УДК 621.391.96

ПОВЫШЕНИЕ ИСПРАВЛЯЮЩЕЙ СПОСОБНОСТИ АЛГОРИТМА ДЕКОДИРОВАНИЯ СТИРАНИЙ С ВЫБОРОМ

А. А. Задерновский, А. А. Бондарь, О. В. Тихонова

Рассмотрены способы повышения исправляющей способности алгоритма декодирования стираний с выбором. Выявлены особенности блочного циклического кодирования, которые способствуют неверному декодированию принятых сообщений. Предложены методы, позволяющие улучшить работу алгоритма декодирования стираний с выбором. Работоспособность предложенных методов подтверждена математическим моделированием.

Ключевые слова: *помехоустойчивое кодирование, блочный код, синдром, систематическое кодирование, циклический код, код Хемминга, алгоритм декодирования стираний, алгоритм декодирования стираний с выбором, алгоритм декодирования стираний с выбором и проверкой синдрома.*

Введение

В системах цифровой связи важное место занимает помехоустойчивое кодирование. Это процесс добавления к передающимся сообщениям дополнительных кодовых битов, позволяющих контролировать и исправлять ошибки, возникающие в результате воздействия шумов. Достоинство помехоустойчивого кодирования заключается в том, что оно является программной составляющей, не требующей специфического оборудования. При необходимости заменить один алгоритм кодирования на другой достаточно перепрограммировать оборудование. Применение более совершенных методов помехоустойчивого кодирования позволяет улучшать качество системы связи без изменения аппаратной части оборудования.

Существует множество алгоритмов и форм помехоустойчивого кодирования и декодирования. К закодированному сообщению могут быть применены несколько разных алгоритмов декодирования, отличающихся исправляющей способностью. Исправляющая способность – это характеристика, показывающая, сколько ошибок в одном принятом сообщении может исправить алгоритм декодирования. В данной статье рассматривается один из способов повышения исправляющей способности алгоритма декодирования.

Код Хемминга, систематическое и несистематическое кодирование

Одним из наиболее распространенных помехоустойчивых кодов является код Хемминга. Это линейный блочный циклический код, который может использоваться в матричной или полиномиальной форме. Кодирование сообщения данным кодом может быть систематическим или несистематическим. Отличает систематическое и несистематическое кодирование способ формирования порождающей матрицы [1, 2].

Для несистематического кодирования порождающая матрица составляется следующим образом: вектор, характеризующий порождающий полином записывается в качестве первых битов первой строки матрицы, а остальные позиции заполняются нулями. Следующие строки матрицы получают путем циклического сдвига первой строки.

Рассмотрим пример построения порождающей несистематической матрицы кода Хемминга (15, 11), основанного на порождающем многочлене:

$$g(x) = x^4 + x + 1.$$

Соответствующий порождающему многочлену вектор имеет вид: [1 0 0 1 1].

Порождающая матрица для несистематического кода Хемминга:

$$\begin{bmatrix}
1&0&0&1&1&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&1&1&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&1&1&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&1&1&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&1&1&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&1&1&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&1&1&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&1&1&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&1&1&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&1&1&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&1&1
\end{bmatrix}.$$

Для систематического кодирования, которое рассматривается в статье, переход от порождающего полинома к матрице осуществляется через вычисление матрицы остатков. Матрица остатков формируется через деление полинома x^{j+n-k} на порождающий многочлен, где j – номер строки матрицы; n – количество битов в кодовом слове; k – количество информационных битов. К матрице остатков дописывается единичная матрица. Матрица для систематического кодирования кодом Хемминга (15, 11) выглядит следующим образом:

$$\begin{bmatrix} 1&0&0&0&0&0&0&0&0&0&0&1&0&0&1 \\ 0&1&0&0&0&0&0&0&0&0&0&1&1&0&1 \\ 0&0&1&0&0&0&0&0&0&0&0&1&1&1&1 \\ 0&0&0&1&0&0&0&0&0&0&0&1&1&1&0 \\ 0&0&0&0&1&0&0&0&0&0&0&0&1&1&1 \\ 0&0&0&0&0&1&0&0&0&0&0&1&0&1&0 \\ 0&0&0&0&0&0&1&0&0&0&0&0&1&0&1 \\ 0&0&0&0&0&0&0&1&0&0&0&1&0&1&1 \\ 0&0&0&0&0&0&0&0&1&0&0&1&1&0&0 \\ 0&0&0&0&0&0&0&0&0&1&0&0&1&1&0 \\ 0&0&0&0&0&0&0&0&0&0&1&0&0&1&1 \end{bmatrix}.$$

Для кодирования как систематического, так и несистематического, информационное сообщение, состоящее в рассматриваемом примере из 11-ти битов, умножается на порождающую матрицу.

При систематическом кодировании кодовое сообщение содержит в первых 11-ти битах исходные информационные биты, а в последних четырех – кодовые биты. При несистематическом кодировании исходное информационное сообщение и кодовый вектор могут сильно отличаться, кодовые и информационные биты перемешаны.

Декодирование в простейшем случае осуществляется вычислением вектора синдрома, который является результатом перемножения принятого кодового вектора на проверочную матрицу. При наличии одной ошибки синдром указывает на ее позицию, а при отсутствии ошибок вектор синдрома будет нулевым.

Проверочные матрицы составляются в соответствии с порождающими матрицами. Для систематического и несистематического кодирования существует своя проверочная матрица.

Алгоритм декодирования стираний с выбором

Синдромное декодирование Хемминга способно исправить одну и обнаружить две ошибки в принятом сообщении.

Большей помехоустойчивостью обладает алгоритм декодирования стираний, способный исправить два стертых бита в кодовом слове. Основной принцип алгоритма декодирования стираний строится на обнаружении ненадежных битов, последующем их стирании и восстановлении по свойству циклического блочного кода: сумма по модулю двух битов на позициях, соответствующих ненулевому коэффициенту проверочного многочлена, равна нулю [3].

На основе алгоритма декодирования стираний был разработан алгоритм декодирования стираний с выбором, который способен исправлять три стертых бита. Алгоритм декодирования стираний с выбором определяет три ненадежных бита и «стирает» два из них, а на позицию третьего ставит единицу, тем самым генерируя первое предполагаемое слово. Второе предполагаемое слово на позиции третьего ненадежного бита имеет ноль. Проведя стандартную операцию декодирования стираний, алгоритм декодирования стираний с выбором по евклидовой метрике определяет какое из двух предполагаемых слов ближе к принятому сообщению [3].

При относительно простой реализации алгоритм декодирования стираний с выбором обладает лучшей исправляющей способностью, чем алгоритмы Хемминга и стираний [4].

Удобство всех вышеперечисленных алгоритмов заключается в том, что все они работают с кодовым словом, полученным в результате кодирования Хемминга. Поэтому при изменении алгоритма декодирования будет меняться только программная часть приемного устройства.

При стирании четырех битов алгоритм декодирования стираний с выбором будет генерировать четыре предполагаемых слова, к которым применяется стандартный алгоритм декодирования стираний.

Проведенное математическое моделирование, использующее систематическое кодирование Хемминга, показало, что при работе с четырьмя стертыми битами алгоритм декодирования стираний с выбором резко ухудшает свою исправляющую способность. Это обусловлено тем, что при стирании четырех битов в набор предполагаемых слов могут попасть слова, являющиеся кодовыми для несистематического кодирования. Такие слова пройдут проверку проверочным многочленом, поскольку он вычисляется по порождающему полиному кода, одинаковому для систематического и несистематического кодирования. При высоком уровне помех и сильных искажениях принятого сообщения евклидова метрика может выбрать одно из таких предполагаемых слов.

Подводя промежуточный итог, можно сделать вывод, что для нормального функционирования алгоритма декодирования стираний с выбором при количестве стертых битов больше трех необходимо использовать дополнительную проверку предполагаемых слов на принадлежность к тому виду кодирования, которое используется в системе связи.

Алгоритм декодирования стираний с выбором и синдромом

В качестве дополнительной проверки в алгоритме декодирования стираний с выбором можно использовать вычисление синдрома. При этом синдром будет использоваться как индикатор, показывающий принадлежность предполагаемого слова к кодовым последовательностям исходного кода. Все предполагаемые слова с ненулевым синдромом отсеиваются как ложные и не участвуют в дальнейших проверках.

Ниже приведен пример проверки двух кодовых слов, одно из которых было получено в результате систематического, а другое – несистематического кодирования кодом Хемминга (15, 11).

Исходное информационное слово, состоящее из 11-ти битов: u = [01011010110].

Кодовое слово, полученное в результате систематического кодирования: $k_{сист}$ = [010110101101011].

Кодовое слово, полученное, в результате несистематического кодирования: $k_{несист}$ = [010101000011010].

Для демонстрации проверки кодовых слов алгоритмом декодирования стираний приведены табл. 1 и 2, в которых проверяется сумма битов на позициях ненулевых коэффициентов проверочного многочлена: $h(x) = x^{11} + x^8 + x^7 + x^5 + x^3 + x^2 + x^1 + 1$.

Проверочный многочлен вычислен по порождающему многочлену $g(x)$ и, следовательно, все кодовые комбинации, полученные в результате систематического и несистематического кодирования, основанного на данном порождающем многочлене, должны проходить проверку многочленом $h(x)$.

В табл. 1 показана проверка кодового слова систематического кода. Цветом выделены столбцы, в которых проверяется сумма битов.

В табл. 2 приведена аналогичная проверка для кодового слова несистематического кода.

Как видно из таблиц, оба кодовых слова проходят проверку полиномом $h(x)$ (всегда сумма по модулю двух битов в выделенных столбцах равна нулю). Поэтому для отделения систематических кодовых слов от несистематических используется дополнительная проверка на синдром. Синдром вычисляется по проверочной матрице, которая, в отличие от проверочного многочлена, у систематического и несистематического кода разная.

При умножении систематического кодового слова на проверочную матрицу систематического кода будет получен нулевой вектор синдрома. При умножении на эту же поверочную матрицу кодового слова несистематического кода будет получен ненулевой синдром, показывающий, что данное слово не является кодовой последовательностью для системного кода.

Таблица 1

Проверка систематического кода

Позиции битов в кодовом слове														
h_0	h_1	h_2	h_3	–	h_5	–	h_7	h_8	–	–	h_{11}	–	–	–
0	1	0	1	1	0	1	0	1	1	0	1	0	1	1
1	0	1	0	1	1	0	1	0	1	1	0	1	0	1
1	1	0	1	0	1	1	0	1	0	1	1	0	1	0
0	1	1	0	1	0	1	1	0	1	0	1	1	0	1
1	0	1	1	0	1	0	1	1	0	1	0	1	1	0
0	1	0	1	1	0	1	0	1	1	0	1	0	1	1
1	0	1	0	1	1	0	1	0	1	1	0	1	0	1
1	1	0	1	0	1	1	0	1	0	1	1	0	1	0
0	1	1	0	1	0	1	1	0	1	0	1	1	0	1
1	0	1	1	0	1	0	1	1	0	1	0	1	1	0
0	1	0	1	1	0	1	0	1	1	0	1	0	1	1
1	0	1	0	1	1	0	1	0	1	1	0	1	0	1
1	1	0	1	0	1	1	0	1	0	1	1	0	1	0
0	1	1	0	1	0	1	1	0	1	0	1	1	0	1
1	0	1	1	0	1	0	1	1	0	1	0	1	1	0
0	1	0	1	1	0	1	0	1	1	0	1	0	1	1

Таблица 2

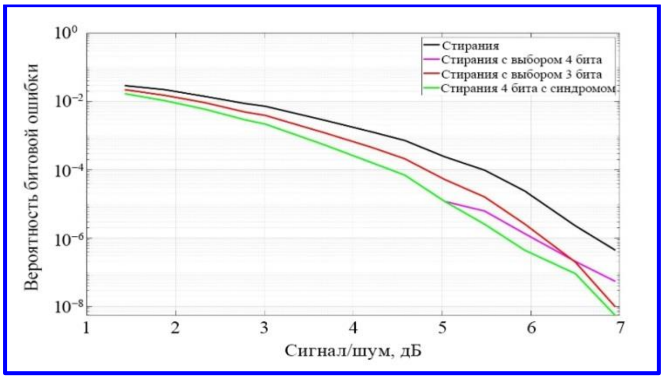
Проверка несистематического кода

Позиции битов в кодовом слове														
h_0	h_1	h_2	h_3	–	h_5	–	h_7	h_8	–	–	h_{11}	–	–	–
0	1	0	1	0	1	0	0	0	0	1	1	0	1	0
0	0	1	0	1	0	1	0	0	0	0	1	1	0	1
1	0	0	1	0	1	0	1	0	0	0	0	1	1	0
0	1	0	0	1	0	1	0	1	0	0	0	0	1	1
1	0	1	0	0	1	0	1	0	1	0	0	0	0	1
1	1	0	1	0	0	1	0	1	0	1	0	0	0	0
0	1	1	0	1	0	0	1	0	1	0	1	0	0	0
0	0	1	1	0	1	0	0	1	0	1	0	1	0	0
0	0	0	1	1	0	1	0	0	1	0	1	0	1	0
0	0	0	0	1	1	0	1	0	0	1	0	1	0	1
1	0	0	0	0	1	1	0	1	0	0	1	0	1	0
0	1	0	0	0	0	1	1	0	1	0	0	1	0	1
1	0	1	0	0	0	0	1	1	0	1	0	0	1	0
0	1	0	1	0	0	0	0	1	1	0	1	0	0	1
1	0	1	0	1	0	0	0	0	1	1	0	1	0	0
0	1	0	1	0	1	0	0	0	0	1	1	0	1	0

Введение проверки на нулевой синдром в алгоритме декодирования стираний с выбором позволяет исключить из проверки предполагаемые слова, не являющиеся кодовыми последовательностями.

Математическое моделирование

В результате математического моделирования были получены кривые помехоустойчивости для алгоритмов декодирования, рассмотренных в статье. Кривые помехоустойчивости представлены на рисунке.



Кривые помехоустойчивости алгоритмов декодирования

Из графика видно, что без проверки на нулевой синдром алгоритм, исправляющий четыре стертых бита, при отношении сигнал/шум больше 6,5 дБ, показывает худшую исправляющую способность, чем алгоритм, исправляющий три бита.

Это обусловлено тем, что при низких уровнях шумов происходит стирание битов, переданных верно. Генерируемые предполагаемые слова в этом случае будут довольно часто являться кодовыми словами несистематического кода, которые проходят проверку стираниями и, вследствие небольших искажений принятого сообщения, могут быть выбраны евклидовой метрикой как верные комбинации.

Добавление в алгоритм декодирования стираний с выбором для четырех битов синдромной проверки исключает из дальнейшей обработки ложные кодовые комбинации.

Алгоритм декодирования стираний для четырех битов с синдромной проверкой имеет преимущество при вероятности битовой ошибки в 10^{-6} перед декодированием Хемминга в 1 дБ и перед алгоритмом декодирования стираний с выбором в 0,5 дБ. При этом не происходит существенного усложнения алгоритма, поскольку вычисление синдрома является стандартной вычислительной операцией.

Заключение

При разработке новых алгоритмов помехоустойчивого декодирования с целью повысить исправляющую способность кода необходимо учитывать особенности корректирующих алгоритмов и кода, на который они опираются.

Результатом проведенной работы является создание алгоритма декодирования стираний с выбором и синдромной проверкой, обладающего лучшей исправляющей способностью, чем алгоритм декодирования стираний с выбором. Математическое моделирование подтверждает целесообразность применения разработанного алгоритма.

В дальнейшем планируется исследование алгоритма декодирования стираний с выбором и синдромной проверкой на кодах Хемминга большей длины (31, 26) и (63, 57).

Литература

1. Скляр, Б. Цифровая связь. Теоретические основы и практическое применение / Б. Скляр ; пер. с англ. – Изд. 2-е, испр. – Москва : Издательский дом «Вильямс», 2003. – 1104 с.
2. Кларк, Дж. Кодирование с исправлением ошибок в системах цифровой связи / Дж. Кларк, Дж. Кейн ; пер. с англ. – Москва : Радио и связь, 1987. – 392 с.
3. Бондарь, А. А. Исследование алгоритма декодирования стираний с выбором / А. А. Бондарь // Системы компьютерной математики и их приложения: материалы XXI Международной научной конференции. – Смоленск : Издательство СмолГУ, 2020. – Вып. 21. – С. 11–19.
4. Бондарь, А. А. Исследование различных алгоритмов декодирования стираний для повышения помехоустойчивости цифровой системы связи / А. А. Бондарь // Системы компьютерной математики и их приложения: материалы XXII Международной научной конференции. – Смоленск : Издательство СмолГУ, 2021. – Вып. 22. – С. 37–42.

Поступила в редакцию 16.04.2024

***Анатолий Андреевич Задерновский**, доктор физико-математических наук, профессор кафедры физики и технической механики, т. +7 (910) 418-37-33, e-mail: zadernovsky@mirea.ru.*
***Ольга Вадимовна Тихонова**, доктор технических наук, профессор, старший научный сотрудник кафедры РЭСК, т. +7 (916) 523-35-68, e-mail: o_tikhonova@inbox.ru.*
***Александр Александрович Бондарь**, соискатель, старший преподаватель кафедры РЭСК, т. +7 (916) 024-76-56, e-mail: alex.kvitkovsky@yandex.ru.*
(МИРЭА – Российский технологический университет).

IMPROVING THE CORRECTING ABILITY OF THE ALGORITHM DECODING ERASURES WITH A CHOICE

A. A. Zadernovsky, O. V. Tikhonova, A. A. Bondar

Methods for enhancing the error-correction capability of the erasure decoding algorithm with choice are considered. Specific features of block cyclic coding that contribute to incorrect decoding of received messages are identified. Methods are proposed to improve the performance of the erasure decoding algorithm with choice. The effectiveness of the proposed methods is confirmed through mathematical modeling.

Key words: *noise-resistant coding, block code, syndrome, systematic coding, cyclic code, Hamming code, erasure decoding algorithm, erasure decoding algorithm with choice, erasure decoding algorithm with choice and syndrome verification*

References

1. Sklar B. Digital Communications: Fundamentals and Applications / B. Sklar; trans. from English – 2nd ed., rev. – Moscow: Publishing House «Williams», 2003. – 1104 p.
2. Clark J. Error-Correction Coding for Digital Communication Systems / J. Clark, J. Cain; trans. from English. – Moscow: Radio and Communications, 1987. – 392 p.
3. Bondar A. A. Investigation of Erasure Decoding Algorithm with Selection / A. A. Bondar // Computer Mathematics Systems and Their Applications: Proceedings of the XXI International Scientific Conference. – Smolensk: Publishing House of SmolSU, 2020. – Issue 21. – P. 11–19.
4. Bondar A. A. Investigation of Various Erasure Decoding Algorithms to Improve the Noise Immunity of a Digital Communication System / A. A. Bondar // Computer Mathematics Systems and Their Applications: Proceedings of the XXII International Scientific Conference. – Smolensk: Publishing House of SmolSU, 2021. – Issue 22. – P. 37–42.

Anatoly Andreevich Zadernovsky*, Doctor of Physics and Mathematics, Professor of the Department of Physics and Technical Mechanics, t. +7 (910)418-37-33, e-mail: zadernovsky@mirea.ru.*
Olga Vadimovna Tikhonova*, Doctor of engineering, Professor, senior fellow at the Department of RSC, t. +7 (916) 523-35-68, e-mail: o_tikhonova@inbox.ru.*
Aleksandr Aleksandrovich Bondar*, applicant, Senior Lecturer at the Department of RSC, t. +7 (916) 024-76-56, e-mail: alex.kvitkovsky@yandex.ru.*
(MIREA – Russian Technological University).