УДК 621.391

И.Е. Кужель

Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков

АЛГЕБРАИЧЕСКОЕ ПОСТРОЕНИЕ СВЕРТОЧНЫХ КОДОВ

Рассматриваются алгебраические сверточные коды, построенные через обобщение недвоичных групповых блоковых кодов на случай полубесконечной длины кодового слова. Предлагается новый способ их описания через ненулевые компоненты спектральных составляющих. Предлагаемый способ позволяет эффективно скрывать правило сверточного кодирования при построении кодовых шифросистем. Приводятся примеры построения алгебраических сверточных кодов с использованием нового способа их описания.

Ключевые слова: *сверточные коды, правило кодирования, порождающая матрица, порождающий многочлен, ненулевые компоненты спектральных составляющих.*

Введение

Постановка проблемы в общем виде и анализ литературы. Для защиты обрабатываемых и передаваемых данных от случайно возникающих ошибок применяют методы помехоустойчивого кодирования [1 – 5]. Наиболее эффективными по обнаруживающей и исправляющей способности являются сверточные коды, принадлежащие к подклассу линейных непрерывных кодовых конструкций и обеспечивающих наибольший энергетический выигрыш от кодирования [1 – 3]. Сложным вопросом их практического использования являются вычислительно затратные методы синтеза, основанные на переборном поиске соответствующих кодовых конструкций с последовательной оценкой их характеристик.

Новым научным направлением в развитии теории кодирования являются алгебраические методы построения и абстрактного описания сверточных кодов через обобщение недвоичных групповых блоковых кодов на случай полубесконечной длины кодового слова. Последние работы в этой области показывают, что алгебраический подход к построению сверточных кодов позволяет без существенного снижения энергетического выигрыша от кодирования строить регулярные алгоритмы их синтеза, а также использовать алгебраические методы кодирования и декодирования [3 – 5].

Важной нерешенной научной задачей является исследование методов описания алгебраических сверточных кодов с большим числом правил кодирования, разработка и теоретическое обоснование кодовых шифросистем на их основе. С одной стороны, применение кодовых шифросистем позволит обеспечить требуемые показатели помехоустойчивости передачи данных, с другой – обеспечить информационную скрытность передаваемых сообщений.

Целью данной статьи является исследование методов построения алгебраических сверточных кодов, разработка нового способа их описания через ненулевые компоненты спектральных составляющих. Предлагаемый способ позволяет эффективно скрывать правило сверточного кодирования при построении кодовых шифросистем.

Основной материал

Алгебраические сверточные коды. Построение сверточных кодов традиционно связывают с описанием правила кодирования в виде умножения информационного слова (многочлена) на проверочную матрицу (множество многочленов) [1 – 3].

Если сверточный (n, k, d_∞) код над GF(q) задан порождающими многочленами $P_1(x)$, $P_2(x)$, …, $P_m(x)$ степени < r и коэффициентами из GF(q) :

$$\begin{aligned} P_1(x) &= p_{1,r-1}x^{r-1} + p_{1,r-2}x^{r-2} + ... + p_{1,1}x + p_{1,0}, \\ P_2(x) &= p_{2,r-1}x^{r-1} + p_{2,r-2}x^{r-2} + ... + p_{2,1}x + p_{2,0}, \\ &\dots \\ P_m(x) &= p_{m,r-1}x^{r-1} + p_{m,r-2}x^{r-2} + ... + p_{m,1}x + p_{m,0}, \end{aligned} \quad (1)$$

тогда правило кодирования состоит в последовательном умножении информационного многочлена $I(x) = i_{r-1}x^{r-1} + i_{r-1}x^{r-1} + ... + i_1x + i_0$ с коэффициентами из GF(q) на все $P_i(x)$, i = 1, 2, …, m и последовательном считывании коэффициентов при одинаковых степенях полученных результатов.

Эквивалентным способом описания сверточных кодов является представление правила кодирования в виде умножения информационной последовательности (коэффициентов многочлена $I(x)$) на порождающую матрицу

$$G = \begin{pmatrix} G_0 & G_1 & G_2 & ... & G_{r-1} & 0 & 0 & 0 & 0 & ... \\ 0 & G_0 & G_1 & ... & G_{r-2} & G_{r-1} & 0 & 0 & 0 & ... \\ 0 & 0 & G_0 & ... & G_{r-3} & G_{r-2} & G_{r-1} & 0 & 0 & ... \\ ... & ... & ... & ... & ... & ... & ... & ... & ... & ... \\ 0 & 0 & 0 & ... & G_0 & G_1 & G_2 & ... & ... & ... \\ ... & ... & ... & ... & ... & ... & ... & ... & ... & ... \end{pmatrix}, \quad (2)$$

где $G_i = (p_{1,i}\ p_{2,i}\ \dots\ p_{m,i})$ – матрица строка, длины m символов.

Матрица G бесконечно продолжается вниз и влево. За исключением диагональной полосы из r ненулевых подматриц G_i, все ее подматрицы нулевые.

Очевидно, что подматрица

$$G = \begin{pmatrix} G_0 & G_1 & G_2 & \dots & G_{r-1} & 0 & \dots & 0 \\ 0 & G_0 & G_1 & \dots & G_{r-2} & G_{r-1} & \dots & 0 \\ 0 & 0 & G_0 & \dots & G_{r-3} & G_{r-2} & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & G_0 & G_1 & \dots & G_{r-1} \end{pmatrix} \quad (3)$$

является порождающей матрицей некоторого алгебраического группового блокового (N, K, D) кода над $GF(q^m)$ с порождающим многочленом

$$G(x) = G_{r-1}x^{r-1} + G_{r-2}x^{r-2} + \dots + G_1 x + G_0,$$

$$\forall i : G_i \in GF(q^m). \quad (4)$$

Тогда правило кодирования сверточного (n, k, d_∞) кода над GF(q) состоит в умножении информационного многочлена

$$I(x) = i_{r-1}x^{r-1} + i_{r-1}x^{r-1} + \dots + i_1 x + i_0$$

с коэффициентами из GF(q) на многочлен (4) с коэффициентами из $GF(q^m)$ и последовательном считывании коэффициентов результата умножения с отображением на подполе $GF(q) \subset GF(q^m)$. Очевидно, что справедлива оценка $d_\infty \geq D$.

Построение алгебраических сверточных кодов над GF(q) состоит в выборе порождающего многочлена $G(x)$ алгебраического блокового (N, K, D) кода над $GF(q^m)$ и в формировании на его основе полубесконечной порождающей матрицы и/или, что эквивалентно, множества порождающих многочленов сверточного кода. Кодовые соотношения синтезированного таким образом алгебраического сверточного (n, k, d_∞) кода над GF(q) непосредственно связаны с кодовыми параметрами исходного алгебраического блокового (N, K, D) кода над $GF(q^m)$:

$$n = k \cdot n^0 / k^0;\ k = (r+1) \cdot k^0;\ n^0 = m,\ m > k^0 \geq 1;$$

$$d_\infty \geq D;\ \nu = r \cdot k^0;\ R = k^0 / m,$$

где ν – длина кодового ограничения; R – скорость кода.

В качестве примера рассмотрим алгебраический блоковый $(7, 5, 3)$ код Рида-Соломона, заданный порождающим многочленом

$$g(x) = (x - \alpha^1)(x - \alpha^2) = x^2 + \alpha^4 x + \alpha^3$$

над $GF(2^3)$.

Соответствующая порождающая матрица $(7, 5, 3)$ кода Рида-Соломона имеет вид

$$G = \begin{vmatrix} \alpha^3 & \alpha^4 & \alpha^0 & 0 & 0 & 0 & 0 \\ 0 & \alpha^3 & \alpha^4 & \alpha^0 & 0 & 0 & 0 \\ 0 & 0 & \alpha^3 & \alpha^4 & \alpha^0 & 0 & 0 \\ 0 & 0 & 0 & \alpha^3 & \alpha^4 & \alpha^0 & 0 \\ 0 & 0 & 0 & 0 & \alpha^3 & \alpha^4 & \alpha^0 \end{vmatrix}.$$

Используя соответствие

$$G_0 = \alpha^3 = (p_{1,0}\ p_{2,0}\ ,\ p_{3,0}) = \{110\};$$

$$G_1 = \alpha^4 = (p_{1,1}\ p_{2,1}\ ,\ p_{3,1}) = \{011\};$$

$$G_2 = \alpha^0 = (p_{1,2}\ p_{2,2}\ ,\ p_{3,2}) = \{100\},$$

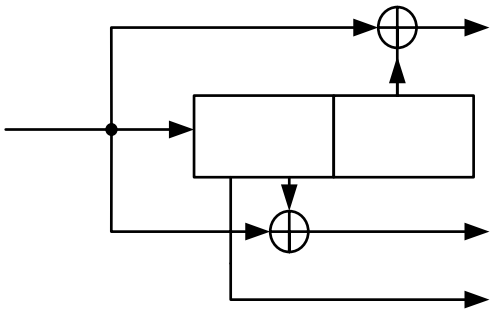
получим множество порождающих многочленов

$$P_1(x) = x^2 + 1, \quad P_2(x) = x + 1, \quad P_3(x) = x$$

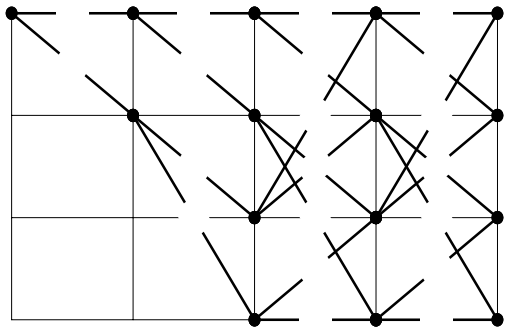
и соответствующую полубесконечную порождающую матрицу

$$G = \begin{vmatrix} G_0 & G_1 & G_2 & 0 & 0 & \dots & 0 & 0 & 0 & \dots \\ 0 & G_1 & G_1 & G_1 & 0 & \dots & 0 & 0 & 0 & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & \dots & G_0 & G_1 & G_2 & 0 & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \end{vmatrix}$$

двоичного алгебраического сверточного $(9, 3, \geq 3)$ кода (реальная величина $d_\infty = 5$). На рис. 1 представлены: а) структурная схема соответствующего кодера; б) его кодовая решетка.



а



б

Рис. 1. Структурная схема кодера двоичного алгебраического сверточного $(9, 3, 5)$ кода и его кодовая решетка

Таким образом, рассмотренный алгебраический подход является эффективным способом построения сверточных кодов с хорошими кодовыми характеристиками. Кроме того он обеспечивает применимость быстрых алгоритмов декодирования.

В тоже время, как показывает анализ выражений (1) – (4) приведенное описание алгебраических сверточных кодов не всегда применимо, особенно в случае построения кодовых криптосистем [6, 7]. Так, для однозначного восстановления правила сверточного кодирования достаточно вычислить коэффициенты в выражении (4), т.е. найти все $G_i \in GF(q^m)$. Для построения кодовых криптосистем необходимо эффективно скрывать правило кодирования и, при возможности, использовать эффективные методы его маскирования.

В данной работе предлагается новый способ описания алгебраических сверточных кодов через ненулевые компоненты спектральных составляющих.

Предлагаемый способ описания алгебраических сверточных кодов. В основе предлагаемого способа описания алгебраических сверточных кодов лежит представление групповых кодов через ненулевые компоненты спектров их кодовых слов.

Определим дискретное преобразование Фурье над конечным полем следующим образом [1].

Пусть $c = (c_0, c_1, \ldots, c_{n-1})$ последовательность n элементов поля $GF(q)$ (где n делит $q^m - 1$ для некоторого m) и пусть $\alpha \in GF(q^m)$ элемент порядка n.

Преобразованием Фурье над конечным полем вектора c будет последовательность $C = (C_0, C_1, \ldots, C_{n-1})$ элементов поля $GF(q^m)$, задаваемых равенством

$$C_j = \sum_{i=0}^{n-1} \alpha^{ij} c_i, \quad j = 0,1,\ldots,n-1.$$

Дискретный индекс i принято называть временем, а c – *временной функцией* или *сигналом*. Аналогично индекс j можно назвать *частотой*, а C – *частотной функцией* или *спектром*.

В качестве длины преобразования Фурье можно выбрать произвольный делитель числа $q^m - 1$, но наиболее важную роль в теории кодирования играют примитивные длины $n = q^m - 1$. В последнем случае α является примитивным элементом поля $GF(q^m)$.

В отличие от поля комплексных чисел в поле Галуа преобразование Фурье существует не для любой длины n, так как не для любого n в поле существует элемент этого порядка. Если m – наименьшее целое, такое, что делит $q^m - 1$, то над полем $GF(q)$ существует преобразование Фурье длины n и компоненты этого преобразования лежат в поле $GF(q^m)$.

Эти два вектора образуют пару, связанную между собой следующим образом [1]:

$$C_j = \sum_{i=0}^{n-1} \alpha^{ij} c_i; \quad (5) \qquad c_i = \frac{1}{n \bmod p} \sum_{j=0}^{n-1} \alpha^{-ij} C_j. \quad (6)$$

Каждое слово группового блокового (n,k,d) кода задается многочленом $c(x)$ степени n или, что эквивалентно, некоторой последовательностью $c = (c_0, c_1, \ldots, c_{n-1})$. Выполнение преобразования Фурье над конечным полем (5) всех векторов (кодовых слов) c дает множество соответствующих векторов (спектров кодовых слов) $C = (C_0, C_1, \ldots, C_{n-1})$. Нулевые компоненты спектральных составляющих векторов $C = (C_0, C_1, \ldots, C_{n-1})$ соответствуют корням кодовых многочленов $c(x)$. Поскольку для всех кодовых многочленов справедливо равенство $c(x) = i(x)g(x)$, где $g(x)$ – порождающий многочлен группового кода, имеем равенство нулю тех спектральных составляющих для всех векторов $C = (C_0, C_1, \ldots, C_{n-1})$, которые соответствуют корням многочлена $g(x)$. Другими словами, групповой (n,k,d) код, заданный своим порождающим многочленом $g(x)$, однозначно задается корнями этого многочлена или, что эквивалентно, совпадающими для всех кодовых слов группового кода нулевыми компонентами спектров его кодовых слов, связанными с временной областью преобразованиями (5), (6).

Обозначим через $\{X_0, X_1, \ldots, X_{n-k-1}\}$ корни многочлена $g(x)$, соответствующие нулевым компонентам спектров кодовых слов группового кода. Тогда для произвольного кодового многочлена $c(x)$, вычисленного в произвольном корне X_i, $i = 0,1,\ldots,n-k-1$ всегда будет выполняться равенство:

$$c(X_i) = c_0 + c_1 X_i + c_2 X_i^1 + \ldots + c_{n-1} X_i^{n-1} = 0.$$

Используя соответствующие равенства для всех $i = 0,1,\ldots,n-k-1$, в матричном виде получим следующее соотношение для произвольного кодового слова $c = (c_0, c_1, \ldots, c_{n-1})$:

$$(c_0, c_1, \ldots, c_{n-1}) \begin{pmatrix} X_0^0 & X_0^1 & X_0^2 & \ldots & X_0^{n-1} \\ X_1^0 & X_1^1 & X_1^2 & \ldots & X_1^{n-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ X_{n-k-1}^0 & X_{n-k-1}^1 & X_{n-k-1}^2 & \ldots & X_{n-k-1}^{n-1} \end{pmatrix}^T = 0.$$

Полученное соотношение означает, что прямоугольная матрица в левой части равенства задает базис линейного пространства – ортогонального дополнения к рассматриваемому линейному групповому коду. Другими словами, мы получили проверочную матрицу кода, выраженную через корни порождающего многочлена – нулевые компоненты спектров кодовых слов группового кода:

$$GH^T = 0;$$

$$H = \begin{pmatrix} X_0^0 & X_0^1 & X_0^2 & \dots & X_0^{n-1} \\ X_1^0 & X_1^1 & X_1^2 & \dots & X_1^{n-1} \\ \dots & \dots & \dots & \dots & \dots \\ X_{n-k-1}^0 & X_{n-k-1}^1 & X_{n-k-1}^2 & \dots & X_{n-k-1}^{n-1} \end{pmatrix}.$$

Предположим, что корни $\{X_0, X_1, \dots, X_{n-k-1}\}$ многочлена $g(x)$ выражены через соответствующие степени примитивного элемента α^i конечного поля. По определению, в качестве корней многочлена $g(x)$ группового кода должны выступать не менее $2t$ подряд следующих элемента поля, где t - исправляющая способность кода [1-3]. Тогда, после подстановки $X_i^j = \alpha^{ij}$ имеем следующее равенство (для любого фиксированного значения i):

$$H = \begin{pmatrix} \alpha^{0i} & \alpha^{1i} & \alpha^{2i} & \dots & \alpha^{(n-1)i} \\ \alpha^{0(i+1)} & \alpha^{1(i+1)} & \alpha^{2(i+1)} & \dots & \alpha^{(n-1)(i+1)} \\ \dots & \dots & \dots & \dots & \dots \\ \alpha^{0(i+n-k-1)} & \alpha^{1(i+n-k-1)} & \alpha^{2(i+n-k-1)} & \dots & \alpha^{(n-1)(i+n-k-1)} \end{pmatrix} =$$

$$= \begin{pmatrix} X_0^i & X_1^i & X_2^i & \dots & X_{n-1}^i \\ X_0^{i+1} & X_1^{i+1} & X_2^{i+1} & \dots & X_{n-1}^{i+1} \\ \dots & \dots & \dots & \dots & \dots \\ X_0^{i+n-k-1} & X_1^{i+n-k-1} & X_2^{i+n-k-1} & \dots & X_{n-1}^{i+n-k-1} \end{pmatrix}.$$

Проведя аналогичные рассуждения, получим, что порождающая матрица группового кода выражается через корни проверочного многочлена, т.е. через ненулевые компоненты спектральных составляющих:

$$G = \begin{pmatrix} X_0^j & X_1^j & X_2^j & \dots & X_{n-1}^j \\ X_0^{j+1} & X_1^{j+1} & X_2^{j+1} & \dots & X_{n-1}^{j+1} \\ \dots & \dots & \dots & \dots & \dots \\ X_0^{j+k-1} & X_1^{j+k-1} & X_2^{j+k-1} & \dots & X_{n-1}^{j+k-1} \end{pmatrix}, \quad (7)$$

где множества индексов $\{i, i+1, \dots, i+n-k-1\}$ и $\{j, j+1, \dots, j+k-1\}$, вычисленные по модулю $n-1$, не пересекаются, т.е. множество элементов $\{X^i, X^{i+1}, \dots, X^{i+n-k-1}, X^j, X^{j+1}, \dots, X^{j+k-1}\}$ образует полное множество ненулевых элементов конечного поля.

Для описания алгебраических сверточных кодов через ненулевые компоненты спектральных составляющих воспользуемся выражениями (2) и (3). По аналогии с симметричностью полубесконечной матрицы (2) и ее повторяющейся подматрицы (3) используя выражение (7) представим полубесконечную порождающую матрицу алгебраического сверточного кода следующим образом:

$$G = \begin{pmatrix} X_0^j & X_1^j & X_2^j & \dots & X_{n-1}^j & 0 & 0 & \dots \\ X_0^{j+1} & X_1^{j+1} & X_2^{j+1} & \dots & X_{n-1}^{j+1} & X_0^{j+1} & 0 & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ X_0^{j+k-1} & X_1^{j+k-1} & X_2^{j+k-1} & \dots & X_{n-1}^{j+k-1} & X_0^{j+k-1} & X_1^{j+k-1} & \dots \\ 0 & X_1^j & X_2^j & \dots & X_{n-1}^j & X_0^j & X_1^j & \dots \\ 0 & 0 & X_2^{j+1} & \dots & X_{n-1}^{j+1} & X_0^{j+1} & X_1^{j+1} & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \end{pmatrix}. \quad (8)$$

Для однозначного восстановления правила сверточного кодирования в приведенном алгебраическом описании достаточно вычислить все элементы подматрицы (8) – матрицу (7). Умножение матрицы (7) на маскирующие невырожденные матрицы не изменяет свойств кода, соответствующая модификация полубесконечной матрицы (8) позволит эффективно скрыть правило быстрого декодирования.

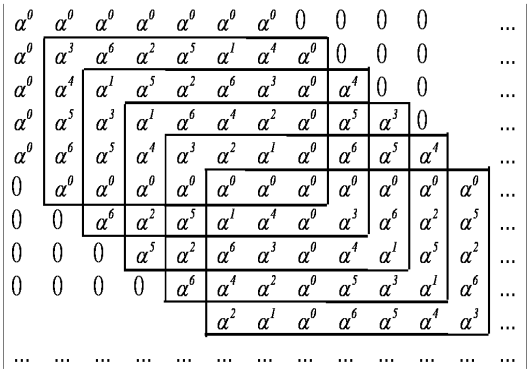
Другими словами, приведенное описание алгебраических сверточных кодов через ненулевые компоненты спектральных составляющих может быть эффективно использовано для построения кодовых криптосистем.

В качестве примера рассмотрим алгебраический блоковый $(7,5,3)$ код Рида-Соломона над $GF(2^3)$ и построенный на его основе алгебраический сверточный код (приведенный выше). Нулевые компоненты спектра кодовых слов $(7,5,3)$ кода Рида-Соломона соответствуют корням порождающего многочлена $g(x) = (x-\alpha^1)(x-\alpha^2) = x^2 + \alpha^4 x + \alpha^3$. Следовательно, ненулевые компоненты спектра кодовых слов соответствуют всем остальным элементам конечного поля $GF(2^3)$: $\{\alpha^0, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$. Используя выражение (7) получим:

$$G = \begin{pmatrix} \alpha^0 & \alpha^0 & \alpha^0 & \alpha^0 & \alpha^0 & \alpha^0 & \alpha^0 \\ \alpha^0 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha^1 & \alpha^4 \\ \alpha^0 & \alpha^4 & \alpha^1 & \alpha^5 & \alpha^2 & \alpha^6 & \alpha^3 \\ \alpha^0 & \alpha^5 & \alpha^3 & \alpha^1 & \alpha^6 & \alpha^4 & \alpha^2 \\ \alpha^0 & \alpha^6 & \alpha^5 & \alpha^4 & \alpha^3 & \alpha^2 & \alpha^1 \end{pmatrix},$$

что после подстановки в (8) дает следующую полубесконечную матрицу

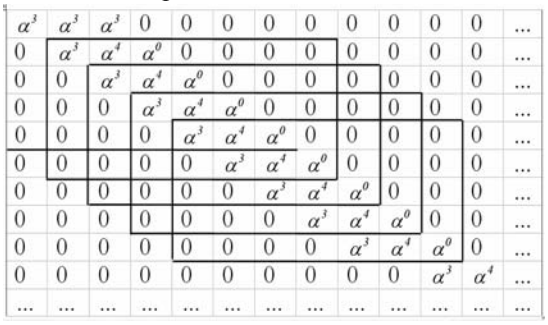
G =



Выделенными линиями здесь отмечена циклически повторяющаяся подматрица, подчеркивающая групповые свойства алгебраического сверточного кода.

Для традиционного описания сверточного кода порождающая матрица имеет вид:

G =



Очевидно, что использование для описания сверточного кода ненулевых компонентов его спектральных составляющих не изменяет групповые свойства кода.

Изменяется лишь правило кодирования, т.е. изменяется соответствие множества информационных слов и множества кодовых слов, сами множества не изменяются, равно как и дистанционные свойства кода.

Выводы

Использование дискретного преобразования Фурье в конечных полях позволяет формировать новые правила кодирования алгебраических сверточных кодов. В ходе исследования предложен новый способ описания алгебраических сверточных кодов через ненулевые компоненты спектральных составляющих. Предложенный способ позволяет эффективно скрывать правило сверточного кодирования при построении кодовых шифросистем.

Перспективным направлением дальнейших исследований является разработка кодовых шифросистем на алгебраических сверточных кодах с использованием аналитических соотношений в спектральной области.

Список литературы

1. *Блейхут Р. Теория и практика кодов, контролирующих ошибки: пер. с англ. / Р. Блейхут. – М.: Мир, 1986. – 576 с.*
2. *Краснобаев В.А. Помехоустойчивое кодирование в АСУ / В.А. Краснобаев, С.И. Приходько, А.Г. Снисаренко. – Х.: ХВВКИУРВ, 1990 – 155 с.*
3. *Алгебраические сверточные коды / Н.И. Данько, С.П. Евсеев, А.А. Кузнецов, П.Ф. Поляков, С.И. Приходько. – Х.: УкрГАЖТ, 2007. – 238 с.*
4. *Алгебраическое построение несистематических сверточных кодов / С.И. Приходько, А.А. Кузнецов, С.А. Гусев, И.Е. Кужель // Системи обробки інформації: зб. наук. пр. – Х.: ХВУ, 2004. – Вип. 8 (36). – С. 170-175.*
5. *Алгебраический метод сверточного кодирования / С.И. Приходько, А.А. Кузнецов, С.А. Гусев, И.Е. Кужель // Комп'ютерні системи та інформаційні технології. – Х.: ХАИ, 2005. – № 1 – С. 35-43.*
6. *Кужель И.Е. Исследование свойств поточных симметричных криптосистем на основе сверточных кодов / И.Е. Кужель // Системи обробки інформації: зб. наук. пр. – Х.: ХВУ, 2004. – Вип. 10. – С. 94-97.*
7. *Поточные криптосистемы на алгебраических сверточных кодах / С.И. Приходько, А.А. Кузнецов, И.Е. Кужель, С.А. Гусев // Східно-Європейський журнал передових технологій. – Х.: Технолоічний центр, 2004. – № 6 (12). – С. 168-174.*

Поступила в редколлегию 19.04.2010

Рецензент: д-р техн. наук, проф. Ю.В. Стасев, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

ПОБУДОВА АЛГЕБРИ ЗГОРТАЛЬНИХ КОДІВ

І.Є. Кужель

Розглядаються згортальні коди алгебри, побудовані через узагальнення недвійкових групових блокових кодів на випадок напівнескінченної довжини кодового слова. Пропонується новий спосіб їх опису через ненульові компоненти спектральних складових. Пропонований спосіб дозволяє ефективно приховувати правило згортального кодування при побудові кодових шифросистем. Наводяться приклади побудови згортальних кодів алгебри з використанням нового способу їх опису.

Ключові слова: *згортальні коди, правило кодування, породжуюча матриця, породжуючий багаточлен, ненульові компоненти спектральних складових.*

ALGEBRAIC CONSTRUCTION OF CONVOLUTIONAL CODES

I.E. Kuzhel'

Algebraic convolutional codes, built through generalization of unbinary codes of blocks of groups in case of semiendless code word capacity, are examined. The new method of their description is offered through unzero components of spectral constituents. The offered method allows effectively to hide the rule of the convolutional encoding at the construction of code-system of codes. Examples of construction of algebraic convolutional codes are made with the use of new method of their description.

Keywords: *convolutional codes, rule of encoding, originative matrix, originative a polynomial, unzero components of spectral constituents.*