УДК 621.391

ШТОМПЕЛЬ Н. А., канд. техн. наук, доцент (УкрГУЖТ)

Адаптивное декодирование алгебраических сверточных кодов перемежения

Обоснована целесообразность применения алгебраических сверточных кодов перемежения для увеличения достоверности передачи информации в каналах с памятью. Предложен метод итеративного декодирования данных кодов на основе комбинированного подхода с использованием процедур адаптивного распространения доверия и природных вычислений. Представлены основные принципы реализации основных этапов предложенного метода декодирования.

Ключевые слова: *адаптивное декодирование, сверточные коды, перемежение, природные вычисления.*

Постановка проблемы и анализ литературы

Для исправления пакетов ошибок, возникающих в каналах с памятью, широко используются различные кодовые конструкции совместно с процедурой перемежения. В работах [1, 2] предложены алгебраические сверточные коды перемежения с заданной скоростью кодирования, основанные на данном подходе. Алгебраическое декодирование данных кодов характеризуется значительной вычислительной сложностью и ограниченной корректирующей способностью [3]. Для повышения эффективности декодирования алгебраических сверточных кодов перемежения предлагается совместно использовать подход на основе адаптивного распространения доверия [4] и процедуры природных вычислений [5, 6].

Таким образом, актуальной задачей является обеспечение передачи информации с заданной достоверностью путем разработки метода адаптивного декодирования алгебраических сверточных кодов перемежения с приемлемой вычислительной сложностью.

Цель статьи

Повышение эффективности декодирования алгебраических сверточных кодов перемежения для обеспечения заданной достоверности передачи информации в телекоммуникационных системах.

Основная часть

Пусть алгебраический сверточный код со скоростью кодирования $R = k_0 / n_0$ задан обобщенным порождающим многочленом, который суть порождающий многочлен (N, K) кода Рида-Соломона:

$$G(x) = (x - \alpha^b)(x - \alpha^{b+1})...(x - \alpha^{b+D-2}), \qquad (1)$$

где $\alpha^b, \alpha^{b+1}, ..., \alpha^{b+D-2}$ – корни многочлена $G(x)$, принадлежащие полю $GF(q^m)$;

b – целое число;

D – минимальное кодовое расстояние кода Рида-Соломона.

Также обобщенный многочлен сверточного кода (1) можно представить как

$$G(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + ... + \alpha_r x^r, \qquad (2)$$

где r – память сверточного кода, соответствующая числу проверочных символов в кодовом слове кода Рида-Соломона, $r = D - 1$;

$\alpha_0, \alpha_1, ..., \alpha_r$ – корни многочлена $G(x)$, принадлежащие полю $GF(q^m)$.

Тогда алгебраический сверточный код со скоростью кодирования $R = k_0 / n_0$, заданный обобщенным порождающим многочленом (2), имеет следующие параметры: длина кадра информационного слова $k_0 = \log_q(H)$ ($H \subseteq GF(q^m)$), длина кадра кодового слова $n_0 = m$, длина кодового ограничения $v = rk_0$, длина информационного слова $k = (r+1)k_0$, длина кодового слова $n = (r+1)n_0 = kn_0 / k_0$, свободное кодовое

расстояние $d_\infty \geq D$.

Пусть информационная последовательность алгебраического сверточного кода со скоростью кодирования $R = k_0 / n_0$ в полиномиальном виде имеет вид:

$$I(x) = I_0 + I_1 x + I_2 x^2 + ... + I_{K-1} x^{K-1}, \quad (3)$$

где I_i – информационные символы, $I_i \in GF(q^m)$.

Тогда кодовый многочлен рассматриваемого сверточного кода равен:

$$C(x) = I(x)G(x) = C_0 + C_1 x + C_2 x^2 + ... + C_{N-1} x^{N-1}, \quad (4)$$

где C_i – кодовые символы сверточного кода, $C_i \in GF(q^m)$.

Для разнесения во времени элементов кодового слова рассматриваемого кода на глубину перемежения M преобразуем информационный (3) и обобщенный порождающий (4) многочлены следующим образом:

$$I(x^M) = I_0 + I_1 x^M + I_2 x^{2M} + ... + I_{K-1} x^{(K-1)M};$$
$$G(x^M) = \alpha_0 + \alpha_1 x^M + \alpha_2 x^{2M} + ... + \alpha_r x^{rM}, \quad (5)$$

а затем, согласно (4), определим частичный кодовый многочлен алгебраического сверточного кода перемежения со скоростью кодирования $R = k_0 / n_0$:

$$C(x^M) = I(x^M)G(x^M) = \\ = C_0 + C_1 x^M + C_2 x^{2M} + ... + C_{N-1} x^{(N-1)M}. \quad (6)$$

Тогда кодовое слово алгебраического сверточного кода перемежения со скоростью $R = k_0 / n_0$ получается в результате применения операции (6) к M кодовым словам исходного сверточного кода, что в полиномиальной форме записи соответствует выражению:

$$C'(x) = \sum_{l=0}^{M-1} C_l(x^M) x^{lN}, \quad (7)$$

где $C_l(x^M)$ – частичные кодовые многочлены, соответствующие отдельным информационным многочленам (3).

Следует отметить, что полиномиальному представлению алгебраических сверточных кодов перемежения на основе выражений (5) – (7) однозначно соответствует матричное представление [2], в соответствии с которым двоичное кодовое слово можно представить следующим образом:

$$c' = \begin{pmatrix} c_{0,0,1},...,c_{0,0,m} & c_{0,1,1},...,c_{0,1,m} & ... & c_{0,M-1,1},...,c_{0,M-1,m} \\ c_{1,0,1},...,c_{1,0,m} & c_{1,1,1},...,c_{1,1,m} & ... & c_{1,M-1,1},...,c_{1,M-1,m} \\ ... & ... & ... & ... \\ c_{N-1,0,1},...,c_{N-1,0,m} & c_{N-1,1,1},...,c_{N-1,1,m} & ... & c_{N-1,M-1,1},...,c_{N-1,M-1,m} \end{pmatrix}, \quad (8)$$

где $c_{u,l,k}$ – кодовые символы, объединенные в кадры по $m = n_0$ символов, $c_{u,l,k} \in GF(q)$.

Следовательно, некоторое кодовое слово рассматриваемого кода перемежения получается путем объединения M кодовых слов исходного сверточного кода в матрицу размером $N \times M$ вида (8). Тогда множество таких кодовых слов образует алгебраический несистематический сверточный код перемежения со скоростью кодирования $R = k_0 / n_0$, параметры которого полностью определяются модифицированным порождающим многочленом (5): длина кадра информационного слова $k'_0 = Mk_0 = M \log_q(H)$, длина кадра кодового слова $n'_0 = Mn_0 = Mm$, скорость кодирования $R = k'_0 / n'_0 = k_0 / n_0$, память кода $r' = Mr$, длина кодового ограничения $v' = r'k'$, длина информационного слова $k' = (r'+1)k'_0$, длина кодового слова $n' = (r'+1)n'_0 = k'n'_0 / k'_0$, свободное кодовое расстояние $d_\infty \geq D$.

Для обобщения полученных результатов на случай информационного слова бесконечной длины достаточно объединить кодовые слова (8) длиной NMn_0 с элементами из поля $GF(q)$ в бесконечное кодовое слово алгебраического сверточного кода перемежения со скоростью кодирования $R = k_0 / n_0$.

Как следует из вышеизложенного, при ограниченной информационной последовательности алгебраические сверточные коды перемежения могут быть представлены как длинные двоичные блоковые

коды, которые можно задать как с помощью порождающей матрицы, так и проверочной матрицы.

Предположим, что передача информации с использованием алгебраических сверточных кодов перемежения осуществляется через канал с использованием двоичной фазовой модуляции, тогда кодовое слово (8) можно представить соответствующим биполярным кодовым словом, а принятая из канала последовательность является априорной информацией для декодера.

Рассмотрим возможность итеративного декодирования данных кодов, цель которого заключается в поиске наиболее вероятного кодового слова на основе оценки соответствующих значений апостериорной вероятности каждого кодового символа, представленных с помощью логарифмического отношения правдоподобия. Для этого предлагается использовать комбинированный подход на основе информации о надежности символов, процедуры адаптивного распространения доверия и процедур природных вычислений. Согласно данному подходу каждая итерация декодирования начинается с поиска предполагаемого кодового слова с использованием процедур природных вычислений. Если полученный вектор не является кодовым словом, то применяются процедуры адаптивного распространения доверия для обновления информации о надежности символов, которая затем используется на следующей итерации декодирования.

Ниже представлены принципы реализации данного подхода при декодировании алгебраических сверточных кодов перемежения.

Обозначим надежность каждого символа на итерации w, представленную в виде соответствующего логарифмического отношения правдоподобия, как $L^w(c_{u,l,k})$. Отметим, что первоначально надежность каждого символа инициализируется как априорная информация, принятая из канала.

На первой стадии сначала осуществляется формирование наиболее надежного базиса с использованием метода исключения Гаусса, а затем происходит поиск предполагаемого кодового слова с использованием процедур природных вычислений, которое обеспечивает минимальное значение соответствующей целевой функции. При этом основными этапами процедур природных вычислений являются инициализация популяции, миграция агентов популяции и завершение поиска. Кроме того, для повышения эффективности поиска предполагаемого кодового слова дополнительно можно применить случайное смещение для формирования различных пробных векторов. Особенности реализации данной стадии декодирования представлены в работах [5, 6].

На второй стадии в начале каждой итерации w процедуры адаптивного распространения доверия проверочная матрица кода H' преобразуется в матрицу H'^w, так что столбцы данной матрицы, соответствующие наименее надежным символам (в соответствии с информацией о надежности символов, полученной на предыдущей итерации, $L^{w-1}(c_{u,l,k})$), имеют единичный вес. Отметим, что всегда можно сформировать $n'-k'$ столбцов матрицы H', имеющих единичный вес, даже если данные $n'-k'$ символы не будут наименее надежными. Пусть $i_1, i_2, ..., i_{n'}$ обозначают индексы символов, соответствующих упорядоченным в порядке возрастания элементам $|L^w(c_{u,l,k})|$. При этом проверочная матрица преобразуется, начиная с i_1-ого столбца, и обрабатывается последовательно для каждого индекса, пока $n'-k'$ столбцов не будут иметь единичный вес. Данное преобразование увеличивает правдоподобность ошибочных символов путем перемещения ветвей в графе, который соответствует проверочной матрице. Таким образом, уменьшается вероятность того, что ошибочный символ участвует в любом цикле графа – в результате чего ограничивается распространение ошибок. Затем осуществляется итерация декодирования на основе распространения доверия с использованием полученной проверочной матрицы. Особенности реализации данной стадии декодирования представлены в работе [4].

Таким образом, w-ю итерацию предложенного метода декодирования алгебраических сверточных кодов перемежения можно представить следующим образом.

Стадия 1. Декодирование на основе процедур природных вычислений.

С использованием логарифмического отношения правдоподобия для каждого символа $L^{w-1}(c_{u,l,k})$ формируется наиболее надежный базис. Далее осуществляется поиск предполагаемого кодового слова с использованием процедур природных вычислений. Если полученный вектор является переданным кодовым словом, то процесс декодирования завершается, в противном случае осуществляется переход к стадии 2.

Стадия 2. Декодирование на основе процедур адаптивного распространения доверия.

На основе логарифмического отношения правдоподобия для каждого символа $L^{w-1}(c_{u,l,k})$ строится обновленная проверочная матрица H'^w. Затем с использованием данной матрицы и внешней

информации $L_{ext}^{w-1}(c_{u,l,k})$ формируется новая внешняя информация $L_{ext}^{w}(c_{u,l,k})$ и обновленная информация о надежности символов $L^{w}(c_{u,l,k})$, которая применяется на следующей итерации декодирования на основе процедур природных вычислений для нахождения наиболее надежного базиса.

Следовательно, предложенный подход можно рассматривать как адаптивную версию комбинированного декодирования кодов с малой плотностью проверок на четность [7]. При этом применение процедур адаптивного распространения доверия позволяет осуществлять итеративное декодирование алгебраических сверточных кодов перемежения, графы которых имеют много коротких циклов, приводящих к распространению ошибок при использовании классического метода декодирования на основе распространения доверия.

Выводы

Для увеличения достоверности передачи информации в каналах с памятью целесообразно применять алгебраические сверточные коды перемежения. Предложен комбинированный подход к итеративному декодированию данных кодов, основанный на совместном использовании процедур адаптивного распространения доверия и природных вычислений. Представлены основные принципы реализации основных этапов предложенного метода декодирования.

Литература

1. Боцул, А. В. Метод построения алгебраических сверточных кодов перемежения [Текст] / А. В. Боцул, А. С. Волков, С. И. Приходько, Н. А. Штомпель // Зб. наук. праць Укр. держ. акад. залізнич. трансп. – Харків: УкрДАЗТ, 2013. – № 136. – С. 232 – 235.
2. Боцул, А. В. Метод построения алгебраических несистематических сверточных кодов перемежения с произвольной скоростью кодирования [Текст] / А. В. Боцул, А. С. Волков, С. И. Приходько, Н. А. Штомпель // Інформаційно-керуючі системи на залізничному транспорті: наук.-техн. журнал. – Харків: УкрДАЗТ, 2014. − Вип. 2 (105). − С. 8 – 11.
3. Боцул, А. В. Метод декодирования алгебраических сверточных кодов перемежения [Текст] / А. В. Боцул, А. С. Волков, С. И. Приходько, Н. А. Штомпель // Системы обработки информации. – 2012. – Вып. 7(105). – С. 172 – 176.
4. Kothiyal, A. A comparison of adaptive belief propagation and the best graph algorithm for the decoding of linear block codes [Text] / A. Kothiyal, O. Y. Takeshita // Proceedings International Symposium on Information Theory (4 – 9 September, 2005). – 2005. – P. 724 – 728.
5. Жученко, А. С. Метод декодирования линейных блоковых кодов на основе популяционных процедур поисковой оптимизации [Текст] / А. С. Жученко, Н. Г. Панченко, С. В. Панченко, Н.А. Штомпель // Інформаційно-керуючі системи на залізничному транспорті: наук.-техн. журнал. – Харків: УкрДУЗТ, 2016. – Вип. 2 (117). – С. 25 – 29.
6. Штомпель, Н. А. Мягкое декодирование алгебраических сверточных кодов на основе природных вычислений [Текст] / Н. А. Штомпель // Інформаційно-керуючі системи на залізничному транспорті: наук.-техн. журнал. – Харків: УкрДУЗТ, 2016. – Вип. 5 (120). – С. 14 – 18.
7. Штомпель, Н. А. Комбинированный метод декодирования кодов с малой плотностью проверок на четность [Текст] / Н. А. Штомпель // Наук.-практ. конф. «Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку» (м. Харків, 12 – 13 берез. 2014 р.): зб. тез доп. – Харків: Академія внутрішніх військ МВС України, 2014. – С. 96 – 97.

Штомпель М. А. Адаптивне декодування алгебраїчних згорткових кодів перемежування. Обґрунтована доцільність застосування алгебраїчних згорткових кодів перемежування для підвищення достовірності передачі інформації у каналах з пам’яттю. Запропоновано метод ітеративного декодування даних кодів на основі комбінованого підходу з використанням процедур адаптивного розповсюдження довіри та природних обчислень. Подано основні принципи реалізації основних етапів запропонованого методу декодування.

Ключові слова: адаптивне декодування, згорткові коди, перемежування, природні обчислення.

Shtompel M. Adaptive decoding algebraic interleaved convolutional codes. For correcting burst errors in channels with memory are widely used various code constructions together with interleaving. For increasing the reliability of information transmission in such channels is advisable to apply algebraic interleaved convolutional codes. The principles of polynomial and matrix representation of algebraic interleaved convolutional codes with predetermined coding rate are given. The parameters of these codes which completely determined by the modified generator polynomial are presented. Algebraic decoding these codes has been a large computational complexity and limited correction capability. Algebraic

interleaved convolutional codes can be represented as a long binary block codes which can be determined with using generator or parity check matrix. The combination approach to iterative decoding these codes whose purpose is to find the most probable codeword by assessing a log likelihood ratio of each code symbol is proposed. The share using information about the reliability of symbols, adaptive belief propagation and natural computing procedures are offered. According to this approach each iteration of decoding starts with finding the expected codeword using natural computing procedures. If the received vector is not codeword, then adaptive belief propagation procedures are used for updating the information about the reliability of symbols which then used in the next iteration of decoding. The basic principles of implementation of the main steps of the proposed method decoding algebraic interleaving convolution codes are presented.

Keywords: adaptive decoding, convolutional codes, interleaving, natural computing.

Надійшла 28.10.2016 р.

Штомпель Микола Анатолійович, *кандидат технічних наук, доцент, доцент кафедри транспортного зв'язку, Український державний університет залізничного транспорту, Харків, Украина. E-mail: shtompel.mykola@kart.edu.ua.*

Shtompel Mykola Anatoliiovych*, Candidate of sciences (technology), Associate professor (docent), Associate professor, Department of transport communication. Ukrainian State University of Railway Transport, Kharkiv, Ukraine. E-mail: shtompel.mykola@kart.edu.ua.*