовательно, сверточный кодер внутренней ступени каскадного ($n_k$, $k_k$)-кода реализует алгебраическое правило кодирования, которое представляет собой умножение входной последовательности f(x) вида (9) на набор порождающих многочленов $g^*_z(x)$ алгебраического сверточного ($n^{(0)}$, $k^{(0)}$)-кода:

$$s_z(x) = f(x)\cdot g^*_z(x), \tag{10}$$

где z = 1, … , m.

Подробнее:

$$\begin{aligned} & s_1(x) = f(x)\cdot g^*_1(x) = \\ &= s_{1,2h-2}x^{2h-2} + s_{1,2h-3}x^{2h-3}+\ldots+s_{1,1}x+s_{1,0}; \\ & s_2(x) = f(x)\cdot g^*_2(x) = \\ &= s_{2,2h-2}x^{2h-2} + s_{2,2h-3}x^{2h-3}+\ldots+s_{2,1}x+s_{2,0}; \\ & s_m(x) = f(x)\cdot g^*_m(x) = \\ &= s_{m,2h-2}x^{2h-2} + s_{m,2h-3}x^{2h-3}+\ldots+s_{m,1}x+s_{m,0}. \end{aligned} \tag{11}$$

Формирование многочлена s(x) кодового слова происходит следующим образом:

$$\begin{aligned} s(x) &= (s_{1,2h-2}s_{2,2h-2}\cdots s_{m,2h-2})x^{2h-2} + \\ &+(s_{1,2h-3}s_{2,2h-3}\cdots s_{m,2h-3})x^{2h-3}+\ldots+ \\ &+(s_{1,1}s_{2,1}\cdots s_{m,1})x+(s_{1,0}s_{2,0}\cdots s_{m,0}). \end{aligned} \tag{12}$$

Многочлен s(x) является кодовым словом алгебраического каскадного сверточного ($n_k$, $k_k$)-кода в полиномиальном виде. В общем случае степень многочлена s(x) можно представить бесконечной.

Работа алгебраического каскадного сверточного кодера заключается в следующем. Кадр информационных символов $k_1 = \log_q |M|$ подается на вход сверточного кодера внешней ступени. Учитывая r кадров хранящихся в памяти, на выходе генерируется кадр кодового слова $n_1$, где $n_1$ – один элемент поля $GF(q^p)$. Таким образом, формируется последовательность кодового слова внешней ступени длины 2r – 1, которая, в последующем, разбивается на кадры по $k_0 = \log_q |Q|$ символов и подается на вход сверточного кодера внутренней ступени. Далее, с учетом h кадров хранящихся в памяти, на выходе кодера внутренней ступени генерируется кодового слова $n_0$.

Следовательно, сформированная таким образом последовательность на длине 2h – 1 является кодовым словом кодера алгебраического каскадного сверточного ($n_k$, $k_k$)-кода со скоростями кодирования $R_1 = k_1/p$ и $R_0 = k_0/m$ на внешней и внутренней ступени кодирования соответственно.

Скорость кодирования $R_k$ алгебраического каскадного сверточного ($n_k$, $k_k$)-кода записывается в виде следующего выражения:

$$R_k = \frac{\log_q/M/\cdot\log_q/Q/}{p\cdot m} = \frac{k_1\cdot k_0}{n_1\cdot n_0} = R_1\cdot R_0. \tag{13}$$

Справедливо следующее утверждение.

Утверждение. Пусть алгебраический нерекурсивный сверточный код в несистематическом виде над $GF(q^p)$ со скоростью кодирования $R_1 = k_1/p$ с порождающим многочленом g(x) степени r – 1 на внешней ступени однозначно определен порождающим многочленом u(x) степени r – 1 недвоичного циклического блокового ($N_1$, $K_1$, $D_1$)-кода над $GF(q^p)$. Алгебраический нерекурсивный сверточный код в несистематическом виде над GF(q) со скоростью кодирования $R_0 = k_0/m$ и с набором из z порождающих многочленов $g^*_z(x)$ степени не выше h – 1 на внутренней ступени задан через порождающий многочлен w(x) степени h – 1 недвоичного циклического блокового ($N_0$, $K_0$, $D_0$)-кода над $GF(q^m)$. Тогда можно построить алгебраический каскадный сверточный ($n_k$, $k_k$)-код с использованием алгебраических нерекурсивных сверточных кодов со следующими параметрами:

$$\begin{cases} k_k = k_1\cdot k_0, \\ n_k = p\cdot m, \\ v_k \leq r\cdot k_1 + h\cdot k_0, \\ R_k = R_1\cdot R_0. \end{cases} \tag{14}$$

Параметр $k_k$ – кадр информационных символов ($k_k = \log_q |M|$); $n_k$ – кадр кодового слова; $v_k$ – длина кодового ограничения.

Важной особенностью алгебраического метода построения каскадного сверточного кода является выбор множества Q.

Пусть множество Q удовлетворяет следующим условиям:

$$|GF(q)| \leq |Q| = |GF(q^p)| \leq |GF(q^m)|. \tag{15}$$

Следовательно?

$$k_0 = \log_q |Q| = p, \quad m > k_0. \tag{16}$$



227

Таким образом, каждый кадр информационных символов $k_0$ кода внутренней ступени принадлежит полю $GF(q^p)$, что соответствует одному элементу $Q_i$ множества Q, принадлежащего полю $GF(q^m)$. Число символов над GF(q) в каждом кадре равно $k_0 = p$. Это существенно облегчает согласование по скорости кодеров внешней и внутренней ступени.

Возможны случаи, когда множество Q выбирается из соотношения:

$$\left|GF(q)\right| \le \left|Q\right| \le \left|GF(q^m)\right| \le \left|GF(q^p)\right|. \quad (17)$$

Тогда для согласованной по скорости работы кодеров внешней и внутренней ступени необходимо выполнение следующих условий:

$$k_0 = \log_q \left|Q\right|, \; Q \in GF(q^m), \; m > k_0, \quad (18)$$

где $k_0$ – делит число p либо $(2r - 1) \cdot p$ без остатка, а именно: $p = k_0 \cdot \varepsilon$, либо $(2r - 1) \cdot p = k_0 \cdot \varepsilon$, $\varepsilon$ – натуральное число.

Такое соотношение символов между кадрами кодового слова сверточного кода внешней ступени и кадрами, поступающими на вход сверточного кодера внутренней ступени, обеспечивает согласование по скорости. В противном случае работа двух кодеров будет проходить некорректно и с задержками по времени, при этом усложняется алгоритм декодирования каскадного $(n_k, k_k)$-кода, так как необходимо введение дополнительных нулей во входную последовательность кодера сверточного кода на внутренней ступени кодирования.

## Выводы

Научно обоснована проблема построения каскадных кодов с большой длиной кодового ограничения с использованием недвоичных сверточных кодов на внешней и внутренней ступени кодирования, найденных переборным методом.

Показано, что разработанный метод позволяет алгебраическим способом определять каскадные коды с большой длиной кодового ограничения и высокими корректирующими способностями.

Метод позволяет алгебраически задавать каскадные сверточные коды с заранее заданными параметрами и согласованными скоростями кодирования внешней и внутренней ступени кодирования.

Использование математического аппарата недвоичных циклических блоковых кодов, конечных полей и полиномиальной алгебры облегчает построение каскадных сверточных кодов на этапе их разработки.

Метод построения алгебраического каскадного сверточного кода отличается от известных использованием порождающих многочленов недвоичных циклических блоковых кодов над различными конечными полями для определения сверточных кодов внешней и внутренней ступени кодирования.

## Список литературы


1. *Форни Д. Каскадные коды: п е р. с англ. / Д. Форни. – М.: Мир, 1970. – 207 с.*
2. *Блох Э.Л. Обобщенные каскадные коды / Э.Л. Блох, В.В. Зяблов. – М.: Связь, 1976. – 240 с.*
3. *Блох Э.Л. Линейные каскадные коды / Э.Л. Блох, В.В. Зяблов. – М.: Наука, 1982. – 229 с.*
4. *Зябов В.В. Обобщенные каскадные помехоустойчивые конструкции на базе сверточных кодов / В.В. Зябов, С.А. Шавгулидзе. – М.: Наука, 1991. – 207 с.*
5. *Блейхут Р. Теория и практика кодов, контролирующих ошибки: пер. с англ. / Р. Блейхут. – М.: Мир, 1986. – 576 с.*
6. *Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение / Р. Морелос-Сарагоса. – М.: Техносфера, 2005. – 320 с.*
7. *Алгебраические сверточные коды / Н.И. Данько, С.П. Евсеев, А.А. Кузнецов и др. – Х.: УкрГАЖТ, 2007. – 238 с.*


*Поступила в редколлегию 23.09.2010*

**Рецензент:** д-р техн. наук, проф. А.А. Кузнецов, Харьковский университет Воздушных Сил имени Ивана Кожедуба, Харьков.

### МЕТОД ПОБУДОВИ АЛГЕБРАЇЧНИХ КАСКАДНИХ ЗГОРТКОВИХ КОДІВ

С.І. Приходько, О.С. Волков

*Запропоновано метод побудови алгебраїчного каскадного згорткового коду, заснований на використанні багаточленів, що породжують, недвійкових циклічних блокових кодів над різними кінцевими полями для визначення згорткових кодів зовнішнього й внутрішнього ступеню кодування. Показано, що метод дозволяє алгебраїчно визначати каскадні згорткові коди з великою довжиною кодового обмеження, із заздалегідь заданими параметрами і узгодженими швидкостями кодів зовнішнього й внутрішнього ступеню кодування.*

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

### METHOD FOR CONSTRUCTING ALGEBRAIC CONCATENATED CONVOLUTIONAL CODES

S.I. Prihodko, A.S. Volkov

*There has been suggested a method of constructing algebraic concatenated convolutional code based on the use of generating polynomials non-binary cyclic block codes over various finite fields to determine the convolutional codes of external and internal level coding. It is shown that the method allows to determine concatenated convolutional codes with large lengths to with code limits with preset parameters and agreed codes of rates of external and internal level coding.*

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