АЛГОРИТМЫ КОДИРОВАНИЯ АЛГЕБРАИЧЕСКИХ НЕДВОИЧНЫХ КАСКАДНЫХ СВЕРТОЧНЫХ КОДОВ УМЕНЬШЕННОЙ СЛОЖНОСТИ

DOI: 10.36724/2072-8735-2024-18-3-11-18

Волков Алексей Станиславович,
Национальный исследовательский университет "Московский институт электронной техники", Зеленоград, Москва, Россия, ***leshvol@mail.ru***

Крейнделин Виталий Борисович,
Московский технический университет связи и информатики, Москва, Россия, ***v.b.kreindelin@mtuci.ru***

Manuscript received 07 February 2024;
Accepted 12 March 2024

Ключевые слова: *помехоустойчивое кодирование, сверточные коды, построение сверточных кодов, вычислительная сложность, порождающий многочлен, каскадные коды*

Для обеспечения высокой достоверности передаваемой информации в проводных и беспроводных телекоммуникационных системах и сетях применяются помехоустойчивые коды. Добиться высокой достоверности при относительно невысокой сложности алгоритмов кодирования и декодирования удается за счет применения каскадных кодов. Каскадный код представляет собой кодовую конструкцию, основанную на последовательном соединении нескольких компонентных помехоустойчивых кодов. С практической точки зрения, наибольший интерес вызывают каскадные коды с двумя ступенями кодирования. Одну ступень кодирования называют внешней, а другую внутренней. В работе разработан алгоритм формирования порождающих многочленов внешней и внутренней ступени, которые позволяют однозначно определять алгебраические каскадные сверточные коды с заранее заданными параметрами и произвольными длинами кодовых ограничений за фиксированное количество шагов. Разработаны алгоритмы кодирования алгебраических каскадных сверточных кодов, с использованием быстрых алгоритмов вычисления циклической свертки на каждой из ступеней, причем, для нахождения многочленов кодовых слов $c(x)$ и $s(x)$, длины порождающих и информационных многочленов выбраны соизмеримыми с длинами циклических сверток на внешней и внутренней ступени соответственно. Применение быстрых алгоритмов вычисления свертки Агарвала-Кули и Винограда целесообразно использовать на внешней ступени кодирования недвоичного алгебраического каскадного сверточного кода. Это дает возможность уменьшить число арифметических операций в поле $GF(q^p)$ при вычислении многочлена кодового слова $c(x)$. Для уменьшения числа арифметических операций в поле $GF(q^m)$ на внутренней ступени, рекомендуется использовать быстрый алгоритм Винограда вычисления свертки. Это связано с тем, что на внутренней ступени кодирования, как правило, рекомендуют использование кодов с меньшей длиной кодового ограничения и построенных над меньшими полями, по сравнению с кодами внешней ступени. Для оценки вычислительной сложности алгоритма кодирования на основе синтеза алгоритмов Агарвала-Кули и Винограда представлены соответствующие выражения для компонентных алгебраических сверточных кодов на каждой из ступени.

Информация об авторах:
Волков Алексей Станиславович, *к.т.н., доцент, доцент кафедры телекоммуникационных систем Национальный исследовательский университет "Московский институт электронной техники", Зеленоград, Москва, Россия*
Крейнделин Виталий Борисович, *д.т.н., профессор, заведующий кафедрой "Теория электрических цепей" "Московский технический университет связи и информатики", Москва, Россия*

Для цитирования:
Волков А.С., Крейнделин В.Б. Алгоритмы кодирования алгебраических недвоичных каскадных сверточных кодов уменьшенной сложности // T-Comm: Телекоммуникации и транспорт. 2024. Том 18. №3. С. 11-18.

For citation:
Volkov A.S., Kreyndelin V.B. (2024) Algorithms for encoding algebraic non-binary concatenated convolutional codes of reduced complexity. *T-Comm*, vol. 18, no.3, pp. 11-18. (*in Russian*)

Введение

В настоящее время для обеспечения высокой достоверности передаваемой информации в телекоммуникационных системах и сетях применяются помехоустойчивые коды [1-4]. Добиться высокой достоверности при относительно невысокой сложности алгоритмов кодирования и декодирования удается за счет применения каскадных кодов [5-8]. Каскадный код представляет собой кодовую конструкцию, основанную на последовательном соединении нескольких компонентных помехоустойчивых кодов [1]. С практической точки зрения, наибольший интерес вызывают каскадные коды с двумя ступенями кодирования. Одну ступень кодирования называют внешней, а другую внутренней [2].

В качестве компонентных кодов внешней и внутренней ступени широкое применение нашли блоковые (коды РС и БЧХ) и сверточные коды [9]. При этом, комбинируя различные компонентные коды в составе каскадного кода, удается получить новые классы кодов [10-12]. Следовательно, построение каскадного кода определяется выбором компонентных кодов.

Класс обобщенных каскадных кодов предусматривает разложение кода внутренней ступени на подкоды, которые соответствуют подкодам внешней ступени кода. Следовательно, такое теоретическое обобщение позволяет строить каскадные коды с числом компонентных кодов больше двух [9-11].

В настоящее время существует множество различных классов каскадных кодов и их модификаций (обобщенные линейные каскадные коды, сверточные каскадные коды, обобщенные сверточные каскадные коды с единичной памятью и т.д.) [12-16].

На рисунке 1 представлен общий принцип построения каскадного сверточного кода [12].

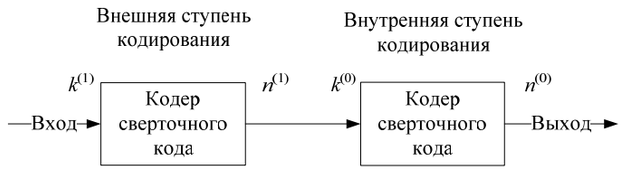

Рис. 1. Принцип построения кодера каскадного сверточного кода

Принцип каскадного сверточного кодирования следующий. На вход каскадного сверточного кодера поступает информационная последовательность, которая разбивается на кадры по $k^{(1)}$ символов в каждом кадре. Результатом кодирования кодера сверточного кода внешней ступени является кадр кодового слова, состоящий из $n^{(1)}$ символов, формирование которого происходит с учетом символов, хранящихся в памяти кодера внешней ступени. При этом считается, что однозначное соответствие (реализация функции кодирования [13, 17]) кадра информационных символов $k^{(1)}$ кадру кодового слова $n^{(1)}$ осуществляется за одну единицу времени работы кодера. Далее предполагается, что выполняется равенство $n^{(1)} = k^{(0)}$ (это необходимо для согласования кодера внешней и внутренней ступени кодирования) и одному кадру информационных символов $k^{(0)}$ с учетом символов, хранящихся в памяти кодера внутренней ступени, сопоставляется кадр кодового слова $n^{(0)}$ [17].

Целью данной работы является разработка алгоритмов построения порождающих многочленов алгебраически заданных сверточных каскадных кодов, а также разработка алгоритмов кодирования алгебраических каскадных сверточных кодов на основе процедур быстрого вычисления сверток для уменьшения вычислительной сложности кодирования.

Результаты исследования

Рассмотрим алгоритм определения порождающих многочленов каскадного $(n^{(k)}, k^{(k)})$-кода пошагово.

ШАГ 1. Ввод параметров $k^{(0)}$, $k^{(1)}$, $n^{(0)}$, $n^{(1)}$, r алгебраических сверточных кодов внешней и внутренней ступени кодирования и требуемой скорости кодирования R_k каскадного $(n^{(k)}, k^{(k)})$-кода.

ШАГ 2. Выбор примитивных многочленов степени p и m и построение конечных полей $GF(q^p)$ и $GF(q^m)$.

ШАГ 3. Выполнение расчета скоростей алгебраических сверточных кодов внешней и внутренней ступени кодирования: $R_1 = k^{(1)}/n^{(1)}$ и $R_0 = k^{(0)}/n^{(0)}$.

ШАГ 4. Проверка условий согласования по скорости сверточного кода внешней и внутренней ступени кодирования. Если $k^{(0)} = p$, либо $k^{(0)}$ – делит число $(2r - 1) \cdot p$ без остатка, то внешняя и внутренняя ступени кодера согласованы по скорости. При невыполнении условия, необходимо изменение одного или нескольких параметров сверточных кодов.

ШАГ 5. Выбор способа обработки символов на каждой из ступени.

ШАГ 6. Построение порождающих многочленов $u(x)$ над $GF(q^p)$ и $w(x)$ $GF(q^m)$ недвоичных циклических блоковых кодов. Пусть многочлен $u(x)$ является порождающим многочленом степени $r - 1$ циклического блокового (N_1, K_1, D_1)-кода РС над $GF(q^p)$. Тогда [15-18]:

$$u(x) = \prod_{y=a}^{a+2t-1} (x - \gamma^y),$$

где t – число исправляемых ошибок (N_1, K_1, D_1)-кодом РС, $N_1 = q^p - 1$, $K_1 = N_1 - \deg u(x)$, $D_1 = 2t + 1$; γ – примитивный элемент поля $GF(q^p)$.

Предположим, что многочлен $w(x)$ является порождающим многочленом степени $h - 1$ циклического блокового (N_0, K_0, D_0) – кода РС над $GF(q^m)$ [18]:

$$w(x) = \prod_{\alpha=a}^{a+2t-1} (x - \alpha^y),$$

где t – число исправляемых ошибок (N_0, K_0, D_0)-кодом РС, $N_0 = q^m - 1$, $K_0 = N_0 - \deg w(x)$, $D_0 = 2t + 1$; α – примитивный элемент поля $GF(q^m)$.

ШАГ 7. Формирование порождающих многочленов $g(x)$ внешней ступени и набора из z порождающих многочленов $g_z^*(x)$ внутренней ступени кодирования алгебраического каскадного сверточного кода. Схемы алгоритмов формирования порождающих многочленов $g(x)$ и $g_z^*(x)$ представлены на рисунках 2 и 3 соответственно.

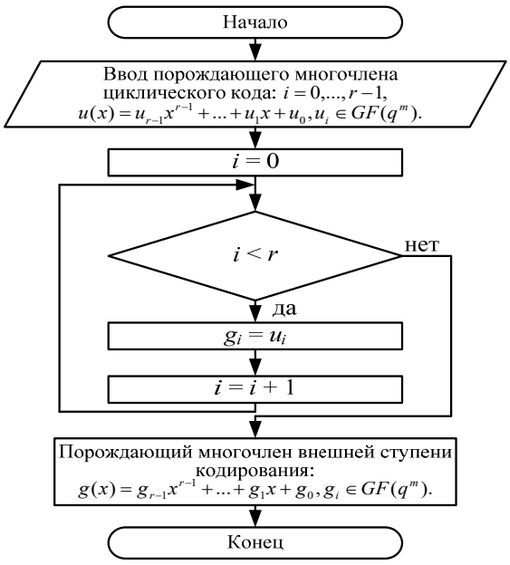

Рис. 2. Схема алгоритма формирования порождающего многочлена внешней ступени алгебраического каскадного сверточного кода

ШАГ 8. Построение схемы кодера алгебраического каскадного сверточного $(n^{(k)}, k^{(k)})$-кода.

Схема алгоритма построения алгебраического каскадного сверточного кода представлена на рисунке 3.

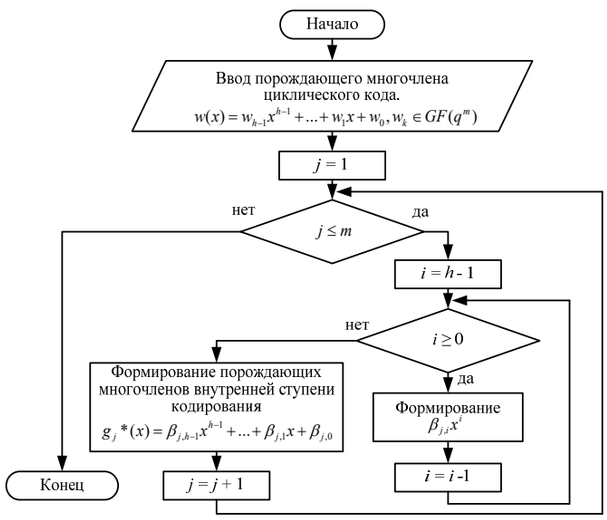

Рис. 3. Схема алгоритма формирования порождающих многочленов внутренней ступени алгебраического каскадного сверточного кода

Для формирования порождающих многочленов алгебраических каскадных сверточных $(n^{(k)}, k^{(k)})$-кодов можно выбирать недвоичные циклические блоковые примитивные или непримитивные коды БЧХ. Выбор кодов РС для построения каскадных $(n^{(k)}, k^{(k)})$-кодов объясняется их высокими корректирующими способностями [21]. Таким образом, за конечное число шагов возможно построение алгебраического каскадного сверточного $(n^{(k)}, k^{(k)})$-кода с параметрами: $k^{(k)} = k^{(1)}$, $n^{(k)} = m$, $v_k = r \cdot k^{(1)} + h \cdot k^{(0)}$, $R_k = R_1 \cdot R_0$.

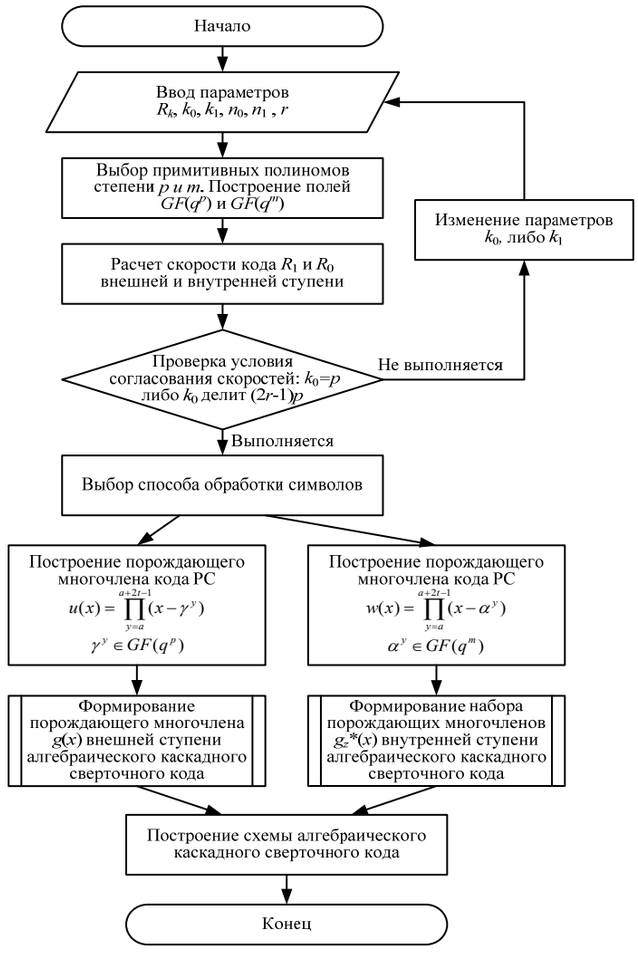

Рис. 4. Схема алгоритма определения алгебраического каскадного сверточного кода

Далее предлагается алгоритм кодирования алгебраических каскадных сверточных кодов с использованием быстрых процедур вычисления циклической свертки [22]. Данный алгоритм позволит уменьшить число арифметических операций умножений и сложений. Алгоритм кодирования каскадным $(n^{(k)}, k^{(k)})$-кодом на внешней ступени рассмотрим пошагово.

ШАГ 1. Ввод информационной последовательности $b(x)$, подлежащей кодированию, в кодер внешней ступени.

ШАГ 2. Используя метод перекрытия с суммированием, выполняется разбиение информационной последовательности $b(x)$ на секции конечной длины $\{b^{(1)}(x), b^{(2)}(x), b^{(3)}(x), ...\}$. Длина каждой секции равна $n - L$. Причем, $L = \deg g(x)$, $n = n' \cdot n'' \ge 2r - 1$, $b_i \in GF(q^p)$, $g_i \in GF(q^p)$, $\deg b^{(l)}(x) = n - L - 1$. Числа n' и n'' – взаимно просты [23-25].

ШАГ 3. Формирование серии циклических сверток для нахождения многочлена $c(x)$ кодового слова внешней ступени для случая бесконечной длины. Каждая из l-тая циклических сверток равна: $c^{(l)}(x) = g(x) \cdot b^{(l)}(x) \bmod(x^n - 1)$.

ШАГ 4. На основе алгоритма Агарвала-Кули [23-25], выполняется преобразование одномерной l-ой циклической свертки в двумерную свертку. Схема алгоритма формирования двумерного кодового слова внешней ступени представлена на рисунке 5.

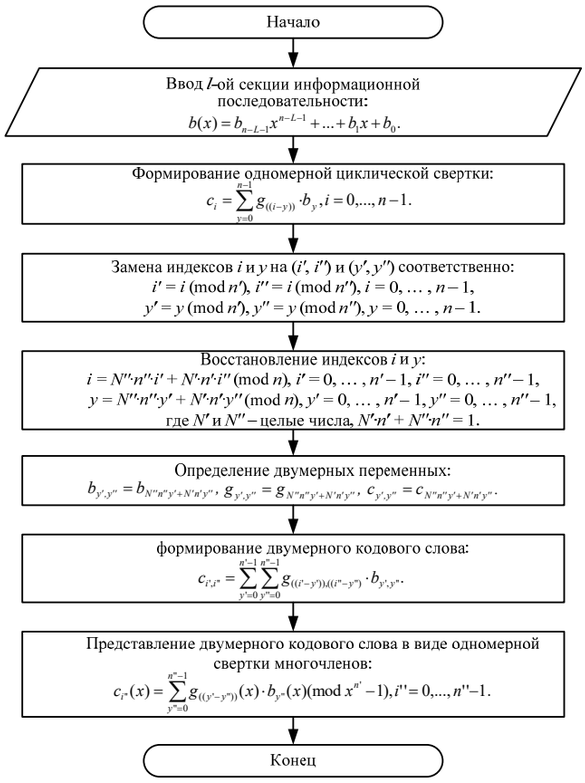

Рис. 5. Схема алгоритма формирования двумерного кодового слова на внешней ступени кодирования

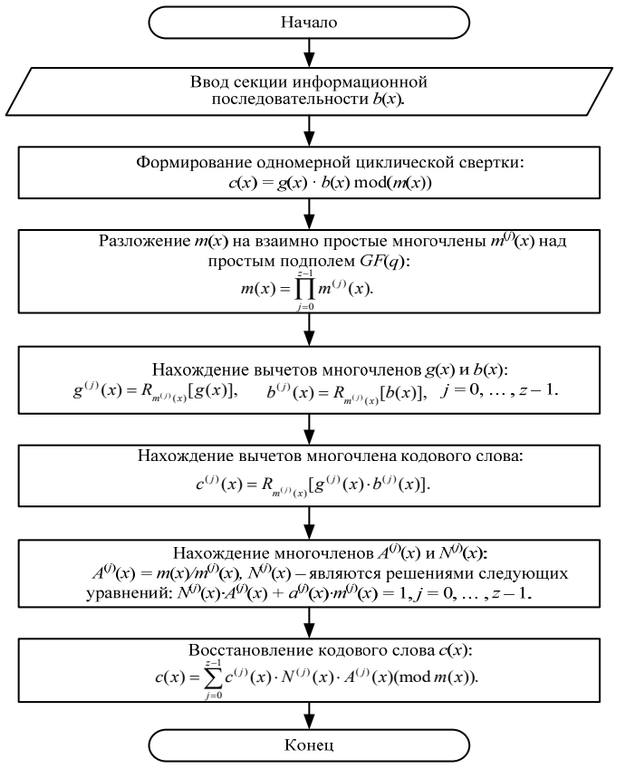

Рис. 6. Схема алгоритма вычисления коротких циклических сверток на внешней ступени кодирования

ШАГ 5. Используя алгоритм Винограда, основанный на китайской теореме об остатках, реализуется вычисление коротких циклических сверток. Схема алгоритма вычисления коротких циклических сверток на внешней ступени кодирования представлена на рисунке 6.

ШАГ 6. Формирование многочлена кодового слова $c(x)$ на внешней ступени алгебраического каскадного сверточного кода, на основе метода перекрытия с суммированием.

На рисунке 7 представлена схема алгоритма кодирования на внешней ступени каскадного $(n^{(k)}, k^{(k)})$-кода.

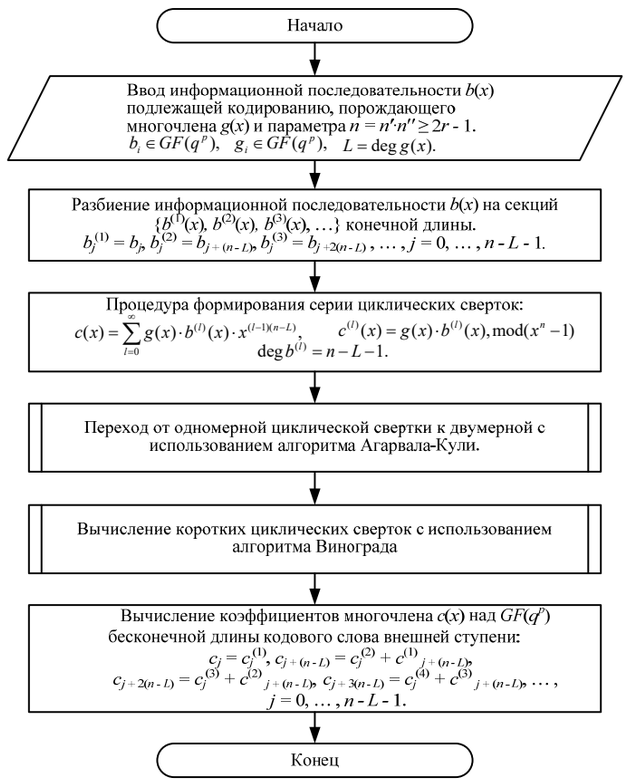

Рис. 7. Схема алгоритма кодирования на внешней ступени алгебраического каскадного сверточного $(n^{(k)}, k^{(k)})$-кода

Далее рассмотрим алгоритм кодирования алгебраического каскадного сверточного $(n^{(k)}, k^{(k)})$-кода на внутренней ступени.

ШАГ 1. Ввод последовательности $f(x)$ подлежащей кодированию на внутреннюю ступень кодера.

ШАГ 2. Преобразование многочлена $f(x)$ с целью нахождения всех коэффициентов (включая первые H) кодового слова $s(x)$ алгебраического каскадного сверточного кода: $f(x) \cdot x^H$.

ШАГ 3. Разбиение $f(x)$ на секции конечной длины $\{f^{(1)}(x), f^{(2)}(x), f^{(3)}(x), \dots\}$ на основе метода перекрытия с накоплением [22-25]. При этом, $f_i \in GF(q^m)$, $g_i^* \in GF(q^m)$, $H = \deg g^*(x)$.

ШАГ 4. Формирование l-ой циклической свертки кодового слова: $s^{(l)}(x) = g^*(x) \cdot f^{(l)}(x) \bmod(x^n - 1)$.

ШАГ 5. Вычисление l-ой циклической свертки $s^{(l)}(x)$ кодового слова с применением алгоритма Винограда рисунке 8.

ШАГ 6. Вычисление коэффициентов многочлена $s(x)$ кодового слова внутренней ступени кодирования алгебраического каскадного сверточного кода на основе метода перекрытия с накоплением.

Схема алгоритма кодирования на внутренней ступени алгебраического каскадного сверточного ($n^{(k)}$, $k^{(k)}$)-кода представлена на рисунке 8.

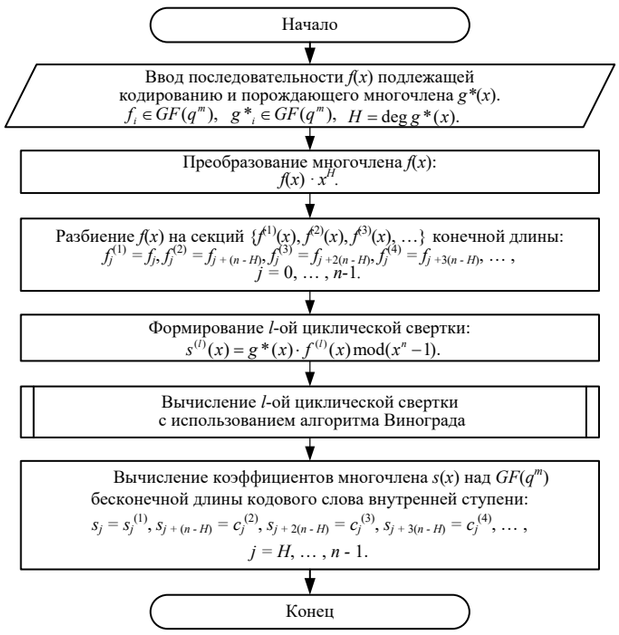

Рис. 8. Схема алгоритма кодирования на внутренней ступени алгебраического каскадного сверточного ($n^{(k)}$, $k^{(k)}$)-кода

В общем случае процедура кодирования алгебраических сверточных кодов в составе каскадного предполагает, что длина многочлена информационной последовательности во много раз превышает длину порождающего многочлена. Следовательно, ее можно представить порождающим многочленом бесконечной степени. Это утверждение справедливо для сверточных кодов внешней и внутренней ступени алгебраического каскадного сверточного кода. Тогда, процедура кодирования алгебраическим сверточным кодом эквивалентна вычислению непрерывной недвоичной линейной свертки большой длины (т.е. длина во много раз превышает длину порождающего многочлена).

Согласно предложенным алгоритмам, определим недвоичный алгебраический каскадный сверточный ($n^{(k)}$, $k^{(k)}$) – код. Положим, что на внешней и внутренней ступени кодирования заданы алгебраические сверточные коды с обработкой символов над $GF(q^p)$, где $q = b^w$, и над $GF(b^m)$ соответственно. Очевидно, что $GF(b^w)$ является подполем поля $GF(q^p)$. При этом нерекурсивный сверточный (n_1, k_1) – код над $GF(q^p)$ в несистематическом виде определяется порождающим многочленом $g(x)$ над $GF(q^p)$ и имеет параметры: $k^{(1)} = \log_q /M/$, $n^{(1)} = p$, $k_1 = (r + 1) \cdot k^{(1)}$, $n_1 = k_1 \cdot n^{(1)}/k^{(1)}$ и скорость кодирования $R_1 = k^{(1)}/p$. Порождающий многочлен $g^*(x)$ над $GF(b^m)$ определяет нерекурсивный сверточный (n_1, k_1) – код над $GF(b^m)$ в несистематическом виде с параметрами: $k^{(0)} = \log_b /Q/$, $n^{(0)} = m$, $k_0 = (h + 1) \cdot k^{(1)}$, $n_0 = k_0 \cdot n^{(0)}/k^{(0)}$ и скоростью кодирования $R_0 = k^{(0)}/m$.

Для оценки минимального кодового расстояния d_k алгебраического каскадного сверточного ($n^{(k)}$, $k^{(k)}$) – кода проведем следующие рассуждения.

Предположим, что на вход кодера внешней ступени ($n^{(k)}$, $k^{(k)}$) – кода поступил кадр информационных символов $k^{(1)}$, который принадлежит множеству M и удовлетворяет следующим условиям: $k^{(1)} = \log_q /M/ \geq 1$, $M \in GF(q^p)$, $p \geq k^{(1)}$. Тогда, с учетом r кадров, хранящихся в памяти кодера внешней ступени, формируется кадр кодового слова $n^{(1)}$, являющийся одним элементом поля $GF(q^p)$.

Пусть число кадров, поступивших на вход сверточного кодера внешней ступени, равно K_1. Тогда последовательность (секция), состоящая из N_1 кадров кодового слова над $GF(q^p)$, является кодовым словом недвоичного циклического блокового (N_1, K_1, D_1) – кода над $GF(q^p)$ в несистематическом виде [9]. Следовательно, справедливо утверждать, что минимальное кодовое расстояние d_1 одной секции длины N_1 сверточного (n_1, k_1) – кода над $GF(q^p)$ внешней ступени кодирования удовлетворяет выражению $d_1 \geq D_1$ [17, 19]. Далее процедура кодирования реализуется на внутренней ступени ($n^{(k)}$, $k^{(k)}$) – кода.

На вход сверточного кодера внутренней ступени кодирования поступает кадр информационных символов $k^{(0)} = \log_b /Q/ \geq 1$, где $Q \in GF(b^m)$, $m \geq k^{(0)}$, $m > w$. Тогда кадр $k^{(0)}$ будет одним элементом множества Q или элементом поля $GF(b^w)$. Следовательно, формирование кадра кодового слова $n^{(0)}$ происходит с учетом h кадров хранящихся в памяти сверточного кодера внутренней ступени. Причем кадра кодового слова n_0 является одним элементом поля $GF(b^m)$.

Зафиксируем $p = K_0$. Аналогично, если подать K_0 кадров информационных символов на вход сверточного кодера внутренней ступени кодирования, то N_0 кадров кодового слова представляют собой кодовое слово циклического блокового (N_0, K_0, D_0) – кода над $GF(b^m)$, также в несистематическом виде [9]. При этом минимальное кодовое расстояние d_0 сверточного (n_0, k_0) – кода над $GF(b^m)$ на внутренней ступени кодирования одной секции длины N_0 удовлетворяет условию $d_0 \geq D_0$ [17, 19].

В тоже время из теории помехоустойчивого блокового кодирования известно, что при последовательном соединении двух недвоичных блоковых кодов РС в несистематическом виде минимальное кодовое расстояние D_k каскадного блокового кода оценивается как $D_k \geq D_1 \cdot D_0$. Причем длина блока информационного слова каскадного блокового кода $K_k = K_1 \cdot K_0$, а длина блока кодового слова каскадного кода $N_k = N_1 \cdot N_0$ [17, 19].

На основании вышеизложенных рассуждений, можно сделать вывод, что минимальное кодовое расстояние d_k недвоичного алгебраического каскадного сверточного ($n^{(k)}$, $k^{(k)}$) – ода можно оценить согласно следующему выражению:

$$d_k \geq d_1 \cdot d_0. \qquad (1)$$

При этом отметим, что длину секции информационного и кодового слова алгебраического каскадного сверточного ($n^{(k)}$, $k^{(k)}$) – кода можно выразить через параметры недвоичных блоковых кодов РС следующим образом:

$$\begin{cases} k_k = K_1 \cdot K_0, \\ n_k = N_1 \cdot N_0, \end{cases} \qquad (2)$$

где k_k – длина секции информационного слова ($n^{(k)}$, $k^{(k)}$) – кода; n_k – длина секции кодового слова ($n^{(k)}$, $k^{(k)}$) – кода.

Известно, что способность блокового кода исправлять t ошибок, можно определить как наибольшее число ошибок, которые блоковый код гарантированно может исправить на длине блока кодового слова N [17-19]. При этом минимальное кодовое расстояние блокового кода $D = 2 \cdot t + 1$ [9, 17].

Тогда можно записать: $t_1 = (d_1 - 1)/2$ и $t_0 = (d_0 - 1)/2$, где t_1 и t_0 число исправляемых ошибок алгебраическими сверточными кодами на внешней и внутренней ступени на длине одной секции N_1 и N_0 соответственно [18].

Так как блоковый код РС является оптимальным согласно границы Синглтона [9, 10, 17-19], то на основании выше изложенных рассуждений для сверточных кодов в составе алгебраического каскадного сверточного $(n^{(k)}, k^{(k)})$ – кода справедливы следующие выражения:

$$\begin{cases} d_1 = 2 \cdot t_1 + 1 = N_1 - K_1 + 1, \\ d_0 = 2 \cdot t_0 + 1 = N_0 - K_0 + 1. \end{cases} \quad (3)$$

Таким образом, возможно алгебраическим способом выполнить оценку минимального кодового расстояния d_k алгебраических каскадных сверточных $(n^{(k)}, k^{(k)})$ – кодов.

Рассмотрим пример оценки минимального кодового расстояния d_k алгебраического каскадного сверточного $(n^{(k)}, k^{(k)})$ – ода.

Пример. Предположим, что заданы следующие конечные поля: $GF(2^3)$, $GF(2^4)$ и $GF((2^3)^3)$.

Пусть задан недвоичный блоковый код РС над $GF((2^3)^3)$ который исправляет 7 ошибок и имеет следующие параметры: $N_1 = 2^9 - 1 = 511$, $K_1 = 511 - 2 \cdot 7 = 497$, $D_1 = 2 \cdot 7 + 1 = 15$ и степень порождающего многочлена deg $u(x) = 14$. Тогда, блоковый (511, 497, 15) – код РС над $GF((2^3)^3)$ полностью определяет алгебраический сверточный (n_1, k_1) – код над $GF((2^3)^3)$ в несистематическом виде на внешней ступени. При этом (n_1, k_1) – код имеет порождающий многочлен $g(x)$ степени deg $g(x) = 14$ и следующие параметры: $k^{(1)} = 2$, $n^{(1)} = 3$, $k_1 = 30$, $n_1 = 45$, $v_1 = 28$, $R_1 = 2/3$, $d_1 \geq 15$.

Далее пусть задан код РС над $GF(16)$ исправляющий 6 ошибок, который имеет следующие параметры: $N_0 = 2^4 - 1 = 15$, $K_0 = 3$, $D_0 = 2 \cdot 6 + 1 = 13$ а степень порождающего многочлена deg $w(x) = 12$. Следовательно, (15, 3, 13) – код РС над $GF(2^4)$ определяет алгебраический сверточный (n_0, k_0) – код над $GF(2^4)$ на внутренней ступени каскадного $(n^{(k)}, k^{(k)})$ – кода. Тогда сверточный (n_0, k_0) – код будет иметь параметры: $k^{(0)} = 3$, $n^{(0)} = 4$, $k_0 = 39$, $n_0 = 52$, $v_0 = 36$, $R_0 = 3/4$, $d_0 \geq 13$ и порождающий многочлен $g^*(x)$ степени deg $g^*(x) = 12$.

Таким образом, согласно выражению (1), минимальное кодовое расстояние d_k алгебраического каскадного сверточного $(n^{(k)}, k^{(k)})$ – кода $d_k \geq 195$. При этом длина секции информационного слова $(n^{(k)}, k^{(k)})$ – кода $k_k = 1491$, а длина секции кодового слова $n_k = 7665$.

Из примера видно, что за фиксированное число шагов удается задать недвоичный алгебраический каскадный сверточный $(n^{(k)}, k^{(k)})$ – код с высоким значением минимального кодового расстояния $d_k \geq 195$ и с заранее заданными параметрами компонентных алгебраических сверточных кодов.

В ряде известных схем последовательного каскадного кодирования в качестве компонентных кодов используют сверточные коды, найденные переборным методом. Тогда число всех возможных компонентных сверточных кодов внешней и внутренней ступени, с длиной кодового ограничения v_1 и v_0 соответственно, можно рассчитать следующим образом: $W = q_1^{v_1} + q_0^{v_0}$ [17].

Далее оценивают минимальное кодовое расстояние d найденных сверточных кодов и каскадного кода в целом. Зачастую, при больших длинах кодового ограничения ($v \geq 10$) данная задача практически неразрешима [14].

Например, при значениях $v_1 = 28$, $v_0 = 36$ и $q_1 = 2^9$, $q_0 = 2^4$ число всех возможных компонентных сверточных кодов составляет $W = (2^9)^{28} + (2^4)^{36}$. Очевидно, что перебрать такое число кодирующих устройств (как правило, это схемы, основанные на регистрах сдвига [17]) сверточных кодов в настоящее время затруднительно. Это доказывает, что способ определения сверточных каскадных кодов, основанных на поиске компонентных кодов переборным методом, является малоэффективным.

Применение быстрых алгоритмов вычисления свертки Агарвала-Кули и Винограда [17, 23-25] целесообразно использовать на внешней ступени кодирования недвоичного алгебраического каскадного сверточного кода. Это дает возможность уменьшить число арифметических операций в поле $GF(q^p)$ при вычислении многочлена кодового слова $c(x)$.

Для уменьшения числа арифметических операций в поле $GF(q^m)$ на внутренней ступени рекомендуется использовать быстрый алгоритм Винограда вычисления свертки. Это связано с тем, что на внутренней ступени кодирования, как правило, рекомендуют использование кодов с меньшей длиной кодового ограничения и построенных над полем с меньшей степенью расширения по сравнению с кодами внешней ступени [23-25].

Следовательно, выражения для оценки вычислительной сложности метода кодирования на основе синтеза методов Агарвала-Кули и Винограда можно представить следующим образом [20-22]:

$$\begin{aligned} M(n) &= M(n') \cdot M(n''); \\ A(n) &= n' \cdot A(n'') + M(n'') \cdot A(n'). \end{aligned} \quad (4)$$

В выражении (4) $M(n')$ и $M(n'')$ – мультипликативная сложность вычисления n' и n'' точечных сверток соответственно, а $A(n')$ и $A(n'')$ – аддитивная сложность вычисления n' и n'' точечных сверток, которые определяются вычислительной сложностью метода Винограда, а именно [23-25]:

$$M(n^*) \approx A(n^*) \approx \sum_{j=0}^{z-1} \left[\deg m^{(j)}(x)\right]^2, \quad (5)$$

где $M(n^*)$ и $A(n^*)$ – число арифметических операций умножений и сложений соответственно для одного из измерений [17].

Согласно выражениям вида (4), основной объем вычислений приходится на вычисление n' и n'' точечных сверток. При вычислении сверток выражение (5) является верхней границей числа операций. Так, например, для сверточного кода внешней ступени при $n = 255$ сложность $M(255) = M(15) \cdot M(17) = 6837$. В то же время для вычисления прямым способом кодового слова сверточного кода внешней ступени понадобится $M(255) = 15876$ операций умножений при длине кодового ограничения сверточного кода, равной $1/2n$.

Таким образом, удается сократить вычислительную сложность сверточного кода внешней ступени при $n = 255$ в 2,32 раза. Для сверточного кода внутренней ступени при $n = 15$ сложность $M(15) = M(3) \cdot M(5) = 53$, а при вычислении прямым способом необходимо выполнить 64 арифметических операций умножений. Следовательно, вычислительную сложность сверточного кода внутренней ступени при $n = 15$ удается сократить в 1,21 раза [17].

Выводы

Разработан алгоритм формирования порождающих многочленов внешней и внутренней ступени, отличающийся от известных возможностью однозначно определять алгебраические каскадные сверточные коды с заранее заданными параметрами и произвольными длинами кодовых ограничений за фиксированное количество шагов. Данный алгебраический подход формирования порождающих многочленов внешней и внутренней ступени позволяет уменьшить сложность поиска новых кодовых конструкций и позволит строить помехоустойчивые сверточные коды большой длины для систем связи следующего поколения.

Разработаны алгоритмы кодирования алгебраических каскадных сверточных кодов, отличающийся от известных, новым подходом использования быстрых алгоритмов вычисления циклической свертки на каждой из ступеней. Для нахождения многочленов кодовых слов $c(x)$ и $s(x)$, длины порождающих и информационных многочленов – соизмеримы с длинами циклических сверток на внешней и внутренней ступени соответственно. Разработанные алгоритмы позволяют уменьшить вычислительную сложность процедуры кодирования алгебраических каскадных сверточных кодов на каждой из ступеней.

Для оценки вычислительной сложности алгоритма кодирования на основе синтеза алгоритмов Агарвала-Кули и Винограда представлены соответствующие выражения для компонентных алгебраических сверточных кодов на каждой из ступени.

Литература

1. *Форни Д.* Каскадные коды. М.: Мир, 1970. 207 с.
2. *Forney G.D.* Generalized minimum distance decoding // IEEE transactions on information theory. 1966. № 12, pp. 125-131.
3. *Бакулин М.Г.*, *Крейнделин В.Б.*, *Панкратов Д.Ю.*, *Степанова А.Г.* Анализ эффективности и сложности демодуляции с использованием негауссовской аппроксимации в системах massive MIMO // Информационные процессы. 2022. Т. 22. № 2. С. 77-92.
4. *Крейнделин В.Б.*, *Григорьева Е.Д.* Анализ быстрого алгоритма умножения матриц и векторов для банка цифровых фильтров // T-Comm: Телекоммуникации и транспорт. 2021. Т. 15. № 1. С. 4-10.
5. *Казак П.Г.*, *Шевцов В.А.* Принципы построения энергоэффективной системы сотовой связи и беспроводного широкополосного доступа в Интернет для Арктики // Труды МАИ. 2021. № 118. URL: https://trudymai.ru/published.php?ID=158239
6. *Богданов А.С.*, *Шевцов В.А.* Передача обслуживания по сигналам локальной радионавигационной сети // Труды МАИ. 2011. № 46. URL: https://trudymai.ru/published.php?ID=26041
7. *Богданов А.С.*, *Шевцов В.А.* Выбор способа синхронизации в имитационной модели адаптивных алгоритмов определения местоположения и управления // Труды МАИ. 2015. № 84. URL: https://trudymai.ru/published.php?ID=63136
8. *Бородин В.В.*, *Петраков А.М.*, *Шевцов В.А.* Имитационная модель для исследования адаптивных сенсорных сетей // Труды МАИ. 2018. № 100. URL: https://trudymai.ru/published.php?ID=93398
9. *Блох Э.Л.*, *Зяблов В.В.* Обобщенные каскадные коды. М.: Связь, 1976. 240 с.
10. *Блох Э.Л.*, *Зяблов В.В.* Линейные каскадные коды. М.: Наука, 1982. 229 с.
11. *Зяблов В.В.*, *Шавгулидзе С.А.* Обобщенные каскадные помехоустойчивые конструкции на базе сверточных кодов. М.: Наука, 1991. 207 с.
12. *Морелос-Сарагоса Р.* Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. М.: Техносфера, 2005. 320 с.
13. *Витерби А.Д.* Принцип цифровой связи и кодирования. М.: Радио и связь, 1982. 536 с.
14. *Волков А.С.* Разработка имитационной модели канала с группирующимися ошибками // Труды МАИ: сетевое научное издание. М.: МАИ, 2023. №128. 31 с.
15. *Волков А.С., Солодков А.В., Суслова К.О., Стрельников А.П.* Прототипирование помехоустойчивых кодов в системах связи с кодовым разделением канала // Труды МАИ: сетевое научное издание. М.: МАИ, 2021. №119. 27 с.
16. *Волков А.С., Солодков А.В., Цимляков Д.В.* Разработка программно-аппаратного стенда для исследования характеристик полярных кодов // Труды МАИ: сетевое научное издание. М.: МАИ, 2021. № 116. 22 с.
17. *Blahut R.* Algebraic codes on lines, planes and curves. Cambridge: Cambrige university press, 2008. 543 p.
18. *Берлекэмп Э.* Алгебраическая теория кодирования. М.: Мир, 1971. 477 с.
19. *Питерсон У.*, *Уэлдон Э.* Коды, исправляющие ошибки. М.: Мир, 1976. 576 с.
20. *Johannesson R.*, *Zigangirov K. Sh.* Fundamentals of convolutional coding. New York: IEEE Pess, Inc, 1983. 428 p.
21. *Скляр Б.* Цифровая связь. Теоретические основы и практическое применение. М.: Издат. дом «Вильямс», 2003. 1104 с.
22. *Höst S.*, *Sidorenko V.R.* Some structural properties of cascaded convolutional codes // Algebraic and combinatorial coding theory. 1996, pp. 146-150.
23. *Трифонов П.В.*, *Сидоренко С.В.* Методы быстрого вычисления преобразования Фурье над конечным полем // Проблемы передачи информации. 2003. Т. 39. №3. С. 3-10.
24. *Nussbaumer H.*, *Quandalle P.* Fast computation of discrete Fourier transform using polynomial transform // IEEE ASSP. 1979. Vol. 27. №2, pp. 169-181.
25. *Зяблов В.В.* Оптимизация алгоритмов каскадного декодирования // Проблемы передачи информации. 1973. Т. 9. № 1. С. 26-32.

ALGORITHMS FOR ENCODING ALGEBRAIC NON-BINARY CONCATENATED CONVOLUTIONAL CODES REDUCED COMPLEXITY

Alexey S. Volkov, *Ph.D, associate professor, department of telecommunication systems National Research University of Electronic Technology, Zelenograd, Moscow, Russia,* ***leshvol@mail.ru***

Vitaly B. Kreyndelin, *Doctor of sciences, professor, head of the department of "Theory of Electric Circuits" "Moscow Technical University of Communications and Informatics", Moscow, Russia,* ***v.b.kreindelin@mtuci.ru***

Abstract

To provide high reliability of transmitted information in wired and wireless telecommunication systems and networks, error correction codes are used. It is possible to achieve high reliability with a relatively low complexity of encoding and decoding algorithms through the use of concatenated codes. A cascade code is a code structure based on the sequential connection of several component error correction codes. From a practical point of view, concatenated codes with two coding stages are of greatest interest. One coding stage is called outer, and the other called inner. The paper proposes an algorithm for constructing of generator polynomial of the outer and inner stages, which make it possible to determine algebraic concatenated convolutional codes with pre-determined parameters and variable constraint length in a fixed number of steps. Encoding algorithms for algebraic concatenated convolutional codes have been designed based on fast algorithms for calculating cyclic convolution at each stage and to find polynomials of code words $c(x)$ and $s(x)$ the lengths of generator and information polynomials are matched with the lengths of cyclic convolutions on the outer and internal stage, respectively. It is suggested to use the fast algorithms Agarwal-Cooley and Winograd for computation the convolution at the outer coding stage of a non-binary algebraic concatenated convolutional code. This makes it possible to reduce the number of arithmetic operations in the $GF(q^p)$ field when calculating the codeword polynomial $c(x)$. To reduce the number of arithmetic operations in the $GF(q^m)$ field at the inner stage, it is proposed to use the fast Winograd algorithm for calculating convolution. This is due to the fact that it's recommended at the inner coding stage to choose codes with a short code constraint length and over smaller fields, compared to codes at the outer stage. To estimate the computational complexity of the proposed encoding algorithm based on the synthesis of the Agarwal-Cooley and Winograd algorithms, the analytic expressions for component algebraic convolutional codes at each stage are presented.

Keywords: *error-correction codes, convolutional codes, construction of convolutional codes, computational complexity, generator polynomial, concatenated codes.*

References

1. D. Forni, "Concatenated Codes," Moscow: Mir, 1970. 207 p.
2. G.D. Forney, "Generalized minimum distance decoding," *IEEE transactions on information theory.* 1966. No. 12, pp. 125-131.
3. M.G. Bakulin, V.B., Kreyndelin, D.Yu. Pankratov, A.G. Stepanova, "Analysis of the efficiency and complexity of demodulation using non-Gaussian approximation in a massive MIMO," *Informatsionnye processy*. 2022. Vol. 22. No.2, pp. 77-92.
4. V.B. Kreyndelin, Ye.D. Grigor'yeva, "Analysis of a fast algorithm for matrix and vector multiplication for a digital filters bank," T-Comm. 2021. Vol. 15. No. 1, pp. 4-10.
5. P.G. Kazak, V.A. Shevtsov, "Principles for building an energy-efficient cellular communication system and wireless broadband Internet access for the Arctic area," *Trudy MAI.* 2021. No.118. URL: https://trudymai.ru/published.php?ID=158239
6. A.S. Bogdanov, V.A. Shevtsov, "Transfer of service using local radio navigation network signals," *Trudy MAI*. 2011. No.46. URL: https://trudymai.ru/eng/published.php?ID=26041
7. A.S. Bogdanov, V.A. Shevtsov, "Synchronization in the simulation model of adaptive algorithms for positioning and control," *Trudy MAI*. 2015. No.84. URL: https://trudymai.ru/eng/published.php?ID=63136
8. V.V. Borodin, A.M. Petrakov, V.A. Shevtsov, "Simulation model for adaptive sensor networks studies," *Trudy MAI*. 2018. No.100. URL: https://trudymai.ru/eng/published.php?ID=93398
9. E.L. Blokh, V.V. Zyablov, "Generalized concatenated codes," Moscow: Svyaz', 1976. 240 p.
10. E.L. Blokh, V.V. Zyablov, "Linear concatenated codes," Moscow: Nauka, 1982. 229 p.
11. V.V. Zyablov, S.A. Shavgulidze, "Generalized concatenated modulation and coding schemes based on convolution codes," Moscow: Nauka, 1991. 207 p.
12. R. Morelos-Saragosa, "The art of error correcting coding," Moscow: Tekhnosfera, 2005. 320 p.
13. A.D. Viterbi, "Principles of digital communication and coding," Moscow: Radio i svyaz', 1982. 536 p.
14. A.S. Volkov, "The development of simulation model of channel with burst error arrays," *Trudy MAI: setevoye nauchnoye izdaniye*. Moscow: MAI, 2023. No. 128. 31 p.
15. A.S. Volkov, A.V. Solodkov, K.O. Suslova, A.P. Strel'nikov, "Prototyping error correction codes in communication systems with channels code division," *Trudy MAI: setevoye nauchnoye izdaniye*. Moscow: MAI, 2021. No. 119. 27 p.
16. A.S. Volkov, A.V. Solodkov, D.V. Tsimlyakov, "Development of a software and hardware stand for studying the characteristics of polar codes," *Trudy MAI: setevoye nauchnoye izdaniye*. Moscow: MAI, 2021. No. 116. 22 p.
17. R. Blahut, "Algebraic codes on lines, planes and curves," Cambridge: Cambrige university press, 2008. 543 p.
18. E. Berlekemp, "Algebraic coding theory," Moscow: Mir, 1971. 477 p.
19. U. Piterson, E. Ueldon, "Error-correcting codes," Moscow: Mir, 1976. 576 p.
20. R. Johannesson, K.Sh. Zigangirov, "Fundamentals of convolutional coding," New York: IEEE Pess, Inc, 1983. 428 p.
21. B. Sklyar, "Digital communications: fundamentals and applications," Moscow: Izdat. dom "Vil'yams", 2003. 1104 p.
22. S. Host, V.R. Sidorenko, "Some structural properties of cascaded convolutional codes," *Algebraic and combinatorial coding theory*. 1996, pp. 146-150.
23. P.V. Trifonov, S.V. Fedorenko, "Methods of fast Fourier transform computation over finite field," *Problemy peredachi informatsii*. 2003. Vol. 39. No.3, pp. 3-10.
24. H. Nussbaumer, P. Quandalle, "Fast computation of discrete Fourier transform using polynomial transform," *IEEE ASSP*. 1979. Vol. 27. No.2, pp. 169-181.
25. V.V. Zyablov, "Optimization of concatenated decoding algorithms," *Problemy peredachi informatsii*. 1973. Vol. 9. No. 1, pp. 26-32.

Information about authors:

Alexey S. Volkov, *Ph.D, associate professor, department of telecommunication systems National Research University of Electronic Technology, Zelenograd, Moscow, Russia*

Vitaly B. Kreyndelin, *Doctor of sciences, professor, head of the department of "Theory of Electric Circuits" "Moscow Technical University of Communications and Informatics", Moscow, Russia*