УДК 621.391.037.3

Д.В. Ганин, Г.М. Тамразян, С.В. Шахтанов, Б. Саид, А.Д. Бакурова

ПРОЦЕДУРА ПОИСКА МНОЖЕСТВА ВЫРОЖДЕННЫХ МАТРИЦ В СИСТЕМЕ ПЕРЕСТАНОВОК ДВОИЧНОГО БЛОКОВОГО КОДА

Ганин Дмитрий Владимирович, *кандидат экономических наук, окончил Нижегородскую сельскохозяйственную академию, проректор по научной работе и инновационной деятельности, доцент кафедры «Инфокоммуникационные технологии и системы связи» Нижегородского государственного инженерно-экономического университета. Имеет статьи и патенты РФ в области помехоустойчивого кодирования и систем восстановления данных. [e-mail: ngiei135@mail.ru].*

Тамразян Георгий Михайлович, *кандидат технических наук, окончил Ульяновский государственный технический университет. Инженер ФНПЦ АО «НПО «Марс». Имеет статьи и патенты РФ в области помехоустойчивого кодирования и защиты информации. [e-mail: tamrazz@bk.ru].*

Шахтанов Сергей Валентинович, *старший преподаватель кафедры «Инфокоммуникационные технологии и системы связи» НГИЭУ. Имеет публикации в области помехоустойчивого кодирования и защиты информации. [e-mail: r155p@bk.ru].*

Саид Басем, *аспирант кафедры «Телекоммуникации» УлГТУ, окончил магистратуру УлГТУ по направлению «Телекоммуникационные технологии и системы связи». Имеет публикации в области помехоустойчивого кодирования и защиты информации. [e-mail: alsamery@mail.ru].*

Бакурова Анастасия Денисовна, *студентка бакалавриата кафедры «Телекоммуникации» УлГТУ по направлению «Телекоммуникационные технологии и системы связи». Имеет публикации в области помехоустойчивого кодирования и защиты информации. [e-mail: bakurova.ad@mail.ru].*

Аннотация

Особенности перестановочного декодирования (ПД) блоковых помехоустойчивых кодов в современных системах обмена данными обсуждались в работах [1–5]. Главными из них являются: асимптотически лучшие по сравнению с известными алгоритмами возможности по исправлению ошибок за счет полного использования введенной в код избыточности; возможности использования применительно к процедуре декодирования прогрессивных технологий, связанных с когнитивными методами обработки данных; исключения из процедуры декодирования сложных алгоритмов поиска локаторов ошибок и их последующего исправления; внятное использование свойств циклических перестановок нумераторов столбцов порождающих матриц кодов в целях существенного сокращения объемов памяти когнитивной карты декодера. Вместе с этим, ряд важных направлений в использовании системы ПД остается нераскрытым. К таким направлениям целесообразно в первую очередь отнести исследования, связанные с поиском возможностей каскадных конструкций блоковых кодов, когда на внешней ступени обработки данных используется некоторый недвоичный код, а на внутренней ступени реализуется подходящий для этого двоичный блоковый код. Главным недостатком двоичных кодов является неоднозначность перестановок нумераторов столбцов порождающих матриц таких кодов, приводящих в ряде случаев к формированию вырожденных информационных матриц и не обеспечивающих в таком случае получение эквивалентного кода. По этой причине выявление указанных перестановок на этапе проектирования кодеков двоичных кодов имеет принципиальное значение. В статье особое внимание уделяется методам регулярного поиска множества вырожденных матриц произвольных блоковых кодов с целью оперативной их замены доброкачественными перестановками и сохранения общего темпа обработки данных в системе каскадной конструкции. Это очень важно для оптических линий связи при реализации сложных видов модуляции совместно с системой прямой коррекции ошибок.

Ключевые слова: порождающая матрица кода, перестановочное декодирование, когнитивная карта декодера.

doi: 10.35752/1991-2927-2019-4-58-82-89

A PROCEDURE FOR FINDING A SET OF DEGENERATE MATRICES IN A BINARY BLOCK CODE PERMUTATION SYSTEM

Dmitrii Vladimirovich Ganin, *Candidate of Sciences in Economics; graduated from the Nizhny Novgorod Agricultural Academy; Vice-rector for Research and Innovation, Associate Professor of the Department of Infocommunication Technologies and Communication Systems of the Nizhny Novgorod State University of Engineering and Economics; an author of articles and patents of the Russian Federation in the field of noise-resistant coding and data recovery systems. e-mail: ngiei135@mail.ru.*

Georgii Mikhailovich Tamrazian, *Candidate of Sciences in Engineering; graduated from Ulyanovsk State Technical University; Engineer of Federal Research-and-Production Center Joint Stock Company 'Research-and-Production Association 'Mars'; an author of research papers, and patents in the field of noiseless coding and information security. e-mail: tamrazz@bk.ru.*

Sergei Valentinovich Shakhtanov, *Senior Lecturer of the Department of Infocommunication Technologies and Communication Systems of the Nizhny Novgorod State University of Engineering and Economics; an author of publications in the field of noise-resistant coding and information protection. e-mail: r155p@bk.ru.*

Basem Said, *Postgraduate Student of the Department of Telecommunications of Ulyanovsk State Technical University; graduated from UlSTU with a Master's degree in Telecommunication Technologies and Communication Systems; an author of publications in the field of noise-resistant coding and information protection. e-mail: alsamery@mail.ru.*

Anastasiia Denisovna Bakurova, *Bachelor Student of the Department of Telecommunications of Ulyanovsk State Technical University in the field of Infocommunication Technologies and Communication Systems; an author of publications in the field of noise-resistant coding and information protection. e-mail: bakurova.ad@mail.ru.*

Abstract

The features of permutation decoding (PD) of block noise-resistant codes in modern data exchange systems were discussed in articles [1–5]. The main of them are: asymptotically better in comparison with the known algorithms possibilities for error correction due to the full use of the redundancy introduced into the code; the possibility of using progressive technologies related to cognitive methods of data processing in relation to the decoding procedure; exceptions to the decoding procedure of complex algorithms for finding error locators and their subsequent correction; intelligible use of the properties of cyclic permutations of column numerators generating matrix codes in order to significantly reduce the memory of the cognitive card decoder. At the same time, several important directions in the use of the PD system remain undisclosed. Primarily, it is advisable to include such areas to research related to the search features of the cascade designs block codes, while a non-binary code is used at the outer processing stage and this appropriate binary block code is implemented at the internal stage. The main disadvantage of binary codes is the ambiguity of permutations of the column numerators of the generating matrices of such codes, which in some cases lead to the formation of degenerate information matrices, and do not provide an equivalent code in this case. For this reason, the identification of these permutations at the design stage of binary codecs is of fundamental importance. Authors pay a special attention to the methods of regular search of a set of degenerate matrices of arbitrary block codes in order to replace them promptly with benign permutations and to preserve the General rate of data processing in the system of cascade construction. This is very important for optical communication lines when implementing complex types of modulation in conjunction with the forward error correction.

Key words: generating code matrix, permutation decoding, cognitive decoder map.

Введение

Объективно возрастающие потребности в передаче больших объемов данных однозначно влияют на поиск путей повышения пропускной способности внутриобъектовых сетей, сетей облачных вычислений, центров обработки данных (ЦОД) и веб-серверов. Поэтому повышение скоростей передачи в таких структурах с 1–10 Гбит/с до 40–100 Гбит/с и выше становится актуальной задачей, и это вызывает необходимость применения в них многомодовых оптических волокон (МОВ), которые успешно справляются с задачей передачи данных для типичных расстояний объектовых или бортовых сетей. В данном случае МОВ остается более предпочтительным, чем одномодовое оптическое волокно (ООВ), которое несомненно имеет преимущество на линиях связи большой протяженности. В этом контексте можно говорить о медных кабелях, но по мере роста скоростей обмена данными расстояния по кабелям «витая пара» категорий 5e/6 значительно сокращались и в отдельных случаях ограничивались 5–6 м. Для соедине-

ний 40 Гбит/с приходится использовать 8-парные медные кабели. Диаметр такого кабеля (не говоря о весе) в 3–4 раза больше диаметра соответствующего оптического кабеля, а дальность передачи для кабеля OM5 для указанной скорости и не лучшего приемопередатчика типа BiDi составляет 200 м. Для нового стандарта SWDM4 эта дальность уже равна 440 м [6].

Для повышения спектральной эффективности подобных систем МОВ используется метод четырехуровневой амплитудно-импульсной модуляции (PAM-4), который представляется как более сложный, чем метод простой бинарной амплитудной модуляции [7]. При использовании PAM-4 передается удвоенное количество данных за единицу времени. Однако для распознавания четырех уровней от приемника потребуется более совершенное решающее правило, при этом требования к приемнику могут быть рационально снижены за счет использования прямой коррекции ошибок (ПКО). Как отмечалось в работе [8], такой метод защиты данных от ошибок является наиболее надежным согласованием скорости обработки данных в демодуляторе и декодере приемника. При этом решающую роль в этом процессе играет когнитивная карта, которая позволяет заменить сложный процесс матричных вычислений в декодере на процедуру лексикографического поиска соответствующего образца эквивалентного кода в памяти когнитивной карты.

Цель работы – повышение производительности алгоритма декодирования двоичных блоковых помехоустойчивых кодов с перестановочным декодированием (ПД) путем упреждающего вычисления непродуктивных перестановок нумераторов и их эффективной корректировки.

Перестановки в системе двоичных групповых кодов и их особенности

Принципиально в системе каскадного кодирования на внутренней ступени обработки данных могут быть использованы как блоковые коды, так и непрерывные коды. Однако в связи с повышением требований к согласованию высоких скоростей поступления данных на вход приемника цифровых оптических сигналов (ожидаются скорости до 400 Гбит/с) и их последующей обработки в декодере выдвигаются на первый план именно блоковые коды. Непрерывные коды при их декодировании классическими методами требуют накопления определённого объема данных и последовательного просмотра данных вначале в прямом направлении, а затем – в обратном направлении. При этом исправление ошибок происходит именно на обратном движении декодера по принятому кортежу данных. Из-за неравномерности временных интервалов указанной процедуры (очевидно при наличии ошибок временной интервал обратного хода декодера будет отличен от подобного интервала при их отсутствии) эта процедура требует определенных усилий по синхронизации внутренних и внешних декодеров в каскадной схеме, задержке по времени принятия решений в декодере недвоичного кода и необходимой организации системы буферных устройств. С учетом перспектив использования помехоустойчивых кодов в системе постквантовой криптографии неравномерные характеристики по времени декодирования данных открывают возможности для организации так называемых таймингновых атак на систему передачи данных [9]. Все это говорит в пользу применения блоковых кодов, для которых выравнивание временных интервалов декодирования кодовых векторов является вполне реализуемой процедурой [10].

При этом определенный интерес вызывают следующие задачи, которые не были поставлены и решены в известных работах по данной предметной области.

Во-первых, не ясно каково должно быть соотношение между числом информационных разрядов k и числом избыточных разрядов $r = n - k$, где n – длина кодового вектора. Это важно с точки зрения трансформации некоторой текущей перестановки в случаях образования такой комбинации нумераторов ранжированных символов из числа n, которые приводят к появлению невырожденных матриц и которые необходимо рационально менять за счет символов из числа r [3].

Во-вторых, в общих чертах известно, что множество допустимых перестановок для произвольного двоичного кода $\{M_R\}$ всегда меньше множества $\{M_F\}$ перестановок, приводящих к вырожденным матрицам. Другими словами, условие $\{M_R\} > \{M_F\}$ говорит о том, что при ПД в процедуре декодирования целесообразно осуществлять проверку принадлежности некоторого переставленного вектора V_{pem} к множеству $\{M_F\}$. Это потенциально обеспечит уменьшение времени обработки данных в декодере и существенно сократит разрыв по времени между условиями $V_{pem} \in \{M_R\}$ и $V_{pem} \in \{M_F\}$, характерными для известных схем ПД, что снизит риски проведения таймингновых атак на систему обмена данными [10].

Приведенные выше условия имеют между собой противоречивую связь. С одной стороны, уменьшение избыточности снижает эффективность ПД, поскольку снижается объем данных, направленных на замену ненадежных символов. С другой стороны, увеличение избыточности расширяет множество $\{M_F\}$, что затрудняет его определение, лексикографическую организацию и хранение в когнитивной карте декодера.

Оценка рациональной избыточности в системе ПД

В работе [11] показано, что при использовании мягких методов декодирования энергетический выигрыш кода оценивается выражением $D_s = 10\lg(Rd_{\min})$ дБ, где R – относительная скорость кода, а $d_{\min}$ – метрика Хэмминга. Предположим, что в некоторой системе управления команды достижения целевой функции передаются короткими блоками, при этом для обеспечения требуемого уровня достоверности осуществляется простой повтор данных. Тогда $k = r$, $n = 2k$

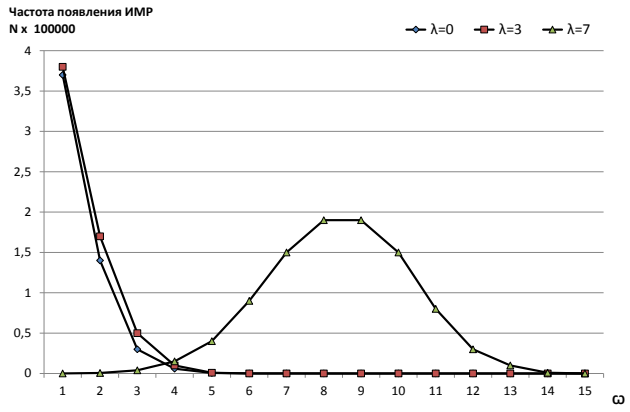

Рис. 1. Частота появления ИМР в кодовом векторе длины $n=15$ при $h=0$ дБ

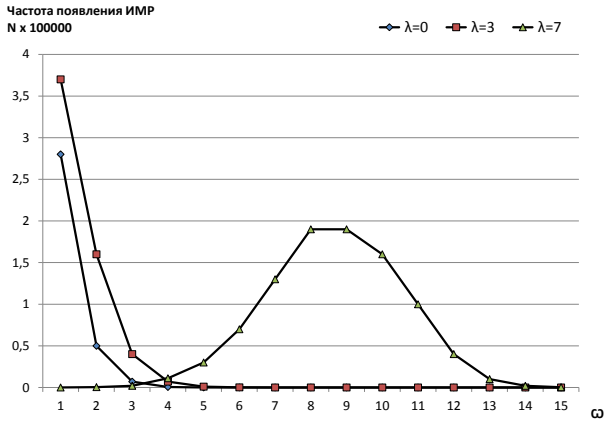

Рис. 2. Частота появления ИМР в кодовом векторе длины $n=15$ при $h=3$ дБ

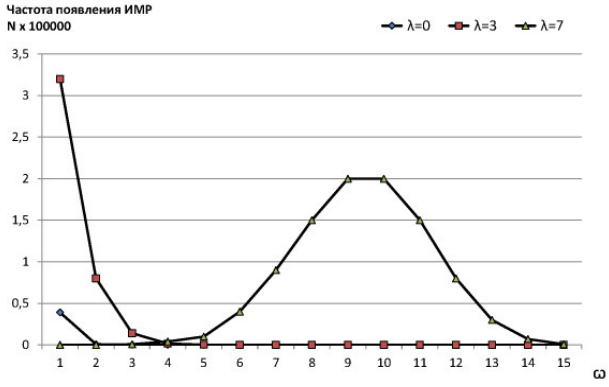

Рис. 3. Частота появления ИМР в кодовом векторе длины $n=15$ при $h=7$ дБ

и $R=0,5$. Легко заметить, что в системе с только жесткими решениями выигрыш $D_s=0$, поскольку $d_{\min}=2$ и декодер не в состоянии исправлять ошибки. Однако в системе с мягкими решениями $\lambda_i=\overline{0,7}$ за счет учета разницы указанных значений при сравнении символов одноименных позиций предпочтение может быть отдано символу с большей оценкой надежности, что равносильно увеличению $d_{\min}$ на единицу. Пусть в системе с повтором данных был передан вектор $V_{pem}=\begin{pmatrix}1 & 1 & 0 & 0 & 1 & 1 & 0 & 0\end{pmatrix}$, а в системе с мягкими решениями приемником был зафиксирован вектор $V_{np}=\begin{pmatrix}1_6 & 1_5 & 0_7 & 1_2 & 1_7 & 1_5 & 0_6 & 0_7\end{pmatrix}$. Нижние индексы при жестких решениях показывают индексы мягких решений (ИМР) λ_i. Посимвольное сравнение данных указывает на то, что на четвертой позиции по результатам сравнения необходимо отдать предпочтение нулю в системе жестких решений, поскольку восьмой символ комбинации при повторе данных имеет более высокий индекс надежности. Очевидно подобным образом можно корректировать все символы вектора при условии высокой корреляции ошибочных символов с низкими оценками. В указанном примере каждый информационный бит имеет свой проверочный разряд. Оценим вариации энергетического выигрыша при изменении параметра k. Пусть код является максимально декодируемым кодом, у которого $d_{\min}=n-k+1$, тогда, подставляя это выражение в выражение для D_s, получаем энергетический выигрыш в оценке вида: $D_{\max}=10\lg\left(k-k^2/n+k/n\right)$ дБ [11]. Пусть вновь $k=r$, упрощая выражение $D_{\max}$, получаем:

$$D_{\max}(k)=10\lg\left(\frac{k+1}{2}\right). \quad (1)$$

Выражение (1) демонстрирует, что при $k=1$ энергетический выигрыш кода равен нулю, а под знаком логарифма находится линейная функция, которая монотонно возрастает по мере увеличения аргумента k и экстремум невозможен. Следовательно, оптимальным соотношением для k и r является их равенство, тогда для каждого символа из k существует ему замена из r. Переход к помехоустойчивому кодированию неизбежно приводит к соотношению вида $k>r$ за счет появления алгебраических зависимостей. В этом случае при $k\gg r$ эффективность ПД снижается. Результаты математического моделирования процесса формирования ИМР при различных отношениях сигнал/шум для вектора длины $n=15$ показаны на рисунках 1–3.

На приведенных рисунках параметр ω указывает на долю конкретной оценки $\lambda_i=\overline{0,7}$ в векторе длиной $n=15$ за весь интервал испытания. Анализ результатов моделирования показывает, что максимум для оценки $\lambda_i=7$ по мере увеличения параметра сигнал/шум смещается вправо, что говорит о повышении потенциальной эффективности ПД и соответствует объективной реальности. В ходе единичного эксперимента интервал испытания включал в себя не менее 10^6 комбинаций, передававшихся по каналу связи с аддитивным белым гауссовским шумом.

Метод выявления вырожденных матриц в системе перестановок

Для оценки множества вырожденных матриц переставленных кодов целесообразно использовать код, у которого $k < r$. При таком соотношении k и r множество $\{M_F\}$ более разнообразно. Поэтому его теоретическая оценка без труда может быть перенесена на код, у которого $k > r$. Исходя из этого в работе был выбран код с параметрами (15, 5, 7) с порождающей матрицей $\boldsymbol{G}$, структура которой приведена ниже.

$$\boldsymbol{G} = \begin{Bmatrix} 1^1 & 0^2 & 0^3 & 0^4 & 0^5 & 1^6 & 0^7 & 1^8 & 0^9 & 0^A & 1^B & 1^C & 0^D & 1^E & 1^F \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \end{Bmatrix}. \quad (2)$$

В выражении (2) по понятным причинам верхними индексами показана нумерация столбцов матрицы $\boldsymbol{G}$, выполненная в шестнадцатеричном формате. Собственно, сама матрица $\boldsymbol{G}$ в систематической форме состоит из двух частей: единичной матрицы $\boldsymbol{E}$ с 1 по 5 столбцы и проверочной части $\boldsymbol{H}$ с 6 по 15 (F-й) столбец. Процесс ПД заключается в замещении столбцов в матрице $\boldsymbol{E}$ на столбцы из матрицы $\boldsymbol{H}$. При этом определитель вновь образованной матрицы $\boldsymbol{Q}$ должен быть равен нулю для возможности формирования эквивалентного кода. Докажем несколько теорем, позволяющих определить структуру перестановок, которые не позволяют получить подобный результат.

Утверждение 1. Перестановки одиночных столбцов, содержащих нули, из проверочной части матрицы в единичную матрицу приводят к вырожденным матрицам, количество которых в точности равно общему числу нулей в проверочной матрице.

Доказательство. Пусть выбран любой столбец из состава матрицы $\boldsymbol{H}$, имеющий хотя бы один нулевой элемент в i-й строке. Тогда подстановка такого столбца в i-й столбец единичной матрицы $\boldsymbol{E}$ приводит к образованию нулевой строки в этой матрице, что однозначно обеспечивает равенство определителя этой новой матрицы нулю. Если в i-й строке матрицы $\boldsymbol{H}$ содержится несколько нулевых элементов, принадлежащих разным столбцам, то каждая подстановка таких столбцов по одному формирует однотипные новые матрицы, отличающиеся только одним элементом. Таким образом, каждый ноль из состава матрицы $\boldsymbol{H}$ формирует новую перестановку, что и требовалось доказать.

По результатам анализа нижней строки части матрицы $\boldsymbol{H}$ возможно получение только четырех переставленных матриц вида, которые приведены ниже.

$$\boldsymbol{Q}_{12346} = \begin{pmatrix} 1^1 & 0^2 & 0^3 & 0^4 & 1^6 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \text{ или}$$

$$\boldsymbol{Q}_{12348} = \begin{pmatrix} 1^1 & 0^2 & 0^3 & 0^4 & 1^8 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \text{ или}$$

$$\boldsymbol{Q}_{12349} = \begin{pmatrix} 1^1 & 0^2 & 0^3 & 0^4 & 0^9 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \text{ и}$$

$$\boldsymbol{Q}_{1234C} = \begin{pmatrix} 1^1 & 0^2 & 0^3 & 0^4 & 1^C \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Таким образом, число одиночных перестановок столбцов из части $\boldsymbol{H}$ в часть $\boldsymbol{E}$ для данного кода составляет 18 вариантов.

В работе [1] было показано, что для кода Хэмминга (7, 4, 3) в системе ПД проявлялась строгая циклическая закономерность в формировании перестановок для конкретного эквивалентного кода. Такая же закономерность наблюдалась и в системе запрещенных перестановок, не обеспечивающих формирование подобного кода. Указанные закономерности позволяли резко сократить объем когнитивной карты декодера. В анализируемом коде подобные закономерности не наблюдаются. Причиной тому служит структура матрицы $\boldsymbol{H}$, которая при $k < r$ носит расширенный характер. Это приводит к необходимости оперативного заполнения когнитивной карты декодера прежде всего для системы отрицательных перестановок.

Можно показать, что, проводя рассуждения, аналогичные перестановкам одиночных столбцов, удается дать приближенную оценку объему отрицательных решений при двух и даже трех подстановках столбцов из матрицы $\boldsymbol{H}$ в матрицу $\boldsymbol{Q}$.

Утверждение 2. Перестановки двух столбцов, содержащих нули на одноименных позициях, из проверочной части матрицы в единичную матрицу приводят к вырожденным матрицам, количество которых равно сумме сочетаний из числа нулей каждой строки проверочной части матрицы по два.

Доказательство. Пусть выбран любой столбец из состава проверочной части матрицы, содержащий нули, и пусть выбрана нулевая позиция, соответствующая аналогичной строке единичной матрицы. В этом случае в соответствии с утверждением 1 будет сформирована переставленная матрица, содержащая чисто нулевую строку. Выбор второго столбца не должен нарушить содержание этой строки наличием единичного элемента, поэтому во втором переставленном столбце на указанной позиции должен находиться нулевой элемент, что и требовалось доказать.

Таким образом, исходя из структуры нулевых элементов строк проверочной части матрицы исследуемого кода, общее число подобных ситуаций будет равно

$$\binom{4}{2}+\binom{3}{2}+\binom{3}{2}+\binom{4}{2}+\binom{4}{2}=$$

$$=3\binom{4}{2}+2\binom{3}{2}=18+6=24.$$

Методом математической индукции приведенные выше утверждения можно распространить на произвольную порождающую матрицу двоичного группового блокового кода.

Проведенными исследованиями установлено, что известная структура проверочной части порождающей матрицы кода, к сожалению, не раскрывает содержания полного множества $\{M_F\}$. Комбинаторный анализ показывает, что причиной вырожденности переставленной матрицы может оказаться совпадение в ней структуры двух строк, предсказать которую по внешнему виду матрицы $\boldsymbol{H}$ не представляется возможным. Пример одной из таких комбинаций переставленных столбцов представлен ниже.

$$\boldsymbol{Q}_{68345}=\begin{pmatrix} 1^6 & 1^8 & 0^3 & 0^4 & 0^5 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Учитывая эту особенность, в декодере необходимо предусматривать проверку перестановок на невырожденность матрицы $\boldsymbol{Q}$, как показано в алгоритме, схема которого представлена на рисунке 4.

После ранжирования символов по значениям ИМР, декодер сверяет полученную последовательность нумераторов столбцов с имеющейся базой. В случае отсутствия данных о выполненной перестановке для нее выполняется проверка определителя не предмет равенства его нулю. В случае положительного решения данная перестановка заносится в базу данных запрещенных перестановок, что соответствует способу, изложенному в работе [12].

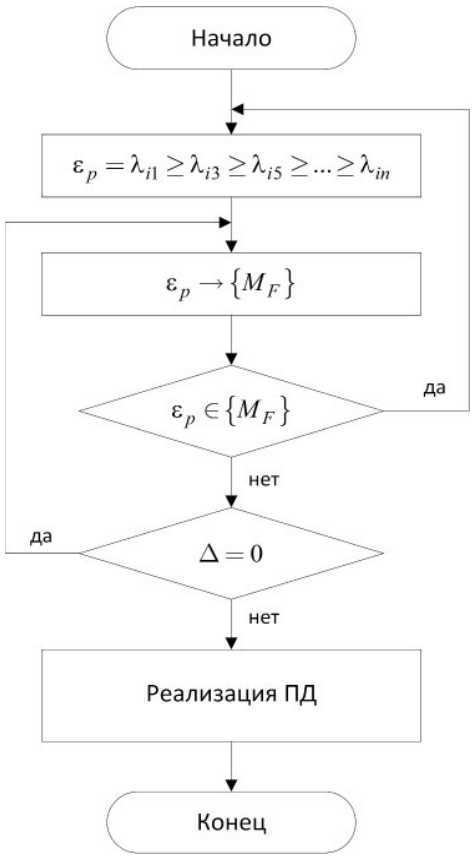

Рис. 4. Алгоритм проверки невырожденности переставленной матрицы кода

Заключение

ПД является разновидностью мягкого декодирования блоковых кодов, что обеспечивает дополнительный энергетический выигрыш в системах внутриобъектовых сетей, строящихся на базе МОВ. Применение в таких системах сложных видов модуляции способно повысить пропускную способность таких сетей, но при этом требует опережающей защиты данных от ошибок. С этой целью используются каскадные методы обработки данных в кодеках, для которых важно эффективно декодировать внутренние коды. В качестве таких кодов целесообразно использовать двоичные блоковые коды с когнитивной обработкой данных, что обеспечивает ускоренное декодирование за счет выбора результата декодирования из списка данных, находящихся в когнитивной карте.

Двоичные коды не являются максимально декодируемыми кодами, поэтому в ПД могут возникать коллизии, суть которых заключается в невозможности сформировать эквивалентные коды для отдельных перестановок. Выявить такие перестановки допустимо с использованием специального раздела когнитивной карты.

Предварительное вычисление элементов такого раздела представляет научную задачу, связанную с анализом структуры проверочной части порождающей матрицы кода. В работе показаны пути решения подобной задачи для кода, у которого информационная часть кодового вектора меньше избыточной в два раза. Показано, что лучшим вариантом ПД блоковых кодов является код, у которого избыточная часть равна избыточной части. Подобного соотношения легко добиться, используя процедуру укорачивания подходящего исходного блокового кода. Проведенными статистическими испытаниями показана целесообразность применения целочисленных ИМР, значения которых принципиально могут быть использованы для декодирования внешнего недвоичного кода в системе каскадного кодирования.

СПИСОК ЛИТЕРАТУРЫ

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

2. Гладких А.А., Ал Тамими Т.Ф.Х. Концепция когнитивной обработки данных в системе перестановочного декодирования недвоичного избыточного кода // Электросвязь. – 2018. – № 9. – С. 69–74.

3. Гладких А.А., Наместников С.М., Пчелин Н.А. Эффективное перестановочное декодирование двоичных блоковых избыточных кодов // Автоматизация процессов управления. – 2017. – № 1 (47). – С. 67–74.

4. Перестановочное декодирование в системе комбинаций кодовых конструкций при оценке биометрических данных / И.Ю. Давыдов, Д.А. Козлов, С.В. Шахтанов, М.Ю. Шибаева // Автоматизация процессов управления. – 2019. – № 3 (47). – С. 67–74.

5. Гладких А.А., Пчелин Н.А., Шахтанов С.В. Минимизация объема памяти когнитивной карты декодера в системе поиска эквивалентных кодов // Радиотехника. – 2018. – № 6. – С. 38–41.

6. Камино Дж. Стандарты внутриобъектового многомодового волокна // Первая миля. – 2019. – № 3. – С. 42–47.

7. Трещиков В.Н., Наний О.Е. Новое поколение DWDM-систем связи / Фотон – экспресс. – 2014. – № 4 (116). – С. 18–23.

8. Гладких А.А., Меновщиков А.В. Методы согласования технологий когерентных сетей с системой прямой коррекции ошибок // Информационно-измерительные и управляющие системы. – 2018. – № 11. – С. 5–10.

9. Goodwil G., Jun B., Pankaj R. A testing methodology for side-channel resistance validation. In: NIST non-invasive attack workshop. 2011. Vol. 7. pp. 115–136.

10. Walters M., Roy S.S. Constant-time BCH error-correcting code. – URL: https://github.com/mjw553/Constant_BCH (дата обращения: 11.09.2019).

11. Гладких А.А. Основы теории мягкого декодирования избыточных кодов в стирающем канала связи. – Ульяновск : УлГТУ, 2010. – 379 с.

12. Пат. 2644507 Российская Федерация, МПК H03M 13/05, G06F 11/10. Перестановочный декодер с режимом обучения / Гладких А.А., Маслов А.А., Пчелин Н.А., Тамразян Г.М., Баскакова Е.С. ; заявитель и патентообладатель ФНПЦ АО «НПО «Марс». – № 2017100488 ; заявл. 09.01.2017 ; опубл. 12.02.2018.

REFERENCES

1. 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 Radio Engineering], 2017, no. 8, pp. 52–56.

2. Gladkikh A.A., Al Tameemi T.F.H. Kontseptsiia kognitivnoi obrabotki dannykh v sisteme perestanovochnogo dekodirovaniia nedvoichnogo izbytochnogo koda [The Concept of Cognitive Data Processing in the System of Permutation Decoding of Non-binary Redundant Code]. *Elektrosviaz* [Telecommunications and Radio Engineering], 2018, no. 9, pp. 69–74.

3. Gladkikh A.A., Namestnikov S.M., Pchelin N.A. Effektivnoe perestanovochnoe dekodirovanie dvoichnykh blokovykh izbytochnykh kodov [Efficient Permutation Decoding of Binary Block Redundant Codes]. *Avtomatizatsiia protsessov upravleniia* [Automation of Control Processes], 2017, no. 1 (47), pp. 67–74.

4. Davydov I.Iu., Kozlov D.A., Shakhtanov S.V., Shibaeva M.Iu. Perestanovochnoe dekodirovanie v sisteme kombinatsii kodovykh konstruktsii pri otsenke

biometricheskikh dannykh [Permutation Decoding in the System of Combinations Code Designs in the Evaluation of Biometric Data]. *Avtomatizatsiia protsessov upravleniia* [Automation of Control Processes], 2019, no. 3 (47), pp. 67–74.

5. Gladkikh A.A., Pchelin N.A., Shakhtanov S.V. Minimizatsiia obema pamiati kognitivnoi karty dekodera v sisteme poiska ekvivalentnykh kodov [Minimizing the Memory Capacity of the Decoder's Cognitive Map in the Search for Equivalent Codes]. *Radiotekhnika* [Journal Radioengineering], 2018, no. 6, pp. 38–41.

6. Kamino J. Standarty vnutriobektovogo mnogomodovogo volokna [Standards of Multimode Intra-Object Fiber]. *Pervaia milia* [Last Mile], 2019, no. 3, pp. 42–47.

7. Treshchikov V.N., Nanii O.E. Novoe pokolenie DWDM-sistem sviazi [New Generation of DWDM Systems]. *Foton – ekspress* [Photonics], 2014, no. 4 (116), pp. 18–23.

8. Gladkikh A.A., Menovshchikov A.V. Metody soglasovaniia tekhnologii kogerentnykh setei s sistemoi priamoi korrektsii oshibok [Prospects of Development of Coherent Networks and Possibilities of Permutation Decoding of Data Coordinated with Speed of Their Receipt]. *Informatsionno-izmeritelnye i upravliaiushchie sistemy* [Journal Information-Measuring and Control Systems], 2018, no. 11, pp. 5–10.

9. Goodwil G., Jun B., Pankaj R. A Testing Methodology for Side-Channel Resistance Validation. *NIST Non-Invasive Attack Workshop*, 2011, vol. 7, pp. 115–136.

10. Walters M., Roy S.S. Constant-Time BCH Error-Correcting Code. Available at: https://github.com/mjw553/Constant_BCH (accessed: 11.09.2019).

11. Gladkikh A.A. *Osnovy teorii miagkogo dekodirovaniia izbytochnykh kodov v stiraiushchem kanale sviazi* [Fundamentals of the Theory of Soft Decoding of Redundant Codes in the Erasure Communication Cannel]. Ulyanovsk, UlSTU Publ., 2010. 379 p.

12. Russian Federation Patent 2644507 MPK H03M 13/05, G06F 11/10. Gladkikh A.A., Maslov A.A., Pchelin N.A., Tamrazyan G.M., Baskakova E.S. *Perestanovochnyi dekoder s rezhimom obucheniia* [Resetting Decoder with Training Mode]. Applicant and Proprietor: FRPC JSC 'RPA 'Mars'. Application: 2017100488. Data of filing: January 09, 2017. Date of publication: February 12, 2018.