

УДК 621.391.14

КОРРЕКЦИЯ МОДУЛЬНЫХ ОШИБОК НА ОСНОВЕ СОСТАВНЫХ ЦИКЛИЧЕСКИХ КОДОВ

Е.Г. МАКЕЙЧИК, В.К. КОНОПЕЛЬКО, А.И. КОРОЛЁВ

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

Поступила в редакцию 25 апреля 2016

Выполнена оценка эффективности предложенного метода коррекции модульных и пакетных ошибок на основе составных циклических кодов и $N(N \geq 2)$ ступенчатого кодирования и декодирования информации. Определены основные параметры канальных кодеров и проведен сравнительный анализ рассчитанных характеристик с параметрами канальных кодеров на основе известных (базисных) кодов. Показано, что для практических целей достаточно использовать коэффициент внутреннего перемежения информационных символов $\alpha = 2$ и не более двух-трех ступеней кодирования и декодирования.

Ключевые слова: групповой (циклический) код, кодер, декодер, модуль ошибок, пакет ошибок, перемежение.

Общий принцип построения составных циклических кодов

В соответствии с [1–3] принцип построения составных циклических кодов состоит в организации «внутреннего» перемежения (разнесения) информационных символов, участвующих в формировании проверочных уравнений или проверок на четность исходного или базового двоичного группового (циклического) кода.

Величина перемежения информационных символов, участвующих в формировании проверочных символов (проверок), носит название коэффициента перемежения α , который может быть равным или больше 2 ($\alpha \geq 2$): при $\alpha = 1$ внутреннее перемежение информационных символов отсутствует [2, 3].

Составной циклический код формируется из исходного (базового) циклического кода путем перевода показателей степеней порождающего полинома базового кода в степени a раз больше. В общем виде это можно записать как $x^l \rightarrow x^{a \cdot l}$, где l – максимальная степень порождающего полинома базового циклического кода (ЦК). Подстановка $x^l \rightarrow x^{a \cdot l}$ приводит к тому, что между символами строк и столбцов порождающий $G(x)$ и проверочной $H(x)$ матриц вставляется $(\alpha - 1)$ нулевых символов. Если базовый циклический код определяется уравнением вида

$$x^n - 1 = p(x) \cdot h(x), \quad (1)$$

где $p(x)$ и $h(x)$ – соответственно порождающий и проверочный полиномы базового циклического кода, то составной ЦК будет удовлетворять следующему равенству [1–3]:

$$x^{a \cdot n} - 1 = p(x^{a \cdot l}) \cdot h(x^{a \cdot k}). \quad (2)$$

Блок информационных и проверочных символов составного ЦК a_0, a_1, \dots, a_{n-1} состоит из a независимых образующих последовательностей. В каждую i -ю образующую

последовательность входят символы a_{i+a_i} , где $i = 0, 1, \dots, n$. Следовательно, каждая такая последовательность является блоком короткого базового циклического кода с порождающим полиномом $p(x)$ с максимальной степенью l . Так как порядок мультипликативной циклической группы полиномов по модулю полинома $p(x)$ равен n , то порядок такой же группы полиномов по модулю полинома $p(x^a)$ равен $\alpha \cdot n$ и, следовательно, будет иметь следующие неравенства [1–3]:

$$(x^i - 1) \leq 0 \pmod{p(x^a)}, \text{ если } i < \alpha \cdot n. \quad (3)$$

В этом случае первые строки порождающей $G'(x)$ и проверочной $H'(x)$ матриц составного ЦК рассматриваются как вектор-строки, соответствующие полиномам $p(x^{a^l})$ и $h(x^{a^k})$ базового ЦК со вставленными нулевыми символами между смежными символами. Остальные строки матриц $p(x^{a^l})$ и $h(x^{a^k})$ образуются в результате последовательных $(\alpha - 1)$ циклических сдвигов каждой вектор-строки [1–3].

Из построения $H'(x)$ составного ЦК следует, что первая строка $H'(x)$ осуществляет проверку символов только группы a_{1+a_i} , следующая строка охватывает проверку символы только группы a_{2+a_i} и так до последней строки $H'(x)$. В этом случае любая из проверок включает в себя символы только какой-либо одной группы и, соответственно, каждая группа будет контролироваться l уравнениями проверок базового ЦК [3–5].

Корректирующая способность составного ЦК определяется как корректирующей способностью базового ЦК, так и величиной коэффициента перемежения a и соответствует следующему выражению:

$$t_{\text{кор.с.}} \leq \alpha \cdot t_{\text{кор.б.}} = \alpha \frac{d_0 - 1}{2}, \quad (4)$$

где $t_{\text{кор.б.}} \leq \frac{d_0 - 1}{2}$ – кратность ошибок корректируемых базовым циклическим кодом, d_0 – минимальное кодовое расстояние базового циклического кода.

Алгоритм декодирования составного ЦК полностью определяется алгоритмом декодирования базового ЦК, что существенно упрощает практическую реализацию канальных кодеров цифровых систем передачи информации.

Корректирующую способность модульных ошибок составными помехоустойчивыми кодами проиллюстрируем на примерах использования циклического кода Хэмминга, корректирующего случайные ошибки модульного кода с параметрами (24;16). Коэффициент перемежения $\alpha = 2$.

Пример 1. Базовый циклический код Хэмминга с параметрами $(n; k; d_0) = (7; 4; 3)$, $p(x) = x^3 + x^2 + 1$, $h(x) = x^4 + x^3 + x^2 + 1$, $t_{\text{кор.б.}} \leq d_0 - 1/2 = 3 - 1/2 = 1$ бит при преобразовании в составной код с параметрами: $(\alpha \cdot n; \alpha \cdot k; \alpha d_0) = (2 \cdot 7; 2 \cdot 4; 2 \cdot 3) = (14; 8; 6)$ корректирует как модульную, так и пакетную ошибку кратностью $t_{\text{кор.с.}} \leq \alpha \cdot t_{\text{кор.б.}} = 2 \cdot 1 = 2$ бита. Алгоритм декодирования – мажоритарный.

Для доказательства корректирующей способности составного циклического кода Хэмминга необходимо сформировать проверочную матрицу составного кода, используя матрицу базового кода, которая формирует систему связанных проверок. Из представленной проверочной матрицы составного кода (5) видно, что при модульной или пакетной ошибке кратностью два бита сумма по модулю два двух соседних столбцов, соответствующих номерам ошибочных кодовых символов, формирует ненулевой вектор.

При наличии в кодовой последовательности плотного модуля ошибок кратности 8 бит, занимающего позиции $a_1 \dots a_8$ кодовой последовательности, структура синдрома, сформированного по уравнениям

$$\begin{aligned} \Pi_{1c} &= a_1 \oplus a_9 \oplus a_{17} \oplus a_{25} \oplus a_{33} & \Pi_{9c} &= a_1 \oplus a_{23} \oplus a_{29} \oplus a_{35} \\ \Pi_{2c} &= a_2 \oplus a_{10} \oplus a_{18} \oplus a_{26} \oplus a_{34} & \Pi_{10c} &= a_2 \oplus a_{24} \oplus a_{30} \oplus a_{36} \\ \Pi_{3c} &= a_3 \oplus a_{11} \oplus a_{19} \oplus a_{27} \oplus a_{35} & \Pi_{11c} &= a_3 \oplus a_9 \oplus a_{31} \oplus a_{37} \\ \Pi_{4c} &= a_4 \oplus a_{12} \oplus a_{20} \oplus a_{28} \oplus a_{36} & \Pi_{12c} &= a_4 \oplus a_{10} \oplus a_{32} \oplus a_{38} \\ \Pi_{5c} &= a_5 \oplus a_{13} \oplus a_{21} \oplus a_{29} \oplus a_{37} & \Pi_{13c} &= a_5 \oplus a_{11} \oplus a_{17} \oplus a_{39} \\ \Pi_{6c} &= a_6 \oplus a_{14} \oplus a_{15} \oplus a_{30} \oplus a_{38} & \Pi_{14c} &= a_6 \oplus a_{12} \oplus a_{18} \oplus a_{40} \\ \Pi_{7c} &= a_7 \oplus a_{15} \oplus a_{16} \oplus a_{31} \oplus a_{39} & \Pi_{15c} &= a_7 \oplus a_{13} \oplus a_{19} \oplus a_{25} \\ \Pi_{8c} &= a_8 \oplus a_{16} \oplus a_{17} \oplus a_{32} \oplus a_{40} & \Pi_{16c} &= a_8 \oplus a_{14} \oplus a_{20} \oplus a_{26} \end{aligned}$$

будет иметь следующий вид: $S(x) = 1111 \parallel 1111 \parallel 1111 \parallel 1111$. При наличии в кодовой последовательности модуля ошибок другой структуры или двух и более модулей ошибок, синдром будет содержать нулевые и ненулевые символы, формирующие разные структуры. Канальный декодер составного модульного кода работает следующим образом [6]:

- вычисляется синдром $S(x) = (S_1, S_2)^T$, содержащий 16 двоичных символов (битов);
- при $S_1(x) = S_2(x) = 0$ ошибки в принятой кодовой последовательности отсутствуют, или ошибки не обнаруживаются, и сигналы коррекции равны 0;

- если $S_1(x) = 0$, а $S_2(x) \neq 0$, то ошибки произошли в шестом модуле: кратность модуля ошибки равна $S_2(x) = 8$ бит;

- при $S_1(x) \neq 0$ и $S_2(x) \neq 0$ вычисляются частные синдромы по правилу $\tilde{S}_i(x) = S_i(x) \cdot A_i^T, i = 1 \dots 5$;

- далее частные синдромы сравниваются с символами синдрома $S_2(x)$ и определяется номер i , для которого выполняется условие $\tilde{S}_i = S_2$. Значение i определяет номер модуля ошибок. Кратность ошибки модуля равно S_i ;

- далее осуществляется коррекция ошибок данного модуля.

Рассмотренный пример показывает возможность эффективного применения внутреннего перемежения информационных символов, для построения составных РС-кодов и кодов Файра, а также возможность организации $N(N \geq 2)$ ступенчатого параллельного кодирования и декодирования групповых кодов.

Метод и характеристики $N(N = 2)$ ступенчатого кодирования и декодирования информации на основе составных циклических кодов

Рассмотрим принцип построения и определим характеристики двухступенчатого ($N = 2$) канального кодера на основе составного ЦК. В качестве базового ЦК выберем БЧХ-код с параметрами $(n_1; k_1; d_{01}) = (15; 7; 5)$. Данный код используется в первой ступени канального кодера. Во второй ступени канального кодера используется ЦК Хэмминга с параметрами $(n_2; k_2; d_{02}) = (7; 4; 3)$. В составные ЦК БЧХ-код и ЦК Хэмминга реорганизованы с коэффициентом преобразования $\alpha = 2$. Параметры составного БЧХ-кода будут равны $(\alpha \cdot n_1; \alpha \cdot k_1; \alpha \cdot d_{01}) = (2 \cdot 15; 2 \cdot 7; 2 \cdot 5) = (30; 14; 10)$, а ЦК Хэмминга – $(14; 8; 6)$.

Сущность двухступенчатого кодирования и декодирования информации на основе составного группового (циклического) кода состоит в том, что сформированные кодовые символы второй ступени канального кодера суммируются по модулю два с проверочными символами первой ступени канального кодера. В декодерах первой и второй ступеней

декодирования используется синдромный алгоритм, обеспечивающий высокую скорость декодирования. На рис. 2, 3 приведены обобщенные структурные схемы соответственно кодера и декодера, реализующие двухступенчатое кодирование и декодирование информации на основе составного БЧХ-кода и ЦК Хэмминга.

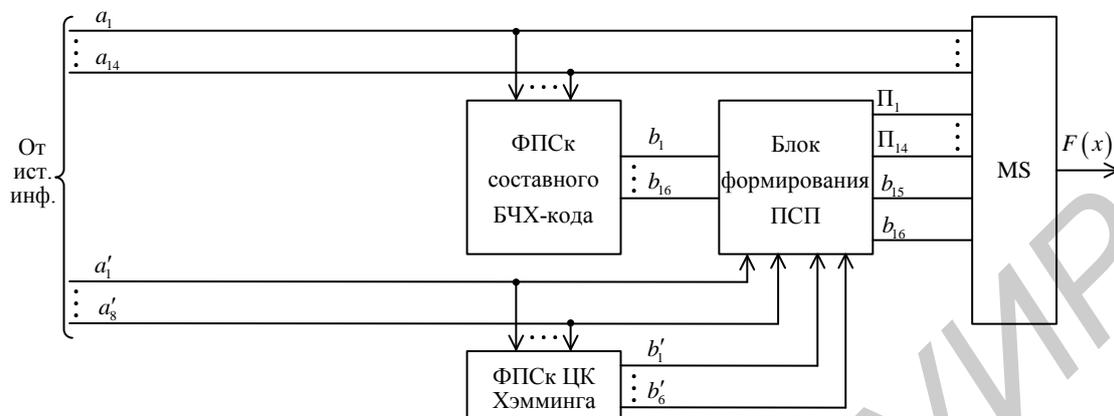


Рис. 2. Схема структурная канального кодера на основе составного БЧХ-кода и ЦК: MS – мультиплексор; ПСП – псевдослучайная последовательность; ФПСк – формирователь проверочных символов кодера

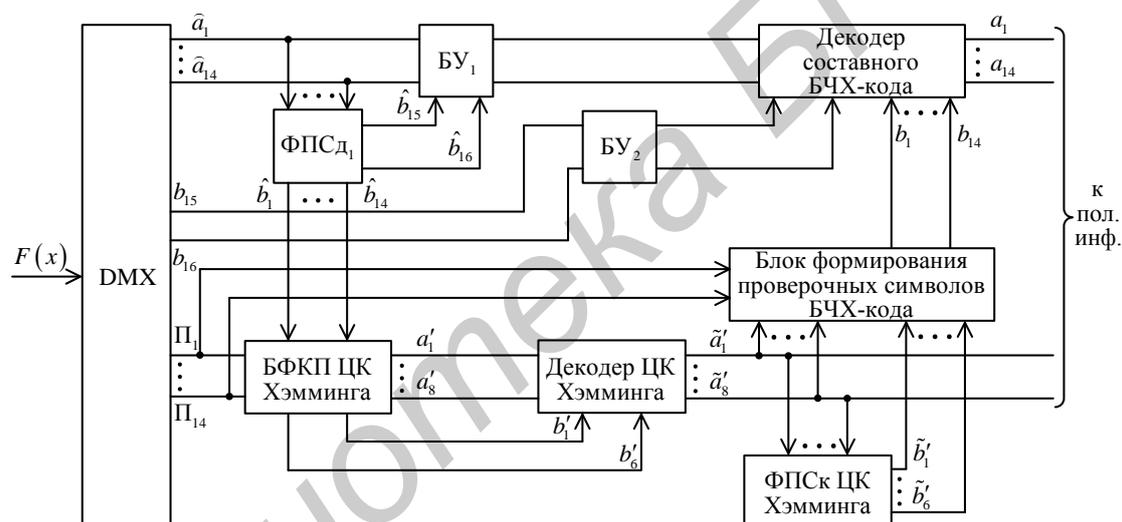


Рис. 3. Схема структурная канального декодера на основе составного БЧХ-кода и ЦК Хэмминга: ДМХ – демультиплексор; БУ – буферное устройство; БФКП ЦК – блок формирования кодовых последовательностей ЦК Хэмминга; ФПСк Д_1 – формирователь проверочных символов декодера составного БЧХ-кода; ФПСк ЦК – формирователь проверочных символов кодера ЦК Хэмминга

В соответствии с рис. 2 информационные символы $(a'_1 \dots a'_8)$ и проверочные символы $(b'_1 \dots b'_6)$ второго канала кодирования, сформированные на основе составного ЦК Хэмминга, суммируются по модулю два с проверочными символами $(b_1 \dots b_{14})$ первого канала кодирования, сформированные на основе составного БЧХ-кода (проверочные символы b_{15} и b_{16} передаются без изменения). В результате чего формируется 14 подпотоков символов псевдослучайной последовательности:

$$\Pi_1 = b_1 \oplus a'_1, \dots, \Pi_8 = b_8 \oplus a'_8, \dots, \Pi_9 = b_9 \oplus b'_1, \dots, \Pi_{14} = b_{14} \oplus b'_6.$$

В канальном декодере (рис. 3) осуществляется одновременно формирование проверочных символов $(\tilde{b}_1 \dots \tilde{b}_{16})$ первого канала декодирования на основе составного БЧХ-кода и кодовых символов $(\tilde{a}'_1 \dots \tilde{a}'_8, b'_1 \dots b'_6)$ на основе составного ЦК Хэмминга. Далее осуществляется поэтапно декодирование кодовых последовательностей составного ЦК

Хэмминга, формирование проверочных символов $(\tilde{b}'_1 \dots \tilde{b}'_6)$ второго канала декодирования, восстановление проверочных символов $(b'_1 \dots b'_{14})$ первого канала декодирования и декодирование кодовых последовательностей составного БЧХ-кода. Для согласования символов кодовых последовательностей каналов декодирования используются два буферных устройства: БУ₁ – для согласования по задержке информационных символов $(\hat{a}_1 \dots \hat{a}_{14})$ и БУ₂ – для согласования по задержке проверочных символов (b_{15}, b_{16}) первого канала декодирования.

Оценка эффективности метода двухступенчатого кодирования и декодирования информации на основе составных циклических кодов

Оценка эффективности метода двухступенчатого кодирования и декодирования информации на основе составных циклических кодов выполняется на основе расчета следующих параметров канального кодера: R_c, d_{oc} и $t_{корр.с.}$.

Определение 1. Если d_{01} и d_{02} – минимальные кодовые расстояния соответственно составных кодов первой и второй ступени кодирования и d_{01}/d_{02} , то минимальное кодовое расстояние канального кодера будет не менее максимального кодового расстояния одного из составных кодов, т.е.

$$d_{ост} = \max \{d_{01}, d_{02}\}. \quad (7)$$

Доказательство данного определения обеспечивается использованием в канальном кодере двух каналов кодирования и декодирования и двух кодов с разной корректирующей способностью $d_{01} > d_{02}$. Следовательно, ошибки минимальной кратности $(t_{корр.2} < (d_{02} - 1)/2)$ корректируются обоими кодами, а ошибки максимальной кратности $(t_{корр.1} < (d_{01} - 1)/2)$ корректируются только кодом первой ступени. Таким образом, минимальное кодовое расстояние $d_{ост}$ канального кодера будет не менее минимального кодового расстояния кода второй ступени кодирования. При $d_{01} = d_{02}$, $d_{ост} = d_{0i}$, $i \in 1; 2$.

Определение 2. Максимальная кратность ошибок корректируемых канальным кодером на длине $n_c = n_1 + n_2$ бит на основе двух составных кодов удовлетворяет следующему неравенству:

$$t_{корр.ст.} \leq t_{корр.1} + t_{корр.2}, \text{ бит} \quad (8)$$

где $t_{корр.1}$ и $t_{корр.2}$ – кратность ошибок корректируемых составными кодами соответственно первого и второго каналов декодирования.

Доказательство данного определения вытекает из принципа работы канального декодера (рис. 3) Для рассматриваемых в качестве примера составных групповых кодов максимальная кратность корректируемых ошибок составляет $t_{корр.ст.} \leq (d_{01} - 2)/2 + (d_{02} - 2)/2 = (10 - 2)/2 + (6 - 2)/2 = 4 + 2 = 6$ бит на длине $n = n_1 + n_2 = 30 + 14 = 44$ бита.

Таким образом, предложенный двухступенчатый метод кодирования и декодирования информации на основе составных циклических кодов позволяет корректировать одновременно модульные и случайные ошибки.

Определение 3. Скорость кода двухступенчатого канального кодера больше максимальной скорости передачи составного циклического кода, т.е. $R_c = \max \{R_{1c}, R_{2c}\}$.

Доказательство определения вытекает из способа формирования символов кодовой последовательности канального кодера и подтверждается численным расчетом для рассматриваемых составных кодов. Общее число информационных символов, входящих в кодовую последовательность составного БЧХ-кода $n_c = 30$ бит, равно

$k_c = k_1 + \overbrace{(\Pi_1 \dots \Pi_8)}^{k_2} = 14 + 8 = 22$ бита, где k_1 – количество информационных символов составного БЧХ-кода, $\Pi_1 \dots \Pi_8 = a'_1 \dots a'_8 = k_2$ – количество информационных символов составного ЦК Хэмминга, наложенных на проверочные символы $b_1 \dots b_8$ составного БЧХ-кода. Следовательно, $R_c = k_c/n_c = 22/30 = 0,73 > R_{2c} = k_2/n_2 = 8/14 = 0,57$ – скорость передачи составного ЦК Хэмминга; $R_{1c} = k_{1c}/n_{1c} = 14/30 = 0,46$ – скорость передачи составного БЧХ-кода.

Заключение

Предложен метод построения составных групповых кодов, обеспечивающих коррекцию как модульных, так и пакетных, и случайных ошибок. Определены основные характеристики одноступенчатого и двухступенчатого канальных кодеков на основе составных циклических кодов БЧХ и Хэмминга. Установлено, что метод построения канальных кодеков на основе составных циклических кодов обеспечивает формирование кодов с характеристиками, отличными от известных: при равной скорости передачи кодов составные коды и $N(N \geq 2)$ – ступенчатые канальные кодеки обеспечивают коррекцию ошибок большей кратности. Для практического применения предложенного метода коррекции модульных (зависимых) ошибок достаточно использования коэффициента внутреннего перемежения информационных символов $\alpha = 2$ и двух ступеней (каналов) кодирования и декодирования.

MODULAR ERRORS CORRECTION BASED ON COMPOSITE CYCLIC CODES

E.G. MAKEICHIK, V.K. KANAPELKA, A.I. KOROLEV

Abstract

The effectiveness evaluation of the proposed method for correction modular and burst errors based on composite and $N(N \geq 2)$ cyclic codes and step encoding and decoding of information is made. The main parameters of the channel codecs are detected and a comparative analysis of the calculated characteristics with channel codec parameters based on the known (basic) codes is realized. It's shown that for practical purposes it's sufficient to use the ratio of internal information symbol interleaving and decoding stages of encoding no more than two or three stages.

Keywords: group (cyclic) code, encoder, decoder, error module, packet errors, interleaving.

Список литературы

1. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. М., 1976.
2. Колесник В.Д., Мирончиков Е.Т. Декодирование циклических кодов. М., 1968.
3. Дмитриев О.Ф. Класс составных циклических кодов с простой реализацией. М., 1968.
4. Meggitt J.E. // IRE Transactions on Information Theory. 1961. Vol. 17, № 4. P. 232–244.
5. Радченко А.Н., Мирончиков Е.Т. // Радиотехника и электроника. 1961. №11. С. 17–21.
6. Конопелько В.К., Липницкий В.А., Дворников В.Д. и др. Теория прикладного кодирования. Минск, 2004.