УДК 621.391.037.3

Н.Ю. Бабанов, А.А. Гладких, С.М. Наместников, С.В. Шахтанов

СВОЙСТВА ЦИКЛИЧЕСКИХ СТРУКТУР В СИСТЕМЕ ПЕРЕСТАНОВОЧНОГО ДЕКОДИРОВАНИЯ ИЗБЫТОЧНЫХ КОДОВ[1]

Бабанов Николай Юрьевич, *доктор технических наук, окончил Нижегородский государственный университет им. Н.И. Лобачевского, проректор по программам развития Нижегородского государственного технического университета им. Р.Е. Алексеева. Имеет монографии и статьи в области обработки сигналов и защиты информации. [e-mail: babanov@nntu.ru].*

Гладких Анатолий Афанасьевич, *доктор технических наук, окончил Военную академию связи (ВАС) им. С.М. Буденного, адъюнктуру ВАС, профессор кафедры «Телекоммуникации» Ульяновского государственного технического университета (УлГТУ). Имеет монографии, учебные пособия, статьи и патенты РФ в области помехоустойчивого кодирования и защиты информации. [e-mail: a.gladkikh@ulstu.ru].*

Наместников Сергей Михайлович, *кандидат технических наук, окончил УлГТУ, аспирантуру УлГТУ, доцент кафедры «Телекоммуникации» УлГТУ. Имеет статьи в области статистической обработки сигналов. [e-mail: sernam@ulstu.ru].*

1 Исследование выполнено при финансовой поддержке РФФИ и Правительства Ульяновской области в рамках научного проекта № 19-47-730011.

Шахтанов Сергей Валентинович, *окончил Ленинградское высшее военное инженерное училище связи, старший преподаватель кафедры «Инфокоммуникационные технологии и системы связи» Нижегородского государственного инженерно-экономического университета. Имеет публикации в области помехоустойчивого кодирования и защиты информации. [e-mail: r155p@bk.ru].*

Аннотация

Практика применения в составе крупных датацентров оптических кабелей приобретает устойчивую тенденцию перехода от одномодовых волокон к многомодовым их аналогам. Это объясняется рядом экономических показателей, выигрышных для многомодовых волокон, и широкими возможностями с их помощью передавать значительные объемы данных с высокими скоростями на короткие расстояния в границах конкретного объекта. По этой причине подобная тенденция начинает прослеживаться на объектах транспортной инфраструктуры, в авиастроении и судостроении. При этом объективно ожидаемый проигрыш по показателям коэффициента битовых ошибок в многомодовых кабелях удачно компенсируется средствами помехоустойчивого кодирования. В этой связи наблюдается повышенный интерес к системам перестановочного декодирования для систематических избыточных кодов, позволяющих использовать когнитивные методы обработки цифровых данных. Это обеспечивает адекватное ускорение процедуры декодирования таких кодов по временным интервалам, близким к скорости обмена данными в оптических кабелях. Выигрыш по времени достигается путем предварительного вычисления порождающих матриц эквивалентных кодов, структура которых задается стохастической перестановкой символов принятых комбинаций в зависимости от текущего вектора помехи. Результат подобного вычисления хранится в когнитивной карте декодера. Благодаря этому, время, необходимое для оперативного вычисления эквивалентного кода, заменяется кратким временем поиска готовой матрицы из памяти когнитивной карты с использованием циклических свойств перестановок.

Ключевые слова: мягкое решение символа, перестановка, орбиты перестановок, эквивалентный код, перестановочное декодирование, когнитивная карта декодера.

doi: 10.35752/1991-2927-2020-2-60-101-108

PROPERTIES OF CYCLIC STRUCTURES IN THE SYSTEM OF PERMUTATION DECODING OF REDUNDANT CODES

Nikolai Iurevich Babanov, *Doctor of Sciences in Engineering; graduated from Lobachevski State University of Nizhny Novgorod; Vice-Rector for Development Programmes of Nizhny Novgorod State Technical University n.a. R.E. Alekseev; an author of articles and monographs in the field of signal processing and information security. e-mail: babanov@nntu.ru.*

Anatolii Afanasevich Gladkikh, *Doctor of Sciences in Engineering; graduated from the Marshal Budjonny Military Academy of Signal Corps; completed his postgraduate studies at the Military Academy of Communications; Professor at the Department of Telecommunications of Ulyanovsk State Technical University; an author of monographs, textbooks, articles, and patents in the field of noise-immune coding and information security. e-mail: a.gladkikh@ulstu.ru.*

Sergei Mikhailovich Namestnikov, *Candidate of Sciences in Engineering; graduated from Ulyanovsk State Technical University, completed postgraduate studies at UlSTU; Associate Professor of the Department of Telecommunications at UlSTU; an author of articles in the field of statistical signal processing. e-mail: sernam@ulstu.ru.*

Sergei Valentinovich Shakhtanov, *graduated from the Leningrad Higher Military Engineering School of Communications; Senior Lecturer of the Department of Infocommunication Technologies and Communication Systems at Nizhny Novgorod State Engineering and Economic University; an author of articles in the field of noise-immune coding and information security. e-mail: r155p@bk.ru.*

Abstract

The practice of using optical cables as part of large data centers is gaining a steady trend of switching from single-mode fibers to their multimode counterparts. This is due to a number of economic indicators that are advantageous for multimode

fibers and their wide capabilities to transmit significant amounts of data at high speeds over short distances within the boundaries of a specific object. For this reason, a similar trend is beginning to be observed in transport infrastructure, aircraft and shipbuilding. At the same time, the objectively expected loss in terms of the bit error rate in multimode cables is successfully compensated by means of noise-tolerant encoding. In this regard, there is an increased interest in permutation decoding systems for systematic redundant codes that allow the use of cognitive methods of digital data processing. This provides an adequate acceleration of the decoding procedure for such codes at time intervals close to the speed of data exchange in optical cables. The time gain is achieved by preliminary calculation of generating matrices of equivalent codes, the structure of which is set by stochastic permutation of the symbols of the accepted combinations depending on the current interference vector. The result of this calculation is stored in the decoder's cognitive map. Due to this, the time required for rapid calculation of the equivalent code is replaced by a short search time for the finished matrix from the memory of the cognitive map using the cyclic properties of permutations.

Key words: soft symbol solution, permutation, permutation orbits, equivalent code, permutation decoding, cognitive decoder map.

Введение

Практически ни одна из известных систем передачи данных с использованием средств избыточного кодирования не позволяет осуществить процедуру обучения декодера для достижения эффекта ускорения обработки принятых данных. Приемник, за редким исключением, не в состоянии предсказать поведение источника информации, который может направить приемнику по каналу с помехами любую из заданного множества комбинаций $I(t)$. Кроме того, априори в канале связи действует неизвестный вектор помехи $Er(t)$, что в совокупности с $I(t)$ усиливает общую неопределенность $Rn(t)$ для приемника. Единственным методом обработки данных на приеме, для которого в процессе декодирования можно указать некую детерминированную составляющую $Dn(t)$, является метод перестановочного декодирования (ПД), описанный в работах [1, 2]. Поэтому в самом общем случае процесс ПД для блоковых систематических кодов можно представить выражением

$$PD(t)=\begin{cases} Rn(t)=I(t)+Er(t), \\ Dn(t). \end{cases}$$

Наличие детерминированной составляющей $Dn(t)$ позволяет осуществить «обучение» декодера, распознавать конкретные перестановки и выдавать готовые решения по обработке данных в зависимости от сложившейся по времени ситуации отбора надежных символов. Результаты обучения, как правило, заносятся в память декодера, которая реализуется в формате когнитивной карты декодера (ККД). Процесс заполнения ККД определяет процедуру обучения декодера. Это может быть выполнено двумя способами. Во-первых, в ходе оперативной работы декодера, когда новые сведения об эквивалентных кодах заносятся в ККД. Во-вторых, когда искусственно генерируются перестановки символов и комбинации перестановок, не имеющие аналогов среди ранее обработанных, заносятся в ККД до начала работы системы ПД. В первом случае процесс обучения является незавершенным и может продолжаться неопределенное время. В этом случае ККД считается несовершенной. Во втором случае обучение считается законченным и ККД является совершенной.

Цель работы – выявить закономерности циклических трансформаций перестановок нумераторов символов кодовых векторов и использовать эти свойства для решения задачи минимизации объема памяти ККД.

ПД с использованием когнитивной карты

Принцип ПД с использованием ККД и его преимущества перед классическим методом описаны в работах [3, 4]. В основном эти преимущества относятся к возможностям наиболее полного использования введенной в код избыточности. Подобная задача решается за счет обязательной процедуры мягкой обработки двоичных или недвоичных символов (в зависимости от расширения двоичного поля Галуа, в котором обрабатываются векторы избыточного кода) и выделения из кортежа принятых символов наиболее надежных из них для формирования эквивалентного кода (ЭК). Поскольку ЭК формируется на приемной стороне, то влияние мешающих факторов оказывается на уровне внутренних сбоев процессора приемника. Важным элементом ПД с использованием ККД является структура заполнения данными ЭК этой карты.

Если использовать все возможные перестановки символов кодовой комбинации, то на это потребуется ровно $n!$ перестановок, где n – длина кодового вектора. Это означает, что в ККД должны быть записаны ровно $n!$ параметров различных ЭК со значениями проверочных частей матриц $\boldsymbol{H}$ из состава порождающих матриц $\boldsymbol{G}$ таких кодов, что является контрпродуктивным.

В условиях реализации алгоритма ПД кодовую комбинацию X некоторого избыточного кода C представляют в виде конечного множества из n элементов, т. е. $|X|=n$. Занумеруем элементы из X в виде последовательности натуральных нумераторов так, чтобы $X=|1, 2, ..., n|$. Применение в процедуре декодирования мягких решений символов (МРС) λ_i обеспечивает возможность образования биекции отображений X в перестановку X_p за счет сортировки нумераторов таким образом, чтобы на позициях информационных

разрядов оказались нумераторы и, следовательно, их жесткие решения с наибольшими значениями λ_i. Такие значения целесообразно вырабатывать на базе стирающего канала связи с широким интервалом стирания в соответствии с аналитическим выражением вида:

$$\lambda_i(z) = \left\| \frac{\lambda_{\max}}{\mu\sqrt{E_b}} \times z_i \right\|, \text{ при } 0 \le z_i \le \mu\sqrt{E_b}, \quad (1)$$

где $\lambda_{\max}$ – максимальное значение мягкого решения (задается конструктором); μ – значение интервала стирания (обычно $0 \le \mu \le 1$); E_b – энергия сигнала на бит; z_i – реально зафиксированное значение сигнала (как правило, из-за воздействия деструктивных факторов отличается от номинального) [5]. Условный оператор выработки МРС представляется выражением

$$\lambda_i(z) = \begin{cases} \left\| \left(\lambda_{\max} / \mu\sqrt{E_b}\right) \times z_i \right\|, \text{ при } 0 \le z_i \le \mu\sqrt{E_b}; \\ \lambda_{\max}, \text{ при } \mu\sqrt{E_b} \le z_i \le (2-\mu)\sqrt{E_b}; \\ -\left\| \left(\lambda_{\max} / \mu\sqrt{E_b}\right) \times z_i \right\|, \text{ при } (2-\mu)\sqrt{E_b} \le z_i \le 3\sigma. \end{cases}$$

Таким образом, выражение (1) характеризует набор линейных функций, имеющих максимальное значение именно в области математического ожидания обрабатываемых сигналов.

В отличие от известного метода отношений правдоподобий [2] представленное выражение (1) не имеет связи с дисперсией помехи, что позволяет применять его в оптических системах связи, например, при использовании модуляции PAM-4. Действительно, в оптических системах при измерении уровня помех вместо дисперсии σ^2 гауссовского шума используется понятие «коэффициента ошибок» и выражение вида $\lambda_i(z) = \left(2z_i\sqrt{E_b}\right)/\sigma^2$ для оптических каналов связи теряет смысл. В новых условиях кодовый вектор длины n в процессоре приемника фиксируется в виде некоторой последовательности $+\lambda_1, +\lambda_2, -\lambda_3, \ldots, +\lambda_k, \ldots, -\lambda_{n-1}, +\lambda_n$, в которой знак «+» соответствует биту со значением 1, а знак «–» соответствует информационному биту со значением 0. Для реализации процедуры упорядочения символов по значениям их МРС знаки жестких решений значения не имеют. Сортировка завершается, если, например, установлено, что $|\lambda_3| \ge |\lambda_n| \ge |\lambda_5| \ge \ldots \ge |\lambda_1| \ge |\lambda_2|$, и на этой основе формируется биекция вида:

$$b = \begin{pmatrix} 1 & 2 & 3 & \ldots & n-1 & n \\ \lambda_3 & \lambda_n & \lambda_5 & \ldots & \lambda_1 & \lambda_2 \end{pmatrix}.$$

В последнем выражении верхняя строка определяет область определения перестановки, которая в прикладном значении для теории избыточного кодирования совпадает с длиной n кодового вектора выбранного кода C_j, а нижняя строка определяет область значений МРС. В биекции b для элементов нижней строки важно выделить две группы значений МРС, которые будут определять два непересекающихся класса эквивалентности элементов из области определения. В общем виде это выражается в виде произведения двух непересекающихся циклов нумераторов вида $(3\,n\,5\ldots) \times (\ldots 12)$. Следовательно, группа нумераторов левого цикла представляет множество наиболее надежных элементов $\{F_{rel}\}$ принятого кодового вектора. Число элементов левого класса эквивалентности определяется значением числа информационных символов k кода C_j, правый класс эквивалентности $\{\overline{F_{rel}}\}$ определяется числом избыточных элементов кода $r = n - k$, где k – число информационных разрядов в коде. Для каждого принятого вектора формируются две орбиты: орбита X_k – с элементами информационных разрядов ЭК и орбита x_r – с элементами избыточных разрядов ЭК. Очевидно, что хранить в памяти ККД все перестановки с соответствующими им элементами проверочных матриц $\boldsymbol{H}$ нерационально. В целях сокращения объема памяти ККД предлагается использовать свойства цикличности перестановок. Для этого доказывается ряд важных утверждений, основанных на свойствах линейных преобразований матриц и циклических особенностях орбит перестановок нумераторов.

Свойства нумераторов перестановок ККД

Высокоскоростная передача данных по оптическим линиям требует особой организации работы декодера избыточного кода, отвечающего заданному темпу поступления данных на его вход. Это становится возможным на основе реализации следующих свойств.

Свойство 1. Образующей комбинацией любого цикла (орбиты) называется та комбинация нумераторов, которая при суммировании всех ее элементов дает наименьшее значение среди оставшихся других подобных сумм комбинаций данной орбиты.

Действительно, любая перестановка нумераторов из множества $\{F_{rel}\}$ всегда может быть циклически приведена к минимальным значениям нумераторов, которые определяют структуру перестановки и формируют ее образ. Например, перестановки для $N = \binom{10}{3} = 120$ формируют 12 орбит, которые в лексикографическом формате представлены ниже. Здесь принято $A = 10$.

123	124	125	126	127	128	129	135	136	137	138	147
234	235	236	237	238	239	23A	246	247	248	249	258
345	346	347	348	349	34A	134	357	358	359	35A	369
456	457	458	459	45A	145	245	468	469	46A	146	47A
567	568	569	56A	156	256	356	579	57A	157	257	158
678	679	67A	167	267	367	467	68A	168	268	368	269
789	78A	178	278	378	478	578	179	279	379	479	37A
89A	189	289	389	489	589	689	28A	38A	48A	58A	148
19A	29A	39A	49A	59A	69A	79A	139	149	159	169	259
12A	13A	14A	15A	16A	17A	18A	24A	25A	26A	27A	36A

Заметно, что числа верхнего ряда, которые являются образующими орбит, минимальны по сумме цифр, входящих в эти числа. Именно этот ряд в последующем будет формировать ККД, что означает уменьшение объема памяти ККД в k раз. Это важно с точки зрения практического использования кодов относительно большой длины.

Свойство 2. Образующая комбинация цикла должна представляться в лексикографическом виде и с увеличением значений нумераторов по мере их циклического сдвига они должны сохранять лексикографическую структуру. Такой порядок способствует быстрому отысканию образующей комбинации и ее орбиты при любом начальном условии перестановки нумераторов в процедуре декодирования кодового вектора.

В таблице приведены орбиты перестановок двоичного кода Хэмминга (7, 4, 3). Для удобства все перестановки представлены в лексикографическом формате.

Таблица

Орбиты перестановок кода Хэмминга (7, 4, 3)

G_1	G_2	G_3	G_4	$\Delta \equiv 0$
1234	**1236**	**1245**	**1246**	***1235***
2345	2347	2356	2357	*2346*
3456	1345	3467	1346	*3457*
4567	2456	1457	2457	*1456*
1567	3567	1256	1356	*2567*
1267	1467	2367	2467	*1367*
1237	1257	1347	1357	*1247*

В таблице данные пятой орбиты, которые указаны курсивом, не образуют ЭК, поскольку определители матриц этой орбиты и соответственно их переставленные варианты равны нулю. Указанная особенность характерна только для двоичных кодов. Четыре других орбиты позволяют сформировать эквивалентные коды и их порождающие матрицы G_1, G_2, ..., G_4, которые могут быть вычислены априори и занесены в память ККД. Длина цикла орбит составляет n шагов. Указанные матрицы являются эталонными для своих орбит и в зависимости от содержания перестановки (порядка следования нумераторов) трансформируются за счет линейных преобразований в соответствующую матрицу ЭК. В качестве примера рассмотрим перестановки первой орбиты. Для этой группы перестановок эталонной матрицей является порождающая матрица кода G_1.

$$G_1 = \begin{pmatrix} 1^1 & 0^2 & 0^3 & 0^4 & 1^5 & 0^6 & 1^7 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}. \qquad (2)$$

В выражении (2) показатели степеней элементов первой строки являются нумераторами столбцов матрицы G_1. Комбинация нумераторов **1234** является образующей комбинацией. Выделим из матрицы (2) элементы проверочной матрицы $\boldsymbol{H}$ и сформулируем свойство 3.

$$H = \begin{pmatrix} 1^5 & 0^6 & 1^7 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}. \qquad (3)$$

Свойство 3. Каждой лексикографически упорядоченной образующей комбинации любого цикла соответствует единственная отличная от других проверочная матрица, которая является обязательным атрибутом эталонной порождающей матрицы систематического ЭК. Действительно, это происходит для любого набора нумераторов всегда после подстановки слева к преобразованной проверочной матрице единичной матрицы размерности $k \times k$.

Указанное утверждение доказано численным методом. Его суть заключается в том, что приемник в группе нумераторов $\{F_{rel}\}$ может зафиксировать любую последовательность из допустимых по параметрам кода, например, 7465. Приводя указанную комбинацию нумераторов к лексикографической форме, получаем 4567 и связываем полученную перестановку единственным образом как комбинацию первой орбиты. Следовательно, в последующих преобразованиях для поиска порождающей матрицы ЭК будет использовано выражение (3).

Свойство 4. При циклическом сдвиге вправо нумераторов образующей комбинации в лексикографически упорядоченном виде происходит только циклический сдвиг столбцов эталонной проверочной матрицы вправо, при условии, что наибольший из допустимых нумераторов справа при движении по циклу не обратился в наименьший нумератор слева.

Это означает, что при циклическом сдвиге нумераторов от значения **1234** к значению 2345 матрица $\boldsymbol{H}$ трансформируется к виду:

$$H_{1234}=\begin{pmatrix}1^5 & 0^6 & 1^7\\ 1 & 1 & 1\\ 1 & 1 & 0\\ 0 & 1 & 1\end{pmatrix}\Rightarrow H_{2345}=\begin{pmatrix}1^7 & 1^5 & 0^6\\ 1 & 1 & 1\\ 0 & 1 & 1\\ 1 & 0 & 1\end{pmatrix}. \quad (4)$$

Такие циклические сдвиги продолжаются до значения перестановки вида 4567. Циклический переход через максимальное значение нумератора, равного n, в разряде лексикографически организованной перестановки с номером k приводит к циклическим сдвигам строк матрицы H_{ijun} снизу вверх, где нумераторы такие, что $i<j<u<n$. Например,

$$H_{4567}=\begin{pmatrix}1^5 & 0^6 & 1^7\\ 1 & 1 & 1\\ 1 & 1 & 0\\ 0 & 1 & 1\end{pmatrix}\Rightarrow H_{1567}=\begin{pmatrix}0^5 & 1^6 & 1^7\\ 1 & 0 & 1\\ 1 & 1 & 1\\ 1 & 1 & 0\end{pmatrix}. \quad (5)$$

Следовательно, для первой орбиты получаем

$$H_{1567}=\begin{pmatrix}0^5 & 0^6 & 1^7\\ 1 & 0 & 1\\ 1 & 1 & 1\\ 1 & 1 & 0\end{pmatrix}\Rightarrow H_{1267}=\begin{pmatrix}1^5 & 1^6 & 0^7\\ 0 & 1 & 1\\ 1 & 0 & 1\\ 1 & 1 & 1\end{pmatrix}. \quad (6)$$

Отсюда вытекает следующее важное свойство.

Свойство 5. В условиях последовательного циклического сдвига комбинации лексикографически упорядоченных нумераторов при переходе наибольшего допустимого нумератора по абсолютному значению справа в единичный элемент слева соответствует перемещению нижней строки части проверочной матрицы снизу вверх и соответствующему циклическому перемещению остальных строк.

Вскрытые особенности матричных преобразований характерны не только для двоичных кодов. Проверкой установлено, что для орбит недвоичных кодов Рида-Соломона указанные закономерности справедливы. Принципиально в памяти декодера может храниться только часть порождающей матрицы в формате элементов части проверочной матрицы $\boldsymbol{H}$. На основании выявленных закономерностей за число шагов $\omega<n$ циклических сдвигов строк и столбцов исходной матрицы $\boldsymbol{H}$ определяется требуемая проверочная составляющая порождающей матрицы ЭК.

Свойство 6. В случаях, отличных от лексикографически упорядоченного следования нумераторов перестановки, эталонная матица орбиты приводится к требуемой проверочной матрице за счет сортировки столбцов эталонной матрицы в порядке, определяемом перестановкой из X_r, а сортировка строк – за счет порядка следования нумераторов, определяемого перестановкой из X_k.

Это происходит по причине определенности размеров матрицы $\boldsymbol{H}$, размерность которой в системе порождающей матрицы составляет значение $k\times r$. Пусть приемник зафиксировал последовательности нумераторов надежных и ненадежных символов $\{F_{rel}\}=\{7154\}$ и $\{\overline{F_{rel}}\}=\{\overline{623}\}$ соответственно. Для решения задачи поиска ЭК первая из этих последовательностей приводится декодером к лексикографическому формату $\{F_{rel}\}_{lex}=\{1457\}$, из которого становится ясно, что данная перестановка относится к третьей орбите, для которой в памяти ККД хранится матрица вида:

$$H_{1245}=\begin{pmatrix}1^3 & 1^6 & 1^7\\ 1 & 0 & 1\\ 0 & 1 & 1\\ 1 & 1 & 0\end{pmatrix}\Rightarrow ...H_{1457}=\begin{pmatrix}1^2 & 0^3 & 1^6\\ 1 & 1 & 1\\ 0 & 1 & 1\\ 1 & 1 & 0\end{pmatrix}. \quad (7)$$

Обозначим в правом столбце матрицы нижним индексом нумераторы строк. Тогда

$$H_{1457}=\begin{pmatrix}1^2 & 0^3 & 1_1^6\\ 1 & 1 & 1_4\\ 0 & 1 & 1_5\\ 1 & 1 & 0_7\end{pmatrix}\Rightarrow H_{7154}=\begin{pmatrix}1^2 & 1^3 & 0_7^6\\ 1 & 0 & 1_1\\ 0 & 1 & 1_5\\ 1 & 1 & 1_4\end{pmatrix}.$$

Выполнена перестановка строк. После чего выполняется перестановка столбцов.

$$H_{7154} = \begin{pmatrix} 1^2 & 1^3 & 0_1^6 \\ 1 & 0 & 1_1 \\ 0 & 1 & 1_5 \\ 1 & 1 & 1_4 \end{pmatrix} \Rightarrow H_{7154\ 623} = \begin{pmatrix} 0^6 & 1^2 & 0_7^3 \\ 1 & 1 & 0_1 \\ 1 & 0 & 1_5 \\ 1 & 1 & 1_4 \end{pmatrix}. \quad (8)$$

Выражение (8) представляет проверочную часть порождающей матрицы ЭК для простановки вида $\{7154\}$ $\{\overline{623}\}$. Это снижает объем ККД и резко уменьшает сложность вычислительного процесса поиска порождающей матрицы ЭК.

Покажем это на примере кода (7, 4, 3). Для такого кода допустимо общее число перестановок, равное значению $N_{\text{общ}} = \binom{7}{4} = 5040$. Собственно, такое число порождающих матриц ЭК должно быть записано в ККД, что крайне нерационально, но наличие орбит X_k и X_r существенно сокращает объем памяти ККД. Действительно, число перестановок для некоторого фиксированного кортежа X_k равняется $k!$, а для соответствующего кортежа из равно (n-r)!. Поскольку для обозначенного в примере кода $k!$ = 4! = 24, а $(n-r)!$ = 3! = 6, то всего комбинаций перестановок для фиксированных орбит X_k и X_r равно 4! × 3! = 144, следовательно, объем ККД может быть уменьшен на три порядка поскольку 5040 : 144 = 35, с учетом длины цикла равного 7, получаем всего 5 комбинаций для образующих орбит из всего множества перестановок. Поиск номера орбиты и, следовательно, поиск соответствующей эталонной матрицы ЭК при произвольной комбинации нумераторов надежных символов возможен при использовании двух алгоритмов. Центральной частью этих алгоритмов является приведение полученных в результате сортировки приемником нумераторов надежных символов в перестановку, организованную лексикографически. Далее возможен тривиальный перебор лексикографической перестановки по циклу до получения по свойству 1 перестановки наименьшего веса по сумме цифр, входящих в перестановку. С учетом суммирования данных сложность такого алгоритма возможно оценить как $O = (n \log n)$.

При использовании второго алгоритма вычислительная система декодера ориентируется на перестановки, которые заканчиваются на максимальное значение нумератора, находящегося в крайнем правом разряде. Поскольку таких комбинаций в цикле ровно k, то сложность этого алгоритма можно оценить как $O = (k \log k)$,что более рационально с токи зрения использования вычислительного ресурса декодера.

Заключение

Использование в процедуре ПД результатов приведенных выше утверждений позволяет резко сократить время обработки данных, что положительно отражается на темпах обработки цифровых данных в условиях применения высокоскоростных многомодовых оптических линий связи, особенно при использовании сложных видов модуляции. Объемы требуемой памяти ККД и методы поиска необходимых порождающих матриц ЭК описан в работах [6, 7]. Подробное описание организации памяти ККД приводится в работе [8]. Кроме того, объем памяти ККД сокращается в k раз.

Важно отметить, что приведенные свойства перестановок в полном объеме справедливы для недвоичных кодов. При этом многие вычислительные операции выполняются на расширенных полях Галуа, в системе десятичных чисел, что выгодно отличает ПД таких кодов от классических алгоритмов. В ходе использования таких кодов основная трудность будет заключаться в выработке МРС, однако эта тема требует специального обсуждения и специфических технических решений.

СПИСОК ЛИТЕРАТУРЫ

1. MacWilliams F.J. Permutation Decoding of Systematic Codes // Bell System Tech. J. 1964. Vol. 43. pp 485–505.

2. Morelos-Zaragoza R. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. Пер. с англ. Афанасьева В.Б. М. : Техносфера, 2005. 320 с.

3. Комашинский В.И., Соколов Н.А. Когнитивные системы и телекоммуникационные сети // Вестник связи. 2011. № 10. С. 4–8.

4. Гладких А.А. Перестановочное декодирование как инструмент повышения энергетической эффективности систем обмена данными // Электросвязь. 2017. № 8. С. 52–56.

5. Ал Тамими Т.Ф.Х. Система быстрых матричных преобразований в процедуре перестановочного декодирования недвоичных избыточных кодов // Докл. XX Междунар. конф. РНТОРЭС «Цифровая обработка сигналов – DSPA». М., 2018. С. 164–169.

6. Конопелько В.К., Липницкий В.А. Теория норм синдромов и перестановочное декодирование помехоустойчивых кодов. 3-е изд. М. : Едиториал УРСС, 2012. 176 с.

7. Пат. 2718224 Российская Федерация, МПК7 H04L 1/20, H03M 13/50. Перестановочный декодер с систе-

мой быстрых матричных преобразований / Пчелин Н.А., Гладких А.А., Климов Д.В. ; заявитель и патентообладатель ФНПЦ АО НПО «Марс». № 2019131005 ; заявл. 30.09.2019 ; опубл. 31.03.2020, Бюл. № 10.

8. Carrasco R., Johnston M.A. Non-binary error control coding for wireless communication and data storage. J. Wiley & Sons, Ltd, 2008. 302 p.

REFERENCES

1. MacWilliams F.J. Permutation Decoding of Systematic Codes. *Bell System Tech. J.*, 1964, vol. 43, pp. 485–505.

2. Morelos-Zaragoza R. *Iskusstvo pomekhoustoichivogo kodirovaniia. Metody, algoritmy, primenenie.* Per. s angl. Afanaseva V.B. [The Art of Noise-Tolerant Coding. Methods, Algorithms, and Applications. Transl. from Engl. by Afanasev V.B.]. Moscow, Technosphere Publ., 2005. 320 p.

3. Komashinskii V.I., Sokolov N.A. Kognitivnye sistemy i telekommunikatsionnye seti [Cognitive Systems and Telecommunication Networks]. *Vestnik sviazi* [Bulletin of Communications], 2011, no. 10, pp. 4–8.

4. Gladkikh A.A. Perestanovochnoe dekodirovanie kak instrument povysheniia energeticheskoi effektivnosti sistem obmena dannymi [Permutation Decoding as a Tool to Improve the Energy Efficiency of Data Exchange Systems]. *Elektrosviaz* [Telecommunications and Radioengineering], 2017, no. 8, pp. 52–56.

5. Al Tamimi T.F.H. Sistema bystrykh matrichnykh preobrazovanii v protsedure perestanovochnogo dekodirovaniia nedvoichnykh izbytochnykh kodov [The System of Fast Matrix Transformations in Permutation Decoding of Non-Binary Redundant Codes]. *Dokl. XX Mezhdunar. konf. RNTORES "Tsifrovaia obrabotka signalov – DSPA"* [Proc. of the 20th Int. Conf. RNTORES "Digital Signal Processing – DSPA"]. Moscow, 2018, pp. 164–169.

6. Konopelko V.K., Lipnitskii V.A. *Teoriia norm sindromov i perestanovochnoe dekodirovanie pomekhoustoichivykh kodov.* 3-e izd. [The Theory of Norms of Syndromes and Permutation Decoding of Error-Correcting Codes. The 3d Edition]. Moscow, Editorial URSS Publ., 2012. 176 p.

7. Russian Federation Patent 2718224. MPK7 H04L 1/20, H03M 13/50. Pchelin N.A., Gladkikh A.A., Klimov D.V. *Perestanovochnyi dekoder s sistemoi bystrykh matrichnykh preobrazovanii* [Permutation Decoder with the System of Fast Matrix Transformations]. Applicant and Proprietor: FRPC JSC 'RPA 'Mars'. Application: 2019131005. Date of filing: September 30, 2019. Date of publication: March 31, 2020. Bull. no. 10.

8. Carrasco R., Johnston M.A. *Non-binary Error Control Coding for Wireless Communication and Data Storage.* J. Wiley & Sons, Ltd, 2008. 302 p.