Оригинальная статья / Original article

https://doi.org/10.21869/2223-1536-2024-14-4-8-27

УДК 621.391

Декодирование помехоустойчивого блокового кода в условиях априорной неопределенности

А. А. Двилянский[1] ✉, А. В. Юрлов[2]

[1] МИРЭА – Российский технологический университет
пр-т Вернадского, д. 78, г. Москва 119454, Российская Федерация

[2] Академия Федеральной службы охраны Российской Федерации
ул. Приборостроительная, д. 35, г. Орёл 302015, Российская Федерация

✉ e-mail: dvilyanskiy@mirea.ru

Резюме

Цель исследования *– повышение эффективности декодирования помехоустойчивых блоковых кодов в условиях априорной неопределенности относительно применяемых параметров.*

Методы. *В современных системах отмечается применение помехоустойчивых блоковых кодов с большой длиной кодового слова, что позволяет в процессе кодирования достаточно далеко разнести друг от друга разрешенные кодовые комбинации и получить при итеративном декодировании возможность их правильного определения при низких значениях отношения сигнал / шум в канале связи. Использование длинных помехоустойчивых кодов требует сокращения сложности алгоритмов коррекции ошибок, оцениваемой числом операций различного типа на одну итерацию декодирования. Число операций различного типа будет зависеть от параметров кода и проверочной матрицы, а также применяемого алгоритма декодирования. Практическая реализация декодера имеет ряд ограничений, и его проектирование представляет сложную задачу, особенно в условиях априорной неопределенности относительно применяемых параметров кода. Для решения этой задачи предлагается использовать метод определения применяемой проверочной матрицы ЛБК на основе анализа принимаемой цифровой последовательности.*

Результаты. *В ходе исследования был проведен сравнительный анализ известных методов определения параметров помехоустойчивого блокового кода и предложена модификация метода Гаусса для решения системы линейных алгебраических уравнений при нахождении проверочной матрицы ЛБК.*

Заключение. *Предложенный метод позволяет избежать выполнения строгой последовательности действий согласно известному методу Гаусса, а также сократить временную сложность за счет распараллеливания вычислений и значительно увеличить эффективность практической реализации алгоритма нахождения проверочной матрицы ЛБК.*

Ключевые слова: *помехоустойчивое кодирование; определение проверочной матрицы; метод Гаусса; метод четырех русских.*

Конфликт интересов: *Автор декларирует отсутствие явных и потенциальных конфликтов интересов, связанных с публикацией настоящей статьи.*

Для цитирования: Двилянский А. А., Юрлов А. В. Декодирование помехоустойчивого блокового кода в условиях априорной неопределенности // Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. 2024. Т. 14, № 4. С. 8–27. https://doi.org/10.21869/ 2223-1536-2024-14-4-8-27

Поступила в редакцию 06.10.2024 *Подписана в печать 04.11.2024* *Опубликована 27.12.2024*

Decoding forward error correction code in a priori uncertainty

Alexei A. Dvilyanskiy[1] ✉, Alexander V. Yurlov[2]

[1]MIREA – Russian Technological University
78 Vernadsky Ave., Moscow 119454, Russian Federation

[2]Academy of the Federal Security Service of the Russian Federation
35 Priborostroitelnaya Str., Orel 302015, Russian Federation

✉ e-mail: dvilyanskiy@mirea.ru

Abstract

The purpose of research *is to increase the efficiency of decoding noise–resistant block codes in conditions of a priori uncertainty about the parameters used.*

Methods. *In modern systems, the use of noise-resistant block codes with a large codeword length is noted, which allows the permitted code combinations to be sufficiently far apart from each other during encoding and to obtain, during iterative decoding, the possibility of their correct determination at low values of the signal-to-noise ratio in the communication channel. The use of long noise-tolerant codes requires a reduction in the complexity of error correction algorithms, which is estimated by the number of operations of various types per decoding iteration. The number of operations of various types will depend on the parameters of the code and the verification matrix, as well as the decoding algorithm used. The practical implementation of the decoder has a number of limitations, and its design is a difficult task, especially in conditions of a priori uncertainty about the applied code parameters. To solve this problem, it is proposed to use the method of determining the applied LBC verification matrix based on the analysis of the received digital sequence.*

Results. *In the course of the study, a comparative analysis of known methods for determining the parameters of an interference-resistant block code was carried out and a modification of the Gauss method was proposed to solve a system of linear algebraic equations when finding the LBC verification matrix.*

Conclusion. *The proposed method avoids performing a strict sequence of actions according to the well-known Gauss method, as well as reducing time complexity by paralleling calculations and significantly increasing the efficiency of practical implementation of the algorithm for finding the LBC verification matrix.*

Keywords: *noise-resistant coding; determination of the verification matrix; Gauss method; four-Russian method.*

Conflict of interest: *The Authors declares the absence of obvious and potential conflicts of interest related to the publication of this article.*

For citation: Dvilyanskiy A.A., Yurlov A.V. Decoding forward error correction code in a priori uncertainty. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Serija: Upravlenie, vychislitel'naja tekhnika, informatika. Meditsinskoe priborostroenie = Proceedings of the Southwest State University. Series: Control, Computer Engineering, Information Science. Medical Instruments Engineering*. 2024;14(4):8–27. (In Russ.) https://doi.org/10.21869/2223-1536-2024-14-4-8-27

Received 06.10.2024 *Accepted 04.11.2024* *Published 27.12.2024*

Введение

В настоящее время применение процедур помехоустойчивого кодирования является неотъемлемой частью любой современной системы связи. Линейные блоковые коды – это класс помехоустойчивых кодов, операция кодирования для которых состоит в разбиении последовательности информационных символов на блоки фиксированной длины k, каждому из которых сопоставляется строго определенное кодовое слово длины n, при этом формируемые кодовые слова не зависят друг от друга.

Совокупность кодовых слов образуют линейное пространство. Для описания линейного блокового кода (ЛБК) достаточно задать базис пространства, а кодирование сводится к умножению на порождающую матрицу. Порождающей матрицей G линейного (n, k)-кода называется матрица размера $k \times n$, строками которой являются его базисные векторы. Чтобы декодировать ЛБК, необходимо определить проверочную матрицу H, строки которой ортогональны к строкам матрицы G. Можно сказать, что элементами систематической формы проверочной матрицы являются коэффициенты проверочных уравнений, на основе которых вычисляются проверочные символы [1].

Особый интерес в настоящее время среди известных линейных блоковых кодов представляют низкоплотностные коды (НПК), задаваемые с помощью проверочной матрицы H, характеризуемой относительно малым числом единиц в строках и столбцах. Их широкое применение на практике обусловлено возможностью почти вплотную приблизиться к пропускной способности канала при относительно небольшой сложности реализации [1].

Благодаря своей корректирующей способности низкоплотностные коды (*LDPC – Low-Density Parity-Check Codes*) стали частью современных телекоммуникационных стандартов, таких как *DVB-S2* (*S2X*) [2], *WiMAX*, *Wi-Fi* [3], а также других стандартов современных радиосистем, прежде всего спутниковых и радиорелейных [4], для которых характерно применение методов адаптации к сложным условиям приема сигналов. Адаптация основывается на подстройке параметров модуляции и помехоустойчивого кодирования в зависимости от качества радиолинии [5], что в случае применения НПК требует разработки методов определения их параметров.

Широкое применение НПК на практике объясняется тем, что они обладают наилучшей помехоустойчивостью по сравнению с используемыми ранее помехоустойчивыми блоковыми кодами (Рида-Соломона, БЧХ, турбокодами и др.), а сложность декодирования НПК составляет O(N). Высокая эффективность декодирования НПК обеспечивается оптимизацией структуры проверочной матрицы H [6].

В отличие от других линейных блоковых кодов, имеющих строгий алгоритм синтеза кодов с заданными параметрами, для НПК существует множество способов построения [7].

Кодирование осуществляется приведением матрицы H к виду $H=[P^T|I_{n-k}]$, из которого можно получить порождающую матрицу в систематической форме $G=[I_k|P]$. Сложность кодирования с использованием матрицы G заключается в том, что подматрица P в общем случае не является разреженной.

Как правило, проверочные матрицы НПК, описанные в телекоммуникационных стандартах [7], определены для некоторого диапазона длин кодовых слов и скоростей кодирования. При введении дополнительных значений кодовых длин и скоростей при использовании методов адаптации в системах связи возникает задача определения проверочной матрицы НПК, необходимой при реализации процедуры декодирования [8].

Материалы и методы

Для декодирования ЛБК требуется знание параметров кода: длины кодового слова, скорости кода, проверочной матрицы кода [9; 10], а также решение задачи синхронизации.

На практике решение задачи синхронизации на уровне кодовых слов ЛБК реализуется путем вставки на передающей стороне уникальной синхропоследовательности – синхрослова (*synchroword*, *SW*) после каждого кодового слова (или нескольких кодовых слов) [11]. Таким образом, появление синхрослова *SW* длиной l бит в цифровом потоке на входе канального декодера происходит периодически с периодом кратным длине n бит кодового слова.

Тогда цифровой двоичный поток, полученный на длине u периодов, можно представить в виде совокупности матриц X и Y:

$$X=\begin{bmatrix} x_{1,1} & x_{1,2} & \cdots & x_{1,l} \\ x_{2,1} & x_{2,2} & \cdots & x_{2,l} \\ \vdots & \vdots & \ddots & \vdots \\ x_{u,1} & x_{u,2} & \cdots & x_{u,l} \end{bmatrix},\quad Y=\begin{bmatrix} y_1 & y_2 & \cdots & y_n \\ y_{n+1} & y_{n+2} & \cdots & y_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ y_{(u-1)n+1} & y_{(u-1)n+2} & \cdots & y_{un} \end{bmatrix}, \qquad (1)$$

где X – матрица, элементы которой представляют собой последовательность повторяющихся детерминированных синхрослов *SW* длиной l бит; Y – матрица, элементы которой представляют собой, соответственно, последовательности случайных кодовых слов длиной n бит.

Данная структура цифрового потока будет наблюдаться только на периоде $l+n$ бит. Так как период цифрового потока изначально неизвестен, то благодаря вставке синхрослов *SW* он может быть определен путем вычисления веса столбцов матрицы X при инкрементировании значения периода. Если веса всех столбцов матрицы X по расстоянию Хемминга равны «0» или «u» (возможны незначительные отклонения в результате возникновения ошибок в канале связи), то принимается решение о нахождении синхрослова *SW* длиной l бит и значения длины кодового слова n бит. Определение значения длины k информационной части кодового слова определяется после дескремблирования цифрового потока.

Данное решение предполагает использование «жестких» решений с выхода демодулятора. При низких значениях отношения сигнал / шум (ОСШ) использование «мягких» решений позволит получить гораздо лучшие результаты [9].

Сигналы одинаковой энергии будут отображаться геометрическими векторами одинаковой длины, концы которых – сигнальные точки размещаются на поверхности гиперсферы радиуса $\sqrt{E}$, где E – энергия сигнала (для упрощения $E = 1$). Евклидово расстояние, характеризующее различие между сигналами, выражается через разность энергий сигналов:

$$d_{ij}^2 = \int_0^T \left[s_i(t) - s_j(t) \right]^2 dt = E_{ij}. \quad (2)$$

Пусть в канал передается последовательность ЛБК $(d \in \{0, 1\})$ с использованием двоичной фазовой манипуляции (*BPSK – binary phase-shift keying*), в результате чего на выходе демодулятора наблюдается сигнал s, принимающий два возможных значения: $s_1 s_1 = 1 + i$ и $s_2 = -1 + i$. Для случая квадратурной фазовой манипуляции (*QPSK – quadrature phase shift keying*) будут наблюдаться сигналы: $s_1 = 1 + i$, $s_2 = -1 + i$, $s_3 = -1 - i$ и $s_4 = 1 - i$.

Под воздействием аддитивного белого гауссова шума (АБГШ) w на входе приемника сигнал $\boldsymbol{s}$ искажается и принимается как $r = s + w$.

Величина r имеет нормальное распределение и для случая *BPSK* определяется функцией плотности вероятности:

$$P(r/d = 0) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{\frac{-(r+1)^2}{2\sigma^2}}, \quad (3)$$

$$P(r/d = 1) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{\frac{-(r-1)^2}{2\sigma^2}}. \quad (4)$$

Полагаем, что длина кодового слова n определена корректно. Так как в канале присутствуют помехи, то кодовые слова ЛБК принимаются с ошибками. Обозначим принимаемые кодовые слова следующим образом: $r_1, r_2, ..., r_u$, где u – количество принятых кодовых слов; $r_i = (r_i^1, r_i^2, ..., r_i^n)$, и $r_i^j \in \mathbf{R}$. «Мягкое» решение или, иначе говоря, логарифмическое отношение правдоподобия (ЛОП) обозначим следующим образом:

$$x_i^j = \ln \frac{P(d_i^j = 0 / r_i^j)}{P(d_i^j = 1 / r_i^j)} = -\frac{2r_i^j}{\sigma^2}.$$

Тогда $x_i = (x_i^1, x_i^2, ..., x_i^n)$ – вектор, содержащий мягкие решения для каждого символа кодового слова длиной n бит.

Под воздействием помех в канале связи на выходе демодулятора наблюдается искаженный сигнал $s : r = s + w$. Значения сигнала r, которые лежат вблизи вещественной оси или мнимой оси, являются малодостоверными и, как правило, приводят к ошибкам.

Число вычислительных операций может быть уменьшено за счет

предварительных жестких решений, формируемых из амплитуд логарифмов отношений правдоподобия (надежностей) для символов, полученных из канала [12]. Множество позиций с очень высокой надежностью может быть выявлено с помощью сравнения значений ЛОП на выходе канала с некоторым порогом. Если надежность символа из канала превышает заданный порог, то соответствующая ему кодовая вершина фиксируется как жесткое решение. Вместо вычислений позиция символа помечается, указывая на высокую надежность значения этого символа. Вследствие этого выполняется меньший объем вычислений, так как для символа с высокой надежностью нет необходимости вычисления значений ЛОП.

Определив порог принятия решения, при анализе столбцов матрицы X наименее достоверные значения должны быть отброшены из дальнейшего рассмотрения. Для случая *QPSK* порог принятия решения *gi* определяется следующим образом:

$$g_i = \max_{i=1,2,3,4} \left\{ \left| r_j - s_i \right| \right\}. \qquad (5)$$

Алгоритмы декодирования, использующие «мягкие» решения демодулятора, обладают большей вычислительной сложностью, но их применение дает дополнительный выигрыш при декодировании аналогичных кодов (кодов с одной и той же избыточностью) по сравнению алгоритмами, которые используют «жесткие» решения [13].

При использовании «мягких» решений значения с выхода демодулятора квантуются с конечной точностью (т. е. представляются конечным числом бит). Другая причина более высокой сложности использования «мягких» решений связана с необходимостью вычисления апостериорных вероятностей для кодовых символов. Однако усложнение реализации окупается потенциальным повышением эффективности системы кодирования – получением энергетического выигрыша от кодирования [14].

Низкоплотностные коды являются одним из наиболее востребованных решений в современных системах связи. Это объясняется тем, что декодирование НПК [6; 15] с большой длиной кодового слова за счет применения итеративных алгоритмов декодирования *SISO* (*Soft Input – Soft Output*) позволяет получить показатели, близкие к границе Шеннона [16]. Идея *SISO* заключается в улучшении исправляющей способности по максимуму апостериорной информации от итерации к итерации, от «мягкого» выхода одного декодера к «мягкому» входу, следующего в применяемой каскадной конструкции [14].

Низкоплотностный код – это линейный блоковый код (ЛБК) с разреженной проверочной матрицей H и большой длиной кодового слова n. Проверочная матрица H для кода с параметрами (n, k) имеет размерность и имеет низкую плотность единиц. Свойства матрицы H можно сформулировать следующим образом:

– проверочная матрица представляет собой систему $m \geq n-k$ проверочных уравнений;

– любая пара строк или столбцов имеет максимум λ общих ненулевых позиций.

Очень низкая плотность единиц ($i<<m$ и $j<<n$) позволяет значительно снизить вычислительные затраты на реализацию алгоритма декодирования при большой длине кодового слова.

В процессе декодирования используется изначально априорные вероятности входных символов, формируя дополнительную информацию в виде значений логарифмического отношения правдоподобия, которые являются мерой надёжности жёсткого решения декодера.

Известно, что получение больших уровней помехоустойчивости всегда связано с применением довольно длинных кодов, т. к. это позволяет достаточно далеко разнести друг от друга разрешенные кодовые комбинации, что и будет обеспечивать их правильное определение декодером. При этом использование весьма длинных кодов требует максимального упрощения алгоритмов коррекции ошибок с целью их достаточно быстрой и эффективной обработки [16; 17].

Для оценки сложности алгоритма декодирования используется методика, учитывающая требуемое число операций различного типа (сложения, умножения, сравнения и т. д.) на одну итерацию декодирования [16]. Число операций различного типа будет зависеть от параметров кода и проверочной матрицы, а также применяемого алгоритма декодирования.

Для декодирования НПК широкое применение получил алгоритм итеративного распространения доверия (*IBP – Iterative Believe Propagation*) и его модификации. Практическая реализация НПК-декодеров имеет ряд ограничений, и их проектирование представляет сложную задачу [6].

Рассмотрим линейный (n, k) код C, который образует k-мерное подпространство в $F^n = GF(q)$, где $q = 0,1,...,p$ – простое число. Матрица, строки которой являются базисными векторами пространства, образующего код C, является порождающей матрицей кода G. Множество строк матрицы G порождает линейный (n, k) код C, а любое кодовое слово образуется линейной комбинацией строк из G. В большинстве случаев порождающая матрица данного кода не является единственной. В [14; 18] представлено выражение для расчета количества возможных матриц для линейного кода $C(n, k)$:

$$M_{\text{возм. матриц}} = \prod_{i=0}^{k-1}\left(2^k - 2^i\right). \quad (6)$$

На рисунке 1 представлена зависимость количества возможных матриц кода от длины и скорости.

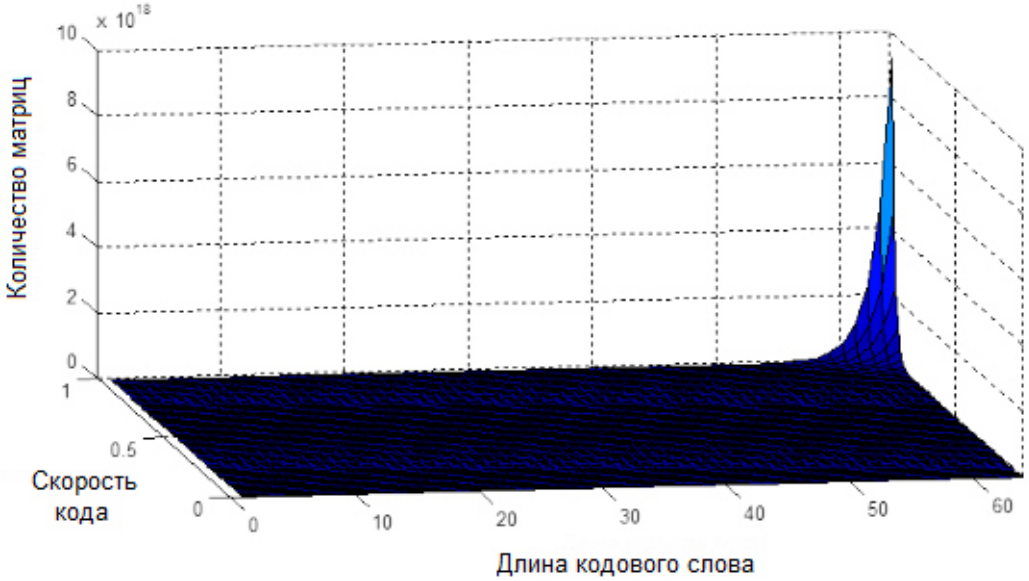

Рис. 1. Зависимость количества возможных матриц кода от длины и скорости кода

Fig. 1. Matrix-candidates dependency on code length and code rate

Среди известных [19] на сегодняшний день подходов к решению задачи определения параметров помехоустойчивого кода и нахождения системы проверочных уравнений (проверочной матрицы) можно выделить следующие: метод полного перебора, статистический метод, алгебраический метод [20].

Статистический метод – метод определения параметров кода, представляющий собой частный случай метода полного перебора и основанный на анализе результатов рассчитанных синдромов кодовых слов, составленных из фрагмента исследуемого цифрового потока, для всего известного набора применяемых ЛБК [19; 21]. Данный метод позволяет идентифицировать известный код, тогда как метод полного перебора может быть применен для определения параметров неизвестного кода [22].

Суть данного метода заключается в последовательном пробном декодировании контрольной выборки, состоящей из принятых кодовых слов (количество кодовых слов, необходимое для идентификации ЛБК, определяется вероятностью ошибки в канале), каждым из предполагаемых декодеров и анализе полученного множества решений декодера или анализе полученных при декодировании синдромов. Если в полученной последовательности с выхода декодера количество ненулевых синдромов больше заданного порога, то принимается решение о том, что выбранные параметры кода являются неправильными. Значение порога определяется путем применения критерия принятия решения, исходными данными для которого выступают допустимые вероятности ложной тревоги и пропуска цели. Метод предполагает, что известны проверочные матрицы, поэтому при анализе неизвестных видов кодирования данный метод не применим [20].

Метод полного перебора – метод определения проверочной матрицы кода путем перебора всех возможных проверочных уравнений и последующим нахождением синдромов рассматриваемых кодовых слов. Этот метод является общим случаем статистического метода определения параметров кода. Вычислительная сложность метода определяется количеством вариантов перебора в процессе определения проверочных уравнений ЛБК [18].

Количество вариантов значительно снижается в случае наличия априорных знаний о параметрах проверочной матрицы (вес строк, тип матрицы, размер циркулянта, расположение циркулянтов в проверочной части). В худшем случае, когда известны только параметры n и k кода, количество возможных проверочных уравнений определяется выражением

$$L_{\text{возм. уравнений}} = 2^k (n-k). \qquad (7)$$

Количество возможных проверочных уравнений получено с учетом того, что они составят базис ортогонального дополнения из $(n-k)$ уравнений в канонической форме с единичной матрицей $I_{(n-k)\times(n-k)}$ в правой части и подматрицей $P_{(n-k)\times k}$, элементы которой могут располагаться произвольно.

Число вариантов перебора снижается при наличии каких-либо априорных знаний о формируемых проверочных уравнениях. Например, известно, что циркулянты в проверочной части кодовых слов образуют двудиагональную структуру, а размер циркулянта равен l. Это означает, что проверочная матрица данного кода имеет квазициркулянтную структуру [23], все проверочные уравнения имеют постоянный вес r, проверочное уравнение содержит ровно $(r-2)$ единиц в левой части проверочной матрицы и ровно две единицы в правой. Так как циркулянтные строки получены циклическим сдвигом некоторой «опорной» строки, задача сводится к поиску только «опорных» строк. Тогда количество возможных проверочных уравнений, определенное формулой (1), примет вид

$$L_{\text{возм. уравнений}} = \frac{\binom{r-2}{k}\cdot\binom{n-k}{2}}{l} = \frac{1}{l}\cdot\frac{(r-2)!}{(r-2-k)!k!}\cdot\frac{(n-k)!}{2!(n-k-2)!} \qquad (8)$$

В таблице 1 представлены расчетные значения количества вариантов проверочных уравнений и времени поиска ортогонального базиса для случая применения НПК со скоростью кодирования 1/2 с различными длинами кодовых слов. Проверка принадлежности уравнения ортогональному базису осуществляется умножением на n кодовых слов и получением синдрома с низким весом по Хэммингу. Приведенные результаты получены с учетом возможности параллельного исполнения восьми потоков на ЭВМ с процессором *Intel*(*R*) *Core*(*TM*) *i*5-8250*U*.

Таблица 1. Время нахождения проверочных матриц НПК

Table 1. Time to find parity matrices of LDPC

Длина кодового слова, бит	Количество вариантов перебора	Время перебора, лет
768	6,5·1013	866,54
1152	7,5·1014	9930,8875
1536	4,3·1015	55968,58
1920	1,6·1016	213893,7225

Анализ значений, представленных в таблице 1, показывает, что априорные знания о весе проверочных уравнений не позволяют найти проверочную матрицу НПК при использовании метода полного перебора за практически приемлемое время даже для относительно коротких длин кодовых слов.

Алгебраический метод – метод определения параметров кода, основанный на свойствах линейного векторного пространства кода, заключающийся в преобразовании матрицы, составленной из кодовых слов, к каноническому виду [11]. Данный подход является наиболее общим из всех известных.

Пусть линейный блоковый код $C(n,k)$ однозначно задается порождающей матрицей $G_{k,n}$, а также получаемой из нее проверочной матрицей $H_{(n-k),n}$. Так как набор строк матрицы $G_{k,n}$ является базисом *k*-мерного подпространства *C*, образованного кодовыми словами линейного блокового кода (ЛБК) в *n*-мерном линейном пространстве, то, определив этот базис, можно идентифицировать ЛБК. В рамках задачи декодирования НПК в условиях априорной параметрической неопределенности, больший интерес представляет ортогональное дополнение подпространства *C*, базис которого используется в качестве проверочной матрицы $H_{(n-k),n}$.

Основным требованием к алгебраическому методу является то, что вероятность битовой ошибки в канале связи (*BER – Bit Error Rate*) должна быть достаточно низкой: 10^{-15}–10^{-12}, что выполняется, например, для случая передачи информации с использованием НПК по волоконно-оптическим линиям связи [24]. При составлении матрицы, состоящей из $f \geq n$ кодовых слов, не должно быть кодовых слов с ошибками, так как иначе будет вычислен базис расширенного подпространства $\hat{C}$, образованного объединением векторов кодовых слов искомого ЛБК и векторов ошибок. Метод предполагает наличие априорной информации относительно длины кодового слова *n*, в противном случае требуется организация дополнительной процедуры перебора значений указанных параметров кода [25].

Результаты и их обсуждение

Алгоритм определения параметров кода состоит из следующих шагов:

Построение матрицы размерностью $f \times n$ $(f \geq n)$ вида

$$M_{f,n} = \begin{bmatrix} p_{11} & p_{12} & \cdots & p_{1k} & \cdots & p_{1n} \\ p_{21} & p_{22} & \cdots & p_{2k} & \cdots & p_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ p_{k1} & p_{k2} & \cdots & p_{ij} & \cdots & p_{kn} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ p_{f1} & p_{f2} & \cdots & p_{fk} & \cdots & p_{fn} \end{bmatrix}, \quad (9)$$

где p_{ij} – символы кодового слова, принимающие значение «0» или «1»; i – номер строки матрицы; j – номер столбца матрицы.

Диагонализация матрицы $M_{f,n}$:

$$M_d = \begin{bmatrix} 1 & 0 & \cdots & 0 & p_{1(k+1)} & \cdots & p_{1n} \\ 0 & 1 & \cdots & 0 & p_{2(k+1)} & \cdots & p_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & p_{k(k+1)} & \cdots & p_{kn} \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{bmatrix}. \quad (10)$$

Получение порождающей матрицы линейного блокового кода (ЛБК):

$$G_{k,n} = \begin{bmatrix} 1 & 0 & \cdots & 0 & p_{1(k+1)} & \cdots & p_{1n} \\ 0 & 1 & \cdots & 0 & p_{2(k+1)} & \cdots & p_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & p_{k(k+1)} & \cdots & p_{kn} \end{bmatrix}. \quad (11)$$

Для проверки правильности полученной порождающей матрицы $G_{k,n}$ необходимо использовать полученную на ее основе проверочную матрицу $H_{(n-k),n}$. Для этого реализуется синдромный метод: если в результате перемножения d кодовых слов получены нулевые синдромы, то $C(n,k)$ найден верно.

При декодировании неизвестного низкоплотностного кода в условиях низких значений ОСШ данный метод не применим, так как кодовые слова с ошибками не принадлежат подпространству C, тем самым получение порождающей матрицы затруднено [17; 26].

Повышение скорости обработки при реализации данного алгоритма возможно путем параллельного выполнения задач обработки за счет использования разнородных блоков обработки (*CPU*, *GPU, FPGA*). Одними из основных принципов построения современных и перспективных вычислительных систем являются возможности реализации [23]:

– параллельного выполнения задач обработки за счет использования разнородных блоков цифровой обработки сигналов (ЦОС);

– балансировки нагрузки;

– вертикальной масштабируемости (наращивание вычислительной мощности за счет внедрения дополнительных блоков обработки);

– горизонтальной масштабируемости (наращивание вычислительной

мощности за счет объединения ресурсов нескольких комплексов);

– программного обеспечения в модульном виде (каждая программа представляет собой модуль, выполняющий частную задачу обработки; коммутация и тиражирование модулей позволяют гибко настраивать процесс обработки входных данных).

Таким образом, для исключения информационных пропусков при реализации режима отложенной обработки необходимо рассмотреть возможности параллельного выполнения наиболее затратных этапов алгоритма с использованием имеющейся аппаратной базы [20].

Значительные вычислительные ресурсы для реализации алгоритма занимает процесс диагонализации матрицы с целью получения ортогонального базиса для рассматриваемого кода. Классический способ [21; 27] получения базиса линейно-векторного пространства с помощью элементарных операций над строками – метод Гаусса – имеет сложность $O(n^3)$. «Метод четырех русских» (*M4RI – Method of the Four Russians Inversion*), который был предложен в [28], уменьшает количество операций сложения строк в ($\log n$) раз за счет процедуры, основанной на перемножении матриц (методе Конрада) [16; 29].

Пусть матрица A имеет размерность $m \times n$, а ее подматрица B размерностью $k \times n$ имеет полный ранг. В результате преобразований, определяемых методом Гаусса, первые k строк матрицы A представят собой диагональную матрицу в каноническом виде. Всего существует 2^k комбинаций первых k строк, которые поместим в таблицу T. В таблице T индекс строки соответствует номерам строк подматрицы $k \times n$, участвующих в получении данной (например, если индекс таблицы $T - 5_{dec}$, т. е. 101_{bin}, то для получения данной строки необходимо было сложить первую и третью строки преобразованной подматрицы B). Тогда для «зануления» первых k столбцов матрицы A необходимо воспользоваться таблицей T – рассмотреть первые k бит строки и в соответствии с полученным значением использовать нужную строку таблицы T. Таким образом, вместо k сложений (в худшем случае) данная операция требует всего одно сложение за счет предварительно составленной таблицы [22]. Алгоритм, реализующий данный метод, представлен ниже (рис. 2).

Индекс строки в таблице T представляет собой число, имеющее разрядность k. Для того чтобы «занулить» k бит строки матрицы A, начиная с позиции ($I \bmod k$), где $0 \le i < m$, необходимо сложить по модулю 2 данную строку со строкой, взятой из таблицы T, полученной на итерации ($i \bmod k$), по индексу, определяемому значением k бит (рис. 3).

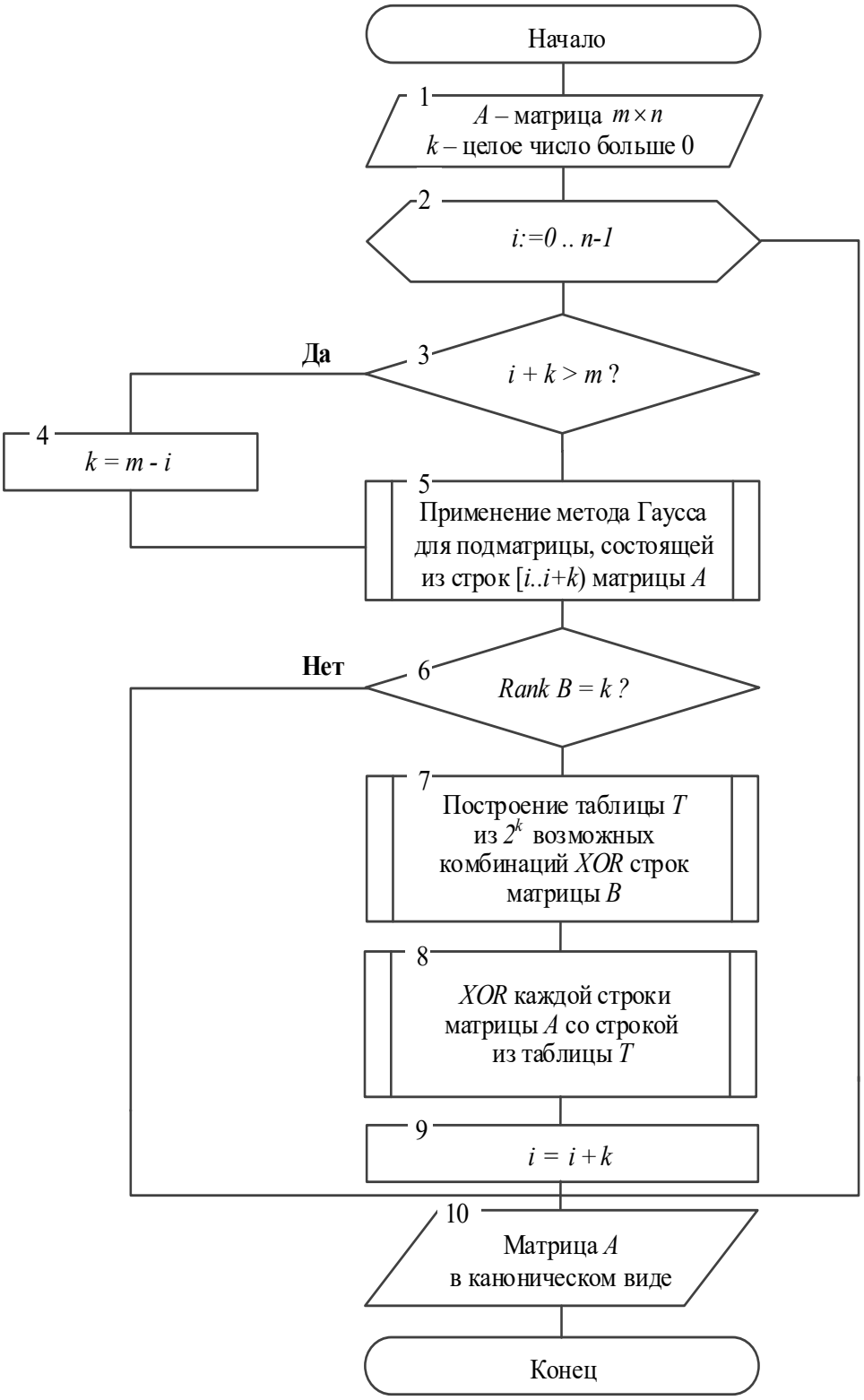

Рис. 2. Алгоритм диагонализации матрицы с применением метода «четырех русских»

Fig. 2. Matrix diagonalization algorithm based on the Method of Four Russians

Вычисление T строк эффективно выполняются с использованием кода Грея. Тогда для ее составления понадобиться $(2^k - 1)$ сложений строк, так как

индексы соседних строк, определяющие, какие строки подматрицы B (подматрица B – результат применения метода Гаусса в «окне» размерностью k строк матрицы A) необходимо сложить между собой по модулю два, отличаются только в одном бите. Прямой подход потребует $\left(\frac{k}{2}\cdot 2^k - 1\right)$ сложений.

$$A = \begin{bmatrix} 100 & 10111 & ... \\ 010 & 11110 & ... \\ 001 & 00111 & ... \\ ... & ... & ... \\ 000 & 11010 & ... \\ 110 & 01011 & ... \\ 010 & 01001 & ... \\ ... & ... & ... \\ 110 & 11101 & ... \end{bmatrix}, \quad T = \begin{bmatrix} 000 & 00000 & ... \\ 001 & 00111 & ... \\ 010 & 11110 & ... \\ 011 & 11001 & ... \\ 100 & 10111 & ... \\ 101 & 10000 & ... \\ 110 & 01001 & ... \\ 111 & 01110 & ... \end{bmatrix}.$$

Рис. 3. Преобразование исходной матрицы с использованием предварительно составленной таблицы

Fig. 3. Transformation initial matrix using look-up table

Процесс сложения строк матрицы A со строками таблицы T можно производить параллельно. Следовательно, предварительные вычисления позволят избежать строгую последовательность действий согласно методу Гаусса, требующую для вычисления текущей строки знать все предыдущие строки в необходимой преобразованной форме [27].

В ходе проведенного исследования установлено, что увеличение значения параметра k приводит к росту размерности таблицы T, обеспечивая повышение эффективности ее использования, – за одну операцию сложения происходит обработка большего количества столбцов [17]. Однако пропорционально увеличивается сложность её построения. В качестве компромисса целесообразно применять метод Гаусса над подматрицей B, состоящей из $(N \times k)$ строк, где N – некоторое целое число (рис. 4), что позволит использовать N таблиц T_1, T_2,…, $T_{N\text{-}1}$, построенных за $(N \times 2^k)$ сложений строк (вместо $2^{N\times k}$ сложений строк при подсчете значений одной таблицы T и кратном N увеличении параметра k), но их применение потребует на $(N-1)$ сложений строк больше, чем применение единственной таблицы соответствующей размерности. Построение таблиц также выполняется параллельно в N потоков [28].

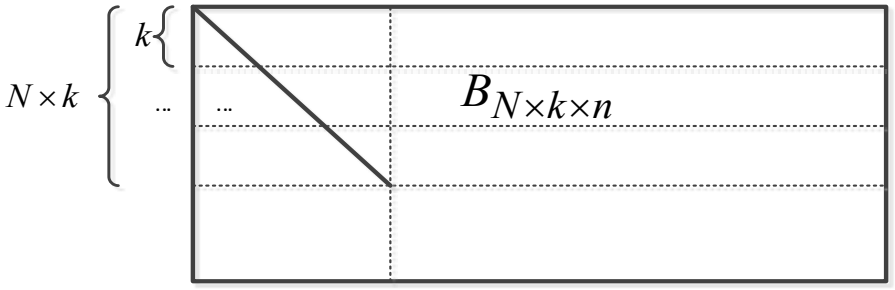

Рис. 4. Разбиение матрицы на подматрицы, позволяющее повысить эффективность параллельной обработки

Fig. 4. Matrix partition for efficient parallel implementation

Выводы

Из рассмотренных методов определения параметров кода наиболее предпочтительным на практике является алгебраический метод, поскольку обладает достаточно невысокой (по сравнению с методом полного перебора) вычислительной сложностью. Однако недостатком алгебраического метода выступает требование к низким значениям вероятности ошибки в канале.

В таком случае необходимо использовать толерантные к ошибкам методы перебора при формировании проверочных уравнений НПК. Найденные уравнения даже в условиях отсутствия полной информации о параметрах кода возможно использовать при помехоустойчивом декодировании для снижения вероятности ошибки в принимаемом сигнале.

Список литературы

1. Performance Analysis of LDPC Decoding Techniques / Abdel Halim A. Zikry, Ashraf Y. Hassan, Wageeda I. Shaban, Sahar F. Abdel-Momen // International Journal of Recent Technology and Engineering (IJRTE). 2021. Vol. 9, is. 5. P. 17–26.

2. Коломенский К. Ю., Демидова А. Ю., Казаринов А. С. От DVB-S к DVB-S2X: прогресс в стандартизации систем цифрового спутникового вещания // Известия высших учебных заведений России. Радиоэлектроника. 2024 Т. 27, № 2. С. 68–78. https://doi.org/10.32603/1993-8985-2024-27-2-68-78

3. Shuang S., Biju I. Analysis of WiFi and WiMAX and Wireless Network Coexistence // International Journal of Computer Networks and Communications (IJCNC). 2014. Vol. 6, N 6. P. 63–78. https://doi.org/10.5121/ijcnc.2014.6605

4. Stepanets I., Odoevskii S. Model of microwave link channel with adaptive modulation under the fading conditions // E3S Web of Conferences. 2022. N 351(23). P. 01064. https://doi.org/10.1051/e3sconf/202235101064

5. CCSDS protocols over DVBS2 – Summary of DVB-S2 summary of definition, implementation, and performance. Washington: Geen Book, 2023. 56 p.

6. Zhou F., Niu L., Tian B. Performance analysis of LDPC decoding algorithm // Journal of Physics. Conference Series. 2020. N 1453(1). P. 012026. https://doi.org/10.1088/1742-6596/1453/1/012026

7. Lulu A., Hudrouss A. A. LDPC Construction using Randomly Permutated Copies of Parity Check Matrix // An-Najah University Journal for Research. 2018. N 32(1). P. 1544. https://doi.org/10.35552/anujr.a.32.1.1544

8. Guan Wu., Liping L. Check-Belief Propagation Decoding of LDPC Codes // IEEE Transactions on Communications. 2023. Vol. 71, is. 12. P. 6849–6858. https://doi.org/10.1109/TCOMM. 2023.3308155

9. Boundaries of signal-to-noise ratio for adaptive code modulations / K. Pinyoanuntapong, M. Goswami, A. B. Habib, H. M. Kwon, K. Pham // IEEE Military Communications Conference. Baltimore, MD, USA, 2016. P. 132–137.

10. Karimian Y., Ziapour S., Ahmadian-Attari M. Parity Check Matrix Recognition from Noisy Codewords. URL: https://arxiv.org/abs/1205.4641 (дата обращения: 11.09.2024).

11. Digital Video Broadcasting (DVB); Second generation framing structure, channel coding and modulation systems for Broadcasting, Interactive Services, News Gathering and other broadband satellite applications; Part 1: DVB-S2. Sophia Antipolis Cedex, 2014. 80 p.

12. Low-complexity LDPC decoding algorithms for ultra-high-order modulated signals / H. Zhu, M. Fu, C. Hou, G. Hu // Optics Express. 2023. Vol. 31, is. 25. P. 41645–41657. https://doi.org/10.1364/OE.507292

13. Le Gal B., Jego C., Pignoly V. High-performance hard-input LDPC decoding on multi-core devices for optical space links // Journal of Systems Architecture. 2023. N 137(9). P. 102832. https://doi.org/10.1016/j.sysarc.2023.102832

14. Zolotarev V. V. Coding Theory as a Simple Optimal Decoding near Shannon's Bound. Optimization Theory of error-correcting coding is a new &quantum mechanics of information theory. M.: Hot Line Telecom, 2018. 334 p.

15. Belief-Propagation Decoding of LDPC Codes with Variable Node-Centric Dynamic Schedules / H. Pin, J. Wang , I. Weng, T. Lee Tofar, C.-Y. Chang // IEEE Transactions on Communications. 2021. Vol. 69, is. 8. P. 5014–5027. https://doi.org/10.1109/TCOMM. 2021.3078776

16. Dietzfelbinger M., Walzer S. Constant-time retrieval with O(log m) extra bits // 36th International Symposium on Theoretical Aspects of Computer Science (STACS 2019). Dagstuhl, Germany: Dagstuhl Publishing, 2019. P. 24:1–24:16. https://doi.org/10.4230/LIPIcs. STACS.2019.24

17. An FPGA-Based LDPC Decoder with Ultra-Long Codes for Continuous-Variable Quantum Key Distribution / S. Yang, J-Q. Liu, Z-Q. Lu, Z-L. Bai, X. Wang, Y. Li // IEEE Access. 2021. Vol. 9. P. 47687–47697. https://doi.org/10.1109/ACCESS.2021.3065776

18. Fast Blind Recovery of Linear Block Codes over Noisy Channels / P. Wang, Y. Liang, G. Lipo, W. Peng Cheng. URL: https://arxiv.org/abs/2305.04190 (дата обращения: 16.09.2024).

19. Multi-Gbps LDPC Decoder on GPU Devices / J. Dai, H. Yin, N. Xu, P. Yang // Electronics. 2022. N 11(21). P. 3447. https://doi.org/10.3390/electronics11213447

20. Maier B. Cockburn. Optimization of Low-Density Parity Check decoder performance for OpenCL designs synthesized to FPGAs // Journal of Parallel and Distributed Computing. 2017. N 107. P. 1. https://doi.org/10.1016/j.jpdc.2017.04.001

21. Gaussian Elimination Method-A Study of Applications / M. Saeed, S. Nisar, S. Razzaq, R. Masood // Global Journal of Science Frontier Research: Mathematics and Decision Sciences. 2021. Vol. 13, is. 4. https://doi.org/10.1109/LES.2021.3052714

22. Albrecht M. R., Pernet C. Efficient Decomposition of Dense Matrices over GF(2). URL: https://arxiv.org/abs/1006.1744/ (дата обращения: 17.09.2010).

23. Sudrastawa P. A., Parwata A. Conceptual and Practical Review of Gaussian Elimination and Gauss-Jordan Reduction // Jurnal Ilmu Komputer Indonesia. 2022. Vol. 7, N 2. P. 19–25.

24. Awatif M., Elsiddieg A. Implementation of Gaussian-Elimination // International Journal of Innovative Technology and Exploring Engineering (IJITEE). 2016. Vol. 5, is. 11. P. 7–20.

25. Karimi-Lenji A., Houshmand M., Zarmehi F. A high-performance belief propagation decoding algorithm for codes with short cycle // International Journal of Communication Systems. 2017. N 30(13). https://doi.org/10.1002/dac.3275

26. Sharma F., Rajesh Pillai N. Blind recognition of parameters of linear block codes from intercepted bit stream // 2016 International Conference on Computing, Communication and Automation (ICCCA). Greater Noida, India: IEEE, 2016. https://doi.org/10.1109/CCAA.2016.7813910

27. Carrier K., Tillich J.-P. Identifying an unknown code by partial Gaussian elimination // Designs, Codes and Cryptography. 2019. Vol. 87(1). P. 685–713. https://doi.org/10.1007/s10623-018-00593-7

28. Donovan D. M., Rao A., Uskuplu E., Yazici E. QC-LDPC Codes from Difference Matrices and Difference Covering Arrays // IEEE Access. 2023. Vol. 11. P. 52141–52157. https://doi.org/10.1109/ACCESS.2023.3279327

29. Yu Hanqi Peng P.-D., Gong K.-X., Chen Z.-L. LDPC code reconstruction based on algorithm of finding low weight code-words // IEEE Access. 2017. Vol. 38, is. 6. P. 108–117. https://doi.org/10.11959/ j.issn.1000-436x.2017116

References

1. Abdel Halim A. Zikry, Ashraf Y. Hassan, Wageeda I. Shaban, Sahar F. Abdel-Momen Performance Analysis of LDPC Decoding Techniques. *International Journal of Recent Technology and Engineering* (*IJRTE*). 2021;9:17–26.

2. Kolomensky K.Y., Demidova A.Y., Kazarinov A.S. From DVB-S to DVB-S2X: Progress in Standardization of Digital Satellite Broadcasting Systems. *Journal of the Russian Universities. Radioelectronics*. 2024;27(2):68–78. https://doi.org/10.32603/1993-8985-2024-27-2-68-78

3. Shuang S., Biju I. Analysis of WiFi and WiMAX and Wireless Network Coexistence. *International Journal of Computer Networks and Communications* (*IJCNC*). 2014;6(6):63–78. https://doi.org/10.5121/ijcnc.2014.6605

4. Stepanets I., Odoevskii S. Model of microwave link channel with adaptive modulation under the fading conditions. *E3S Web of Conferences*. 2022;351:01064. https://doi.org/10.1051/e3sconf/202235101064

5. CCSDS protocols over DVBS2 – Summary of DVB-S2 summary of definition, implementation, and performance. Washington: Geen Book; 2023. 56 p.

6. Zhou F., Niu L., Tian B. Performance analysis of LDPC decoding algorithm. *Journal of Physics. Conference Series*. 2020;(1453):012026. https://doi.org/10.1088/1742-6596/1453/1/012026

7. Lulu A., Hudrouss A. A. LDPC Construction using Randomly Permutated Copies of Parity Check Matrix. *An-Najah University Journal for Research*. 2018;(32):1544. https://doi.org/10.35552/anujr.a.32.1.1544

8. Guan Wu., Liping L. Check-Belief Propagation Decoding of LDPC Codes. *IEEE Transactions on Communications*. 2023;71:6849–6858. https://doi.org/10.1109/TCOMM.2023.3308155

9. Pinyoanuntapong K., Goswami M., Habib A. B., Kwon H. M., Pham K. Boundaries of signal-to-noise ratio for adaptive code modulations. In: *IEEE Military Communications Conference*. Baltimore, MD, USA; 2016. P. 132–137.

10. Karimian Y., Ziapour S., Ahmadian-Attari M. Parity Check Matrix Recognition from Noisy Codewords. Available at: https://arxiv.org/abs/1205.4641 (accessed 11.09.2024).

11. Digital Video Broadcasting (DVB); Second generation framing structure, channel coding and modulation systems for Broadcasting, Interactive Services, News Gathering and other broadband satellite applications; Part 1: DVB-S2. Sophia Antipolis Cedex, 2014. 80 p.

12. Zhu H., Fu M., Hou C., Hu G. Low-complexity LDPC decoding algorithms for ultra-high-order modulated signals. *Optics Express*. 2023;31:41645–41657. https://doi.org/10.1364/OE.507292

13. Le Gal B., Jego C., Pignoly V. High-performance hard-input LDPC decoding on multi-core devices for optical space links. *Journal of Systems Architecture*. 2023;137:102832. https://doi.org/10.1016/j.sysarc.2023.102832

14. Zolotarev V.V. Coding Theory as a Simple Optimal Decoding near Shannon's Bound. Optimization Theory of error-correcting coding is a new &quantum mechanics of information theory. Moscow: Hot Line Telecom; 2018. 334 p.

15. Pin H., Wang J., Weng I., Lee Tofar T., Chang C.-Y. Belief-Propagation Decoding of LDPC Codes with Variable Node-Centric Dynamic Schedules. *IEEE Transactions on Communications*. 2021;69:5014–5027. https://doi.org/10.1109/TCOMM. 2021.3078776

16. Dietzfelbinger M., Walzer S. Constant-time retrieval with O(log m) extra bits. In: *36th International Symposium on Theoretical Aspects of Computer Science* (*STACS 2019*). Dagstuhl, Germany: Dagstuhl Publishing; 2019. P. 24:1–24:16. https://doi.org/10.4230/LIPIcs. STACS.2019.24

17. An FPGA-Based LDPC Decoder with Ultra-Long Codes for Continuous-Variable Quantum Key Distribution / S. Yang, J-Q. Liu, Z-Q. Lu, Z-L. Bai, X. Wang, Y. Li. *IEEE Access*. 2021;9:47687–47697. https://doi.org/10.1109/ACCESS.2021.3065776

18. Wang P., Liang Y., Lipo G., Peng Cheng W. Fast Blind Recovery of Linear Block Codes over Noisy Channels. Available at: https://arxiv.org/abs/2305.04190 (accessed 16.09.2024).

19. Dai J., Yin H., Xu N., Yang P. Multi-Gbps LDPC Decoder on GPU Devices. *Electronics*. 2022;11(21):3447. https://doi.org/10.3390/electronics11213447

20. Maier B. Cockburn. Optimization of Low-Density Parity Check decoder performance for OpenCL designs synthesized to FPGAs. *Journal of Parallel and Distributed Computing*. 2017;(107):1. https://doi.org/10.1016/j.jpdc.2017.04.001

21. Saeed M., Nisar S., Razzaq S., Masood R. Gaussian Elimination Method-A Study of Applications. *Global Journal of Science Frontier Research: Mathematics and Decision Sciences*. 2021;13. https://doi.org/10.1109/LES.2021.3052714

22. Albrecht M.R., Pernet C. Efficient Decomposition of Dense Matrices over GF(2). URL: https://arxiv.org/abs/1006.1744/ (accessed 17.09.2010).

23. Sudrastawa P.A., Parwata A. Conceptual and Practical Review of Gaussian Elimination and Gauss-Jordan Reduction. *Jurnal Ilmu Komputer Indonesia*. 2022;7(2):19–25.

24. Awatif M., Elsiddieg A. Implementation of Gaussian-Elimination. *International Journal of Innovative Technology and Exploring Engineering* (*IJITEE*). 2016;5(11):7–20.

25. Karimi-Lenji A., Houshmand M., Zarmehi F. A high-performance belief propagation decoding algorithm for codes with short cycle. *International Journal of Communication Systems*. 2017;30. https://doi.org/10.1002/dac.3275

26. Sharma F., Rajesh Pillai N. Blind recognition of parameters of linear block codes from intercepted bit stream. In: *2016 International Conference on Computing, Communication and*

Automation (*ICCCA*). Greater Noida, India: IEEE; 2016. https://doi.org/10.1109/CCAA.2016.7813910

27. Carrier K., Tillich J.-P. Identifying an unknown code by partial Gaussian elimination. *Designs, Codes and Cryptography*. 2019;87:685–713. https://doi.org/10.1007/ s10623-018-00593-7

28. Donovan D.M., Rao A., Uskuplu E., Yazici E. QC-LDPC Codes from Difference Matrices and Difference Covering Arrays. *IEEE Access*. 2023;11:52141–52157. https://doi.org/10.1109/ACCESS.2023.3279327

29. Yu Hanqi Peng P.-D., Gong K.-X., Chen Z.-L. LDPC code reconstruction based on algorithm of finding low weight code-words. *IEEE Access*. 2017;38:108–117. https://doi.org/10.11959/ j.issn.1000-436x.2017116

Информация об авторах / Information about the Authors

Алексей Аркадьевич Двилянский, кандидат технических наук, доцент, МИРЭА – Российский технологический университет, г. Москва, Российская Федерация, e-mail: dvilyanskiy@mirea.ru, ORCID: 0000-0002-0648-3651

Dvilyanskiy A. Alexei, Candidate of Sciences (Engineering), Associate Professor, MIREA – Russian Technological University, Moscow, Russian Federation, e-mail: dvilyanskiy@mirea.ru, ORCID: 0000-0002-0648-3651

Александр Владимирович Юрлов, кандидат технических наук, сотрудник, Академия Федеральной службы охраны Российской Федерации, г. Орёл, Российская Федерация, e-mail: yurlov@bk.ru

Alexander V. Yurlov, Candidate of Sciences (Engineering), Employee, Academy of the Federal Security Service of the Russian Federation, Orel, Russian Federation, e-mail: yurlov@bk.ru