DOI: 10.18372/2410-7840.20.13071
УДК 621.396.67

КОДИРОВАНИЕ И ДЕКОДИРОВАНИЕ СИСТЕМАТИЧЕСКИХ КОДОВ РИДА-СОЛОМОНА ПО МЕТОДУ, АЛЬТЕРНАТИВНОМУ АЛГОРИТМУ ПИТЕРСОНА-ГОРЕНСТЕЙНА-ЦИРЛЕРА

Анатолий Белецкий

Коды Рида-Соломона являются эффективными и широко применяемыми во многих областях науки и техники, связанными с помехоустойчивым преобразованием (приёма-передачей) цифровой информации. С момента появления и до настоящего времени описание РС-кодов, включая синтез кодовых слов, локализацию и устранение ошибок, базируется на использовании формальных элементов, которыми являются корни генераторных, информационных и проверочных полиномов. Перегруженность технологических операций алгебраическими элементами является в определенной мере «балластом», не только усложняющим процесс вычислений в аппаратно-программной реализации, но и создающим определенные затруднения при изучении алгоритмов РС-кодирования и декодирования. В связи с этим в работе предложен вариант построения РС-кодов, значительно упрощающий как освоение самого алгоритма, так и алгебраические преобразования, выполняемые при обнаружении и устранении ошибок в искаженных данных. Предложения основаны на переносе преобразований из пространства оригиналов в пространство изоморфного изображения. В результате предлагаемой замены вычислительный процесс оказывается сведенным к простым операциям модулярной арифметики над целочисленными операндами, легко реализуемыми средствами компьютерной техники.

Ключевые слова: *коды Рида-Соломона, поля Галуа, образующие полиномы, матрицы проверочных символов, изоморфные преобразования..*

1. Введение и постановка задачи

Коды Рида-Соломона (РС-коды) заслуженно располагаются на вершине пирамиды линейных блочных помехоустойчивых кодов и превосходят большинство современных кодов по одному из важнейших критериев эффективности – относительной скорости кода, под которой понимают отношение числа информационных символов k к длине кода n. $(n,k,t)-$коды Рида – Соломона это недвоичные циклические коды, исправляющие ошибки кратности t в $(n,k)-$блоках данных [1-3]. Элементами кодовых слов являются не биты, а группы битов размерности m. Наиболее распространёнными являются РС-коды, работающие с байтами, $m=8$, (октетами). Элементы (символы) таких кодов, обозначим их a, являются элементами полной системы (множества) наименьших неотрицательных вычетов Z_N по модулю $N=2^m$, т.е. $a\in Z_{256}$. Нередко применяются РС-коды, в которых элементами a выступают бинарные кодовые комбинации, состоящие из четырёх бит, – полубайтов, $m=4$, (или квартетов) и тогда $a\in Z_{16}$.

Множество Z_N содержит N элементов $a\in\{0,1,\dots,N-1\}$. Наряду с системами вычетов, такими, например, как Z_{16} и Z_{256}, в кодах Рида-Соломона применяются также расширенные поля $GF(2^m)$ характеристики 2, причём показатель m степени двойки совпадает с размерностью бинарных компонент кода. Это соответствие (но никак не равенство) между системами вычетов Z_N, $N=2^m$, и расширенными полями Галуа $GF(2^m)$ обозначим символом $\mapsto$, отмечая тем самым, что $Z_{16}\mapsto GF(2^4)$ и $Z_{256}\mapsto GF(2^8)$. Таким образом, если символами a кода Рида-Соломона являются четырёхбитные кодовые комбинации, то для построения таких кодов применяют множества Z_{16} и поля $GF(2^4)$, тогда как для РС-кодов с восьмибитными символами – множества Z_{256} и поля $GF(2^8)$.

Коды Рида-Соломона являются частным случаем циклических кодов Боуза-Чоудхури-Хоквингема (БЧХ) и для их синтеза (кодирования) и анализа (декодирования) могут быть использованы все методы, которые применяются в соответствующих задачах, решаемых кодами БЧХ. К настоящему времени наработано представительное множество различных алгоритмов РС кодирования и декодирования; при этом значительная часть из них в той или мере содержат символьные переменные, например, такие как степени примитивных элементов α конечных полей Галуа, используемых в качестве компонентов РС-кодов, что и обуславливает определённые затруднения при аппаратно-программной реализации алгоритмов обработки кодов.

Преодоление обозначенной проблемы как раз и составляет *основную цель* данной работы, которая состоит в том, чтобы *предложить способ кодирования и декодирования РС-сообщений, свободный от символьных (буквенных) элементов*, что упрощает их аппаратно-программную реализацию.

2. Общие положения

В кодах Рида-Соломона сообщение представляется в виде набора символов некоторого алфавита, в качестве которого используется алфавит множества вычетов Z_N. Пусть $N=16$, т.е. каждый символ представляет собой четы-рёхбитную кодовую комбинацию. Это означает, что символы сообщения являются элементами расширенного поля $GF(2^4)$. То есть если мы хотим закодировать сообщение, представленное двоичным кодом, то мы разбиваем его на группы по четыре бита и дальше работаем с каждой группой как с числами из поля $GF(2^4)$.

Исходными данными для построения РС-кода являются пара чисел n и t, где $n-$длина кода (число $m-$битных символов в коде), а $t-$ максимальное количество ошибочных символов, обнаруживаемых и устраняемых кодом. Для *примитивных* РС-кодов (а только такие коды мы и будем рассматривать далее) длина кода определяется соотношением $n=2^m-1$. Корни порождающего полинома кода Рида-Соломона лежат в том же поле $GF(2^m)$, над которым строится код. Пусть α – примитивный элемент поля $GF(2^m)$. Порождающий (образующий) полиномом кода Рида-Соломона представляет собой нормированный полином $\boldsymbol{g}(x)$ минимальной степени, корнями которого являются $2t$ подряд идущих степеней $\alpha^1,\alpha^2,\ldots,\alpha^{2t}$ примитивного элемента α поля $GF(2^m)$, то есть

$$\boldsymbol{g}(x)=\prod_{i=1}^{2t}(x-\alpha^i)= (x-\alpha^1)(x-\alpha^2)\ldots(x-\alpha^{2t}). \quad (1)$$

Если в двоичных кодах расстояние Хемминга d равно числу разрядов двух равномерных слов (т.е. слов одинаковой длины) с различными значениями, то в РС-кодах – числу разрядов с различными символами. Рассмотрим, для примера, два равномерных РС-кода, элементы которых представляют собой четырёхбитные кодовые комбинации. Коды отличаются только одним символом, первый из которых положим равным 0000, а второй – 1111. Расстояние Хемминга для этих РС-кодов равно 1, тогда как их двоичные эквиваленты находятся на расстоянии $d=4$.

Число информационных символов k в коде Рида-Соломона определяется соотношением $k=n-r=n-2t$. Еще одним параметром, знание которого необходимо для построения РС-кода, является неприводимый полином $f(x)$, порождающий поле $GF(2^m)$.

Кодирование с помощью кода Рида-Соломона может быть реализовано двумя способами: систематическим или несистематическим. При несистематическом кодировании информационное слово умножается на некий образующий полином $\boldsymbol{g}(x)$. Полученное закодированное слово полностью отличается от исходного и для извлечения информационного слова нужно сначала выполнить операцию декодирования и уже потом можно проверить данные на содержание ошибок. Такое декодирование требует значительных затрат ресурсов только на извлечение информационных данных, при этом они могут быть без ошибок. По этой причине большее практическое применение получили систематические РС-коды.

Технологию систематического РС-кодирования и декодирования поясним далее на числовых примерах, выбрав такие параметры: длина кода $n=15$; кратность ошибки $t=3$; информационный блок, который упаковывается в РС-код, содержит $k=n-2t=9$ символов; число битов m, используемых для представления символов кода, равно четырём ($m=4$); генератор символов кода – поле Галуа $GF(2^4)$, порождается примитивным полиномом (ПрП) четвертой степени $f(x)=x^4+x+1$, векторная форма которого такова $f=10011$.

Обозначим через α корень полинома $f(x)$ – т.е. то значение аргумента x, которое обращает функцию в нуль. Тем самым $f(\alpha)=\alpha^4+\alpha+1=0$ и, следовательно,

$$\alpha^4=\alpha+1. \quad (2)$$

Равенство (2), соблюдаемое только для двоичных $m-$ разрядных символов РС-кода, однозначно определяет (табл. 1) компоненты мультипликативной группы (МПГ), а также основные формы (полиномиальную и векторную) элементов расширенного поля $GF(2^4)$, образуемого ПрП $f=10011$.

На основании табл. 1 составим табл. 2 сложения элементов α^i и α^j поля $GF(2^4)$. Цифрами в табл. 2 указаны показатели степени $s=\overline{0,14}$ элемента α, взаимно однозначно отображающие множество натуральных чисел s во множество элементов α^s, т.е. s и α^s связаны *отношением биекции* (изоморфизма), которое представим в виде $s\leftrightarrow\alpha^s$.

Таблица 1

Мультипликативная группа и элементы поля $GF(2^4)$, порождаемого ПрП $f = 10011$

Элем. МПГ	Числовой эквивалент элем. МПГ	Полином. форма элем. поля $GF(2^4)$	Векторная форма эл. поля $GF(2^4)$			
			x^3	x^2	x^1	x^0
—	$\overline{0}$	0	0	0	0	0
α^0	0	1	0	0	0	1
α^1	1	x	0	0	1	0
α^2	2	x^2	0	1	0	0
α^3	3	x^3	1	0	0	0
α^4	4	$x+1$	0	0	1	1
α^5	5	x^2+x	0	1	1	0
α^6	6	x^3+x^2	1	1	0	0
α^7	7	x^3+x+1	1	0	1	1
α^8	8	x^2+1	0	1	0	1
α^9	9	x^3+x	1	0	1	0
α^{10}	10	x^2+x+1	0	1	1	1
α^{11}	11	x^3+x^2+x	1	1	1	0
α^{12}	12	x^3+x^2+x+1	1	1	1	1
α^{13}	13	x^3+x^2+1	1	1	0	1
α^{14}	14	x^3+1	1	0	0	1
$\alpha^{15}=\alpha^0$	0	1	0	0	0	1

Таблица 2

Таблица сложения ($\hat{+}$) элементов α^i и α^j поля $GF(2^4)$ над ПрП $f = 10011$

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	i
0	$\overline{0}$	4	8	14	1	10	13	9	2	7	5	12	11	6	3	
1	4	$\overline{0}$	5	9	0	2	11	14	10	3	8	6	13	12	7	
2	8	5	$\overline{0}$	6	10	1	3	12	0	11	4	9	7	14	13	
3	14	9	6	$\overline{0}$	7	11	2	4	13	1	12	5	10	8	0	
4	1	0	10	7	$\overline{0}$	8	12	3	5	14	2	13	6	11	9	
5	10	2	1	11	8	$\overline{0}$	9	13	4	6	0	3	14	7	12	
6	13	11	3	2	12	9	$\overline{0}$	10	14	5	7	1	4	0	8	
7	9	14	12	4	3	13	10	$\overline{0}$	11	0	6	8	2	5	1	
8	2	10	0	13	5	4	14	11	$\overline{0}$	12	1	7	9	3	6	
9	7	3	11	1	14	6	5	0	12	$\overline{0}$	13	2	8	10	4	
10	5	8	4	12	2	0	7	6	1	13	$\overline{0}$	14	3	9	11	
11	12	6	9	5	13	3	1	8	7	2	14	$\overline{0}$	0	4	10	
12	11	13	7	10	6	14	4	2	9	8	3	0	$\overline{0}$	1	5	
13	6	12	14	8	11	7	0	5	3	10	9	4	1	$\overline{0}$	2	
14	3	7	13	0	9	12	8	1	6	4	11	10	5	2	$\overline{0}$	

j

Поясним, например, почему все же в табл. 2 сумма $0 \hat{+} 1 = 4$? В самом деле, согласно табл. 1 число 0 есть ничто иное, как $\alpha^0 = 0001$, тогда как число 1 это $\alpha^1 = 0010$. Поразрядно суммируя полубайты 0001 и 0010, получим $0 \hat{+} 1 \to 0001 \oplus 0010 = 0011$, которому в табл. 1 отвечает элемент $0011 = \alpha^4 \leftrightarrow 4$ и т.д. На главной диагонали табл. 2 находятся элементы $\overline{0}$, равные нулевому полубайту, т.е. $\overline{0} = 0000$, так как $\alpha^l \oplus \alpha^l = \overline{0}$. Элементы 0 и $\overline{0}$ также связаны отношением изоморфизма, т.е. $0 \leftrightarrow \overline{0}$. Составлять отдельную таблицу умножения элементов поля $GF(2^4)$ нет необходимости, поскольку эта операция выполняется достаточно просто, а именно, $\alpha^i \cdot \alpha^j = \alpha^{(i+j) \bmod 15}$.

Особенности обратного элемента i^{-1} и операций сложения $\hat{+}$ и умножения $\cdot$ в пространстве изображений наглядно можно проследить по следующим преобразованиям:

$$i \hat{+} i = \overline{0}; \qquad i \cdot \overline{0} = \overline{0};$$
$$i \hat{+} \overline{0} = i; \qquad i \cdot 0 = i;$$
$$i \hat{+} 0 \to \mathrm{T}; \qquad i \cdot j = (i + j) \bmod 15;$$
$$i \hat{+} j \to \mathrm{T}; \qquad i^{-1} = 15 - i,$$

где $\hat{+}$ есть оператор сложения операндов в соответствии с табл. 2 (ссылка на неё вводится символом $\to \mathrm{T}$) для $GF(2^4)$ при $f = 10011$.

Если $\alpha -$ корень образующего полинома $\boldsymbol{g}(x)$ формируемого РС-кода, одновременно являющийся примитивным элементом поля $GF(2^4)$, порождаемого ПрП $f = 10011$, то по формуле (1) после замены знака «минус» на «плюс», поскольку поразрядные преобразования осуществляются над двоичными числами (полубайтами), составим полином

$$\boldsymbol{g}(x) = \left[(x + \alpha^1)(x + \alpha^2)\right] \cdot \left[(x + \alpha^3)(x + \alpha^4)\right] \cdot \left[(x + \alpha^5)(x + \alpha^6)\right] =$$
$$= \left[x^2 + \left(\alpha^1 + \alpha^2\right)x + \alpha^3\right] \cdot \left[x^2 + \left(\alpha^3 + \alpha^4\right)x + \alpha^7\right] \cdot \left[x^2 + \left(\alpha^5 + \alpha^6\right)x + \alpha^{11}\right],$$

который на основании табл. 2 примет вид:

$$\boldsymbol{g}(x) = \left(x^2 + \alpha^5 x + \alpha^3\right)\left(x^2 + \alpha^7 x + \alpha^7\right) \left(x^2 + \alpha^9 x + \alpha^{11}\right). \qquad (3)$$

Перемножим первых два полинома в правой части равенства (3), обозначив результат умножения как $(1 \cdot 2)$:

$$(1 \cdot 2) = \left(x^2 + \alpha^5 x + \alpha^3\right)\left(x^2 + \alpha^7 x + \alpha^7\right) =$$
$$= x^4 + (\alpha^5 + \alpha^7)x^3 + (\alpha^3 + \alpha^7 + \alpha^{12})x^2 + (\alpha^{10} + \alpha^{12})x + \alpha^{10} =$$
$$= x^4 + \alpha^{13}x^3 + \alpha^6 x^2 + \alpha^3 x + \alpha^{10}.$$

Домножим $(1 \cdot 2)$ на третий полином из (3):

$$\boldsymbol{g}(x) = \left(x^4 + \alpha^{13}x^3 + \alpha^6 x^2 + \alpha^3 x + \alpha^{10}\right)\left(x^2 + \alpha^9 x + \alpha^{11}\right) =$$
$$= x^6 + (\alpha^9 + \alpha^{13})x^5 + (\alpha^{11} + \alpha^{22} + \alpha^6)x^4 + (\alpha^{24} + \alpha^{15} + \alpha^3)x^3 +$$
$$(\alpha^{17} + \alpha^{12} + \alpha^{10})x^2 + (\alpha^{14} + \alpha^{19})x + \alpha^{21} = \qquad (4)$$
$$= x^6 + (\alpha^9 + \alpha^{13})x^5 + (\alpha^{11} + \alpha^7 + \alpha^6)x^4 + (\alpha^9 + \alpha^0 + \alpha^3)x^3 +$$
$$(\alpha^2 + \alpha^{12} + \alpha^{10})x^2 + (\alpha^{14} + \alpha^4)x + \alpha^6.$$

После элементарных преобразований в (4) с помощью табл. 2 приходим к окончательному выражению для порождающего многочлена в полиномиальной (алгебраической) форме

$$\boldsymbol{g}(x) = x^6 + \alpha^{10}x^5 + \alpha^{14}x^4 + \alpha^4 x^3 + \alpha^6 x^2 + \alpha^9 x + \alpha^6. \qquad (5)$$

3. Кодирование сообщений

Систематические РС-кодовые слова $\boldsymbol{C}(x)$, как, впрочем, и все систематические коды, представляют собой конкатенацию информационного слова $\boldsymbol{I}(x)$, содержащего k символов, и проверочного слова $\boldsymbol{R}(x)$, которое включает $2t$ символов [4], т.е.:

$$\boldsymbol{C}(x) = \boldsymbol{I}(x) \circ \boldsymbol{R}(x), \qquad (6)$$

где $\circ -$ знак конкатенации.

Конкретизируем компоненты РС-кода с параметрами $(n,k,t)=(15,9,3)$, выбрав в качестве информационного слова $\boldsymbol{I}(x)$ полином восьмой степени, содержащий девять мономов с коэффициентами α^s, в которых показатели степени $s\in GF(16)$. Пусть

$$\boldsymbol{I}(x)=\alpha^3x^8+\alpha^{12}x^7+0x^6+\alpha^9x^5+\alpha^7x^4+0x^3+0x^2+\alpha^{14}x+\alpha^6. \quad (7)$$

Информационное слово (7) может быть представлено также векторной формой

$$\boldsymbol{I}=\alpha^3\alpha^{12}0\alpha^9\alpha^700\alpha^{14}\alpha^6, \quad (8)$$

или изоморфным отображением (биекцией)

$$\hat{\boldsymbol{I}}=3,12,\overline{0},9,7,\overline{0},\overline{0},14,6, \quad (9)$$

где элемент $\overline{0}$ из пространства изображений (9) есть 0 в пространстве оригиналов (8).

Относительно элементов α^s кодов Рида-Соломона (коэффициентов полиномов: кодовых слов $\boldsymbol{C}(x)$, информационных слов $\boldsymbol{I}(x)$, проверочных слов $\boldsymbol{R}(x)$ или других полиномов) будем говорить, что они (коэффициенты) принадлежат пространству оригиналов, тогда как показатели степени s при основании α, являющиеся натуральными числами, включая 0, биективно связанными с элементами α^s, принадлежат пространству изображений. Элементы α^s из пространства оригиналов и показатели степени s из пространства изображений связаны отношением изоморфизма.

Поставим в соответствие формам информационных слов (8) и (9) аналогичные формы образующего полинома (5). Имеем

$$\boldsymbol{g}=\alpha^0\alpha^{10}\alpha^{14}\alpha^4\alpha^6\alpha^9\alpha^6, \quad (10)$$

и

$$\hat{\boldsymbol{g}}=0,10,14,4,6,9,6. \quad (11)$$

Перейдем к вычислению проверочного слова $\boldsymbol{R}(x)$, в качестве алгоритма синтеза которого используем метод *матриц проверочных символов* кодов Рида-Соломона [5]. Матрица проверочных символов (МПС), обозначив её через $\boldsymbol{P}$, блочного систематического $(n,k)-$кода представляет собой прямоугольную $(k,r)-$матрицу, содержащую k строк (по числу информационных символов в кодовом слове) и $r=n-k=2t$ столбцов (по числу проверочных символов). Матрица $\boldsymbol{P}$, будучи дополненной слева единичной матрицей $k-$го порядка $\boldsymbol{E}$, составляют совместно образующую матрицу $\boldsymbol{G}$ систематического кода. Если же под матрицей $\boldsymbol{P}$ разместить единичную матрицу $r-$го порядка, то приходим к проверочной матрице $\boldsymbol{H}$. Построим МПС для того же $(15,9,3)-$кода РС. Основу построения МПС составляют векторные формы образующих полиномов $\boldsymbol{g}$, например (10). Для $(15,9,3)-$кода РС таковым полиномом в пространстве изображений является полином (11). Обратим внимание на то, что старший (левый) нулик в (11) есть единичка в пространстве оригиналов, поскольку согласно условию изоморфизма $0\leftrightarrow\alpha^0=1$.

Разместим полином (11), исключая старший нулик в нижней (первой) строке формируемой матрицы $\hat{\boldsymbol{P}}$. Последующая (вторая) строка матрицы $\hat{\boldsymbol{P}}$ образуется сдвигом предыдущей (первой) строки на один разряд влево. В освободившемся младшем разряде второй строки синтезируемой матрицы $\hat{\boldsymbol{P}}$ появляется символ $\overline{0}$ (нулевой элемент в пространстве изображений), а символ 10 («десять», как элемент множества Z_{16}) первой строки из $\hat{\boldsymbol{P}}$ перемещается в младший разряд второй строки матрицы, являющейся единичной матрицей $\boldsymbol{E}$ девятого порядка, предшествующей $\hat{\boldsymbol{P}}$ в образующей матрице $\boldsymbol{G}$ $(15,9,3)-$кода РС. Но в этом разряде матрицы $\boldsymbol{E}$ должен находится нулик.

Для того чтобы обнулить указанный разряд матрицы $\boldsymbol{E}$ достаточно проделать следующие операции. Во-первых, просуммировать каждый разряд полинома (14) с элементом 10 по модулю 15, а затем, во-вторых, преобразованный полином (14) поразрядно сложить (с помощью табл. 2) с младшими семью разрядами второй строки матрицы $\boldsymbol{G}$. Имеем

$$\begin{array}{l} 10,14,\ 4,\ 6,9,6,\overline{0} \leftarrow \textit{вторая строка матрицы } \hat{\boldsymbol{P}} \\ \hat{+}\ \underline{10,\ 5,\ 9,14,1,\ 4,1} \leftarrow \textit{домноженная первая строка матрицы } \hat{\boldsymbol{P}}. \\ \overline{0},12,14,\ 8,3,12,1 \end{array}$$

Отбрасывая старший нулевой элемент (элемент $\overline{0}$), получим вторую строку матрицы $\hat{\boldsymbol{P}}$. Продолжая аналогичные вычисления, приходим схеме вычисления строк (подчёркнутых и слева

пронумерованных) МПС $\hat{\boldsymbol{P}}$ $(15, 9, 3)$ – кода РС, представленных соотношением:

$$
\begin{array}{ll}
1 & \hat{+}\ \underline{10, 14,\ 4,\ 6,\ 9,\ 6},\ \overline{0} \\
 & \quad 10,\ 5,\ 9, 14,\ 1,\ 4,\ 1 \\
2 & \quad \hat{+}\ \underline{12, 14,\ 8,\ 3, 12,\ 1},\ \overline{0} \\
 & \quad\ 12,\ 7, 11,\ 1,\ 3,\ 6,\ 3 \\
3 & \quad\ \hat{+}\ \underline{1,\ 7,\ 9, 10, 11,\ 3},\ \overline{0} \\
 & \quad\ 1, 11,\ 0,\ 5,\ 7, 10,\ 7 \\
4 & \quad\ \hat{+}\ \underline{8,\ 7,\ 0,\ 8, 12,\ 7},\ \overline{0} \\
 & \quad\ 8,\ 3,\ 7, 12, 14,\ 2, 14 \\
5 & \quad\ \hat{+}\ \underline{4,\ 9,\ 9,\ 5, 12, 14},\ \overline{0} \\
 & \quad\ 4, 14,\ 3,\ 8, 10, 13, 10 \\
6 & \quad\ \hat{+}\ \underline{4,\ 1,\ 4,\ 3,\ 2, 10},\ \overline{0} \\
 & \quad\ 4, 14,\ 3,\ 8, 10, 13, 10 \\
7 & \quad\ \hat{+}\ \underline{7,\ 7, 13,\ 4,\ 9, 10},\ \overline{0} \\
 & \quad\ 7,\ 2,\ 6, 11, 13,\ 1, 13 \\
8 & \quad\ \hat{+}\ \underline{12,\ 0, 13, 10,\ 8, 13},\ \overline{0} \\
 & \quad\ 12,\ 7, 11,\ 1,\ 3,\ 6,\ 3 \\
9 & \quad\ \underline{9,\ 4,\ 8, 13,\ 0,\ 3}.
\end{array}
\qquad (12)
$$

На основании системы (12) получим матрицу проверочных символов $(15, 9, 3)$ – кода Рида-Соломона, элементами которой являются компоненты множества Z_{16}:

$$
\hat{\boldsymbol{P}} = \begin{pmatrix}
9 & 4 & 8 & 13 & 0 & 3 \\
12 & 0 & 13 & 10 & 8 & 13 \\
7 & 7 & 13 & 4 & 9 & 10 \\
4 & 1 & 4 & 3 & 2 & 10 \\
4 & 9 & 9 & 5 & 12 & 14 \\
8 & 7 & 0 & 8 & 12 & 7 \\
1 & 7 & 9 & 10 & 11 & 3 \\
12 & 14 & 8 & 3 & 12 & 1 \\
10 & 14 & 4 & 6 & 9 & 6
\end{pmatrix}. \qquad (13)
$$

Воспользовавшись матрицей (13), определим значения проверочных разрядов в пространстве изображений $\hat{\boldsymbol{R}}_I$, отвечающие изоморфному отображению слова $\boldsymbol{I}$, заданного вектор-строкой (9):

$$\widehat{\boldsymbol{R}}_{\hat{I}}^{T} = \widehat{\boldsymbol{I}\cdot\boldsymbol{P}} = \widehat{\boldsymbol{I}}^{T} \overset{15}{\underline{\oplus}} \widehat{\boldsymbol{P}} = \begin{pmatrix} 3 \\ 12 \\ \overline{0} \\ 9 \\ 7 \\ \overline{0} \\ \overline{0} \\ 14 \\ 6 \end{pmatrix} \overset{15}{\underline{\oplus}} \begin{pmatrix} 9 & 4 & 8 & 13 & 0 & 3 \\ 12 & 0 & 13 & 10 & 8 & 13 \\ 7 & 7 & 13 & 4 & 9 & 10 \\ 4 & 1 & 4 & 3 & 2 & 10 \\ 4 & 9 & 9 & 5 & 12 & 14 \\ 8 & 7 & 0 & 8 & 12 & 7 \\ 1 & 7 & 9 & 10 & 11 & 3 \\ 12 & 14 & 8 & 3 & 12 & 1 \\ 10 & 14 & 4 & 6 & 9 & 6 \end{pmatrix}, \qquad (14)$$

где $\overset{15}{\underline{\oplus}}$ – оператор, которым осуществляется сложение по модулю 15 элементов вектор-столбца $\widehat{\boldsymbol{I}}^{T}$ со всеми элементами соответствующих строк матрицы $\widehat{\boldsymbol{P}}$ в этом же выражении, причём строки матрицы $\widehat{\boldsymbol{P}}$, расположенные напротив элемента $\overline{0}$ столбца $\widehat{\boldsymbol{I}}^{T}$ $\widehat{\boldsymbol{I}}^{T}$, обнуляются, поскольку они обнуляются также и в пространстве оригиналов за счет нулевого значения элемента вектор-строки $\boldsymbol{I}$. Выполнив указанные преобразования в (14), получим промежуточную матрицу:

$$\begin{pmatrix} 12 & 7 & 11 & 1 & 3 & \mathbf{6} \\ 9 & 12 & \mathbf{10} & 7 & 5 & 10 \\ \overline{0} & \overline{0} & \overline{0} & \overline{0} & \overline{0} & \overline{0} \\ 13 & 10 & 13 & \mathbf{12} & \mathbf{11} & 4 \\ \mathbf{11} & 1 & 1 & \mathbf{12} & 4 & \mathbf{6} \\ \overline{0} & \overline{0} & \overline{0} & \overline{0} & \overline{0} & \overline{0} \\ \overline{0} & \overline{0} & \overline{0} & \overline{0} & \overline{0} & \overline{0} \\ \mathbf{11} & 13 & 7 & 2 & \mathbf{11} & 0 \\ 1 & 5 & \mathbf{10} & 12 & 0 & 12 \end{pmatrix}. \qquad (15)$$

Исключим из столбцов матрицы (15) одинаковые пары элементов, выделенные жирным шрифтом, заменив их элементами $\overline{0}$, поскольку в пространстве изображений $i \hat{+} i = \overline{0}$:

$$\begin{pmatrix} 12 & 7 & 11 & 1 & 3 & \overline{0} \\ 9 & 12 & \overline{0} & 7 & 5 & 10 \\ \overline{0} & \overline{0} & \overline{0} & \overline{0} & \overline{0} & \overline{0} \\ 13 & 10 & 13 & \overline{0} & \overline{0} & 4 \\ \overline{0} & 1 & 1 & \overline{0} & 4 & \overline{0} \\ \overline{0} & \overline{0} & \overline{0} & \overline{0} & \overline{0} & \overline{0} \\ \overline{0} & \overline{0} & \overline{0} & \overline{0} & \overline{0} & \overline{0} \\ \overline{0} & 13 & 7 & 2 & \overline{0} & 0 \\ 1 & 5 & \overline{0} & 12 & 0 & 12 \end{pmatrix}. \qquad (16)$$

Суммируя элементы столбцов матрицы (16) по данным табл. 2, приходим к такому значению проверочных разрядов $\boldsymbol{R}_{\hat{I}}$ для информационного слова $\widehat{\boldsymbol{I}}$ в пространстве изображений

$$\boldsymbol{R}_{\hat{I}} = 9, 9, 9, 1, 6, 9, \qquad (17)$$

которые аналогично (8) и (9) можно представить также в пространстве оригиналов в векторной (18) и полиномиальной (19) формах

$$\boldsymbol{R}_{\hat{I}} = \alpha^{9}\alpha^{9}\alpha^{9}\alpha^{1}\alpha^{6}\alpha^{9}, \qquad (18)$$

$$\boldsymbol{R}_{\hat{I}}(x) = \alpha^{9}x^{5} + \alpha^{9}x^{4} + \alpha^{9}x^{3} + \alpha^{1}x^{2} + \alpha^{6}x + \alpha^{9}. \qquad (19)$$

Теперь на основании выражения (6), систем равенств (7) – (9) и (17) – (19) составим все три формы разрешённых $(15, 9, 3)$ – РС кодовых слов с коэффициентами из поля $GF(2^4)$ в пространствах оригиналов ($\boldsymbol{C}(x)$, $\boldsymbol{C}$) и изображений ($\widehat{\boldsymbol{C}}$):

$$\boldsymbol{C}(x) = \alpha^3 x^{14} + \alpha^{12} x^{13} + 0x^{12} + \alpha^9 x^{11} + \alpha^7 x^{10} + 0x^9 + 0x^8 + \alpha^{14} x^7 + \alpha^6 x^6 + \alpha^9 x^5 + \alpha^9 x^4 + \alpha^9 x^3 + \alpha^1 x^2 + \alpha^6 x + \alpha^9. \quad (20)$$

$$\boldsymbol{C} = \alpha^3 \alpha^{12} 0 \alpha^9 \alpha^7 0 0 \alpha^{14} \alpha^6 \alpha^9 \alpha^9 \alpha^9 \alpha^1 \alpha^6 \alpha^9;$$

$$\hat{\boldsymbol{C}} = 3,12,\overline{0},9,7,\overline{0},\overline{0},14,6,9,9,9,1,6,9. \quad (21)$$

Для контроля корректности вычислений поделим в пространстве изображений кодовое слово (21) на образующий полином (14). Данная операция подобна схеме вычислений в системе (12) и представима такой последовательностью преобразований:

$$\hat{\boldsymbol{I}} \rightarrow \hat{+}\ 3,12,\overline{0},9,7,\overline{0},\overline{0},14,6,9,9,9,1,6,9 : 0,10,14,4,6,9,6 \leftarrow \hat{\boldsymbol{g}}$$

$$3,\underline{13,\ 2,\ 7,\ 9,12,\ 9} \qquad \textit{частное} \rightarrow\ 3,1,9,4,5,11,8,0,1$$

$$\hat{+}\ 1,\ 2,\ 0,\ 0,12,\ 9,14$$

$$1,\underline{11,\ 0,\ 5,\ 7,10,\ 7}$$

$$\hat{+}\ 9,\ \overline{0},10,\ 2,13,\ 1,\ 6$$

$$9,\ \underline{4,\ 8,13,\ 0,\ 3,\ 0}$$

$$\hat{+}\ 4,\ 1,14,\ 6,\ 9,13,\ 9$$

$$4,\underline{14,\ 3,\ 8,10,13,10}$$

$$\hat{+}\ 7,\ 0,14,13,\ \overline{0},13,\ 9$$

$$7,\ \underline{2,\ 6,11,13,\ 1,13}$$

$$\hat{+}\ 8,\ 8,\ 4,13,12,10,\ 9$$

$$8,\ \underline{3,\ 7,12,14,\ 2,14}$$

$$\hat{+}\ 13,\ 3,\ 1,\ 5,\ 4,\ 4,\ 1$$

$$13,\ \underline{8,12,\ 2,\ 4,\ 7,\ 4}$$

$$\hat{+}\ 13,13,\ 1,\ \overline{0},\ 3,\ 0,\ 6$$

$$13,\ \underline{8,12,\ 2,\ 4,\ 7,\ 4}$$

$$\hat{+}\ 3,13,\ 2,\ 7,\ 9,12,\ 9$$

$$3,\underline{13,\ 2,\ 7,\ 9,12,\ 9}$$

$$\overline{0},\ \overline{0},\ \overline{0},\ \overline{0},\ \overline{0},\ \overline{0} \leftarrow \textit{остаток}\ \left(\hat{\boldsymbol{R}}\right).$$

Нулевой остаток $\hat{\boldsymbol{R}}$ является свидетельством того, что вычисления, предшествующие оценке $\hat{\boldsymbol{R}}$, были выполнены без ошибок.

4. Декодирование сообщений

Пусть $\hat{\boldsymbol{C}}^*$ – кодовая комбинация (в обозначении, принятом для пространства изображений), поступившая на вход приёмного устройства, и, возможно, искажённая помехой, что подчёркивается верхним индексом *. Каждый разряд кода $\hat{\boldsymbol{C}}^*$ представляет собой полубайт, который записывается в виде элемента множества Z_{16}, но физически является элементом расширенного поля $GF(2^4)$. Для декодирования кодов Рида-Соломона могут быть использованы методы [6, 7], применяемые при декодировании кодов БЧХ. Воспользуемся далее алгоритмом Питерсона-Горенштейна-Цирлера (ПГЦ). Все вычисления будем проводить в пространстве изображений.

Исходными данными для реализации ПГЦ-алгоритма РС-декодирования являются:

1. Информационное слово (9);
2. Образующий полином (11);
3. Вектор проверочных символов исходного информационного слова (17);
4. Неискаженное кодовое слово (21);
5. Помеху зададим пятнадцатисимвольным вектором

$$\hat{\boldsymbol{e}} = \overline{0},\overline{0},8,\overline{0},\overline{0},\overline{0},\overline{0},\overline{0},\overline{0},\overline{0},5,\overline{0},\overline{0},\overline{0},\overline{0}. \quad (22)$$

То есть двукратная помеха поражает двенадцатый (информационный) и четвертый (проверочный) символы кодового слова $\widehat{\boldsymbol{C}}$ (21), которые суммируются оператором $\hat{+}$ с символами помехи (22) по табл. 2. На вход приёмного устройства поступает искаженное кодовое слово:

$$\widehat{\boldsymbol{C}}^{*} = \widehat{\boldsymbol{C}} \overset{15}{\oplus} \boldsymbol{e} = 3,12,\mathbf{8},9,7,\overline{0},\overline{0},14,6,9,\mathbf{6},9,1,6,9. \quad (23)$$

Искаженные помехой символы в (23) отмечены жирным шрифтом, при чём младший пораженный символ равен **6**, поскольку $9 \hat{+} 5 = 6$ (см. табл. 2), а старший – **8**, так как $\overline{0} \hat{+} 8 = 8$.

Рассматриваемый $(15, 9, 3)$ – код РС ориентирован на обнаружение и устранение не более трёх ошибок. Это означает, что на первом этапе необходимо сначала вычислить символы шести синдромов в пространстве изображений:

$$\widehat{\boldsymbol{S}}_i = \widehat{\boldsymbol{C}}^{*}(\alpha^i), \quad i = \overline{1,6}. \quad (24)$$

В соответствии с выражениями (20), (23) и (24) составим развернутую схему последовательного вычисления синдромов входного кодового слова:

$$\begin{aligned} \boldsymbol{C}^{*}(x) &= \alpha^3 x^{14} + \alpha^{12} x^{13} + \boldsymbol{\alpha^8} x^{12} \\ &+ \alpha^9 x^{11} + \alpha^7 x^{10} + \alpha^{14} x^7 + \\ &+ \alpha^6 x^6 + \alpha^9 x^5 + \boldsymbol{\alpha^6} x^4 + \\ &\alpha^9 x^3 + \alpha^1 x^2 + \alpha^6 x + \alpha^9. \end{aligned} \quad (25)$$

Жирным шрифтом в (25), как и в (23), выделены априори неизвестные искаженные помехой символы:

$$\begin{aligned} \boldsymbol{C}^{*}(\alpha^i) &= \alpha^3 \alpha^{i\cdot 14} + \alpha^{12} \alpha^{i\cdot 13} + \alpha^8 \alpha^{i\cdot 12} \\ &+ \alpha^9 \alpha^{i\cdot 11} + \alpha^7 \alpha^{i\cdot 10} + \alpha^{14} \alpha^{i\cdot 7} + \\ &+ \alpha^6 \alpha^{i\cdot 6} + \alpha^9 \alpha^{i\cdot 5} + \alpha^6 \alpha^{i\cdot 4} + \\ &\alpha^9 \alpha^{i\cdot 3} + \alpha^1 \alpha^{i\cdot 2} + \alpha^6 \alpha^i + \alpha^9. \end{aligned} \quad (26)$$

На основании (26) приходим к такому общему выражению для синдрома $\widehat{\boldsymbol{S}}_i$ в пространстве изображений, отбросив, для простоты, полудугу над символом синдрома:

$$\begin{aligned} \boldsymbol{S}_i = \widehat{\boldsymbol{C}}^{*}(\alpha^i) &= (3 + i\cdot 14) \hat{+} \\ &(12 + i\cdot 13) \hat{+} (8 + i\cdot 12) \hat{+} \\ &\hat{+}(9 + i\cdot 11) \hat{+} (7 + i\cdot 10) \hat{+} \\ &(14 + i\cdot 7) \hat{+} (6 + i\cdot 6) \hat{+} (9 + i\cdot 5) \\ &\hat{+}(6 + i\cdot 4) \hat{+} (9 + i\cdot 3) \hat{+} \\ &(1 + i\cdot 2) \hat{+} (6 + i) \hat{+} 9, \end{aligned} \quad (27)$$

в котором сумма чисел, расположенных в круглых скобках, должна быть приведена к остатку по модулю 15, а оператором $\hat{+}$ обозначено суммирование по табл. 2.

Итак, согласно (27), имеем (жирным шрифтом отмечены повторяющиеся символы, которые, естественно, оператором $\hat{+}$ обнуляются):

$$\begin{aligned} \boldsymbol{S}_1 &= (3+14) \hat{+} (12+13) \hat{+} (8+12) \hat{+} (9+11) \hat{+} (7+10) \hat{+} (14+7) \hat{+} \\ &\hat{+}(6+6) \hat{+} (9+5) \hat{+} (6+4) \hat{+} (9+3) \hat{+} (1+2) \hat{+} (6+1) \hat{+} 9 = \\ &= \mathbf{2} \hat{+} \mathbf{10} \hat{+} \mathbf{5} \hat{+} \mathbf{5} \hat{+} \mathbf{2} \hat{+} 6 \hat{+} \mathbf{12} \hat{+} 14 \hat{+} \mathbf{10} \hat{+} \mathbf{12} \hat{+} 3 \hat{+} 7 + 9 = 6 \hat{+} 14 \hat{+} 3 \hat{+} 7 \hat{+} 9 = 6. \end{aligned} \quad (28)$$

$$\begin{aligned} \boldsymbol{S}_2 &= (3+28) \hat{+} (12+26) \hat{+} (8+24) \hat{+} (9+22) \hat{+} (7+20) \hat{+} (14+14) \hat{+} \\ &\hat{+}(6+12) \hat{+} (9+10) \hat{+} (6+8) \hat{+} (9+6) \hat{+} (1+4) \hat{+} (6+2) \hat{+} 9 = \\ &= \mathbf{1} \hat{+} \mathbf{8} \hat{+} 2 \hat{+} \mathbf{1} \hat{+} 12 \hat{+} 13 \hat{+} 3 \hat{+} 4 \hat{+} 14 \hat{+} 0 \hat{+} 5 \hat{+} \mathbf{8} \hat{+} 9 = \\ &= 2 \hat{+} 12 \hat{+} 13 \hat{+} 3 \hat{+} 4 \hat{+} 14 \hat{+} 0 \hat{+} 5 \hat{+} 9 = 7 \hat{+} 8 \hat{+} \mathbf{9} \hat{+} 10 \hat{+} \mathbf{9} = 11 \hat{+} 10 = 14. \end{aligned} \quad (29)$$

$$\begin{aligned} \boldsymbol{S}_3 &= (3+42) \hat{+} (12+39) \hat{+} (8+36) \hat{+} (9+33) \hat{+} (7+30) \hat{+} (14+21) \hat{+} \\ &\hat{+}(6+18) \hat{+} (9+15) \hat{+} (6+12) \hat{+} (9+9) \hat{+} (1+6) \hat{+} (6+3) \hat{+} 9 = \\ &= 0 \hat{+} 6 \hat{+} 14 \hat{+} 12 \hat{+} \mathbf{7} \hat{+} 5 \hat{+} \mathbf{9} \hat{+} \mathbf{9} \hat{+} \mathbf{3} \hat{+} \mathbf{3} \hat{+} \mathbf{7} \hat{+} \mathbf{9} \hat{+} \mathbf{9} = 0 \hat{+} 6 \hat{+} 14 \hat{+} 12 \hat{+} 5 = 13. \end{aligned} \quad (30)$$

$$\begin{aligned} \boldsymbol{S}_4 &= (3+56) \hat{+} (12+52) \hat{+} (8+48) \hat{+} (9+44) \hat{+} (7+40) \hat{+} (14+28) \hat{+} \\ &\hat{+}(6+24) \hat{+} (9+20) \hat{+} (6+16) \hat{+} (9+12) \hat{+} (1+8) \hat{+} (6+4) \hat{+} 9 = \\ &= \mathbf{14} \hat{+} 4 \hat{+} 11 \hat{+} 8 \hat{+} 2 \hat{+} 12 \hat{+} 0 \hat{+} \mathbf{14} \hat{+} 7 \hat{+} 6 \hat{+} \mathbf{9} \hat{+} 10 \hat{+} \mathbf{9} = \\ &= 4 \hat{+} 11 \hat{+} 8 \hat{+} 2 \hat{+} 12 \hat{+} 0 \hat{+} 7 \hat{+} 6 \hat{+} 10 = 13 \hat{+} 2 \hat{+} 7 = 1. \end{aligned} \quad (31)$$

$$\begin{gathered}\boldsymbol{S}_5 = (3+70)\hat{+}(12+65)\hat{+}(8+60)\hat{+}(9+55)\hat{+}(7+50)\hat{+}(14+35)\hat{+} \\ \hat{+}(6+30)\hat{+}(9+25)\hat{+}(6+20)\hat{+}(9+15)\hat{+}(1+10)\hat{+}(6+5)\hat{+}9 = \\ = 13\hat{+}2\hat{+}8\hat{+}4\hat{+}12\hat{+}\mathbf{4}\hat{+}6\hat{+}\mathbf{4}\hat{+}11\hat{+}\mathbf{9}\hat{+}\mathbf{11}\hat{+}\mathbf{11}\hat{+}\mathbf{9} = \\ = 13\hat{+}2\hat{+}8\hat{+}4\hat{+}12\hat{+}6\hat{+}11 = 14\hat{+}5\hat{+}4\hat{+}11 = 1.\end{gathered} \tag{32}$$

$$\begin{gathered}\boldsymbol{S}_6 = (3+84)\hat{+}(12+78)\hat{+}(8+72)\hat{+}(9+66)\hat{+}(7+60)\hat{+}(14+42)\hat{+} \\ \hat{+}(6+36)\hat{+}(9+30)\hat{+}(6+24)\hat{+}(9+18)\hat{+}(1+12)\hat{+}(6+6)\hat{+}9 = \\ = \mathbf{12}\hat{+}\mathbf{0}\hat{+}5\hat{+}\mathbf{0}\hat{+}7\hat{+}11\hat{+}\mathbf{12}\hat{+}\mathbf{9}\hat{+}0\hat{+}\mathbf{12}\hat{+}13\hat{+}\mathbf{12}\hat{+}\mathbf{9} = 5\hat{+}7\hat{+}11\hat{+}0\hat{+}13 = 12.\end{gathered} \tag{33}$$

Для проверки корректности вычислений в соотношениях (28)-(33) определим синдромы $\boldsymbol{S}_i^{(e)}$, $i = \overline{1,6}$, помехи $\boldsymbol{e}(x) = \alpha^8 x^{12} + \alpha^5 x^4$, определяемые выражением

$$\boldsymbol{S}_i^{(e)} = (8 + i\cdot 12)\hat{+}(5 + i\cdot 4).$$

Имеем

$$\begin{aligned}\boldsymbol{S}_1^{(e)} &= (8+12)\hat{+}(5+4) = 5\hat{+}9 = 6; \\ \boldsymbol{S}_2^{(e)} &= (8+24)\hat{+}(5+8) = 2\hat{+}13 = 14; \\ \boldsymbol{S}_3^{(e)} &= (8+36)\hat{+}(5+12) = 14\hat{+}2 = 13; \\ \boldsymbol{S}_4^{(e)} &= (8+48)\hat{+}(5+16) = 11\hat{+}6 = 1; \\ \boldsymbol{S}_5^{(e)} &= (8+60)\hat{+}(5+20) = 8\hat{+}10 = 1; \\ \boldsymbol{S}_6^{(e)} &= (8+72)\hat{+}(5+24) = 5\hat{+}14 = 12.\end{aligned} \tag{34}$$

Совпадение результатов (34) с оценками синдромов (28) -(33) подтверждает, что все вычисления были выполнены без ошибок.

Априори нам не известно, сколько ошибочных символов содержит входное слово $\widehat{\boldsymbol{C}}^*$. Для оценки их числа первоначально составляется матрица синдромов $\boldsymbol{S}^{(t)}$, порядок которой t должен быть выбран равным максимальному числу обнаруживаемых и устраняемых ошибок, на которое рассчитан код РС, т.е. $t = 3$,

$$\boldsymbol{S}^{(3)} = \begin{bmatrix}\boldsymbol{S}_1 & \boldsymbol{S}_2 & \boldsymbol{S}_3 \\ \boldsymbol{S}_2 & \boldsymbol{S}_3 & \boldsymbol{S}_4 \\ \boldsymbol{S}_3 & \boldsymbol{S}_4 & \boldsymbol{S}_5\end{bmatrix} = \begin{bmatrix}6 & 14 & 13 \\ 14 & 13 & 1 \\ 13 & 1 & 1\end{bmatrix}$$

и вычисляется определитель $\Delta^{(3)}$ матрицы $\boldsymbol{S}^{(3)}$:

$$\begin{gathered}\Delta^{(3)} = (6+13+1)\hat{+}(\mathbf{14}+\mathbf{1}+\mathbf{13})\hat{+}(\mathbf{14}+\mathbf{1}+\mathbf{13})\hat{+} \\ \hat{+}(13+13+13)\hat{+}(6+1+1)\hat{+}(14+14+1) = \\ 5\hat{+}9\hat{+}8\hat{+}14 = 6\hat{+}6 = \overline{0}.\end{gathered}$$

Поскольку $\Delta^{(3)}$ оказался равным нулю, то понижаем порядок матрицы синдромов $\boldsymbol{S}^{(t)}$, полагая его равным двум. Имеем

$$\boldsymbol{S}^{(2)} = \begin{bmatrix}\boldsymbol{S}_1 & \boldsymbol{S}_2 \\ \boldsymbol{S}_2 & \boldsymbol{S}_3\end{bmatrix} = \begin{bmatrix}6 & 14 \\ 14 & 13\end{bmatrix}. \tag{35}$$

Матрице в (35) отвечает определитель

$$\Delta^{(2)} = (6+13)\hat{+}(14+14) = 4\hat{+}13 = 11.$$

Поскольку матрица синдромов второго порядка $\boldsymbol{S}^{(2)}$ оказалась невырожденной, то это означает, что кодовая комбинация $\widehat{\boldsymbol{C}}^*$ в (27) содержит две ошибки, которые могут быть получены на основании решения ключевого уравнения. Матричная форма ключевого уравнения имеет вид:

$$\begin{bmatrix}\boldsymbol{S}_1 & \boldsymbol{S}_2 & \cdots & \boldsymbol{S}_t \\ \boldsymbol{S}_2 & \boldsymbol{S}_3 & \cdots & \boldsymbol{S}_{t+1} \\ \vdots & \vdots & \ddots & \vdots \\ \boldsymbol{S}_t & \boldsymbol{S}_{t+1} & \cdots & \boldsymbol{S}_{2t-1}\end{bmatrix}\cdot\begin{bmatrix}\boldsymbol{\Lambda}_t \\ \boldsymbol{\Lambda}_{t-1} \\ \vdots \\ \boldsymbol{\Lambda}_1\end{bmatrix} = \begin{bmatrix}\boldsymbol{S}_{t+1} \\ \boldsymbol{S}_{t+2} \\ \vdots \\ \boldsymbol{S}_{2t}\end{bmatrix},$$

где $\boldsymbol{\Lambda}_i$ – коэффициенты полинома локатора ошибок.

Для $(15, 9, 3)$ – кода РС с коррекцией двухсимвольных ошибок ключевое уравнение запишется следующим образом:

$$\begin{bmatrix}\boldsymbol{S}_1 & \boldsymbol{S}_2 \\ \boldsymbol{S}_2 & \boldsymbol{S}_3\end{bmatrix}\cdot\begin{bmatrix}\boldsymbol{\Lambda}_2 \\ \boldsymbol{\Lambda}_1\end{bmatrix} = \begin{bmatrix}\boldsymbol{S}_3 \\ \boldsymbol{S}_4\end{bmatrix}. \tag{36}$$

Чтобы найти коэффициенты $\boldsymbol{\Lambda}_1$ и $\boldsymbol{\Lambda}_2$ полинома $\boldsymbol{\Lambda}^{(2)}$ локатора ошибок, сначала необходимо найти обратную матрицу $\overline{\boldsymbol{S}}^{(2)}$ для уравнения (36), т.е. для уравнения:

$$\begin{bmatrix}6 & 14 \\ 14 & 13\end{bmatrix}\cdot\begin{bmatrix}\boldsymbol{\Lambda}_2 \\ \boldsymbol{\Lambda}_1\end{bmatrix} = \begin{bmatrix}13 \\ 1\end{bmatrix}. \tag{37}$$

Матрица $\overline{\boldsymbol{S}}^{(2)}$, обратная матрице $\boldsymbol{S}^{(2)}$, определяется так:

$$\overline{\boldsymbol{S}}^{(2)} = \frac{\text{Матрица кофакторов } \boldsymbol{S}^{(2)}}{\text{Det}(\boldsymbol{S}^{(2)})} = \frac{\begin{bmatrix}13 & 14\\ 14 & 6\end{bmatrix}}{11} = \tag{38}$$

$$= 4 \overset{15}{\oplus} \begin{bmatrix}13 & 14\\ 14 & 6\end{bmatrix} = \begin{bmatrix}(13+4) & (14+4)\\ (14+4) & (6+4)\end{bmatrix} = \begin{bmatrix}2 & 3\\ 3 & 10\end{bmatrix}.$$

Если обратная матрица $\overline{\boldsymbol{S}}^{(2)}$ в (38) вычислена правильно, то произведение исходной $\boldsymbol{S}^{(2)}$ и обратной матрицы $\overline{\boldsymbol{S}}^{(2)}$ должно дать единичную матрицу $\hat{\boldsymbol{E}}^{(2)}$:

$$\boldsymbol{S}^{(2)} \cdot \overline{\boldsymbol{S}}^{(2)} = \begin{bmatrix}6 & 14\\ 14 & 13\end{bmatrix} \cdot \begin{bmatrix}2 & 3\\ 3 & 10\end{bmatrix} = \tag{39}$$

$$= \begin{bmatrix}(6+2)\hat{+}(14+3) & (6+3)\hat{+}(14+10)\\ (14+2)\hat{+}(13+3) & (14+3)\hat{+}(13+10)\end{bmatrix} = \begin{bmatrix}8\hat{+}2 & 9\hat{+}9\\ 1\hat{+}1 & 2\hat{+}8\end{bmatrix} = \begin{bmatrix}0 & \overline{0}\\ \overline{0} & 0\end{bmatrix}.$$

Матрица в правой части равенства (39) есть единичная матрица второго порядка в пространстве изображений, т.е. обратная матрица $\overline{\boldsymbol{S}}^{(2)}$ вычислена правильно. Теперь можем обратиться к решению уравнения (37), умножив слева обе части уравнения на $\overline{\boldsymbol{S}}^{(2)}$:

$$\begin{bmatrix}\boldsymbol{\Lambda}_2\\ \boldsymbol{\Lambda}_1\end{bmatrix} = \begin{bmatrix}2 & 3\\ 3 & 10\end{bmatrix} \cdot \begin{bmatrix}13\\ 1\end{bmatrix} = \begin{bmatrix}(2+13)\hat{+}(3+1)\\ (3+13)\hat{+}(10+1)\end{bmatrix} = \begin{bmatrix}0\hat{+}4\\ 1\hat{+}11\end{bmatrix} = \begin{bmatrix}1\\ 6\end{bmatrix}. \tag{40}$$

Решение (40) даёт возможность составить полином локаторов ошибок:

$$\Lambda^{(2)}(x) = 1 + \Lambda_1 x + \Lambda_2 x^2 = \alpha^0 + \alpha^6 x + \alpha^1 x^2,$$

изображение которого (для аргумента $x = \alpha^i$) таково:

$$\hat{\Lambda}^{(2)}(i) = 0\,\hat{+}\,(6+i)\,\hat{+}\,(1+2i). \tag{41}$$

Корни $\hat{\Lambda}^{(2)}(i)$, являющимися числами, обратными к положениям ошибок, определяются с помощью процедуры Ченя, равносильной полному перебору, т.е. последовательным отысканием тех значений i, которые обращают полином (41) в нуль (в пространстве изображений это $\overline{0}$). Вариант Ченя для полинома (41) показан в табл. 3. Знаком « — » в табл. 3 обозначено, что $\hat{\Lambda}^{(2)}(i) \neq \overline{0}$. Таким образом, корнями ε полинома (41) в пространстве изображений являются $\varepsilon_1 = 3$ и $\varepsilon_2 = 11$. Обратные значения корней $\beta = \overline{\varepsilon}$, равные $15 - \varepsilon$, как раз и определяют номера позиций (символов) входного кодового слова $\boldsymbol{C}^*$, которые поражены помехой. Следовательно, искаженные символы находятся на позициях $\beta_1 = 15 - \varepsilon_1 = 12$ и $\beta_2 = 4$, т.е. как раз на тех позициях, которые определены моделью (вектором) помехи (22).

Таблица 3

К определению корней полинома (41)

i	$\hat{\Lambda}^{(2)}(i)$	Решение	i	$\hat{\Lambda}^{(2)}(i)$	Решение
1	$0\hat{+}7\hat{+}3 \neq \overline{0}$	—	8	$0\hat{+}14\hat{+}2 \neq \overline{0}$	—
2	$0\hat{+}8\hat{+}5 \neq \overline{0}$	—	9	$0\hat{+}0\hat{+}4 \neq \overline{0}$	—
3	$0\hat{+}9\hat{+}7 = \overline{0}$	Корень	10	$0\hat{+}1\hat{+}6 \neq \overline{0}$	—
4	$0\hat{+}10\hat{+}9 \neq \overline{0}$	—	11	$0\hat{+}2\hat{+}8 = \overline{0}$	Корень
5	$0\hat{+}11\hat{+}11 \neq \overline{0}$	—	12	$0\hat{+}3\hat{+}10 \neq \overline{0}$	—
6	$0\hat{+}12\hat{+}13 \neq \overline{0}$	—	13	$0\hat{+}4\hat{+}12 \neq \overline{0}$	—
7	$0\hat{+}13\hat{+}0 \neq \overline{0}$	—	14	$0\hat{+}5\hat{+}14 \neq \overline{0}$	—

Теперь переходим к вычислению пока неизвестных значений ошибок e_i, $i=\overline{1,t}$. С этой целью можно воспользоваться системой синдромных уравнений, которые в пространстве изображений отображаются в матричной форме следующим образом:

$$\begin{bmatrix} \beta_1 & \beta_2 & \cdots & \beta_t \\ 2\beta_1 & 2\beta_2 & \cdots & 2\beta_t \\ \cdots & \cdots & \cdots & \cdots \\ t\beta_1 & t\beta_2 & \cdots & t\beta_t \end{bmatrix} \cdot \begin{bmatrix} e_1 \\ e_2 \\ \cdots \\ e_t \end{bmatrix} = \begin{bmatrix} \boldsymbol{S}_1 \\ \boldsymbol{S}_2 \\ \cdots \\ \boldsymbol{S}_t \end{bmatrix}. \qquad (42)$$

Поскольку для рассматриваемого примера $t=2$, то система уравнений (42) примет вид:

$$\begin{bmatrix} \beta_1 & \beta_2 \\ 2\beta_1 & 2\beta_2 \end{bmatrix} \cdot \begin{bmatrix} e_1 \\ e_2 \end{bmatrix} = \begin{bmatrix} \boldsymbol{S}_1 \\ \boldsymbol{S}_2 \end{bmatrix}. \qquad (43)$$

Подставив в (43) полученные ранее значения номеров β повреждённых символов в кодовом слове $\boldsymbol{C}^*$ и синдромов $\boldsymbol{S}$ этого слова, имеем:

$$\begin{bmatrix} 12 & 4 \\ 9 & 8 \end{bmatrix} \cdot \begin{bmatrix} e_1 \\ e_2 \end{bmatrix} = \begin{bmatrix} 6 \\ 14 \end{bmatrix}. \qquad (44)$$

Чтобы найти значения ошибок e_1 и e_2, нужно определить обратную (Inv) матрицу $(\bar{\boldsymbol{M}}^{(2)})$ для уравнения (44):

$$\bar{\boldsymbol{M}}^{(2)} = Inv \begin{bmatrix} 12 & 4 \\ 9 & 8 \end{bmatrix} = \frac{\begin{bmatrix} 8 & 4 \\ 9 & 12 \end{bmatrix}}{(8+12)\hat{+}(4+9)} = \frac{\begin{bmatrix} 8 & 4 \\ 9 & 12 \end{bmatrix}}{5\hat{+}13} = \frac{\begin{bmatrix} 8 & 4 \\ 9 & 12 \end{bmatrix}}{7}$$

и далее

$$\bar{\boldsymbol{M}}^{(2)} = 8 \cdot \begin{bmatrix} 8 & 4 \\ 9 & 12 \end{bmatrix} = \begin{bmatrix} 8+8 & 4+8 \\ 9+8 & 12+8 \end{bmatrix} = \begin{bmatrix} 1 & 12 \\ 2 & 5 \end{bmatrix}.$$

Проверка

$$\boldsymbol{M}^{(2)} \cdot \bar{\boldsymbol{M}}^{(2)} = \begin{bmatrix} 12 & 4 \\ 9 & 8 \end{bmatrix} \cdot \begin{bmatrix} 1 & 12 \\ 2 & 5 \end{bmatrix} =$$

$$= \begin{bmatrix} (12+1)\hat{+}(4+2) & (12+12)\hat{+}(4+5) \\ (9+1)\hat{+}(8+2) & (9+12)+(8+5) \end{bmatrix} = \begin{bmatrix} 13\hat{+}6 & 9+9 \\ 10+10 & 6\hat{+}13 \end{bmatrix} = \begin{bmatrix} 0 & \bar{0} \\ \bar{0} & 0 \end{bmatrix} = \hat{\boldsymbol{E}}^{(2)},$$

то есть обратная матрица $\bar{\boldsymbol{M}}^{(2)}$ вычислена правильно.

Определим из уравнения (44) значения ошибок

$$\begin{bmatrix} e_1 \\ e_2 \end{bmatrix} = \bar{\boldsymbol{M}}^{(2)} \cdot \begin{bmatrix} 6 \\ 14 \end{bmatrix} = \begin{bmatrix} 1 & 12 \\ 2 & 5 \end{bmatrix} \cdot \begin{bmatrix} 6 \\ 14 \end{bmatrix} =$$

$$\begin{bmatrix} (1+6)\hat{+}(12+14) \\ (2+6)\hat{+}(5+14) \end{bmatrix} = \begin{bmatrix} 7\hat{+}11 \\ 8\hat{+}4 \end{bmatrix} = \begin{bmatrix} 8 \\ 5 \end{bmatrix}.$$

Следовательно $e_1=8$ и $e_2=5$, что совпадает с условием (22). Коррекция кодового слова $\hat{\boldsymbol{C}}^*$ осуществляется в результате суммирования (с помощью оператора $\hat{+}$) вычисленных ошибок со значениями **8** и **6** искаженных разрядов в (23). Тем самым получим $e_1\hat{+}8=8\hat{+}8=\bar{0}$ и $e_2\hat{+}6=5\hat{+}6=9$, что приводит к восстановлению исходного слова $\hat{\boldsymbol{C}}$, заданного формулой (21).

ВЫВОДЫ

Коды Рида-Соломона являются эффективными и широко распространенными кодами, применяемыми во многих областях науки и техники, связанными с помехоустойчивым преобразованием (приёма-передачей) цифровой информации. С момента его появления (1960) и до настоящего времени описание РС-кода, включая синтез кодовых слов, а также локализацию и устранение ошибок, базируется на использовании формальных элементов, которыми являются корни генераторных, информационных и проверочных полиномов. Перегруженность технологических операций такими алгебраическими элементами является в определенной мере «балластом», не только усложняющим процесс вычислений в аппаратно-программной реализации, но и создающим определенные затруднения при изучении алгоритмов РС-кодирования и декодирования. В связи с этим в работе предложен вариант построения РС-кодов, значительно упрощающий как освоение самого алгоритма, так и процесс обнаружения и устранения ошибок в искаженных данных. Предложения основаны на переносе преобразований из пространства оригиналов в пространство изоморфного изображения. В результате предлагаемой замены вычислительный процесс оказывается

сведенным к простым операциям модулярной арифметики над целочисленными операндами, легко реализуемыми средствами компьютерной техники.

ЛИТЕРАТУРА

[1]. Р. Блейхут, *Теория и практика кодов, контролирующих ошибки: Пер. с англ.,* М.: Мир, 1986, 576 с.

[2]. Э. Берлекэмп, *Алгебраическая теория кодирования*: *Пер. с англ.,* М.: Мир, 1971, 478 с.

[3]. У. Питерсен, Э. Уэндон, *Коды, исправляющие ошибки*: *Пер. с англ.*, М.: Мир, 1976, 593 с.

[4]. П. Рахман, *Кодирование информации с применением кодов Рида-Соломона.* [Электронный ресурс]. Режим доступа: http://bugtraq.ru/library/crypto/.keep/rscodes.pdf.

[5]. А. Белецкий, Д. Конюший, Д. Полторацкий, "Систематические байт-ориентированные коды", *Захист інформації*, Том. 20, № 1, С. 18-31, 2018.

[6]. С. Федоренко, *Методы быстрого декодирования линейных блоковых кодов*: *Моногр.*, СПб: ГУАП, 2008, 199 с.

[7]. С. Бернард, *Цифровая связь. Теоретические основы и практическое применение: Пер. с англ.*, М.: Изд. дом «Вильямс», 2004, 1104 с.

КОДУВАННЯ І ДЕКОДУВАННЯ СИСТЕМАТИЧНИХКОДІВ РІДА-СОЛОМОНА ЗА МЕТОДОМ, АЛЬТЕРНАТИВНОГО АЛГОРИТМУ ПІТЕРСОНА-ГОРЕНШТЕЙНА-ЦІРЛЕРА

Коди Ріда-Соломона є ефективними і широко використовуються в багатьох областях науки і техніки, пов'язаними з перешкодостійким перетворенням (прийому-передачею) цифрової інформації. З моменту появи (1960) і до теперішнього часу опис РС-коду, включаючи синтез кодових слів, а також локалізацію і усунення помилок, базується на використанні формальних елементів, якими є коріння генераторних, інформаційних і перевірочних поліномів. Перевантаженість технологічних операцій алгебраїчними елементами є в певній мірі «баластом», що не тільки ускладнює процес обчислень в апаратно-програмної реалізації, а й створює певні труднощі при вивченні алгоритмів РС-кодування і декодування. У зв'язку з цим в роботі запропоновано варіант побудови РС-кодів, що значно спрощує як засвоєння самого алгоритму, так і процес виявлення і усунення помилок в спотворених даних. Пропозиції засновані на перенесенні перетворень з простору оригіналів в простір ізоморфного зображення. В результаті запропонованої заміни обчислювальний процес виявляється зведеним до простих операцій модулярної арифметики над цілочисельними операндами, що легко реалізується засобами комп'ютерної техніки.

Ключові слова: коди Ріда-Соломона, поля Галуа, утворюючі поліноми, матриці перевірочних символів, ізоморфні перетворення.

CODING AND DECODING OF SYSTEMATIC RIDA-SOLOMON CODES BY METHOD, WHICH ALTERNATIVE OF ALGORITHM OF PETERSON-GORENSTEIN-ZIRLER

Reed-Solomon codes are effective and widely used in many fields of science and technology related to noise-immune conversion (reception-transmission) of digital information. Since the advent of (1960) and up to now, the description of the PC-code, including the synthesis of code words, as well as the localization and elimination of errors, is based on the use of formal elements, which are the roots of generator, information and test polynomials. The congestion of technological operations by algebraic elements is to a certain extent "ballast", which not only complicates the computation process in the hardware-software implementation, but also creates certain difficulties in the study of PC-encoding and decoding algorithms. In this regard, the paper proposes a variant of constructing PC-codes, greatly simplifying both the mastering of the algorithm itself and the process of detecting and eliminating errors in distorted data. Proposals are based on the transfer of transformations from the space of originals to the space of an isomorphic image. As a result of the proposed replacement, the computational process turns out to be reduced to simple operations of modular arithmetic over integer operands easily realized by computer hardware.

Keywords: Reed-Solomon codes, Galois fields, forming polynomials, matrices of parity symbols, isomorphic transformations.

Белецкий Анатолий Яковлевич, доктор технических наук, профессор, Заслуженный деятель науки и техники Украины, лауреат Гос. премии Украины в области науки и техники, профессор кафедры электроники Национального авиационного университета.
E-mail: abelnau@ukr.net.

Білецький Анатолій Якович, доктор технічних наук, професор, Заслужений діяч науки і техніки України, лауреат Державної премії України в галузі науки і техніки, професор кафедри електроніки Національного авіаційного університету.

Beletsky Anatoly, Doctor of Science, Professor, Honored Scientist of Ukraine, Laureate of the State Prize of Ukraine in Science and Technology, Professor of Department Electronics of National Aviation University.