УДК 621.391

С.И. Приходько[1], С.А. Гусев[1], В.А. Зубенко[2]

[1] *Украинская государственная академия железнодорожного транспорта, Харьков*
[2] *Кировоградский национальный технический университет, Кировоград*

РАЗРАБОТКА КАСКАДНЫХ КОДОВЫХ КОНСТРУКЦИЙ С УЛУЧШЕННЫМИ СВОЙСТВАМИ

Рассматриваются методы построения каскадных кодовых конструкций, в том числе, турбо-продуктивные коды (Turbo Product Codes). Развивается подход турбо-продуктивного кодирования на основе обобщения каскадных кодовых конструкций на случай недвоичных последовательностей с возможностью использования методов декодирования с итеративным обменом мягкими решениями.

Ключевые слова: *кодовые конструкции, турбо-продуктивное кодирование.*

1. Постановка проблемы в общем виде и анализ литературы

Перспективным направлением в развитии теории помехоустойчивого кодирования и, в частности, каскадных кодовых конструкций, являются коды, образованные каскадированием линейных блоковых кодов с быстрыми алгоритмами мягкого декодирования и итеративным обменом полученных решений. В зарубежной литературе такие каскадные кодовые конструкции получили название турбо-продуктивных кодов (Turbo Product Codes) [1 – 3].

В упрощенном варианте по своей структуре турбо-продуктивные коды (другое название – турбо-коды-произведения) повторяют хорошо известные и изученные итеративные коды и, в то же время, наследуют принцип турбо-кодирования, перенесенный с каскадных кодовых конструкций на сверточных кодах. Это с одной стороны, позволяет сохранить идеологию турбо-кодирования [4, 5], т.е. возможность реализовывать обмен мягкими решениями в итеративной многошаговой процедуре декодирования для обеспечения высокой энергетической эффективности помехоустойчивого кода. С другой стороны, данный подход позволит существенно снизить сложность реализации алгоритмов декодирования [1 – 3], что наряду с высокой энергетической эффективностью позволяет реализовать данный класс каскадных кодов в телекоммуникационных системах и сетях специального назначения, в том числе и в системах управления и связи на транспорте [6].

В данной статье развивается подход турбо-продуктивного кодирования на основе обобщения каскадных кодовых конструкций на случай недвоичных последовательностей с возможностью использования методов декодирования с итеративным обменом мягкими решениями.

2. Турбо-продуктивные коды

Рассмотрим структуру турбо-продуктивных кодов, исследуем их внутреннее логическое построение и закономерности синтеза. Для этого рассмотрим кодовое слово турбо-продуктивного кода, которое в упрощенном виде приведено на рис. 1.

На рис. 1 приведен трехмерный куб, хотя в общем случае размерность p пространства может быть произвольна, и в некоторых случаях увеличение этой размерности (p > 3) приводит к повышению конструктивных свойств турбо-продуктивного кода [1 – 3].

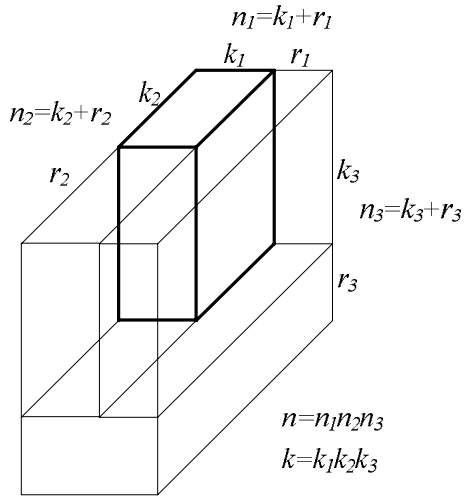

Рис. 1. Графическая интерпретация структуры кодового слова турбо-продуктивного кода

Анализ структуры кодового слова турбо-продуктивного кода, схема которого в упрощенном виде приведена на рис. 1, показывает, что в упрощенном варианте она сводится к структуре хорошо известного итерированного кода. Действительно, структура турбо-продуктивного кода представляет собой p-мерный куб (см. рис. 1), в выделенном подкубе которого размещаются информационные символы сообщения, а проверочные символы формируются в результате кодирования по строкам и столбцам куба простейшим блоковым кодом. При p = 2 имеем структуру кодового слова типа «квадрат», информационные символы которого записаны в левой верхней части кодового слова, а провероч-

ные символы формируются посредством кодирования по строкам и столбцам «квадрата», что полностью соответствует схеме кодирования итерированным кодом (см. рис. 2). Действительно, по определению линейный итеративный код задается схемой кодирования, представленной на рис. 2 [6, 7].

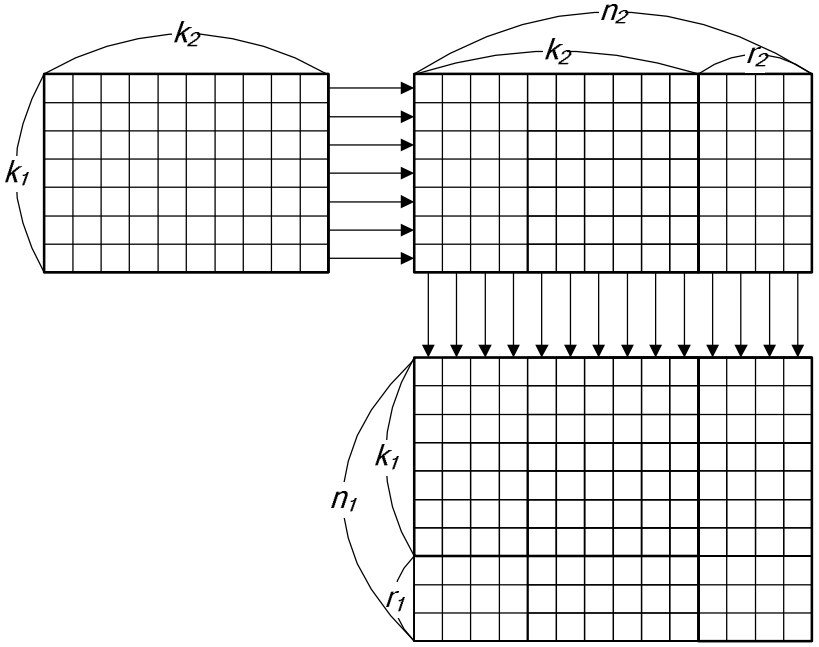

Рис. 2. Схема построения итеративного кода

Информационные символы $I = \{I_1, I_2, ..., I_k\}$ разбиваются на k_2 подблоков, содержащих по k_1 двоичных символов в каждом, т.е., выполняется равенство $k = k_1 \cdot k_2$. Информационные символы записываются в виде матрицы размером $k_1 \times k_2$, у которой каждый столбец является подблоком из k_1 символов (см. рис. 2). Каждая строка полученной матрицы кодируется линейным блоковым (n_2, k_2, d_2) кодом, называемый кодом второй (внешней) ступени. В результате умножения получаем 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, называемый кодом первой (внутренней) ступени.

В результате выполнения последней операции получаем матрицу размеров $k_1 \times k_2$, у которой каждый столбец есть кодовое слово кода первой ступени, а каждая строка – кодовое слово кода второй ступени (для последних r_1 строк это является следствием линейности кодов первой и второй ступеней).

Полученная матрица является кодовым словом итерированного кода с параметрами: $n = n_1 n_2$, $k = k_1 k_2$, $d = d_1 d_2$.

Таким образом, результаты исследований показывают, что кодовое слово турбо-продуктивного кода по своей алгебраической структуре обобщает кодовое слово итерированного кода на случай р-мерного куба.

Идеология турбо-кодирования, присущая построенным на основе рекурсивных систематических сверточных кодов с вероятностными процедурами декодирования, реализована в турбо-продуктивных кодах следующим образом.

Декодирование осуществляется параллельно (по столбцам или по строкам) в одной из плоскостей р-мерного куба с использованием алгоритмов декодирования блоковых кодов с мягкими решениями. Далее происходит последовательный переход на следующую плоскость куба и возобновляется параллельное декодирование (по столбцам или по строкам) уже в новой плоскости куба. Процесс повторяется для всех плоскостей куба, после чего возможна следующая итерация декодирования. Идеология турбо-декодирования в данном случае состоит в обмене мягкими решениями при декодировании в различных плоскостях, само декодирование представляет собой симбиоз параллельно-последовательного выполнения алгоритмов декодирования с мягкими решениями над соответствующими строками-столбцами р-мерного куба.

Следует отметить, что итерированный код (турбо-продуктивный код для случая кодового слова «квадрат», т.е. для р = 2) является подклассом рассмотренного в работе [6] обобщенного каскадного кода (с m = 1), впервые подробно описанного и исследованного в монографии [7]. Исходными данными для его описания да являются [7]:

1) двоичное слово с длины $n = n_1 n_2$, которое представляется в виде последовательности двоичных векторов C_j, $j = \overline{1, n_2}$, длины n_1, т.е.

$$c=\left(c_1,c_2,...,c_{n_1},c_{n_1+1},...,c_{2n_1},c_{2n_1+1},...,c_{n_2n_1}\right)=$$
$$=\left(\left(c_1,c_2,...,c_{n_1}\right),\left(c_{n_1+1},...,c_{2n_1}\right),...,\left(c_{2n_1+1},...,c_{n_2n_1}\right)\right)=(1)$$
$$=\left(C_1,C_2,...,C_{n_2}\right),C_j=\left(c_{(j-1)n_1+1},...,c_{jn_1}\right);$$

2) n_2 квадратных двоичных матриц H_0^j, $j=\overline{1,n_2}$, порядка n_1;

3) $m+1$ групповых над $GF(2^{a_i})$, $i=\overline{1,m+1}$ кодов (кодов второй ступени) с параметрами (n_2,b_i,d_{2i}). При этом выполняется равенство

$$\sum_{i=1}^{m+1}a_i=n_1.$$

В основном варианте построения обобщенных каскадных кодов в качестве матриц H_0^j для всех $j=\overline{1,n_2}$ выбирается одна и та же треугольная матрица H_0 порядка n_1, которая в клеточной форме имеет вид

$$H_0=\begin{Vmatrix} I_{a_1} & & & & & \\ P_{11} & I_{a_2} & & 0 & & \\ P_{21} & P_{22} & I_{a_3} & & & \\ ... & ... & ... & ... & ... & ... \\ P_{m1} & P_{m2} & P_{m3} & ... & P_{mm} & I_{a_{m+1}} \end{Vmatrix}=\begin{Vmatrix} \tilde{H}_0 \\ \tilde{H}_1 \\ \tilde{H}_2 \\ ... \\ \tilde{H}_m \end{Vmatrix}, \quad (2)$$

где $\tilde{H}_0=\left\| I_{a_1} \quad 0 \right\|$,

$$\tilde{H}_i=\left\| P_{i_1} \quad P_{i_2} \quad ... \quad P_{i_i} \quad I_{a_1} \quad 0 \quad ... \quad 0 \right\|, \ i=\overline{1,m}, \quad (3)$$

клетки P_{i_s} – двоичные матрицы размеров $a_{i+1}\times a_s$; I_{a_s} – единичная матрица порядка a_s.

Проверочная матрица H_i, вида

$$H_i=\begin{Vmatrix} \tilde{H}_i \\ \tilde{H}_{i+1} \\ ... \\ \tilde{H}_m \end{Vmatrix}=$$

$$=\begin{Vmatrix} P_{i_1} & P_{i_2} & ... & P_{i_i} & I_{a_{i+1}} & & 0 & \\ P_{i+1_1} & P_{i+1_2} & ... & P_{i+1_i} & P_{i+1_{i+1}} & I_{a_{i+2}} & & \\ ... & ... & ... & ... & ... & ... & ... & ... \\ P_{m_1} & P_{m_2} & ... & P_{m_i} & P_{m_{i+1}} & ... & P_{m_m} & I_{a_{m+1}} \end{Vmatrix}, \quad i=\overline{1,m}, \quad (4)$$

полностью определяемая матрицей H_0 (состоит из $m-i+1$ клеточных строк матрицы H_0) задает i-й код первой ступени с параметрами (n_1,k_i,d_{1i}). При этом для числа информационных символов i-го кода выполняется соотношение $k_i=a_1+a_2+...+a_i$.

Зафиксируем линейное отображение векторов C_j:

$$C_jH_0^T=\left(\gamma_{1j},\gamma_{2j},...,\gamma_{m+1j}\right), \ j=\overline{1,n_2}, \quad (5)$$

где γ_{ij} – двоичный вектор длины a_i.

Трактуя векторы γ_{ij} как элементы поля $GF(2^{a_i})$, составим из этих элементов, полученных в результате отображения (5) (для каждого слова c), векторы $\gamma_i=\left(\gamma_{i1},\gamma_{i2},...,\gamma_{in_2}\right)$, $i=\overline{1,m+1}$.

По определению [7] двоичное слово c длины $n=n_1n_2$ является кодовым словом обобщенного каскадного кода порядка m тогда и только тогда, когда все связанные со словом c векторы γ_i, $i=\overline{1,m+1}$, представляют собой кодовые слова соответствующих (i-х) кодов второй ступени.

Во многих случаях удобна следующая геометрическая трактовка обобщенного каскадного кода (см. рис. 3).

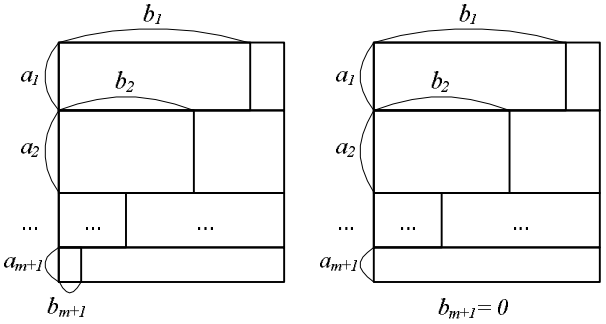

Рис. 3. Геометрическая трактовка обобщенного каскадного кода

Величины $a_i>0$ и $b_i\geq 0$, определяющие внутреннюю структуру обобщенного каскадного (n,k,d) кода, выбираются произвольно, при этом (n,k,d) параметры удовлетворяют следующим соотношениям [7]:

$$n=n_1n_2; \ k=\sum_{i=1}^{m+1}a_ib_i;$$
$$d\geq\begin{cases} \min\left\{ d_{1i}d_{2i} : i=\overline{1,m} \right\} \text{ при } b_{m+1}=0, \\ \min\left\{ d_{2m+1}, d_{1i}d_{2i} : i=\overline{1,m} \right\} \text{ при } b_{m+1}\neq 0. \end{cases} \quad (6)$$

В работе [7] показано, что нетривиальные обобщенные каскадные коды (с $m>1$) по своим конструктивным показателям превосходят итерированные коды и по кодовым соотношениям приближаются к теоретической границе Варшамова-Гилберта. Другими словами, с точки зрения развития идей турбо-кодирования целесообразным представляется построение (обобщение) нетривиального ($p>2$) турбо-продуктивного кода по нетривиальному обобщенному каскадному коду (с $m>1$).

Таким образом, естественным направлением дальнейшего развития каскадных кодовых конструкций есть применение турбо-подхода к аналитическому описанию, построению и декодированию

обобщенных каскадных кодов. Данный подход позволяет обобщить как вероятностные процедуры декодирования, присущие древовидным, сверточным кодам, позволяющие достичь показателей энергетической эффективности, близкой к верхнему теоретическому пределу, так и быстрые алгебраические процедуры синтеза и декодирования блоковых кодов, позволяющие строить вычислительно эффективные устройства кодирования и декодирования как в программном, так и в аппаратном виде.

3. Предлагаемые каскадные кодовые конструкции

Проведенные исследования показали, что наиболее общим классом каскадных кодовых конструкций, построенных на линейных блоковых кодах, есть обобщенные каскадные коды [6, 7]. В то же время, анализ структуры кодового слова, графическая интерпретация которого приведена на рис. 3, исследование особенностей аналитического описания и процедур построения показывает, что обобщенным каскадным кодам присущи следующие конструктивные недостатки.

1. Как следует из графической интерпретации кодового слова (рис. 3) и аналитических выражений (1) – (5), для построения обобщенного каскадного кода используется n_2 квадратных двоичных матриц H_0^j, $j=\overline{1,n_2}$, порядка n_1 (в основном варианте построения используется одна матрица для всех $j=\overline{1,n_2}$), которые задают коды первой ступени. Причем каждая матрица H_0^j содержит m подматриц H_i, $i=\overline{1,m}$, однозначно определяющих правило кодирования i-м кодом первой ступени с параметрами (n_1,k_i,d_{1i}). Другими словами все m кодов первой ступени подобраны так, что i-й код первой ступени является подкодом (как линейное подпространство) $i+1$-го кода первой ступени. На практике такое построение вызывает существенные трудности, поскольку, как правило, известные методы построения цепочки из m кодов первой ступни не всегда дают требуемые кодовые показатели, прежде всего по минимальному кодовому расстоянию. Поскольку кодовые параметры результирующего обобщенного каскадного кода определяются по кодовым соотношениям соответствующих кодов первой и второй ступени, а минимальное кодовое расстояние определяется по критерию минимума произведений кодовых расстояний соответствующих кодов первой и второй ступени (см. выражение (6)), синтез обобщенного каскадного кода с требуемыми для инженерных приложений свойствами затруднителен. В подтверждение этого тезиса приведем тот факт, что наряду с потенциально высокими кодовыми соотношениями и низкой сложностью процедур кодирования и декодирования обобщенные каскадные коды на сегодняшний день не нашли практического использования ни в одной из известных авторам телекоммуникационных систем.

2. По определению, обобщенный каскадный код – двоичный линейный блоковый код. В то же время, как показывает проведенный анализ [8, 9], наиболее эффективным средством борьбы с группирующимися ошибками, которым подвержены практически все реальные каналы передачи данных, являются недвоичные коды, обработка символов которых выполняется с использованием арифметики конечного поля $GF(q)$, $q>2$. Очевидно, что существующий научно-методический аппарат, методы построения и декодирования обобщенных каскадных кодов не подразумевают синтез недвоичных кодовых конструкций, отсутствуют вычислительные алгоритмы кодирования и декодирования.

Свободными от указанных недостатков являются предлагаемые каскадные кодовые конструкции с улучшенными свойствами.

В основе предлагаемых каскадных кодовых конструкций с улучшенными свойствами лежит дальнейшее развитие обобщенных каскадных кодов посредством их аналитического описания, исследования методов синтеза и декодирования на случай недвоичных кодовых слов с дальнейшим применением алгоритмов декодирования с мягкими решениями.

Для аналитического описания предлагаемых каскадных кодовых конструкций воспользуемся абстрактным определением обобщенных каскадных кодов, обобщим их на случай невоичных кодовых слов над $GF(q)$, $q>2$.

Рассмотрим структуру кодового слова, представленного на рис. 4. В отличие от обобщенного каскадного кода предлагаемые каскадные кодовые конструкции являются недвоичными линейными блоковыми кодами. Величина $a>0$ задает степень расширения двоичного поля, т.е. мощность алфавита символов, над которым построены предлагаемые каскадные коды. Величины $A_i>0$ и $b_i\geq 0$, как и для обобщенных каскадных кодов, определяют внутреннюю структуру предлагаемого каскадного (n,k,d) кода над $GF(2^a)$, они выбираются произвольно, с обязательным выполнением соотношений: $A_i=p_i a$, $i=\overline{1,m}$, где p_i – степень расширения поля $GF(2^a)$, т.е. $GF(2^{A_i})$ – поле, над которым построен i-й код второй ступени.

Исходными данными для описания предлагаемых каскадных кодовых конструкций являются:

1) недвоичное слово с длины $n=n_1n_2$, с элементами из конечного поля $GF(2^a)$, которое пред-

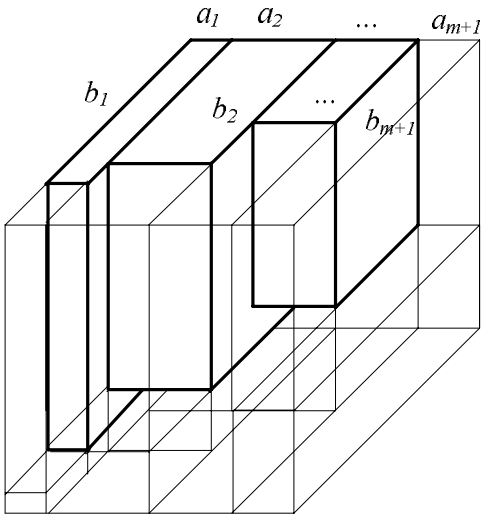

Рис. 4. Структура кодового слова предлагаемых каскадных кодовых конструкций с улучшенными свойствами

ставляется в виде последовательности недвоичных векторов C_j, $j=\overline{1,n_2}$, длины n_1, т.е.

$$c=\left(c_1,c_2,...,c_{n_1},c_{n_1+1},...,c_{2n_1},c_{2n_1+1},...,c_{n_2n_1}\right)=$$
$$=\left(\left(c_1,c_2,...,c_{n_1}\right),\left(c_{n_1+1},...,c_{2n_1}\right),...,\left(c_{2n_1+1},...,c_{n_2n_1}\right)\right)=(7)$$
$$=\left(C_1,C_2,...,C_{n_2}\right),C_j=\left(c_{(j-1)n_1+1},...,c_{jn_1}\right);c_l\in GF(2^a);$$

2) n_2 квадратных недвоичных матриц H_0^j с элементами из $GF(2^a)$, $j=\overline{1,n_2}$, порядка n_1;

3) $m+1$ групповых над $GF(2^{A_i})$, $i=\overline{1,m+1}$, кодов (кодов второй ступени) с параметрами (n_2,b_i,d_{2i}). При этом выполняется равенство

$$\sum_{i=1}^{m+1}A_i=n_1.$$

Так же как и для обобщенных каскадных кодов, определим основной вариант построения, в котором в качестве матриц H_0^j для всех $j=\overline{1,n_2}$ выбирается одна и та же треугольная матрица H_0 порядка n_1, которая в клеточной форме имеет вид

$$H_0=\begin{Vmatrix} I_{A_1} & & & & & \\ P_{11} & I_{A_2} & & & 0 & \\ P_{21} & P_{22} & I_{A_3} & & & \\ ... & ... & ... & ... & ... & ... \\ P_{m1} & P_{m2} & P_{m3} & ... & P_{mm} & I_{A_{m+1}} \end{Vmatrix}=\begin{Vmatrix}\tilde H_0\\ \tilde H_1\\ \tilde H_2\\ ...\\ \tilde H_m\end{Vmatrix},\ (8)$$

где

$$\tilde H_0=\left\|I_{A_1}\quad 0\right\|,$$
$$\tilde H_i=\left\|P_{i_1}\quad P_{i_2}\quad ...\quad P_{i_i}\quad I_{A_1}\quad 0\quad ...\quad 0\right\|,\ i=\overline{1,m},\ (9)$$

клетки P_{i_s} – недвоичные матрицы с элементами из $GF(2^a)$ размеров $p_{i+1}\times p_s$, I_{A_s} – единичная матрица порядка p_s.

Проверочная матрица H_i, вида

$$H_i=\begin{Vmatrix}\tilde H_i\\ \tilde H_{i+1}\\ ...\\ \tilde H_m\end{Vmatrix}=$$
$$=\begin{Vmatrix} P_{i_1} & P_{i_2} & ... & P_{i_i} & I_{A_{i+1}} & & 0 & \\ P_{i+1_1} & P_{i+1_2} & ... & P_{i+1_i} & P_{i+1_{i+1}} & I_{A_{i+2}} & & \\ ... & ... & ... & ... & ... & ... & ... & ... \\ P_{m_1} & P_{m_2} & ... & P_{m_i} & P_{m_{i+1}} & ... & P_{m_m} & I_{A_{m+1}} \end{Vmatrix},$$
$$i=\overline{1,m},\qquad (10)$$

полностью определяемая матрицей H_0 (состоит из $m-i+1$ клеточных строк матрицы H_0) задает i-й недвоичный код первой ступени с параметрами (n_1,k_i,d_{1i}) над $GF(2^a)$. При этом для числа информационных символов i-го кода выполняется соотношение $k_i=p_1+p_2+...+p_i$.

Зафиксируем линейное отображение векторов C_j:

$$C_jH_0^T=\left(\gamma_{1j},\gamma_{2j},...,\gamma_{m+1j}\right),\ j=\overline{1,n_2},\qquad (11)$$

где γ_{ij} – недвоичный вектор длины p_i с элементами из $GF(2^a)$.

Трактуя векторы γ_{ij} как элементы поля $GF(2^{A_i})$, $A_i=p_ia$, составим из этих элементов, полученных в результате отображения (11) (для каждого слова c), векторы

$$\gamma_i=\left(\gamma_{i1},\gamma_{i2},...,\gamma_{in_2}\right),\ i=\overline{1,m+1}.$$

Недвоичное слово c длины $n=n_1n_2$ с элементами из $GF(2^a)$ (см. выражение (7)) является кодовым словом предлагаемого каскадного кода порядка m тогда и только тогда, когда все связанные со словом c векторы γ_i, $i=\overline{1,m+1}$, представляют собой кодовые слова соответствующих (i-х) кодов второй ступени над $GF(2^{A_i})$.

Кодовые параметры предлагаемого каскадного кода удовлетворяют выражениям:

$$n=n_1n_2;\ k=\sum_{i=1}^{m+1}A_ib_i;$$
$$d\ge\begin{cases}\min\left\{d_{1i}d_{2i}:i=\overline{1,m}\right\}\text{ при }b_{m+1}=0,\\ \min\left\{d_{2m+1},d_{1i}d_{2i}:i=\overline{1,m}\right\}\text{ при }b_{m+1}\ne 0.\end{cases}$$

Очевидно, что предлагаемые каскадные кодовые конструкции по своим корректирующим свойствам не уступают обобщенным каскадным кодам, и являются обобщением кодового слова на недвоичный случай. В упрощенном виде при $a = 1$ предлагаемые кодовые конструкции сводятся к двоичному обобщенному каскадному коду. Действительно, в этом случае коды первой ступени задаются n_2 квадратными двоичными матрицами H_0^j, $j = \overline{1, n_2}$, порядка n_1, а $m+1$ групповых кодов второй ступени определены над полем $GF(2^{A_i})$, $i = \overline{1, m+1}$, где $A_i = p_i a = p_i$, т.е. над $GF(2^{p_i})$, что согласуется с определением двоичных обобщенных каскадных кодов. Выполняется также равенство

$$\sum_{i=1}^{m+1} A_i = \sum_{i=1}^{m+1} p_i a = \sum_{i=1}^{m+1} p_i = n_1 .$$

Основное преимущество предлагаемых кодовых конструкций перед обобщенными каскадными кодами состоит в существенном упрощении процедуры синтеза на этапе формирования матриц H_0^j (в основном варианте построения – матрицы H_0), задающих недвоичные коды первой ступени с элементами из поля $GF(2^a)$. Исследуем особенности синтеза предлагаемых каскадных кодовых конструкций в сравнении с процедурами синтеза обобщенного каскадного кода.

4. Алгебраические процедуры синтеза предлагаемых каскадных кодовых конструкций

В соответствии с формальным аналитическим определением и структурой кодового слова предлагаемых каскадных кодовых конструкций, графическая интерпретация которого приведена на рис. 4, основными этапами синтеза являются:

1. Выбор величин $A_i > 0$ и $b_i \geq 0$, определяющих внутреннюю структуру каскадного кода.

2. Построение n_2 квадратных матриц H_0^j, $j = \overline{1, n_2}$, порядка n_1 (в основном варианте одной двоичной матрицы H_0). Каждая матрица H_0^j содержит m подматриц H_i, $i = \overline{1, m}$, однозначно определяющих правило кодирования i-м кодом первой ступени с параметрами (n_1, k_i, d_{1i}), который является подкодом $i+1$-го кода первой ступени.

3. Построение $m+1$ групповых кодов (кодов второй ступени) с параметрами (n_2, b_i, d_{2i}).

Очевидно, что основные этапы синтеза предлагаемых каскадных кодовых конструкций и обобщенных каскадных кодов практически идентичны. Основное различие состоит в построении n_2 квадратных матриц (двоичных для обобщенных каскадных кодов и над полем $GF(2^a)$ для предлагаемых каскадных кодовых конструкций) H_0^j, $j = \overline{1, n_2}$, порядка n_1, однозначно определяющих правило кодирования i-м кодом первой ступени с параметрами (n_1, k_i, d_{1i}), который, в свою очередь, является подкодом $i+1$-го кода первой ступени. Другими словами, на этом этапе требуется найти такой набор кодов первой ступени, чтобы они помимо конструктивных (n_1, k_i, d_{1i}) параметров удовлетворяли условию вложения i-м кода в $i+1$-й код первой ступени.

Рассмотрим особенности синтеза рассматриваемых каскадных кодов на этом этапе.

В монографии [7], посвященной исследованию алгебраических процедур синтеза обобщенных каскадных кодов, в качестве кодов первой ступени предлагается использовать двоичные коды БЧХ. Этот подход позволяет строить регулярные алгоритмы синтеза n_2 квадратных двоичных матриц H_0^j, определяющих цепочки вложенных друг в друга кодов БЧХ. Данный класс кодов привлекателен простотой алгебраических методов построения и позволяет для сравнительно небольшой длины кодового слова добиться высоких конструктивных кодовых характеристик.

В соответствии с основными положениями алгебраической теории блоковых кодов, коды БЧХ задаются порождающим многочленом вида [8, 9]:

$$g(x) = \prod_i (x - \alpha^i), \text{ где } \alpha^i \in GF(2^m). \qquad (12)$$

Рассмотрим структуру конечного поля $GF(2^m)$ как множество многочленов степени $\leq m$ с коэффициентами из $GF(2)$, т.е. структуру кольца многочленов $GF(2)[x]/(x^m - 1)$.

В соответствии с общими положениями теории полей Галуа [8], кольцо многочленов $GF(2)[x]/(x^m - 1)$ с операциями по модулю неприводимого многочлена является расширенным полем Галуа $GF(2^m)$. Такое поле состоит из совокупности циклотомических классов (классов сопряженных элементов), схематично представленных в табл. 1 в виде соответствующих степеней примитивного элемента поля.

Анализ табл. 1 показывает, что выражение (12) можно переписать в виде:

$$g(x) = \prod_i f_i(x), \qquad (13)$$

причем, в соответствии с теоремой БЧХ параметры циклического кода, заданного порождающим многочленом (13), связаны соотношениями:

$$n = 2^m - 1, \; k = n - r = n - mt, \; d = 2t .$$

Таблица 1

Классы сопряженных элементов и соответствующие им минимальные многочлены

Элементы циклотомических классов					Минимальные многочлены
α^0					$f_0(x) = (x - \alpha^0)$
α^1	α^2	α^{2^2}	...	α^{2^m}	$f_1(x) = f_2(x) = f_{2^2}(x) = ... = f_{2^m}(x) = (x - \alpha^1)\cdot(x - \alpha^2)\cdot(x - \alpha^{2^2})\cdot(x - \alpha^{2^m})$
...	...	...	...	...	...
α^i	α^{i2}	α^{i2^2}	...	α^{i2^m}	$f_i(x) = f_{i2}(x) = f_{i2^2}(x) = ... = f_{i2^m}(x) = (x - \alpha^i)\cdot(x - \alpha^{i2})\cdot(x - \alpha^{i2^2})\cdot(x - \alpha^{i2^m})$
...	...	...	...	...	...

Алгебраические методы построения кодов БЧХ дают возможность синтезировать цепочку вложенных друг в друга кодов, о чем свидетельствует следующее утверждение.

Утверждение 1. Код БЧХ с порождающим многочленом (13), содержащим в качестве сомножителей минимальные многочлены

$$g_1(x) = f_i(x), f_{i+1}(x), ..., f_{i+j+1}(x),$$

является подкодом (как линейное подпространство) кода БЧХ с порождающим многочленом (13), содержащим в качестве сомножителей минимальные многочлены

$$g_2(x) = f_i(x), f_{i+1}(x), ..., f_{i+j}(x).$$

Доказательство. Как следует из определения циклических кодов, произвольное кодовое слово $c(x)$ можно представить в виде произведения некоторого информационного слова $i(x)$ на порождающий многочлен $g(x)$:

$$c(x) = i(x)g(x).$$

С учетом (13) перепишем последнее выражение в виде:

$$c(x) = i(x)\prod_i f_i(x),$$

что для кодов БЧХ с порождающими многочленами $g_1(x)$ и $g_2(x)$ даст следующую цепочку равенств:

$$c(x) = i(x)g_1(x) = i(x)f_i(x), f_{i+1}(x), ..., f_{i+j+1}(x) =$$
$$= \left(i(x)f_{i+j+1}(x)\right)f_i(x), f_{i+1}(x), ..., f_{i+j}(x) =$$
$$= i'(x)f_i(x), f_{i+1}(x), ..., f_{i+j}(x) = i'(x)g_2(x),$$

т.е. кодовое слово кода БЧХ с порождающим многочленом $g_1(x)$ всегда принадлежит коду БЧХ с порождающим многочленом $g_2(x)$.

Таким образом, применение кодов БЧХ для синтеза двоичных обобщенных каскадных кодов оправдано возможностью построения цепочки вложенных друг в друга двоичных кодов первой ступени на втором этапе синтеза. Подробно алгебраические процедуры построения матриц H_0^j рассмотрены в монографии [7]. Других конструктивных способов построения матриц H_0^j авторами обобщенных каскадных кодов не предложено [7].

Следует отметить, что рассматриваемый подход построения матриц H_0^j не позволяет в полной мере реализовать потенциальные возможности обобщенных каскадных кодов. Действительно, как следует из теоремы БЧХ и структуры расширенного конечного поля $GF(2^m)$ (см. табл. 1), для фиксированной длины кода БЧХ число проверочных символов может изменяться лишь в соответствии со структурой конечного поля, т.е., в соответствии с теоремой БЧХ число информационных символов кода изменяется «скачкообразно»: $k = n - mt$, т.е. на m символов.

Подбор требуемых для построения обобщенного каскадного кода (с заданными величинами $a_i > 0$) цепочки вложенных друг в друга кодов может явиться практически неразрешимой задачей. В практических примерах авторы обобщенных каскадных кодов использовали либо простейшие, тривиальные случаи, либо пользовались методами модификации линейных блоковых кодов, что не всегда эффективно и удобно в инженерных приложениях. Таким образом, наряду с высокими потенциальными характеристиками обобщенные каскадные коды с известными процедурами синтеза кодов первой ступени практически малопригодны для повышения помехоустойчивости передачи дискретных сообщений в телекоммуникационных системах и сетях.

Переход в предлагаемых каскадных кодовых конструкциях к недвоичным блоковых кодам на первой ступени обобщенного каскадного кода позволяет использовать хорошо известные линейные коды с максимально достижимым кодовым расстоя-

нием (МДР коды), например, коды Рида-Соломона (РС), а также недвоичные коды, ассоциированные с алгебраическими кривыми (алгеброгеометрические коды). Рассмотрим алгебраические процедуры синтеза цепочки вложенных друг в друга недвоичных кодов РС и алгеброгеометрических кодов.

4.1. Использование кодов Рида-Соломона на первом каскаде. Коды РС – это недвоичные коды БЧХ, у которых длина кода равна мощности алфавита символов, над которыми построен код. Другими словами, РС коды – это недвоичные коды БЧХ над GF(q), у которых поле символов над GF(q) совпадает с полем $GF(q^m)$, т.е. m=1, q > 2.

В соответствии с положениями алгебраической теории блоковых кодов РС код, как и всякий код БЧХ, задается порождающим многочленом (12). В то же время, в силу того, что мощность алфавита символов определяет длину кода, порождающий многочлен РС кода можно выразить как произведение вида (12) с произвольным числом последовательных степеней примитивного элемента поля: $g(x) = \prod_i (x - \alpha^i)$, где $\alpha^i \in GF(q)$.

Параметры кодов РС удовлетворяют верхней кодовой границе Синлгтона: $d \le n - k + 1$, а число информационных символов кода изменяется не «скачкообразно», а может быть произвольной величиной в пределах длины кода.

Кроме того, исходя из структуры конечного поля, над которым строится РС кода, следует отметить простоту построения цепочки вложенных друг в друга кодов. Действительно, рассмотрим множество порождающих многочленов:

$$g_l(x) = (x - \alpha^i)(x - \alpha^{i+1})...(x - \alpha^{i+j})$$

$$g_2(x) = (x - \alpha^i)(x - \alpha^{i+1})...(x - \alpha^{i+j-1})$$

$$...$$

$$g_j(x) = (x - \alpha^i)$$

и соответствующих им кодов РС над GF(q), $\alpha \in GF(q)$.

Справедливо следующее утверждение о цепочке кодов, являющихся подкодами друг друга.

Утверждение 2. Для любого $1 \le l \le q - 1$ код РС над GF(q), заданный порождающим многочленом $g_l(x)$, является подкодом РС кода с порождающим многочленом $g_{l+1}(x)$.

Доказательство. Рассмотрим кодовое слово РС кода с порождающим многочленом $g_l(x)$ для любого $1 \le l \le q - 1$. Код РС – циклический код, следовательно, его можно выразить как произведение

$$c(x) = i(x)g_l(x).$$

С учетом введенных выше обозначений имеем:

$$c(x) = i(x)(x - \alpha^i)(x - \alpha^{i+1})...(x - \alpha^{i+l}).$$

Перегруппируем сомножители, запишем:

$$c(x) = \left(i(x)(x - \alpha^{i+l})\right)(x - \alpha^i)(x - \alpha^{i+1})...(x - \alpha^{i+l-1}).$$

Обозначим

$$i'(x) = i(x)(x - \alpha^{i+l}),$$

получим:

$$c(x) = i'(x)(x - \alpha^i)(x - \alpha^{i+l})...(x - \alpha^{i+l-1}) = i'(x)g_{l+1}(x).$$

Таким образом, произвольное кодовое слово РС кода с порождающим многочленом $g_l(x)$ обязательно является кодовым словом РС кода с порождающим многочленом $g_{l+1}(x)$. Следовательно, для любого $1 \le l \le q - 1$ код РС над GF(q), заданный порождающим многочленом $g_l(x)$, является подкодом РС кода с порождающим многочленом $g_{l+1}(x)$.

Алгебраическую процедуру синтеза (второй этап) предлагаемых каскадных кодовых конструкций с кодами РС на первом каскаде представим в следующем виде.

Шаг 1. Ввод исходных данных. Расчет параметров $A_i > 0$ и $b_i \ge 0$, определяющих внутреннюю структуру каскадного кода.

Шаг 2. Расчет $p_i = \frac{A_i}{a}$ и конструктивных кодовых параметров i-го кода первой ступени.

Шаг 3. Формирование множества $(x - \alpha^s)(x - \alpha^{s+1})...(x - \alpha^{s+q-k_i-1})$ корней порождающего многочлена кода РС для i-го кода первой ступени, причем $k_i = p_1 + p_2 + ... + p_i$, $s = const$.

Шаг 4. Формирование порождающего многочлена кода РС для i-го кода первой ступени.

Шаг 5. Если $i < m + 1$ переход к шагу 2.

Шаг 6. С использованием методов линейной алгебры по m сформированным порождающим многочленам РС кода построение квадратной матрицы H_0^j.

Шаг 7. Если $j \le n_2$ переход к шагу 2.

Шаг 8. Вывод результата: n_2 квадратных матриц H_0^j, $j = \overline{1, n_2}$, порядка n_1.

Разработанные алгебраические процедуры позволяют реализовать второй этап синтеза предлагаемых каскадных кодовых конструкций с кодами РС на первом каскаде. Ниже исследуются алгебраические процедуры синтеза с алгеброгеометрическими кодами на первом каскаде предлагаемых каскадных кодовых конструкций.

4.2. Использование алгеброгеометрических кодов на первом каскаде. Алгеброгеометрические коды – линейные блоковые коды, ассоциированные с алгебраическими кривыми [10, 11]. В основе их построения лежат фундаментальные понятия о линейных пространствах, построенных посредством

отображения множества точек гладкой проективной кривой.

Рассмотрим алгеброгеометрический код, заданный через порождающую матрицу

$$G = \begin{pmatrix} F_0(p_0) & F_0(p_1) & ... & F_0(p_{n-1}) \\ F_1(p_0) & F_1(p_1) & ... & F_1(p_{n-1}) \\ ... & ... & ... & ... \\ F_{k-1}(p_0) & F_{k-1}(p_1) & ... & F_{k-1}(p_{n-1}) \end{pmatrix} = \left\| F_j(p_i) \right\|_{n,k}.$$

По определению [10, 11], кодовые слова $(c_0, c_1, ..., c_{n-1})$ такого алгеброгеометрического (n, k, d) кода над GF(q) задаются равенством

$$\sum_{j=0}^{k-1} I_j F_j(P_i) = c_i ,$$

где I_j – значения символов информационной последовательности, $j = \overline{0, k-1}$; P_i – проективные точки алгебраической кривой, т.е. решения однородного алгебраического уравнения, задающие кривую, $i = \overline{0, n-1}$; $F_j(P_i)$ – значения генераторных функций в точках кривой.

Очевидно, что значения символов кодового слова c_i зависят как от значений символов информационной последовательности I_j, так и значений генераторных функций в точках кривой $F_j(P_i)$. В то же время, исходя из определения алгеброгеометрических кодов, каждое кодовое слово можно представить как произведение некоторой информационной последовательности (как вектора) на матрицу G, составленную из значений генераторных функций. Это положение дает возможность построения цепочки вложенных друг в друга алгеброгеометрических кодов, для их использования на первом каскаде предлагаемых каскадных кодовых конструкций. Справедливо следующее утверждение.

Утверждение 3. Пусть P_i – проективные точки алгебраической кривой, $F_j(P_i)$ – значения генераторных функций в точках кривой, $j = \overline{0, M-1}$, используемые для построения алгеброгеометриеского кода. Тогда линейный блоковый код, заданный порождающей матрицей $G = \left\| F_j(p_i) \right\|_{n,l+1}$, $1 \le M-1$, является подкодом линейного блокового кода с порождающей матрицей $G = \left\| F_j(p_i) \right\|_{n,l}$.

Доказательство. Рассмотрим кодовое слово алгеброгеометического кода с порождающей матрицей $G = \left\| F_j(p_i) \right\|_{n,l+1}$. По определению, его можно представить в виде:

$$(c_0, c_1, ..., c_{n-1}) = \left(\sum_{j=0}^{l} I_j F_j(P_0), \sum_{j=0}^{l} I_j F_j(P_1), ..., \sum_{j=0}^{l} I_j F_j(P_{n-1}) \right).$$

Перегруппируем слагаемые, получим:

$$\left(\sum_{j=0}^{l-1} I_j F_j(P_0) + I_l F_l(P_0), \sum_{j=0}^{l-1} I_j F_j(P_1) + I_l F_l(P_1), ..., \sum_{j=0}^{l-1} I_j F_j(P_{n-1}) + I_l F_l(P_{n-1}) \right).$$

Заметим, что

$$\left(\sum_{j=0}^{l-1} I_j F_j(P_0), \sum_{j=0}^{l-1} I_j F_j(P_1), ..., \sum_{j=0}^{l-1} I_j F_j(P_{n-1}) \right) = (c'_0, c'_1, ..., c'_{n-1}),$$

где $(c'_0, c'_1, ..., c'_{n-1})$ – кодовое слово алгеброгеометрического кода с порождающей матрицей $G = \left\| F_j(p_i) \right\|_{n,l}$.

Тогда, после подстановки получим:

$$(c_0, c_1, ..., c_{n-1}) = \left(c'_0 + I_l F_l(P_0), c'_1 + I_l F_l(P_1), ..., c'_{n-1} + I_l F_l(P_{n-1}) \right).$$

Заметим, что для алгеброгеометрического кода с $G = \left\| F_j(p_i) \right\|_{n,l}$ для $j \ge 1$ все соответствующие $F_j(p_i) = 0$, т.е. для любого кодового слова $(c_0, c_1, ..., c_{n-1})$ имеем равенство

$$(c_0, c_1, ..., c_{n-1}) = (c'_0, c'_1, ..., c'_{n-1}).$$

Следовательно, любое кодовое слово алгеброгеометического кода с порождающей матрицей $G = \left\| F_j(p_i) \right\|_{n,l+1}$ принадлежит алгеброгеометрическому коду с порождающей матрицей $G = \left\| F_j(p_i) \right\|_{n,l}$, т.е. имеем искомую цепочку подкодов.

Алгебраическую процедуру синтеза (второй этап) предлагаемых каскадных кодовых конструкций с алгеброгеометрическими кодами на первом каскаде представим в следующем виде.

Шаг 1. Ввод исходных данных. Расчет параметров $A_i > 0$ и $b_i \ge 0$, определяющих внутреннюю структуру каскадного кода.

Шаг 2. Расчет $p_i = \frac{A_i}{a}$ и конструктивных кодовых параметров i-го кода первой ступени.

Шаг 3. Формирование множества генераторных функций алгеброгеометрического кода для i-го кода первой ступени, причем $k_i = p_1 + p_2 + ... + p_i$, $s = \text{const}$.

Шаг 4. Формирование порождающей матрицы алгеброгеометрического кода для i-го кода первой ступени.

Шаг 5. Если $i < m+1$, переход к шагу 2.

Шаг 6. С использованием методов линейной алгебры по m сформированным порождающим мат-

рицам алгеброгеометрического кода построение квадратной матрицы H_0^j.

Шаг 7. Если $j \le n_2$, переход к шагу 2.

Шаг 8. Вывод результата: n_2 квадратных матриц H_0^j, $j = \overline{1, n_2}$, порядка n_1.

Разработанные алгебраические процедуры позволяют реализовать второй этап синтеза предлагаемых каскадных кодовых конструкций с алгеброгеометрическими кодами на первом каскаде.

Выводы

Таким образом, в результате проведенных исследований теоретически обоснованы и аналитически формализованы каскадные кодовые конструкции с улучшенными свойствами.

В основе предлагаемых каскадных кодовых конструкций лежит дальнейшее развитие обобщенных каскадных кодов посредством их аналитического описания, исследования методов синтеза и декодирования на случай недвоичных кодовых слов с дальнейшим возможным применением алгоритмов декодирования с мягкими решениями.

Предложены также алгебраические процедуры синтеза разработанных каскадных кодовых конструкций с использованием недвоичных блоковых кодов (кодов РС и алгеброгеометрических кодов).

Разработанные алгебраические процедуры позволяют практически реализовать синтез предлагаемых каскадных кодовых конструкций с улучшенными свойствами.

Перспективным направлением дальнейших исследований является разработка алгоритмов декодирования предлагаемых каскадных кодовых конструкций с мягкими решениями, исследование возможности обмена мягкими решениями в итеративной процедуре турбо-продуктивного декодирования.

Список литературы

1. Turbo Product Code Encoder / Decoder. [Электронный ресурс]. – Режим доступа к ресурсу: www.aha.com.

2. IEEE 802.16 Broadband Wireless Access Working Group. Turbo Code Comparison (TCC v TPC). [Электронный ресурс]. – Режим доступа к ресурсу: http://ieee802.org/16.

3. Turbo Product Code FEC. Comtech EF Data Corp. [Электронный ресурс]. – Режим доступа к ресурсу: available at www.comtechefdata.com.

4. Berrou C. Near Shannon Limit Error- Correcting Coding and Decoding: Turbo Codes / C. Berrou, A. Glavieux, P. Thitimajshima // Proc. of the Intern. Conf. on Commun. – 1993, May. – P. 1064-1070.

5. MacKay D.J.C. Near Shannon limit performance of low density parity check codes / D.J.C. MacKay, R.M. Neal // IEEE Electronics Letters. – Aug. 1996.– V.32, №18. – P. 1645-646.

6. Приходько С.И. Исследование методов построения каскадных кодовых конструкций для повышения помехоустойчивости передачи дискретных сообщений / С.И. Приходько, С.А. Гусев, В.А. Зубенко // Системи управління, навігації та зв'язку. – К.: ГП «ЦНИИ навигации и управления», 2011. – Вып. 1(17). – С. 219-224.

7. Блох Э.Л. Обобщенные каскадные коды (Алгебраическая теория и сложность реализации) / Э.Л. Блох, В.В. Зяблов. – М.: Связь, 1976. – 240 с.

8. Мак-Вильямс Ф.Дж. Теория кодов, исправляющих ошибки / Ф.Дж. Мак-Вильямс, Н.Дж.А. Слоэн. – М.: Связь, 1979. – 744 с.

9. Скляр Б. Цифровая связь. Теоретические основы и практическое применение / Б. Скляр. – М.: Вильямс, 2003. – 1104 с.

10. Гоппа В.Д. Коды на алгебраических кривых / В.Д. Гоппа // Докл. АН СССР. – 1981. – Т. 259, № 6. – С. 1289-1290.

11. Влэдуц С.Г. Линейные коды и модулярные кривые / С.Г. Влэдуц, Ю.И. Манин // Современные проблемы математики. – М.: ВИНИТИ. – 1984. – Т. 25. – С. 209-257.

Поступила в редколлегию 1.02.2011

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

РОЗРОБКА КАСКАДНИХ КОДОВИХ КОНСТРУКЦІЙ З ПОКРАЩУВАНИМИ ВЛАСТИВОСТЯМИ

С.І. Приходько, С.А. Гусев, В.А. Зубенко

Розглядаються методи побудови каскадних кодових конструкцій, зокрема, турбо-продуктивні коди (Turbo Product Codes). Розвивається підхід турбо-продуктивного кодування на основі узагальнення каскадних кодових конструкцій на випадок недвійкових послідовностей з можливістю використання методів декодування з ітеративним обміном м'якими рішеннями.

Ключові слова: *кодові конструкції, турбо-продуктивне кодування.*

DEVELOPMENT OF CASCADE CODE CONSTRUCTIONS WITH THE IMPROVED PROPERTIES

S.I. Prikhod'ko, S.A. Gusev, V.A. Zubenko

The methods of construction of cascade code constructions are examined, including turbo product codes. Approach of the turbo product encoding develops on the basis of generalization of cascade code constructions in case of unbinary sequences with possibility of the use of methods of decoding with a iterative exchange by soft decisions.

Keywords: *code constructions, turbo product encoding.*