УДК 621.391

АСПЕКТЫ ВЫБОРА ПОМЕХОУСТОЙЧИВОГО КОДА ДЛЯ КОНТРОЛЯ ЦЕЛОСТНОСТИ ИНФОРМАЦИИ

Г.А. Власова

Институт информационных технологий

Белорусского государственного университета информатики и радиоэлектроники,

Минск, Республика Беларусь

Аннотация. Рассмотрены задачи, возникающие при обеспечении контроля целостности информации методами помехоустойчивого кодирования. Систематизированы критерии для оценки эффективности выбора кода, контролирующего ошибки. Помимо классических критериев, к которым относятся кратность контролируемых ошибок, скорость кода, использование пошаговых либо параллельных методов обработки, предлагается рассматривать и другие параметры. Добавочные преимущества позволяет получить использование дополнительных возможностей по контролю ошибок, в том числе группирующихся, без значительного увеличения аппаратных затрат. Особенности реализации устройств обработки в интегральном исполнении либо на дискретных элементах также требуют выбора кода и алгоритма декодирования с определенными параметрами. Коды с однородной структурой и разделение ошибок на классы позволяют обеспечить высокое быстродействие и наращиваемость устройств обработки. На примере кодов Боуза-Чоудхури-Хоквингема и их модификаций показаны этапы проектирования устройств контроля ошибок в сообщениях.

Ключевые слова: целостность информации; коды, контролирующие ошибки; кратность ошибки; коды Боуза-Чоудхури-Хоквингема; модификации кодов; дополнительные корректирующие возможности; пошаговое декодирование; параллельное декодирование; аппаратная сложность; быстродействие.

ASPECTS OF SELECTING A NOISE-RESISTANT CODE FOR INFORMATION INTEGRITY CONTROL

G. A. Vlasova
Institute of Information Technologies of the Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. The tasks that arise in ensuring information integrity control by noise-resistant coding methods are considered. The criteria for evaluating the effectiveness of error control code selection are systematized. In addition to the classical criteria, which include the multiplicity of controlled errors, the code speed, the use of step-by-step or parallel processing methods, it is proposed to consider others. Using additional error control capabilities, including clustering errors, without significantly increasing hardware costs allows you to get additional advantages. The features of the implementation of processing devices in integrated design or on discrete elements also require the choice of a code and a decoding algorithm with certain parameters. Codes with a uniform structure and dividing errors into classes allow for high processing speed and extensibility of processing devices. Using the example of Bose-Chaudhuri-Hocquenghem codes and their modifications, the design stages of devices for error control in the message are shown.
Keywords: information integrity; error control codes; error order; Bose-Chaudhuri-Hocquenghem codes; codes modifications; additional error correction possibilities; step-by-step decoding; parallel decoding; hardware complexity; processing speed.

Введение

Согласно Закону Республики Беларусь «Об информации, информатизации и защите информации» под защитой информации понимается комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации. Целостность и сохранность необходимо обеспечить в условиях действия помех при передаче, обработке, распределении и хранении информации. Эффективным методом обнаружения, идентификации и коррекции ошибок в передаваемых сообщениях является помехоустойчивое кодирование. Однако задача выбора помехоустойчивого кода, алгоритма его обработки и аппаратной реализации является сложной многопараметрической задачей.

Основная часть

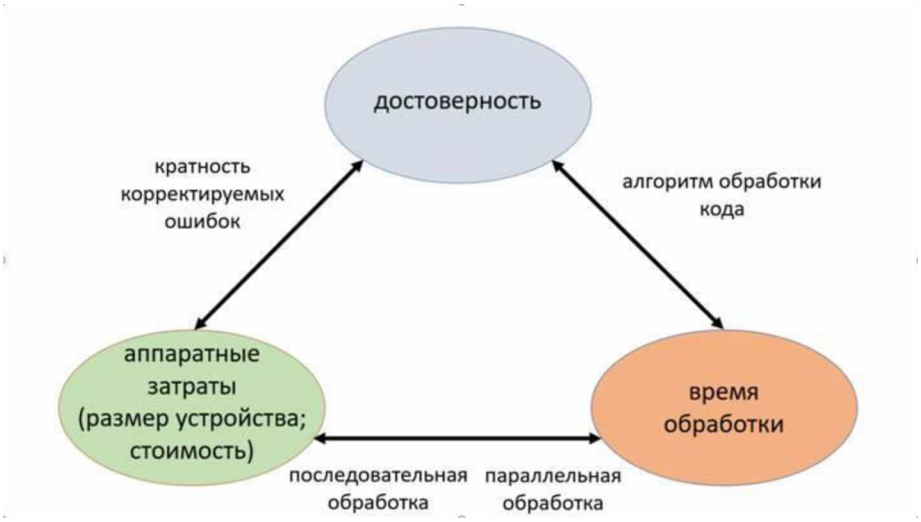
Теория и аппаратная реализация кодов, контролирующих ошибки, характеризуются тем, что разработка кодов и алгоритмов их обработки исследовались, как правило, алгебраистами; в то время как устройства проектируют инженеры [1–3]. В результате построены коды с высокими корректирующими возможностями и малой вносимой избыточностью, близкими к теоретически достижимым значениям. Однако их практическое использование ограничено сложностью устройств обработки. В то же время, коды с хорошими, но не предельно достижимыми параметрами, и приемлемыми аппаратными и временными затратами на декодирование находят широкое применение на практике [2, 3].

При проектировании устройств обработки кодов следует искать компромисс между противоречивыми задачами (см. рисунок). Так, необходимость сокращения времени обработки кода ведет к росту аппаратных затрат и, соответственно, размеров устройства и его стоимости. Увеличение требований к достоверности информации, а, следовательно, к числу контролируемых кодом ошибок, также ведет к росту затрат

на его обработку. Затраты на декодирование зависят и от выбора алгоритма обработки кода.

Рассмотрим возможную последовательность этапов выбора кода, контролирующего ошибки, с учетом требований к его практическому использованию.

Во-первых, следует оценить помеховую обстановку и определить требования к кратности обнаруживаемых, идентифицируемых и корректируемых кодом ошибок. Поскольку помехоустойчивое кодирование основано на введении в информационное сообщение избыточности, одной из основных характеристик кода является скорость R, то есть отношение числа информационных символов k к общей длине последовательности n. Возможности кода по контролю ошибок определяет кодовое расстояние d (минимальное расстояние Хемминга). Геометрически расстояние Хэмминга – это число ребер в n-мерном кубе между i-м и j-м кодовыми словами. В теории помехоустойчивого кодирования построены оценки зависимости скорости кода от кодового расстояния. Код считается хорошим, если его параметры лежат выше нижней границы Варшамова–Гильберта и ниже верхней границы Хэмминга [1]. Например, одними из лучших кодов, контролирующих независимые ошибки, являются коды Боуза-Чоудхури-Хоквингема (БЧХ) [2].



Критерии выбора помехоустойчивого кода и метода его обработки
Criteria for selecting a noise-resistant code and its processing method

Следующим этапом является оценка допустимых значений аппаратных и временных затрат на контроль ошибок. В зависимости от этих критериев выбирается параллельная (с минимальными временными затратами) либо последовательная (с минимальными аппаратными затратами) обработка [2]. В [4] рассмотрены варианты пошагового декодирования БЧХ-кодов. Показано, что известный декодер Меггитта [2] возможно использовать не только для низкоскоростных, но и для классических кодов БЧХ. Причем время декодирования при коррекции одиночных и двойных ошибок возможно уменьшить с $3n$ до $2{,}5n$ тактов, то есть увеличить быстродействие на 16 % по сравнению с известными устройствами без увеличения аппаратных затрат. В случае, когда требуется увеличить быстродействие устройства декодирования, обработка кода проводится по параллельным алгоритмам. Основной задачей при этом является минимизация сложности селектора (устройства, которое по виду синдрома принятой последовательности определяет вид ошибки). Сократить в n раз сложность селектора

для циклических кодов, к которым относятся коды БЧХ, без значительного увеличения временных затрат позволяет разделение ошибок на классы [5, 6].

В классических трудах теории помехоустойчивого кодирования рассматриваются коды, корректирующие определенный вид ошибок: независимые либо группирующиеся в модули и пакеты [1-3]. Однако проведенные исследования показали, что осуществимо расширить корректирующие возможности кодов. Так модифицированный код, полученный перестановкой в лексикографическом порядке столбцов в проверочной матрицы реверсивного БЧХ-кода, корректирующего двойные независимые ошибки, позволяет дополнительно исправлять модульные ошибки длины четыре и пакетные ошибки длины три [7]. Перестановка столбцов проверочной матрицы эквивалентна перестановке разрядов в кодовом слове и не влияет на сложность устройства. Дополнительные элементы, вводимые в устройство для коррекции группирующихся ошибок, составляют порядка 5% аппаратных затрат на коррекцию независимых ошибок [6, 8] и не влияют на быстродействие устройства. Поэтому при выборе помехоустойчивого кода необходимо исследовать его дополнительные возможности по контролю ошибок, что позволит получить конкурентные преимущества.

При проектировании следует учитывать также, будет ли устройство разрабатываться на дискретных элементах, либо в интегральном исполнении. Реализация на дискретных элементах позволяет разрабатывать оригинальные устройства с максимальным учетом требований заказчика. Кроме того, подобная реализация позволяет минимизировать не декларируемые возможности при эксплуатации [4]. Устройства в интегральном исполнении, напротив, должны быть унифицированы и иметь возможность наращивания для увеличения длины корректирумой последовательности либо кратности контролируемых ошибок. Это позволит обеспечить рентабельность производства подобных схем. Разделение ошибок на классы дает возможность проектировать устройства с регулярной однородной структурой на вентильных матрицах, быстродействие которых не зависит от длины кодового слова и кратности корректируемых ошибок [8]. Высокая скорость обработки достигается за счет уменьшения числа последовательно соединенных элементов по сравнению с известными решениями. Благодаря однородной структуре при интегральном исполнении устройство будет занимать значительно меньшую площадь кристалла. Кроме того, обеспечена возможность наращиваемости: в случае возникновения необходимости увеличения кратности исправляемых ошибок, в устройство вводятся дополнительные блоки (вентильные матрицы).

Заключение

Выбор помехоустойчивого кода для контроля целостности информации является компромиссным решением. Так увеличение скорости декодирования ведет к росту аппаратных затрат, а, следовательно, размеров и стоимости устройства обработки. Необходимость увеличения кратности корректируемых ошибок также приводит к дополнительным аппаратным и временным затратам. Для решения данной проблемы необходим комплексный системный подход. Следует оценить кратность корректируемых ошибок, допустимые аппаратные и временные затраты, особенности исполнения устройств обработки кода, а также возможности модификации кода для получения дополнительных корректирующих возможностей.

Список использованных источников

1. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. (1979) *Теория кодов, исправляющих ошибки.* Москва, Издательство «Связь».

2. Блейхут Р. (1986) *Теория и практика кодов, контролирующих ошибки.* Москва, Издательство «Мир».

3. Морелос-Сарагоса Р. (2005) *Искусство помехоустойчивого кодирования: методы, алгоритмы, применение.* Москва, Издательство «Техносфера».

4. Власова Г. А. (2022) Устройства пошагового декодирования кодов Боуза-Чоудхури-Хоквингема. *Восьмой Белорусский космический конгресс.* Том 1, 141–144.

5. Власова Г. А. (2024) Проектирование устройств обработки модификаций кодов Боуза-Чоудхури-Хоквингема на основе разделения ошибок на классы. *Компьютерное проектирование в электронике.* 60–62.

6. Власова Г. А. (2021) Устройство декодирования реверсивных кодов Боуза-Чоудхури-Хоквингема с дополнительными корректирующими возможностями для контроля целостности информации. *Комплексная защита информации.* 240-242.

7. Липницкий В. А., Конопелько В. К., Власова Г. А., Осипов А. Н., (2000) Двоичные реверсивные коды для контроля байтовых ошибок. *Известия национальной академии наук Беларуси. Серия физико-математических наук.* (1), 127-131.

8. Власова Г. А., Конопелько В. К. (1998) Параллельное декодирование БЧХ-кодов с идентификацией ошибок. *Цифровая обработка сигналов и ее применения.* Том II, II-75–II-78.

References

1. Mac Williams E. J., Sloane N. J. A. (1979) *The Theory of Error-Correcting Codes.* Moscow, Svyaz Publishing House (in Russian).

2. Blahut R. E. (1986) *Theory and Practice of Error Contril Codes.* Moscow, Tekhnosfera Publishing House (in Russian).

3. Morelos-Zaragoza R. (2005) *The Art of Error Correcting Coding.* Moscow, Mir Publishing House (in Russian).

4. Vlasova G. A. (2022) Devices for step-by-step decoding of Bose-Chaudhuri- Hocquenghem codes. *The eighth Belarusian Space Congress.* Vol 1, 141–144 (in Russian).

5. Vlasova G. A. (2024) Design of devices for processing Bose-Chaudhuri- Hocquenghem codes modifications based on dividing errors into classes. *Electronic Design Automation.* 60–62 (in Russian).

6. Vlasova G. A. (2021) A Device for Decoding Reverse Bose-Chaudhuri- Hocquenghem codes with Additional Correction Capabilities for Information Integrity Control. *Comprehensive Information Protection.* 240-242 (in Russian).

7. Lipnitsky V. A., Konopelko V. K., Vlasova G. A., Osipov A. N. Binary Reverse Codes for Byte Error Control. *Proceedings of the National Academy of Sciences of Belarus.* (1), 127-131 (in Russian).

8. Vlasova G. A., Konopelko V. K. (1998) Decoding of BCH Codes with Error Identification. *Digital signal processing and its applications.* Vol. II-E, II-E-55–II-E-58.

Сведения об авторе

Власова Г.А., канд. техн. наук, доц., доцент кафедры информационных систем и технологий, Институт информационных технологий Белорусского государственного университета информатики и радиоэлектроники, g.vlasova@bsuir.by.

Information about the author

Vlasova G.A., Cand. Sci. (Tech.). Associate Professor. Associate Professor of the Department of Information Systems and Technologies. Institute of Information Technologies of the Educational Institution "Belarusian State University of Informatics and Radioelectronics", g.vlasova@bsuir.by.