УДК 621.391

А.С. Волков

Украинская государственная академия железнодорожного транспорта, Харьков

МЕТОД ЧАСТОТНОГО КОДИРОВАНИЯ СВЕРТОЧНЫХ КОДОВ УМЕНЬШЕННОЙ СЛОЖНОСТИ НА ОСНОВЕ БПФ-АЛГОРИТМА ГУДА-ТОМАСА

Предложен метод помехоустойчивого кодирования данных алгебраическими сверточными кодами в частотной области с применением быстрого преобразования Фурье Гуда-Томаса в конечных полях. Показано, что разработанный метод позволяет уменьшить вычислительную сложность процедур кодирования данных алгебраическими сверточными кодами в частотной области.

Ключевые слова: *сверточные коды, преобразование Фурье, БПФ-алгоритм, алгебраические помехоустойчивые коды.*

Введение

Постановка проблемы в общем виде и анализ литературы. В настоящее время наблюдается интенсивное развитие методов помехоустойчивого кодирования, среди которых можно выделить два основных направления: методы блокового и сверточного кодирования [1, 4].

Известно, что большей эффективностью обладают сверточные коды [1, 4, 6]. При этом повышение эффективности допускается при использовании помехоустойчивых кодов большой длины (с большой длиной кодового ограничения), что следует из теоремы Шеннона [3, 4].

Среди известных методов построения помехоустойчивых кодов, допускающих большие длины кодового ограничения, можно выделить так называемые алгебраические методы построения сверточных кодов (алгебраические сверточные коды) [4, 5, 7]. Недостатком известных алгебраических сверточные кодов является высокая вычислительная сложность процедур кодирования и декодирования при больших длинах кодового ограничения [1 – 5, 10].

При этом под вычислительной сложностью понимают число арифметических операций умножений и сложений в конечном поле GF(2) или GF(q^m), где $q = 2^p$, p – целое число.

Уменьшение вычислительной сложности процедур (алгоритмов) кодирования и декодирования алгебраических сверточных кодов возможно при переходе в частотную область [2, 7, 9 – 10].

Представление алгебраических сверточных кодов реализуется на основе применения преобразования Фурье в конечном поле.

Цель статьи – разработка метода кодирования данных алгебраическими сверточными кодами в частотной области уменьшенной сложности на основе быстрого преобразования Фурье Гуда-Томаса.

Основной материал

Пусть на вход кодирующего устройства сверточного кода поступает входная (информационная) последовательность полубесконечной длины. Представим входную последовательность в виде вектора B бесконечной длины: $B = (B_0, B_1, B_2, \dots)$. При этом компоненты вектора B удовлетворяют условиям: $B_i \in M$, $|M| \geq |GF(q)|$, $M \in GF(q^m)$, $i = 0, 1, 2, \dots$ [4, 7].

Запишем вектор B в виде полубесконечной последовательности секций конечной длины следующим образом:

$$B = (B_0, B_1, B_2, \dots, B_{K_0-1}) \cup \cup (B_{K_0}, B_{K_0+1}, B_{K_0+2}, \dots B_{2K_0-1}) \cup \cup (B_{2K_0}, B_{2K_0+1}, B_{2K_0+2}, \dots B_{3K_0-1}) \cup \dots, \quad (1)$$

где $K_0 = N_0 - 2 \cdot t_0$; $N_0 = q^m - 1$; t_0 – кратность исправляемых ошибок алгебраическим сверточным кодом [1 – 5, 7]; m – целое число.

Метод частотного кодирования сверточных кодов предусматривает введение в каждую секцию (вектор) информационной последовательности $2 \cdot t_0$ проверочных символов (частот) [1, 3, 5, 7]. Последовательность проверочных частот, представляющих собой $2 \cdot t_0$ компонент вектора, введем на младшие позиции каждой секции вектора B. Тогда длина каждой секции полубесконечного вектора B увеличится на $2 \cdot t_0$ компонент и будет удовлетворять длине [3, 4, 7]:

$$N_0 = 2 \cdot t_0 + K_0 = q^m - 1, \quad (2)$$

где m – целое число.

Следовательно, кодовое слово алгебраического сверточного кода в частотной области можно представить в виде полубесконечного вектора C следующим образом:

$$C = (P_0, P_1, P_2, \dots, P_{2t_0-2}, P_{2t_0-1}, B_{N_0-K_0}, B_{N_0-K_0+1}, B_{N_0-K_0+2}, \dots, B_{N_0-2}, B_{N_0-1}) \cup$$

$$\cup(P_{N_0}, P_{N_0+1}, P_{N_0+2}, ..., P_{N_0+2t_0-2}, P_{N_0+2t_0-1},$$
$$B_{2N_0-K0}, B_{2N_0-K_0+1}, B_{2N_0-K_0+2}, ..., B_{2N_0-2},$$
$$B_{2N_0-1}) \cup (P_{2N0}, P_{2N_0+1}, P_{2N_0+2}, ..., P_{2N_0+2t_0-2}, \quad (3)$$
$$P_{2N_0+2t_0-1}, B_{3N_0-K0}, B_{3N_0-K_0+1}, B_{3N_0-K_0+2},$$
$$, ..., B_{3N_0-2}, B_{3N_0-1}) \cup \ldots .$$

Последовательность $2 \cdot t_0$ проверочных частот кодового слова алгебраического сверточного кода в частотной области представляет собой последовательность нулевых символов [1, 5 – 7].

Тогда выражение (3) перепишем следующим образом:

$$C = (0,0,0,...,0,0,B_{N_0-K_0}, B_{N_0-K_0+1},$$
$$B_{N_0-K_0+2}, ..., B_{N_0-2}, B_{N_0-1}) \cup$$
$$\cup(0,0,0,...,0,0,B_{2N_0-K0}, B_{2N_0-K_0+1}, \quad (4)$$
$$B_{2N_0-K_0+2}, ..., B_{2N_0-2}, B_{2N_0-1}) \cup$$
$$(0,0,0,...,0,0,B_{3N_0-K0}, B_{3N_0-K_0+1},$$
$$B_{3N_0-K_0+2}, , ..., B_{3N_0-2}, B_{3N_0-1}) \cup \ldots .$$

Следовательно, выражение (4) является алгебраическим представлением кодового слова бесконечной длины алгебраического сверточного кода в частотной области. При этом: $N_0 = q^m - 1$; $2 \cdot t_0 = N_0 - K_0$; $B_i \in M$, $|M| \geq |GF(q)|$, $M \in GF(q^m)$; $i = 0, 1, 2, \ldots$.

Тогда многочлен C(x) кодового слова полубесконечной длины алгебраического сверточного кода в частотной области над $GF(q^m)$ можно записать:

$$C = B_{N_0-K_0} x^{N_0-K_0} + B_{N_0-K_0+1} x^{N_0-K_0+1} +$$
$$+B_{N_0-K_0+2} x^{N_0-K_0+2} + ... + B_{N_0-2} x^{N_0-2} +$$
$$+B_{N_0-1} x^{N_0-1} + B_{2N_0-K0} x^{2N_0-K0} +$$
$$+B_{2N_0-K_0+1} x^{2N_0-K_0+1} + B_{2N_0-K_0+2} x^{2N_0-K_0+2} +$$
$$+ ... + B_{2N_0-2} x^{2N_0-2} + B_{2N_0-1} x^{2N_0-1} +$$
$$+B_{3N_0-K0} x^{3N_0-K0} + B_{3N_0-K_0+1} x^{3N_0-K_0+1} +$$
$$+B_{3N_0-K_0+2} x^{3N_0-K_0+2} +$$
$$+ ... + B_{3N_0-2} x^{3N_0-2} + B_{3N_0-1} x^{3N_0-1} + \ldots .$$

Далее метод частотного кодирования сверточных кодов предполагает выполнение процедуры перехода из частотной области во временную [5 – 7]. Для этого необходимо воспользоваться обратным преобразованием Фурье в конечном поле и применить его для каждой секции кодового слова сформированного в частотной области.

Обратное преобразование Фурье каждой секции выполняется на длине $N_0 = q^m - 1$ над полем $GF(q^m)$. Пусть α – примитивный элемент поля $GF(q^m)$ [3, 5 – 7]. Тогда обратное преобразование Фурье над полем $GF(q^m)$ одной секции кодового слова бесконечной длины алгебраического сверточного кода в частотной области возможно записать [3, 5]:

$$c_i = \frac{1}{N_0} \sum_{j=0}^{N_0-1} \alpha^{-i \cdot j} \cdot B_j , \quad (5)$$

где c_i – компонента вектора кодового слова во временной области; $c_i \in GF(q^m)$; $i = 0, \ldots, N_0 - 1$.

Таким образом, выражение (5) позволяет вычислить все компоненты c_i над $GF(q^m)$ одной секции кодового слова (вектора) полубесконечной длины алгебраического сверточного кода заданного в частотной области. При этом компоненты c_i, над $GF(q^m)$ рассматриваются как компоненты вектора во временной области [8, 4 – 7]. Тогда одну секцию c_v во временной области вектора кодового слова алгебраического сверточного кода, заданного в частотной области, можно представить следующим образом:

$$c_v = (c_0, c_1, c_2, ..., c_{N_0-2}, c_{N_0-1}) , \quad (6)$$

где $c_i \in GF(q^m)$; $N_0 = q^m - 1$; $v = 0, 1, 2, 3, \ldots$.

Выражение (6) является одномерным обратным преобразованием Фурье и имеет n^2 умножений и n^2 сложений в конечном поле $GF(q^m)$ [4, 5, 7, 10].

Если длина N_0 одной секции кодового слова алгебраического сверточного кода разлагается на множители $N_0 = N_0' \cdot N_0''$, где N_0' и N_0'' являются взаимно простыми числами, то возможно применение обратного алгоритма быстрого преобразования Фурье (БПФ-алгоритма) Гуда-Томаса, который является двумерным обратным преобразованием Фурье [5, 7, 8 – 10].

Для этого необходимо выполнить определение пары входных индексов [3, 5]:

$$i' = i \ (\mathrm{mod}\ N_0'); \quad (7)$$
$$i'' = i \ (\mathrm{mod}\ N_0''), \quad (8)$$

где $i = 0, \ldots, N_0 - 1$; $N_0 = 2 \cdot t_0 + K_0 = q^m - 1$.

Китайская теорема об остатках для целых чисел [5] предполагает существование целых чисел n' и n'' для которых справедливо следующее соотношение [3, 5, 6]:

$$i = i' \cdot n'' \cdot N_0'' + i'' \cdot n' \cdot N_0' (\mathrm{mod}\, N_0) , \quad (9)$$

где $n' \cdot N_0' + n'' \cdot N_0'' = 1$.

Тогда пара выходных индексов определяется:

$$j' = n'' \cdot j (\mathrm{mod}\, N_0') ; \quad (10)$$
$$j'' = n' \cdot j (\mathrm{mod}\, N_0'') , \quad (11)$$

где $j = 0, \ldots, N_0 - 1$.

Следовательно, по известной паре выходных индексов (j', j'') восстановление индекса j осуществляется следующим образом:

$$j = N_0'' \cdot j' + N_0' \cdot j'' (\mathrm{mod}\, N_0) . \quad (12)$$

Согласно переиндексации, соответствующей выражениям (7) – (12), обратный БПФ-алгоритм Гуда-Томаса над полем $GF(q^m)$ одной секции кодового слова полубесконечной длины алгебраического сверточного кода заданного в частотной области можно записать [3, 5, 8 – 11]:

$$c_{i',i''} = \frac{1}{N_0} \sum_{j'=0}^{N_0'-1} \sum_{j''=0}^{N_0''-1} \beta^{i' \cdot j'} \cdot \gamma^{i'' \cdot j''} \cdot B_{j',j''} , \quad (13)$$

где $\beta = \alpha^{-n''\cdot(N_0'')^2}$ – элемент, порядок которого равен N_0'; $\gamma = \alpha^{-n'\cdot(N_0')^2}$ – элемент, порядок которого равен N_0''.

Далее, согласно переиндексации формируется секция c_v во временной области вида (6) вектора кодового слова алгебраического сверточного кода заданного в частотной области. При этом выражение (13) является двумерным обратным БПФ-алгоритмом Гуда-Томаса в конечном поле [1, 3, 6].

Выполним преобразование вида (13) для каждой секции кодового слова алгебраического сверточного кода в частотной области. Тогда справедливо записать вектор кодового слова c во временной области алгебраического сверточного кода заданного в частотной области над $GF(q^m)$ следующим образом:

$$\begin{aligned} c = (&c_0, c_1, c_2, ..., c_{N_0-2}, c_{N_0-1}, c_{N0}, c_{N_0+1}, \\ &c_{N_0+2}, ..., c_{2N_0-2}, c_{2N_0-1}, c_{2N0}, c_{2N_0+1}, \\ &c_{2N_0+2}, ..., c_{3N_0-2}, c_{3N_0-1}, ...), \end{aligned} \tag{14}$$

где $c_i \in GF(q^m)$; $N_0 = q^m - 1$; $i = 0, 1, 2, 3 \ldots$.

Сопоставим индексы компонент вектора c над $GF(q^m)$ выражения (14) в соответствие коэффициентам многочлен c(x) с соответствующими степенями. Тогда многочлен c(x) кодового слова алгебраического сверточного кода заданного в частотной области над $GF(q^m)$ бесконечной степени запишем:

$$\begin{aligned} c(x) = &c_0 + c_1 x + c_2 x^2 + ... + c_{N_0-2} x^{N_0-2} + \\ &c_{N_0-1} x^{N_0-1} + c_{N_0} x^{N_0} + c_{N_0+1} x^{N_0+1} + \\ &+ c_{N_0+2} x^{N_0+2} + ... + c_{2N_0-2} x^{2N_0-2} + \\ &+ c_{2N_0-1} x^{2N_0-1} + c_{2N_0} x^{2N_0} + \\ &+ c_{2N_0+1} x^{2N_0+1} + c_{2N_0+2} x^{2N_0+2} + ... + \\ &+ {}_{3N_0-2} x^{3N_0-2} + c_{3N_0-1} x^{3N_0-1} + ..., \end{aligned} \tag{15}$$

где $c_i \in GF(q^m)$; $N = q^m - 1$; $i = 0, 1, 2, 3, \ldots$.

Следовательно, одна секция вектора кодового слова вида (6) соответствует многочлену кодового слова степени не выше $N_0 - 1$:

$$\begin{aligned} c_v(x) = &c_0 + c_1 x + c_2 x^2 + \\ &+ ... + c_{N_0-2} x^{N_0-1}, c_{N_0-1} x^{N_0-1}, \end{aligned} \tag{16}$$

где $c_i \in GF(q^m)$; $N_0 = q^m - 1$; $v = 0, 1, 2, 3, \ldots$.

Тогда многочлен c(x) кодового слова алгебраического сверточного кода заданного в частотной области над $GF(q^m)$ бесконечной степени перепишем следующим образом:

$$c(x) = \sum_{v=0}^{\infty} m_v(x) \cdot x^{v \cdot N_0} . \tag{17}$$

При вычислении одной секции длины N_0 кодового слова алгебраического сверточного кода заданного в частотной области над $GF(q^m)$ определим число умножений $M(N_0)$ и число сложений $A(N_0)$ следующими выражениями [3, 5]:

$$\begin{aligned} M(N_0) &= N_0' \cdot M(N_0'') + \\ &+ N_0'' \cdot M(N_0') = N_0(N_0' + N_0''); \\ A(N_0) &= N_0' \cdot A(N_0'') + \\ &+ N_0'' \cdot A(N_0') = N_0(N_0' + N_0''). \end{aligned} \tag{18}$$

Если длину N_0 одной секции кодового слова алгебраического сверточного кода после разложения на произведение взаимно простых чисел удается разложить еще на множители, то на первом шаге можно воспользоваться обратным БПФ-алгоритмом Гуда-Томаса, далее применить обратный БПФ-алгоритм Кули-Тьюки [5], а затем каждое измерение вычислить при помощи малого обратного БПФ-алгоритма Винограда [3, 5].

На рис. 1, а, б представлены графики, отражающие результаты оценки вычислительной сложности алгоритмов кодирования сверточных кодов заданных в частотной области над $GF(2^m)$ с применением обратного БПФ-алгоритма Гуда-Томаса. На рис. 1, в, г представлены результаты оценки вычислительной сложности по числу умножений и сложений соответственно алгоритмов кодирования сверточных кодов во временной и частотной области над GF(2).

Результаты оценки вычислительной сложности известного и предлагаемого алгоритмов кодирования сверточных кодов в частотной области для поля $GF(2^m)$ представлены в виде графиков (рис. 2). Отметим, что здесь и далее при оценке вычислительной сложности известного частотного алгоритма будем учитывать, что в его основе БПФ-алгоритм Гуда-Томаса. Графики оценки числа двоичных операций умножений и сложений представлены на рис. 3.

На графиках (рис. 1 – 3) введены следующие обозначения: $Mt(N_0)$ и $At(N_0)$ – число арифметический операций умножений и сложений известного метода кодирования сверточных кодов во временной области; $MF(N_0)$ и $AF(N_0)$ – число арифметический операций умножений и сложений известного метода кодирования сверточных кодов в частотной области; $MGT(N_0)$ и $AGT(N_0)$ – число арифметический операций умножений и сложений предлагаемого метода частотного кодирования сверточных кодов уменьшенной сложности на основе БПФ-алгоритма Гуда-Томаса.

Выводы

Предлагаемый метод частотного кодирования сверточных кодов уменьшенной сложности на основе БПФ-алгоритма Гуда-Томаса обладает меньшей вычислительной сложностью, чем известный метод сверточных кодов во временной области (рис. 1, 2).

С увеличением длины секции кодового слова N_0 вычислительная сложность предложенного метода не имеет столь резкого роста, как существующий метод во временной области (рис. 1). При каждом увеличении значения N_0 предложенный метод позволяет сократить число арифметических операций

умножений и сложений в поле GF(2^m) и GF(2). Так, например, при N_0 = 63 метод частотного кодирования сверточных кодов уменьшенной сложности на основе БПФ-алгоритма Гуда-Томаса позволяет сократить число арифметических операций умножений и сложений в 3,7 раза.

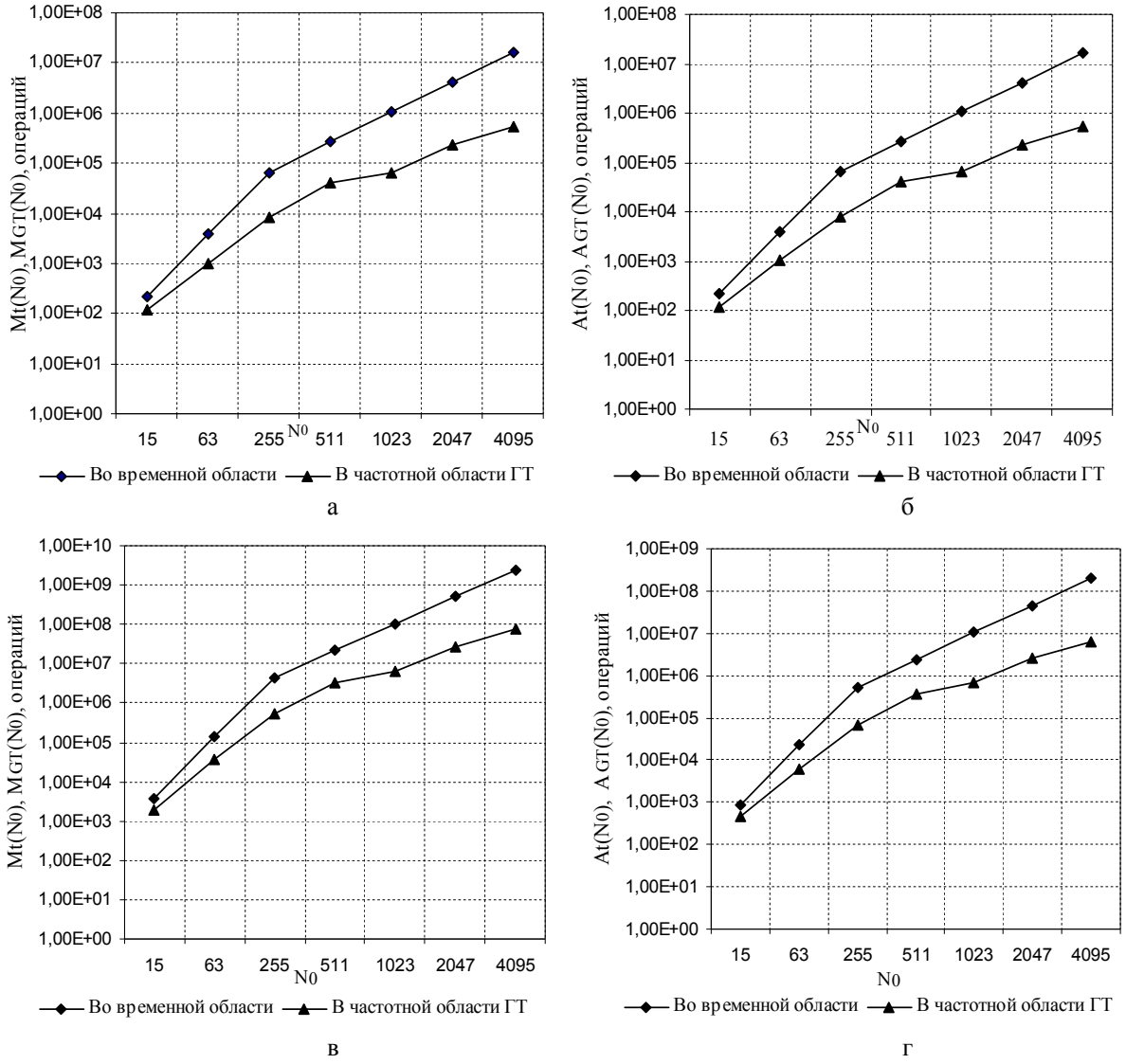

Рис. 1. Сравнение вычислительной сложности алгоритмов кодирования сверточных кодов во временной и частотной области над GF(2^m) на основе БПФ-алгоритма Гуда-Томаса

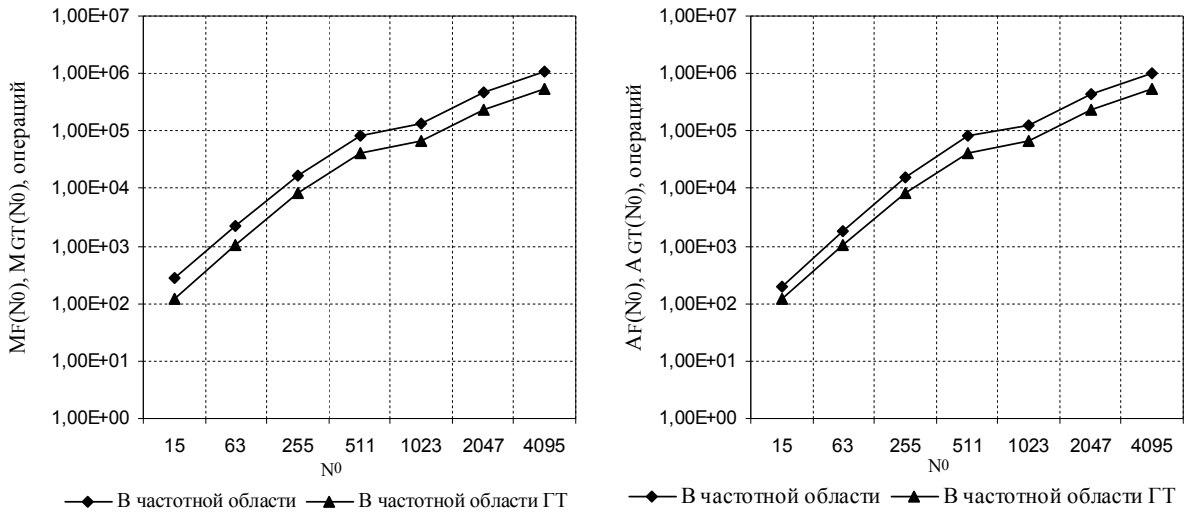

Рис. 2. Сравнение вычислительной сложности известного и предлагаемого алгоритмов кодирования сверточных кодов в частотной области над GF(2^m)

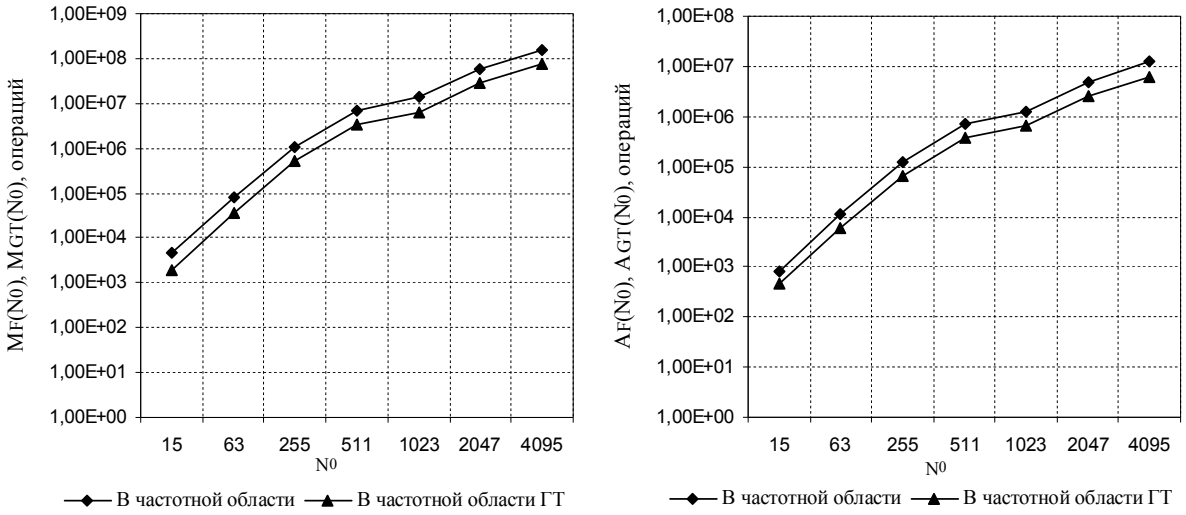

Рис. 3. Сравнение вычислительной сложности известного и предлагаемого алгоритмов кодирования сверточных кодов в частотной области над GF(2)

Метод частотного кодирования сверточных кодов уменьшенной сложности на основе БПФ-алгоритма Гуда-Томаса позволяет снизить вычислительную сложность в 2 раза по сравнению с известным алгоритмом частотного кодирования (рис. 2, 3). При этом для всех исследуемых значений N_0 уменьшение числа умножений и числа сложений для полей $GF(2^m)$ и GF(2) остается неизменным.

Список литературы

1. Blahut R. Algebraic codes on lines, planes and curves / R. Blahut. – Cambridge: Cambrige university press, 2008. – 543 p.

2. Carrasco R.A. Non-binary error control coding for wireless communication and data storage / R.A. Carrasco, M. Johnston. – Chichester: John Wiley & Sons Ltd., 2008. – 303 p.

3. Blahut R. Transform techniques for error control codes / R. Blahut // IBM J. research and development. – 1979. – Vol. 23, №3. – P. 299-315.

4. Данько Н.И. Алгебраические сверточные коды: учеб. пособие / Н.И. Данько, С.П. Евсеев, А.А. Кузнецов, П.Ф. Поляков, С.И. Приходько. – Х.: УкрГАЖТ, 2007. – 238 с.

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

6. Муттер В.М. Основы помехоустойчивой телепередачи информации / В.М. Муттер. – Л.: Энергоатомиздат. Ленингр. отд-ние, 1990. – 288 с.

7. Волков А.С. Метод построения и кодирования алгебраических сверточных кодов в частотной области на основе быстрого преобразования Фурье Кули-Тьюки / А.С. Волков // Інформаційно-керуючі системи на залізничному транспорті. – Х.: УкрДАЗТ. – 2013. – №4. – С. 37-41.

8. Wang Y. Fast algorithm for the Fourier transform over finite fields and its VLSI implementation / Y. Wang, X. Zhu // IEEE J. on selected areas in communications. – 1988. – Vol. 6, №3. – P. 572-577.

9. Auslander L. New algorithms for the multidimensional discrete Fourier transform / L. Auslander, E. Feig, S. Winograd // IEEE ASSP. – 1983. – Vol. 31, №2. – P. 388-403.

10. Justesen J. On the complexity of decoding Reed-Solomon codes / J. Justesen // IEEE transactions on information theory. – 1976. – Vol. 22, №2. – P. 237-238.

11. Fedorenko S.V. Finding roots of polynomials over finite fields / S.V. Fedorenko, P.V. Trifonov // IEEE transactions on communications. – 2002. – Vol. 50, №11. – P. 1709-1711.

Поступила в редколлегию 23.11.2013

Рецензент: д-р техн. наук, проф. С.И. Приходько, Украинская государственная академия железнодорожного транспорта, Харьков.

МЕТОД ЧАСТОТНОГО КОДУВАННЯ ЗГОРТКОВИХ КОДІВ ЗМЕНШЕНОЇ СКЛАДНОСТІ НА ОСНОВІ ШПФ-АЛГОРИТМУ ГУДА-ТОМАСА

О.С. Волков

Запропоновано метод завадостійкого кодування даних алгебраїчними згортковими кодами у частотній області з використанням швидкого перетворення Фур'є Гуда-Томаса у кінцевих полях. Показано, що розроблений метод дозволяє зменшити обчислювальну складність процедур кодування даних алгебраїчними згортковими кодами у частотній області.

Ключові слова: *згорткові коди, перетворення Фур'є, ШПФ-алгоритм, алгебраїчні завадостійкі коди.*

THE METHOD OF FREQUENCY CODING OF THE REDUCED COMPLEXITY OF CONVOLUTIONAL CODES BASED ON FFT ALGORITHM GOOD-THOMAS

A.S. Volkov

We propose a method of algebraic error-correcting coding data convolutional codes in the frequency domain using a fast Fourier transform Good-Thomas in the finite fields. It is shown that the method allows to reduce the computational complexity of encoding data algebraic procedures convolutional codes in the frequency domain.

Keywords: *convolutional codes, Fourier transform, FFT algorithm, algebraic error correcting codes.*