УДК 621.391.037.3

А.А. Гладких, С.М. Наместников, Н.А. Пчелин

ЭФФЕКТИВНОЕ ПЕРЕСТАНОВОЧНОЕ ДЕКОДИРОВАНИЕ ДВОИЧНЫХ БЛОКОВЫХ ИЗБЫТОЧНЫХ КОДОВ[1]

Гладких Анатолий Афанасьевич, *доктор технических наук, окончил Военную академию связи им. С.М. Буденного, адъюнктуру ВАС, профессор кафедры «Телекоммуникации» Ульяновского государственного технического университета. 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 там же, доцент кафедры «Телекоммуникации» УлГТУ. Имеет статьи в области статистической обработки сигналов. [e-mail: sernam@ulstu.ru].*

Пчелин Никита Александрович, *окончил Ульяновское высшее военное командное училище связи. Главный конструктор ФНПЦ АО «НПО «Марс». Имеет публикации в области помехоустойчивого кодирования. [e-mail: pna3@yandex.ru].*

Аннотация

В статье рассматривается метод декодирования двоичных блоковых избыточных кодов по упорядоченным статистикам, который реализуется в формате перестановочного декодирования (ПД). Подобные алгоритмы с наибольшей эффективностью используются в системах управления для защиты данных от ошибок при передаче их по каналам, подверженным влиянию деструктивных факторов. С одной стороны, достоинством ПД является возможность обработки кодовых векторов вычисленного эквивалентного кода за пределами метрики Хэмминга, что обеспечивает существенный энергетический выигрыш кода. С другой стороны, процедура выявления свойства линейности переставленной порождающей матрицы эквивалентного кода и последующего приведения этой матрицы к систематической форме, в случае подтверждения свойств ее линейности, является сложной в вычислительном отношении. При этом сложность вычислительного процесса становится экспоненциальной по мере увеличения длины кодовых векторов. В этой связи предлагается новый способ быстрых матричных преобразований, позволяющий привести вычислительный процесс поиска матрицы эквивалентного блокового кода практически любой длины к полиномиальной сложности. Вводится понятие когнитивной карты декодера. Приводятся вероятностные характеристики предложенных декодеров, полученные методом аналитического моделирования каналов связи с различными потоками ошибок.

Ключевые слова: мягкое решение символа, перестановочное декодирование, когнитивная карта декодера, каскадное кодирование.

EFFICIENT PERMUTATION DECODING OF BINARY BLOCK REDUNDANT CODES

Anatolii Afanasevich Gladkikh, *Doctor of Engineering, graduated from S.M. Budyonny Military Communication Academy, finished his postgraduate studies at the same Academy; Professor at the Department of Telecommunications at Ulyanovsk State Technical University; an author of monographs, textbooks, research papers, and patents in the field of noiseless coding and information security. e-mail: a.gladkikh@ulstu.ru.*

Sergei Mikhailovich Namestnikov, *Candidate of Engineering, graduated from Ulyanovsk State Technical University, finished his postgraduate studies at the same University; an author of papers in the field of static methods of signals processing. e-mail: sernam@ulstu.ru.*

Nikita Aleksandrovich Pchelin, *graduated from Ulyanovsk High Education Military Communications Academy; Chief Designer at Federal Research-and-Production Center Joint Stock Company 'Research-and-Production Association 'Mars'; an author of papers in the field of noiseless coding. e-mail: pna3@yandex.ru.*

1 Работа поддерживается грантом РФФИ по проекту № 16-47-732011\16.

Abstract

The article describes a method of decoding of binary block redundant codes with the use of ordered statistics, which is implemented in the framework of permutation decoding (PD). Such algorithms are most effectively used in control systems in order to protect data against errors when sending them along the channels subjected to the influence of destructive factors. On the one hand, the advantage of permutation decoding is the possibility of processing of code vectors of the computed equivalent code outside the Hamming metric, which provides a significant energy code gain (ECG). On the other hand, the process of identifying the properties of rearranged matrix linearity of the equivalent code and bringing this matrix to the systematic form in case of confirmation of the properties of linearity, is a difficult task in the attitude of computation. The complexity of the computational process becomes exponential with increasing length of code vectors. In this context, the authors propose a new method for fast matrix transformations to allow normalizing the computational process of finding the matrix of the equivalent block code of virtually any length to polynomial complexity. The authors also introduce the concept of a decoder cognitive map. The probabilistic characteristics of the proposed decoders obtained by analytical modelling of communication channels with various streams of errors are given.

Key words: soft symbol solution, permutation decoding, decoder cognitive map, concatenated coding.

Введение

Применение средств помехоустойчивого кодирования в современных автоматизированных системах управления обусловлено объективными условиями использования в подобных системах каналов связи с различным уровнем деструктивных факторов [1, 2]. Реализация в таких условиях максимальных возможностей корректирующего кода по исправлению ошибок, как правило, связывается с мягкими методами обработки данных в условиях применения метрики Хэмминга. При этом для многих современных и перспективных систем управления возникает проблема сокращения цикла управления элементами системы, что вызывает необходимость использования коротких блоковых кодов, исправляющих ошибки, которые в лучшей степени приспособлены к системе пакетной передачи данных и синхронизации коротких сигналов управления. Следовательно, в системе защиты от ошибок необходимо реализовать все потенциальные возможности используемых кодов. Естественно, что максимальные возможности кодов по исправлению ошибок реализуются только при использовании мягких методов декодирования. Перестановочное декодирование (ПД) является мощным развитием этого метода, которое базируется на новых методах матричных преобразований и удачно развивает принципы когнитивной организации алгоритмов работы декодеров групповых кодов [3].

Цель работы – разработка алгоритма ПД двоичных блоковых кодов каскадных конструкций на базе быстрых матричных преобразований элементов когнитивной карты внутреннего декодера и оценка их вероятностных характеристик.

Асимптотические оценки различных подходов к обработке принятых данных

В современных телекоммуникационных системах в качестве критерия эффективности применения в них помехоустойчивого кодирования выбирают значение получаемого от этой процедуры энергетического выигрыша. Известно, что в канале с гауссовским шумом при условии, что отношение $E_b/N_0 \to \infty$, в котором значение E_b – энергия сигнала, приходящаяся на бит, N_0 – спектральная плотность гауссовского шума, в случае жестких решений и реализации алгоритма исправления t ошибок энергетический выигрыш оценивается выражением $D_h = 10lg(R(t+1))$ дБ. При использовании алгоритмов исправления стираний энергетический выигрыш оценивается выражением $D_s = 10lg(Rd_{min})$ дБ, где d_{min} – метрика Хэмминга [1]. В приведенных формулах отношение $R = k/n$ – относительная скорость кода, где k – число информационных символов в кодовом векторе длины n. Отсюда следует, что при $E_b/N_0 \to \infty$ энергетический выигрыш при исправлении стираний в два раза выше, чем при обработке жестких решений, поскольку параметр $d_{min} = 2t+1$, и поэтому в пределе выигрыш составляет не более 3 дБ. Указанные соотношения показывают, что безызбыточное кодирование при $n = k$, $t = 0$ и $d_{min} = 1$ в рассматриваемых системах вообще не в состоянии обеспечить какой-либо энергетический выигрыш.

Оценка возможности декодирования двоичных кодов как блоковых, так и сверточных за пределами границ, обозначенных метрикой Хэмминга, важна с точки зрения применения этих кодов в составе композиции кодов в виде последовательных или параллельных соединений кодеков. Идея мягкого декодирования непосредственно вытекает из теоремы Л.М. Финка [4]: при любом коде имеет место неравенство $p_1 \geq p_2 \geq p_3 \geq p_4$. Здесь p_1 – вероятность того, что при посимвольном методе приема (суть жесткого декодера) кодовая комбинация принята с ошибкой (независимо от того, можно ли эту ошибку исправить или обнаружить); p_2 – вероятность того, что при посимвольном методе приема в ходе исправления максимально возможного числа ошибок произошла неисправимая ошибка; p_3 – вероятность того, что при идеальном приеме в целом (аналог мягкого декодера) комбинация ошибочна; p_4 – вероятность того, что при посимвольном приеме принятая комбинация окажется совпадающей с одной из комбинаций кода, но не с той, которая передавалась.

Известны методы декодирования помехоустойчивых кодов, которые реализуют максимальное использование

введенной в код избыточности и обеспечивают получение минимальных вероятностей ошибок p_3 и p_4. Это означает, что код способен исправить больше ошибок (стираний), чем это возможно при использовании метрики Хэмминга. В этом случае асимптотической оценкой энергетического выигрыша от применения блокового двоичного кода может служить выражение $D_m = 10lg(k(1-R+1/n))$ дБ. Предполагается, что $d_{min} = n-k+1$, что соответствует максимально декодируемым кодам.

Известно, что недвоичные коды, например коды Рида-Соломона (РС), достигают значения D_m, что нельзя сказать о двоичных кодах, которые не являются максимально декодируемыми кодами [3]. Как показано в работе [2], максимальной исправляющей способности в процедуре декодирования таких кодов возможно достичь при использовании кластерного подхода. В основе метода лежит принцип разбиения пространства $\{\Omega\}$ разрешенных кодовых векторов на списки, которые в общей классификации имеют свои уникальные номера, характерные для каждого списка. По этому признаку каждый список можно назвать кластером. Номер кластера определяется заранее оговоренными элементами кодовых комбинаций, и эти номера одинаковы для всего множества комбинаций $\{\Omega\}$. Число бит, определяющих номер кластера $0 < n_{cl} \le k$, естественно меньше длины кодового вектора n, поэтому вероятность искажения номера списка $P(n_{cl})$ меньше искажения всего кодового блока $P(n_{cl}) < P(n)$. Для точного определения номера кластера необходимо и достаточно, чтобы биты n_{cl} сопровождались высокими значениями мягких решений символов (МРС). Пусть МРС определяются целочисленными индексами вида λ_i, где $0 \le i \le 7$, тогда для надежного определения номера кластера желательно, чтобы все биты этого номера сопровождались МРС со значениями $\lambda_7 = \lambda_{max}$. Вероятность подобного исхода изучалась с использованием имитационных моделей для блоковых кодов различной длины. В качестве непрерывного канала связи использовался канал с независимым потоком ошибок. В частности, рассматривались коды Боуза-Чоудхури-Хоквингема (БЧХ), для которых выбирались значения n_{cl} от двух до пяти. Результаты отдельных испытаний приведены на рисунке 1. В качестве аргумента использовалось отношение $h = E_b/N_0$, которое показывало вероятность безошибочного определения номера кластера в кодовых комбинациях различной длины. На рисунке 1 в списке кодов параметр n_{cl} указан последней цифрой. Заметно, что даже небольшое увеличение этого параметра приводит к существенному снижению вероятности правильного определения номера кластера $P_{пр}(h)$.

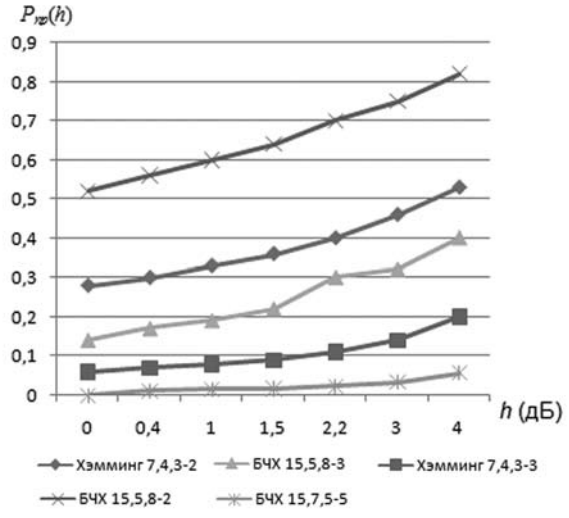

Рис. 1. Вероятности правильного определения номера кластера в зависимости от его длины

Таким образом, выбор номера кластера по максимальным оценкам, следующим друг за другом, является сильным отрицательным условием, которое увеличивает риски неправильного определения списка.

ПД этого правила не требует. Максимальные оценки на длине кодового вектора могут располагаться произвольно. Именно это обстоятельство делает ПД более привлекательным. Исходя из этого и не оценивая на данном этапе анализа сложность построения декодера, можно утверждать, что сохраняется соотношение по вероятности ошибочного декодирования комбинаций блоковых кодов в виде: $P_{перест} < P_{кластер} < P_{мягк} < P_{алгебр}$. При этом достигается максимальный энергетический выигрыш D_m, поскольку в большинстве случаев обеспечивается исправление ошибок за пределами метрики Хэмминга. Доказательства этого утверждения приводятся в работах [5, 6].

Классический алгоритм ПД

Вычислительный процесс при реализации алгоритма ПД осуществляется по шагам.

Шаг 1. Принять биты пришедшего из канала с ошибками кодового вектора $V_{пр}$, сопровождая каждый из них значением МРС λ_i.

Шаг 2. Ранжировать значения МРС и соответствующие им биты по убыванию.

Шаг 3. Сформировать на основе выполнения шага 2 биекцию вида $f\colon V_{пр} \to V_{пер}$ и соответствующую ей перестановочную матрицу P.

Шаг 4. По результатам реализации шага 2 выделить первые k наиболее надежных символов и запомнить их.

Шаг 5. Умножить порождающую матрицу исходного кода G на матрицу P для перестановки столбцов матрицы G в соответствии с шагом 2 и получения новой переставленной матрицы $G_{пер}$.

Шаг 6. Выделить первые k столбцов в матрице $G_{пер}$, получить матрицу $Q_{k \times k}$ и вычислить определитель этой матрицы Δ. Если $\Delta \ne 0$, перейти к шагу 7. Если $\Delta = 0$, отказаться от декодирования, перейти к шагу 2 и выполнить новые перестановки, поменяв местами символ с номером k с символом $k+1$.

Шаг 7. Для матрицы $Q_{k\times k}$ подсчитать матрицу миноров M_Q.

Шаг 8. Найти обратную матрицу $Q^{-1}_{k\times k}$, разделив элементы матрицы $Q^{T}_{k\times k}$ на значение Δ.

Шаг 9. По значениям матрицы $Q^{-1}_{k\times k}$ преобразовать матрицу $G_{пер}$ к систематическому виду $G^{сис}_{пер}$.

Шаг 10. Умножить вектор длины k из шага 4 на матрицу $G^{сис}_{пер}$, получив вектор эквивалентного кода $n_{экв}$.

Шаг 11. Умножить $n_{экв}$ на P^T, выполнив обратное биективное отображение f: $V_{пр} \rightarrow V_{пер}$, и получить вектор $n_{пер}$.

Шаг 12. Складывая поразрядно векторы $V_{пр} \oplus n_{пер} = V_{ош}$, получают вектор ошибок, действовавший в канале связи в моменты фиксации битов вектора $V_{пр}$.

Совершенно очевидно, что производительность декодера существенно снижается в системе матричных вычислений при выполнении шагов алгоритма с шестого по девятый. Главным недостатком алгоритма является необходимость выполнения последовательности шагов даже в том случае, если отдельные комбинации, защищаемые кодом данных в сообщении, повторяются.

Напрашивается техническое решение, которое заключается в том, чтобы запомнить те перестановки столбцов порождающей матрицы G основного кода, которые не приводят к вырождению матрицы $Q_{k\times k}$, и одновременно с этим удержать в памяти декодера содержание преобразованной матрицы $G^{сис}_{пер}$, которая соответствует конкретной перестановке матрицы $Q_{k\times k}$. Это позволяет осуществлять предварительное «обучение» декодера возникновению подобных ситуаций и за счет расширения памяти реализовать когнитивные функции декодера, создавая когнитивную карту тех перестановок столбцов матрицы G, которые обеспечивают получение положительного результата декодирования. В когнитивную карту декодера могут включаться отрицательные решения по перестановкам столбцов. Это необходимо для ускорения процедуры отказа от декодирования или организации повтора данных в случае использования системы с запросом и повторением данных. Когнитивный процесс в таком случае может быть представлен схемой, показанной на рисунке 2.

В указанном процессе можно выделить два режима: режим оперативного обмена данными и режим обучения. В первом случае работа декодера по сути не отличается от классической схемы, но данные по обработке матриц заносятся в когнитивную карту декодера. Во втором случае при отсутствии оперативной работы декодер искусственно генерирует различные последовательности $V_{пр}$, и если они не проявлялись в предыдущих случаях, то новые данные заносятся в когнитивную карту декодера. Наличие такой карты в последующем исключает выполнение шагов с шестого по девятый. Это позволяет существенно сократить время вычислительного процесса декодера и ускорить обработку данных.

Принцип создания когнитивной карты декодера

Применение когнитивных принципов в телекоммуникационных технологиях рассмотрены в работах [7, 8]. Принцип функционирования когнитивного декодера рассмотрим на примере обработки комбинаций кода Хэмминга (7,4,3) с порождающей матрицей вида:

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix}.$$

Каноническая нумерация столбцов матрицы осуществляется слева направо с использованием нумератора столбцов, при этом за каждым номером нумератора постоянно закрепляется конкретный столбец матрицы G. В режиме обучения генератор данных случайным образом формирует наборы из неповторяющихся четырех столбцов (номеров) матрицы G, которые в процедуре декодирования на четвертом шаге будут совпадать с наиболее надежными символами вектора $V_{пр}$. Обозначим эти последовательности через Z_i. В соответствии с этим может быть образованно $C^4_7 = 35$ неповторяющихся последовательностей длины $k = 4$. На основании одной из

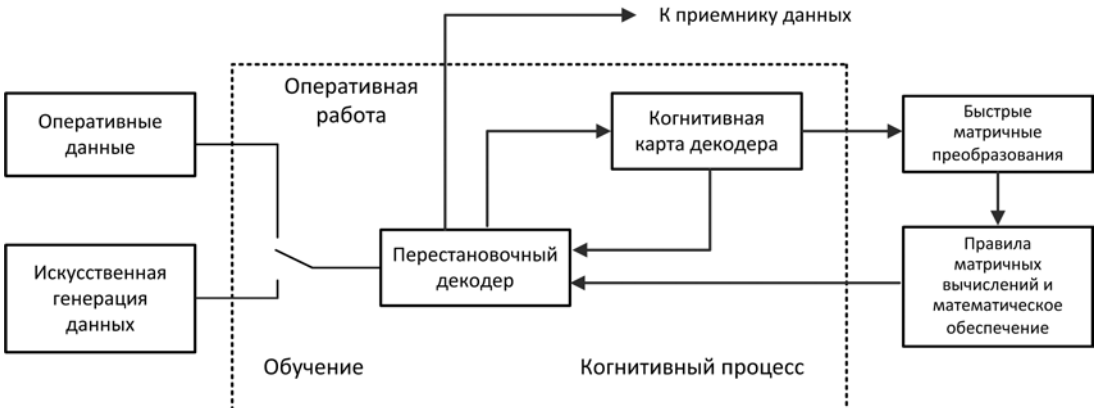

Рис. 2. Структура когнитивного процесса применительно к перестановочному декодеру

таких последовательностей Z_i из порождающей матрицы кода G извлекаются столбцы, последовательность номеров которых в точности соответствует последовательности номеров символов Z_i. Если в результате проверки вырожденности полученной матрицы $Q_{k\times k}$ размерности $k\times k$ определитель этой матрицы $\Delta\neq 0$, то такая последовательность номеров Z_i заносится в базу положительных решений и далее по основному алгоритму отыскивается матрица $G_{пер}^{сис}$, которая также заносится в базу данных и всегда для данного кода будет соответствовать уникальной последовательности Z_i. В случае повторения подобной последовательности номеров символов эта последовательность уже не потребует вычисления матрицы $G_{пер}^{сис}$, что обеспечивает выигрыш временного ресурса, так как матрица извлекается из базы данных в готовом виде. В случае отрицательного исхода, когда определитель матрицы $Q_{k\times k}$ $\Delta=0$, значение последовательности Z_i записывается в базу отрицательных решений. Из 35 различных сочетаний номеров для комбинаций рассматриваемого кода 27 комбинаций отвечают условию $\Delta\neq 0$ и только 8 значений соответствуют условию $\Delta=0$. Базовые значения Z_i по первому условию, когда $\Delta\neq 0$, приведены в таблице 1.

Таблица 1

База положительных решений когнитивной карты декодера

1234	2345	3456	4567	5671	6712	7123	1236	2347
3451	4562	5673	6714	7125	1254	1264	2365	2375
3476	4517	4527	5621	6732	6742	7143	7153	3457

Базовые значения Z_i по условию, когда $\Delta=0$, приведены в таблице 2.

Таблица 2

База отрицательных решений когнитивной карты декодера

1235	2346	4561	5672	6713	7124	3416	5631

Соотношение объемов таблиц указывает на целесообразность применения метода ПД не только для коротких кодов, но и кодов, имеющих большую длину, чем 7. Каждая комбинация цифр из таблиц 1 и 2 включает в себя 4! = 24 перестановки, поэтому предусматривается фиксация иных перестановок указанных групп в базе как положительных, так и отрицательных решений. Так как база положительных решений в три раза больше базы отрицательных решений, целесообразно проверку осуществлять, начиная с проверки отрицательного результата последовательности номеров Z_i. В случае появления последовательности вида Z_x, не равной ни одной из ранее обработанных последовательностей Z_i, вариант Z_x сверяется с базой данных отрицательных решений, и в случае отсутствия подобной комбинации в этой базе данных декодер приступает к обработке данных по основному алгоритму, пополняя по итогам работы либо базу данных положительных решений, либо базу данных отрицательных решений.

Например, для образца $Z_i = 1264$ матрица $G_{пер}$ имеет вид:

$$G_{пер}=\begin{pmatrix}1&0&0&0&0&1&1\\0&1&1&0&0&1&1\\0&0&1&0&1&1&0\\0&0&1&1&0&0&1\end{pmatrix},$$

для которой $\Delta\neq 0$.

В результате тривиальных линейных преобразований, которые достаточно подробно описаны в работе [1], формируется матрица $G_{пер}^{сис}$, которая для образца $Z_i=$ 1264 имеет вид:

$$G_{пер}^{сис}=\begin{pmatrix}1&0&0&0&1&0&1\\0&1&0&0&1&1&0\\0&0&1&0&1&1&1\\0&0&0&1&0&1&1\end{pmatrix}.$$

Набор $Z_i=1264$ и соответствующая ему матрица $G_{пер}^{сис}$ заносятся в базу данных положительных решений. Аналогично выполняется задача в случае отрицательных решений, когда $\Delta=0$. Предложенный способ мягкого когнитивного декодирования систематических блоковых кодов позволяет:

- по крайней мере, в 75% случаев исправлять стирания, кратность которых определяется соотношением $n-k$;
- по сравнению с аналогами существенно сократить время обработки кодовых комбинаций за счет готовых решений по структуре переставленных матриц эквивалентных кодов;
- осуществить предварительное обучение декодера до включения его в оперативную работу, заполнив базы данных декодера по положительным и отрицательным решениям;
- осуществить пополнение баз данных декодера для положительных и отрицательных решений за счет новых комбинаций, не учтенных в ходе предварительного обучения декодера;
- подготовку баз данных положительных и отрицательных решений выполнить на внешней вычислительной системе и ввести в декодер с помощью переносного носителя данных или специально организованного канала связи.

Быстрые матричные преобразования в системе эквивалентных кодов

Предложенный алгоритм обработки данных не является совершенным. Для коротких кодов он вполне приемлем, но с ростом длины кодовых векторов вычислительные затраты на преобразование матриц увеличиваются и становятся заметным препятствием для реализации метода. В ходе исследований была доказана возможность

дополнительного сокращения вычислительных затрат за счет использования быстрых матричных преобразований для поиска эквивалентных кодов.

По сути, эквивалентный блоковый код относительно комбинаций основного кода является отображением конечного множества в себя. Это справедливо и для каждой кодовой комбинации в ходе ее сортировки по значениям МРС, действительно $a,\ b \in X$, где $b = f(\lambda_i)$. В таблицах 1 и 2 приведены неупорядоченные последовательности номеров столбцов порождающей матрицы G исходного кода.

Если упорядочить номера когнитивной карты в порядке возрастания, то появляется возможность быстрого поиска требуемого образца и открываются новые закономерности в преобразованиях матриц. Когнитивная карта декодера в этом случае принимает вид, представленный в таблицах 3 и 4.

Таблица 3

Каноническая база положительных решений когнитивной карты декодера

1234	1236	1237	1245	1246	1256	1257	1267	1345
1347	1357	1457	1467	1567	2345	2347	2356	2357
2367	2456	2457	2467	3456	3457	3467	3567	4567

Таблица 4

Каноническая база отрицательных решений когнитивной карты декодера

1235	1247	1346	1356	1367	1456	2346	2567

Каждое положительное решение из таблицы 3 сопровождается базовой порождающей матрицей, которая в случае перестановки цифр канонического значения положительного решения быстро преобразуется в порождающую матрицу эквивалентного кода в систематической форме.

Пусть в результате обработки данных и выполнения процедуры ранжирования столбцов порождающей матрицы G основного кода была сформирована последовательность 4261 735. Декодер канонизирует эту последовательность, получая 1246 357. В базе данных положительных решений когнитивной карты декодера хранится заранее вычисленная матрица для такой последовательности, которая имеет вид:

	1	2	4	6	3	5	7	Номера столбцов
	1	0	0	0	0	1	1	1
$G_{баз1246357}$	0	1	0	0	1	0	1	2
	0	0	1	0	1	1	1	4
	0	0	0	1	1	1	0	6

Данные базовой матрицы в условиях фиксации последовательности 4261 735 за счет соответствующей перестановки строк и столбцов проверочной матрицы будут приведены к виду, который соответствует заданному образцу эквивалентного кода:

	4	2	6	1	7	3	5	Номера столбцов
	1	0	0	0	1	1	1	4
$G_{экв1246735}$	0	1	0	0	1	0	1	2
	0	0	1	0	1	1	0	6
	0	0	0	1	0	1	1	1

В эквивалентном коде относительно исходного кода меняется содержимое проверочной матрицы и, как следствие, структура порождающего полинома, конфигурация которого зависит от содержания последней строки матрицы в том или ином виде эквивалентной формы. Применение подобного подхода в процессе выполнения классических матричных преобразований позволяет по ориентировочным оценкам сократить вычислительный процесс для кода Хэмминга (7,4,3) на 581 элементарную операцию, а для кода БЧХ (15,5,7) – на 10952 элементарные операции.

Еще больший эффект следует ожидать от применения регистровой логики. Действительно, исходный код имеет порождающий полином $g(x)=x^3+x+1$. Три других формы по структуре строк порождающей матрицы имеют вид $g_{экв1}=x^3+x^2+x+1$, $g_{экв2}=x^3+x^2+1$ и $g_{экв3}=x^3+x^2+x$. Это открывает возможность получать комбинации эквивалентного кода с использованием регистров сдвига, подключая в зависимости от биэкции данных тот или иной регистр сдвига. Последнее обстоятельство значительно упрощает схему реализации кодера эквивалентного кода в системе декодера основного кода. Следует отметить, что полиномы вида $g_{экв1}=x^3+x^2+x+1$ и $g_{экв3}=x^3+x^2+x$ не формируют коды с циклическими свойствами.

Вероятностные характеристики перестановочных декодеров

Для любой системы обмена данными важнейшим показателем является оценка энергетического выигрыша, который обеспечивает та или иная схема защиты данных от ошибок. Подобные асимптотические оценки безотносительно моделей непрерывного канала связи показаны в первой части работы. Применительно к каналу с независимым потоком ошибок такие оценки для классических схем обработки данных, работающих в пределах метрики Хэмминга, обсуждались в [1]. Очевидно, что вероятность ошибки на бит p_b является функцией отношения сигнал-шум, которое в аналитической модели определяется выражением E_b/N_0, где $N_0=2\sigma^2$. Здесь σ^2 – дисперсия белого гауссовского шума. Тогда

$$p_b = \frac{1}{\sigma\sqrt{2\pi}} \int_0^{\sqrt{E_b}} e^{-\frac{(x+\sqrt{E_b})^2}{2\sigma^2}} dx. \qquad (1)$$

Отсюда для кода (7,4,3) легко найти вероятность ошибочного декодирования комбинации при исправлении только одной ошибки алгебраическим методом.

Результаты аналитического моделирования различных схем декодирования кода Хэмминга (7,4,3) представлены на рисунке 3 , где в явной форме проявляется преимущество метода ПД.

Исходя из характеристик, представленных на рисунке 3, всегда можно вычислить вероятность ошибки на бит по соотношению $p_b \approx P_{ком}/n$. В этом случае получаемый энергетический выигрыш в системе с кодом Хэмминга при использовании ПД составит около 6 дБ, что соответствует приведенным выше асимптотическим оценкам.

Наибольший эффект от использования ПД двоичных кодов становится заметным при их применении в составе последовательных турбокодов в качестве внутренних кодов [9]. Вероятность ошибочной регистрации недвоичного символа в коде РС в этом случае определяется отношением:

$$P_{симРС} = \frac{1}{2^m - 1} \sum_{i=(n_2-k_2)/2}^{n_2} i \times C_{n_2}^i \times P_{ком}^i \times \left(1 - P_{ком}\right)^{n_2 - i}, \quad (2)$$

где n_2 – длина кодового вектора кода РС, k_2 – число информационных символов в нем, а m – степень расширения двоичного поля Галуа. Характеристики различных вариантов построения подобных конструкций приведены на рисунке 4.

Вероятность ошибки на бит в этом случае определяется по формуле $p_b \approx P_{симРС}/n$. Вновь заметно, что преимущество имеют коды, декодируемые по принципу ПД.

Заключение

ПД является разновидностью мягкого декодирования блоковых помехоустойчивых кодов. Оно основано на вычислении для каждого кодового вектора, переданного по каналу с ошибками, вектора эквивалентного кода, который образуется за счет последовательного ранжирования мягких решений и создания биекции принятому вектору, на основе которой вырабатывается вектор эквивалентного кода.

Основные трудности при реализации классического алгоритма ПД заключаются в преобразованиях матриц на предмет выявления свойства невырожденности переставленной матрицы кода и приведения такой матрицы к систематической форме.

В работе вскрыты закономерности матричных преобразований, которые характерны для групповых избыточных кодов, применение которых существенно сокращает сложность реализации декодера.

Основой подобной реализации является создание когнитивной карты декодера в канонической форме, которая позволяет выполнить вычисление эквивалентного кода по заранее подготовленному шаблону.

Использование метода позволяет существенно снизить вероятность ошибочного приема кодового вектора за счет исправления стираний за пределами метрики Хэмминга. Это по-

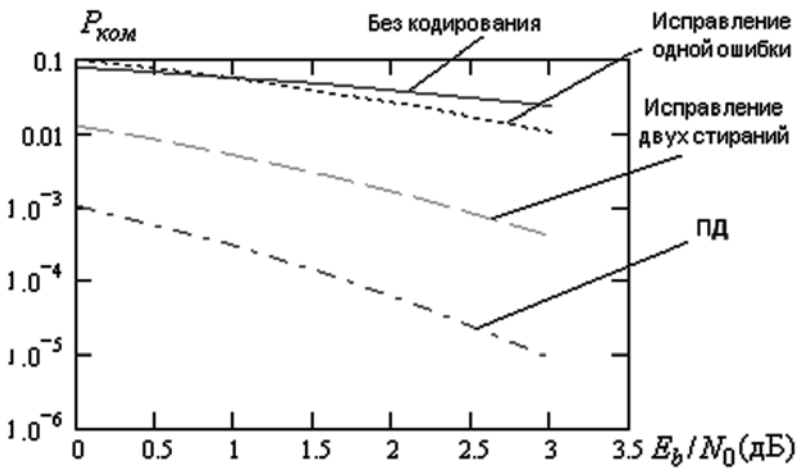

Рис. 3. Вероятности ошибочного приема комбинации в зависимости от отношения сигнал-шум для кода Хэмминга (7,4,3)

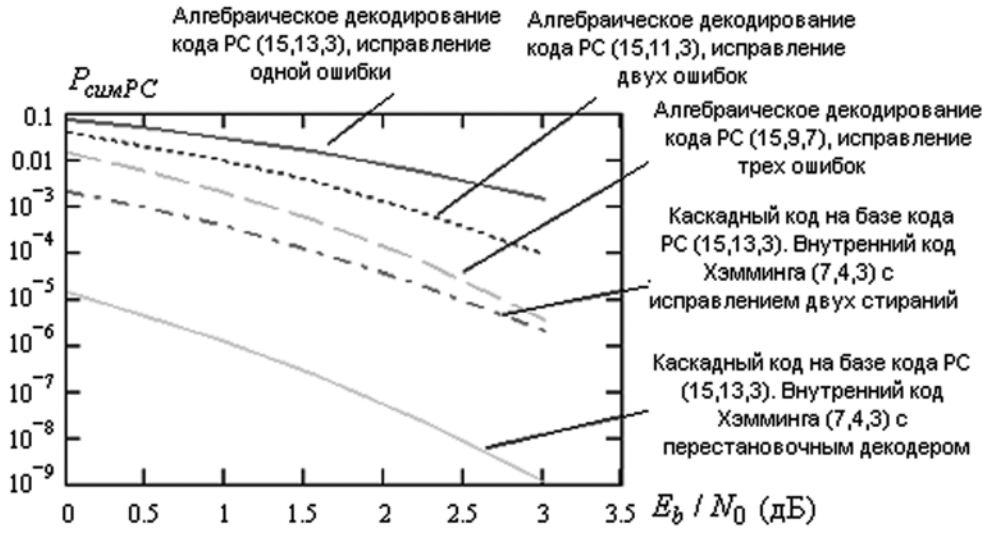

Рис. 4. Сравнительные оценки искажения недвоичных символов в зависимости от метода обработки данных и отношения сигнал-шум

зволяет повысить эффективность схем каскадного кодирования и получить в системе обмена данными дополнительный энергетический выигрыш.

СПИСОК ЛИТЕРАТУРЫ

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

2. Dilip V.S. High-speed Architectures for Reed-Solomon decoders // IEEE Trans. VLSI systems, 2001. vol. 34. pp. 388–396.

3. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки / под ред. Р.Л. Добрушина и С.Н. Самойленко. – М. : Мир, 1976. – 594 с.

4. Финк Л.М. Теория передачи дискретных сообщений. – М. : Сов. радио, 1970. – 728 с.

5. Гладких А.А. Обобщенный метод декодирования по списку на базе кластеризации пространства кодовых векторов // Радиотехника. – 2015. – № 6. – С. 37–41.

6. Гладких А.А., Климов Р.В., Чилихин Н.Ю. Методы эффективного декодирования избыточных кодов и их современные приложения. – Ульяновск : УлГТУ, 2016. – 258 с.

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

8. Комашинский В.И., Комашинский Д.В Когнитивная метафора в развитии телекоммуникационных и индустриальных сетевых инфраструктур, или первые шаги к постинформационной эпохе // Технологии и средства связи. – 2015. – № 1. – С 62–66.

9. Скляр Б. Цифровая связь. Теоретические основы и практическое применение : изд. 2-е, испр.; пер. с англ. – М. : Издательский дом «Вильямс», 2003. – 1104 с.

REFERENCES

1. 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.

2. Dilip V.S. High-speed Architectures for Reed-Solomon Decoders. *IEEE Trans. VLSI Systems,* 2001, vol. 34, pp. 388–396.

3. Peterson U., Weldon E. *Kody, ispravliaiushchie oshibki. Pod red. R.L. Dobrushina i S.N. Samoilenko* [Error-Correcting Codes. Edited by R.L. Dobrushin and S.N. Samoilenko]. Moscow, Mir Publ., 1976. 594 p.

4. Fink L.M. *Teoriia peredachi diskretnykh soobshchenii* [The Theory of Discrete Message Transmission]. Moscow, Sov. Radio Publ., 1970. 728 p.

5. Gladkikh A.A. Obobshchennyi metod dekodirovaniia po spisku na baze klasterizatsii prostranstva kodovykh vektorov [Generalized Method of List Decoding on the Basis of Code Vectors Space Clustering]. *Radiotekhnika* [Radioengineering], 2015, no. 6, pp. 37–41.

6. Gladkikh A.A., Klimov R.V., Chilikhin N.Iu. *Metody effektivnogo dekodirovaniia izbytochnykh kodov i ikh sovremennye prilozheniia* [Methods of the Effective Decoding of Redundant Codes and the its Modern Applications]. Ulyanovsk, UlSTU Publ., 2016. 258 p.

7. 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.

8. Komashinskii V.I., Komashinskii D.V Kognitivnaia metafora v razvitii telekommunikatsionnykh i industrialnykh setevykh infrastruktur, ili pervye shagi k postinformatsionnoi epokhe [The Cognitive Metaphor in the Evolution of Telecommunication and Industrial Network Infrastructures or the First Steps Towards the Post-Information Society]. *Tekhnologii i sredstva sviazi* [Communication Technologies and Equipment Magazine], 2015, no. 1, pp. 62–66.

9. Sklar B. Tsifrovaia sviaz. *Teoreticheskie osnovy i prakticheskoe primenenie. Izd. 2-e, ispr.; per. s angl.* [Digital Communications. Fundamentals and Applications. Second Edition. Translated from Engl.]. Moscow, Williams Publ., 2003. 1104 p.