УДК 621.391

МНОГОМЕРНЫЕ СПЕКТРЫ ДЛЯ ОПИСАНИЯ КАСКАДНЫХ КОДОВ В ЧАСТОТНОЙ ОБЛАСТИ

А.А. КУЗНЕЦОВ, С.И. ПРИХОДЬКО, БИЛАЛ ХАМЗЕ

Рассматривается математический аппарат многомерного дискретного преобразования Фурье в конечных полях. Исследуются методы описания линейных блоковых кодов в частотной области. Показано, что, в отличие от итеративных кодов (кодов-произведений) каскадные коды в общем случае не могут быть описаны в частотной области в терминах многомерных спектров. Получены аналитические выражения, устанавливающие взаимно-однозначное функциональное соответствие спектра последовательности над конечным полем и спектров соответствующих слов, полученных ограничением этого слова на подполе. Получено общее решение задачи представления каскадных кодов в частотной области, что позволит, используя выведенные аналитические зависимости компонентов многомерных спектров, строить в частотной области вычислительно эффективные алгоритмы кодирования и декодирования.

Ключевые слова: многомерное дискретное преобразование Фурье, каскадные коды, конечные поля.

1. ПОСТАНОВКА ПРОБЛЕМЫ В ОБЩЕМ ВИДЕ И АНАЛИЗ ЛИТЕРАТУРЫ

Математический аппарат дискретного преобразования Фурье в полях Галуа используется в современной теории помехоустойчивого кодирования как для описания в частотной области наиболее важных в прикладном отношении блоковых кодов, так и для построения новых кодовых конструкций с улучшенными свойствами [1–4]. За счет применения алгоритмов быстрого преобразования Фурье удается существенно сократить вычислительную сложность алгоритмов кодирования и декодирования, а также реализовать некоторые вычислительные процессы параллельно [4, 5].

Преобразования Фурье в конечных полях могут быть обобщены и на многомерный случай. Если кодовые слова блоковых кодов представимы в виде кодовых многочленов от нескольких переменных, а соответствующие кодовые символы записываются некоторой многомерной матрицей, тогда математический аппарат многомерных спектров, как правило, позволяет задавать коды в многомерной частотной области. К кодам, допускающим такое описание, относятся простейшие итеративные коды (коды-произведения), для которых перенос вычислений в многомерную частотную область позволяет повысить вычислительную эффективность алгоритмов кодирования-декодирования и выполнить многие операции параллельно [2, 3]. В то же время кодовые соотношения итеративных кодов далеки от оптимальных, что и объясняет их малое практическое использование [1–3].

Наибольшее распространение в технике помехоустойчивого кодирования получили т.н. каскадные коды, в конструкции которых используются два кода – код внутренней (первой) ступени над конечным полем $GF(q)$ и код внешней (второй) ступени над расширенным полем $GF(q^m)$ [1–3]. Полученный блоковый код определен над полем $GF(q)$, однако при формировании кодовых слов и их декодировании выполняются преобразования как над полем $GF(q)$, так и над его расширением $GF(q^m)$. Кодовые слова каскадного кода также представляют в виде матрицы, однако математический аппарат многомерных спектров к каскадным кодам не применим. Невозможно использовать и быстрые многомерные преобразования Фурье, т.е. получить тот эффект, который дают в технике помехоустойчивого кодирования преобразования в частотной области. Разрешению этого противоречия и посвящена данная работа.

Таким образом, *целью статьи* является развитие математического аппарата многомерных спектров для представления каскадных кодовых конструкций в частотной области и реализации на их основе эффективных алгоритмов кодирования и декодирования.

Работа структурирована следующим образом. В п. 2 приводятся основные положения и аналитические соотношения для дискретного преобразования Фурье в конечных полях, показана их связь с полиномиальным описанием блоковых кодов. В п. 3 преобразования Фурье обобщены на многомерный случай. На примере итеративного кода дается описание многомерных кодов в частотной области. Показано, что для каскадных кодов соответствующее представление получить не удается. П. 4 посвящен решению этой задачи. Через введение взаимно-однозначного функционального соответствия спектров кодовых слов произвольного вектора над конечным полем и спектров его слов-ограничений на произвольное подполе удается получить аналитические выражения, которые дополняют математический аппарат многомерных спектров, что позволяет дать описание каскадных кодов в частотной области. В п. 5 полученные результаты обобщаются, обсуждается их прикладное значение для реализации вычислительно эффективных алгоритмов кодирования и декодирования каскадными кодами. Все

сформулированные утверждения по тексту работы дополняются примерами, которые наглядно демонстрируют справедливость приведенных рассуждений и упрощают их восприятие.

2. ДИСКРЕТНОЕ ПРЕОБРАЗОВАНИЕ ФУРЬЕ В КОНЕЧНЫХ ПОЛЯХ

Преобразование Фурье играет важнейшую роль в развитии современных методов теории обработки и передачи информации. В частности, для обработки и исследования сигналов, непрерывных во времени и принимающих вещественные и комплексные значения, используют интегральное преобразование Фурье [6, 7]. Для цифровой обработки сигналов, дискретных во времени используют дискретное преобразование Фурье [3–7]:

$$X_k = \sum_{j=0}^{n-1} e^{\frac{-2\pi i}{n} jk} x_j, k = 0,...,n-1, \quad (1)$$

$$x_j = \frac{1}{n}\sum_{k=0}^{n-1} e^{\frac{2\pi i}{n} jk} X_k, j = 0,...,n-1, \quad (2)$$

где n — количество значений сигнала и компонент разложения (спектра); $x = \{x_j, j = 0,...,n-1\}$ — значения сигнала в дискретных временных точках с номерами $j = 0,...,n-1$; $X = \{X_k, k = 0,...,n-1\}$ — n комплексных амплитуд синусоидальных сигналов, слагающих исходный сигнал; k —индекс частоты.

Для многих длин последовательностей определено также преобразование Фурье в полях Галуа, которое представляет собой развитый аналитический аппарат, используемый для описания блоковых кодов в частотной области, исследования их корректирующих свойств, построения вычислительно эффективных алгоритмов кодирования и декодирования [3].

Ядром дискретного преобразования Фурье в (1) и (2) является комплексный корень n-й степени из единицы $e^{\frac{-2\pi i}{n}}$. Проводя аналогию с конечным полем, в котором элемент α порядка n является корнем n-й степени из единицы, в работе [3] введено следующее определение дискретного преобразования Фурье над полями Галуа.

Пусть $v = \{v_i, i = 0,...,n-1\}$ — вектор над $GF(q)$, где n делит $q^m - 1$ при некотором m и пусть α — элемент порядка n в поле $GF(q^m)$. Преобразование Фурье в поле Галуа вектора v определяется как вектор $c = \{c_j, j = 0,...,n-1\}$ над $GF(q^m)$, задаваемый равенствами [3]:

$$c_j = \sum_{i=0}^{n-1} \alpha^{ij} v_i, j = 0,...,n-1. \quad (3)$$

Дискретный индекс i в (1) принято назвать временем, а v — временной функцией или сигналом. Соответствующий индекс j принято назвать частотой, а c — частотной функцией или спектром [3].

Порядок элемента $\alpha \in GF(q^m)$ в (3) обязан быть делителем $q^m - 1$, следовательно, в отличие от поля комплексных чисел, в конечном поле преобразование Фурье определено не для любой длины, а только для соответствующих делителей $q^m - 1$. Наиболее важную в прикладном отношении роль играет выбор в качестве $\alpha \in GF(q^m)$ примитивного элемента с максимальным порядком $n = q^m - 1$. В общем случае в качестве длины n может быть выбран произвольный делитель $q^m - 1$ для некоторого положительного целого m и элемента $\alpha \in GF(q^m)$ порядка n в качестве ядра преобразования. Спектр в этом случае будет определен над расширением $GF(q^m)$, хотя и будет содержать лишь элементы порядка n из этого поля.

Таким образом, над полем $GF(q)$ вектор v и его спектр c связаны соотношениями [3]:

$$c_j = \sum_{i=0}^{n-1} \alpha^{ij} v_i, \quad (4)$$

$$v_i = \frac{1}{n}\sum_{j=0}^{n-1} \alpha^{-ij} c_j, \quad (5)$$

где n интерпретируется как элемент поля $GF(q)$, $n \mid (q^m - 1)$, а $c_j \in GF(q^m)$.

Так как сигнал v определен над полем $GF(q)$, а его спектр A определен над расширением $GF(q^m)$, не все векторы над $GF(q^m)$ могут быть спектрами каких либо сигналов над $GF(q)$. Обратное преобразование Фурье сигнала c над $GF(q^m)$ является вектором v с компонентами из $GF(q)$ тогда и только тогда, когда выполняются следующие равенства (ограничения сопряженности):

$$c_j^q = c_{qj \bmod n}, j = 0,...,n-1. \quad (6)$$

Действительно, согласно малой теореме Ферма,

$$c_j^q = \left(\sum_{i=0}^{n-1} \alpha^{ij} v_i\right)^q = \sum_{i=0}^{n-1} \alpha^{i(qj)} v_i = c_{qj \bmod n}, j = 0,...,n-1.$$

Разобьем числа $0,...,n-1$ по $\bmod n$ на подмножества [3]:

$$A_j = \{j, jq, ..., jq^{m_j - 1}\}, \quad (7)$$

где m_j — наименьшее положительное целое, удовлетворяющее равенству $jq^{m_j - 1} = j \bmod n$, в силу конечности поля такое m_j всегда существует.

Множество A_j выделяет в спектре такое множество частот, называемых хордой, что если сигнал принимает значения в поле $GF(q)$, то значение спектра в одной из частот хорды определяет значения спектра при всех частотах этой хорды [3]. Другими словами, для того, чтобы задать сигнал через обратное преобразование Фурье (5) достаточно определить все хорды (7) с учетом ограничений (6). Выбор хорды A_j соответствует определению такого минимального многочлена

$f_{\alpha^j}(x)$, корнями которого являются все элементы α^{jq^s}, $s = 0,...,m_j - 1$:

$$f_{\alpha^j}(x) = \prod_{s=0}^{m_j-1} (x - \alpha^{jq^s}). \quad (8)$$

Рассмотренные преобразования широко используются в теории помехоустойчивого кодирования для описания кодов в частотной области и для исследования их свойств. Например, наиболее важные в прикладном отношении полиномиальные коды задаются в частотной области через определенные нулевые компоненты спектра их кодовых слов.

Если элементы вектора v заданы в виде коэффициентов многочлена $v(x)$:

$$v(x) = v_0 + v_1 x + ... + v_{n-1} x^{n-1},$$

тогда с помощью преобразования Фурье в поле Галуа он может быть преобразован в многочлен

$$c(x) = c_0 + c_1 x + ... + c_{n-1} x^{n-1},$$

который называется спектральным многочленом или ассоциированным с многочленом $v(x)$ [3].

Свойства спектра тесно связаны с корнями многочленов [3]:

– элемент α^j является корнем многочлена $v(x)$ тогда и только тогда, когда j-я частотная компонента c_j равна нулю.

– элемент α^{-i} является корнем многочлена $c(x)$ тогда и только тогда, когда i-я временная компонента v_i равна нулю.

Действительно, вычисление значения многочлена $v(x)$ в точке α^j дает:

$$v(\alpha^j) = v_0 + v_1\alpha^j + ... + v_{n-1}\alpha^{jn-1} = \sum_{i=0}^{n-1} \alpha^{ij} v_i = c_j,$$

т.е. равенство нулю частотной компоненты c_j означает, что соответствующий элемент α^j — корень многочлена $v(x)$.

Отсюда следует, что полиномиальные коды, задаваемые порождающими и/или проверочными многочленами, определяются в частотной области нулевыми частотными компонентами, непосредственно связанными с корнями этих многочленов. В частности, если код Боуза-Чоудхури-Хоквингема (БЧХ) над $GF(q)$ задан своим порождающим $g(x)$ и/или проверочным $h(x)$ многочленами, т.е. если с учетом (6) – (8):

$$g(x) = \quad . \quad . \quad . \left(\prod_j f_{\alpha^j}(x) \right) = \prod_j (x - \alpha^j),$$

$$h(x) = \quad . \quad . \quad . \left(\prod_{i \neq j} f_{\alpha^i}(x) \right) = \prod_{i \neq j} (x - \alpha^i),$$

тогда спектры всех кодовых слов такого кода обязательно содержат нули в компонентах c_j и могут быть не нулевыми в компонентах c_i.

Это наглядно продемонстрировано на рис. 1, на котором схематично отмечены нулевые компоненты спектра – корни порождающего многочлена $g(x)$ и ненулевые элементы – корни проверочного многочлена $h(x)$.

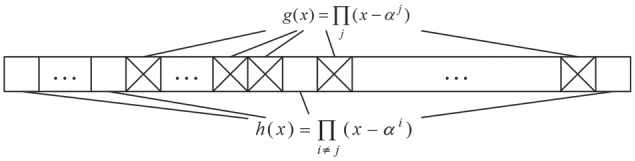


Рис. 1. Структура кодовых слов полиномиальных кодов в спектральной области

Преобразование Фурье для функций, заданных над вещественным пространством, обобщается в виде т.н. многомерных спектров [3]. Соответствующие многомерные обобщения преобразования Фурье могут быть также введены и на дискретных последовательностях из многомерных пространств над конечными полями.

3. МНОГОМЕРНЫЕ СПЕКТРЫ И ИХ ПРИМЕНЕНИЕ В ТЕОРИИ КОДИРОВАНИЯ

Пусть длины $n_1, n_2, ..., n_p$ одновременно являются делителями порядка мультипликативной группы конечного поля $GF(q^m)$ для некоторого положительного целого m, т.е.

$$n_1 \big| (q^m - 1) \wedge n_2 \big| (q^m - 1) \wedge ... \wedge n_p \big| (q^m - 1).$$

Тогда произвольный p-мерный сигнал

$$v = \{v_{i_1,i_2,...,i_p}, i_1 = 0,...,n_1 - 1, i_2 = 0,..., n_2 - 1,..., i_p = 0,..., n_p - 1\}$$

и его p-мерный спектр

$$c = \{c_{j_1,j_2,...,j_p}, j_1 = 0,...,n_1 - 1, j_2 = 0,..., n_2 - 1,..., j_p = 0,..., n_p - 1\}$$

связаны соответствующими преобразованиями:

$$c_{j_1,j_2,...,j_p} = \sum_{i_1=0}^{n_1-1} \sum_{i_2=0}^{n_2-1} ... \sum_{i_p=0}^{n_p-1} \alpha_1^{i_1 j_1} \alpha_2^{i_2 j_2} ... \alpha_p^{i_p j_p} v_{i_1,i_2,...,i_p}, \quad (8)$$

$$v_{i_1,i_2,...,i_p} = \frac{1}{n_1}\frac{1}{n_2}...\frac{1}{n_p} \times \times \sum_{j_1=0}^{n_1-1} \sum_{j_2=0}^{n_2-1} ... \sum_{j_p=0}^{n_p-1} \alpha_1^{-i_1 j_1} \alpha_2^{-i_2 j_2} ... \alpha_p^{-i_p j_p} c_{j_1,j_2,...,j_p}, \quad (9)$$

где α_1, α_2, ..., α_p – элементы конечного поля $GF(q^m)$ порядка n_1, n_2, ..., n_p, соответственно.

По аналогии с ограничениями сопряженности одномерных спектров (6) введем соответствующие условия для многомерного случая:

$$c^q_{j_1,j_2,...,j_p} = c_{q_{j_1} \bmod n, qj_2 \bmod n, ..., qj_p \bmod n}, \quad i_1 = 0,...,n_1 - 1, i_2 = 0,...,n_2 - 1,..., i_p = 0,...,n_p - 1, \quad (10)$$

справедливость которых легко проверяется

$$c^q_{j_1,j_2,\ldots,j_p} = \left(\sum_{i_1=0}^{n_1-1} \sum_{i_2=0}^{n_2-1} \ldots \sum_{i_p=0}^{n_p-1} \alpha_1^{i_1 j_1} \alpha_2^{i_2 j_2} \ldots \alpha_p^{i_p j_p} v_{i_1,i_2,\ldots,i_p} \right)^q =$$

$$= \sum_{i_1=0}^{n_1-1} \sum_{i_2=0}^{n_2-1} \ldots \sum_{i_p=0}^{n_p-1} \alpha_1^{i_1 (qj_1)} \alpha_2^{i_2 (qj_2)} \ldots \alpha_p^{i_p (qj_p)} v_{i_1,i_2,\ldots,i_p} =$$

$$= c_{qj_1 \bmod n,\, qj_2 \bmod n,\, \ldots,\, qj_p \bmod n},$$

$$i_1 = 0,\ldots,n_1-1, i_2 = 0,\ldots,n_2-1,\ldots,i_p = 0,\ldots,n_p-1.$$

Разобьем кортежи чисел

$$i_1 = 0,\ldots,n_1-1, i_2 = 0,\ldots,n_2-1,\ldots,i_p = 0,\ldots,n_p-1$$

на подмножества:

$$A_{j_1,j_2,\ldots,j_p} = \begin{Bmatrix} \{j_1, j_1 q, \ldots, j_1 q^{m_{j_1}-1}\}, \{j_2, j_2 q, \ldots, j_2 q^{m_{j_2}-1}\}, \\ \ldots, \{j_p, j_p q, \ldots, j_p q^{m_{j_p}-1}\} \end{Bmatrix}, \quad (11)$$

где m_{j_s} — наименьшее положительное целое, удовлетворяющее равенству $j_s q^{m_{j_s}} = j_s \bmod n_s$, в силу конечности поля такое m_{j_s} всегда существует.

Множество $A_{j_1,j_2,\ldots,j_p}$ выделяет в многомерном спектре многомерную хорду, причем, если временной сигнал принимает значения в поле $GF(q)$, то значение спектра в одной из частот хорды определяет значения спектра при всех частотах этой хорды [3]. Таким образом, сигнал может быть задан через обратное многомерное преобразование Фурье (9), если определить хорды (11) с учетом ограничений (10).

Многомерные спектры используются в теории помехоустойчивого кодирования для описания т.н. итеративных кодов (или кодов-произведений) в частотной области. Рассмотрим, без потери общности, наиболее простой, двумерный случай.

Информационные символы $I = \{I_1, I_2, \ldots, I_k\}$, подлежащие кодированию двумерным итеративным (n,k,d) кодом над $GF(q)$, разобьем на k_2 подблоков, содержащих по k_1 символов в каждом, т.е. $k = k_1 k_2$. Запишем их в виде матрицы размером $k_1 \times k_2$, у которой каждый столбец является подблоком из k_1 символов. Каждая строка полученной матрицы кодируется линейным блоковым (n_2,k_2,d_2) кодом над $GF(q)$, называемым кодом второй (внешней) ступени. Результат кодирования дает матрицу, содержащую n_2 столбцов по k_1 символов в каждом.

Каждый из n_2 столбцов полученной матрицы кодируется линейным блоковым (n_1,k_1,d_1) кодом над $GF(q)$, называемым кодом первой (внутренней) ступени. В результате выполнения последней операции получаем матрицу размером $n_1 \times n_2$ символов из $GF(q)$, у которой каждый столбец есть кодовое слово кода первой ступени, а каждая строка – кодовое слово кода второй ступени (для последних $r_1 = n_1 - k_1$ строк это является следствием линейности кодов первой и второй ступеней). Полученная матрица является кодовым словом итеративного кода с параметрами: $n = n_1 n_2$, $k = k_1 k_2$, $d = d_1 d_2$.

Для исследования спектральных свойств итеративного кода в работе [3] использован математический аппарат многомерных спектров. Кодовое слово $v = \{v_{i_1,i_2}, i_1 = 0,\ldots,n_1-1, i_2 = 0,\ldots,n_2-1\}$ двумерного кода-произведения можно записать в виде многочлена от двух переменных:

$$v(x,y) = \sum_{i_1=0}^{n_1-1} \sum_{i_2=0}^{n_2-1} v_{i_1,i_2} x^{i_1} y^{i_2}, \quad (12)$$

где v_{i_1,i_2} — символы из $GF(q)$ (компоненты сигнала).

Используя (8) и (9) для $p = 2$ по заданному сигналу — двумерной матрице v во временной области можно вычислить все компоненты спектра $A = \{A_{j_1,j_2}, j_1 = 0,\ldots,n_1-1, j_2 = 0,\ldots,n_2-1\}$ и наоборот. Таким образом, с многочленом (12) можно ассоциировать его спектральный многочлен

$$c(x,y) = \sum_{j_1=0}^{n_1-1} \sum_{j_2=0}^{n_2-1} c_{j_1,j_2} x^{j_1} y^{j_2}, \quad (13)$$

где c_{j_1,j_2} — символы из $GF(q^m)$ являются компонентами спектра.

Представление кодовых слов итеративного кода в виде многочлена (12) и ассоциированного с ним спектрального многочлена (13) особенно полезно при использовании на первом и втором каскаде полиномиальных кодов, в первую очередь, кодов БЧХ. Корни порождающих многочленов таких кодов соответствуют нулевым значениям спектральных компонент, что для двумерного случая может быть схематично представлено в виде рис. 2.

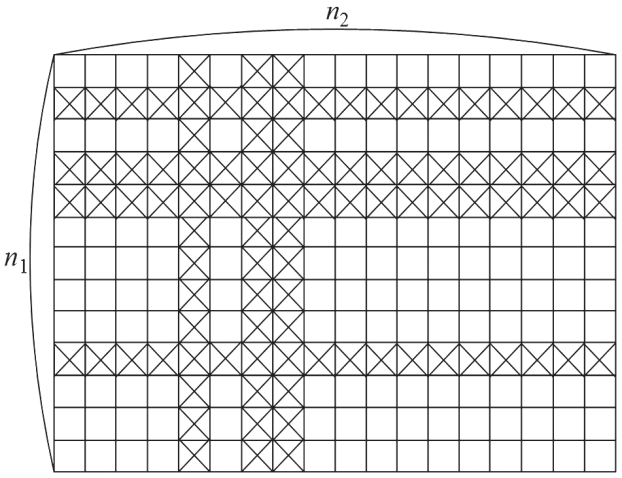


Рис. 2. Структура кодовых слов двумерного кода-произведения в частотной области (по аналогии с рис. 1)

Определение итеративного кода (многомерного кода-произведения) в частотной области позволяет использовать развитый аппарат быстрого преобразования Фурье для снижения вычислительной сложности алгоритмов кодирования и декодирования, а также выполнять некоторые вычислительные процессы параллельно [3]. Например, для рассмотренного выше двумерного случая вычисление $n_2 - k_2$ последних слов

кода первой ступени во временной области может быть реализовано только после вычисления всех слов кода второй ступени. Используя многомерные преобразования Фурье, вычисление каждого кодового символа v_{i_1,i_2} может быть организовано параллельно и независимо друг от друга посредством вычисления обратного преобразования по формуле (9) с $p=2$.

Следует однако отметить, что кодовые соотношения итеративных кодов далеки от оптимальных и при фиксированных (n,k,d) параметрах они, как правило, проигрывают другим известным конструкциям, например, каскадным кодам.

Рассмотрим каскадный (Nn,Kk,Dd) код над $GF(q)$, образованный из (N,K,D) кода над $GF(q^m)$ на внешней ступени каскада и $(n,k=m,d)$ кода над $GF(q)$ на внутренней ступени каскада.

Схематично структуру кодового слова каскадного кода представим на рис. 3 в виде матрицы из n строк и N столбцов, в ячейках которой записаны кодовые символы, принадлежащие полю $GF(q)$.

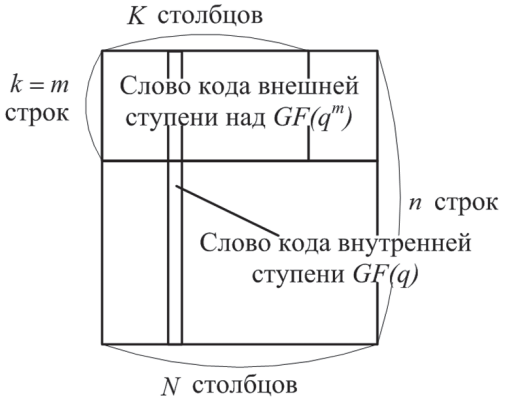


Рис. 3. Структура кодового слова каскадного кода

Левая верхняя область, состоящая из $k=m$ строк и K столбцов, соответствует информационным символам из $GF(q)$. Каждый столбец в этой области, состоящий из m символов из $GF(q)$ представляется как один символ из $GF(q^m)$:

$$V_i \Rightarrow \begin{pmatrix} v_{0,i} \\ v_{1,i} \\ \dots \\ v_{m-1,i} \end{pmatrix},\ i=0,\dots,K-1, \qquad (14)$$

т.е. для полиномиального представления элементов поля имеем:

$$V_i(z)=v_{0,i}+v_{1,i}z+\dots+v_{m-1,i}z^{m-1},\ V_i(z)\in GF(q^m).$$

Все K столбцов, таким образом, представляются как K символов из $GF(q^m)$, которые обрабатываются как информационная последовательность

$$I=(V_0,\ V_1,\dots,\ V_{K-1})$$

(N,K,D) кода внешней ступени. Кодовое слово такого кода представляется в виде последовательности

$$V=(V_0,\ V_1,\dots,\ V_{K-1},\ V_K,\ V_{K+1},\dots,\ V_N), \qquad (15)$$

где проверочные символы V_K, V_{K+1}, ..., V_N формируются в процессе кодирования (N,K,D) кодом внешней ступени и записываются в матрицу в виде соответствующих векторов-столбцов в верхней правой области (см. рис. 3).

Таким образом, первые m строк в матричном представлении кодового слова каскадного кода соответствуют N символам из $GF(q^m)$ кодового слова кода внешней ступени. Каждый такой символ, представленный вектором из m символов

$$I_i=(v_{0,i},\ v_{1,i},\dots,\ v_{m-1,i}),\ i=0,\dots,N-1$$

обрабатывается как i-я информационная последовательность кода внутренней ступени. Соответствующее кодовое слово представляется в виде последовательности

$$v_i=(v_{0,i},\ v_{1,i},\dots,\ v_{m-1,i},\ v_{m,i},\ v_{m+1,i},\dots,\ v_{n-1,i}), \qquad (16)$$

где проверочные символы $v_{m,i}$, $v_{m+1,i}$,..., $v_{n-1,i}$ формируются в процессе кодирования $(n,k=m,d)$ кодом внутренней ступени и записываются по столбцам матрицы (см. рис. 3).

Таким образом, кодовое слово (сигнал) каскадного кода представляется в виде следующего массива символов из $GF(q)$:

$$v=\begin{pmatrix} v_{0,0} & v_{0,1} & \dots & v_{0,K-1} & v_{0,K} & v_{0,K+1} & \dots & v_{0,N-1} \\ v_{1,0} & v_{1,1} & \dots & v_{1,K-1} & v_{1,K} & v_{1,K+1} & \dots & v_{1,N-1} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ v_{m-1,0} & v_{m-1,1} & \dots & v_{m-1,K-1} & v_{m-1,K} & v_{m-1,K+1} & \dots & v_{m-1,N-1} \\ v_{m,0} & v_{m,1} & \dots & v_{m,K-1} & v_{m,K} & v_{m,K+1} & \dots & v_{m,N-1} \\ v_{m+1,0} & v_{m+1,1} & \dots & v_{m+1,K-1} & v_{m+1,K} & v_{m+1,K+1} & \dots & v_{m+1,N-1} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ v_{n-1,0} & v_{n-1,1} & \dots & v_{n-1,K-1} & v_{n-1,K} & v_{n-1,K+1} & \dots & v_{n-1,N-1} \end{pmatrix}. \qquad (17)$$

Очевидно, что выполняя двумерное преобразование Фурье матрицы (17) по выражению (9) с $p=2$, получим соответствующий двумерный спектр

$$c=\begin{pmatrix} c_{0,0} & c_{0,1} & \dots & c_{0,K-1} & c_{0,K} & c_{0,K+1} & \dots & c_{0,N-1} \\ c_{1,0} & c_{1,1} & \dots & c_{1,K-1} & c_{1,K} & c_{1,K+1} & \dots & c_{1,N-1} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ c_{m-1,0} & c_{m-1,1} & \dots & c_{m-1,K-1} & c_{m-1,K} & c_{m-1,K+1} & \dots & c_{m-1,N-1} \\ c_{m,0} & c_{m,1} & \dots & c_{m,K-1} & c_{m,K} & c_{m,K+1} & \dots & c_{m,N-1} \\ c_{m+1,0} & c_{m+1,1} & \dots & c_{m+1,K-1} & c_{m+1,K} & c_{m+1,K+1} & \dots & c_{m+1,N-1} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ c_{n-1,0} & c_{n-1,1} & \dots & c_{n-1,K-1} & c_{n-1,K} & c_{n-1,K+1} & \dots & c_{n-1,N-1} \end{pmatrix}, \qquad (18)$$

который, хотя и будет взаимно-однозначно соответствовать временному сигналу (17) над $GF(q)$,

однако не будет соответствовать слову (15) с символами из $GF(q^m)$.

Другими словами, вычисленный спектр (18) будет соответствовать такому временному сигналу (17), который является кодовым словом некоторого итеративного кода, в котором код второй ступени образован посредством ограничения слова (15) с символами из $GF(q^m)$ на подполе $GF(q)$. Под ограничением здесь и далее понимается формирование слов

$$\begin{gathered} v_0 = (v_{0,0}, v_{0,1}, v_{0,2}, ..., v_{0,N-1}), \\ v_1 = (v_{1,0}, v_{1,1}, v_{1,2}, ..., v_{1,N-1}), \\ ... \\ v_{m-1} = (v_{m-1,0}, v_{m-1,1}, v_{m-1,2}, ..., v_{m-1,N-1}), \end{gathered} \quad (19)$$

из слова (15) с помощью правила (14).

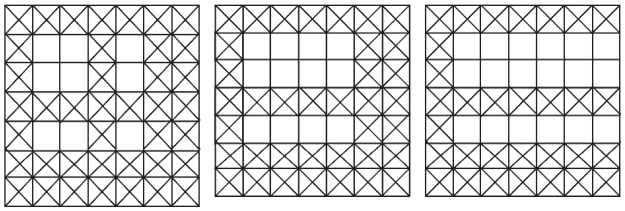
Практически это означает, что прямое двумерное преобразование Фурье матрицы (17) будет давать такие сигналы-матрицы (18), которые *не будут* соответствовать словам каскадного (Nn, Kk, Dd) кода над $GF(q)$.

Для наглядности приведенных выше рассуждений рассмотрим пример.

Пример 1. Вначале рассмотрим итеративный двоичный (49,9,16) код, образованный произведением двух двоичных (7,3,4) кодов БЧХ с порождающим многочленом

$$g(x) = f_{\alpha^0}(x) f_{\alpha^3}(x) =$$
$$= (x-\alpha^0)(x-\alpha^3)(x-\alpha^5)(x-\alpha^6) = 1 + x + x^2 + x^4.$$

Двумерный спектр кодовых слов заданного таким образом итеративного кода схематично представим на рис. 4, *а*.



а *б* *в*

Рис. 4. Структура кодовых слов двумерного кода-произведения в частотной области

Как видно на рис. 4, *а* в двумерном спектре всего имеется девять не обязательно нулевых спектральных компонент. Используя выражение (11) для этих компонент, сформируем три двумерных множества

$$A_{1,1} = \{\{1,2,4\},\{1,2,4\}\};\ A_{1,2} = \{\{1,2,4\},\{2,4,1\}\};$$
$$A_{1,4} = \{\{1,2,4\},\{4,1,2\}\},$$

которые реализуют ограничения сопряженности (10) и выделяют в двумерном спектре три двумерные хорды

$$c_{1,1}^2 = c_{2,2},\ c_{2,2}^2 = c_{4,4},\ c_{4,4}^2 = c_{1,1};$$
$$c_{1,2}^2 = c_{2,4},\ c_{2,4}^2 = c_{4,1},\ c_{4,1}^2 = c_{1,2};$$
$$c_{1,4}^2 = c_{2,1},\ c_{2,1}^2 = c_{4,2},\ c_{4,2}^2 = c_{1,4}.$$

Задав по одному (произвольному) представителю каждой хорды, вычислим остальные спектральные компоненты этих хорд по правилу сопряженности. Соответствующий двумерный сигнал получим через обратное двумерное преобразование Фурье сформированного спектра. Справедливо и обратное: сформировав сигнал по правилу кодирования БЧХ кодами с порождающим многочленом

$$g(x) = (x-\alpha^0)(x-\alpha^3)(x-\alpha^5)(x-\alpha^6)$$

и выполнив над ним прямое двумерное преобразование Фурье, получим спектр с нулевыми компонентами c_{j_1,j_2} для $j_1, j_2 \in \{0,3,5,6\}$ и не обязательно нулевыми спектральными компонентами c_{j_1,j_2} для $j_1, j_2 \in \{1,2,4\}$.

Рассмотрим теперь двоичный каскадный (49,12,16) код, образованный из кода Рида-Соломона (РС) над $GF(2^3)$ с параметрами (7,4,4) на внешней ступени и двоичного кода БЧХ с параметрами (7,3,4) на внутренней ступени.

Зададим РС код порождающим многочленом

$$G(X) = (X-\alpha^0)(X-\alpha^5)(X-\alpha^6) =$$
$$= \alpha^4 + \alpha^2 x + \alpha^3 x^2 + x^3.$$

На внутренней ступени каскада будем использовать тот же двоичный код БЧХ, заданный порождающим многочленом

$$g(x) = (x-\alpha^0)(x-\alpha^3)(x-\alpha^5)(x-\alpha^6) =$$
$$= 1 + x + x^2 + x^4.$$

Прежде всего отметим, что все слова рассмотренного выше итеративного (49,9,16) кода содержатся среди слов каскадного (49,12,16) кода, т.е. итеративный код является в данном случае подкодом каскадного кода. При этом, только за счет изменения правила кодирования для фиксированного кодового расстояния, удалось на треть повысить относительную скорость кода.

Исходя из значения корней многочлена

$$G(X) = (X-\alpha^0)(X-\alpha^5)(X-\alpha^6),$$

логичной структурой спектра кодовых слов каскадного кода была бы изображенная на рис. 4, *б* схема, т.е. матрица с нулевыми столбцами, соответствующими корням $G(X)$. Однако применение к кодовым словам каскадного кода двумерного преобразования Фурье приведет к представлению слов РС кода в виде соответствующих ограничений на двоичное подполе. С учетом ограничений сопряженности (6) полученные по правилу (18) двоичные слова образуют двоичный (7,6,2) код БЧХ с проверочным многочленом

$$h(x) = (x-\alpha^1)(x-\alpha^2)(x-\alpha^4)(x-\alpha^3)(x-\alpha^5)(x-\alpha^6) =$$
$$= 1 + x + x^2 + x^3 + x^4 + x^5 + x^6$$

и порождающим многочленом

$g(x) = (x-\alpha^0) = 1 + x$, соответственно.

Другими словами, ненулевые спектральные компоненты $c_{i,3}$ двумерного спектра могут привести к ненулевым значениям всех спектральных компонент внутри соответствующих хорд:

$$c_{1,3}^2 = c_{2,6},\ c_{2,6}^2 = c_{4,5},\ c_{4,5}^2 = c_{1,3};$$
$$c_{2,3}^2 = c_{4,6},\ c_{4,6}^2 = c_{1,5},\ c_{1,5}^2 = c_{2,3};$$
$$c_{4,3}^2 = c_{1,6},\ c_{1,6}^2 = c_{2,5},\ c_{2,5}^2 = c_{4,3}$$

и спектр кодового слова в общем виде будет иметь вид, схематично представленный на рис. 4, *в*.

Задавая кодовые слова через обратное двумерное преобразование Фурье спектра, соответствующего рис. 4, *в*, получим не каскадный (49,12,16) код, а некоторый итеративный (49,18,8), как код-произведение двоичных (7,3,4) и (7,6,2) кодов БЧХ.

Таким образом, математический аппарат многомерных спектров *не позволяет* дать описание кодовых слов каскадных кодов в частотной области. Соответственно для этих кодов *невозможно* получить и тот полезный эффект, который дают в технике помехоустойчивого кодирования быстрые многомерные преобразования Фурье. Разрешению этого противоречия и посвящен следующий раздел данной работы.

4. ОПИСАНИЕ КАСКАДНЫХ КОДОВ В ЧАСТОТНОЙ ОБЛАСТИ

Для решения задачи описания каскадных кодов в частотной области необходимо аналитически связать значения спектральных компонент кода внешней ступени с соответствующими спектральными компонентами его ограничения на подполе. Тогда математический аппарат многомерных спектров, с учетом этой введенной аналитической связи, очевидно, позволит вычислить кодовое слово каскадного кода в частотной области.

Таким образом, необходимо решить следующие ***частные задачи***:

1. Аналитически выразить спектр вектора (15) по заданным спектрам произвольных последовательностей (19).
2. Аналитически выразить спектр последовательностей (19) по заданному спектру произвольного вектора (15).
3. Аналитически выразить многомерный спектр вида (18) по заданным спектрам последовательностей (19) и/или (15).

Решение задачи 1.

Обозначим в общем виде спектр последовательности (15) в виде

$$C = (C_0, C_1, C_2, ..., C_{N-1}), \qquad (20)$$

причем $V_i, C_j \in GF(q^m)$, т.е. поле символов сигнала и его спектра совпадают.

Для каждого вектора из (19) найдем спектр, получим

$$c_0 = (c_{0,0}, c_{0,1}, c_{0,2}, ..., c_{0,N-1}),$$
$$c_1 = (c_{1,0}, c_{1,1}, c_{1,2}, ..., c_{1,N-1}), \qquad (21)$$
$$...$$
$$c_{m-1} = (c_{m-1,0}, c_{m-1,1}, c_{m-1,2}, ..., c_{m-1,N-1}),$$

где спектральные компоненты $c_{i,j}$ для всех m спектров c_0, c_1,..., c_{m-1} принадлежат, как и компоненты спектра C, расширенному полю $GF(q^m)$.

Утверждение 1. Спектр произвольного временного вектора есть линейная комбинация спектров его векторов-ограничений на произвольное подполе.

Доказательство. Найдем спектр сигнала V над $GF(q^m)$. Ядром преобразования Фурье в поле Галуа выступает элемент α порядка n, равный корню степени n из единицы. Выберем этот элемент, например, в виде $\alpha = z$. Тогда

$$V_i = v_{0,i} + v_{1,i} z + ... + v_{m-1,i} z^{m-1} =$$
$$= v_{0,i} + \alpha v_{1,i} + ... + \alpha^{m-1} v_{m-1,i}$$

и, соответственно,

$$V = v_0 + \alpha v_1 + ... + \alpha^{m-1} v_{m-1}.$$

То есть вектор V может быть записан как линейная комбинация векторов v_0, v_1, ..., v_{m-1} из (19) (выбор другого элемента $\alpha \in GF(q^m)$ порядка n приведет к изоморфному представлению элемента V, т.е. изменит лишь вид этой линейной комбинации).

Преобразование Фурье, по определению, является линейным и для конечных полей может быть записано в виде матричного умножения сигнала V на матрицу Вандермонда W, составленную из всех степеней элемента α (ядра преобразования), т.е.:

$$C = VW,\ c_i = v_i W,\ i = 0,..,m-1,$$

где

$$W^T = \begin{pmatrix} \alpha^0 & \alpha^0 & \alpha^0 & ... & \alpha^0 \\ \alpha^0 & \alpha^1 & \alpha^2 & ... & \alpha^{N-1} \\ \alpha^0 & \alpha^2 & \alpha^4 & ... & \alpha^{N-2} \\ ... & ... & ... & ... & ... \\ \alpha^0 & \alpha^{N-1} & \alpha^{N-2} & ... & \alpha^1 \end{pmatrix},\ n = N = q^m - 1.$$

Для обратного преобразования следует использовать обратную матрицу:

$$(W^{-1})^T == \begin{pmatrix} \alpha^0 & \alpha^0 & \alpha^0 & ... & \alpha^0 \\ \alpha^0 & \alpha^{N-1} & \alpha^{N-2} & ... & \alpha^1 \\ \alpha^0 & \alpha^{N-2} & \alpha^{N-3} & ... & \alpha^2 \\ ... & ... & ... & ... & ... \\ \alpha^0 & \alpha^1 & \alpha^2 & ... & \alpha^{N-1} \end{pmatrix}.$$

Используя последние выражения, т.е. свойство линейности преобразования Фурье, получим:

$$C = VW = v_0 W + \alpha v_1 W + ... + \alpha^{m-1} v_{m-1} W =$$
$$= c_0 + \alpha c_1 + ... + \alpha^{m-1} c_{m-1}, \qquad (22)$$

следовательно, *спектр C произвольного временного вектора V над $GF(q^m)$ есть линейная комбинация спектров c_0, c_1, ..., c_{m-1} векторов v_0, v_1, ..., v_{m-1} — ограничений V на подполе $GF(q) \subseteq GF(q^m)$*. Конкретный вид этой линейной комбинации определяется, очевидно, выбором элемента α –ядра преобразования Фурье.

Доказанное утверждение позволяет вычислить спектр кодового слова РС кода по известным спектрам его ограничения на подполе, т.е. по известным спектрам соответствующих кодовых слов некоторого БЧХ кода.

Пример 2. Рассмотрим произвольное кодовое слово (7,4,4) РС кода над $GF(2^3)$ из примера 1. Пусть, например,

$$V = (\alpha^6, \alpha^4, \alpha^2, 0, 0, \alpha^4, \alpha^0).$$

Ограничением (14) на двоичное подполе получим три кодовых слова v_0, v_1 и v_2 двоичного (7,6,2) кода БЧХ (см. пример 1). Конкретный вид этих векторов зависит от способа представления элементов поля $GF(2^3)$. Пусть, например, поле $GF(2^3)$ построено по кольцу многочленов с операциями по модулю неприводимого многочлена $f(z) = 1 + z + z^3$ и примитивный элемент $\alpha = z$ поля $GF(2^3)$ является корнем этого многочлена. Тогда слова v_0, v_1 и v_2 примут вид:

$$v_0 = (1,0,0,0,0,0,1),$$
$$v_1 = (0,1,0,0,0,1,0),$$
$$v_2 = (1,1,1,0,0,1,0).$$

Найдем спектр векторов v_0, v_1 и v_2, для чего используем преобразование Фурье вида (4) с ядром $\alpha = z$, получим:

$$c_0 = (0, \alpha^2, \alpha^4, \alpha^5, \alpha^1, \alpha^6, \alpha^3),$$
$$c_1 = (0, \alpha^6, \alpha^5, \alpha^0, \alpha^3, \alpha^0, \alpha^0),$$
$$c_2 = (0,0,0, \alpha^6, 0, \alpha^3, \alpha^5).$$

Используя (22), найдем спектр C вектора V:

$$C = c_0 + \alpha c_1 + \alpha^2 c_2 = = \begin{pmatrix} 0+0+0 \\ \alpha^2+\alpha^0+0 \\ \alpha^4+\alpha^6+0 \\ \alpha^5+\alpha^1+\alpha^1 \\ \alpha^1+\alpha^4+0 \\ \alpha^6+\alpha^1+\alpha^5 \\ \alpha^3+\alpha^1+\alpha^0 \end{pmatrix}^T = \begin{pmatrix} 0 \\ \alpha^6 \\ \alpha^3 \\ \alpha^5 \\ \alpha^2 \\ 0 \\ 0 \end{pmatrix}^T.$$

Непосредственная проверка показывает, что спектр вектора

$$V = (\alpha^6, \alpha^4, \alpha^2, 0, 0, \alpha^4, \alpha^0),$$

вычисленный по правилу (4), действительно равен

$$C = (0, \alpha^6, \alpha^3, \alpha^5, \alpha^2, 0, 0).$$

Решение задачи 2.

Решим теперь обратную задачу, т.е. нахождение спектров (21) по известному спектру (20). Воспользуемся введенными выше обозначениями. Справедливо следующее утверждение.

Утверждение 2. Компоненты спектров векторов-ограничений произвольного временного вектора на произвольное подполе есть линейная комбинация результатов степенных отображений компонентов спектра этого вектора.

Доказательство. Используя (22), запишем

$$\begin{aligned} C_0 &= c_{0,0} + \alpha c_{1,0} + \ldots + \alpha^{m-1} c_{m-1,0}, \\ C_1 &= c_{0,1} + \alpha c_{1,1} + \ldots + \alpha^{m-1} c_{m-1,1}, \\ C_2 &= c_{0,2} + \alpha c_{1,2} + \ldots + \alpha^{m-1} c_{m-1,2}, \\ &\ldots \\ C_{n-1} &= c_{0,n-1} + \alpha c_{1,n-1} + \ldots + \alpha^{m-1} c_{m-1,n-1}, \end{aligned} \qquad (23)$$

т.е. нахождение компонентов спектров (21) сводится к решению недоопределенной системы из n линейных уравнений от nm неизвестных.

Недоопределенная система в общем виде либо имеет бесконечное число решений, либо не имеет их вовсе, однако в данном случае систему уравнений можно несколько упростить.

Действительно, первое уравнение при $\alpha = z$ примет вид

$$C_0 = c_{0,0} + c_{1,0} z + \ldots + c_{m-1,0} z^{m-1},$$

что с учетом $C_0 \in GF(q^m)$ и $c_{i,0} \in GF(q)$ для $i = 0,1,\ldots,m-1$ означает, что элементы ($c_{0,0}$, $c_{1,0}$, ..., $c_{m-1,0}$) определяются как q-ичное представление C_0.

Для остальных уравнений используем ограничения сопряженности (10), которые, для двумерного случая ($p = 2$), перепишем следующим образом: $(c_{i,j})^q = c_{i,jq \bmod (q^m-1)}$.

Ограничения сопряженности преобразуют недоопределенную систему линейных уравнений (23) в множество из u определенных подсистем по u_s нелинейных уравнений (и по u_s неизвестных) в каждой подсистеме, соответственно:

$$\begin{aligned} C_s &= c_{0,s} + \alpha c_{1,s} + \ldots + \alpha^{m-1} c_{m-1,s}, \\ C_{sq \bmod N} &= (c_{0,s})^q + \alpha (c_{1,s})^q + \ldots + \alpha^{m-1} (c_{m-1,s})^q, \\ &\ldots \\ C_{sq^{u_s-1} \bmod N} &= (c_{0,s})^{q^{u_s-1}} + \alpha (c_{1,s})^{q^{u_s-1}} + \ldots + \alpha^{m-1} (c_{m-1,s})^{q^{u_s-1}}, \end{aligned} \qquad (24)$$

где u — число нетривиальных классов сопряженных элементов поля $GF(q^m)$ (или, что эквивалентно, число различных нетривиальных хорд A_s в спектре одномерных сигналов длины N над $GF(q)$), u_s — число элементов в s-м классе (или, что эквивалентно, число элементов в хорде A_s), s — положительное целое, пробегающее все степени примитивного элемента из разложения поля $GF(q^m)$ на классы $\{\alpha^s, \alpha^{sq}, \ldots, \alpha^{sq^{u_s}}\}$ так, что

$$\sum_s u_s = q^m - 2\,,\ \#s = u\,.$$

Найдем решение для произвольной подсистемы нелинейных уравнений (24), т.е. для произвольного s. Для этого используем следующее свойство конечных полей [3–5]:

$$(\alpha+\beta)^{q^b} = \alpha^{q^b} + \beta^{q^b}\,,$$

справедливое для любых $\alpha,\beta \in GF(q^m)$ и любого положительного целого b.

Возведем w-е уравнение подсистемы (24)

$$C_{sq^w \bmod N} = (c_{0,s})^{q^w} + \alpha(c_{1,s})^{q^w} + \ldots + \alpha^{m-1}(c_{m-1,s})^{q^w},$$
$$w = 0,1,..,u_s - 1$$

в степень q^{m-w}, получим:

$$\left(C_{sq^w \bmod N}\right)^{q^{m-w}} =$$
$$= (c_{0,s})^{q^m} + \alpha^{q^{m-w}}(c_{1,s})^{q^m} + \ldots + \alpha^{(m-1)q^{m-w}}(c_{m-1,s})^{q^m},$$

что, согласно малой теореме Ферма, дает линейное уравнение:

$$\left(C_{sq^w \bmod N}\right)^{q^{m-w}} = c_{0,s} + \alpha^{q^{m-w}} c_{1,s} + \ldots + \alpha^{(m-1)q^{m-w}} c_{m-1,s}.$$

Обозначим множество свободных членов в левой части системы (24) через

$$C^s = \{C_s, C_{sq \bmod N}, \ldots, C_{sq^{u_s-1} \bmod N}\}.$$

Тогда функциональное соответствие

$$\left(C_{sq^w \bmod N}\right)^{q^{m-w}} = \varphi\left(C_{sq^w \bmod N}\right),\ w = 0,\ldots,u_s - 1 \quad (25)$$

реализует *степенное отображение* $\varphi: C^s \to \overline{C^s}$ множества C^s в множество

$$\overline{C^s} = \left\{(C_s)^{q^m}, \left(C_{sq \bmod N}\right)^{q^{m-1}}, \ldots, \left(C_{sq^{u_s-1} \bmod N}\right)^{q^{m-u_s+1}}\right\}.$$

Записав поэлементно результат отображения φ, т.е. найдя $\left(C_{sq^w \bmod N}\right)^{q^{m-w}}$ для всех $w = 0,\ldots,u_s - 1$, получим систему линейных уравнений

$$(C_s)^{q^m} = c_{0,s} + \alpha^{q^m} c_{1,s} + \ldots + \alpha^{(m-1)q^m} c_{m-1,s},$$

$$\left(C_{sq \bmod N}\right)^{q^{m-1}} = c_{0,s} + \alpha^{q^{m-1}} c_{1,s} + \ldots + \alpha^{(m-1)q^{m-1}} c_{m-1,s},$$

$$\ldots \quad (26)$$

$$\left(C_{sq^{u_s-1} \bmod N}\right)^{q^{m-u_s+1}} = c_{0,s} + \alpha^{q^{m-u_s+1}} c_{1,s} + \ldots + \alpha^{(m-1)q^{m-u_s+1}} c_{m-1,s},$$

решение которой и дает искомые компоненты спектра для s-й подсистемы.

Найденное решение будет выражаться линейной комбинацией от свободных членов в левой части системы, т.е. от элементов множества $\overline{C^s}$ — результатов степенного отображения компонентов спектра C вектора V.

Выполнив аналогичные преобразования для всех u определенных подсистем, получим, с учетом ограничений сопряженности (10), решения для всех неизвестных компонентов спектров векторов-ограничений временного вектора V на произвольное подполе. Очевидно, что найденные таким образом *компоненты спектров векторов-ограничений произвольного временного вектора на произвольное подполе также будут выражаться линейной комбинацией результатов степенных отображений компонентов спектра этого вектора.*

Сформулированное и доказанное утверждение позволяет аналитически связать спектр векторов-ограничений произвольного кодового слова со спектром этого кодового слова. Для наглядности приведем пример вычисления спектра кодовых слов БЧХ кода по известному спектру кодового слова РС кода из примера 2.

Пример 3. Рассмотрим произвольное кодовое слово $V = (V_0, V_1, V_2, V_3, V_4, V_5, V_6)$ РС кода над $GF(2^3)$ из предыдущего примера.

Запишем его спектр C с компонентами из $GF(2^3)$ в общем виде: $C = (C_0, C_1, C_2, C_3, C_4, C_5, C_6)$. Спектр соответствующих кодовых слов БЧХ кода (или, что эквивалентно, спектр векторов-ограничений v_0, v_1, v_2 слова V на двоичное подполе) запишем в виде:

$$c_0 = (c_{0,0}, c_{0,1}, c_{0,2}, c_{0,3}, c_{0,4}, c_{0,5}, c_{0,6}),$$
$$c_1 = (c_{1,0}, c_{1,1}, c_{1,2}, c_{1,3}, c_{1,4}, c_{1,5}, c_{1,6}),$$
$$c_2 = (c_{2,0}, c_{2,1}, c_{2,2}, c_{2,3}, c_{2,4}, c_{2,5}, c_{2,6}).$$

Используя выражение (22), получим

$$C = c_0 + \alpha c_1 + \alpha^2 c_2\,,$$

что в поэлементной записи (23) дает следующую недоопределенную систему из 6 уравнений и 18 неизвестных

$$C_0 = c_{0,0} + \alpha c_{1,0} + \alpha^2 c_{2,0}\,,$$
$$C_1 = c_{0,1} + \alpha c_{1,1} + \alpha^2 c_{2,1}\,,$$
$$C_2 = c_{0,2} + \alpha c_{1,2} + \alpha^2 c_{2,2}\,,$$
$$C_3 = c_{0,3} + \alpha c_{1,3} + \alpha^2 c_{2,3}\,,$$
$$C_4 = c_{0,4} + \alpha c_{1,4} + \alpha^2 c_{2,4}\,,$$
$$C_5 = c_{0,5} + \alpha c_{1,5} + \alpha^2 c_{2,5}\,,$$
$$C_6 = c_{0,6} + \alpha c_{1,6} + \alpha^2 c_{2,6}\,.$$

Рассмотрим первое уравнение, заметим, что $C_0 \in GF(2^3)$ и все $c_{i,0} \in GF(2)$. Тогда для $\alpha = z$ имеем $C_0 = c_{0,0} + c_{1,0} z + c_{2,0} z^2$, т.е. элементы

$$(c_{0,0},\ c_{1,0},\ c_{2,0})$$

определяются как двоичное представление C_0.

Используя ограничения сопряженности

$$(c_{i,j})^2 = c_{i,2j \bmod(7)}\,,$$

перепишем оставшиеся уравнения в виде:

$$C_1 = c_{0,1} + \alpha c_{1,1} + \alpha^2 c_{2,1},$$
$$C_2 = (c_{0,1})^2 + \alpha (c_{1,1})^2 + \alpha^2 (c_{2,1})^2,$$
$$C_3 = c_{0,3} + \alpha c_{1,3} + \alpha^2 c_{2,3},$$
$$C_4 = (c_{0,1})^4 + \alpha (c_{1,1})^4 + \alpha^2 (c_{2,1})^4,$$
$$C_5 = (c_{0,3})^4 + \alpha (c_{1,3})^4 + \alpha^2 (c_{2,3})^4,$$
$$C_6 = (c_{0,3})^2 + \alpha (c_{1,3})^2 + \alpha^2 (c_{2,3})^2.$$

Элементы поля $GF(2^3)$ образуют $u = 2$ нетривиальных класса сопряженных элементов $\{\alpha^1, \alpha^2, \alpha^4\}$ и $\{\alpha^3, \alpha^6, \alpha^5\}$, т.е. по (24) для $s = 1$ и для $s = 3$ имеем две подсистемы из $u_1 = u_3 = 3$ нелинейных уравнений (и по столько же неизвестных) в каждой подсистеме:

$$C_1 = c_{0,1} + \alpha c_{1,1} + \alpha^2 c_{2,1},$$
$$C_2 = (c_{0,1})^2 + \alpha (c_{1,1})^2 + \alpha^2 (c_{2,1})^2,$$
$$C_4 = (c_{0,1})^4 + \alpha (c_{1,1})^4 + \alpha^2 (c_{2,1})^4;$$
$$C_3 = c_{0,3} + \alpha c_{1,3} + \alpha^2 c_{2,3},$$
$$C_5 = (c_{0,3})^4 + \alpha (c_{1,3})^4 + \alpha^2 (c_{2,3})^4,$$
$$C_6 = (c_{0,3})^2 + \alpha (c_{1,3})^2 + \alpha^2 (c_{2,3})^2.$$

Для каждого $s = 1,3$, используя функциональное соответствие (25)

$$\left(C_{s2^w \bmod 7}\right)^{2^{3-w}} = \varphi\left(C_{s2^w \bmod 7}\right),\ w = 0,...,2,$$

реализуем степенные отображения $\varphi : C^s \to \overline{C^s}$ множеств $C^s = \{C_s, C_{s2 \bmod 7}, C_{s4 \bmod 7}\}$ в множества

$$\overline{C^s} = \left\{C_s, \left(C_{s2 \bmod 7}\right)^4, \left(C_{s4 \bmod 7}\right)^2\right\},$$

результат запишем поэлементно в форме (26).

Получим две системы линейных уравнений:

$$C_1 = c_{0,1} + \alpha c_{1,1} + \alpha^2 c_{2,1},$$
$$(C_2)^4 = c_{0,1} + \alpha^4 c_{1,1} + \alpha c_{2,1},$$
$$(C_4)^2 = c_{0,1} + \alpha^2 c_{1,1} + \alpha^4 c_{2,1};$$
$$C_3 = c_{0,3} + \alpha c_{1,3} + \alpha^2 c_{2,3},$$
$$(C_5)^2 = c_{0,3} + \alpha^2 c_{1,3} + \alpha^4 c_{2,3},$$
$$(C_6)^4 = c_{0,3} + \alpha^4 c_{1,3} + \alpha c_{2,3},$$

решение которых имеет вид линейных комбинаций:

$$c_{0,1} = C_1 + (C_2)^4 + (C_4)^2,$$
$$c_{1,1} = \alpha^2 C_1 + \alpha (C_2)^4 + \alpha^4 (C_4)^2,$$
$$c_{2,1} = \alpha C_1 + \alpha^4 (C_2)^4 + \alpha^2 (C_4)^2;$$
$$c_{0,3} = C_3 + (C_5)^4 + (C_6)^2,$$
$$c_{1,3} = \alpha^2 C_3 + \alpha (C_5)^4 + \alpha^4 (C_6)^2,$$
$$c_{2,3} = \alpha C_3 + \alpha^4 (C_5)^4 + \alpha^2 (C_6)^2.$$

Остальные компоненты спектра получим из условий сопряженности (10):

$$c_{0,2} = (c_{0,1})^2 = (C_1)^2 + C_2 + (C_4)^4,$$
$$c_{0,4} = (c_{0,1})^4 = (C_1)^4 + (C_2)^2 + C_4,$$
$$c_{1,2} = (c_{1,1})^2 = \alpha^4 (C_1)^2 + \alpha^2 C_2 + \alpha (C_4)^4,$$
$$c_{1,4} = (c_{1,1})^4 = \alpha (C_1)^4 + \alpha^4 (C_2)^2 + \alpha^2 C_4,$$
$$c_{2,2} = (c_{2,1})^2 = \alpha^2 (C_1)^2 + \alpha C_2 + \alpha^4 (C_4)^4,$$
$$c_{2,4} = (c_{2,1})^4 = \alpha^4 (C_1)^4 + \alpha^2 (C_2)^2 + \alpha C_4,$$
$$c_{0,6} = (c_{0,3})^2 = (C_3)^2 + C_6 + (C_5)^4,$$
$$c_{0,5} = (c_{0,3})^4 = (C_3)^4 + (C_6)^2 + C_5,$$
$$c_{1,6} = (c_{1,3})^2 = \alpha^4 (C_3)^2 + \alpha^2 C_6 + \alpha (C_5)^4,$$
$$c_{1,5} = (c_{1,3})^4 = \alpha (C_3)^4 + \alpha^4 (C_6)^2 + \alpha^2 C_5,$$
$$c_{2,6} = (c_{2,3})^2 = \alpha^2 (C_3)^2 + \alpha C_6 + \alpha^4 (C_5)^4,$$
$$c_{2,5} = (c_{2,3})^4 = \alpha^4 (C_3)^4 + \alpha^2 (C_6)^2 + \alpha C_5.$$

Таким образом, в общем виде решение системы уравнений для $0 < j \le 6$ запишем как *линейную комбинацию результатов степенных отображений компонентов спектра* C:

$$c_{0,j} = C_j + (C_{2j \bmod 7})^4 + (C_{4j \bmod 7})^2,$$
$$c_{1,j} = \alpha^2 C_j + \alpha (C_{2j \bmod 7})^4 + \alpha^4 (C_{4j \bmod 7})^2,$$
$$c_{2,j} = \alpha C_j + \alpha^4 (C_{2j \bmod 7})^4 + \alpha^2 (C_{4j \bmod 7})^2.$$

Проверка для спектра

$$C = (0, \alpha^6, \alpha^3, \alpha^5, \alpha^2, 0, 0)$$

дает

$$c_0 = (0, \alpha^2, \alpha^4, \alpha^5, \alpha^1, \alpha^6, \alpha^3),$$
$$c_1 = (0, \alpha^6, \alpha^5, \alpha^0, \alpha^3, \alpha^0, \alpha^0),$$
$$c_2 = (0, 0, 0, \alpha^6, 0, \alpha^3, \alpha^5),$$

что полностью совпадает с данными из примера 2.

Полученные аналитические решения первых двух задач, связанных с поиском взаимно-однозначного функционального соответствия спектра вектора (15) и спектров произвольных последовательностей (19), позволяют в общем виде решить задачу аналитического представления многомерного спектра вида (18) по заданным спектрам последовательностей (19) и/или (15).

Решение задачи 3.

Вернемся к рассмотрению кодового слова каскадного кода над $GF(q)$ в форме (17) и соответствующего ему спектра (18) с компонентами из $GF(q^m)$. Если первые m строк матрицы (17) являются векторами-ограничениями (19) кодового слова (15) на подполе $GF(q) \subseteq GF(q^m)$, тогда спектр слов (19) взаимно-однозначно функционально связан со спектром слова (15), что и доказывают предыдущие утверждения. Рассмотрим теперь оставшиеся $n - m$ строк матрицы (17).

Утверждение 3. Кодовое слово каскадного кода есть линейная комбинация векторов-ограничений кодового слова внешней ступени.

Доказательство. Структура каскадного кода (см. рис. 3) такова, что после кодирования кодом внешней ступени (формирование первых m строк матрицы (17)) каждый полученный столбец рассматривается как информационная последовательность $(n,k=m,d)$ кода внутренней ступени. Соответствующие ему кодовые слова записываются по столбцам матрицы (17). Для линейного кода это эквивалентно умножению $v_i=(v_{0,i},v_{1,i},...,v_{m-1,i})g$, где v_i – кодовое слово (16) кода внутренней степени, записываемое в i-й столбец матрицы (17).

Другими словами, процесс формирования всего кодового слова (17) может быть представлен как умножение $N\times k$ матрицы ($k=m$), образованной элементами векторов (19), на порождающую $k\times n$ матрицу g кода первой ступени:

$$v=\begin{pmatrix} v_{0,0} & v_{1,0} & \dots & v_{m-1,0} \\ v_{0,1} & v_{1,1} & \dots & v_{m-1,1} \\ \dots & \dots & \dots & \dots \\ v_{0,N-1} & v_{1,N-1} & \dots & v_{m-1,N-1} \end{pmatrix} g .$$

Это эквивалентно формированию строк матрицы v, как линейной комбинации векторов:

$$v_0=(v_{0,0},v_{0,1},v_{0,2},...,v_{0,N-1}),$$
$$v_1=(v_{1,0},v_{1,1},v_{1,2},...,v_{1,N-1}),$$
$$\dots$$
$$v_{m-1}=(v_{m-1,0},v_{m-1,1},v_{m-1,2},...,v_{m-1,N-1}),$$

т.е. *линейной комбинации векторов-ограничений (19) кодового слова внешней ступени на произвольное подполе*.

Рассмотрим теперь спектр двумерного слова v. Вначале отметим, что для общего случая вычисления многомерных спектров (8) справедливо следующее утверждение.

Утверждение 4. Многомерный спектр многомерного слова есть результат многократного вычисления одномерного спектра ко всем одномерным представлениям этого слова.

Доказательство. Многомерное преобразование Фурье (8) является линейным и может быть записано посредством многократного (p раз, т.е. по каждому измерению матрицы v с учетом транспонирования) умножения матрицы v на матрицу Вандермонда W из утверждения 1:

$$A=\underbrace{\left(\left((vW)^TW\right)^T\dots W\right)^T}_{p\text{ раз}} .$$

Однако результат вычисления vW в построчной записи дает множество спектров, соответствующих строкам матрицы v, т.е. ее одномерному представлению. Другими словами, *многомерный спектр многомерного слова v есть результат многократного вычисления одномерного спектра ко всем одномерным представлениям слова v*.

Объединив предыдущие два утверждения, получим следующее.

Утверждение 5. Спектр кодового слова каскадного кода является, в построчной записи, множеством результатов двукратного вычисления одномерного спектра ко всем линейным комбинациям векторов-ограничений кодового слова внешней ступени.

Доказательство. Применение утверждения 4 к каскадному коду дает следующее выражение

$$A=(vW)^TW , \qquad (27)$$

т.е. спектр кодового слова каскадного кода является, в построчной записи, множеством спектров, соответствующих спектрам строк (v_0, v_1, ..., v_{N-1}) матрицы v.

Однако, как показано в утверждении 3, строки матрицы v являются линейными комбинациями векторов-ограничений v_0, v_1, ..., v_{m-1} из (19) кодового слова внешней ступени. Преобразование Фурье, по определению, линейно, следовательно, спектр линейной комбинации векторов (v_0, v_1, ..., v_{m-1}) из (19) дает линейную комбинацию соответствующих спектров (c_0, c_1, ..., c_{m-1}) из (21). Тогда спектр кодового слова каскадного кода является, в построчной записи, множеством спектров линейных комбинаций спектров (21), или, что эквивалентно, *множеством результатов двукратного вычисления одномерного спектра ко всем линейным комбинациям векторов-ограничений кодового слова внешней ступени*.

Аналитическую связь спектра кодового слова каскадного кода со спектром слов кода внешней ступени дает применение утверждения 2 к последнему результату.

Утверждение 6. Компоненты спектра произвольного кодового слова каскадного кода определяются линейной комбинацией результатов степенных отображений компонентов спектра кодового слова кода внешней ступени.

Доказательство. Действительно, если, согласно утверждению 2, компоненты спектров векторов-ограничений произвольного временного вектора на произвольное подполе есть линейная комбинация результатов степенных отображений компонентов спектра этого вектора, тогда, из утверждения 5 следует, что и *компоненты спектра кодового слова каскадного кода определяются линейной комбинацией результатов этих отображений*.

Приведем пример, наглядно демонстрирующий справедливость приведенных соображений. В качестве исходных данных будем использовать пример 1. Напомним, что использование двумерных спектров в примере 1 *не позволило* дать описание каскадных кодов в частотной области. Покажем теперь как, используя полученные аналитические закономерности, можно решить эту задачу и реализовать кодирование каскадными кодами в частотной области.

Пример 4. Рассмотрим двоичный каскадный (49,12,16) код, образованный из кода РС над $GF(2^3)$ с параметрами (7,4,4) на внешней

ступени и двоичного кода БЧХ с параметрами $(7,3,4)$ на внутренней ступени (см. пример 1).

Спектр векторов-ограничений кодового слова РС кода внешней ступени в общем виде дает результат утверждения 2. Для данного случая (см. пример 2) соответствующие аналитические выражения имеют вид:

$$c_{0,j} = C_j + (C_{2j \bmod 7})^4 + (C_{4j \bmod 7})^2,$$
$$c_{1,j} = \alpha^2 C_j + \alpha(C_{2j \bmod 7})^4 + \alpha^4 (C_{4j \bmod 7})^2,$$
$$c_{2,j} = \alpha C_j + \alpha^4 (C_{2j \bmod 7})^4 + \alpha^2 (C_{4j \bmod 7})^2,$$

справедливые для всех $j = 0,\ldots,N-1$.

Предположим, что на внутренней ступени каскада правило кодирования кодом БЧХ с $g(x) = 1 + x + x^2 + x^4$ задано в систематическом виде через умножение на порождающую матрицу g (см. утверждение 3):

$$g = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

Тогда промежуточный результат vW в (27) в построчной записи будет определяться линейными комбинациями векторов $c_{0,j}$, $c_{1,j}$, $c_{2,j}$ по правилу, задаваемому матрицей g, т.е. для всех $j = 0,\ldots,6$ имеем:

$$c_{3,j} = c_{0,j} + c_{2,j} = \alpha^3 C_j + \alpha^5 (C_{2j \bmod 7})^4 + \alpha^6 (C_{4j \bmod 7})^2,$$

$$c_{4,j} = c_{0,j} + c_{1,j} + c_{2,j} =$$
$$= \alpha^5 C_j + \alpha^6 (C_{2j \bmod 7})^4 + \alpha^3 (C_{4j \bmod 7})^2,$$
$$c_{5,j} = c_{0,j} + c_{1,j} =$$
$$= \alpha^6 C_j + \alpha^3 (C_{2j \bmod 7})^4 + \alpha^5 (C_{4j \bmod 7})^2,$$
$$c_{6,j} = c_{1,j} + c_{2,j} =$$
$$= \alpha^4 C_j + \alpha^2 (C_{2j \bmod 7})^4 + \alpha^1 (C_{4j \bmod 7})^2.$$

Вычисление одномерного преобразования Фурье вектора $c_j = (c_{0,j}, c_{1,j}, c_{2,j}, c_{3,j}, c_{4,j}, c_{5,j}, c_{6,j})$ для всех $j = 0,\ldots,6$ даст все строки спектра кодового слова каскадного кода. То есть общее решение запишем в следующем виде:

$$c_{0,j} = c_j\left(\alpha^i\right)^0 = 0;\ c_{j,0} = c_0\left(\alpha^i\right)^j = 0;$$
$$c_{1,1} = \alpha^6 C_1 + \alpha^0 (C_2)^4 + \alpha^5 (C_4)^2,$$
$$c_{2,2} = (c_{1,1})^2 = \alpha^5 (C_1)^2 + \alpha^0 (C_2)^1 + \alpha^3 (C_4)^4,$$
$$c_{4,4} = (c_{2,2})^2 = \alpha^6 (C_1)^4 + \alpha^0 (C_2)^2 + \alpha^6 (C_4)^1,$$
$$c_{1,2} = \alpha^6 C_2 + \alpha^0 (C_4)^4 + \alpha^5 (C_1)^2,$$
$$c_{2,4} = (c_{1,2})^2 = \alpha^5 (C_2)^2 + \alpha^0 (C_4)^1 + \alpha^3 (C_1)^4,$$
$$c_{4,1} = (c_{2,4})^2 = \alpha^6 (C_2)^4 + \alpha^0 (C_4)^2 + \alpha^6 (C_1),$$
$$c_{1,3} = \alpha^6 C_3 + \alpha^0 (C_6)^4 + \alpha^5 (C_5)^2,$$
$$c_{2,6} = (c_{1,3})^2 = \alpha^5 (C_3)^2 + \alpha^0 (C_6)^1 + \alpha^3 (C_5)^4,$$
$$c_{4,5} = (c_{2,6})^2 = \alpha^6 (C_3)^4 + \alpha^0 (C_6)^2 + \alpha^6 (C_5),$$
$$c_{1,4} = \alpha^6 C_4 + \alpha^0 (C_1)^4 + \alpha^5 (C_2)^2,$$
$$c_{2,1} = (c_{1,4})^2 = \alpha^5 (C_4)^2 + \alpha^0 (C_1)^1 + \alpha^3 (C_2)^4,$$
$$c_{4,2} = (c_{2,1})^2 = \alpha^6 (C_4)^4 + \alpha^0 (C_1)^2 + \alpha^6 (C_2),$$
$$c_{1,5} = \alpha^6 C_5 + \alpha^0 (C_3)^4 + \alpha^5 (C_6)^2,$$
$$c_{2,3} = (c_{1,5})^2 = \alpha^5 (C_5)^2 + \alpha^0 (C_3)^1 + \alpha^3 (C_6)^4,$$
$$c_{4,6} = (c_{2,3})^2 = \alpha^6 (C_5)^4 + \alpha^0 (C_3)^2 + \alpha^6 (C_6),$$
$$c_{1,6} = \alpha^6 C_6 + \alpha^0 (C_5)^4 + \alpha^5 (C_3)^2,$$
$$c_{2,5} = (c_{1,6})^2 = \alpha^5 (C_6)^2 + \alpha^0 (C_5)^1 + \alpha^3 (C_3)^4,$$
$$c_{4,3} = (c_{2,5})^2 = \alpha^6 (C_6)^4 + \alpha^0 (C_5)^2 + \alpha^6 (C_3),$$
$$c_{3,j} = 0,\ c_{5,j} = 0,\ c_{6,j} = 0.$$

Для проверки зададим спектр кодового слова РС кода как в примере 3: $C = (0, \alpha^6, \alpha^3, \alpha^5, \alpha^2, 0, 0)$, что дает

$$c_0 = (0, \alpha^2, \alpha^4, \alpha^5, \alpha^1, \alpha^6, \alpha^3),$$
$$c_1 = (0, \alpha^6, \alpha^5, \alpha^0, \alpha^3, \alpha^0, \alpha^0),$$
$$c_2 = (0, 0, 0, \alpha^6, 0, \alpha^3, \alpha^5)$$

и соответствующий спектр кодового слова каскадного кода, вычисленный по выведенным аналитическим выражениям, примет вид:

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

Не трудно убедиться, что обратное двумерное преобразование Фурье матрицы c дает матрицу

$$v = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}, \qquad (28)$$

которая действительно является кодовым словом каскадного $(49,12,16)$ кода.

Таким образом, пример 4 наглядно демонстрирует реализацию кодирования каскадным кодом через преобразования в частотной области. Этот результат, по мнению автора, получен *впервые*.

В заключение приведем выражения для получения компонентов сигнала v над $GF(q)$ по задаваемым в частотной области компонентам спектра кодовых слов кода внешней ступени над

$GF(q^m)$. Для этого сформулируем и докажем следующее утверждение.

Утверждение 7. Компоненты произвольного кодового слова каскадного кода (во временной области) определяются линейной комбинацией результатов степенных отображений компонентов спектра кодового слова кода внешней ступени.

Доказательство. Из (27) следует, что для нахождения вектора v необходимо выполнить двукратное обратное одномерное преобразование Фурье над строками матрицы c с учетом транспонирования. При этом промежуточный результат vW уже известен из утверждения (5). В построчной записи vW представляет собой линейные комбинации спектров (21), которые, по утверждению 2, определяются линейными комбинациями результатов степенных отображений (25) компонентов спектра (20). Таким образом, для вычисления кодового слова v достаточно выполнить обратное преобразование Фурье всех линейных комбинаций векторов (21), т.е., с учетом линейности преобразования, *кодовое слово v определяется линейной комбинацией результатов степенных отображений компонентов спектра кодового слова кода внешней ступени.*

Покажем вид этих линейных комбинаций для рассмотренного в примере 4 случая.

Пример 5. Вычисляя обратное преобразование Фурье для всех векторов c_j, $j=0,...,6$ (см. пример 4), получим:

$$v_{0,0}=\sum_{j=0}^{6}\left(C_j+(C_{2j \bmod 6})^4+(C_{4j \bmod 6})^2\right),$$

$$v_{1,0}=\sum_{j=0}^{6}(\alpha^j)^{-1}\left(C_j+(C_{2j \bmod 6})^4+(C_{4j \bmod 6})^2\right),$$

$$\ldots$$

$$v_{6,0}=\sum_{j=0}^{6}(\alpha^j)^{-6}\left(C_j+(C_{2j \bmod 6})^4+(C_{4j \bmod 6})^2\right),$$

$$v_{0,1}=\sum_{j=0}^{6}\left(\alpha^2 C_j+\alpha(C_{2j \bmod 7})^4+\alpha^4(C_{4j \bmod 7})^2\right),$$

$$v_{1,1}=\sum_{j=0}^{6}(\alpha^j)^{-1}\left(\alpha^2 C_j+\alpha(C_{2j \bmod 7})^4+\alpha^4(C_{4j \bmod 7})^2\right),$$

$$\ldots$$

$$v_{6,1}=\sum_{j=0}^{6}(\alpha^j)^{-6}\left(\alpha^2 C_j+\alpha(C_{2j \bmod 7})^4+\alpha^4(C_{4j \bmod 7})^2\right),$$

$$\ldots$$

$$v_{6,6}=\sum_{j=0}^{6}(\alpha^j)^{-6}\left(\alpha^4 C_j+\alpha^2(C_{2j \bmod 7})^4+\alpha^1(C_{4j \bmod 7})^2\right).$$

Непосредственная проверка со спектром $C=(0,\alpha^6,\alpha^3,\alpha^5,\alpha^2,0,0)$ из примера 4 дает кодовое слово (28), что подтверждает справедливость и адекватность приведенных рассуждений.

ВЫВОДЫ

Таким образом, в результате проведенных исследований получено общее решение задачи представления каскадных кодов в частотной области, что позволит, используя выведенные аналитические зависимости компонентов многомерных спектров, строить в частотной области вычислительно эффективные алгоритмы кодирования и декодирования. Наиболее перспективным в этом смысле является использование быстрых многомерных преобразований Фурье.

Решение задачи описания каскадных кодов в частотной области потребовало нетривиальных абстрактных представлений соответствующих кодовых слов и их ограничений на подполе. Тем не менее, полученный результат связывает спектр кодового слова внешней ступени с кодовым словом каскадного кода (и/или его спектром) в виде простых аналитических выражений (см. примеры 4 и 5). Прикладное значение этого результата состоит в возможности построения кодовых слов каскадного кода в частотной области через соответствующие компоненты спектра кодового слова внешней ступени. Анализируя полученные результаты, следует также отметить специфическую структуру конечных выражений. Действительно, переменные в правой части уравнений (см. примеры 4 и 5) сгруппированы по классам сопряженных элементов, что указывает на непосредственное влияние групповых свойств конечного поля. Это наблюдение, очевидно, также может служить предметом дальнейших исследований с целью сокращения вычислительной сложности соответствующих преобразований.

Литература

[1] Скляр Б. Цифровая связь. Теоретические основы и практическое применение / Б. Скляр. – М.: Вильямс, 2007. – 1104 с.

[2] Кларк Дж. – мл., Кейн Дж. Кодирование с исправлением ошибок в системах цифровой связи: пер. с англ. / под ред. Б.С. Цыбакова. – М.: Радио и связь, 1987. – 392 с.

[3] Блейхут Р. Теория и практика кодов, контролирующих ошибки: пер. с англ. / Р. Блейхут. – М.: Мир, 1986. – 576 с.

[4] Федоренко С.В. Методы быстрого декодирования линейных блоковых кодов. – СПб.: ГУАП, 2008. – 199 с.

[5] Василенко О. Н. Теоретико-числовые алгоритмы в криптографии. – М.: МЦНМО, 2003. – 328 с.

[6] Сергиенко А. Б. Цифровая обработка сигналов. - 2-е. – СПб: Питер, 2006. – С. 751.

[7] Блейхут Р. Быстрые алгоритмы цифровой обработки сигналов: пер. с англ. / Р. Блейхут. – М.: Мир, 1989. – 448 с.

Поступила в редколлегию 20.03.2013

Кузнецов Александр Александрович, доктор технических наук, профессор, профессор кафедры БИТ ХНУРЭ. Научные интересы: теория кодирования и аутентификации.

Приходько Сергей Иванович, заведующий кафедрой транспортной связи Украинской академии железнодорожного транспорта. Научные интересы: теория помехоустойчивого кодирования, передача и обработка информации.

Билал Хамзе, аспирант кафедры транспортной связи Украинской академии железнодорожного транспорта. Научные интересы: теория помехоустойчивого кодирования, передача и обработка информации.

УДК 621.391

Багатовимірні спектри для опису каскадних кодів у частотній області // О.О. Кузнецов, С.І. Приходько, Білал Хамзе // Прикладна радіоелектроніка: наук.-техн. журнал. – 2013. – Том 12. – № 2. – С. 319–332.

Розглядається математичний апарат багатовимірного дискретного перетворення Фур'є в кінцевих полях. Досліджуються методи опису лінійних блокових кодів у частотній області. Показано, що, на відміну від ітеративних кодів (кодів-добутків) каскадні коди в загальному випадку не можуть бути описані в частотній області в термінах багатовимірних спектрів. Отримано аналітичні вирази, що встановлюють взаємно-однозначну функціональну відповідність спектру послідовності над кінцевим полем і спектрів відповідних слів, отриманих обмеженням цього слова на підполе. Отримано загальне розв'язання задачі подання каскадних кодів у частотній області, що дозволить, використовуючи виведені аналітичні залежності компонентів багатовимірних спектрів, будувати в частотній області обчислювально ефективні алгоритми кодування і декодування.

Ключові слова: багатовимірне дискретне перетворення Фур'є, каскадні коди, кінцеві поля.

Іл.: 4. Бібліогр.: 7 найм.

UDC 621.391

Multidimensional spectra for describing cascade codes in the frequency domain // A.A. Kuznetsov, S.I.Prihod'ko, Bilal Hamse // Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. – № 2. – P. 319–332.

Mathematical tools of multidimensional discrete Fourier transformation over finite fields are considered. Methods for describing linear block codes in the frequency domain are researched. It is shown that unlike iterative codes (product codes) in the general case cascade codes cannot be described in the frequency domain in terms of multidimensional spectra. Analytical expressions establishing one-to-one functional correspondence of a spectrum of sequence over a finite field and spectra of relevant words derived by restriction of the word to the subfield are obtained. A general solution of the problem of cascade code representation in the frequency domain is obtained which makes it possible to construct computationally efficient algorithms for encoding and decoding using the derived analytical relations of multidimensional spectra.

Keywords: multidimensional discrete Fourier transformation, cascade codes, finite fields.

Fig.: 4. Ref.: 7 items.