

УДК 621.391

Н.А. Штомпель

Украинская государственная академия железнодорожного транспорта, Харьков

ВЫЧИСЛИТЕЛЬНАЯ СЛОЖНОСТЬ МЕТОДОВ ДЕКОДИРОВАНИЯ КОДОВ С МАЛОЙ ПЛОТНОСТЬЮ ПРОВЕРОК НА ЧЕТНОСТЬ

Проведена оценка вычислительной сложности методов жесткого и мягкого декодирования кодов с малой плотностью проверок на четность для обоснования необходимости их адаптации к особенностям волоконно-оптических телекоммуникационных систем со спектральным разделением каналов.

Ключевые слова: *вычислительная сложность, декодирование, коды с малой плотностью проверок на четность, волоконно-оптические телекоммуникационные системы.*

Введение

Постановка проблемы и анализ литературы.
Коды с малой плотностью проверок на четность

(МППЧ-коды) были предложены Р. Галлагером в 1962 году в [1]. Несмотря на то, что характеристики данных кодов близки к идеальным, их не использовали в течение практически 30 лет из-за высокой, на

тот момент, вычислительной сложности декодирования. В [2, 3] показано, что МППЧ-коды обладают высокой эффективностью и находятся в 0,0045 дБ от предела Шеннона для случая передачи двоичных сигналов по каналу с аддитивным белым гауссовским шумом (АБГШ). Кроме высокой эффективности вблизи пропускной способности канала, МППЧ-коды обеспечивают дополнительные преимущества по сравнению с турбо-кодами: простота технической реализации с применением параллельной архитектуры, более высокое значение скорости кода, меньшее значение спада вероятности ошибки при увеличении отношения сигнал/шум (эффект «error floor»), возможность исправления пачек ошибок и т.д. Недостатками МППЧ-кодов являются сравнительно высокая вычислительная сложность кодирования, нерегулярность соединений элементов в декодере, а также более низкая эффективность, по сравнению с турбо-кодами, при коротких длинах кодовых слов.

МППЧ-коды находят применение в стандарте беспроводного доступа IEEE 802.16, стандарте передачи данных Ethernet IEEE 802.3an, стандарте спутникового цифрового телевидения DVB-S2 и др. С точки зрения внедрения в существующие и проектируемые телекоммуникационные системы дополнительным достоинством МППЧ-кодов по сравнению с турбо-кодами является отсутствие ограничений, связанных с авторскими правами [4].

Перспективным направлением применения помехоустойчивых кодов, в частности МППЧ-кодов, является повышение достоверности передаваемых данных в волоконно-оптических телекоммуникационных системах со спектральным разделением каналов (ВОТС-СРК) [5].

Целью статьи является оценка вычислительной сложности классических методов декодирования МППЧ-кодов для обоснования необходимости их адаптации к особенностям ВОТС-СРК.

Основная часть

МППЧ-кодами называются линейные блочные (N, K) коды, у которых проверочная матрица H состоит из малого числа 1 по сравнению с количеством 0, т.е. данная матрица является разреженной. Данные коды имеют следующие параметры: N – длина кодового слова, K – длина информационного слова, $M = N - K$ – число проверочных символов. Кроме того, для описания характеристик проверочной матрицы H размерности $M \times N$ этих кодов вводятся такие параметры как вес столбца J и вес строки L , равные числу ненулевых элементов в столбце и строке соответственно. При этом, т.к. матрица H является разреженной, выполняются условия $J \ll N$ и $L \ll M$.

МППЧ-код будет регулярным, если J и L являются константами для каждого столбца и каждой строки проверочной матрицы H . С другой стороны, если проверочная матрица H разреженная, но J и L не являются постоянными величинами, то МППЧ-код называется нерегулярным. Часто регулярный МППЧ-код также обозначается как (N, J, L) код.

Тогда при условии, что все строки проверочной матрицы H линейно независимы, для регулярных МППЧ-кодов выполняется равенство $ML = NJ$ и скорость кода рассчитывается по формуле

$$R = \frac{K}{N} = \frac{N - M}{N} = 1 - \frac{J}{L}. \quad (1)$$

Например, проверочная матрица регулярного $(6, 2, 3)$ МППЧ-кода имеет вид

$$H = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}, \quad (2)$$

а скорость данного кода, согласно (1), $R = 1/3$.

МППЧ-коды можно также представить графически с помощью двудольных графов, известных в теории кодирования как графы Таннера. Вершины данных графов разделяются на две группы, которые соединены между собой ребрами. Первая группа состоит из N битовых вершин, а вторая – из M проверочных вершин. Принцип построения графа Таннера состоит в следующем: проверочная вершина i соединяется с битовой вершиной j , если элемент проверочной матрицы H равен 1 ($h_{ij} = 1$), в противном случае ребро между вершинами отсутствует. Следовательно, граф Таннера регулярного (N, J, L) МППЧ-кода содержит $ML = NJ$ ребер. Очевидно, что граф Таннера однозначно соответствует проверочной матрице H , которая фактически является его матрицей инцидентности.

Например, граф Таннера $(6, 2, 3)$ МППЧ-кода, имеющего порождающую матрицу (2), представлен на рис. 1.

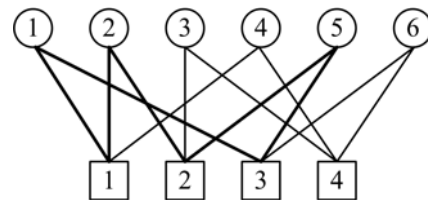


Рис. 1. Граф Таннера $(6, 2, 3)$ МППЧ-кода

Замкнутый путь, содержащий P ребер в графе Таннера, называется циклом длины P . Цикл минимальной длины в графе Таннера называется обхватом графа W . Кратчайшим возможным циклом в

графе Таннера является цикл длиной $P = 4$. Например, на рис. 1 показан один из циклов графа Таннера длиной $P = 6$, при этом обхват данного графа $W = 6$.

Для декодирования МППЧ-кодов, как и для турбо-кодов, применяют итеративный принцип с последовательным уточнением каждого символа предполагаемого кодового слова c' . С графической точки зрения, это эквивалентно итеративному обмену сообщениями между битовыми и проверочными вершинами графа Таннера. Декодирование осуществляется альтернативно в битовых вершинах и проверочных вершинах графа для нахождения наиболее похожего кодового слова c , удовлетворяющего условию $c'N^T = 0$.

Существует два классических метода декодирования МППЧ-кодов для получения жесткого и мягкого решений соответственно. Для жесткого декодирования применяется метод инвертирования бита, а для мягкого – метод суммы-произведения, также известный как алгоритм распространения доверия или алгоритм Перла.

Суть метода инвертирования бита заключается в итеративном вычислении всех проверок принятого вектора g с определением количества невыполненных проверок N_m и инвертированием бита g_j принятого вектора, который входит в наибольшее число невыполненных проверок N_m из m проверочных уравнений, представленных строками матрицы H .

Алгоритм, соответствующий данному методу декодирования МППЧ-кодов, приведен ниже.

Шаг 1. Вычислить каждую проверку m_j принятого вектора g .

Шаг 2. Для каждого принятого бита g_j определить число невыполненных проверок N_m .

Шаг 3. Инвертировать бит g_j с наибольшим числом невыполненных проверок N_m .

Шаг 4. Повторить шаги 1 – 3 до тех пор, пока все проверки m_j не будут выполняться или до достижения заданного количества итераций N_{it} . В наихудшем случае, если некоторые проверки m_j остаются невыполненными, – объявить ошибку декодирования принятого вектора g .

Из анализа этапов представленного алгоритма следует простота его технической реализации, т.к. требуется выполнение лишь операций «сложение по модулю 2» и «сравнение». При этом вычислительная сложность данного метода декодирования для заданных значений J и L растет линейно с увеличением длины кодового слова N . Для повышения эффективности жесткого декодирования МППЧ-кодов предлагаются различные модификации дан-

ного метода, например использование «взвешенного» инвертирования битов [4].

Вместо инвертирования битов метод суммы-произведения обеспечивает обмен вероятностными значениями битов g_j принятого вектора между битовыми и проверочными вершинами графа Таннера для повышения уверенности в выполнении каждой проверки m_j . Такой обмен вероятностями называется передачей сообщений или распространением доверия. Когда граф Таннера не содержит циклов, данный метод использует точные значения вероятностей, что позволяет обеспечить точное декодирование принятого вектора g . При наличии циклов возможно только приближенное решение задачи декодирования МППЧ-кодов. Алгоритм, реализующий метод декодирования суммы-произведения МППЧ-кодов для канала с АБГШ, представлен ниже.

Шаг 1. Инициализация.

Для битовой вершины j , соединенной ребром с проверочной вершиной i , установить следующие значения вероятностей:

$$P_j^1 = \frac{1}{1 + e^{2g_j/\sigma^2}}, \quad P_j^0 = 1 - P_j^1, \quad (3)$$

$$P_{ij}^1 = P_j^1, \quad P_{ij}^0 = 1 - P_{ij}^1, \quad (4)$$

где P_j^1, P_j^0 – вероятности того, что в принятом векторе g на j -й позиции находится бит «1» или «0» соответственно;

g_j – принятый бит, искаженный шумом в канале;

$$\sigma^2 = \frac{N_0}{2} \text{ – дисперсия канала с АБГШ;}$$

P_{ij}^1, P_{ij}^0 – вероятности того, что g_j имеет значение «1» или «0» на основе информации, полученной из всех проверок m , кроме проверки m_i , соответственно.

Шаг 2. Передача сообщений от проверочных вершин к битовым вершинам.

Для каждой проверочной вершины i , связанной ребром с битовой вершиной j , вычислить разницу между значениями вероятностей (4):

$$\Delta P_{ij} = P_{ij}^0 - P_{ij}^1.$$

Затем определить вспомогательную величину

$$\Delta Q_{ij} = \prod_j \Delta P_{ij'},$$

где $j' = 1, 2, \dots, N, j' \neq j$.

Рассчитать вероятности того, что проверка m_i выполняется, если g_j имеет значение «1» или «0»:

$$Q_{ij}^0 = \frac{1}{2}(1 + \Delta Q_{ij}), \quad Q_{ij}^1 = \frac{1}{2}(1 - \Delta Q_{ij}). \quad (5)$$

Шаг 3. Передача сообщений от битовых вершин к проверочным вершинам.

Для каждой битовой вершины j , соединенной ребром с проверочной вершиной i , пересчитать вероятности (4) и с учетом условия нормировки $P_{ij}^0 + P_{ij}^1 = 1$:

$$P_{ij}^0 = p_j^0 \prod_{i'} Q_{i'j}^0, \quad P_{ij}^1 = p_j^1 \prod_{i'} Q_{i'j}^1,$$

где $i' = 1, 2, \dots, M$, $i' \neq i$.

С учетом (5) и условия нормировки $P_j^0 + P_j^1 = 1$ определить апостериорные вероятности, уточняющие значения вероятностей (3):

$$P_j^0 = p_j^0 \prod_i Q_{ij}^0, \quad P_j^1 = p_j^1 \prod_i Q_{ij}^1, \quad (6)$$

где $i = 1, 2, \dots, M$.

Шаг 4. Результат декодирования.

На основе значений вероятностей, полученных в (6), определить значение каждого декодированного бита

$$c_j^i = \begin{cases} 0, & \text{если } \ln(P_j^1/P_j^0) \geq 0, \\ 1, & \text{если } \ln(P_j^1/P_j^0) < 0, \end{cases}$$

где $\ln(P_j^1/P_j^0)$ – логарифмическое отношение вероятностей (мягкие решения).

Если $c^T H^T = 0$, то выдать предполагаемое кодовое слово c' и/или вектор мягких решений C' на основе полученных значений $\ln(P_j^1/P_j^0)$, в противном случае перейти к Шагу 2. В наихудшем случае, если количество итераций N_{it} превышает заданное число, то объявить ошибку декодирования принятого вектора r .

Рассмотренный выше алгоритм декодирования обладает следующими недостатками. Во-первых, существенный динамический диапазон используемых числовых значений потенциально может привести к неустойчивости вычислений. Во-вторых, значительное число умножений в данном алгоритме представляет проблему для технической реализации. Более высокая вычислительная сложность метода суммы-произведения компенсируется увеличением эффективности декодирования, снижением требований к отношению сигнал-шум и т.д.

ОБЧИСЛЮВАЛЬНА СКЛАДНІСТЬ МЕТОДІВ ДЕКОДУВАННЯ КОДІВ З МАЛОЮ ЩІЛЬНІСТЮ ПЕРЕВІРОК НА ПАРНІСТЬ

М.А. Штомпель

Проведено оцінку обчислювальної складності методів жорсткого та м'якого декодування кодів з малою щільністю перевірок на парність для обґрунтування необхідності їх адаптації до особливостей волоконно-оптичних телекомунікаційних систем зі спектральним розділенням каналів.

Ключові слова: обчислювальна складність, декодування, коди з малою щільністю перевірок на парність, волоконно-оптичні телекомунікаційні системи.

COMPUTATIONAL COMPLEXITY OF DECODING METHODS OF LOW-DENSITY PARITY-CHECK CODES

N.A. Shtompel

The estimation of computational complexity of the hard and soft decoding methods of low-density parity-check to justify the need for their adaptation to the characteristics of fiber-optic communication systems with wavelength-division multiplexing.

Keywords: computational complexity, decoding, low-density parity-check codes, fiber-optic telecommunication systems.

Выводы

1. В ВОРС-СРК для декодирования МППЧ-кодов целесообразно использовать метод суммы-произведения, который обладает большей эффективностью по сравнению с методом инвертирования бита.

2. Необходимо осуществить уменьшение вычислительной сложности метода суммы-произведения для адаптации к высокой скорости передачи данных, характерной для ВОРС-СРК, например за счет перехода в частотную область как в [6, 7] или на основе некоторого другого подхода.

Список литературы

1. Gallager R.G. Low-density parity-check codes / R.G. Gallager // *IRE Transaction on Information Theory*. – 1962. – January. – P. 21-28.
2. MacKay D.J.C. Good error correcting codes based on very sparse matrices / D.J.C. MacKay // *IEEE Transaction on Information Theory*. – 1999. – Vol. 45, №2. – March. – P. 399-432.
3. Richardson T.J. Design of capacity-approaching irregular low-density parity check codes / T.J. Richardson, M.A. Shokrollahi, R.L. Urbanke // *IEEE Transaction on Information Theory*. – 2001. – Vol. 47, №2. – February. – P. 599-618.
4. Jiang Y. A practical guide to error-control coding using MATLAB / Y. Jiang. – Artech house, 2010. – 293 p.
5. Kumar P.V. Error-control coding techniques and applications / P. Vijay Kumar, Moe Z. Win, Hsiao-Feng Lu, Costas N. Georghiadis // *Optical fiber telecommunication IV B: Systems and impairments / edited by Ivan P. Kaminow, Tingye Li*. – Elsevier Science, 2002. – P. 902-964.
6. Штомпель М.А. Обчислювальна складність методу частотного декодування згорткових кодів [Текст] / М.А. Штомпель // *Зб. наук. праць УкрДАЗТ*. – 2010. – Вип. 116. – С. 106-110.
7. Приходько С.И. Метод декодирования алгебраических каскадных сверточных кодов в частотной области с применением быстрого преобразования Фурье [Текст] / С.И. Приходько, А.С. Волков // *Системи управління, навігації та зв'язку*. – К.: ДП «ЦНДІ НІУ», 2011. – Вип. 1(17). – С. 116-119.

Поступила в редколлегию 26.06.2013

Рецензент: д-р техн. наук, проф. С.И. Приходько, Украинская государственная академия железнодорожного транспорта, Харьков.