Оптимизация, системный анализ и исследование операций

© 2026 г. Ф.И. ИВАНОВ, д-р физ.-мат. наук (fivanov@hse.ru),
А.В. КУВШИНОВ (akuvshinov@hse.ru)
(Национальный исследовательский университет
«Высшая школа экономики», Москва)

ЭФФЕКТИВНОЕ ДЕКОДИРОВАНИЕ БЧХ-КОДОВ ПО МАКСИМУМУ АПОСТЕРИОРНОЙ ВЕРОЯТНОСТИ[1]

В данной статье предложен алгоритм упрощенного декодирования по максимуму апостериорной вероятности расширенных кодов БЧХ. В основе алгоритма лежат декодирование по максимуму апостериорной вероятности с использованием дуального кода, предложенное Хартманом и Рудольфом, и быстрое декодирование по МАВ кодов Хэмминга, предложенное Лицыным и Ашихминым. Рассмотренные модификации позволяют существенно снизить сложность декодирования по максимуму апостериорной вероятности при сохранении его корректирующей способности.

Ключевые слова: БЧХ, декодирование по максимуму апостериорной вероятности, декодер с «мягким» выходом.

DOI: 10.7868/S2413977726120062

1. Введение

В теории помехоустойчивого кодирования особое место занимают алгоритмы оптимального декодирования коротких кодов. Примерами таких алгоритмов являются декодирование по максимуму правдоподобия (МП) и декодирование по максимуму апостериорной вероятности (МАВ). МП-декодер является первоначальным подходом к подобному роду алгоритмов, он формирует глобально оптимальное решение с точки зрения вероятности кодового слова при условии заданной принятой последовательности, в то время как выходом МАВ-декодера являются посимвольно-оптимальные решения, т.е. алгоритм производит оценку апостериорных вероятностей для каждого символа по отдельности и принимает решение по наибольшей вероятности.

Востребованность МАВ-алгоритмов обусловлена появлением итеративных алгоритмов декодирования каскадных кодов. В частности, от декодера требуется наличие «мягкого» выхода при «мягком» входе. В этом случае выход декодера каждого компонента должен предоставлять не только «жесткое»

[1] Работа выполнена при финансовой поддержке Российского научного фонда (грант № 24-19-00299).

решение обо всем кодовом слове или каждом символе в отдельности, но и давать «мягкий» выход, т.е. надежность каждого такого «жесткого» решения (апостериорная вероятность, посчитанная МАВ). Подобный «мягкий» выход учитывается на следующей итерации путем обновления информации, полученной из канала. Подобные схемы, позволяющие не только снизить сложность, но и улучшить корректирующую способность, получили активное распространение в 1990-х годах после появления турбо-кодов [1], где в качестве декодера сверточных кодов-компонентов используется алгоритм Бала–Кука–Джелинека–Равива (БКДР) [2]. Алгоритм БКДР использует представление кода в виде решетки, что позволяет снизить сложность декодирования по сравнению с МАВ-декодером с прямым вычислением всех апостериорных вероятностей.

Коды Боуза–Чоудхури–Хоквингема (БЧХ) являются представителями класса циклических линейных кодов и широко применяются во многих приложениях [3]. Коды БЧХ обладают простой конструкцией и алгоритмом декодирования при условии их рассмотрения в канале с «жесткими» решениями. Наиболее известными декодерами БЧХ-кодов являются алгоритмы Питерсона–Горенстейна–Цирлера [4] и Берлекампа–Месси [5]. Однако, являясь декодерами с «жесткими» решениями, данные алгоритмы не могут быть применены в итеративных схемах декодирования. Проблеме «мягкого» декодирования БЧХ-кодов посвящено несколько работ. Авторы [6, 7] рассматривают МП-декодер БЧХ с «мягким» выходом, однако предложенный алгоритм может быть применен для ограниченного числа длин кодов БЧХ. Более универсальные с точки зрения параметров кода мягкие МП-декодеры для БЧХ-кодов рассмотрены в [8, 9]. По сути данные алгоритмы являются декодерами Витерби с решетками Вульфа [10].

Одним из возможных способов получения «мягкого» выхода декодера БЧХ является списочный подход к классическим декодерам с «жестким» списком в совокупности с алгоритмом Пиндиаха [11]. В основе такого метода – декодер Чейза, формирующий список из «жестких» кандидатов со всеми возможными комбинациями двоичных символов на самых ненадежных позициях принятого из канала вектора [12]. Каждый кандидат из списка декодируется далее классическим декодером с «жесткими» решениями. Далее эти решения вместе с принятой из канала последовательностью используются для формирования «мягкого» выхода. Списочному декодированию БЧХ-кодов посвящено недавнее исследование [13].

В [14] был рассмотрен подход, уменьшающий сложность декодирования расширенных кодов Хэмминга по МАВ по сравнению с декодированием по алгоритму БКРД. Используя быстрое преобразование Адамара, авторы упрощают вычисления по формулам декодирования по МАВ, выведенным в [15], применительно к расширенным кодам Хэмминга и указывают на возможность применения данного подхода к любым линейным кодам.

В данной работе рассмотрено применение предложенного в [14] подхода к расширенным кодам БЧХ. В статье разработаны методы, которые позволяют существенно уменьшить сложность подхода, предложенного в [14]. Основная идея упрощений основана на том, что структура кода Хэмминга, являющегося основой для декодирования БЧХ-кодов в [14], позволяет произвести расчет некоторых параметров заранее, а не в процессе непосредственного декодирования. Таким образом, разработанные процедуры, примененные к алгоритму декодирования, уменьшают его сложность при сохранении корректирующей способности декодера по максимуму апостериорной вероятности.

2. Декодирование по максимуму апостериорной вероятности

Вначале рассмотрим общий принцип МАВ-декодирования.

Ограничимся рассмотрением линейных (n, k) блоковых кодов C над полем $GF(2)$: $C = \{\mathbf{c}_m, m = 1, \ldots, 2^k\} \subseteq \{0,1\}^n$, слова кодовой книги которых передаются через канал с двоичным входом и без памяти. Таким образом, на вход в канал поступают векторы $\mathbf{c} = (c_1, c_2, \ldots, c_n)$, $\mathbf{c} \in C$ длины n.

На приемном конце наблюдаются последовательности $\mathbf{r} = (r_1, \ldots, r_n)$, $r_i \in \mathcal{Y}$ ($\mathcal{Y}$ – выходной алфавит канала), искаженные шумом.

МАВ-декодер является побитовым декодером и для каждой j-й позиции кодового слова оценивает условную (апостериорную) вероятность отправки каждого из символов $\{0,1\}$ в кодовом слове $\mathbf{c}$ и вычисляет значение j-го символа следующим образом:

$$\hat{c_j} = \arg \max_{k \in \{0,1\}} P(c_j = k|\mathbf{r}).$$

Для случая передачи в дискретном канале апостериорная вероятность может быть выражена через функции правдоподобия с использованием формулы Байеса. Обозначим $C_j(k)$ множество кодовых слов, в которых символ на j-й позиции равен k, тогда при условии равномерного распределения на множестве кодовых слов, имеем:

$$P(c_j = k|\mathbf{r}) = \sum_{\mathbf{s} \in C_j(k)} P(\mathbf{c} = \mathbf{s}|\mathbf{r}) =$$

$$= \sum_{\mathbf{s} \in C_j(k)} \frac{P(\mathbf{r}|\mathbf{s})}{P(\mathbf{r})} P(\mathbf{s}) = \frac{1}{2^k P(\mathbf{r})} \sum_{\mathbf{s} \in C_j(k)} \prod_{i=1}^{n} P(r_i|s_i). \quad (1)$$

Таким образом, для каждой позиции передаваемой последовательности МАВ-декодер вычисляет (1) для символов из $\{0,1\}$ и принимает «жесткое» решение по наибольшей апостериорной вероятности. Надежностью данного решения (т.е. «мягким» выходом декодера) и служит вероятность $P(c_j = k|\mathbf{r})$.

3. Упрощенное декодирование по максимуму апостериорной вероятности кодов Хэмминга

Для кодов скорости $R = \frac{k}{n} > \frac{1}{2}$ можно добиться упрощения вычисления (1) за счет декодирования в дуальном коде, что было предложено в [15]. Код, дуальный коду C, будем обозначать $C^{\perp}$, а кодовые слова такого кода – $\mathbf{c}'$. В [15] была доказана теорема, из которой следует соотношение для разности между апостериорными вероятностями, по сути являющаяся искомым «мягким» выходом декодера, которое для двоичных кодов выглядит следующим образом:

$$P(c_j = 0|\mathbf{r}) - P(c_j = 1|\mathbf{r}) = \frac{P(c_j = 0|\mathbf{r}) - P(c_j = 1|\mathbf{r})}{P(c_j = 0|\mathbf{r}) + P(c_j = 1|\mathbf{r})} = \frac{\sum\limits_{i=1}^{2^{n-k}} \prod\limits_{l=1}^{n} \rho_l^{c'_{il} \oplus \delta_{jl}}}{\sum\limits_{i=1}^{2^{n-k}} \prod\limits_{l=1}^{n} \rho_l^{c'_{il}}}, \tag{2}$$

где c'_{ij} – j-й элемент i-го кодового слова дуального кода $C^{\perp}$, δ_{ij} – символ Кронекера и ρ_j может быть выражено через отношение правдоподобия $\frac{P(r_j|c_j=1)}{P(r_j|c_j=0)}$ следующим образом:

$$\rho_j = \frac{1 - \frac{P(r_j|c_j=1)}{P(r_j|c_j=0)}}{1 + \frac{P(r_j|c_j=1)}{P(r_j|c_j=0)}} = P(c_j = 0|r_j) - P(c_j = 1|r_j). \tag{3}$$

В [14] был предложен метод для быстрого подсчета (2) для расширенного $(2^m, 2^m - m - 1)$ кода Хэмминга. В основе алгоритма лежит быстрое преобразование Адамара.

Опишем кратко основные этапы декодирования по данному алгоритму. Введем обозначения $\mathcal{I}_j(0)$, $\mathcal{I}_j(1)$ для набора позиций, в которых символ j-го кодового слова равен 0 или 1 соответственно, причем $\mathcal{I}_j(0) \cap \mathcal{I}_j(1) = \emptyset$ и $\mathcal{I}_j(0) \cup \mathcal{I}_j(1) = \{1, \ldots, 2^m\}$. После подсчета элементов вектора $\boldsymbol{\rho}$ процесс декодирования сводится к двум шагам.

- Посчитаем элементы векторов $\boldsymbol{\omega}^{(0)}$ и $\boldsymbol{\omega}^{(1)}$ следующим образом:

$$\omega_j^{(0)} = \sum_{\mathbf{c}'_{\mathbf{t}} \in C_j^{\perp}(0)} \prod_{l \in \mathcal{I}_t(1)} \rho_l + \sum_{\mathbf{c}'_{\mathbf{t}} \in C_j^{\perp}(1)} \prod_{l \in \mathcal{I}_t(0)} \rho_l, \ j = 1, \ldots, 2^m, \tag{4}$$

$$\omega_j^{(1)} = \sum_{\mathbf{c}'_{\mathbf{t}} \in C_j^{\perp}(0)} \prod_{l \in \mathcal{I}_t(0)} \rho_l + \sum_{\mathbf{c}'_{\mathbf{t}} \in C_j^{\perp}(1)} \prod_{l \in \mathcal{I}_t(1)} \rho_l, \ j = 1, \ldots, 2^m. \tag{5}$$

- В результате искомый «мягкий» выход декодера для каждой j-й позиции кодового слова может быть выражен через соответствующие элементы найденных векторов $\boldsymbol{\omega}$ и $\boldsymbol{\rho}$:

$$z_j = \frac{\omega_j^{(0)} \rho_j + \frac{\omega_j^{(1)}}{\rho_j}}{\omega_j^{(0)} + \omega_j^{(1)}} = P(c_j = 0|\mathbf{r}) - P(c_j = 1|\mathbf{r}). \tag{6}$$

Данный результат декодирования (как и в выражении (2)) без труда можно перевести в отношение апостериорных вероятностей, логарифм от которого как правило используется в схемах декодирования, например, для последующего обновления информации из канала в итеративных декодерах каскадных кодов.

4. Упрощенное декодирование по максимуму апостериорной вероятности кодов БЧХ

В данном разделе описан алгоритм декодирования по МАВ, адаптированный для декодирования расширенных БЧХ-кодов. Идея распространения алгоритма декодирования, описанного в предыдущем разделе, на любые линейные высокоскоростные коды была предложена в [14]. Основная идея заключается в декодировании предложенным алгоритмом $(2^m, 2^m - tm - 1)$-кода БЧХ с использованием проверочной матрицы кода Хэмминга с тем же числом строк, что и в соответствующей матрице расширенного БЧХ-кода. Тогда для указанного кода БЧХ рассмотрим расширенный $(2^{tm+1}, 2^{tm+1} - tm - 2)$-код Хэмминга (с параметрами $n - k = tm + 2,\ n = 2^{tm+1}$). Идея декодирования заключается в том, что проверочная матрица кода Хэмминга длины $2^{n-k} - 1$ обязательно содержит все столбцы проверочной матрицы любого кода избыточности $(n - k)$. Следует отметить, что рассмотренный далее алгоритм применим для декодирования кодов с минимальным расстоянием $d \geqslant 3$, поскольку проверочные матрицы таких кодов не содержат одинаковые столбцы.

В таком случае процесс декодирования расширенного $(2^m, 2^m - tm - 1)$-кода БЧХ можно свести к алгоритму, описанному в разделе 3. Данный алгоритм будет использовать дуальный код расширенного $(2^{tm+1}, 2^{tm+1} - tm - 2)$-кода Хэмминга, который, как известно, является $(2^{tm+1}, tm + 1)$-кодом Рида–Маллера первого порядка $RM(1, tm+1)$. На его вход будет поступать вектор $\boldsymbol{\rho}$ длины 2^{tm+1}. Если j-й столбец проверочной матрицы кода Хэмминга не являются одновременно столбцом проверочной матрицы соответствующего кода БЧХ, то элемент ρ_j вектора $\boldsymbol{\rho}$ приравниваются единице в начале процедуры декодирования. В противном случае, ρ_j вычисляется по формуле (3).

Ключевым недостатком такого подхода является большой размер кодовой книги кода, дуального коду Хэмминга, даже для небольших длин соответствующего кода БЧХ. В процессе декодирования одной принятой последовательности необходимо использовать каждое слово такой кодовой книги при основных подсчетах, что существенно замедляет алгоритм. Далее будут предложены модификации, упрощающие процесс вычислений.

Для удобства длину принятой последовательности $\boldsymbol{r}$, соответствующей длине $(2^m, 2^m - tm - 1)$ БЧХ-кода будем по-прежнему обозначать $n = 2^m$. Длину расширенного кода Хэмминга, имеющего то же число проверок, что и БЧХ-код, обозначим $N = 2^{tm+1}$ (число столбцов в кодовой книге, используемой в процессе декодирования). Будем далее для удобства рассматривать вектор $\boldsymbol{\omega}^{(0)}$ как матрицу с элементами $\omega_{ij}^{(0)},\ i = 1, \ldots, n,\ j = 1, \ldots, N$. Для

получения $\omega_j^{(0)}$ необходимо просуммировать $\omega_{ij}^{(0)}$ по i, т.е.

$$\omega_j^{(0)} = \sum_{i=1}^{n} \omega_{ij}^{(0)},$$

$$\omega_j^{(1)} = \sum_{i=1}^{n} \omega_{ij}^{(1)},$$

где элементы $\omega_{ij}^{(0)}$ и $\omega_{ij}^{(1)}$ определяются далее в выражениях (8) и (9).

Структура кода $RM(1, tm+1)$ позволяет ввести в процесс декодирования следующие модификации:

а) Введем множество $\mathcal{R} : \mathcal{R} = \{i : \rho_i \neq 1\}$, которое совпадает с индексами столбцов проверочной матрицы расширенного $(2^m, 2^m - tm - 1)$-кода БЧХ в проверочной матрице $(2^{tm+1} - 1, 2^{tm+1} - tm - 2)$-кода Хэмминга. В виду того, что $\forall j = \{1, \ldots, 2^{tm+1}\}$, $\forall \mathbf{c} \in RM(1, tm+1) \cap \mathcal{I}_j(0)$ $\exists\, \tilde{\mathbf{c}} \in RM(1, tm+1) \cap \mathcal{I}_j(1)$: $\tilde{\mathbf{c}} = \mathbf{1} + \mathbf{c}$, где $\mathbf{1}$ – вектор из единиц, то при подсчете (4) и (5) будем рассматривать только половину кодовых слов (например, $C_j^{\perp}(0)$) в процессе декодирования, поэтому

$$\omega_j^{(0)} = 2 \sum_{\mathbf{c}'_{\mathbf{t}} \in C_j^{\perp}(0)} \prod_{l \in \mathcal{I}_t(1)} \rho_l,$$

$$\omega_j^{(1)} = 2L \sum_{\mathbf{c}'_{\mathbf{t}} \in C_j^{\perp}(0)} \frac{1}{\prod\limits_{l \in \mathcal{I}_t(1)} \rho_l},$$

где константа L вычисляется как произведение элементов вектора $\boldsymbol{\rho}$ на позициях $\mathcal{R}$:

$$L = \prod_{l \in \mathcal{R}} \rho_l.$$

б) В связи с тем, что на результат декодирования влияют только строки кодовой книги $C_j^{\perp}(0)$ с индексами из $\mathcal{R}$, достаточно ограничиться рассмотрением n таких кодовых слов.

в) Для результата декодирования достаточно посчитать только элементы z_j, $j \in \mathcal{R}$ в формуле (6), которые зависят от $\rho_j, j \in \mathcal{R}$.

г) Для каждой пары столбцов кодовой книги $C_j^{\perp}(0)$ может быть посчитано единственное значение ρ_{ij}. Остальные элементы $\boldsymbol{\rho}$ равны либо данному значению, либо $\frac{L}{\rho_{ij}}$ (в произведении берутся только индексы $j \in \mathcal{R}$).

д) Используя кодовую книгу, можно заранее посчитать индексы элементов вектора $\boldsymbol{\rho}$, произведение от которых будет использовано в процессе декодирования для поиска соответствующих элементов векторов $\boldsymbol{\omega}^{(\mathbf{0})}$, а также индексы соответствующих произведений для каждого элемента.

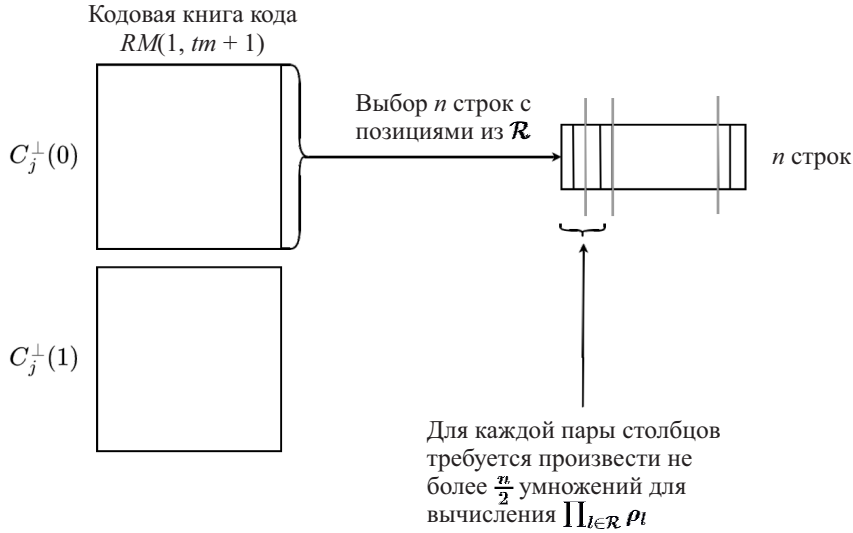


Рис. 1. Упрощение обработки кодовой книги.

Основные модификации MAB-декодера с точки зрения обработки только части кодовой книги соответствующего расширенного кода Хэмминга продемонстрированы в виде схемы на рис. 1.

В соответствии с перечисленными пунктами (а)–(д) декодирование расширенных кодов БЧХ можно представить в виде двух этапов – предварительного подсчета, не зависящего от принятой последовательности, и непосредственного декодирования принятого вектора $\mathbf{r}$:

- Предварительный расчет. Множества пересечений позиций $\mathcal{R}$ и позиций, в которых $C_j^{\perp}(0)$ равно единице, посчитаем заранее для каждого j. Запишем такие пересечения в виде матрицы $\mathcal{A}$, которая будет иметь размеры N на N, и каждый элемент α которой является множеством указанных пересечений: $\alpha_{ji} = \mathcal{R} \cap \{i : c'_i = 1, \mathbf{c}' \in C_j^{\perp}(0)\}$. Ввиду пункта (а) пересечения $\mathcal{R} \cap \{i : c'_i = 1, \mathbf{c}' \in C_j^{\perp}(1)\}$ хранить не нужно. Полученную матрицу можем сократить до размеров n на N, сохранив только строки с индексами из $\mathcal{R}$.

  Матрица $\mathcal{A}$ имеет N уникальных элементов. В процессе декодирования будут использоваться только произведения элементов вектора $\boldsymbol{\rho}$ на позициях, хранящихся в данных элементах. Запишем такие элементы в виде массива $\mathcal{J}$.

  Тогда матрицу соответствия между элементами $\mathcal{J}$ и $\mathcal{A}$ получим как позиции элементов $\mathcal{J}$ в матрице $\mathcal{A}$ и обозначим $\mathcal{P}$. Элементы данной матрицы будут указывать на одно из N произведений, использующихся в (4) и (5).

  Для каждой пары соседних столбцов в матрице $\mathcal{A}$ справедливо следующее:

$$\alpha_{j,2i-1} \cup \alpha_{j,2i} = \mathcal{R}, \quad i = 1, \ldots, \frac{n}{2}.$$

- Непосредственный процесс декодирования принятой последовательности $\mathbf{r}$:

  1) Посчитаем N произведений элементов вектора $\boldsymbol{\rho}$ на соответствующих позициях: Для каждого j-го символа в декодируемой последовательности вычислим произведение элементов вектора $\boldsymbol{\rho}$ на позициях $\mathcal{J}(j)$

  $$P_j = \prod_{s \in \mathcal{J}(j)} \rho_s. \tag{7}$$

  2) Используем полученный результат для вычисления элементов $\omega_{ij}^{(0)}$ и $\omega_{ij}^{(1)}$

  $$\omega_{ij}^{(0)} = P(\mathcal{P}(i,j)), \tag{8}$$

  $$\omega_{ij}^{(1)} = \frac{L}{\omega_{ij}^{(0)}}. \tag{9}$$

  3) Формула для подсчета «мягкого» результата z_j для каждого j-го символа совпадает с (6).

При вычислениях в (7) можно использовать функцию sum-product (по аналогии с функциями декодирования кодов с малой плотностью проверок на четность:

$$P_j = \prod_{s \in \mathcal{J}(j)} \beta_s \exp\left(\sum_{s \in \mathcal{J}(j)} \varphi_s \right),$$

где $\beta_i = \operatorname{sign}(\rho_i)$, $\varphi_i = ln(|\rho_i|)$.

5. Результаты моделирования и сравнение по сложности

В данном разделе представлено сравнение производительности (с точки зрения корректирующей способности и вычислительной сложности) расширенных БЧХ-кодов с использованием классического MAB-декодера, описанного в [15] и модифицированного для БЧХ-кодов декодером из [14].

На рис. 2 показано сравнение MAB-декодеров для $(32, 21)$ расширенного БЧХ-кода с точки зрения вероятности ошибки на бит (bit error rate, BER). Кроме того, на рисунке показаны вероятности ошибки на бит для декодера Чейза с параметром $p = 6$ (число перебираемых ненадежных позиций) и для декодера sum-product, примененного к проверочной матрице расширенного БЧХ-кода. В качестве канала для моделирования был выбран канал с аддитивным белым гауссовским шумом (АБГШ), модуляция – двоичная фазовая манипуляция (binary phase shift keying, BPSK).

На рис. 3 продемонстрировано аналогичное сравнение MAB-декодеров для $(16, 7)$ расширенного БЧХ-кода по BER.

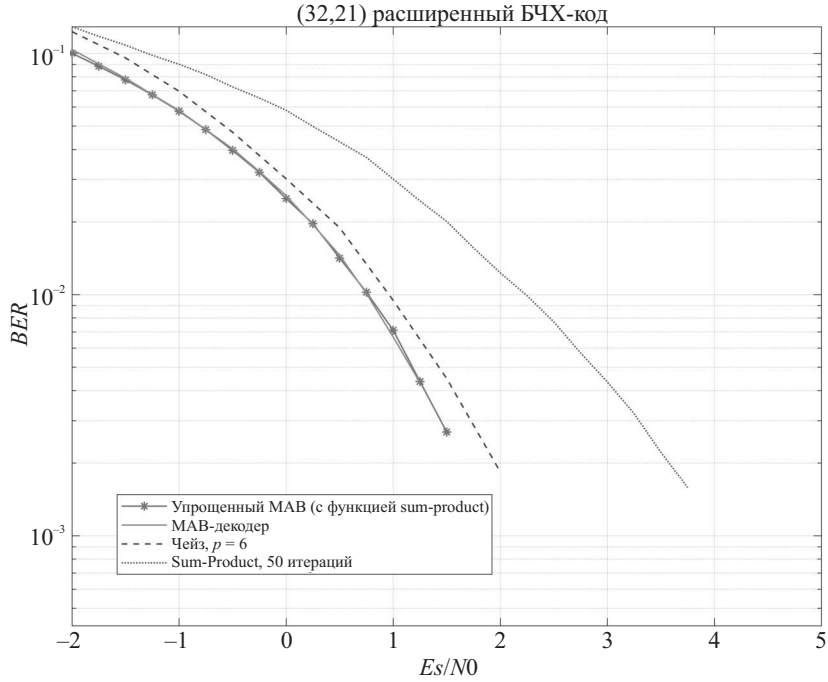


Рис. 2. BER-характеристика предложенного МАВ-декодера для $(32, 21)$ расширенного БЧХ-кода.

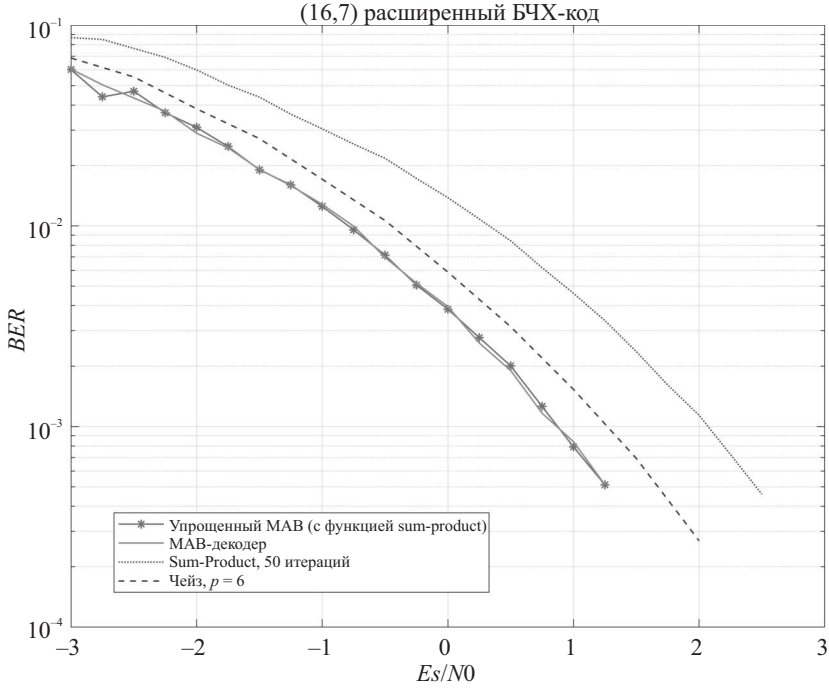


Рис. 3. BER-характеристика предложенного МАВ-декодера для $(16, 7)$ расширенного БЧХ-кода.

Как видно из представленных результатов, корректирующая способность представленного упрощенного МАВ-декодера совпадает с классическим подходом декодирования по МАВ при выборе в качестве функции для подсчета (7) функции sum-product.

Для сравнения предложенных алгоритмов декодирования по сложности запишем количество затрачиваемых на каждом этапе операций в виде формул по элементарным операциям:

для базового декодера МАВ без упрощений с функцией sum-product для подсчета (4) и (5):

$$2N^t \left(NC_+ + C_* + C_{\exp}\right),$$

для упрощенной версии декодера МАВ с функцией sum-product:

$$n^t \left(\frac{n}{2}C_+ + C_* + C_{\exp}\right),$$

для декодера Чейза:

$$2^p * (t * (n \log nC_{prod} + n \log nmC_{XOR}) + 2C_{prod} + 2mC_{XOR}),$$

где

1) C_+ – сложность вычисления суммы в $\mathbb{R}$,

2) C_* – сложность умножения (деления) в $\mathbb{R}$,

3) $C_{\exp}$ – сложность вычисления $\exp(\cdot)$,

4) C_{XOR} – сложность операции XOR (mC_{XOR} – сложность вычисления суммы в поле $GF(2^m)$),

5) C_{prod} – сложность умножения (деления) в $GF(2^m)$,

6) p – параметр декодера Чейза,

7) t – число исправляемых кодом ошибок.

Декодер Чейза 2^p раз применяет базовый декодер БЧХ с «жестким» выходом (декодер Берлекампа–Месси). Сложность декодера Берлекампа–Месси заключается в составлении квадратного уравнения, требующего вычисления t компонентов синдрома (каждое из которых равносильно быстрому преобразованию Фурье и требует $n \log nC_{prod} + n \log nmC_{XOR}$), и его решении (подстановка элементов поля $GF(2^m)$ в уравнение, что требует $2C_{prod} + 2mC_{XOR}$ операций).

Далее в табл. 1 и 2 продемонстрировано сравнение рассмотренных декодеров для расширенного БЧХ-кода с параметрами, соответствующими результатам моделирования, с точки зрения элементарных операций, использующихся для декодирования одной принятой последовательности.

Таблица 1. Сравнение декодеров по элементарным операциям для $(32, 21)$ расширенного кода БЧХ

(32,21) расширенный БЧХ	Exp	Умножения в поле GF	Умножения в $\mathbb{R}$	Сложения в $\mathbb{R}$	Сложения в поле GF
Чейз, $p = 6$	0	20 608	0	0	20 608
Упрощенный МАВ-декодер	1024	0	1024	16 384	0
МАВ-декодер [14]	8 388 608	0	8 388 608	1.7180e+10	0

Таблица 2. Сравнение декодеров по элементарным операциям для $(16, 7)$ расширенного кода БЧХ

(16,7) расширенный БЧХ	Exp	Умножения в поле GF	Умножения в $\mathbb{R}$	Сложения в $\mathbb{R}$	Сложения в поле GF
Чейз, $p = 6$	0	8320	0	0	8320
Упрощенный МАВ-декодер	256	0	256	2048	0
МАВ-декодер [14]	524 288	0	524 288	268 435 456	0

6. Заключение

В настоящей работе рассмотрено эффективное по сложности декодирование расширенных кодов БЧХ. Предложены различные модификации, касающиеся декодирования кодов БЧХ по максимуму апостериорной вероятности, использующего кодовую книгу кода, дуального расширенному коду Хэмминга с тем же числом проверок, что и расширенный код БЧХ. Изначально такой подход имеет высокую сложность в виду большой длины соответствующего кода Хэмминга. Однако этап предварительного подсчета некоторых параметров, предложенный в данной статье, позволяют существенно снизить сложность такого декодера.

СПИСОК ЛИТЕРАТУРЫ

1. *Berrou C., Glavieux A.* Near optimum error correcting coding and decoding: Turbo-codes // IEEE Trans. on Commun. 1996. V. 44. No. 10. P. 1261–1271.
2. *Bahl L., Cocke J., Jelinek F., Raviv J.* Optimal decoding of linear codes for minimizing symbol error rate // IEEE Trans. on Inform. Theory. 1974. V. 20. No. 2. P. 284–287.
3. *Bose R.C., Ray-Chaudhuri D.K.* On a class of error correcting binary group codes // Information and Control. 1960. V. 3. No. 1. P. 68–79.
4. *Peterson W.* Encoding and error-correction procedures for the Bose-Chaudhuri codes // IRE Trans. on Inform. Theory. 1960. V. 6. No. 4. P. 459–470.
5. *Massey J.* Shift-register synthesis and BCH decoding // IEEE Trans. on Inform. Theory. 1969. V. 15. No. 1. P. 122–127.
6. *Kasami T., Takata T., Fujiwara T., Lin S.* Trellis diagram construction for some BCH codes // IEEE Int. Symp. Inform. Theory and Appl. Honolulu. HI. 1990.

7. *Kasami T., Takata T., Fujiwara T., Lin S.* On the optimum bit orders with respect to the state complexity of trellis diagrams for binary linear codes // IEEE Trans. on Inform. Theory. 1993. V. 39. P. 242–243.
8. *Snyders J., Be'ery Y.* Maximum likelihood soft decoding of binary block codes and decoders for the Golay codes // IEEE Trans. on Inform. Theory. 1989. V. 35. No. 5. P. 963–975.
9. *Berger Y., Be'ery Y.* Soft trellis-based decoder for linear block codes // IEEE Trans. on Inform. Theory. 1994. V. 40. No. 1. P. 764–773.
10. *Wolf J.* Efficient maximum likelihood decoding of linear block codes using a trellis // IEEE Trans. on Inform. Theory. 1978. V. 24. No. 1. P. 76–80.
11. *Pyndiah R.* Near-optimum decoding of product codes: block turbo codes // IEEE Trans. on Commun. 1998. V. 46. No. 8. P. 1003–1010.
12. *Chase D.* Class of algorithms for decoding block codes with channel measurement information // IEEE Trans. on Inform. Theory. 1972. V. 18. No. 1. P. 170–182.
13. *Bossert M., Schulz R., Bitzer S.* On hard and soft decision decoding of BCH codes // IEEE Trans. on Inform. Theory. 2022. V. 68. No. 11. P. 7107–7124.
14. *Ashikhmin A., Litsyn S.* Simple MAP decoding of first-order Reed-Muller and Hamming codes // IEEE Trans. on Inform. Theory. 2004. V. 50. No. 8. P. 1812–1818.
15. *Hartmann C., Rudolph L.* An optimum symbol-by-symbol decoding rule for linear codes // IEEE Trans. on Inform. Theory. 1976. V. 22. No. 5. P. 514–517.

Статья представлена к публикации членом редколлегии А.И. Ляховым.

Поступила в редакцию 16.12.2024

После доработки 21.07.2026

Принята к публикации 03.08.2026