УДК 621.391.14

МЕТОД И ХАРАКТЕРИСТИКИ ВЛОЖЕННОГО КОДИРОВАНИЯ ГРУППОВЫХ КОДОВ НА ОСНОВЕ ЦИКЛИЧЕСКОЙ ПОДСТАНОВКИ КОРРА

АЛЬ-АЛЕМ АХМЕД САИД, А.И. КОРОЛЕВ

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск 20013, Беларусь

Поступила в редакцию 13 октября 2009

Выполнена оценка эффективности предложенного метода вложенного кодирования групповых кодов, построенных на основе циклической подстановки Корра. Определены основные параметры циклического кода и канального кодека, реализующего метод вложенного кодирования и приведен сравнительный анализ рассчитанных параметров с параметрами известных кодов. Показано, что для практических целей достаточно использовать циклическую подстановку Корра степени $\alpha = 3$. В качестве внутреннего кода используется базовый (исходный) групповой (циклический) код с реализацией в декодере алгоритма декодирования базового группового кода.

Ключевые слова: групповой код, циклический код, кодер, декодер, кодек, кодовая последовательность, модуль ошибок, пакет ошибок, порождающая матрица, проверочная матрица, скорость кода, перемежение.

Общие принципы построения модифицированных групповых кодов на основе циклической подстановки Корра

Высокую скорость декодирования кодовых последовательности (КП) двоичных групповых кодов при минимальной сложности реализации декодирующих устройств (декодеров) обеспечивают алгебраические алгоритмы декодирования, а именно, мажоритарный, пороговый и синдромный. Однако данные алгоритмы декодирования чаще всего используются для коррекции случайных (независимых) ошибок. Кроме того, количество кодов, обеспечивающих реализацию данных алгоритмов существенно ограничен. Увеличить количество кодов и их корректирующую способность представляется возможным на основе использования циклической подстановки Корра и метода вложенного кодирования сформированных групповых кодов.

В соответствии с [1-3] сущность циклической подстановки Корра состоит в организации “внутреннего” перемежения (разнесения) информационных (кодовых) символов на основе которых осуществляется формирование проверочных уравнений (проверок на четность) базового двоичного группового кода.

Утверждение 1. Модифицированный групповой ($\alpha \cdot n$; $\alpha \cdot k$; $\alpha \cdot d_o$) – код построенный на основе базового (исходного) циклического (n ; k ; d_o) – кода путем циклической подстановки Корра степени $\alpha \geq 2$ корректирует любые $\alpha \cdot t$ или менее ошибочных символов при формировании $\alpha \cdot м$ проверочных уравнений ; $t \leq \frac{d_o\text{-}1(2)}{2}$ и $t \leq \frac{\mu}{2}$ ошибочных символов, корректируемых соответственно при синдромном и мажоритарном алгоритмах декодирования.

Данное утверждение легко доказывается построением конкретного модифицированного группового кода. Пусть в качестве исходного группового кода используется циклический максимальной длины с параметрами:

$$(n;k;d_0)=(7;3;4),\ R=k/n=3/7=0,428,\ P(x)=x^4+x^3+x^2+1,\ h(x)=x^3+x^2+1,$$

$$t_{\text{исп.}}\le\frac{d_0-1}{2}=3-1/2=1 \text{ бит и } \text{r}=(1\text{-R})\cdot100\%=(1\text{-}0{,}428)\cdot100\%=57{,}2\%$$

Для декодирования кодовых последовательностей (КП) используется мажоритарный алгоритм с формированием проверочных уравнений (проверок) а на основе проверочной матрицы вида (б):

а)

$$\begin{aligned}
&м_1=a_1=a_1',\\
&м_2=a_1\oplus a_2\oplus a_4,\\
&м_3=a_2\oplus a_3\oplus a_5,\\
&м_4=a_3\oplus a_4\oplus a_6,\\
&м_5=a_4\oplus a_5\oplus a_7,
\end{aligned}$$

где $\oplus$ - знак суммирования двоичных символов по модулю два.

б)

$$\text{H}_{(7,4)}\begin{bmatrix}1101000\\0110100\\0011010\\0001101\end{bmatrix}, \qquad (1)$$

Примем значение циклической подстановка $\alpha=2$. В результате чего модифицированный циклический код (ЦК) будет иметь следующие параметры:

$$(\alpha\cdot n;\alpha\cdot k;\alpha\cdot d_0)=(2\cdot7;2\cdot3;2\cdot4)=(14;6;8),\ P_{\text{м}}(x)=x^{\alpha\cdot4}+x^{\alpha\cdot3}+x^{\alpha\cdot2}+1=x^8+x^6+x^4+1,$$

$$h_{\text{м}}(x)=x^{\alpha\cdot3}+x^{\alpha\cdot2}+1=x^6+x^4+1,\ t_{\text{исп.м}}\le\frac{\alpha\cdot d_0-1(2)}{2}=\frac{2\cdot4-2}{2}=\frac{8-2}{2}=3 \text{ ошибочных}$$

двоичных символа, $R_m=k/n=6/14=0,428,\ \ r=(1-R_m)\cdot100\%=(1-0,428)\cdot100\%=57,2\%$

Проверочная матрица модифицированного ЦК будет иметь следующее построение:

$$\text{H}_{(14,6)}\begin{bmatrix}10100010000000\\01010001000000\\00101000100000\\00010100010000\\00001010001000\\00000101000100\\00000010100010\\00000001010001\end{bmatrix}. \qquad (2)$$

Из структуры данной проверочной матрицы следует, что для реализации мажоритарного алгоритма декодирования необходимо формировать $M=(k+2)$ проверочных уравнений с порогом принятия решения $П\ge\frac{M}{2}$; (с учетом тривиального соотношения $a_1 = a_1^{/}$ будет сформировано $M'=M+1$ проверочных уравнении). В этом случае все ошибочные информационные символы кратностью $t_{\text{ош.}}\le3$ будут скорректированы.

Например: пусть передавалась по каналу связи КП вида: $F(x)=00000000000000$, а на вход мажоритарного декодера поступила КП вида $F'(x)=11100000000000$ (старшие информационные символы слева), т.е. принятая КП содержит пакет ошибок из трех информационных символов. В декодере в соответствии проверочной матрицей (2) для данной структуры ошибок будут сформированы проверочные уравнения результатами. $A_1 \div A_3$ для первого, второго и третьего информационного символа соответственно (рис.1.).

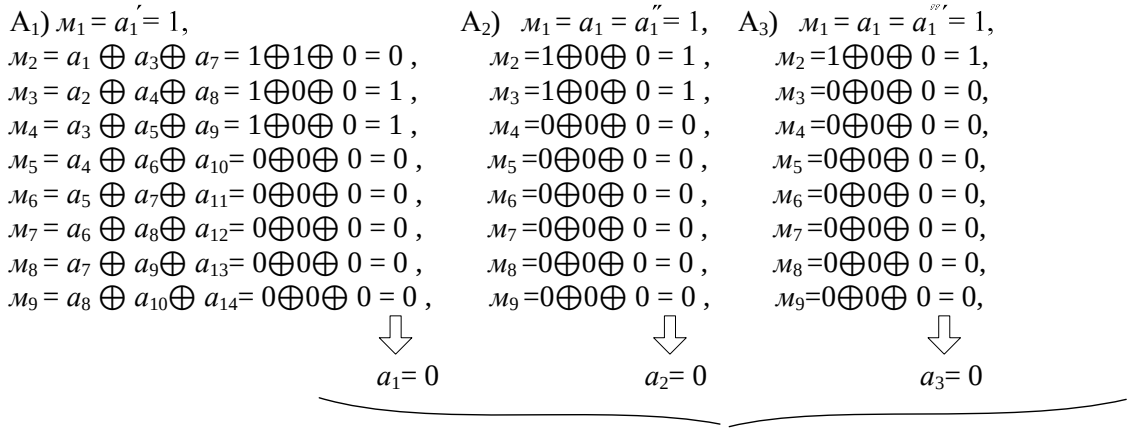

Рис.1. Сформированы проверочные уравнения результатами. $A_1 \div A_3$ для первого, второго и третьего информационного символа в декодере

Таким образом, все ошибочные информационные символы скорректированы. Аналогичным образом можно показать, что модифицированный $(\alpha \cdot n; \alpha \cdot k; \alpha \cdot d_0) = (14; 6; 8)$ – код обеспечивает коррекцию трех информационных символов $(t_{\text{исп.}} \le \frac{8-2}{2} = 3)$ при реализации синдромного алгоритма декодирования.

Метод вложенного кодирования групповых кодов на основе циклической подстановки

Возможность построения модифицированных групповых кодов на основе циклической подстановки Корра позволяет реализовать эффективный метод вложенного кодирования данных кодов, используя в качестве внутреннего базовый ЦК(при двух ступенях кодирования; базовый ЦК и модифицированный(ые) групповой(ые) код(ы)) – при трех и более ступенях кодирования. В соответствии с [4,5] для практического применения вложенного кодирования групповых кодов достаточно использование 2-3 ступеней кодирования.

На рис. 2 и рис. 3 приведены обобщенные структурные схемы соответственно кодера и декодера, реализующие двухступенчатое вложенное кодирование-декодирование информации на основе базового ЦК с параметрами (7;3;4) (внутренний код) и модифицированного ЦК (внешний код).

В декодерах данных кодов используется синдромный алгоритм декодирования, обеспечивающий высокое быстродействие декодирования кодовых последовательностей.

В соответствии с рис.2. информационные ($a_7 \div a_9$) и проверочные ($\alpha_1 \div \alpha_4$) символы второго канала кодирования (базового ЦК Хэмминга) суммируются по модулю два с проверочными ($в_1 \div в_7$) символами первого канала кодирования (модифицированного кода). В результате чего формируются семь потоков символов псевдослучайной последовательности:

$$\Pi_1 = в_1 \oplus a_7, \Pi_2 = в_2 \oplus a_8, \Pi_3 = в_3 \oplus a_9, \Pi_4 = в_4 \oplus \alpha_1, ..., \Pi_7 = в_7 \oplus \alpha_4;$$

проверочный символ $в_8$ первого канала кодирования передается без преобразования.

В декодере (рис.3) осуществляется одновременно формирование проверочных ($в_1' \div в_8'$) символов первого канала декодирования (модифицированного кода) и кодовых ($a_7' \div a_9'$, $\alpha_1' \div \alpha_4'$) символов второго канала кодирования (базового ЦК Хэмминга). Далее осуществляется поэтапно декодирование КП ЦК Хэмминга, формировании проверочных ($\alpha_1 \div \alpha_4$) символов второго канала декодирования, восстановление проверочных ($в_1 \div в_7$) символов перворго канала

декодирования и декодирование КП модифицированного кода. Для согласования по задержке декодированных информационных символов первого и второго каналов используется буферное устройство БУ.

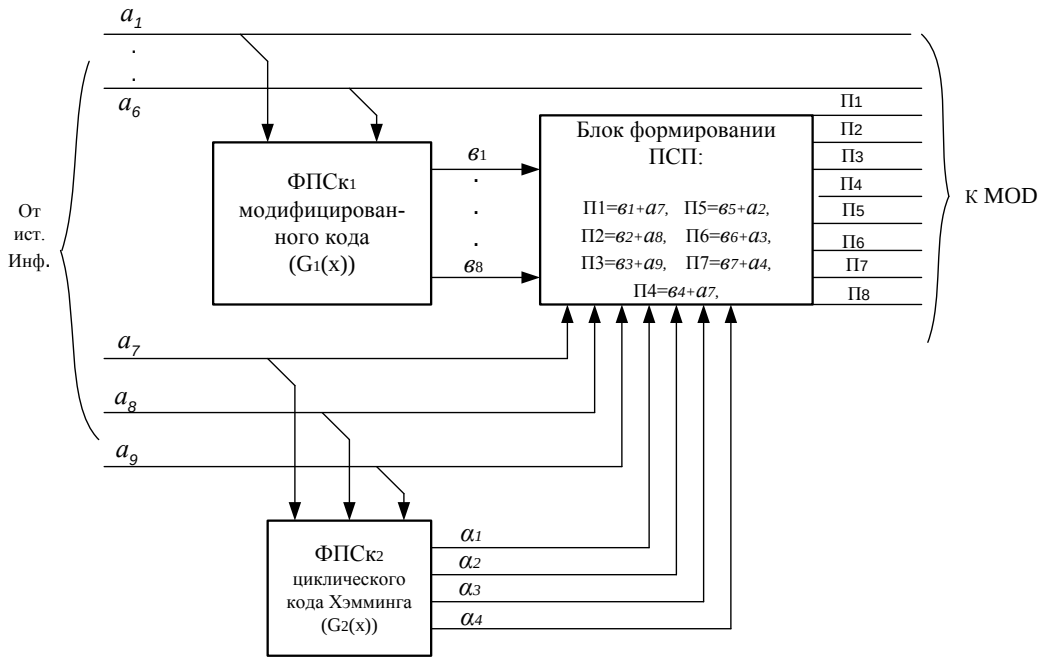

Рис. 2. Кодирующие устройство модифицированного ЦК: ФПСк$_1$ и ФПСк$_2$ – формирователи проверочных символов соответственно первого и второго каналов кодирования; ПСП – псевдослучайная последовательность

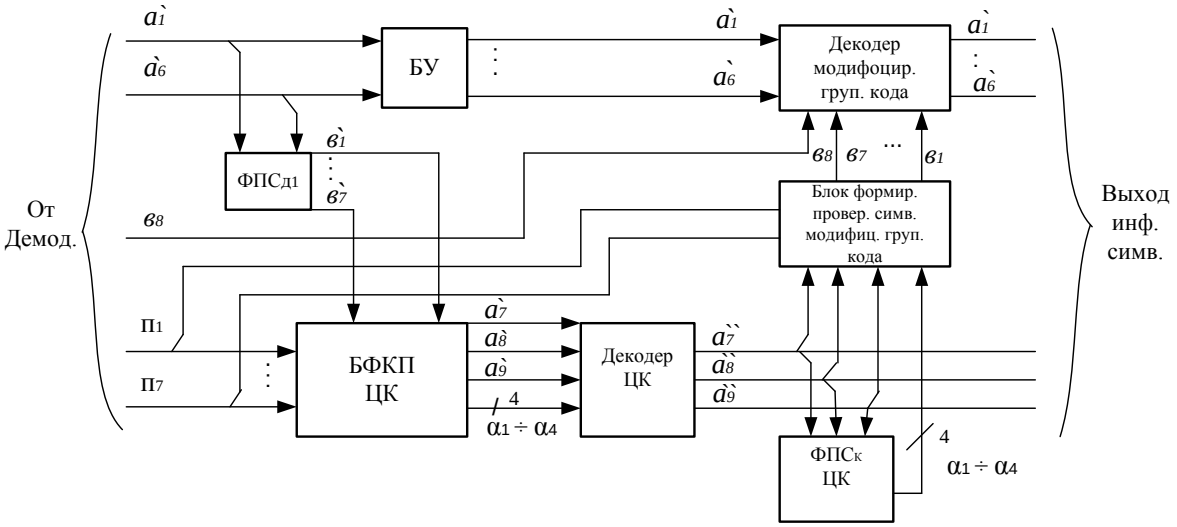

Рис. 3. Декодирующие устройство модифицированного ЦК: БУ – буферное устройство, БФКП – блок формирования кодовых последовательностей, ФПСд$_1$ – формирователь проверочных символов декодера модифицированного группового кода

В соответствии с рис.1. информационные ($a_7 \div a_9$) и проверочные ($\alpha_1 \div \alpha_4$) символы второго канала кодирования (базового ЦК Хэмминга) суммируются по модулю два с проверочными ($в_1 \div в_7$) символами первого канала кодирования (модифицированного кода). В результате чего формируются семь потоков символов псевдослучайной последовательности:

Оценка эффективности метода вложенного кодирования групповых кодов

Для оценки эффективности метода вложенного кодирования групповых кодов необходимо получить выражения количественно и качественно определяющие параметры данного метода, а именно: $R_B = k_B / n_B$ – скорость передачи кода; $d_{ов}$ – минимальное кодовое расстояние; $t_{исп.\ в}$ – общую кратность исправляемых ошибочных информационных символов; алгоритмы декодирования, обеспечивающие минимальную задержку информации и сложность реализации кодека, измеряемую количеством ячеек памяти.

Оценку параметров метода вложенного кодирования групповых кодов выполним для двух ступеней (каналов) кодирования-декодирования групповых кодов: полученные выражения не трудно обобщить на $N(N>2)$ ступеней кодирования.

Утверждение 2. Если $R_1 = k_1 / n_1$ – скорость передачи кода первой ступени (первого канала) кодирования и $R_2 = k_2 / n_2$ – скорость передачи кода второй ступени (второго канала) кодирования, то скорость передачи кода $R_в$, на основе которого реализуется метод вложенного кодирования групповых кодов, больше наибольшей скорости передачи используемых кодов, т.е. $R_B \geq R_{i\max}$, где $i \in 1;2.$

Доказательство. Избыточность используемых групповых кодов первого и второго каналов кодирования соответственно равны: $r_1 = \frac{n_1 - k_1}{n_1} = \frac{l_1}{n_1}$ и $r_2 = \frac{n_2 - k_2}{n_2} = \frac{l_2}{n_2}$.

Так как в соответствии с методом вложенного кодирования производится суммирование по модулю два символов КП второго канала и проверочных символов первого канала кодирования, то избыточность КП группового кода, реализующего метод вложенного кодирования будет равна произведению избыточностей исходных групповых кодов т.е. $r_в = r_1 \cdot r_2$.

Так как $r_1 < 1$ и $r_2 < 1$, то их произведение будет меньше наименьшего из сомножителей т.е. $r_в < r_{i\,min}$, где $i \in 1;2$.

Следовательно, скорость передачи группового кода $R_в = 1 - r_в$, на основе которого реализуется метод вложенного кодирования групповых кодов, будет больше наибольшей скорости передачи исходного группового кода, т.е.

$$R_B = 1 - r_B \rangle r_{i\max},\ i \in 1;2, \qquad \text{ч.т.д.} \tag{3}$$

Утверждение 3. Если d_{01} и d_{02} – соответственно минимальные кодовые расстояния исходных групповых кодов и $d_{01} \neq d_{02}$, то минимальное кодовое расстояние $d_{0в}$ группового кода, на основе которого реализуется метода вложенного кодирования информации , будет не менее максимального кодового расстояния исходного кода, т.е. $d_{0в} = \max.\ d_{01}, d_{02}$.

Доказательство данного утверждение обеспечивается использованием в кодеке двух каналов кодирования – декодирования и двух групповых кодов с разной корректирующей способностью: $d_{01} \langle\rangle d_{02}$. Следовательно, ошибки минимальной кратности корректируются обоими кодами, а ошибки максимальной кратности корректируются только один из кодов с наибольшим значением минимального кодового расстояния(в приведенной структурной схеме кодека модифицированный ЦК Хэмминга используемой в первом канале кодирования имеет наибольшее минимальное кодовое расстояние, а именно, $d_{01} = 8$). Исходя из того следует, что минимальное кодовое расстояние $d_{ов}$ группового кода, на основе которого реализуется метод вложенного кодирования – декодирования исходных групповых кодов, будет не менее максимального минимального кодового расстояния из исходных групповых кодов, т.е.

$$d_{0в} = \max.\ d_{01}, d_{02}\ , \qquad \text{ч.т.д.} \tag{4}$$

При $d_{01} = d_{02}$, $d_{ов} = d_{oi}$, $i \in 1;2$.

Утверждение 4. Максимальная кратность ошибок $t_{корр.в}$ корректируемые кодеком реализующего метод вложенного кодирования – декодирования исходных групповых кодов, удовлетворяет следующему равенству – неравенству:

$$t_{корр.в} \leq t_{корр.1} + t_{корр.2}\ , \tag{5}$$

где $t_{\text{корр.1}}$ и $t_{\text{корр.2}}$ – кратность ошибок корректируемых групповыми кодами первого и второго канала кодирования соответственно.

Доказательство данного утверждения выполним численным расчетом для кодека, реализующего вложенное кодирование групповых кодов с параметрами:

$(n_1; k_1; d_{01}) = (14; 6; 8)$ и $(n_2; k_2; d_{02}) = (7; 3; 4)$.

Наличие двух каналов декодирования и организация процедуры коррекции ошибок первоначально во втором канале кодека обеспечивает разделение ошибок по КП групповых кодов, а далее осуществляется поэтапное (последовательное) исправление ошибок данными кодами. Таким образом, независимые ошибки кратностью $t_{\text{корр.2}} \le \frac{d_{02} - 1(2)}{2}$ двоичных символов будет исправлены базовым ЦК Хэмминга, а группирующиеся ошибки кратностью $t_{\text{корр.1}} \le \frac{d_{01} - 1(2)}{2}$ двоичных символов будет исправлены модифицированным групповым кодом. Следовательно, общее количество корректируемых ошибок кодеком.

$$t_{\text{корр.В}} \le t_{\text{корр.1}} + t_{\text{корр.2}}, \qquad \text{ч.т.д.}$$

Задержка информации при декодировании метода вложенного кодирования зависит от используемых алгоритмов декодирования групповых кодов и способа передачи информации.

В соответствии со структурной схемой кодека (рис.1 и рис.2) минимальная задержка информации при декодировании будет обеспечиваться при реализации синдромного алгоритма декодирования и практически будет зависит от выбранного способа передачи информации.

При параллельном способе передачи информации задержка информации при декодировании будет определяться способом реализации кодека и выбранной элементной базой.

При последовательном способе передачи информации и синдромном алгоритме декодирования начальная задержка информации декодера равна длине КП модифицированного кода; для рассматриваемых групповых кодов начальная задержка информации $L_{\text{задер.синдр.}} = 14$ тактам.

При реализации мажоритарного алгоритма декодирования и последовательного способа передачи информации задержка информации будет составлять: $L_{\text{задер.синдр.}} \approx: L_{\text{задер.2k}} + L_{\text{задер.1k}} \approx (n_2 + k_2) + 2(n_1 + k_1)$ тактов, где $L_{\text{задер.2k}}$ и $L_{\text{з а д е р}}$ – задержка информации при декодировании во втором и в первом каналах соответственно.

Заключение

В данной статье предложен метод вложенного кодирования и декодирования групповых кодов, когда в качестве внешнего кода используется групповой код, построенный на основе известного циклического кода путём подстановки Корра. Определены основные характеристики группового кода при использовании двух каналов кодирования и декодирования, которые могут быть легко обобщены на групповые коды с большим количеством каналов кодирования – декодирования. Установлено, что метод вложенного кодирования и декодирования групповых кодов обеспечивает формирование кодов с характеристиками отличными от известных: при равной скорости кодов (равной избыточности кодов) модифицированный групповой код и метод вложенного кодирования – декодирования обеспечивает коррекцию ошибок большей кратности.

Для практического применения предложенного метода кодирования информации достаточно реализация двухканального кодека на основе базового и модифицированного групповых кодов. Минимальная задержка информации при декодировании обеспечивается при использовании синдромного алгоритма декодирования и параллельного способа передачи информации.

В данной статье не рассматривались вопросы организации цикловой синхронизации и сложности реализации кодека, которые требуют самостоятельных исследований.

Метод вложенного кодирования – декодирования групповых кодов может быть обобщен на сверточные коды.

METHOD AND CHARACTERISTIC CODING GROUP OF EMBEDDED CODES BASED ON CYCLIC SUBSTITUTION CORR

ALALEM AHMED SAID, A.E. KOROLEV

Abstract

Completed assessment of the effectiveness of the proposed method the embedded coding group codes constructed on the basis of a cyclic substitution Corr. The main parameters of a cyclic code and the channel codec that implements the method of the embedded coding and comparative analysis of calculated parameters with the parameters of known codes. It is shown that for practical purposes it is sufficient to use the cyclic substitution Corr degree $\alpha = 3$. As an internal code used by the base (initial) group (cyclic) code with the implementation of the decoder algorithm for decoding the base of the group code.

Литература

1. *Блейхут, Р.* Теория и практика кодов, контролирующих ошибки. М., 1986.
2. *Кларк, Дж*. Кодирование с исправлением ошибок в системах цифровой связи. М., 1986.
3. *Морелос – Сарагоса, Р*. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. М., 2005.
4. *Колесник В.Д.* Декодирование циклических кодов. М., 1968.
5. *Конопелько В.К., Аль-алем Ахмед Саид, А.И. Королев.* Устройство вложенного кодирования и декодирования групповых кодов // Заявка №. А 20080773. М., 2008.