

УДК 621.391

ИСПРАВЛЕНИЕ И ОБНАРУЖЕНИЕ ОШИБОК КОДОМ РИДА–СОЛОМОНА НА ОСНОВЕ СПЕКТРАЛЬНОГО ОПИСАНИЯ

В. А. Вершинин

**Рыбинский государственный авиационный технический университет
им. П. А. Соловьева, 152934, г. Рыбинск Ярославской обл., ул. Пушкина, 53**

Статья поступила в редакцию 15 января 2017 г., после доработки - 27 января 2017 г.

Аннотация. В статье рассматривается спектральное описание кода Рида – Соломона. Предлагается кодирование для исправления ошибок и обнаружения ошибок, когда число ошибок в кодовом слове больше числа гарантированно исправляемых ошибок. Для этого проверочные элементы делятся на две группы. Первая группа используется для исправления ошибок, а вторая (вместе с первой) – для обнаружения неисправимых ошибок. Получена оценка вероятности необнаруженной ошибки. Моделирование процесса декодирования подтверждает правильность полученной оценки. Если число ошибок в кодовом слове больше числа гарантированно исправляемых ошибок, то при увеличении длины кодового слова и неизменном числе элементов второй группы можно получить приемлемое значение вероятности необнаруженной ошибки.

Ключевые слова: спектральное описание, исправление и обнаружение ошибок, код Рида – Соломона.

Abstract. The article discusses the spectral description of the Reed – Solomon code. The encoding for error correction and error detection is proposed for the case, when the number of errors in the code word is greater than the number of guaranteed correctable errors. To do this, test items are divided into two groups. The first group is used for error correction, and the second (with the first) – for the detection of uncorrectable errors. The resulting estimate of the probability of undetected error is obtained. Simulation of the decoding process confirms the correctness of the assessment. If the number of errors in the code word is greater than the number of guaranteed correctable errors, it is possible to obtain an acceptable value of probab-

ity of undetected value in the case when the length of the code words increases and the value of the code distance is constant.

Key words: spectral description, correction and error detection, Reed – Solomon code.

1. Введение

Спектральное описание кода Рида – Соломона основано [1] на дискретном преобразовании Фурье (ДПФ).

Блоку элементов сообщения длиной k соответствует вектор $a = (a_0 a_1 \dots a_{n-1})$, у которого $n - k$ последовательных элементов являются нулевыми и называются проверочными, а остальные k равны элементам сообщения и называются информационными. Число проверочных элементов выбирается четным. Кодовый вектор $c = (c_0 c_1 \dots c_{n-1})$ получается [2] с помощью матрицы F_n^{-1} обратного ДПФ:

$$c = aF_n^{-1}. \quad (1)$$

Элементы сообщения и вектора c могут принимать значения $0, 1, 2, \dots, n$. Такой код называется кодом Рида – Соломона, его кодовое расстояние $d = n - k + 1$. Если все проверочные элементы используются для исправления ошибок, то код позволяет исправлять $(d - 1)/2 = (n - k)/2$ ошибок.

2. Декодирование с исправлением и обнаружением ошибок

Пусть кодовому слову на входе декодера соответствует вектор

$$c' = c + e, \quad (2)$$

где e – вектор ошибок. Этот вектор связан с наличием помех в канале связи. Если в результате действия помех искажаются элементы кодового слова, то соответствующие элементы вектора ошибок принимают значение $1, 2, \dots, n$. Неискаженным элементам кодового слова соответствуют нулевые элементы вектора ошибок. В декодере осуществляется прямое ДПФ вектора c' , в результате

получается вектор $a' = c'F_n$. Здесь F_n – матрица прямого ДПФ [2], причем $F_n^{-1}F_n = 1$. Учитывая (1) и (2),

$$a' = (c + e)F_n = (aF_n^{-1} + e)F_n = aF_n^{-1}F_n + eF_n = a + f, \quad (3)$$

где $f = eF_n$ – вектор, определяющий искажение вектора a' относительно a . Очевидно, что при отсутствии ошибок $e = 0$ и $a' = a$. Поскольку проверочные элементы вектора a равны нулю, согласно (3) соответствующие элементы вектора a' равны элементам вектора f . Таким образом, можно считать известными элементы вектора f с номерами равными номерам проверочных элементов. Остальные элементы вектора f неизвестны, их требуется определить при помощи алгоритма декодирования. Затем, вычитая f из a' , можно определить исходный вектор a . Сущность спектрального метода декодирования [1], если все проверочные элементы используются для исправления ошибок, заключается в следующем. Вводится так называемый вектор локаторов ошибок λ . Элементы этого вектора с номерами, равными номерам ненулевых элементов вектора e , равны нулю, остальные отличны от нуля. Таким образом, $\lambda e = 0$. Тогда i -й элемент вектора, полученного прямым ДПФ вектора λe , равен $\sum_{j=0}^{n-1} \Lambda_j f_{[i-j]} = 0$, где

Λ_j – элемент вектора Λ , являющегося прямым ДПФ вектора λ ; индекс в квадратных скобках вычисляется по модулю n . Если число ошибок не превышает $(d-1)/2 = (n-k)/2$, то существует вектор локаторов ошибок, для которого $\Lambda_0 = 1$ и $\Lambda_j = 0$ при $j > (n-k)/2$. Учитывая это, приведенные выше уравнения можно записать в виде

$$f_i = - \sum_{j=1}^{(n-k)/2} \Lambda_j f_{[i-j]}. \quad (4)$$

Эти n уравнений включают первую систему из $(n-k)/2$ уравнений ($i = (n-k)/2, (n-k)/2 + 1, (n-k)/2 + 2, \dots, n-k-1$), содержащих $(n-k)/2$ неизвестных элементов вектора Λ и $n-k$ известных элементов вектора f , и вторую систему из k уравнений ($i = n-k, n-k+1, n-k+2, \dots, n-1$), содержащих те же

$(n - k)/2$ неизвестных элементов вектора Λ и k неизвестных элементов вектора f . Таким образом, из первой системы уравнений можно определить неизвестные элементы вектора Λ , затем из второй системы уравнений определяются неизвестные элементы вектора f .

Для декодирования с исправлением и обнаружением ошибок автором предлагается проверочные элементы вектора a разделить на две группы с числом элементов v и w , $w \leq v$. Первая группа используется для исправления ошибок, если их число не больше $v/2$, а вторая (вместе с первой) – для обнаружения неисправимых ошибок. Значение v и w выбирается четным. Таким образом, $n - k = v + w$. Соответственно на две группы разделятся известные элементы вектора f : $f_0, f_1, \dots, f_{v-1}$ и $f_w, f_{w+1}, \dots, f_{v+w-1}$.

Предлагаемый алгоритм декодирования реализуется следующим образом.

1. Осуществляется прямое ДПФ (3), в результате определяются известные элементы вектора f : $f_0, f_1, \dots, f_{v+w-1}$. Если все эти элементы равны нулю, принимается решение об отсутствии ошибок. Это решение может быть ошибочным.

2. Считая известными только элементы $f_0, f_1, \dots, f_{v-1}$, а остальные – неизвестными, формула (4) записывается в виде $f_i = -\sum_{j=1}^{v/2} \Lambda_j f_{[i-j]}$. Отсюда получаем первую систему при $i = v/2, v/2 + 1, v/2 + 2, \dots, v - 1$ и вторую при $i = v, v + 1, v + 2, \dots, n - 1$. В первую систему входит $v/2$ неизвестных элементов вектора Λ и v известных элементов вектора f . Во вторую – те же $v/2$ неизвестных элементов вектора Λ и $n - v/2$ неизвестных элементов вектора f . Заметим, что элементы вектора f с номерами $i = v, v + 1, v + 2, \dots, v + w - 1$ входят как неизвестные во вторую систему. Обозначим их $f'_v, f'_{v+1}, \dots, f'_{v+w-1}$.

Если определитель первой системы уравнений равен нулю, то обнаруживается неисправляемое число ошибок.

3. Если определитель первой системы уравнений не равен нулю, то из первой системы уравнений определяются неизвестные элементы вектора Λ , затем из второй системы уравнений определяются неизвестные элементы вектора f , в том числе $f'_v, f'_{v+1}, \dots, f'_{v+w-1}$.

Если хотя бы один из элементов $f_v, f_{v+1}, \dots, f_{v+w-1}$ не равен соответственно $f'_v, f'_{v+1}, \dots, f'_{v+w-1}$, то обнаруживается неисправляемое число ошибок. При равенстве соответствующих элементов принимается решение, что ошибки можно исправить. Для этого вычитается f из a' и определяется исходный вектор a . Это решение может быть ошибочным.

Предлагаемый алгоритм позволяет: исправлять не более $v/2$ ошибок; обнаруживать все неисправимые ошибки, если их число не превышает $d - 3$ (установлено экспериментально); с определенной вероятностью обнаруживать ошибки, число которых превышает $d - 3$.

3. Вероятность необнаруженных ошибок

Будем оценивать вероятность необнаруженных ошибок при фиксированном числе r ненулевых элементов вектора ошибок. При этом предполагается, что все возможные варианты размещения ненулевых элементов равновероятны и каждый из этих элементов с равной вероятностью принимает значение $1, 2, \dots, n$.

В таблице 1 показаны результаты моделирования при использовании (15,7) кода Рида – Соломона с $d = 9$ при $w = v = 4$. Такой код может исправлять ошибки, если $r \leq 2$; обнаруживать все неисправимые ошибки, если $r \leq 6$; с определенной вероятностью обнаруживать ошибки, если $r > 6$. Было проведено 10^7 испытаний с использованием пакета Matlab. Определялось число необнаруженных ошибок N_1 при выполнении п.1 алгоритма и число необнаруженных ошибок N_3 при выполнении п. 3 алгоритма. Заметим, что нулевые значения N_1 при $r > 8$ связаны с малой вероятностью необнаруженных ошибок при выполнении п. 1.

Таблица 1

r	2	3	4	5	6	7	8	9	10	11	12	13	14	15
N_1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
N_3	0	0	0	0	0	20	15	18	10	15	11	12	17	23

Оценка сверху вероятности необнаруженных ошибок при выполнении п. 1 алгоритма [2] $P_1 = 1/n^{v+w}$. Будем предполагать, что при выполнении п. 3 различные комбинаций элементов $f'_v, f'_{v+1}, \dots, f'_{v+w-1}$ и элементов $f_v, f_{v+1}, \dots, f_{v+w-1}$ независимы и равновероятны, число комбинаций $(n+1)^w$, вероятность комбинации $1/(n+1)^w$. Тогда вероятность совпадения комбинаций (вероятность необнаруженных ошибок при выполнении п. 3) $P_3 = (1/(n+1)^w)(1/(n+1)^w)(n+1)^w = 1/(n+1)^w$

Очевидно, что вероятность необнаруженных ошибок при предлагаемом алгоритме декодирования $P = P_1 + P_3$. Значения P , полученные для некоторых кодов Рида – Соломона помещены в таблице 2.

Таблица 2

Код (n,k)	(15,7)	(63,55)	(255,247)	(255,231)
v,w	4,4	4,4	4,4	20,4
P	$1.52 \cdot 10^{-5}$	$5.96 \cdot 10^{-8}$	$2.33 \cdot 10^{-10}$	$2.33 \cdot 10^{-10}$

4. Выводы

Если число ошибок в кодовом слове больше числа гарантированно исправляемых ошибок, то при увеличении длины кодового слова n и неизменном v можно получить приемлемое значение вероятности необнаруженной ошибки.

При неизменной длине кодового слова n вероятность необнаруженных ошибок практически зависит только от v .

Литература

1. Блейхут Р. Теория и практика кодов, контролирующих ошибки. Пер. с англ.– М.: Мир, 1986.– 576 с.
2. В. А. Вершинин. Обнаружение ошибок кодом Рида – Соломона на основе спектрального описания. // Журнал радиоэлектроники: электронный журнал. 2016. N11. URL: <http://jre.cplire.ru/jre/nov16/16/text.pdf>

Ссылка на статью:

Исправление и обнаружение ошибок кодом Рида–Соломона на основе спектрального описания. В.А.Вершинин. Журнал радиоэлектроники [электронный журнал]. 2017. №1. Режим доступа: <http://jre.cplire.ru/jre/jan17/13/text.pdf>