УДК 621.391

С.И. Приходько, А.С. Волков

Украинская государственная академия железнодорожного транспорта, Харьков

ВЫЧИСЛИТЕЛЬНАЯ СЛОЖНОСТЬ МЕТОДОВ КОДИРОВАНИЯ И ДЕКОДИРОВАНИЯ АЛГЕБРАИЧЕСКИХ КАСКАДНЫХ СВЕРТОЧНЫХ КОДОВ ВО ВРЕМЕННОЙ И ЧАСТОТНОЙ ОБЛАСТИ

Предлагаются аналитические оценки вычислительной сложности методов кодирования и декодирования алгебраических каскадных сверточных кодов во временной и частотной области. Показано, что методы кодирования и декодирования алгебраических каскадных сверточных кодов в частотной области на основе БПФ-алгоритмов Кули-Тьюки и Гуда-Томаса позволяют уменьшить вычислительную сложность.

Ключевые слова: *помехоустойчивое кодирование, сверточные коды, каскадные коды, БПФ-алгоритм, преобразование Фурье, вычислительная сложность*

Введение

Постановка проблемы в общем виде и анализ литературы. Перспективным направлением теории помехоустойчивого кодирования является разработка методов построения, кодирования и декодирования кодов большой длины. Наибольший интерес в данном направлении вызывают каскадные коды, представляющие собой кодовую конструкцию, основанную на последовательном соединении нескольких компонентных помехоустойчивых кодов [1, 2].

В настоящее время известен класс обобщенных каскадных кодов, в котором предусмотрено разложение кода внутренней ступени на подкоды, соответствующие подкодам внешней ступени каскадного кода [2]. С практической точки зрения, каскадные коды с двумя ступенями кодирования являются наиболее важными [2, 5].

На внешней и внутренней ступени широкое применение нашли блоковые (РС, БЧХ, – коды) и сверточные коды. Комбинация различных компонентных коды в составе каскадного кода позволяет получить новые классы кодов [6]. Следовательно, построение каскадного кода определяется выбором компонентных кодов.

В то же время известно, что при фиксированных длинах характеристики сверточных кодов превосходят характеристики блоковых кодов [2, 3].

Таким образом, разработка методов построения, кодирования и декодирования каскадных сверточных кодов является актуальной научной задачей.

С ростом длины кодового ограничения компонентных сверточных кодов внешней и внутренней ступени сложность методов кодирования и декодирования существенно возрастает, что сдерживает их практическую реализацию.

Под сложностью в данной работе будем понимать число арифметических операций сложений и умножений, которое необходимо выполнить для вычисления кодового слова или для его декодирования на некоторой конечной длине блока (секции) компонентного сверточного кода [3, 4].

Обозначим M(n) – число арифметических операций умножений (число операций мультипликативной группы) и A(n) – число арифметических операций сложений (число операций аддитивной группы) алгоритмов кодирования и декодирования каскадных сверточных кодов [3, 4]. Оценка вычислительной сложности производится для наихудшего случая (верхние границы).

В работах [7 – 11] предложены методы кодирования и декодирования каскадных сверточных кодов во временной и частотной области с компонентными алгебраическими сверточными кодами на основе методов Агарвала-Кули и Винограда, Кули-Тьюки и Гуда-Томаса соответственно [3, 4]. При этом удается достигать больших длин кодового ограничения высокой корректирующей способности кодов [7 – 11]. Однако оценки вычислительной сложности методов кодирования и декодирования алгебраических каскадных сверточных кодов во временной и частотной области в известных работах отсутствуют. При этом данные оценки представляют большой интерес с теоретической и практической точки зрения.

Цель статьи – Оценка вычислительной сложности методов кодирования и декодирования алгебраических каскадных сверточных кодов во временной и частотной области основанных на синтезе методов быстрого вычисления свертки Агарвала-Кули и Винограда, а также применения алгоритмов быстрого преобразования Фурье Кули-Тьюки и Гуда-Томаса в полях Галуа.

Основной материал

Алгоритм, реализующий процедуру кодирования на внешней и внутренней ступени каскадного сверточного кода, представляет собой вычисление линейной свертки (в общем случае бесконечной длины) [3, 4, 9, 10]. При этом длина регистра сдвига

сверточных кодов (память кодера) определяется степенью порождающего многочлена, которая может возрастать до значения n. Тогда при равенстве длины входной последовательности длине регистра сдвига, вычислительную сложность известных алгоритмов кодирования можно оценить следующим выражением [3, 4, 7]:

$$M(n) \approx A(n) \approx (\deg g(x)+1)\cdot(\deg b(x)+1) \approx n^2, \quad (1)$$

где $\deg g(x)$ и $\deg b(x)$ – степени порождающего и информационного многочлена соответственно.

Синтез методов Агарвала-Кули и Винограда позволяет снизить вычислительную сложность метода кодирования [9, 10].

Пусть длина кодового слова n кодирования разлагается на $n = n' \cdot n''$, причем n' и n'' – взаимно просты. Тогда возможно применение алгоритма Агарвала-Кули, благодаря которому можно преобразовать одномерную циклическую свертку в двумерную (в общем случае в многомерную). На следующем этапе метода кодирования рассматривается применение быстрого алгоритма Винограда вычисления одномерной циклической свертки вдоль каждого из двух измерений [9, 10].

Таким образом, выражения для оценки вычислительной сложности метода кодирования на основе синтеза методов Агарвала-Кули и Винограда можно представить следующим образом [3, 4]:

$$\begin{aligned} M(n) &= M(n')\cdot M(n''); \\ A(n) &= n'\cdot A(n'') + M(n'')\cdot A(n'). \end{aligned} \quad (2)$$

В выражении (9) 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 [3, 4]:

$$M(n^*) \approx A(n^*) \approx \sum_{k=1}^{s} \left[\deg d_k(x)\right]^2, \quad (3)$$

где M(n*) и A(n*) – число арифметических операций умножений и сложений для одного из измерений; $d_k(x)$ – множество k многочленов, полученных в результате разложения d(x) [3, 4, 9].

При этом $\deg d_k(x)$ зависит от выбора d(x) [3, 4, 9].

Согласно выражениям вида (2), основной объем вычислений приходится на вычисление n' и n'' точечных сверток. При вычислении сверток выражение (3) является верхней границей числа операций. Так, например, для сверточного кода внешней ступени при n = 255 сложность M(255) = M(15) · M(17) = 6837. В то же время для вычисления прямым способом кодового слова сверточного кода внешней ступени понадобится M(255) = 15876 операций при длине кодового ограничения сверточного кода, равной ½ n. Таким образом, удается сократить вычислительную сложность сверточного кода внешней ступени при n = 255 в 2,32 раза.

Следовательно, можно сделать вывод, что применение методов быстрого вычисления свертки Агарвала-Кули и Винограда, можно уменьшить число арифметических операций метода кодирования алгебраических каскадных сверточных кодов во временной области.

Недостатком данного метода кодирования на основе синтеза методов Агарвала-Кули и Винограда является то, что уменьшение число арифметических операций возможно только при реализации процедур кодирования.

Для оценки вычислительной сложности метода алгебраического декодирования сверточных кодов внешней и внутренней ступени каскадного кода рассмотрим несколько этапов.

На первом этапе метода декодирования вычисляется синдромная последовательность одной секции длины n кодового слова сверточного кода принятого декодером. Сложность данного вычисления составляет [3, 14]:

$$M_s(n) \approx A_s(n) \approx 2\cdot t(n-1), \quad (4)$$

где t – число исправляемых сверточным кодом ошибок.

На втором этапе метода декодирования сверточных кодов выполняется рекуррентная процедура Берлекэмпа – Месси [3, 5, 6, 13], вычислительная сложность которой определяется следующим выражением [3]:

$$M_{BM}(n) = A_{BM}(n) = 6\cdot t^2. \quad (5)$$

Далее, для определения корней многочлена локаторов ошибок, выполняется процедура Ченя [3, 5], имеющая арифметическую сложность, представленную в виде выражений [12, 14]:

$$M_{Ch}(n) = A_{Ch}(n) = n\cdot t. \quad (6)$$

Вычислительную сложность нахождения значений ошибок (данная процедура известна в литературе как алгоритм Форни [3, 5, 6]) представим следующим образом [14]:

$$M_{For}(n) = 2\cdot t^2 - t;\ A_{For}(n) = 2\cdot t^2 - 2\cdot t. \quad (7)$$

Вычислительная сложность этапа, на котором выполняется коррекция принятой секции кодового слова, состоит из n числа сложений:

$$A_{Cor}(n) = n, \quad (8)$$

при этом последний этап метода декодирования не содержит операций умножений [12, 13, 14].

Таким образом, аналитические выражения вычислительной сложности метода алгебраического декодирования сверточных кодов во временной области имеют следующий вид:

$$M(n) = M_s(n) + M_{BM}(n) + M_{Ch}(n) + M_{For}(n);$$
$$A(n) = A_s(n) + A_{BM}(n) + A_{Ch}(n) + \quad (9)$$
$$+A_{For}(n) + A_{Cor}(n).$$

С учетом выражений (4) – (8) выражение (9) можно записать:

$$M(n) = 2 \cdot t(n-1) + 6 \cdot t^2 + n \cdot t + 2 \cdot t^2 - t =$$
$$= 8 \cdot t^2 + 3 \cdot n \cdot t - 3 \cdot t;$$
$$A(n) = 2 \cdot t(n-1) + 6 \cdot t^2 + n \cdot t + \quad (10)$$
$$+2 \cdot t^2 - 2 \cdot t + n = 8 \cdot t^2 - 4 \cdot t + 3 \cdot n \cdot t + n.$$

Сверточные коды, допускающие данный метод декодирования, обладают высокой корректирующей способностью, но с ростом длины кодового ограничения v_0 наблюдается увеличение числа арифметических операций.

Ниже предлагаются аналитические выражения, на основании которых возможно производить оценку вычислительной сложности методов кодирования и декодирования алгебраических каскадных сверточных кодов в частотной области с применением алгоритмов быстрого преобразования Фурье (БПФ-алгоритм) Кули-Тьюки и Гуда-Томаса [3, 8, 10].

В основе метода кодирования компонентных сверточных кодов в частотной области лежит быстрый алгоритм обратного преобразования Фурье Кули-Тьюки или Гуда-Томаса [8]. Вычислительную сложность метода кодирования компонентных сверточных кодов в составе каскадного кода в частотной области с применением обратного БПФ-алгоритма Кули-Тьюки можно представить в виде следующих аналитических выражений [3, 4, 8]:

$$M_{KT}(n) = n'(n'')^2 + n''(n')^2 + n' \cdot n'' =$$
$$= n(n' + n'' + 1);$$
$$A_{KT}(n) = n' \cdot n''(n'' - 1) + n'' \cdot n'(n' - 1) = \quad (11)$$
$$= n(n' + n'' - 2),$$

где $M_{KT}(n)$ и $A_{KT}(n)$ – число умножений и сложений соответственно; n' и n'' – делители, на которые можно разложить длину секции n.

Для случая применения обратного БПФ-алгоритма Гуда-Томаса выражения вычислительной сложности принимают вид [3, 4, 8]:

$$M_{GT}(n) =$$
$$= n' M \cdot (n'') + n'' \cdot M(n') = n(n' + n''); \quad (12)$$
$$A_{GT}(n) =$$
$$= n' A \cdot (n'') + n'' \cdot A(n') = n(n' + n''),$$

где n' и n'' – взаимно простые делители n.

Результаты оценки вычислительной сложности методов кодирования алгебраических каскадных сверточных кодов в частотной области представлены на рис. 1 и 2.

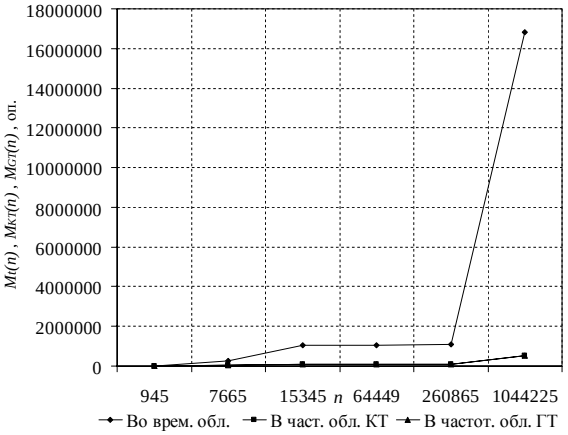

Рис. 1. Сложность методов кодирования каскадных сверточных кодов во временной и частотной области (по числу умножений)

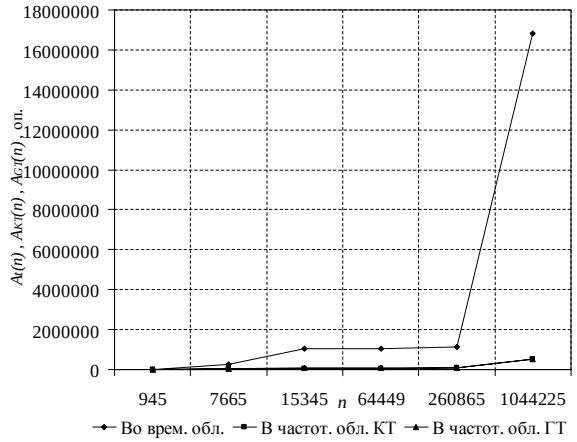

Рис. 2. Сложность методов кодирования каскадных сверточных кодов во временной и частотной области (по числу сложений)

Анализ графиков, представленных на рис.1 и 2 позволяет сделать вывод, что методы кодирования алгебраических каскадных сверточных кодов в частотной области на основе БПФ-алгоритмов [3, 4, 8] позволяют снизить вычислительную сложность при всех исследуемых значений n. Например, при n = 945 метод кодирования в частотной области на основе БПФ-алгоритма Кули-Тьюки позволяет сократить вычислительную сложность в 3,4 раза по числу умножений и в 4,3 раза по числу сложений по сравнению с известным методом кодирования во временной области. При этом результаты справедливы для $GF(2^m)$ и GF(2).

В то же время, как показано на графиках, с ростом n выигрыш по числу арифметических операций возрастает.

Для получения аналитических выражений, позволяющих оценить сложность методов алгебраического декодирования компонентных сверточных кодов в частотной области на основе БПФ-алгоритмов Кули-Тьюки и Гуда-Томаса, рассмотрим следующие этапы метода [11].

На первом этапе методов декодирования компонентных сверточных кодов выполняется прямое преобразование Фурье одной секции кодового слова длины n. Следовательно, сложность данного этапа определяется аналитическими выражениями вида (11) или (12), в зависимости от того, какой БПФ-алгоритм применяется [8, 11].

На втором этапе методов алгебраического декодирования решается ключевое уравнение [3, 6, 11] рекуррентным методом Берлекэмпа-Месси [3, 11], вычислительную сложность которого можно представить в виде следующих аналитических выражений [3]:

$$M_{BM}(n) = 6 \cdot t^2 ;\ A_{BM}(n) = 6 \cdot t^2 . \qquad (13)$$

На третьем этапе методов реализуется рекуррентное продолжение, которое, в конечном счете, позволяет вычислить искомый вектор ошибок. Тогда, вычислительная сложность методов декодирования на данном этапе удовлетворяет следующим выражениям [12]:

$$M_R(n) = t \cdot (n - 2 \cdot t) ;\ A_R(n) = t \cdot (n - 2 \cdot t) . \qquad (14)$$

На четвертом этапе выполняется исправление одной секции кодового слова сверточного кода внутренней ступени. При этом выполняется только n операций сложений, а операции умножения отсутствуют [12, 13, 14]:

$$A_C(n) = n . \qquad (15)$$

Тогда, справедливы следующие аналитические выражения, позволяющие выполнять оценку метода алгебраического декодирования компонентных сверточных кодов в частотной области:

$$\begin{aligned} M(n) &= M_{БПФ}(n) + M_{BM}(n) + M_R(n); \\ A(n) &= A_{БПФ}(n) + A_{BM}(n) + A_R(n) + A_C(n), \end{aligned} \qquad (16)$$

где $M_{БПФ}(n)$ и $A_{БПФ}(n)$ – число арифметических операций умножений и сложений прямых БПФ-алгоритмов соответственно.

Если метод алгебраического декодирования сверточных кодов в частотной области основан на прямом БПФ-алгоритме Кули-Тьюки, то с учетом выражений (11), (13) – (15) выражение (16) приобретает следующий вид:

$$\begin{aligned} M(n) &= n \cdot (n' + n'' + 1) + 6 \cdot t^2 + t \cdot (n - 2 \cdot t) = \\ &= n \cdot (n' + n'' + t + 1) + 4 \cdot t^2; \\ A(n) &= n \cdot (n' + n'' - 2) + 6 \cdot t^2 + t \cdot (n - 2 \cdot t) + n = \\ &= n \cdot (n' + n'' + t - 2) + 4 \cdot t^2. \end{aligned} \qquad (17)$$

В случае использования прямого БПФ-алгоритма Гуда-Томаса, с учетом выражений (12 – 15), выражение (16) можно представить:

$$\begin{aligned} M(n) &= n \cdot (n' + n'') + 6 \cdot t^2 + t \cdot (n - 2 \cdot t) = \\ &= n \cdot (n' + n'' + t) + 4 \cdot t^2; \\ A(n) &= n \cdot (n' + n'') + 6 \cdot t^2 + t \cdot (n - 2 \cdot t) + n = \\ &= n \cdot (n' + n'' + t) + 4 \cdot t^2. \end{aligned} \qquad (18)$$

Таким образом, полученные аналитические выражения вида (17) и (18) позволяют выполнять оценку вычислительной сложности алгоритмов алгебраического декодирования компонентных сверточных кодов в частотной области на основе БПФ-алгоритмов Кули-Тьюки и Гуда-Томаса соответственно (результаты представлены на рис. 3 и 4).

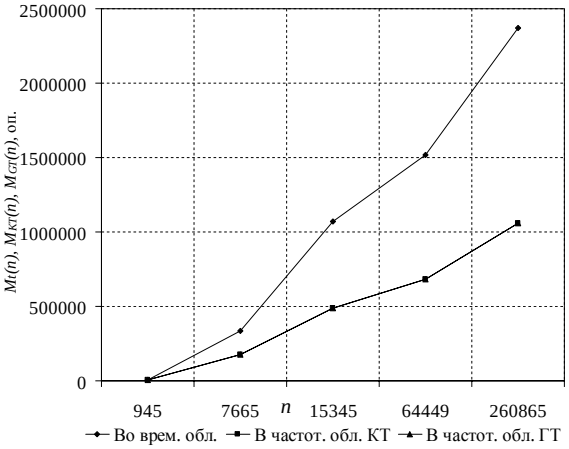

Рис. 3. Сложность методов декодирования каскадных сверточных кодов во временной и частотной области (по числу умножений)

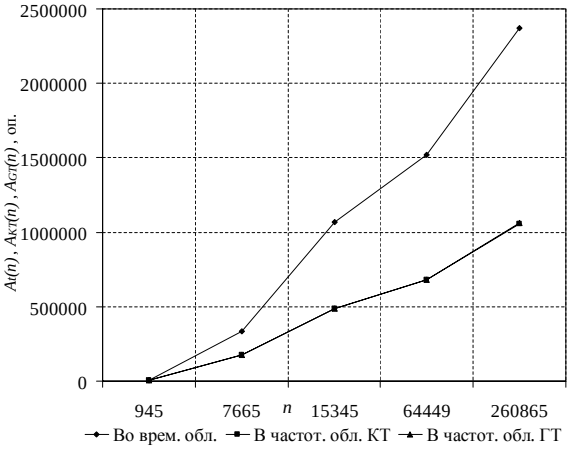

Рис. 4. Сложность методов декодирования каскадных сверточных кодов во временной и частотной области (по числу сложений)

Из анализа графиков, представленных на рис. 3 и 4, можно сделать вывод, что методы алгебраического декодирования в частотной области [11] обладают меньшей вычислительной сложностью, чем метод во временной области, как по числу операций умножений, так и по числу сложений. При этом с ростом длины секции кодового слова n выигрыш по числу операций возрастает.

В случае применения БПФ-алгоритма Кули-Тьюки при значении n = 945 удается уменьшить

число умножений в 1,67 раза и число сложений в 1,76 раза, а при значении n = 64449 число умножений уже сокращается в 2,23 раза и число сложений 2,24 раза по сравнению с алгоритмом во временной области.

В то же время, алгоритм декодирования на основе БПФ-алгоритма Гуда-Томаса при n = 945 уменьшает число умножений в 1,71 раза и число сложений в 1,69 раза, а при n = 64449 число умножений в 2,23 раза и число сложений 2,23 раза.

Выводы

Получены аналитические оценки вычислительной сложности методов кодирования и декодирования алгебраических каскадных сверточных кодов во временной и частотной области основанных на синтезе методов быстрого вычисления свертки Агарвала-Кули и Винограда, а также применения БПФ-алгоритмов Кули-Тьюки и Гуда-Томаса.

Показано, что применение методов быстрого вычисления свертки Агарвала-Кули и Винограда, БПФ-алгоритмов Кули-Тьюки и Гуда-Томаса позволяют уменьшить вычислительную сложность методов кодирования и декодирования алгебраических каскадных сверточных кодов.

Список литературы

1. *Форни Д. Каскадные коды / Д. Форни; [пер. с англ. В.В. Зяблова, О.В. Попова]; под ред. С.И. Самойленко. – М.: Мир, 1970. – 207 с.*
2. *Блох Э.Л., Зяблов В.В. Обобщенные каскадные коды / Э.Л. Блох, В.В. Зяблов. –М.: Связь, 1976. – 240 с.*
3. *Блейхут Р. Теория и практика кодов, контролирующих ошибки / Р. Блейхут; [пер. с англ. И.И. Грушко, В.М. Блиновского]; под ред. К.Ш. Зигангирова. – М.: Мир, 1986. – 576 с.*
4. *Блейхут Р. Быстрые алгоритмы цифровой обработки сигналов / Р. Блейхут; [пер. с англ. И.И. Грушко]. – М.: Мир, 1989. – 448 с.*
5. *Кларк Дж. Кодирование с исправлением ошибок в системах цифровой связи / Дж. Кларк, мл., Дж. Кейн; пер. с англ. С.И. Гельфанда; под ред. Б.С. Цыбакова. – М.: Радио и связь, 1987. – 392 с.*
6. *Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение / Р. Морелос-Сарагоса; [пер. с англ. В.Б. Афанасьева]. – М.: Техносфера, 2005. – 320 с.*
7. *Алгебраические сверточные коды: [учебное пособие] / [Н.И. Данько, С.П. Евсеев, А.А. Кузнецов и др.]. – Харьков: УкрГАЖТ, 2007. – 238 с.*
8. *Приходько С.И. Метод построения алгебраических каскадных сверточных кодов в частотной области / С.И. Приходько, А.С. Волков // Системи обробки інформації. – 2010. – Вип. 9 (90). – С. 194-197.*
9. *Приходько С.И. Метод кодирования алгебраическим каскадным сверточным кодом на базе синтеза процедур вычисления сверток / С.И. Приходько, А.С. Волков // Системи управління, навігації та зв'язку. – 2010. – Вип. 4(16). – С. 165 – 168.*
10. *Приходько С.И. Метод построения алгебраических каскадных сверточных кодов / С.И. Приходько, А.С. Волков // Системи обробки інформації. – 2010. – Вип. 6(87). – С. 224-228.*
11. *Приходько С.И. Метод декодирования алгебраических каскадных сверточных кодов в частотной области с применением быстрого преобразования Фурье / С.И. Приходько, А.С. Волков // Системи управління, навігації та зв'язку. – 2011. – Вип. 1 (17). – С. 116-119.*
12. *Choomchuay S. Fast transform techniques for RS codes / S. Choomchuay // Ladkrabang Engineering Journal. – 1995. – V. 12, №1. – P. 32-41.*
13. *Sugiyama Y. A method for solving key equation for decoding Goppa codes / Y. Sugiyama, M. Kasahara, S. Hirasawa, T. Namekawa // Inform. Contr. – 1975. – V. 27. – P. 87-99.*
14. *Hong J. Simple algorithms for BCH decoding / J. Hong, M. Vetterly // IEEE transactions on communications. – 1995.– V. 43, № 8. – P. 2324-2333.*

Поступила в редколлегию 8.02.2011

Рецензент: д-р техн. наук, проф. А.А. Кузнецов, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

ОБЧИСЛЮВАЛЬНА СКЛАДНІСТЬ МЕТОДІВ КОДУВАННЯ ТА ДЕКОДУВАННЯ АЛГЕБРАЇЧНИХ КАСКАДНИХ ЗГОРТКОВИХ КОДІВ В ЧАСОВІЙ ТА ЧАСТОТНІЙ ОБЛАСТІ

С.І. Приходько, О.С. Волков

Пропонуються аналітичні оцінки обчислювальної складності методів кодування та декодування алгебраїчних каскадних згорткових кодів у часовій та частотній області. Показано, що методи кодування та декодування алгебраїчних каскадних згорткових кодів в частотній області на основі ШПФ-алгоритмів Кулі-Т'юкі та Гуда-Томаса дозволяють зменшити обчислювальну складність.

Ключові слова: *завадостійке кодування, згорткові коди, каскадні коди, ШПФ-алгоритм, перетворення Фур'є, обчислювальна складність.*

THE COMPUTATIONAL COMPLEXITY OF CODING AND DECODING OF ALGEBRAIC CONCATENATED CONVOLUTIONAL CODES IN THE TIME AND FREQUENCY DOMAIN

S.I. Prihodko, A.S. Volkov

The proposed complexity of methods for encoding and decoding of algebraic concatenated convolutional codes in the time and frequency domain. It is shown that the methods of encoding and decoding of algebraic concatenated convolutional codes in the frequency domain based on FFT-algorithms the Cooley-Tukey and Good-Thomas can reduce the computational complexity.

Keywords: *error correcting coding, convolutional codes, concatenated codes, FFT-algorithm, Fourier transform, computational complexity.*