УДК 004.056.55

Филатов В.И.,
кандидат технических наук (ктн), доцент кафедры МГТУ им. Н.Э. Баумана факультета «Информатика и системы управления», кафедры «Защита информации»,
Россия, 105005, г. Москва
Борукаева А.О.,
студент МГТУ им. Н.Э. Баумана факультета «Информатика и системы управления», кафедры «Защита информации»,
сотрудник регионального учебно-научного центра «Безопасность» МГТУ им. Н.Э. Баумана,
Россия, 105005, г. Москва
Бердиков П.Г.,
студент МГТУ им. Н.Э. Баумана факультета «Информатика и системы управления»,
кафедры «Защита информации»,
Россия, 105005, г. Москва

ПРОЦЕССЫ КОДИРОВАНИЯ И ДЕКОДИРОВАНИЯ ПРИ ПЕРЕДАЧЕ ДИСКРЕТНЫХ СООБЩЕНИЙ

Аннотация: *Статья посвящена тому, что помехоустойчивое кодирование является одной из главных задач и целей современных систем хранения и передачи информации. Существует большое количество кодов, которые исправляют ошибки, примером таких кодов является код Рида-Соломона. Не менее важным кодом в сфере передачи информации является код Хэмминга [1,2,3]. В данной статье мы рассмотрим, как функционирует код Рида-Соломона, а также предоставим в результате практического применения, сравнение с уже всем так хорошо известным кодом Хэмминга.*

***Ключевые слова**: код Рида-Соломона, код Хэмминга, кодирование, декодирование, алгоритм, полином, матрица.*

***Annotation**: Noiseless coding is one of the main goals and objectives of today's storage and transmission systems. There are a large number of codes which correct errors, an example of such codes is the Reed–Solomon codes. No less important source in the field of information transfer is Hamming code [1,2,3]. In this article we will look at how the Reed-Solomon codes, and give as a result of practical application, a comparison with the already well-known to all as a Hamming code. Clearly demonstrate that the valuable property of cyclic codes is that they have the largest possible minimum distance.*

***Key words:** Reed-Solomon code, Hamming code, encoding, decoding, algorithm, polynomial, matrix.*

Кодирование-Декодирование при передаче дискретных сообщений кодом Рида-Соломона

Цель работы: изучение способов задания, оценки конкретных свойств, принципа построения и работы кодирующих и декодирующих устройств кодов Рида-Соломона (РС).

Теоретическая часть

В кодах Рида-Соломона сообщение представляется в виде набора символов некоторого алфавита. В качестве алфавита используется поле Галуа.

При построении кода Рида-Соломона задаётся пара чисел N, K, где N – общее количество символов, а K – «полезное» количество символов, остальные N-K символов представляют собой избыточный код, предназначенный для восстановления ошибок [4].

«Расстояние Хэмминга» D = N – K +1. Расстояние Хэмминга является параметром кода и определяется как минимальное число различий между двумя различными кодовыми словами. В соответствии с теорией кодирования, код,

имеющий расстояние Хемминга D = 2t+1, позволяет восстанавливать t=(N-K)/**2** ошибок.

Сообщения при кодировании Рида-Соломона представляются полиномами. Исходное сообщение представляется как коэффициенты полинома p(x) степени K-1, имеющего K коэффициентов. Порождающий многочлен Рида-Соломона, g(x):

$$g(x) = \Pi_{(i=1)}^{(D-1)}(x + a^i) = (x + a^1)(x + a^2)...(x + a^{(D-1)})$$

здесь a – это примитивный член (из поля Галуа).

Кодирование с помощью кода РС может быть реализовано двумя способами: систематическим и несистематическим.

Представим исходное информационное слово как информационный полином p(x) степени k − 1, а кодовое слово кода РС в виде полинома s(x) степени n – 1 (порождающий многочлен).

В случае несистематического кодирования кодовое слово находится из соотношения: s(x) = p(x)g(x)

где g(x) — порождающий многочлен кода РС.

Данный алгоритм реализуется кодирующим устройством, которое показано на рисунке ниже [5]. Данное устройство представляет из себя обычную схему перемножения двух многочленов. При этом результирующая кодовая комбинация не содержит в явном виде исходных информационных элементов.

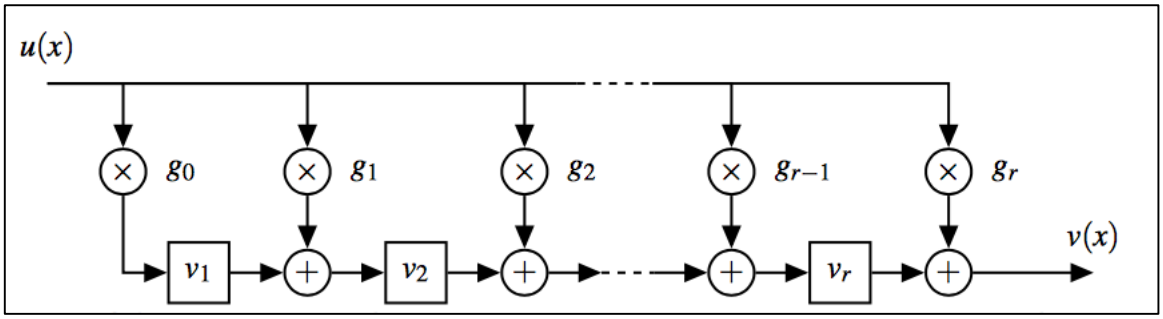

Рисунок 1. Блок-схема кодирующего устройства несистематического кода РС

При *систематическом* кодировании используется следующий алгоритм:

1. Осуществляется сдвиг информационного полиному u(x) в крайние старшие k разрядов кодового слова путем умножения полинома u(x) на x^(n-k)

2. Полученный полином u(x)*x^(n-k) делится на порождающий многочлен g(x) для получения остатка от деления r(x)

3. Искомое кодовое слово v(x) определяется как v(x)= u(x)* x^(n-k)+ r(x)

На рисунке приведена схема, реализующая вышеприведённый алгоритм кодирования. При использовании данного метода, результирующее кодовое слово содержит в явном виде исходные информационные элементы [6-9].

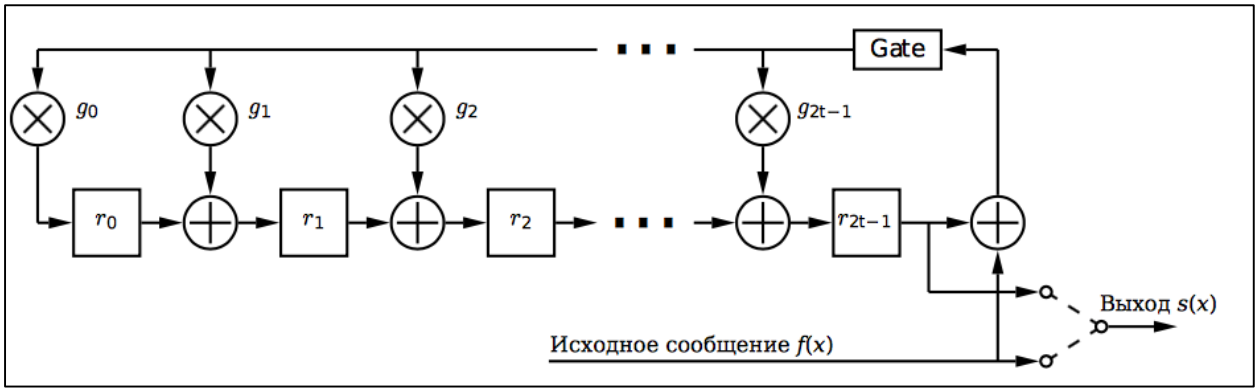

Рисунок 2. Блок-схема кодирующего устройства систематического кода РС

Способы декодирования кодов РС достаточно хорошо проработаны в теоретическом и реализационном плане, но, тем не менее, представляют собой довольно сложную задачу. Типовая схема декодирования, получившая название авторегрессионого спектрального метода декодирования, состоит из следующих шагов:

– вычисления синдрома ошибки (синдромный декодер);

– построения полинома локаторов ошибок, осуществляемого либо посредством высокоэффективного, но сложно реализуемого алгоритма Берлекэмпа – Месси (БМА), либо посредством простого, но медленного алгоритма Евклида (метод НОК);

– нахождения корней данного полинома, обычно решающегося полным перебором всех возможных значений (алгоритм Ченя);

– определения характера ошибки, сводящегося к построению битовой маски, вычисляемой на основе обращения алгоритма Форни или любого другого алгоритма обращения матрицы;

– исправления ошибочных символов путем наложения битовой маски на информационное слово и последовательного инвертирования всех искаженных бит с помощью операции XOR [10-11].

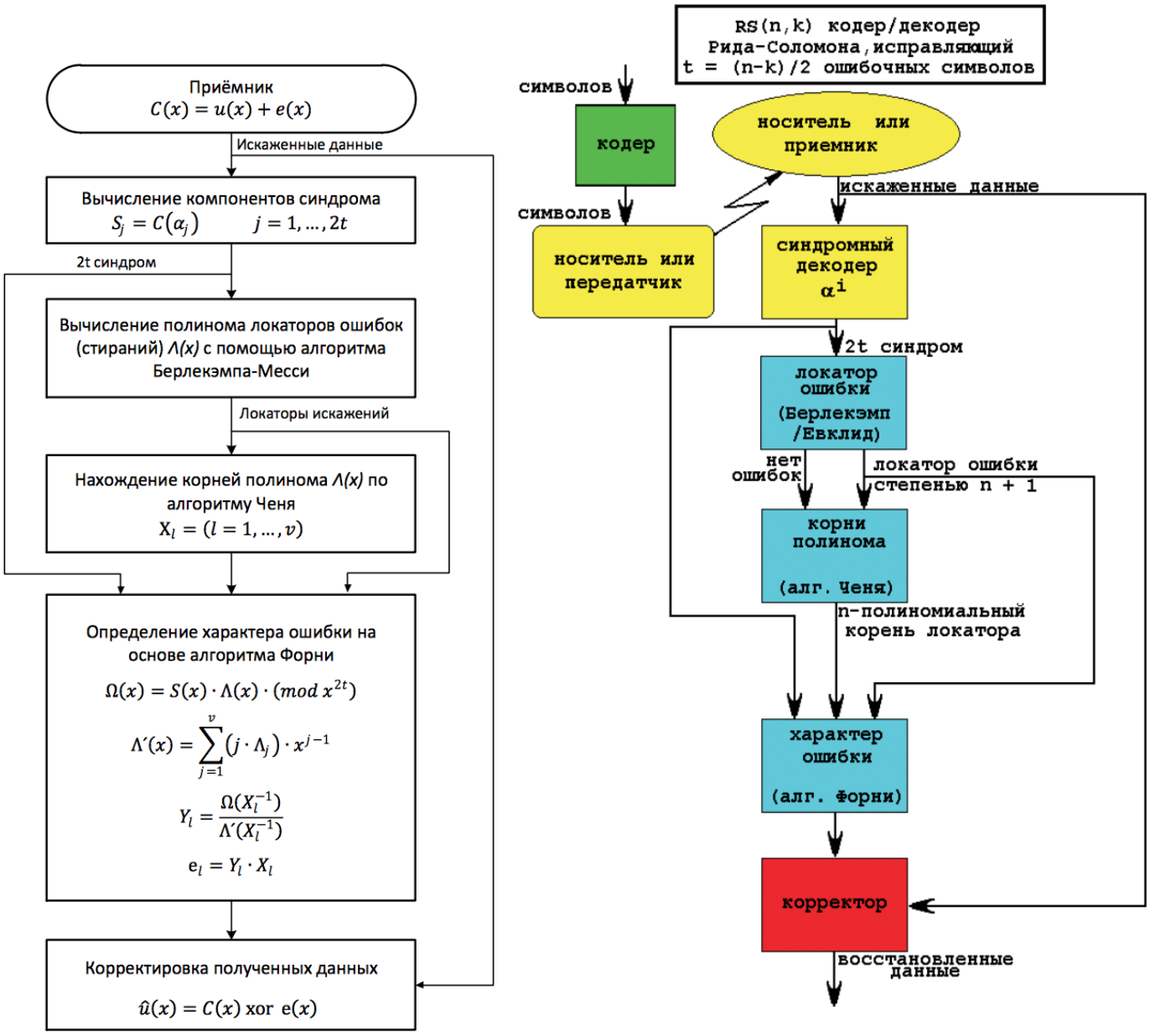

Рисунок 3. Алгоритмы быстрого детектирования кодов РС

Алгебраический подход (Рисунок 4, 5, 6, 7, 8, 9):

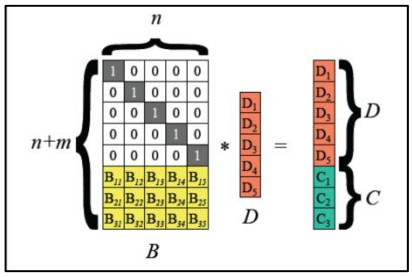

Рисунок 4. Шаг 1

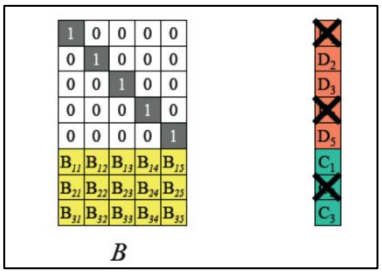

Рисунок 5. Шаг 2

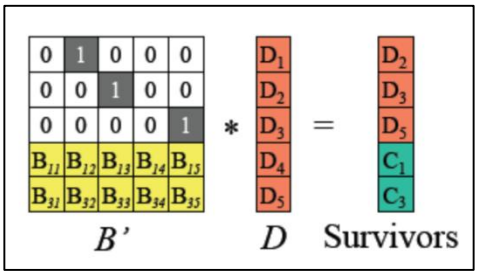

Рисунок 6. Шаг 3

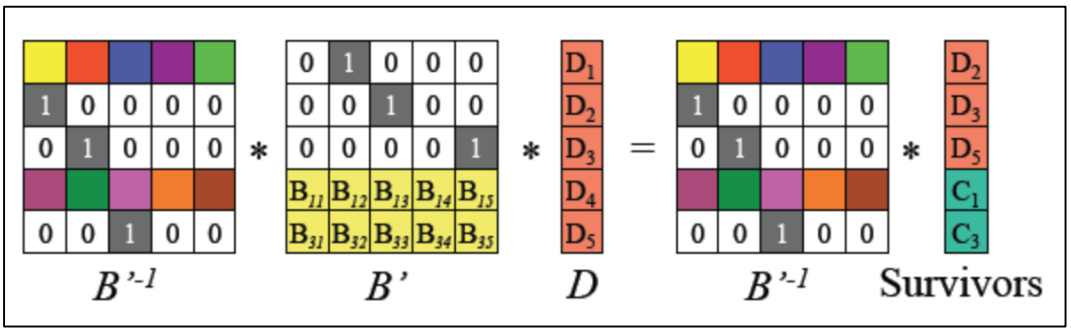

Рисунок 7. Шаг 4

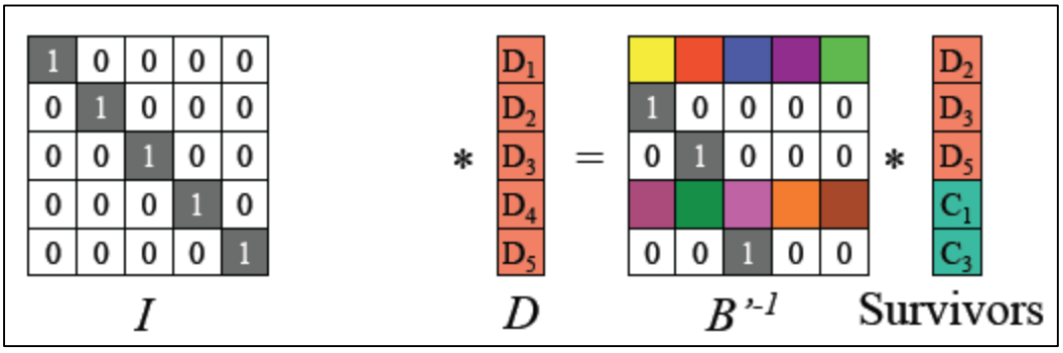

Рисунок 8. Шаг 5

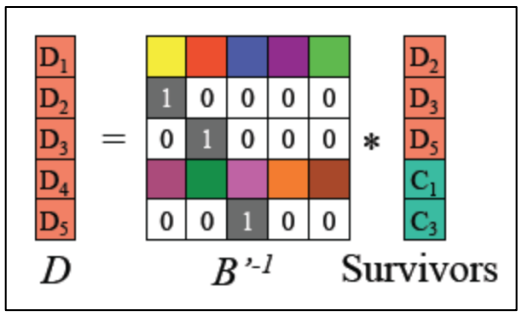

Рисунок 9. Шаг 6

Составляется матрица специального вида размера 8×5. Первые пять строк этой матрицы образуют единичную матрицу, а последние три — это некоторые числа — порождающая матрица. Умножим сконструированную матрицу на вектор, составленный из исходных чисел D_1- D_5. В результате умножения матрицы на вектор с данными получаем три «избыточных» числа. Давайте посмотрим, как с помощью этих «избыточных» данных можно восстановить, к примеру, потерянные D_1, D_4, C_2. Вычеркнем из порождающей матрицы строки, соответствующие «пропавшим» данным. В нашем случае соответствует первой, четвертой и шестой строке. Полученную матрицу умножим на вектор с данными (шаг 3). Вычеркнем соответствующие строки из порождающей матрицы и найдём обратную к ней, домножим левую и правую части исходного уравнения на эту обратную матрицу (шаг 4).

Сокращая матрицы в левой части уравнения (произведение обратной и прямой матриц есть единичная матрица), и учитывая тот факт, что в правой части уравнения нет неизвестных параметров, получаем выражения для искомых D_1, D_4 (шаг 6).

Это основа всех типов кодов Рида-Соломона, применяемых в системах хранения данных.

Процесс кодирования заключается в нахождении «избыточных» данных C_1- C_3, а процесс декодирования — в нахождении обратной матрицы и умножения её на вектор «сохранившихся» данных.

Нетрудно заметить, что рассмотренная схема может быть обобщена на произвольное количество «исходных» и «избыточных» данных. Другими словами, по исходным N числам можно построить K избыточных, причем всегда возможно восстановить потерю любых K из N+K чисел. В этом случае порождающая матрица будет иметь размер (N+K)×N, а верхняя часть матрицы размером N×N будет единичной.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Борисов В.И., Зинчук В.М., Лимарев А.Е. и др. Системы радиосвязи с

расширением спектра сигналов. // Теория и техника радиосвязи. 1998, вып. 1, с 18-48.

2. Куприянов А.И. Радиосигналы и радиоустройства в информационных системах. М: Вузовская книга, 2014. 376 с.

3. Куприянов А.И., Сахаров А.В. Теоретические основы радиоэлектронной борьбы: Учебное пособие. М.: Вузовская книга, 2007. - 356 с.

4. Дмитриев Е.А., Танаев И.В., Швейкин В.В. [и др.] помехоустойчивое кодирование. КОД РИДА – СОЛОМОНА // Научное сообщество студентов XXI столетия. ТЕХНИЧЕСКИЕ НАУКИ: сб. ст. по мат. XLIII междунар. студ. науч.-практ. конф. № 6(42).

5. Тузов Г.И., Козлов М.Р. Помехозащищенность систем связи, использующих сигналы с псевдослучайной перестройки рабочей частоты. // Зарубежная радиоэлектроника. 1983.- № 3. с.19-32.

6. Гриссер Х., Сидоренко В. Апостериорно-вероятностное декодирование несистематических блоковых кодов // Проблемы передачи информации. — 2002. — Т. 38, № 3. — С. 20–33.

7. Torrieri D.J. Fundamental Limitations on Repeater Jamming of Frequency - Hopping Communications // IEEE Journal on Selected Areas in Commun. 1989. May.- V.7, № 4, P 569-575.