

УДК 621.391.14

МАЖОРИТАРНЫЙ ДЕКОДЕР ЦИКЛИЧЕСКОГО КОДА С ДВУХЭТАПНОЙ ОЦЕНКОЙ ДОСТОВЕРНОСТИ ИНФОРМАЦИОННЫХ СИМВОЛОВ

А.И. КОРОЛЕВ, В.К. КОНОПЕЛЬКО, Н.А. САЛАС, Е.Г. МАКЕЙЧИК, К.И. ПИРОГОВ

Белорусский государственный университет информатики и радиоэлектроники
П. Бровка, 6, Минск, 220013, Беларусь

Поступила в редакцию 1 февраля 2012

Рассматривается эффективность двухэтапного (двухступенчатого) алгоритма мажоритарного декодирования циклических кодов при коррекции ошибок кратности $t > t_{г.исп} \leq \frac{\mu}{2}$ двоичных символов: μ – количество проверочных уравнений, необходимых для гарантированной коррекции $t_{г.исп}$ ошибочных символов. Проанализированы условия, при которых осуществляется коррекция ошибочных символов кратности $t = t_{г.исп} + i$, где $i = 1; 2$, а также определены нижние границы количества комбинаций корректируемых ошибок кратности $t_{ош.1} = t_{г.исп} + 2$ и $t_{ош.2} = t_{г.исп} + 1$ двоичных символов на примере использования БЧХ-кода, корректирующего двукратные ошибки ($t_{г.исп} = 2$) и вероятность ошибочного декодирования двухступенчатого мажоритарного декодера при передаче данных по каналу связи с аддитивным белым гауссовым шумом (АБГШ).

Ключевые слова: кодер, декодер, циклический код, мажоритарный элемент, вероятность ошибок, система отдельных проверок, кодовое расстояние, кратность ошибок.

Одноэтапное мажоритарное декодирование циклических кодов

Известно, что классический одноэтапный (одноступенчатый) мажоритарный алгоритм декодирования циклических кодов (ЦК) при формировании системы отдельных проверок (СПП) имеет (обеспечивает) минимальную сложность реализации и задержку данных при декодировании ($L_3 = n + k$ тактов при декодировании « k » информационных символов: $n = k + \ell$ – длина кодовой последовательности в двоичных символах, ℓ – количество проверочных символов), а также количество ошибочных кодовых (информационных) символов вне границ минимального кодового расстояния (d_0), т.е. $t_{корр} \geq t_{г.исп} \leq \frac{\mu}{2}$ двоичных символов (бит) [1–4, 6].

В [5] для одноступенчатого (одношагового) алгоритма мажоритарного декодирования определены условия и максимальное количество корректируемых комбинаций ошибок кратности $t_{г.исп} \leq \frac{\mu}{2} + i$, $i = 1-8$ для циклических кодов с параметрами (7;3), (15;4), (15;7), (17;8) и (21;11) при передаче данных по каналам связи с аддитивным белым гауссовым шумом (АБГШ). Установлено, что общее количество корректируемых комбинаций ошибок кратности $t = 3$ и 4 двоичных символа для циклических кодов с параметрами (15;7) и (17;8) не превышает 20%. Следовательно, увеличение количества корректируемых комбинаций ошибок данной кратности на основе данного или модифицированного мажоритарного алгоритма декодирования обеспечит повышение достоверности передачи данных.

Далее анализируется корректирующая способность мажоритарного декодера с двухэтапной оценкой достоверности принятых информационных символов на примере использования циклического БЧХ-кода с параметрами $(n; k; d_0) = (15; 7; 5)$, $P(x) = x^8 + x^7 + x^6 + x^4 + 1$ и $h(x) = x^7 + x^6 + x^4 + 1$.

Двухэтапное мажоритарное декодирование циклических кодов

При анализе корректирующей способности мажоритарного декодера с двухэтапной оценкой достоверности принятых кодовых (информационных) символов принято следующее:

- между крайними ошибочными кодовыми символами может быть один (при $t_{\text{ош}} = 3$ двоичных символа) или два (при $t_{\text{ош}} = 4$ двоичных символа) безошибочных кодовых символов. Комбинации ошибок вида $t_1 = 1011$ или 1101 (при $t_{\text{ош}} = 3$) и $t_2 = 10111$, или 11011 и 11101 (при $t_{\text{ош}} = 4$) считаются четырех и пятикратными соответственно при $t_{\text{ош}} = 3$ и $t_{\text{ош}} = 4$ двоичных символа;

- трех- и четырехкратные ошибки распределены по всей длине ($n=15$) кодовых символов с безошибочным интервалом ($L_{\text{зош}}$) между соседними ошибочными символами не менее, чем $L_{\text{зош}} = t + 1$ кодовых символов: $t = t_{\text{ош}} = 3$ или 4 двоичных символов;

- каждое проверочное уравнение, число которых $\mu = 2 \cdot t_{\text{исп}} = 2 \cdot 2 = 4$ (кроме тривиального уравнения) содержит не менее $m = (n - 1) / (d_0 - 1) = (15 - 1) / (5 - 1) = 3,5$ кодовых символа: принимаем $m = 3$. На рис. 1 представлена система отдельных проверочных уравнений (как один из вариантов) БЧХ-кода с параметрами $(n; k; d_0) = (15; 7; 5)$, которая далее будет использована при анализе корректирующей способности мажоритарного декодера с двухэтапной оценкой достоверности принятых кодовых (информационных) символов.

$$\mu = \begin{cases} \Pi_1 = a_1 = a_1' \\ \Pi_2 = a_2 \oplus a_4 \oplus a_{12} \\ \Pi_3 = a_3 \oplus a_7 \oplus a_{14} \\ \Pi_4 = a_5 \oplus a_9 \oplus a_{13} \\ \Pi_5 = a_{10} \oplus a_{12} \oplus a_{15} \end{cases}$$

Рис. 1. Система отдельных проверочных уравнений циклического кода $(n; k; d_0) = (15; 7; 5)$,

$$P(x) = x^8 + x^7 + x^6 + x^4 + 1 \text{ и } h(x) = x^7 + x^6 + x^4 + 1:$$

\oplus – знак суммирования по модулю два двоичных символов

На рис. 2 и 3 представлены соответственно функциональная схема одноступенчатого мажоритарного декодера циклического $(15; 7; d_0)$ кода и временные диаграммы сигналов управления ключами декодера.

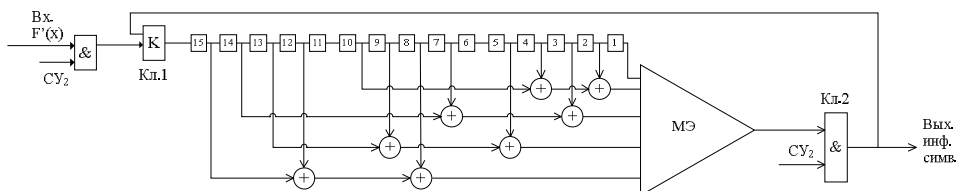


Рис. 2. Функциональная схема одноступенчатого мажоритарного декодера циклического $(15; 7; d_0)$ – кода: \oplus – сумматор по модулю два, $\square_{\text{к}}$ – ключ управления декодера; $\square_{\text{и}}$ – ячейка памяти регистра сдвига, $\square_{\text{к}}$ – коммутатор; МЭ – мажоритарный элемент

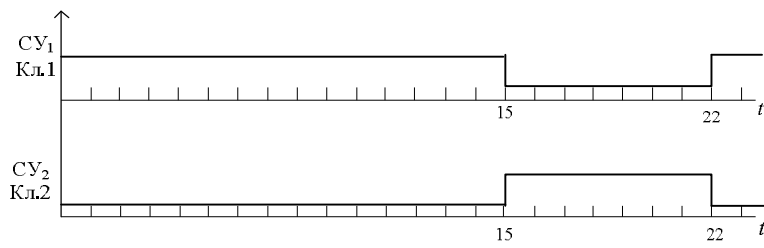


Рис. 3. Временные диаграммы сигналов управления ключами декодера

Обобщенная структурная схема мажоритарного декодера с двухэтапной оценкой достоверности принятых информационных символов приведена на рис. 4, а на рис. 5 – временные диаграммы сигналов управления ключами декодера.

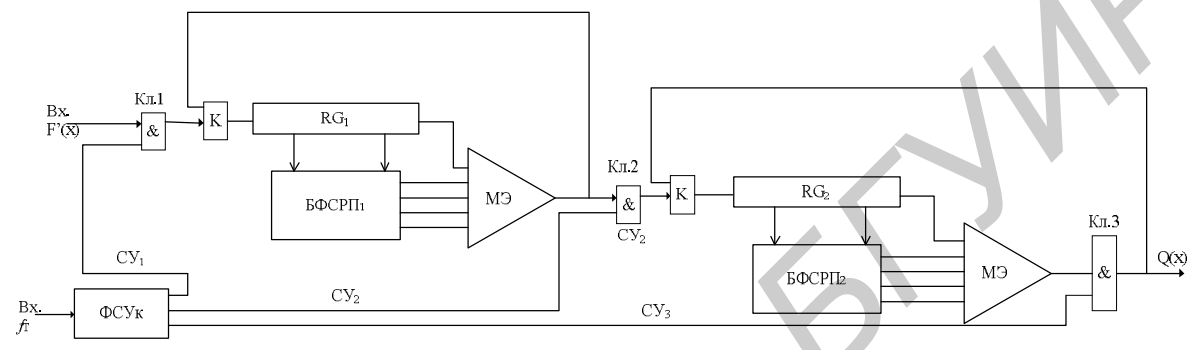


Рис. 4. Обобщенная структурная схема мажоритарного декодера с двухэтапной оценкой достоверности информационных символов: ФСУК – формирователь сигналов управления ключами; БФСРП – блок формирования системы раздельных проверок; МЭ – мажоритарный элемент, RG – регистр сдвига; $\square_{\text{к}}$ – коммутатор, $\square_{\text{к}}$ – ключ управления; CY_1-CY_3 – сигналы управления

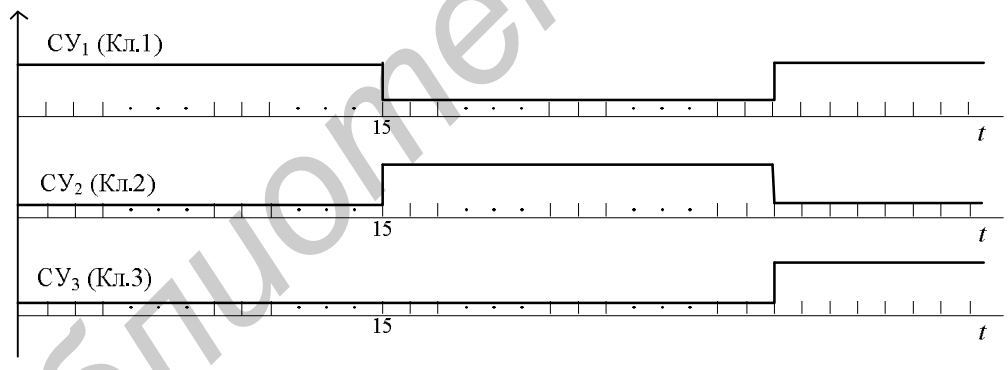


Рис. 5. Временные диаграммы сигналов управления ключами декодера

Так как при использовании ЦК система раздельных проверочных уравнений (проверок), сформированная относительно первого (информационного) символа, для всех остальных кодовых (информационных) символов кода формируется путем циклического сдвига кодовых символов на $(n-1)$ такт соответственно, то далее анализируется алгоритм мажоритарного декодирования только для первого информационного символа в каждой ступени декодера.

Структура ошибок кратности $t_{\text{г.исп}} \leq \frac{\mu}{2}$ или $t_{\text{г.исп}} \leq \frac{\mu-1}{2}$ соответственно при четном и нечетном значениях μ получили название исправимой, т.е. все комбинации ошибок $N_{01} = C_n^{t_{\text{г.исп}}}$ кратности $t_{\text{г.исп}} \geq 2$ двоичных символа будут исправлены [1–3].

В случае, если $t_{\text{ош}} = t_{\text{г.исп}} + i, i = 1; 2$, количество исправленных комбинаций ошибок данной кратности зависит как от структуры ошибок (четное или нечетное число ошибочных кодовых символов входит в $\mu - j (j \geq 1)$ проверочных уравнений), сформированной системы

проверочных уравнений, так и от реализуемого алгоритма мажоритарного декодирования. Если $t_{\text{ош}} > t_{\text{г.исп}} + i$, $i = 1; 2$, и осуществляется безошибочное декодирование одного или более кодовых (информационных) символов из комбинации ошибок данной кратности, то введение безошибочных символов в регистр сдвига по цепи обратной связи (ОС) приводит к уменьшению количества ошибочных кодовых (информационных) символов в регистре сдвига соответствующей ступени декодирования и, следовательно, к уменьшению вероятности принятия решения по следующим кодовым (в первой ступени декодирования) и информационным (во второй ступени декодирования) символам, а в противном случае – к увеличению (размножению) количества ошибок в регистрах сдвига и, соответственно, к увеличению вероятности ошибочного декодирования мажоритарного декодера.

Уменьшение вероятности ошибочного принятия решения и, следовательно, вероятности ошибочного декодирования данных в целом можно обеспечить выбором соответствующего количества ступеней (этапов) декодирования и значений порогов мажоритарных элементов: в первой(ых) ступени(ях) декодирования «целесообразно пропустить» (оставить без коррекции) один или более ошибочных кодовых символов, а «случайное» исправление одного или более ошибочных кодовых символов в данной (ых) ступенях декодирования обеспечивает уменьшение ошибок для коррекции ошибочных символов во второй или в последующих ступенях декодирования. Данный принцип коррекции ошибок кратности $t_{\text{ош}} = t_{\text{г.исп}} + i$, $i = 1; 2$ положен в основу работы двухступенчатого мажоритарного декодера циклического БЧХ-кода, приведенного на рис. 4. В первой ступени мажоритарного декодера порог принятия решения для первого мажоритарного элемента (МЭ1) принят равным $\Pi_1 = \mu - 1 = t_{\text{г.исп}} + 2 = 5 - 1 = 4$, а во второй ступени для второго мажоритарного элемента (МЭ2) порог принятия решения $\Pi_2 \geq \mu - 2 = t_{\text{г.исп}} + 1 = 2 + 1 = 3$, при этом в первой ступени, или на первом этапе декодирования, производится оценка достоверности всех n ($n = 15$) кодовых символов, а во второй ступени, или при реализации второго этапа декодирования, выполняется оценка только k ($k = 7$) информационных символов.

Вероятностные оценки эффективности двухэтапного мажоритарного алгоритма декодирования

На основании установленных ограничений на функционирование двухступенчатого мажоритарного декодера можно сделать следующие утверждения:

Утверждение 1: двухступенчатый мажоритарный декодер исправляет некоторые комбинации ошибок кратности $t_{\text{ош.1}} = t_{\text{г.исп}} + 2 = \frac{\mu}{2} + 2 = \frac{4}{2} + 2 = 4$ бита после первой ступени декодирования и $t_{\text{ош.2}} = \frac{\mu}{2} + 1 = \frac{4}{2} + 1 = 3$ бита после второй ступени декодирования, если только

ошибки данной кратности не нарушают ортогональности более, чем на $\frac{\mu}{2} + 1$ проверочных уравнений или в проверочные уравнения входит четное число ошибочных кодовых символов.

Доказательство данного утверждения определяется принципом работы декодера и системой сформированных отдельных проверочных уравнений (рис. 5).

Утверждение 2: с увеличением численных значений параметров ЦК, т.е. n и k при $t_{\text{ош}} = t_{\text{ош}} + i = \text{const}$ и $i = 1; 2$, для коррекции максимального количества комбинаций ошибок кратности $t_{\text{ош}}$ необходимо использовать более двух ступеней декодирования (двух этапов декодирования) с измененными (разными) порогами декодирования.

Доказательство данного утверждения вытекает из определения количества комбинаций заданной кратности, а именно $N = C_n^{t_{\text{ош}}}$; с увеличением n количество комбинаций ошибок кратности $t_{\text{ош}}$ увеличивается.

Утверждение 3: пусть N_{01} и N_{02} – число всех комбинаций ошибок кратности $t_{\text{ош.1}} = 4$ и $t_{\text{ош.2}} = 3$ бита, а вероятность посимвольной ошибки в канале связи $P_k \ll \frac{1}{n}$, тогда количество корректируемых комбинаций ошибок каждой кратности может быть приближенно определено с использованием выражения [7]:

$$N_{0i} \geq \binom{n-t_i}{t_i} - \binom{2t_i+1}{t_i} \binom{n-t_i}{2t_i+1}^{t_i}, \quad (1)$$

где $t_i = t_{\text{ош.1}}; t_{\text{ош.2}}$ – ошибки кратности 4 и 3 бита соответственно.

Вероятность ошибочного декодирования может быть приближенно определена с использованием выражения

$$P_{\text{ош.дек}} = C_n^{t_i+1} \cdot P_{\text{ош.1}}^{t_i+1} (1 - P_{\text{ош.1}})^{n-t_i-1}, \quad (2)$$

где $P_{\text{ош.1}} = \sum_{i=t_{\text{г.исп}}+1}^n C_n^i \cdot P_k^i (1 - P_k)^{n-i}$ – вероятность ошибочного декодирования первой ступени мажоритарного декодера.

Доля комбинаций ошибок кратности $t_{\text{ош}} = t_{\text{г.исп}} + i, i = 1; 2$, которые являются корректируемыми, определяется следующим неравенством:

$$Q \leq N_{0i} / C_{n-t_{\text{ош}}}^{t_{\text{ош}}} \quad (3)$$

На рис. 6 приведены кривые вероятности ошибочного декодирования мажоритарных декодеров циклического БЧХ-кода с одной (кривая 2) и двумя (кривая 3) ступенями декодирования. Моделирование корректирующей способности мажоритарных декодеров выполнялось для канала связи с АБГШ и ОФМ-4 с когерентным способом обработки ФМ-сигналов.

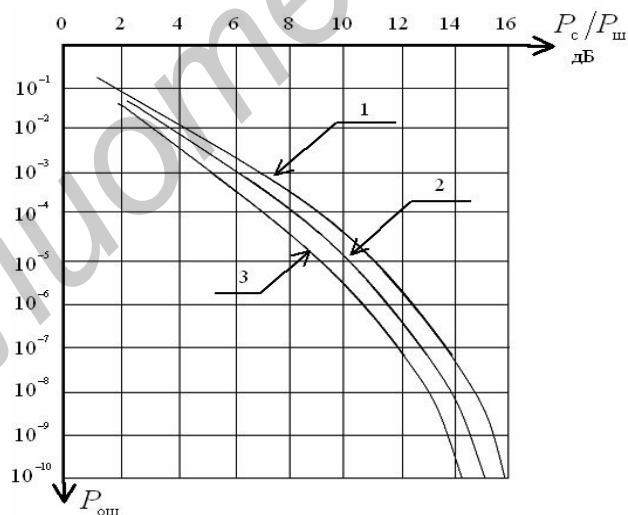


Рис. 6. Вероятности ошибочного приема данных при кодировании БЧХ-кодом с параметрами (15;7;5) с одной и двумя ступенями мажоритарного декодирования: 1 – помехоустойчивость когерентной ОФМ-4; 2 – вероятность ошибочного декодирования мажоритарного декодера с одной ступенью; 3 – вероятность ошибочного декодирования мажоритарного декодера с двумя ступенями.

Результаты моделирования показывают, что при использовании мажоритарного декодера с одной ступенью декодирования обеспечивается энергетический выигрыш кодирования (ЭВК) порядка 0,8–0,9 дБ при $P_k = 10^{-3} - 10^{-4}$ соответственно. Введение второй ступени декодирования, или второго этапа декодирования, обеспечит дополнительное увеличение ЭВК порядка 0,25–0,32 дБ соответственно при $P_k = 10^{-3} - 10^{-4}$. Следовательно, использование двух-

этапного алгоритма мажоритарного декодирования БЧХ-кода обеспечивает общий ЭВК порядка 1,05–1,22 дБ при $P_k = 10^{-3} - 10^{-4}$ соответственно или уменьшение вероятности ошибочного приема данных на два порядка, т.е. $P_{\text{ош.пр}} = 10^{-5} - 10^{-6}$, при использовании ОФМ-4 с когерентным способом обработки ФМ-сигналов.

Заключение

Предложен двухэтапный алгоритм мажоритарного декодирования циклических кодов с жестким принятием решения на выходе дискретного канала связи, обеспечивающий коррекцию ошибок в 1,5–2 раза больше гарантированной исправляющей способности одноэтапного алгоритма декодирования. Установлено, что введение второго этапа, или второй ступени декодирования позволяет увеличить на два порядка достоверность передачи данных. Разработано правило выбора порогов мажоритарных элементов ступеней декодирования.

В данной статье не рассматривался алгоритм мажоритарного декодирования с мягким принятием решения как на входе, так и выходе первой ступени мажоритарного декодера, а также вопросы цикловой синхронизации, которые требуют самостоятельных исследований.

MAJORITY DECODER OF CYCLIC CODE WITH TWO-STAGE ESTIMATION OF RELIABILITY OF INFORMATION

A.I. KOROLEV, V.K. KONOPELKO, N.A. SALAS, E.G. MAKEICHNIK, K.I. PIROGOV

Abstract

The efficiency two-stage majority decoding algorithm for cyclic codes in the correction of error of multiplicity $t > t_{\text{г.исп}} \leq \frac{\mu}{2}$ binary symbols where μ – the number of test equations, needed to guarantee the correction of $t_{\text{г.исп}}$ erroneous symbols is studied. The conditions under which correction of erroneous symbols of multiplicity $t = t_{\text{г.исп}} + i$ where $i = 1; 2$ is executed, are analyzed, and also the lower bound of the number of combinations of corrected errors of multiplicity $t_{\text{ош.1}} = t_{\text{г.исп}} + 2$ and $t_{\text{ош.2}} = t_{\text{г.исп}} + 1$ binary symbols is identified for the 2 bits correcting BCH-code. The erroneous decoding probability of the two-stage majority decoder in presence of a communication channel with the additive white Gaussian noise (AWGN) is defined.

Список литературы

1. Блейхут Р. Теория и практика кодов, контролирующих ошибки. М., 1986.
2. Кларк Дж. мл. Кодирование с исправлением ошибок в системах цифровой связи. М., 1987.
3. Портной С.Л. // Тр. НИИР. 1981. №4. С. 44–54.
4. Townsend R.L., Weldon E.J. // IEEE Trans. Inform. Theory. Vol. 1967. T-13. P 183–195.
5. Штарьков Ю.М. // Проблемы передачи информации. 1966. Вып. 3. С. 39–47.
6. Колесник В.Д. // Проблемы передачи информации. 1971. Вып. 3. С. 3–12.
7. Питерсон У. Коды, исправляющие ошибки. М, 1964.