О. С. Когновицкий, В. М. Охорзин

ТЕОРИЯ ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ

ПРАКТИКУМ

САНКТ-ПЕТЕРБУРГ
2013

ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

Федеральное государственное
образовательное бюджетное учреждение
высшего профессионального образования
«САНКТ-ПЕТЕРБУРГСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ
им. проф. М. А. БОНЧ-БРУЕВИЧА»

О. С. Когновицкий, В. М. Охорзин

ТЕОРИЯ ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ

ПРАКТИКУМ

СПбГУТ)))

САНКТ-ПЕТЕРБУРГ
2013

УДК 621.301(077)
ББК 32.811я73
К57

Рецензент
доктор технических наук,
профессор кафедры обработки и передачи дискретных сообщений
В. И. Комашинский

Рекомендован к печати
редакционно-издательским советом СПбГУТ

Когновицкий, О. С.

К57 Теория помехоустойчивого кодирования : практикум / О. С. Когновицкий, В. М. Охорзин ; СПбГУТ. – СПб., 2013. – 68 с.

Содержатся методические указания к лабораторным занятиям и вопросы, подлежащие проработке в ходе проведения практических занятий со студентами по дисциплинам: «Математическая теория помехоустойчивого кодирования» (для бакалавров), «Современные проблемы помехоустойчивого кодирования» (для магистров) по теме «Помехоустойчивые коды».

Темы лабораторных работ и практических занятий связаны с построением и исследованием процедур кодирования и декодирования современных помехоустойчивых кодов. Учитывая сложность изучаемых вопросов, отсутствие адаптированных учебных пособий и трудную доступность научно-технической литературы по теме занятий, авторы включили в издание в достаточно полном объеме необходимый теоретический материал, снабдив его многочисленными примерами и задачами с пояснениями методов решения типовых задач.

Предназначено для студентов, обучающихся по специальностям: 210700.68 «Инфокоммуникационные технологии и системы связи», 210700.68 «Инфокоммуникационные технологии в сервисах и услугах связи», 210700.62 «Сети связи и системы коммутации».

Материалы пособия могут быть использованы для подготовки студентов, обучающихся по всем техническим специальностям.

УДК 621.301(077)
ББК 32.811я73

СОДЕРЖАНИЕ

ПРЕДИСЛОВИЕ

В современных телекоммуникационных системах для повышения достоверности передаваемых сообщений широкое применение получили циклические коды БЧХ. Наиболее перспективным в настоящее время является частный случай кодов БЧХ – коды Рида–Соломона. Разработанные для этих кодов методы быстрого декодирования позволяют решать задачи декодирования с исправлением любых ошибок в пределах гарантийной исправляющей способности применяемого кода. Наряду с этим ведутся активные работы по поиску методов декодирования, позволяющих исправлять ошибки, кратность которых превышает гарантийную. Одним из перспективных классов кодов, позволяющих решать эту задачу, являются коды БЧХЭ. Разработанный для этих кодов метод мажоритарного декодирования с применением двойственного базиса открывает возможность исправления значительной части ошибок за пределами гарантийно исправляемых ошибок.

Предлагаемое издание имеет целью сделать доступным для обучаемых освоение современных методов кодирования и декодирования кодов Рида–Соломона, основанных на алгоритме Евклида, а также методов кодирования и декодирования кодов БЧХЭ с применением двойственного базиса. Учебные вопросы, включенные в практикум, отрабатываются на двух видах занятий: в ходе выполнения двух лабораторных работ и двух практических занятий. Одно лабораторное занятие посвящено исследованию принципов кодирования и декодирования кодов БЧХЭ, а другое – исследованию принципов кодирования и декодирования кодов Рида–Соломона с использованием алгоритма Евклида. Методические указания к каждой работе содержат теоретическую часть, изучение которой даст обучаемому студенту необходимые теоретические сведения для понимания процедур кодирования и декодирования рассматриваемых кодов. Базовые теоретические сведения закрепляются и углубляются на двух практических занятиях. В целях расширения теоретической подготовки и привития навыков работы с научно-технической литературой на практических занятиях предполагается заслушивание и обсуждение рефератов, самостоятельно подготовленных студентами по теме занятий. Проверка степени усвоения изучаемого материала осуществляется решением предлагаемых задач. Приведены примеры решения типовых задач. Успешное выполнение программы практикума требует от обучаемых знания основ помехоустойчивого кодирования и принципов построения кодов БЧХ.

Авторы выражают признательность выпускникам СПбГУТ О. Ю. Брянцевой, А. И. Загрядской, Е. В. Заниной, А. О. Говоровой и И. Г. Петрову, принявшим активное участие в разработке программного обеспечения представленных лабораторных работ.

Лабораторная работа 1

ИССЛЕДОВАНИЕ ПРИНЦИПОВ КОДИРОВАНИЯ И ДЕКОДИРОВАНИЯ КОДОВ БЧХЭ

1.1. Цель работы

Изучить принципы кодирования и декодирования кодов БЧХЭ, получить навыки в построении кодов БЧХЭ с заданными корректирующими свойствами, а также в построении и анализе работы кодирующих и декодирующих устройств этих кодов. Исследовать возможность и механизм коррекции кодами БЧХЭ ошибок, кратность которых превышает гарантийно исправляемую.

1.2. Задание на лабораторную работу

1. Для кода БЧХЭ (15,6) с заданным характеристическим многочленом $P(x) = (x^4 + x + 1)(x^2 + x + 1) = p_0x^6 + p_1x^5 + p_2x^4 + p_3x^3 + p_4x^2 + p_5x + p_6 = x^6 + x^5 + x^4 + x^3 + 1$ построить схему кодера и с ее помощью сформировать кодовую комбинацию $f(x)$ по заданной информационной последовательности (C, D), где C – последовательность из четырех информационных символов, являющаяся элементом поля $GF(2^4)$, а D – последовательность из двух информационных символов, являющаяся элементом поля $GF(2^2)$.

2. Построить схему декодера и декодировать принятую последовательность $v_1(x) = f(x) + e_1(x)$, где $e_1(x)$ – гарантийно исправляемый кодом БЧХЭ (15,6) многочлен ошибок, $f(x)$ – комбинация кода (15,6), сформированная в п. 1.

3. Выполнить декодирование последовательности $v_2(x) = f(x) + e_2(x)$, где $e_2(x)$ – неисправляемый кодом БЧХЭ (15,6) многочлен ошибок.

4. Децимировать последовательность $v_2(x) = f(x) + e_2(x)$ с индексом два и выполнить декодирование децимированной последовательности $v_2(x) = f(x) + e_2(x)$.

Перед началом выполнения работы необходимо изучить теоретические сведения по кодам БЧХЭ, приведенные в разд. 4, и процедуры кодирования и декодирования кода БЧХЭ (15,6), приведенные в разд. 5. Проверку готовности к выполнению работы можно оценить по возможности дать ответы на контрольные вопросы.

1.3. Варианты задания

Варианты задания приведены в табл. 3.1.

Таблица 3.1

№ варианта	(C,D)	$e_1(x)$	$e_2(x)$
1	(ε^1, μ^0)	$x^{14}+x^{13}$	$x^{13}+x^{11}+x^9$
2	(ε^2, μ^1)	$x^{13}+x^{12}$	$x^{12}+x^{10}+x^8$
3	(ε^3, μ^2)	$x^{12}+x^{11}$	$x^{11}+x^9+x^7$
4	(ε^4, μ^0)	$x^{11}+x^{10}$	$x^{10}+x^8+x^6$
5	(ε^5, μ^1)	$x^{10}+x^9$	$x^9+x^7+x^5$
6	(ε^6, μ^2)	x^9+x^8	$x^8+x^6+x^4$
7	(ε^7, μ^0)	x^8+x^7	$x^7+x^5+x^3$
8	(ε^8, μ^1)	x^7+x^6	$x^6+x^4+x^2$
9	(ε^9, μ^2)	x^6+x^5	$x^5+x^3+x^1$
10	$(\varepsilon^{10}, \mu^0)$	x^5+x^4	$x^4+x^2+x^0$
11	$(\varepsilon^{11}, \mu^1)$	x^4+x^3	$x^{14}+x^8+x^6$
12	$(\varepsilon^{12}, \mu^2)$	x^3+x^2	$x^{13}+x^9+x^5$
13	$(\varepsilon^{13}, \mu^0)$	x^2+x^1	$x^{12}+x^8+x^4$
14	$(\varepsilon^{14}, \mu^1)$	x^1+x^0	$x^{11}+x^7+x^3$
15	(ε^1, μ^2)	x^0+x^{14}	$x^{10}+x^6+x^2$
16	(ε^2, μ^0)	$x^{14}+x^{12}$	$x^9+x^5+x^1$
17	(ε^3, μ^1)	$x^{14}+x^{11}$	$x^8+x^4+x^0$
18	(ε^4, μ^2)	$x^{14}+x^{10}$	$x^{14}+x^{13}+x^6$
19	(ε^5, μ^0)	$x^{14}+x^9$	$x^{13}+x^{12}+x^5$
20	(ε^6, μ^1)	$x^{14}+x^4$	$x^{12}+x^8+x^4$
21	(ε^7, μ^2)	$x^{14}+x^3$	$x^{11}+x^{10}+x^3$
22	(ε^8, μ^0)	$x^{14}+x^2$	$x^{10}+x^9+x^2$
23	(ε^9, μ^1)	$x^{14}+x^1$	$x^9+x^8+x^1$
24	$(\varepsilon^{10}, \mu^2)$	$x^{13}+x^0$	$x^8+x^7+x^0$
25	$(\varepsilon^{11}, \mu^0)$	$x^{12}+x^0$	$x^{14}+x^7+x^6$

Здесь символы $C = \varepsilon^i$ и $D = \mu^j$, являются элементами поля $GF(2^4)$ и $GF(2^2)$ соответственно (табл. 5.2, 5.3).

1.4. Теоретические сведения

В настоящее время в технике связи широко используются циклические коды. Вопросу описания циклических кодов, методов их кодирования и декодирования посвящено значительное число научных и научно-методических работ. В монографии профессора О. С. Когновицкого [1] разработаны коды БЧХЭ, методы их кодирования и декодирования, исследована эффективность этих кодов. Лабораторная работа посвящена изучению методов кодирования и декодирования кодов БЧХЭ, описанных в монографии [1], и исследованию эффективности метода декодирования этих кодов. Коды БЧХ – это циклические коды, конструкция которых определяется заданием корней порождающего многочлена [2]. БЧХ код с кодовым расстоянием $d_{\min} \geq 2t + 1$ является циклическим кодом, порождающий многочлен которого имеет $2t$ последовательных корней $\alpha^b, \alpha^{b+1}, \ldots \alpha^{b+2t-1}$, где

α – примитивный элемент некоторого расширенного поля Галуа GF(2^m). Теория кодов БЧХ позволяет создавать коды с заданными свойствами. Достаточно простые методы кодирования и декодирования этих кодов способствовали их широкому распространению в различных областях связи. Недостатком используемых синдромных процедур декодирования кодов БЧХ является неспособность использовать все возможности этих кодов для исправления ошибок. Все известные методы декодирования позволяют исправить только $\sum_{i=1}^{t} C_n^i$ различных ошибок при потенциальной возможности исправления 2^{n-k} ошибок. Заметим, что $\sum_{i=1}^{t} C_n^i = 2^{n-k}$ только для кодов Хемминга и Голея [2]. В приведенных формулах n, k, t – длина кодовой комбинации, число информационных элементов и кратность гарантийно исправляемых кодом ошибок соответственно.

Код БЧХЭ – циклический (n, k)-код, построенный по некоторому многочлену $P(x)$ степени k, является эквивалентным циклическому (n, k)-коду с порождающим многочленом $G(x) = (x^n - 1) / P(x)$, т. е. для соответствующего кода БЧХ $P(x)$ является проверочным многочленом. Чтобы избежать путаницы в названиях, далее многочлен $P(x)$ будет называться проверочным и в отношении кодов БЧХЭ. Причем $P(x)$ в общем случае является разложимым, т. е. представляет собой произведение нескольких неприводимых многочленов. Комбинации (n, k)-кода БЧХЭ рассматриваются как рекуррентные (возвратные) последовательности в общем случае с приводимым (разложимым) характеристическим многочленом степени k. Этим многочленом является проверочный многочлен кода $P(x)$. Для декодирования комбинаций (n, k)-кода БЧХЭ используется аппарат двойственного базиса расширенного поля Галуа GF(2^m).

Поскольку коды БЧХЭ эквивалентны кодам БЧХ, то и для них существует возможность создавать коды с заранее заданными свойствами. Процедура декодирования с использованием двойственного базиса проста в аппаратной реализации и позволяет исправлять большее, чем $\sum_{i=1}^{t} C_n^i$ число ошибок. Рассмотрим теоретические основы, положенные в основу кодов БЧХЭ.

1.4.1. Базисы поля Галуа

Расширенное поле Галуа GF(p^m) является векторным пространством размерности m над простым полем GF(p). Любое множество из m линейно независимых элементов GF(p^m) может быть выбрано в качестве базиса этого векторного пространства. При задании поля GF(p^m) примитивным неприводимым многочленом $\pi(x)$ в качестве базиса обычно выбираются эле-

менты поля GF(p^m) : {1, α, α^2,…, α^{m-1}}, где α – корень многочлена π(x). Такой базис называют каноническим, или левым степенным. Все базисные элементы поля GF(p^m) при представлении их последовательностями длины m из поля GF(p) содержат по одной единице в различных разрядах при нулевых значениях остальных разрядов. В ряде приложений используют нормальный базис {γ, γ^2, γ^4,…, $\gamma^{2^{m-1}}$}, где γ – некоторый элемент GF(p^m).

Из теории конечных полей [3] известно, что в любом поле существует хотя бы один нормальный базис. Кроме того, и для канонического, и для нормального базисов имеются двойственные базисы. Для определения двойственного базиса рассмотрим понятие функции-след.

След (функция-след). Сумма $T_m(\beta) = \beta + \beta^p + \beta^{p^2} + \ldots + \beta^{p^{m-1}} = \sum_{j=0}^{m-1} \beta^{p^j}$ называется следом (функцией-след) элемента β, принадлежащего полю GF(p^m). Ниже приводятся некоторые полезные свойства [4] функции-след.

- След элемента β из поля GF(p^m) $T_m(\beta)$ принимает одно из значений простого поля GF(p), т. е. $T_m(\beta)$ отображает элемент β поля GF(p^m) на некоторый элемент поля GF(p). В частности, след элемента расширенного поля GF(2^m) равен либо 0, либо 1.
- Каждое из значений в GF(p) функция-след $T_m(\beta)$ для различных β из GF(p^m) принимает одинаковое число раз, т. е. p^{m-1} раз.
- Справедливо: $T_m(\beta + \gamma) = T_m(\beta) + T_m(\gamma)$, где β, γ – элементы поля GF(p^m).

Далее будем рассматривать только поля характеристики p =2.

Двойственные (дополнительные) базисы. Пусть K – конечное поле и F – его конечное расширение степени m. Тогда два базиса {α_1,…,α_m} и {β_1,…,β_m} поля F над K называются *дуальными (двойственными)*, если для $1 \le i, j \le m$ [3]:

$$T_{q/p}(\alpha_i \beta_j) = \begin{cases} 0 \text{ при } i \neq j, \\ 1 \text{ при } i = j. \end{cases}$$

Рекуррентные последовательности. Пусть имеется последовательность $U = u_0, u_1, u_2, \ldots, u_s$ и для каждых k+1 ее элементов, начиная с некоторого $n < s$, справедливо:

$$u_{n+k} = p_1 u_{n+k-1} + p_2 u_{n+k-2} + \ldots + p_k u_n + a \ (n \ge 0),$$

где $p_1, p_2, \ldots, p_k$ – коэффициенты, элементы конечного поля.

Такое уравнение называют возвратным, или рекуррентным уравнением порядка k. Если $a = 0$, то рекуррентное уравнение называют однородным и неоднородным – в противном случае. Последовательность U называют периодической, когда для любых целых положительных n и m $u_{n+m} = u_n$.

Число m называют периодом последовательности. Если $n = 0$, то последовательность является полностью периодической с периодом m и называется возвратной, или рекуррентной. Любая линейная однородная рекуррентная последовательность U k-го порядка над полем GF(p) является полностью периодической с периодом $m \le p^k - 1$. Линейная однородная рекуррентная последовательность k-го порядка над полем GF(p) с периодом $p^k - 1$ является последовательностью максимальной длины. При этом период $p^k - 1$ является делителем максимального периода рекуррентной последовательности U.

Каждой линейной однородной рекуррентной последовательности k-го порядка над простым полем с характеристикой p соответствует характеристический многочлен

$$P(x) = p_0x^k - p_1x^{k-1} - p_2x^{k-2} - \ldots - p_{k-1}x - p_k,\ p_i \in \mathrm{GF}(p).$$

Одним из свойств однородных линейных рекуррентных последовательностей является то, что любой ее элемент u_n может быть вычислен [3]. Так: $u_n = \sum_{i=1}^{k} c_i\varepsilon_i^n$, $n = 0, 1, 2\ldots$, где $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_k$ – корни характеристического многочлена $P(x)$, $c_1, c_2, \ldots, c_k$ – элементы расширенного поля GF(p^k), которые однозначно определяются первыми k элементами последовательности $(u_0, u_1, \ldots, u_{k-1})$.

Запишем это выражение в виде системы уравнений:

$$\begin{cases} u_n = c_1\varepsilon_1^{\,n} + c_2\varepsilon_2^{\,n} + \ldots + c_k\varepsilon_k^{\,n} \\ u_{n+1} = c_1\varepsilon_1^{\,n+1} + c_2\varepsilon_2^{\,n+1} + \ldots + c_k\varepsilon_k^{\,n+1} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ u_{n+k-1} = c_1\varepsilon_1^{\,n+k-1} + c_2\varepsilon_2^{\,n+k-1} + \ldots + c_k\varepsilon_k^{\,n+k-1}. \end{cases}$$

Здесь неизвестными выступают коэффициенты $c_1, c_2, \ldots, c_k$. Зная их, можно вычислить любой элемент последовательности.

Для решения этой системы составляется матрица A:

$$A = \begin{pmatrix} \varepsilon_1^{\,n} & \varepsilon_2^{\,n} & \ldots & \varepsilon_k^{\,n} \\ \varepsilon_1^{\,n+1} & \varepsilon_2^{\,n+1} & \ldots & \varepsilon_k^{\,n+1} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \varepsilon_1^{\,n+k-1} & \varepsilon_2^{\,n+k-1} & \ldots & \varepsilon_k^{\,n+k-1} \end{pmatrix} = \begin{pmatrix} \gamma_1 & \gamma_1^{\,2} & \ldots & \gamma_1^{\,2^{k-1}} \\ \gamma_2 & \gamma_2^{\,2} & \ldots & \gamma_2^{\,2^{k-1}} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \gamma_k & \gamma_k^{\,2} & \ldots & \gamma_k^{\,2^{k-1}} \end{pmatrix}$$

Таким образом, получаем уравнение: U=A*C, где U, C – матрица-столбец, содержащая элементы (u_n, u_{n+1},..., u_{n+k-1}) и (c_1, c_2,..., c_k) соответственно. Решением уравнения будет: $C=A^{-1}*U$.

Находим A^{-1}:

$$A^{-1}=\begin{pmatrix} \omega_1 & \omega_2 & \dots & \omega_k \\ \omega_1^2 & \omega_2^2 & \dots & \omega_k^2 \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot^{k-1} & \cdot^{k-1} & & \cdot^{k-1} \\ \omega_1^{k-1} & \omega_2^{k-1} & \dots & \omega_k^{k-1} \end{pmatrix}$$

Если рассматривать элементы матрицы A (γ_1, γ_2,...,γ_k) как базис, то элементы обратной матрицы A^{-1} (ω_1, ω_2,...,ω_k) представляют двойственный базис, так как имеет место равенство:

$$A*A^{-1}=E.$$

Каждый элемент двойственного базиса находится из соотношения:

$$\omega_i=\frac{A_{i1}}{D},\ \omega_i\in GF(p^k),$$

где D – определитель матрицы A,

A_{i1} – алгебраическое дополнение элемента a_{i1} определителя матрицы A. В [1] автором доказывается следующая теорема, которая позволяет достаточно легко найти элементы двойственного базиса.

Теорема 1. Если степенной базис (γ_1, γ_2,..., γ_k) поля $GF(p^k)$ равен (ε^n,ε^{n+1}, ..., ε^{n+k-1}), где ε – корень примитивного многочлена $\pi(x)$ степени k, то двойственный базис (ω_1, ω_2,...,ω_k) определяется выражением:

$$\omega_i=\varepsilon^{-n}*\alpha_i;\quad i=1,2,...,k,$$

$$\alpha_i=\frac{\sum_{l=0}^{k-l}p_{k-i-l}\varepsilon^l}{P'(\varepsilon)},\ \alpha_i\in GF(p^k),$$

где p_m – коэффициенты характеристического многочлена P(x).

Вернемся к задаче нахождения коэффициентов c_1, c_2, ..., c_k.

В [1] показано, что значение c_1 определяется так:

$$c_1=\sum_{i=1}^{k}\frac{A_{i1}}{D}u_{n+i-1}=\sum_{i=1}^{k}\omega_i u_{n+i-1}=\varepsilon_1^{-n}\sum_{i=1}^{k}\alpha_i u_{n+i-1}=\frac{\varepsilon_1^{-n}}{P'(\varepsilon)}\sum_{i=1}^{k}[\sum_{l=0}^{k-i}p_{k-i-l}\varepsilon_1^l]u_{n+i-1}.$$

Остальные коэффициенты c_2, ..., c_k в общем виде определяются выражением для c_1 с той лишь разницей, что вместо корня ε_1 будет ε_j. Если также учесть, что $\varepsilon_j=\varepsilon_1^{p^{j-1}}$, то становится очевидным равенство $c_2=(c_1)^p$. Заме-

ним c_1 на c, и тогда: $c_2=(c)^p$, а все остальные коэффициенты равны $c_3=c^{p^2}$, …, $c_k=c^{p^{k-1}}$, где p – характеристика простого поля GF(p).

Поэтому для решения задачи определения начальных элементов рекуррентной последовательности по ее произвольному k-элементному участку достаточно вычислить c и тогда любой элемент кодовой последовательности будет определяться так:

$$u_m = \sum_{i=1}^{k} c_i \varepsilon_i^m = \sum_{i=1}^{k} (c)^{p^{i-1}} \varepsilon_i^m = \sum_{i=1}^{k} \left[c\varepsilon_1^{\,m} \right]^{p^{i-1}} = T(c\varepsilon_1^{\,m}),$$

где m – расстояние искомого элемента от начала последовательности.

Таким образом, рекуррентную последовательность $\{u\}$ можно записать так:

$$\{u\}=\{\mathrm{T}(c), \mathrm{T}(c\varepsilon), \mathrm{T}(c\varepsilon^2), \ldots, \mathrm{T}(c\varepsilon^{n-2}), \mathrm{T}(c\varepsilon^{n-1})\}.$$

Децимация. Как известно, одним из ценных свойств последовательностей максимальной длины, является свойство децимации (или разрядки) [3]. Это свойство заключается в том, что если из элементов последовательности $\{s\}=(s_0 s_1 \ldots s_{2^k-1})$ составить другую последовательность $\{v\}=(v_0 v_1 \ldots v_{2^k-1})$, где $v_j = s_{qj}$, а $q = 2^i$ – индекс децимации, $i = 0, 1, \ldots, (k-1)$, то разряженная последовательность $\{v\}$ также будет последовательностью максимальной длины с тем же периодом и удовлетворяющей тому же рекуррентному правилу, что и последовательность $\{s\}$.

Следовательно, к последовательности $\{v\}$ могут быть применены такие же алгоритмы обработки, что и к последовательности $\{s\}$. Комбинации кодов БЧХЭ в общем случае представляют собой поэлементные суммы r последовательностей максимальной длины, потому можно ожидать, что процедура децимации применима также и к комбинациям кодов БЧХЭ.

В [1] доказана следующая теорема.

Теорема 2. Если последовательность $\{s\}=(s_0, s_1, \ldots s_{2^k-1})$, являющуюся кодовой комбинацией кода БЧХЭ над полем GF(2^k), удовлетворяющую некоторому рекуррентному уравнению, подвергнуть децимации с индексом $q = 2^i$, $i = 0, 1, \ldots, (k-1)$, то полученная последовательность $\{v\}_q=(v_0 v_1 \ldots v_{2^k-1})$, где $v_i = s_{j\cdot q(\mathrm{mod}(2^k-1))}$, также будет удовлетворять тому же рекуррентному уравнению.

1.4.2. Кодирование кодов БЧХЭ

1.4.2.1. Кодирующее устройство кодов БЧХЭ на базе рекуррентного регистра

Известно, что линейная однородная рекуррентная последовательность $\{s\}$, порождаемая разложимым характеристическим многочленом $P(x)$ степени m с неприводимыми сомножителями степеней, не старших k, удовлетворяет условию цикличности, т. е. является кодовой комбинацией цикли-

ческого $(2^k-1, m)$ кода. Как известно [3], линейная рекуррентная последовательность может быть получена с помощью регистра сдвига с обратными связями. Кодирующее устройство такого кода будет являться регистром сдвига с обратными связями.

Регистры сдвига для линейных однородных рекуррентных последовательностей строятся из конструктивных элементов трех типов. Элементами первого типа являются сумматоры (рис. 4.1, а). Сумматоры имеют два входа и один выход, если на входах появляются два элемента поля GF(q), то на выход поступает их сумма. Элементами второго типа являются умножители (рис. 4.1, б). Умножитель имеет один вход и один выход, если на вход поступает элемент поля GF(q), то на выходе появляется произведение этого элемента на некоторый постоянный коэффициент, также принадлежащий полю GF(q). Элементом третьего типа является элемент задержки (триггер), он имеет один вход и один выход, а его работа регулируется внешними синхронизирующими часами таким образом, что элемент поля GF(q), поступивший на вход элемента на текущем такте работы, появляется на его выходе на следующем такте (рис. 4.1, в).

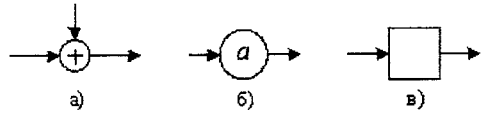


Рис. 4.1. Схематические изображения конструктивных элементов

Длина регистра определяется степенью многочлена $P(x)$, т. е. равна m ячеек, а обратные связи регистра – коэффициентами p_i характеристического многочлена $P(x)$. На выходе регистра формируется рекуррентная последовательность, благодаря чему характеристический многочлен $P(x)$ называют рекурсивным. Процедура кодирования является чрезвычайно простой: m информационных элементов исходного кода $(s_0, s_1, \ldots, s_{m-1})$ записываются в ячейки памяти регистра с обратными связями, а затем содержимое регистра сдвига последовательно считывается на его выход в течение n тактов, где n – длина комбинации циклического (n, m)-кода.

Общий вид такого кодера для кода БЧХЭ, построенного по рекурсивному многочлену $P(x)$ степени m, представлен на рис. 4.2 [3].

Часто в литературе такое устройство называют схемой решения разностных уравнений, а при этом также схема является кодером кода БЧХ, построенного по проверочному многочлену.

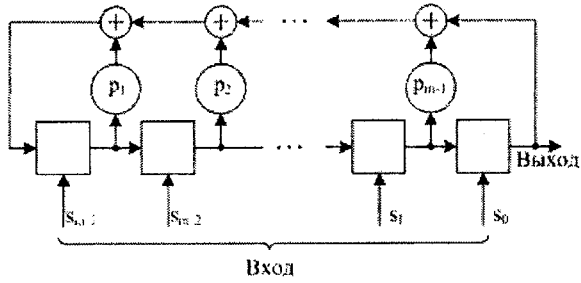


Рис. 4.2. Схема кодера кода БЧХЭ на базе рекуррентного регистра

1.4.2.2. Кодирующее устройство кода БЧХЭ на базе автономных генераторов элементов поля Галуа

Обозначим корни проверочного многочлена $P(x)$ через $\varepsilon_1, \varepsilon_2, \varepsilon_3, \ldots, \varepsilon_m$, где ε_i являются элементами поля $GF(p^k)$. При этом пусть элемент ε является корнем некоторого примитивного многочлена степени k, образующего поле $GF(p^k)$. Поскольку проверочный многочлен $P(x)$ является произведением некоторых минимальных многочленов $f_i(x)$, множеству корней многочлена $P(x)$ $\varepsilon_1, \varepsilon_2, \varepsilon_3, \ldots, \varepsilon_m$ можно поставить в соответствие объединение подмножеств, которые представляют собой циклотомические классы $C(i)$ минимальных многочленов $f_i(x)$ соответственно. Обозначим представитель циклотомического класса $C(i)$ через $\varepsilon_{i,1}$ или ε_i, а остальные его элементы через $\varepsilon_{i,j}$.

На основании теоремы 1 произвольный элемент s_n последовательности $\{s\}$, удовлетворяющий рекуррентному соотношению может быть найден по формуле:

$$s_n = \sum_{i=1}^{r} \sum_{j=1}^{k_i} c_{i,j} (\varepsilon_{i,j})^n, \qquad (4.1)$$

где r – число неприводимых многочленов $f_i(x)$ в разложении $P(x)$, k_i – старшая степень многочлена $f_i(x)$, коэффициенты $c_{i,j}$ принадлежат полю $GF(p^k)$, а их значения зависят от исходных элементов последовательности, а именно: $s_0, s_1, \ldots, s_{m-1}$.

Задачей разрешения линейных уравнений (4.1) для рекуррентных последовательностей с приводимым характеристическим многочленом является нахождение коэффициентов $c_{i,j}$.

Для нахождения значений коэффициентов $c_{i,j}$ используем метод двойственного базиса, изложенный в п. 1.4.1. В соответствии с этим методом на основании m линейных уравнений для элементов $s_n, s_{n+1}, \ldots, s_{n+m-1}$ составим матрицу A, имеющую вид:

$$A = \begin{bmatrix} \varepsilon_1^n & \varepsilon_2^n & . & \varepsilon_m^n \\ \varepsilon_1^{n+1} & \varepsilon_2^{n+1} & . & \varepsilon_m^{n+1} \\ . & . & . & . \\ \varepsilon_1^{n+m+1} & \varepsilon_2^{n+m+1} & . & \varepsilon_m^{n+m+1} \end{bmatrix}$$

Затем по методике, подробно изложенной в [1], находится обратная матрица A^{-1}. Обратная матрица A^{-1} существует, так как определитель матрицы A не равен нулю:

$$|A| = (\varepsilon_1\varepsilon_2 \ldots \varepsilon_m)^n \, \Delta,$$

где Δ – определитель Вандермонда, составленный из корней проверочного многочлена $P(x)$.

Поскольку все корни разные, определитель Δ будет отличным от нуля. Произведение корней $(\varepsilon_1\varepsilon_2 \ldots \varepsilon_m)$ также по теореме Виета будет отличным от нуля, если коэффициент p_m многочлена $P(x)$ не равен нулю. Учитывая, что многочлен $P(x)$ является произведением нескольких неприводимых многочленов $f_i(x)$, коэффициент p_m всегда будет ненулевым.

Обратная матрица для случая, когда $P(x)$ является произведением r неприводимых многочленов, будет иметь следующий вид:

$$A^{-1} = \begin{bmatrix} \omega_{1,1} & \omega_{1,2} & . & \omega_{1,m} \\ \omega_{1,1}^2 & \omega_{1,2}^2 & . & \omega_{1,m}^2 \\ . & . & . & . \\ \omega_{1,1}^{k_1} & \omega_{1,2}^{k_1} & . & \omega_{1,m}^{k_1} \\ \text{----------} & & & \\ \omega_{r,1} & \omega_{r,2} & . & \omega_{r,m} \\ \omega_{r,1}^2 & \omega_{r,2}^2 & . & \omega_{r,m}^2 \\ . & . & . & . \\ \omega_{r,1}^{k_r} & \omega_{r,2}^{k_r} & . & \omega_{r,m}^{k_r} \end{bmatrix}, \omega_{i,j} = \varepsilon_i^{-n}\alpha_{i,j},$$

где ε_i – представитель циклотомического класса $C(i)$ для многочлена $f_i(x)$. Коэффициенты $\alpha_{i,j}$ в свою очередь определяются через коэффициенты p_i проверочного многочлена $P(x)$ и корни минимальных многочленов $f_i(x)$ следующим образом:

$$\alpha_{i,j} = \frac{\sum_{l=0}^{m-i} p_{m-i-l}\varepsilon_i^l}{P'(\varepsilon_i)}.$$

Тогда искомые коэффициенты $c_{i,j}$ уравнения (4.1) могут быть найдены по любому m-элементному безошибочному участку $(s_n s_{n+1} \ldots s_{n+m-1})$ принятой рекуррентной последовательности так:

$$c_{i,j} = \varepsilon_{i,j}^{-n} \sum_{l=1}^{m} s_{n+l-1} \alpha_{i,l}. \tag{4.2}$$

Учитывая, что корнями минимального многочлена $f_i(x)$ являются элементы $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{k_i}$, для которых справедливо $\varepsilon_t = \varepsilon_l^{2^{t-l}}$, получаем, что

$$c_{i,j} = (c_{i,1})^{2^{j-1}}.$$

Обозначим $c_{i,1}$ через C_i, тогда общее выражение (4.1) для определения произвольного элемента кодовой последовательности s_n запишется в следующем виде:

$$\begin{aligned} s_n &= \sum_{t=l}^{k_1} C_1^{2^{t-l}} \varepsilon_1^{2^{t-l} n} + \ldots + \sum_{t=l}^{k_i} C_i^{2^{t-l}} \varepsilon_i^{2^{t-l} n} + \ldots + \sum_{t=1}^{k_r} C_r^{2^{t-l}} \varepsilon_r^{2^{t-l} n} = \\ &= T_l(C_1 \varepsilon_1^n) + \ldots + T_i(C_i \varepsilon_i^n) + \ldots + T_r(C_r \varepsilon_r^n) = \sum_{i=l}^{r} T_i(C_i \varepsilon_i^n), \end{aligned} \tag{4.3}$$

где $T_i()$ – функция-след.

Таким образом, можно предложить способ построения кодирующего устройства кода БЧХЭ на основе вычисления функции-след. Функциональная схема кодера кода БЧХЭ, реализующего формулу (4.3), представлена на рис. 4.3, а, а блок-схема алгоритма работы этого кодера – на рис. 4.3, б.

В частном случае, если $P(x)$ является примитивным многочленом, кодер будет состоять из одного генератора элементов поля и одной схемы вычисления функции-след, на выходе которой будут появляться элементы рекуррентной последовательности.

Известно, что рекуррентная последовательность, порождаемая примитивным многочленом, является последовательностью максимальной длины. Значит, в частном случае, когда кодер построен на основе примитивного многочлена, порождается M-последовательность. А в общем случае, когда проверочный многочлен $P(x)$ является разложимым, выходные последовательности кодера будут являться поэлементными суммами по модулю 2 последовательностей максимальной длины, причем, если период какой-либо из этих последовательностей меньше $2^m - 1$, то в кодовую последовательность входит несколько ее периодов.

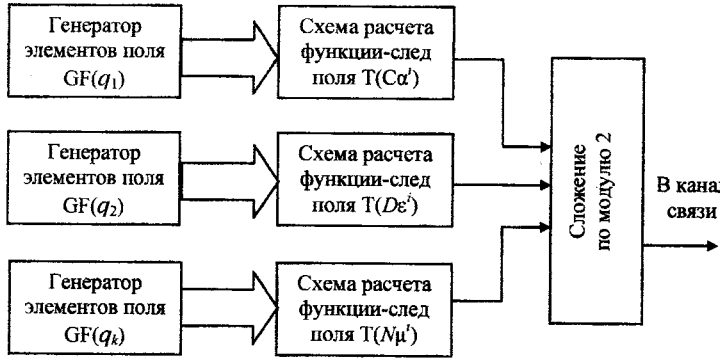


Рис. 4.3, а. Схема кодера кода БЧХЭ на основе вычисления функции-след

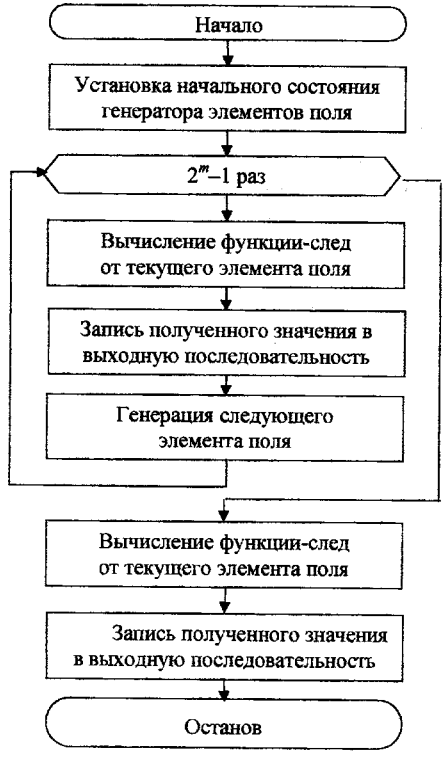


Рис. 4.3, б. Блок-схема алгоритма работы кодера кода БЧХЭ

1.4.3. Декодирование кодов БЧХЭ

Декодирование кодов БЧХЭ представляет собой мажоритарное декодирование комбинаций кодов БЧХЭ по k-элементным участкам на основе двойственного базиса $GF(p^k)$.

Поскольку комбинации кода БЧХЭ представляют собой линейные рекуррентные последовательности, декодировать код БЧХЭ означает то же самое, что найти начальные m элементов (обозначаемых C_i, где C_i элемент поля $GF(p^k)$), которые формируют переданную последовательность. Эти элементы и являются информационными в кодах БЧХЭ. Чтобы понять алгоритм декодирования кодов БЧХЭ на основе двойственного базиса, обратимся к формуле (4.1). Из нее следует, чтобы найти любые члены последовательности, в том числе и m начальных, нужно определить по принятой комбинации коэффициенты C_i. В свою очередь процедура определения этих коэффициентов описывается формулой (4.2). Если ввести в эту формулу введенные выше обозначения $c_{i,1} = C_i$ и $\varepsilon_{i,1} = \varepsilon_i$, то она примет следующий вид:

$$C_i = \varepsilon_i^{-n} \sum_{j=1}^{m} S_{n+j-1} \alpha_{i,j}.$$

С помощью этой формулы по каждому из 2^m–1 m-элементных участков замкнутого в кольцо вектора принятой последовательности S рассчитываются совместные значения коэффициентов C_i для каждого неприводимого многочлена из разложения проверочного многочлена $P(x)$. Затем принимается решение по большинству появления совместных значений C_i о том, какая комбинация была передана.

Таким образом, для построения декодера необходимо предварительно рассчитать только коэффициенты $\alpha_{i,j}$, которые однозначно определяются коэффициентами проверочного многочлена $P(x)$.

Функциональная схема декодера кода БЧХЭ представлена на рис. 4.4, а, где приняты обозначения: «$\alpha_{i,j}$» – схема умножения элемента поля на коэффициент $\alpha_{i,j}$;

«×» – схема умножения элементов расширенного поля $GF(2^{k_i})$ на элементы простого поля $GF(2)$;

«+» – схемы поразрядного сложения по модулю 2;

«МЭ» – мажоритарный элемент.

Блок-схема алгоритма работы этого декодера – на рис. 4.4, б.

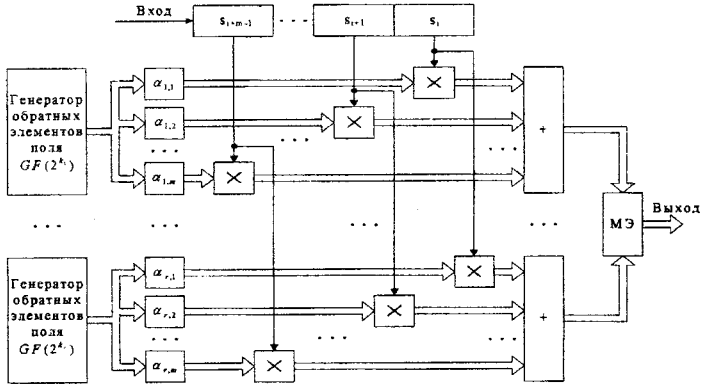


Рис. 4.4, а. Функциональная схема декодера кода БЧХЭ

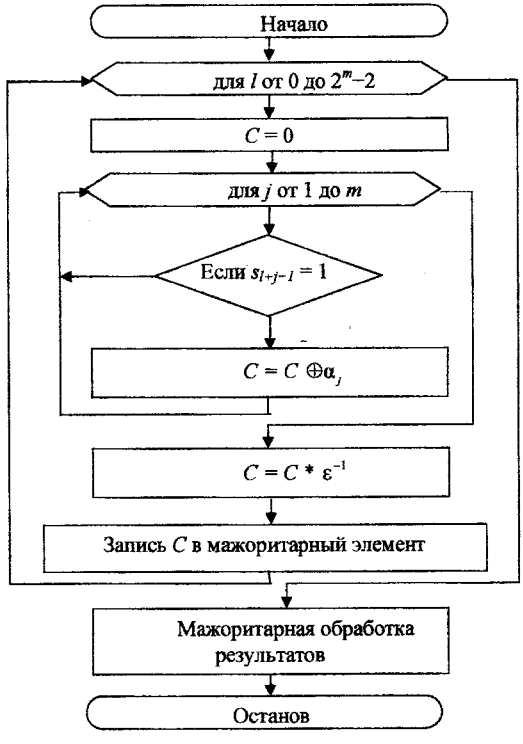


Рис. 4.4, б. Блок-схема алгоритма работы декодера кода БЧХЭ

1.5. Код (15,6) БЧХЭ

1.5.1. Характеристический многочлен

Двоичная рекуррентная последовательности длины $n = 15$ порождается примитивным многочленом степени 4 с корнями из поля GF(2^4). Этот многочлен должен быть сомножителем $x^{15} + 1$. В табл. 5.1 приведены неприводимые сомножители $x^{15} + 1$, их корни в виде элементов поля GF(2^4), значения функций-след этих элементов и периоды рекуррентных последовательностей, порождаемых представленными многочленами.

Таблица 5.1

№ п/п	Обозначение	Многочлен	Корни	Функция-след $T_4(\varepsilon^i)$	Период последовательности
1	$f_1(x)$	x^4+x+1	$\varepsilon^1, \varepsilon^2, \varepsilon^4, \varepsilon^8$	0	15
2	$f_2(x)$	$x^4+x^3+x^2+x+1$	$\varepsilon^3, \varepsilon^6, \varepsilon^9, \varepsilon^{12}$	1	5
3	$f_3(x)$	x^2+x+1	$\varepsilon^5, \varepsilon^{10}$	0	3
4	$f_4(x)$	x^4+x^3+1	$\varepsilon^7, \varepsilon^{11}, \varepsilon^{13}, \varepsilon^{14}$	1	15
5	$f_5(x)$	$x+1$	$\varepsilon^{15}=\varepsilon^0$	0	1

Выбираем характеристический многочлен для кода (15,6) в виде $P(x) = (x^4 + x + 1)(x^2 + x + 1) = p_0 x^6 + p_1 x^5 + p_2 x^4 + p_3 x^3 + p_4 x^2 + p_5 x + p_6 = x^6 + x^5 + x^4 + x^3 + 1$, из чего следует, что $p_0 = p_1 = p_2 = p_3 = p_6 = 1$ и $p_4 = p_5 = 0$.

Рекуррентное уравнение, которому должны соответствовать связи между символами кодовой комбинации кода с данным характеристическим многочленом имеет вид: $s_{e+6} = s_{e+5} + s_{e+4} + s_{e+3} + s_e$.

Порождающий многочлен данного кода (15,6) имеет среди своих корней пять подряд идущих степеней примитивного элемента поля GF(2^4): $\varepsilon^{11}, \varepsilon^{12}, \varepsilon^{13}, \varepsilon^{14}, \varepsilon^{15}$, т. е. минимальное кодовое расстояние данного кода (15,6) равно 6 и этот код способен гарантийно исправить все однократные и двухкратные ошибки.

1.5.2. Кодирующее устройство

1.5.2.1. Схема кодирующего устройства

Схема кодирующего устройства рассматриваемого кода (15.6) БЧХЭ, представленная в общем виде на рис. 4.3, может быть реализована на регистрах сдвига с обратными связями, как показано на рис. 5.1.

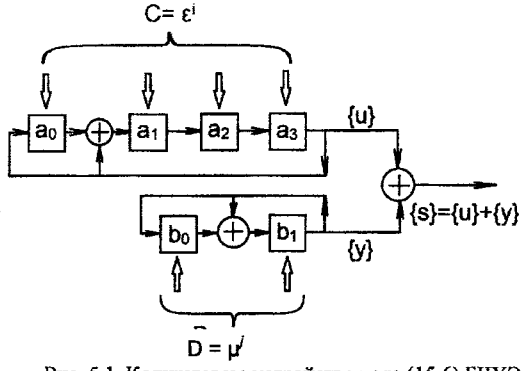


Рис. 5.1. Кодирующее устройство кода (15.6) БЧХЭ

Кодируемая информация представляется в виде двоичной последовательности длины 6, в которой выделяют две части – (C,D), где C – последовательность из четырех информационных символов, а D – из двух. Верхний регистр является генератором элементов поля $GF(2^4)$, а нижний – генератор элементов поля $GF(2^2)$. При поступлении в кодер кодируемой последовательности (C,D) элементы C параллельным кодом вводятся в ячейки верхнего регистра, а D – нижнего. После этого генераторы запускаются и подают на вход сумматора пятнадцатиэлементные последовательности $\{u\}$ и $\{y\}$ соответственно.

Последовательность $\{u\}$ – это последовательность максимальной длины с характеристическим многочленом $x^4 + x + 1$, т. е. комбинация циклического кода (15,4).

Последовательность $\{y\}$ – это пятикратно повторенная последовательность максимальной длины с характеристическим многочленом $x^2 + x + 1$, т. е. комбинация циклического кода (3,2). Начальными фазами этих последовательностей максимальной длины являются информационные символы $C = \varepsilon^j$ и $D = \mu^i$, представленные элементами поля $GF(2^4)$ (ε^j) и $GF(2^2)$ (μ^i) соответственно. На выходе сумматора формируется результирующая последовательность $\{s\}$ – комбинация неразделимого (несистематического) циклического кода БЧХЭ (15,6). Как исходные $\{u\}$ и $\{y\}$, так и результирующая $\{s\}$ последовательности могут быть представлены через совокупности функции-след:

$$\{u\} = \{T_m(\varepsilon^{i+14})...T_m(\varepsilon^i)\},\ \{y\} = \{T_m(\mu^{j+2})\ ...T_m(\mu^j)\},$$

$$\{s\} = \{[T_m(\varepsilon^{i+14}) + T_m(\mu^{j+2})]...[T_m(\varepsilon^i) + T_m(\mu^j)]\}.$$

1.5.2.2. Работа схемы кодирующего устройства

Проиллюстрируем изложенное выше конкретным примером.

Пусть значения $C = \varepsilon^j = 1$ и $D = \mu^i = 1$. Необходимо представить эти значения в двоичном представлении. Элементы поля $GF(2^2)$ (μ^i) и $GF(2^4)$ (ε^j) в различном представлении имеют вид, представленный в табл. 5.2 и 5.3, из которых видно, что C = 1000, D = 10. Введем комбинацию 1000 в ячейки верхнего регистра, а комбинацию 10 – в ячейки нижнего и произведем синхронный запуск обоих генераторов.

Таблица 5.2

$GF(2^2)$: $\pi(\mu) = \mu^2 + \mu + 1 = 0$			
Формы элементов			Функция-след $T_2(\mu)$
целочисленная	степенная	векторная μ^0 μ^1	
0	$\mu^{-\infty}$	00	0
1	$\mu^0 = 1 = \mu^3 = \mu^{-3}$	10	0
2	$\mu^1 = \mu^{-2}$	01	1
3	$\mu^2 = 1 + \mu = \mu^{-1}$	11	1

Таблица 5.3

$GF(2^4)$: $\pi(\varepsilon) = \varepsilon^4 + \varepsilon + 1 = 0$			
Формы элементов			Функция-след $T_4(\varepsilon)$
целочисленная	степенная	векторная ε^0 ε^1 ε^2 ε^3	
0	$\varepsilon^{-\infty}$	0000	0
1	$\varepsilon^0 = 1 = \varepsilon^{15} = \varepsilon^{-15}$	1000	0
2	$\varepsilon = \varepsilon^{-14}$	0100	0
3	$\varepsilon^2 = \varepsilon^{-13}$	0010	0
4	$\varepsilon^3 = \varepsilon^{-12}$	0001	1
5	$\varepsilon^4 = 1 + \varepsilon = \varepsilon^{-11}$	1100	0
6	$\varepsilon^5 = \varepsilon + \varepsilon^2 = \varepsilon^{-10}$	0110	0
7	$\varepsilon^6 = \varepsilon^2 + \varepsilon^3 = \varepsilon^{-9}$	0011	1
8	$\varepsilon^7 = 1 + \varepsilon + \varepsilon^3 = \varepsilon^{-8}$	1101	1
9	$\varepsilon^8 = 1 + \varepsilon^2 = \varepsilon^{-7}$	1010	0
10	$\varepsilon^9 = \varepsilon + \varepsilon^3 = \varepsilon^{-6}$	0101	1
11	$\varepsilon^{10} = 1 + \varepsilon + \varepsilon^2 = \varepsilon^{-5}$	1110	0
12	$\varepsilon^{11} = \varepsilon + \varepsilon^2 + \varepsilon^3 = \varepsilon^{-4}$	0111	1
13	$\varepsilon^{12} = 1 + \varepsilon + \varepsilon^2 + \varepsilon^3 = \varepsilon^{-3}$	1111	1
14	$\varepsilon^{13} = 1 + \varepsilon^2 + \varepsilon^3 = \varepsilon^{-2}$	1011	1
15	$\varepsilon^{14} = 1 + \varepsilon^3 = \varepsilon^{-1}$	1001	1

Они начнут генерировать элементы полей: $GF(2^4)$ – верхний и $GF(2^2)$ – нижний. При этом элементы поля будут появляться в ячейках регистра строго в той последовательности, как это представлено в табл. 5.2 и 5.3. Рекуррентные последовательности, а это последовательности максимальной

длины, вводятся в сумматор из крайних справа (старших) ячеек, т. е. значение элементов этих последовательностей представлено значением старших разрядов элементов в двоичном представлении. Из таблиц видно, что значения функции-след в точности равны значению этих старших разрядов для соответствующего элемента поля.

Поскольку $GF(2^2)$ является подполем $GF(2^4)$, то элементу μ из поля $GF(2^2)$ соответствует элемент ε^5 из поля $GF(2^4)$ и любой элемент s^i последовательности $\{s\}$ может быть представлен в виде $s^i = T_4(\varepsilon^i) + T_{4\backslash 2}[(\varepsilon^5)^{i\ (mod3)}]$. Нижний индекс функции-след $T_{4\backslash 2}[(\varepsilon^5)^{i\ (mod3)}]$ указывает, что ε^5 – элемент поля $GF(2^4)$, а функция-след $T_{4\backslash 2}[(\varepsilon^5)^{i\ (mod3)}]$ должна вычисляться как для поля $GF(2^2)$. Результирующая последовательность $\{s\}$, полученная поэлементным суммированием последовательностей $\{u\}$и $\{y\}$, представлена в табл. 5.4. Здесь же показаны связи между элементами последовательностей, определяемые характеристическими многочленами $P(x)$.

Таблица 5.4

Код	Рекуррентная последовательность
(15,4) :{U}	1 1 1 1 0 1 0 1 1 0 0 1 0 0 0
Связи между элементами $p(x) = x^4+x+1$	↑ ↑ ↑ ← (□ + □+□) = 0
(3.2) : {Y}	1 1 0 1 1 0 1 1 0 1 1 0 1 1 0
Связи между элементами $p(x) = x^2+x+1$	↑ ↑ ↑ ← (□ +□+□) = 0
(15,6) : {S}	0 0 1 0 1 1 1 0 1 1 1 1 1 1 0
Связи между элементами $p(x) = x^6+x^5+x^4+x^3+1$	↑ ↑ ↑ ↑ ↑ ← (□+□+ □+□ + □) = 0

1.5.3. Декодирующее устройство

1.5.3.1. Схема декодирующего устройства

Схема декодирующего устройства кода БЧХЭ (15.6) , построенная на основе схемы рис. 4.4, приведена на рис. 5.2.

Схема декодирующего устройства кода БЧХЭ (15.6) состоит из входного регистра, генераторов *обратных элементов поля* ГОЭ $GF(2^2)$ и $GF(2^4)$, шести умножителей обратных элементов поля $GF(2^4)$ на коэффициенты α_i, шести умножителей обратных элементов поля $GF(2^2)$ на коэффициенты β_i, двенадцати ключевых схем – по одной на выходе каждого умножителя, схемы суммирования элементов поля $GF(2^4)$ и схемы суммирования элементов поля $GF(2^2)$, на выходах которых формируются предварительные значения фрагментов переданного сообщения C и D соответственно, а также мажоритарного элемента, выносящего решение о принятом сообщении

(C, D) по большинству совпадений пар, принятых от схем суммирования значений (C, D).

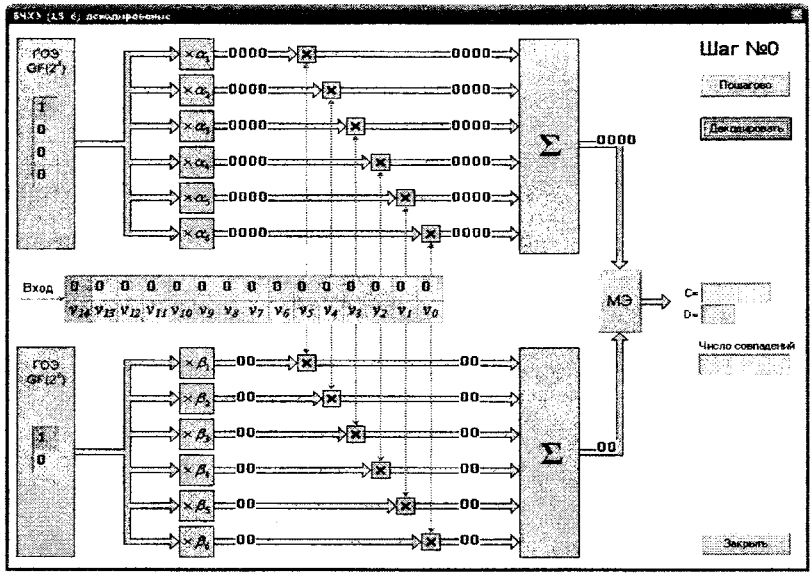
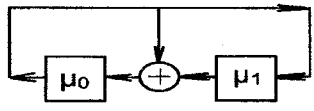
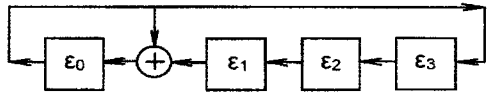


Рис. 5.2. Декодирующее устройство кода (15.6) БЧХЭ на нулевом шаге

Генератор обратных элементов поля $GF(2^m)$ представляет собой генератор элементов поля $GF(2^m)$ с измененным на противоположное направление перемещения информации по регистру (рис. 5.3).



а)



б)

Рис. 5.3. Генераторы обратных элементов поля: а – $GF(2^2)$, б – $GF(2^4)$

Значения обратных элементов $GF(2^2)$ и $GF(2^4)$ представлены в табл. 5.2 и 5.3.

Значения коэффициентов α_i и β_i вычисляются по формуле, обоснованной в теореме 1:

$$\alpha_i = \frac{\sum_{l=0}^{m-1} p_{m-1-l}\varepsilon^l}{P'(\varepsilon)} = \frac{p_5 + p_4\varepsilon + p_3\varepsilon^2 + p_2\varepsilon^3 + p_1\varepsilon^4 + p_0\varepsilon^5}{\varepsilon^2 + \varepsilon^4} = \varepsilon^4,$$

где p_i – коэффициенты характеристического многочлена;

$$P(x) = x^6 + x^5 + x^4 + x^3 + 1, \text{ т. е.} \quad p_0 = p_1 = p_2 = p_3 = p_6 = 1 \text{ и } p_4 = p_5 = 0;$$
$$\varepsilon^l - \text{корни } P(x): \quad \{\varepsilon^1, \varepsilon^2, \varepsilon^4, \varepsilon^5, \varepsilon^8, \varepsilon^{10}\}.$$

Подставляя в указанную формулу остальные значения ε^l, получим:
$\alpha_2 = \varepsilon^3$, $\alpha_3 = \varepsilon^2$, $\alpha_4 = 1$, $\alpha_5 = \varepsilon^9$, $\alpha_6 = \varepsilon^5$.
Заменив в формуле для α_l значения ε^l на μ^l, находим β_l:
$\beta_1 = \varepsilon^{10}$, $\beta_2 = \varepsilon^5$, $\beta_3 = 1$, $\beta_4 = 0$, $\beta_5 = \varepsilon^{10}$, $\beta_6 = 1$.

1.5.3.2. Работа схемы декодирующего устройства

Работает декодирующее устройство следующим образом. Пусть с выхода передатчика к приемнику была передана комбинация $f(x)$=(0 0 1 0 1 1 1 0 1 1 1 1 1 1 0), а в декодирующее устройство поступила комбинация $f'(x)$=(0 0 1 0 0 1 1 0 1 0 1 1 1 1 0) с ошибками в пятом и десятом разрядах. Как только входной регистр полностью заполнится, начнется обработка старших шести разрядов принятой комбинации $f'(x)$ (0 1 1 1 1 0). Для этого в каждом из генераторов обратных элементов поля будут принудительно установлены единичные элементы поля : $\mu^0 = 1$ в $GF(2^2)$ и $\varepsilon^0 = 1$ в $GF(2^4)$ и на выходе схем суммирования появятся первые предварительные значения фрагментов переданного сообщения C и D. По следующему такту принятая последовательность сдвигается по регистру на один символ вправо, генераторы обратных элементов генерируют следующие по очереди элементы $\varepsilon^{-1} = \varepsilon^{14}$ и $\mu^{-1} = \mu^2$ соответственно , происходит обработка следующих шести разрядов принятой комбинации (1 0 1 1 1 1) и на выходе схем суммирования появится вторая пара предварительных значений фрагментов переданного сообщения C и D. Этот процесс повторяется 15 раз. Значения пар C и D в виде двоичных последовательностей, отображающих элементы $GF(2^2)$ и $GF(2^4)$, с выходов схем суммирования поступают в мажоритарный элемент, который из 15 пар выбирает значение (C, D) по наибольшему количеству совместных совпадений. Для получения 15 пар решений необходимо старшие 5 разрядов принятой комбинации $f'(x)$ сохранить в дополнительном регистре и подключать их к обработке по мере необходимости. В табл. 5.5 представлен процесс декодирования комбинации $f'(x)$ = = (0 0 1 0 0 1 1 0 1 0 1 1 1 1 0) . По большинству совместных значений пар (C, D) декодирующее устройство принимает решение C = 1000, D = 10.

Таблица 5.5

Такты i	S_{i-5}	S_{i-4}	S_{i-3}	S_{i-2}	S_{i-1}	S_i	Вычисление значения C_i											Вычисление значения D_i										Результат декодирования	
							C_i	ε^{-i}	Коэффициент двойственного базиса						$\varepsilon^{-i}\Sigma^{\cdots}$	D_i	ε^{-i}	Коэффициент двойственного базиса						$\varepsilon^{-i}\Sigma^{\cdots}$	$(C_i\ D_i)$	Число совпадений		
									ε^5	ε^9	1	ε^2	ε^3	ε^4				1	ε^{10}	0	1	ε^5	ε^{10}					
0	0	1	1	1	1	0	C_0	1 (		ε^9+	1+	ε^2+	ε^3	)=	ε^{10}	D_0	1 (		ε^{10}	+	1+	ε^5	)=	0	(1110 00)	1		
1	1	0	1	1	1	1	C_1	ε^{-1} (	ε^5+		1+	ε^2+	ε^3+	ε^4)=	ε^2	D_1	ε^{-5} (	1+			1+	ε^5+	ε^{10})=	$\varepsilon^{10}=\mu^2$	(0010 11)	1		
2	0	1	0	1	1	1	C_2	ε^{-2} (		ε^9+		ε^2+	ε^3+	ε^4)=	ε^6	D_2	ε^{-10}(		ε^{10}	+	1+	ε^5+	ε^{10})=	1	(0011 10)	1		
3	1	0	1	0	1	1	C_3	ε^{-3} (	ε^5+		1+		ε^3+	ε^4)=	ε^3	D_3	1 (	1+				ε^5+	ε^{10})=	0	(0001 00)	1		
4	1	1	0	1	0	1	C_4	ε^{-4} (	ε^5+	ε^9+		ε^2+		ε^4)=	ε^3	D_4	ε^{-5} (	1+	ε^{10}	+	1+		ε^{10})=	0	(0001 00)	2		
5	0	1	1	0	1	0	C_5	ε^{-5} (		ε^9+	1+		ε^3	)=	ε^{14}	D_5	ε^{-10}(		ε^{10}	+		ε^5	)=	$\varepsilon^5=\mu$	(1001 01)	1		
6	0	0	1	1	0	1	C_6	ε^{-6} (			1+	ε^2+		ε^4)=	ε^{14}	D_6	1 (				1+		ε^{10})=	$\varepsilon^5=\mu$	(1001 01)	2		
7	1	0	0	1	1	0	C_7	ε^{-7} (	ε^5+			ε^2+	ε^3	)=	ε^2	D_7	ε^{-5} (	1+			1+	ε^5	)=	1	(0010 10)	1		
8	0	1	0	0	1	1	C_8	ε^{-8} (		ε^9+			ε^3+	ε^4)=	ε^7	D_8	ε^{-10}(		ε^{10}	+		ε^5+	ε^{10})=	$\varepsilon^{10}=\mu^2$	(1101 11)	1		
9	0	0	1	0	0	1	C_9	ε^{-9} (			1+			ε^4)=	ε^7	D_9	1 (						ε^{10})=	$\varepsilon^{10}=\mu^2$	(1101 11)	2		
10	0	0	0	1	0	0	C_{10}	ε^{-10}(				ε^2		)=	ε^7	D_{10}	ε^{-5} (				1		)=	$\varepsilon^{10}=\mu^2$	(1101 11)	3		
11	1	0	0	0	1	0	C_{11}	ε^{-11}(	ε^5+				ε^3	)=	1	D_{11}	ε^{-10}(	1+				ε^5	)=	1	(1000 10)	1		
12	1	1	0	0	0	1	C_{12}	ε^{-12}(	ε^5+	ε^9+				ε^4)=	1	D_{12}	1 (	1+	ε^{10}	+			ε^{10})=	1	(1000 10)	2		
13	1	1	1	0	0	0	C_{13}	ε^{-13}(	ε^5+	ε^9+	1			)=	1	D_{13}	ε^{-5} (	1+	ε^{10}				)=	1	(1000 10)	3		
14	1	1	1	1	0	0	C_{14}	ε^{-14}(	ε^5+	ε^9+	1+	ε^2		)=	1	D_{14}	ε^{-10}(	1+	ε^{10}	+	1		)=	1	(1000 10)	4		

Таким образом, передаваемая информационная последовательность (C, D) определена, и процесс декодирования успешно завершен. Однако изложенная выше теория позволяет полностью восстановить всю переданную кодовую комбинацию $f(x)$.

В п. 1.4.2.2 было показано, что на основе выражения (4.3) любой элемент ν_i принятой последовательности $\{\nu\}$ может быть представлен в виде $\nu_i = T_4(C\,\varepsilon^{i\ mod15}) + T_2(D\,\mu^{i\ mod3})$. Значения $C = \varepsilon^0$ и $D = \mu^0$ определены в результате мажоритарного декодирования и теперь любой элемент ν_i может быть вычислен. В качестве примера найдем истинные значения принятых с ошибкой элементов ν_5 и ν_{10}. Используя выражение для ν_i через функцию-след, находим: $\nu_5 = T_4(C\,\varepsilon^{5\ mod15}) + T_2(D\,\mu^{5\ mod3}) = T_4(\varepsilon^5) + T_2(\mu^2)$. Из табл. 5.2 находим $T_2(\mu^2) = 1$, а из табл. 5.3 – $T_4(\varepsilon^5) = 0$. Итак, $\nu_5 = 0 + 1 = 1$. Аналогично вычисляем: $\nu_{10} = T_4(\varepsilon^{10\ mod15}) + T_2(\mu^{10\ mod3}) = T_4(\varepsilon^{10}) + T_2(\mu) = 0+1=1$.

1.5.3.3. Декодирование кодов БЧХЭ с использованием децимации принятых кодовых комбинаций

В [1] доказано, что начальная фаза C рекуррентной последовательности $\{s\} = (s_0, s_1, \ldots s_{2^k-1})$ и начальная фаза $\check{C}$ рекуррентной последовательности $\{\nu\} = (\nu_0, \nu_1, \ldots \nu_{2^k-1})$, где $\nu_j = s_{qj}$, полученной из {s} путем децимации с индексом $q = 2^i$, связаны равенством: $C = \check{C}^q$.

Пусть {s} – поступившая в декодер кодовая комбинация кода БЧХЭ $s(x) = s_{n-1}x^0 + s_{n-2}x^1 + \ldots + s_1 x^{n-2} + s_0 x^{n-1}$. Децимированная с индексом 2 последовательность символов этой комбинации имеет вид:

$$(\nu_{n-1}, \nu_{n-2}, \ldots, \nu_2, \nu_1, \nu_0) = (s_{n-2}, \ldots s_1, s_{n-1}, \ldots, s_4, s_2, s_0).$$

В результате декодирования определяется начальная фаза децимированной последовательности $\check{C}$. Начальная фаза переданной последовательности может быть найдена как $C = \check{C}^2$.

Проиллюстрируем возможности декодирования кодов БЧХЭ с использованием децимации принятых кодовых комбинаций применительно к коду (15,6), рассмотренному выше.

Пусть с выхода передатчика в канал поступила комбинация этого кода (0 0 1 0 1 1 1 0 1 1 1 1 1 1 0), имеющая начальную фазу вида C = 1000, D = 10. На вход декодера поступила комбинация (0 0 1 0 1 1 1 0 1 1 0 1 0 1 1) с ошибками в символах s_4, s_2, s_0, выделенных подчеркиванием.

Процедура мажоритарного декодирования принятой комбинации представлена в табл. 5.6, из которой видно, что декодер не может принять решение о значении начальной фазы принятой комбинации, так как два набора значений пар (C, D) имеют по пяти совпадений.

Выполним децимацию принятой комбинации с индексом два, т. е. представим ее в виде: $(s_{13}, s_{11}, s_9, s_7, s_5, s_3, s_1, s_{14}, s_{12}, s_{10}, s_8, s_6, s_4, s_2, s_0) =$ = (0 0 1 0 1 1 1 0 1 1 1 1 0 0 1). Здесь ошибочные символы оказались в начале последовательности.

Таблица 5.6

Такты i	S_{i6}	S_{i4}	S_{i3}	S_{i2}	S_{i1}	S_i	Вычисление значения C_i									Вычисление значения D_i								Результат декодирования	
							C_i	Коэффициенты двойственного базиса								D_i	Коэффициенты двойственного базиса								$(C_i\ D_i)$	Число совпадений
								ε^{-1}	ε^5	ε^9	1	ε^2	ε^3	ε^4	$\varepsilon^{-1}\Sigma\cdots$		ε^{-1}	1	ε^{10}	0	1	ε^5	ε^{10}	$\varepsilon^{-1}\Sigma\cdots$		
0	1	0	1	0	1	1	C_0	1 (	ε^5	+	1+		ε^3+	ε^4)=	ε^6	D_0	1 (	1		+		ε^5+	ε^{10})=	0	(0011 00)	1
1	1	1	0	1	0	1	C_1	ε^{-1} (	ε^5+	ε^9	+	ε^2+		ε^4)=	ε^6	D_1	ε^{-5}(	1+	ε^{10}	+	1+		ε^{10})=	**0**	(0011 00)	2
2	0	1	1	0	1	0	C_2	ε^{-2} (		ε^9+	1	+	ε^3	)=	ε^2	D_2	ε^{-10}(		ε^{10}	+		ε^5	)=	$\varepsilon^5=\mu$	(0010 01)	1
3	1	0	1	1	0	1	C_3	ε^{-3} (	ε^5+		1+	ε^2+		ε^4)=	**0**	D_3	1 (	1		+	1	ε^5+	ε^{10})=	1	(0000 10)	1
4	1	1	0	1	1	0	C_4	ε^{-4} (	ε^5+	ε^9+		ε^2+	ε^3	)=	**0**	D_4	ε^{-5}(	1+	ε^{10}	+	1+	ε^5	)=	$\varepsilon^{10}=\mu^2$	(0000 11)	1
5	1	1	1	0	1	1	C_5	ε^{-5} (	ε^5+	ε^9+	1+		ε^3+	ε^4)=	**1**	D_5	ε^{-10}(	1	ε^{10}			ε^5+	ε^{10})=	**1**	(1000 10)	1
6	0	1	1	1	0	1	C_6	ε^{-6} (		ε^9+	1+	ε^2+		ε^4)=	**1**	D_6	1 (		ε^{10}	+	1+		ε^{10})=	**1**	(1000 10)	2
7	1	0	1	1	1	0	C_7	ε^{-7} (	ε^5+		1	ε^2+	ε^3	)=	**1**	D_7	ε^{-5}(	1		+	1+	ε^5	)=	1	(1000 10)	3
8	0	1	0	1	1	1	C_8	ε^{-8} (		ε^9+		ε^2+	ε^3+	ε^4)=	**1**	D_8	ε^{-10}(		ε^{10}	+	1	ε^5+	ε^{10})=	**1**	(1000 10)	4
9	0	0	1	0	1	1	C_9	ε^{-9} (			1+		ε^3+	ε^4)=	**1**	D_9	1 (					ε^5+	ε^{10})=	**1**	(1000 10)	5
10	1	0	0	1	0	1	C_{10}	ε^{-10}(	ε^5	+		ε^2	+	ε^4)=	ε^5	D_{10}	ε^{-5}(	1		+	1	+	ε^{10})=	$\varepsilon^5=\mu$	(0110 01)	1
11	1	1	0	0	1	0	C_{11}	ε^{-11}(	ε^5+	ε^9	+		ε^3	)=	ε^6	D_{11}	ε^{-10}(	1+	ε^{10}	+			ε^{10})=	$\varepsilon^5=\mu$	(0011 01)	1
12	0	1	1	0	0	1	C_{12}	ε^{-12}(		ε^9+	1			ε^4)=	ε^6	D_{12}	1 (		ε^{10}	+			ε^{10})=	0	(0011 00)	3
13	1	0	1	1	0	0	C_{13}	ε^{-13}(	ε^5+		1	ε^2		)=	ε^6	D_{13}	ε^{-5}(	1		+	1		)=	0	(0011 00)	4
14	0	1	0	1	1	0	C_{14}	ε^{-14}(		ε^9+		ε^2+	ε^3	)=	ε^6	D_{14}	ε^{-10}(		ε^{10}	+	1	ε^5	)=	0	(0011 00)	5

Таблица 5.7

Такты i	S_{i6}	S_{i-4}	S_{i-3}	S_{i-2}	S_{i-1}	S_i	Вычисление значения C_i									Вычисление значения D_i								Результат декодирования	
							$\check{C}_i$	Коэффициенты двойственного базиса								$\check{D}_i$	Коэффициенты двойственного базиса								$(C_i\ D_i)$	Число совпадений
								ε^{-i}	ε^5	ε^9	1	ε^2	ε^3	ε^4	$\varepsilon^{-i}\Sigma\cdots / c_i$		ε^{-i}	1	ε^{10}	0	1	ε^5	ε^{10}	$\varepsilon^{-i}\Sigma\cdots / D_i$		
0	1	1	1	0	0	1	$\check{C}_0$	1 (	ε^5+	ε^9+	1+			ε^4 =	$\varepsilon^{11}/\varepsilon^7$	$\check{D}_0$	1 (	1+	ε^{10}	+			ε^{10})=	1 / 1	(1101 10)	1
1	1	1	1	1	0	0	$\check{C}_1$	ε^{-1} (	ε^5+	ε^9+	1+	ε^2+		)=	$\varepsilon^{13}/\varepsilon^{11}$	$\check{D}_1$	ε^{-5}(	1+	ε^{10}	+		ε^5	)=	0 / 0	(0111 00)	1
2	0	1	1	1	1	0	$\check{C}_2$	ε^{-2} (		ε^9+	1+	ε^2+	ε^3+	)=	$\varepsilon^8/\varepsilon^1$	$\check{D}_2$	ε^{-10}(		ε^{10}	+	1+	ε^5	)=	0 / 0	(0100 00)	1
3	1	0	1	1	1	1	$\check{C}_3$	ε^{-3} (	ε^5+		1+	ε^2+	ε^3+	ε^4)=	1 / 1	$\check{D}_3$	1 (	1+			1	ε^5+	ε^{10})=	1 / 1	(1000 10)	1
4	1	1	0	1	1	1	$\check{C}_4$	ε^{-4} (	ε^5+	ε^9+		ε^2+	ε^3+	ε^4)=	1 / 1	$\check{D}_4$	ε^{-5}(	1+	ε^{10}	+	1	ε^5+	ε^{10})=	1 / 1	(1000 10)	2
5	1	1	1	0	1	1	C_5	ε^{-5} (	ε^5+	ε^9+	1+		ε^3	ε^4)=	1 / 1	$\check{D}_5$	ε^{-10}(	1	+ε^{10}	+		ε^5+	ε^{10})=	1 / 1	(1000 10)	3
6	0	1	1	1	0	1	$\check{C}_6$	ε^{-6} (		ε^9+	1+	ε^2+		ε^4)=	1 / 1	$\check{D}_6$	1 (		ε^{10}	+	1+		ε^{10})=	1 / 1	(1000 10)	4
7	1	0	1	1	1	0	$\check{C}_7$	ε^{-7} (	ε^5+		1+	ε^2+	ε^3	)=	1 / 1	$\check{D}_7$	ε^{-5}(	1		+	1+	ε^5	)=	1 / 1	(1000 10)	5
58	0	1	0	1	1	1	$\check{C}_8$	ε^{-8} (		ε^9+		ε^2+	ε^3+	ε^4)=	1 / 1	$\check{D}_8$	ε^{-10}(		ε^{10}	+	1+	ε^5+	ε^{10})=	1 / 1	(1000 10)	6
9	0	0	1	0	1	1	$\check{C}_9$	ε^{-9} (			1+		ε^3+	ε^4)=	1 / 1	$\check{D}_9$	1 (					ε^5+	ε^{10})=	1 / 1	(1000 10)	7
10	1	0	0	1	0	1	$\check{C}_{10}$	ε^{-10}(	ε^5+			ε^2		ε^4)=	$\varepsilon^5/\varepsilon^{10}$	$\check{D}_{10}$	ε^{-5}(	1		+	1	+	ε^{10})=	μ/μ^2	(1110 11)	1
11	0	1	0	0	1	0	$\check{C}_{11}$	ε^{-11}(		ε^9+			ε^3	)=	$\varepsilon^5/\varepsilon^{10}$	$\check{D}_{11}$	ε^{-10}(		ε^{10}	+		ε^5	)=	μ/μ^2	(1110 11)	2
12	0	0	1	0	0	1	$\check{C}_{12}$	ε^{-12}(			1+			ε^4)=	$\varepsilon^4/\varepsilon^8$	$\check{D}_{12}$	1 (						ε^{10})=	μ^2/μ	(1010 01)	1
13	1	0	0	1	0	0	$\check{C}_{13}$	ε^{-13}(	ε^5+			ε^2		)=	$\varepsilon^3/\varepsilon^6$	$\check{D}_{13}$	ε^{-5}(	1+			1		)=	0 / 0	(0011 00)	1
14	1	1	0	0	1	0	$\check{C}_{14}$	ε^{-14}(	ε^5+	ε^9+			ε^3	)=	$\varepsilon^3/\varepsilon^6$	$\check{D}_{14}$	ε^{-10}(	1+	ε^{10}	+		ε^5+	)=	0 / 0	(0011 00)	2

Процедура мажоритарного декодирования децимированной комбинации представлена в табл. 5.7 (здесь $\check{C}_i$ и $\check{D}_i$ – результаты вычисления значения начальной фазы децимированной последовательности. Для определения начальной фазы переданной последовательности (C_i, D_i) вычисленные значения $\check{C}_i$ и $\check{D}_i$ помещены в последнем столбце «вычисление значений» $\check{C}_i$ и $\check{D}_i$ после вычисленных значений $\check{C}_i$ и $\check{D}_i$ за дробной чертой. Теперь декодер уверенно выдает правильный результат декодирования. Кроме того, в работе предполагается использование децимации принятой комбинации кода БЧХЭ (15,6) с индексом децимации 4 и 8.

Соответствующие последовательности имеют вид:

$(s_{11}, s_7, s_3, s_{14}, s_{10}, s_6, s_2, s_{13}, s_9, s_5, s_1, s_{12}, s_8, s_4, s_0)$ – децимация с индексом 4,

$(s_7, s_{14}, s_6, s_{13}, s_5, s_{12}, s_4, s_{11}, s_3, s_{10}, s_2, s_9, s_1, s_8, s_0)$ – децимация с индексом 8.

Децимация с индексом 16 приводит к исходной последовательности.

1.6. Порядок выполнения работы

1.6.1. Кодирование

Изучить пп. 1.5.2. Построить схему кодера (рис. 5.1) и с ее помощью сформировать кодовую комбинацию $f(x)$ по заданной информационной последовательности (C, D). Заданные значения информационной последовательности (C, D) ввести в соответствующие регистры программной модели кодера и выполнить пошагово процедуру кодирования. Сравнить результаты с расчетными и занести их в табл. 6.1. В качестве примера в табл. 6.1 показан процесс формирования кодовой комбинации кода БЧХЭ (15,6), соответствующей информационной последовательности (1000 10).

Таблица 6.1

№ тактов	ε'				μ'		$T_4(\varepsilon')+T_2(\mu')$
	a_0	a_1	a_2	$a_3=T_4(\varepsilon')$	b_0	$b_1=T_2(\mu')$	
0	1	0	0	0	1	0	–
1	0	1	0	0	0	1	0
2	0	0	1	0	1	1	1
3	0	0	0	1	1	0	1
4	1	1	0	0	0	1	1
5	0	1	1	0	1	1	1
6	0	0	1	1	1	0	1
7	1	1	0	1	0	1	1
8	1	0	1	0	1	1	0
9	0	1	0	1	1	0	1
10	1	1	1	0	0	1	1
11	0	1	1	1	1	1	1
12	1	1	1	1	1	0	0
13	1	0	1	1	0	1	1
14	1	0	0	1	1	1	0
15	1	0	0	0	1	0	0

Схему кодера и заполненную табл. 6.1 поместить в отчет по лабораторной работе. В отчете объяснить, что представляет собой содержимое регистров кодера на каждом такте, какие последовательности записаны в столбцах табл. 6.1, озаглавленных символами $T_4(\varepsilon^3)$, $T_2(\mu^1)$ и $T_4(\varepsilon^i) + T_2(\mu^i)$, и как отдельные символы этих последовательностей связаны с функциями-след $T_4(\varepsilon)$, $T_2(\mu)$.

1.6.2. Декодирование с гарантийно исправляемой ошибкой

Изучить пп. 1.5.3.1, 1.5.3.2. Построить схему декодера. Внимательно проследить процесс заполнения табл. 5.5. Выписать из табл. 6.1 сформированную в п. 1 комбинацию кода (15,6) $f(x)$ и прибавить к ней заданный $e_1(x)$ – гарантийно исправляемый кодом БЧХЭ (15,6) многочлен ошибок. Выполнить процедуру декодирования последовательности $\nu_1(x) = f(x) + e_1(x)$, используя шаблон табл. 6.2, содержащий исходные данные декодера, представленные в табл. 5.5, и описание формирования данных этой таблицы в пп. 1.5.3.2. Ввести элементы последовательности $\nu_1(x)$ во входной регистр программной модели декодера и проверить совпадение результатов декодирования. Поместить заполненную табл. 6.2 в отчет. В отчете кратко сформулировать суть используемого метода мажоритарного декодирования и условия, при которых передаваемая информационная последовательность (C, D) может быть успешно восстановлена при поражении передаваемого сообщения ошибками. Показать возможность исправления ошибок в принятой последовательности $\{\nu\}$, используя связи между элементами этой последовательности и функциями-след $T_4(\varepsilon)$, $T_2(\mu)$.

1.6.3. Декодирование с гарантийно неисправляемой ошибкой

Аналогично п. 6.2 составить последовательность $\nu_2(x) = f(x) + e_2(x)$, где $f(x)$ – полученная в п. 6.1 в соответствии с заданием кодовая комбинация кода БЧХЭ (15,6), $e_2(x)$ – неисправляемый кодом БЧХЭ (15,6) многочлен ошибок, определенный заданием, и выполнить декодирования этой последовательности. Процедуру декодирования последовательности $\nu_2(x) = f(x) + e_2(x)$ выполнить и отразить в табл. 6.3, используя шаблон табл. 6.2. Ввести элементы последовательности $\nu_2(x)$ во входной регистр программной модели декодера и проверить совпадение результатов декодирования с расчетными. Поместить заполненную табл. 6.3 в отчет. В отчете кратко сформулировать причины, вызвавшие невозможность правильного решения декодера.

Таблица 6.2

Такты i	S_{i-5} S_{i-4} S_{i-3} S_{i-2} S_{i-1} S_i	Вычисление значения Ci									Вычисление значения D_i								Результат декодирования	
		Ci	Коэффициенты двойственного базиса								D_i	Коэффициенты двойственного базиса							$(C_i\ D_i)$	Число совпадений
			ε^{-i}	ε^{5}	ε^{9}	1	ε^{2}	ε^{3}	ε^{4}	$\varepsilon^{-i}\Sigma\ldots$		ε^{-i}	1	ε^{10}	0	1	ε^{5}	ε^{10}	$\varepsilon^{-i}\Sigma\ldots$		
0		C_0	1 (						)=		D_0	1 (						)=			
1		C_1	ε^{-1} (						)=		D_1	ε^{-5} (						)=			
2		C_2	ε^{-2} (						)=		D_2	ε^{-10} (						)=			
3		C_3	ε^{-3} (						)=		D_3	1 (						)=			
.....																					
14		C_{14}	ε^{-14} (						)=		D_{14}	ε^{-10} (						)=			

Таблица 6.4

Такты i	S_{i-5} S_{i-4} S_{i-3} S_{i-2} S_{i-1} S_i	Вычисление значения C_i									Вычисление значения D_i									Результат декодирования	
		$\check{C}_i$	Коэффициенты двойственного базиса								$\check{D}_i$	Коэффициенты двойственного базиса								$(C_i\ D_i)$	Число совпадений
			ε^{-i}	ε^{5}	ε^{9}	1	ε^{2}	ε^{3}	ε^{4}	$\varepsilon^{-i}\Sigma\ldots / C_i$		ε^{-i}	1	ε^{10}	0	1	ε^{5}	ε^{10}	$\varepsilon^{-i}\Sigma\ldots /D_i$		
0		$\check{C}_0$	1 (						)=		$\check{D}_0$	1 (						)=			
1		$\check{C}_1$	ε^{-1} (						)=		$\check{D}_1$	ε^{-5} (						)=			
2		$\check{C}_2$	ε^{-2} (						)=		$\check{D}_2$	ε^{-10} (						)=			
3		$\check{C}_3$	ε^{-3} (						)=		$\check{D}_3$	1 (						)=			
.....																					
14		$\check{C}_{14}$	ε^{-14} (						)=		$\check{D}_{14}$	ε^{-10} (						)=			

1.6.4 Декодирование с гарантийно неисправляемой ошибкой с предварительной децимацией

Приступая к выполнению этого пункта задания, внимательно изучить понятие о децимации (п. 1.4.1) и пример использования децимации для повышения эффективности декодирования (пп. 1.5.3.3). Анализ исправляемых изучаемым методом декодирования ошибок показал уверенное исправление подряд идущих ошибок в кодовой комбинации кратностью до пяти включительно при использовании кода БЧХЭ (15,6). При выборе индекса децимации рекомендуется учесть этот факт и определить по децимированным последовательностям пп. 1.5.3.3 требуемый индекс. Децимировать последовательность $v_2(x) = f(x) + e_2(x)$ с выбранным индексом и выполнить декодирование полученной децимированной последовательности $\overline{v}_2(x)$. Процедуру декодирования децимированной последовательности $\overline{v}_2(x)$ выполнить, используя шаблон табл. 6.4. Ввести элементы децимированной последовательности $\overline{v}_2(x)$ во входной регистр программной модели декодера и проверить совпадение результатов декодирования с расчетными. Поместить заполненную табл. 6.4 в отчет. В отчете кратко сформулировать причины, обеспечившие правильное решение декодера. При выполнении этого пункта работы необходимо учитывать связь между начальными фазами исходной и децимированной последовательностей, отмеченную в пп. 1.5.3.3.

Контрольные вопросы

1. Дайте определение:
- кода БЧХЭ,
- линейной однородной рекуррентной последовательности (далее рекуррентной последовательности),
- характеристического многочлена,
- базиса поля $GF(2^\kappa)$,
- функции-след,
- децимации.

2. Поясните:
- основные отличия кода БЧХЭ от кода БЧХ,
- возможные базисы поля $GF(2^\kappa)$,
- основные свойства характеристического многочлена,
- как характеристический многочлен связан с порождаемой им рекуррентной последовательностью,
- основные особенности рекуррентной последовательности,
- роль двойственного базиса в вычислении значений элементов рекуррентной последовательности,

- каким образом функция-след связана с элементами поля $GF(2^K)$,

- каким образом функция-след связана с рекуррентной последовательностью,

- каким образом функция-след связана с понятием двойственного базиса,

- принцип работы кодера кода БЧХЭ,

- принцип работы мажоритарного декодера кода БЧХЭ,

- состав и назначение основных функциональных узлов декодера кода БЧХЭ,

- необходимость применения децимации при декодировании кода БЧХЭ.

3. Вычислите:

- значение $g(x)$ для кода БЧХЭ (15,6),

- значение $P(x)$ для кода БЧХЭ (15,7),

- значение $P(x)$ для кода БЧХЭ (7,4),

- значение функции-след для элементов поля $GF(2^3)$ с $\pi(\varepsilon) = \varepsilon^3 + \varepsilon + 1 = 0$.

4. Нарисуйте:

- структурную схему кодера для кода БЧХЭ (15,7) и поясните принцип формирования кодовых комбинаций этого кода,

- структурную схему кодера для кода БЧХЭ (7,4) и поясните принцип формирования кодовых комбинаций этого кода,

- структурную схему генератора обратных элементов поля $GF(2^3)$ по многочлену $\pi(\varepsilon) = \varepsilon^3 + \varepsilon + 1 = 0$.

СОДЕРЖАНИЕ ОТЧЕТА

1. Название, цель работы и задание на лабораторную работу с указанием заданных значений информационной последовательности (C, D) и многочленов ошибок $e_1(x)$ и $e_2(x)$ из варианта задания.

2. Схема кодера кода БЧХЭ (15,6), (рис. 5.1) и сформированная кодовая комбинация $f(x)$ по заданной информационной последовательности (C, D) (табл. 6.1). Сформированную кодовую комбинацию представить в виде многочлена $f(x)$. Пояснения согласно п. 1.6.1.

3. Схема декодера кода БЧХЭ (15,6), (рис. 5.2) и последовательность $v_1(x) = f(x) + e_1(x)$, подлежащая декодированию. Процедуру декодирования последовательности $v_1(x) = f(x) + e_1(x)$ в виде заполненной табл. 6.2. Пояснения согласно п. 1.6.2.

4. Последовательность $v_2(x) = f(x) + e_2(x)$, подлежащая декодированию. Процедуру декодирования последовательности $v_2(x) = f(x) + e_2(x)$ в виде заполненной табл. 6.3. Пояснения согласно п. 1.6.3.

5. Обоснованный выбор индекса децимации, при котором возможно успешное декодирование последовательности $v_2(x) = f(x) + e_2(x)$ с гарантийно неисправляемой ошибкой. Децимированную с выбранным индексом последовательность $\overline{v}_2(x)$. Процедуру декодирования децимированной последовательности $\overline{v}_2(x)$ в виде заполненной табл. 6.4. Пояснения согласно п. 1.6.4.

6. Выводы относительно эффективности и области применения исследованных методов кодирования и декодирования кодов БЧХЭ.

Список литературы

1. Когновицкий, О. С. Двойственный базис и его применение в телекоммуникациях / О. С. Когновицкий. – СПб. : Линк, 2009. – 424 с.

2. Мареллос-Сарагоса, Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение / Р. Мареллос-Сарагоса ; пер. с англ. В. Б. Афанасьева. – М. : Техносфера, 2006. – 320 с.

3. Лидл, Р. Конечные поля. В 2-х т. / Р. Лидл, Г. Нидеррайтер ; пер. с англ. – М. : Мир, 1988. – 818 с.

4. Мак-Вильямс Ф. Дж., Теория кодов, исправляющих ошибки / Ф. Дж. Мак-Вильямс, Н. Дж. А. Слоэн ; пер. с англ. – М. : Связь, 1979. – 744 с.

Лабораторная работа 2

ИССЛЕДОВАНИЕ ПРИНЦИПОВ КОДИРОВАНИЯ И ДЕКОДИРОВАНИЯ КОДОВ РИДА–СОЛОМОНА С ИСПОЛЬЗОВАНИЕМ АЛГОРИТМА ЕВКЛИДА

2.1. Цель работы

Изучить принципы кодирования и декодирования кодов Рида–Соломона на примере кода (7,3) над полем $GF(2^3)$ и исследовать процедуры формирования кодовых комбинаций в кодере, и процедуры исправления ошибок в декодере, построенных на основе алгоритма Евклида.

2.2. Задание на лабораторную работу

1. Для кода Рида–Соломона (7,3) над полем $GF(2^3)$ сформировать кодовую комбинацию $f(x)$ по заданной информационной последовательности $K(x)$;

2. Декодировать принятую последовательность $f'(x) = f(x) + e(x)$, где $e(x)$ – многочлен ошибок, $f(x)$ – комбинация кода (7,3) с информационной частью $K(x)$; по результатам декодирования определить вид многочлена $e(x)$;

3. Перед началом выполнения работы дать ответы на контрольные вопросы.

2.3. Вариант задания

Значения $K(x)$, $f'(x)$, определяемые вариантом задания, приведены в табл. 2.1. В этой таблице α^i – элемент поля $GF(2^3)$.

Таблица 2.1

$g(x)=(x-\alpha)\cdot(x-\alpha^2)\cdot(x-\alpha^3)\cdot(x-\alpha^4)$		
№ варианта	$K(x)$ для кодирования	$f'(x)$ для декодирования
1	$\alpha^0x^4+\alpha^0x^5+\alpha^0x^6$	$\alpha^0+\alpha^3x^1+\alpha^0x^6$
2	$\alpha^0x^4+\alpha^0x^5+\alpha^1x^6$	$\alpha^3x^3+\alpha^2x^4$
3	$\alpha^0x^4+\alpha^0x^5+\alpha^2x^6$	$\alpha^0x^5+\alpha^0x^6$
4	$\alpha^0x^4+\alpha^1x^5+\alpha^2x^6$	$\alpha^3+\alpha^4x^2+\alpha^0x^5+\alpha^0x^6$
5	$\alpha^0x^4+\alpha^1x^5+\alpha^3x^6$	α^4x^2
6	$\alpha^0x^4+\alpha^1x^5+\alpha^4x^6$	$\alpha^6+\alpha^3x^5$
7	$\alpha^1x^4+\alpha^1x^5+\alpha^4x^6$	$\alpha^0x^3+\alpha^2x^4$
8	$\alpha^1x^4+\alpha^2x^5+\alpha^4x^6$	$\alpha^1x^3+\alpha^5x^4$
9	$\alpha^1x^4+\alpha^3x^5+\alpha^4x^6$	α^6x^2
10	$\alpha^1x^4+\alpha^4x^5+\alpha^4x^6$	$\alpha^1x^3+\alpha^5x^4+\alpha^3x^5$
11	$\alpha^1x^4+\alpha^4x^5+\alpha^4x^6$	α^5x^1

Окончание табл. 2.1

12	$\alpha^1x^4+\alpha^5x^5+\alpha^4x^6$	$\alpha^3x^3+\alpha^3x^4$
13	$\alpha^1x^4+\alpha^6x^5+\alpha^4x^6$	$\alpha^1x^1+\alpha^3x^3$
14	$\alpha^2x^4+\alpha^1x^5+\alpha^1x^6$	$\alpha^3+\alpha^3x^5$
15	$\alpha^2x^4+\alpha^2x^5+\alpha^1x^6$	$\alpha^5+\alpha^1x^2$
16	$\alpha^2x^4+\alpha^3x^5+\alpha^3x^6$	$\alpha^1+\alpha^0x^2+\alpha^3x^4$
17	$\alpha^5x^4+\alpha^1x^5+\alpha^2x^6$	$\alpha^1x^2+\alpha^2x^5$
18	$\alpha^5x^4+\alpha^2x^5+\alpha^2x^6$	$\alpha^0x^5+\alpha^5x^6$
19	$\alpha^5x^4+\alpha^3x^5+\alpha^2x^6$	$\alpha^2x^3+\alpha^5x^4$
20	$\alpha^5x^4+\alpha^4x^5+\alpha^2x^6$	α^5x^5
21	$\alpha^5x^4+\alpha^5x^5+\alpha^2x^6$	$\alpha^3x^2+\alpha^3x^6$
22	$\alpha^5x^4+\alpha^6x^5+\alpha^2x^6$	$\alpha^6x^1+\alpha^3x^4$
23	$\alpha^4x^4+\alpha^1x^5+\alpha^6x^6$	$\alpha^2x^2+\alpha^5x^6$
24	$\alpha^4x^4+\alpha^2x^5+\alpha^6x^6$	$\alpha^0x^5+\alpha^6x^6$
25	$\alpha^4x^4+\alpha^3x^5+\alpha^6x^6$	$\alpha^1x^1+\alpha^5x^4$

2.4. Теоретические сведения

2.4.1. Поля Галуа

Поля с конечным числом элементов p называют полями Галуа по имени их первого исследователя Эвариста Галуа и обозначают GF(p). Поле, образованное многочленами над полем GF(p) по модулю неприводимого многочлена $\pi(\alpha)$ степени m, называется расширением поля степени m над GF(p) или расширенным полем. Оно содержит p^m элементов и обозначается GF(p^m).

В данной лабораторной работе используется поле GF(2^3). В табл. 2.2 представлены различными способами элементы этого поля, образованного по модулю неприводимого примитивного многочлена $\pi(\alpha)=1+\alpha+\alpha^3$.

Таблица 2.2

Последовательность длины 3	Многочлен	Степень
000	0	0
100	1	α^0
010	α	α^1
001	α^2	α^2
110	$\alpha^3=1+\alpha$	α^3
011	$\alpha^4=\alpha+\alpha^2$	α^4
111	$\alpha^5=1+\alpha+\alpha^2$	α^5
101	$\alpha^6=1+\alpha^2$	α^6

Для удобства выполнения вычислений в поле $GF(2^3)$ ниже приведены таблицы сложения в поле $GF(2^3)$ (табл. 2.3) и умножения в этом поле (табл. 2.4).

Таблица 2.3

+	0	1	α^1	α^2	α^3	α^4	α^5	α^6
0	0	1	α^1	α^2	α^3	α^4	α^5	α^6
1	1	0	α^3	α^6	α^1	α^5	α^4	α^2
α^1	α^1	α^3	0	α^4	1	α^2	α^6	α^5
α^2	α^2	α^6	α^4	0	α^5	α^1	α^3	1
α^3	α^3	α^1	1	α^5	0	α^6	α^2	α^4
α^4	α^4	α^5	α^2	α^1	α^6	0	1	α^3
α^5	α^5	α^4	α^6	α^3	α^2	1	0	α^1
α^6	α^6	α^2	α^5	1	α^4	α^3	α^1	0

Таблица 2.4

×	0	1	α^1	α^2	α^3	α^4	α^5	α^6
0	0	0	0	0	0	0	0	0
1	0	1	α^1	α^2	α^3	α^4	α^5	α^6
α^1	0	α^1	α^2	α^3	α^4	α^5	α^6	1
α^2	0	α^2	α^3	α^4	α^5	α^6	1	α^1
α^3	0	α^3	α^4	α^5	α^6	1	α^1	α^2
α^4	0	α^4	α^5	α^6	1	α^1	α^2	α^3
α^5	0	α^5	α^6	1	α^1	α^2	α^3	α^4
α^6	0	α^6	1	α^1	α^2	α^3	α^4	α^5

2.4.2. Код Рида–Соломона (7,3)

Код Рида–Соломона (7,3), рассматриваемый в данной лабораторной работе, является циклическим кодом, множество кодовых комбинаций которого представляется многочленами степени 6 и менее с коэффициентами из поля $GF(2^3)$. Для кодов Рида–Соломона справедливо, что символы кодовых комбинаций (коэффициенты кодовых многочленов) и корни этих многочленов – это элементы одного и того же поля – в рассматриваемом случае расширенного поля $GF(2^3)$. Каждая кодовая комбинация имеет

3 информационных элемента и 4 проверочных. Минимальное кодовое расстояние $d = n - k + 1 = 5$. Кратность гарантийно исправляемых ошибок $t = 2$.

Порождающий многочлен кода (7,3) – $g(x)=(x-\alpha)\cdot(x-\alpha^2)\cdot(x-\alpha^3)\cdot(x-\alpha^4)$, где α^1, α^2, α^3 и α^4 – корни порождающего многочлена – элементы расширенного поля $GF(2^3)$.

Коды Рида–Соломона (РС-коды) являются частным случаем кодов БЧХ. Для них справедлив алгебраический метод декодирования, известный под названием «Быстрое декодирование кодов БЧХ» [1].

2.4.3. Быстрое декодирование кодов БЧХ

2.4.3.1. Ключевое уравнение

Быстрое декодирование кодов БЧХ основывается на решении уравнения, которое получило название *ключевого уравнения*. Рассмотрим предпосылки формирования ключевого уравнения.

Пусть в приемник АПД поступила кодовая комбинация РС-кода

$$C(x) = f(x) + e(x),$$

где $f(x)$ – переданная передатчиком АПД кодовая комбинация, в которой в процессе передачи по каналу связи произошло v ошибок, отображаемых многочленом $e(x)$. Здесь $0 \le v \le t$.

Многочлен ошибок можно представить в виде

$$e(x) = e(x) = e_{i_1} x^{i_1} + e_{i_2}, \qquad x^{i_2} + \ldots + e_{i_v} x^{i_v},$$

где e_{i_1} – значение ошибки, а x^{i_1} – локатор ошибки, т. е. номер позиции кодовой комбинации, в которой произошла ошибка.

Задачей декодирования является исправление ошибок на основе вычисления значений e_{i_1} и x^{i_1} для каждой из $v \le t$ ошибок. С этой целью и составляется ключевое уравнение. Его компонентами являются синдромный многочлен $S(x)$, многочлен локаторов ошибок $\Lambda(x)$ и многочлен значений ошибок $\Omega(x)$.

Синдромный многочлен $S(x) = S_1 x^0 + S_2 x^1 + \ldots + S_{n-k} x^{n-k-1}$ является расширением понятия синдрома принятой кодовой комбинации и содержит $n - k$ синдромов S_l в качестве своих коэффициентов.

Коэффициенты $S(x)$ – синдромы S_l, вычисляются подстановкой в принятую комбинацию $C(x)$ каждого из $n - k$ корней α^l порождающего многочлена кода РС:

$$S_l = C(x = \alpha^l) = f(x = \alpha^l) + e(x = \alpha^l) = e(\alpha^l), \text{ где } 1 \le l \le 2t.$$

Например, для l=1 получим: $S_1 = e_{i1}\alpha^{i1} + e_{i2}\alpha^{i2} + \ldots + e_{iv}\alpha^{iv}$ и т. д.

Для упрощения записи компонентов синдромного многочлена обозначим в выражении для $e(x) = e_{i1}x^{i1} + e_{i2}x^{i2} + \ldots + e_{iv}x^{iv}$ значения ошибки e_{il}

через Y_l, $Y_l = e_{il}$, а локаторы ошибок $x^{il} = \alpha^l$ через X_l, $X_l = \alpha^l$, где α – примитивный элемент поля GF(q), над которым построен код.

В этих новых обозначениях S_1 запишется в виде

$$S_1 = Y_1X_1 + Y_2X_2 + \ldots + Y_vX_v,$$

где Y_l – значение ошибки на позиции l кодовой комбинации, $X_l = \alpha^l$ – локатор этой ошибки.

В результате получим следующую систему из $n - k = 2t$ уравнений относительно v неизвестных локаторов $X_1,\ldots, X_v$ и v неизвестных значений ошибок $Y_1,\ldots, Y_v$:

$$\begin{cases} S_1 = Y_1X_1 + Y_2X_2 + \ldots + Y_vX_v, \\ S_2 = Y_1X_1^2 + Y_2X_2^2 + \ldots + Y_vX_v^2 \\ \ldots \\ S_{2t} = Y_1X_1^{2t} + Y_2X_2^{2t} + \ldots + Y_vX_v^{2t}. \end{cases}$$

В силу определения синдрома эта система уравнений должна иметь хотя бы одно решение. В теории кодирования доказано, что это решение единственно и вытекает из решения ключевого уравнения [1]. Для его формирования вводятся еще два многочлена.

Многочлен локаторов ошибок $\Lambda(x) = 1 + \Lambda_1 x + \Lambda_2 x^2 + \Lambda_v x^v$, имеющий корни, обратные локаторам ошибок X_l^{-1}, $l = 1,\ldots, v$.

Это позволяет представить $\Lambda(x)$ в следующем виде:

$$\Lambda(x) = \prod_{l=1}^{v}(1 + xX_l),$$

здесь $X_l = \alpha^l$ – локатор ошибки, α^l – элемент поля GF(q).

Из данной формы многочлена локаторов ошибок непосредственно видно, что его корнями являются элементы поля GF(q), обратные локаторам ошибок: $X_l^{-1} = \alpha^{-l}$, где $1 \le l \le v$.

Многочлен значений ошибок $\Omega(x)$, определяющийся через $S(x)$ и $\Lambda(x)$ в соответствии с видом введенного выше многочлена ошибок [1]:

$$\Omega(x) = S(x)\Lambda(x) (\mathrm{mod}\, x^{2t}) = [(S_1x^0 + S_2x^1 + \ldots + S_{2t}\, x^{2t-1}) \prod_{l=1}^{v}(1 + xX_l)] (\mathrm{mod}\, x^{2t}) =$$

$$= \sum_{j=1}^{v} Y_jX_j \prod_{l \ne j}(1 + xX_l).$$

Компоненты синдромного многочлена $S(x)$ известны лишь до коэффициента при степени x^{n-k-1}. Это обусловило необходимость приведения результата умножения $S(x) \cdot \Lambda(x)$ в определении многочлена значений ошибок $\Omega(x)$ по модулю $x^{n-k=2t}$. Степень многочлена значений ошибок, как это видно из приведенного выше выражения $\Omega(x) = \sum_{j=1}^{v} Y_jX_j \prod_{l \ne j}(1 + xX_l)$, меньше сте-

пени многочлена локаторов ошибок. Если степень $\Lambda(x)$ равна v, то степень $\Omega(x)$ меньше v.

Уравнение $\Omega(x) = S(x)\Lambda(x) (\mathrm{mod}\, x^{2t})$ определяет множество из $2t - v$ уравнений и называется *ключевым уравнением*, так как оно является ключом решения задачи декодирования.

Ключевое уравнение позволяет получить v уравнений для v неизвестных коэффициентов $\Lambda(x)$. Эти уравнения являются линейными. Они могут быть решены обычными методами либо с помощью итерационных процедур. Исходными данными для составления и решения ключевого уравнения являются синдромный многочлен $S(x)$ и x^{2t}. После нахождения $\Lambda(x)$ или одновременно с ним ключевое уравнение позволяет найти многочлен значений ошибок $\Omega(x)$, а с их помощью – неизвестные компоненты многочлена $e(x)$ и затем – переданную кодовую комбинацию $f(x)=C(x)+e(x)$.

Из изложенного можно сделать вывод, что декодирование кодов БЧХ на основе решения ключевого уравнения распадается на два этапа.

I этап – вычисление многочлена локаторов ошибок $\Lambda(x)$. Для двоичных кодов БЧХ этим этапом декодирование завершается.

II этап – для недвоичных кодов, какими являются РС-коды, вычисление многочлена значений ошибок $\Omega(x)$, позволяющего вычислить значение каждой из v ошибок в принятой комбинации.

Известны три алгоритма решения ключевого уравнения:

1) алгоритм Питерсона,

2) алгоритм Берлекэмпа–Месси,

3) алгоритм Евклида – алгоритм СКХН.

Авторы первого и второго алгоритмов указаны в их названии. Алгоритм Евклида для целей решения ключевого уравнения был впервые предложен четырьмя авторами: Сугияма, Касахара, Хирасава и Намекава. В дальнейшем для краткости будем называть алгоритмом Евклида.

2.4.3.2. Решение ключевого уравнения

Как отмечалось выше, целью настоящей работы является изучение принципов кодирования и декодирования кодов Рида–Соломона на примере кода (7,3) над полем $GF(2^3)$ и исследование процедур кодирования и декодирования с исправлением ошибок соответственно в кодере и в декодере, построенных на основе алгоритма Евклида.

Прежде чем приступить к реализации поставленной цели целесообразно более детально освоить процедуры декодирования и кодирования кодов Рида–Соломона на основе решения ключевого уравнения. Для этого рассмотрим два примера.

Пример 1. Декодирование с исправлением ошибок

Порождающий многочлен кода РС (7,3) $g(x) = \alpha^3 + \alpha x + x^2 + \alpha^3 x^3 + x^4$ над полем GF(2^3) является одной из возможных кодовых комбинаций рассматриваемого кода. Предположим, что эта комбинация при передаче по каналу связи под воздействием помех исказилась и на вход декодера поступила комбинация $f'(x)= \alpha x + x^2 + \alpha^3 x^3$. Задачей декодирования кодов Рида–Соломона на основе процедур быстрого декодирования кодов БЧХ является нахождение многочлена локаторов ошибок $\Lambda(x)$ как многочлена минимальной степени, удовлетворяющего ключевому уравнению, и многочлена значений ошибок $\Omega(x)$.

Анализ комбинации $f'(x)$ показывает, что многочлен ошибок для принятой комбинации имеет вид $e(x) = \alpha^3 + x^4$, т. е. локаторы ошибок равны $X_0 = \alpha^0$ и $X_4 = \alpha^4$, а значения ошибок равны $Y_0 = \alpha^3$ и $Y_4 = 1$. Рассмотрим, как эти же значения локаторов и значений ошибок вычисляются на основе алгоритма быстрого декодирования кодов БЧХ с помощью ключевого уравнения. Исходными данными для решения поставленной задачи являются: принятая кодовая комбинация $f'(x)= \alpha x + x^2 + \alpha^3 x^3$, корни порождающего многочлена α^1, α^2, α^3, α^4 и способность кода исправлять ошибки кратности до $t=2$ включительно. Заметим, что локаторы ошибок, значения ошибок и корни порождающего многочлена это элементы поля GF(2^3). Решение возможно, если число ошибок в принятой комбинации $\nu \le 2$.

Процесс декодирования начинается с вычисления синдромного многочлена:

$$S(x)= S_1 x^0 + S_2 x^1 + S_3 x^2 + S_4 x^3.$$

Находим:

$S_1 = f'(x = \alpha^1) = \alpha\alpha + \alpha^2 + \alpha^3\alpha^3 = \alpha^2 + \alpha^2 + \alpha^6 = \alpha^6$,

$S_2 = f'(x = \alpha^2) = \alpha\alpha^2 + \alpha^4 + \alpha^3\alpha^6 = \alpha^3 + \alpha^4 + \alpha^2 = 1$,

$S_3 = f'(x = \alpha^3) = \alpha\alpha^3 + \alpha^6 + \alpha^3\alpha^9 = \alpha^4 + \alpha^6 + \alpha^5 = \alpha^2$,

$S_4 = f'(x = \alpha^4) = \alpha\alpha^4 + \alpha^8 + \alpha^3\alpha^{12} = \alpha^5 + \alpha + \alpha = \alpha^5$.

Итак, $S(x)= \alpha^6 + x + \alpha^2 x^2 + \alpha^5 x^3$.

Условия нашей задачи позволяют найти многочлен локаторов ошибок без решения ключевого уравнения, что невозможно в реальной процедуре декодирования.

Вычисляем $\Lambda(x)$ по известным локаторам ошибок ($X_0 = \alpha^0$ и $X_4 = \alpha^4$) по формуле $\Lambda(x) = \prod_{l=1}^{\nu}(1+xX_l) = (1+x\,\alpha^0)\,(1+x\alpha^4) = 1 + \alpha^4 x + x + \alpha^4 x^2 = 1 + \alpha^5 x + \alpha^4 x^2$. Легко видеть, что корни $\Lambda(x)$ есть: $x_1 = 1/\,\alpha^0 = 1$ и $x_2 = 1/\,\alpha^4 = \alpha^3$. Производная от $\Lambda(x)$ равна $\Lambda'(x)= 0 + \alpha^5 + 2\,\alpha^4 x = \alpha^5$.

В соответствии с ключевым уравнением находим многочлен значений ошибок:

$$\Omega(x) = S(x)*\Lambda(x)(\mathrm{mod}\, x^{2t})=(\alpha^6 + x + \alpha^2x^2 + \alpha^5x^3)(1+ \alpha^5x + \alpha^4x^2)(\mathrm{mod}\, x^4) = \\ = \alpha^6 + \alpha^5x.$$

Выражение для вычисления значения ошибки имеет вид, определяемый [1, 2] как алгоритм Форни:

$$Y_i = \alpha^{i(1-m)} \frac{\Omega(x=\alpha^{-i})}{\Lambda'(x=\alpha^{-i})},$$

здесь α^{-i} – корень $\Lambda(x)$, α^i – локатор ошибки, m – степень первого корня в последовательности корней порождающего многочлена РС кода.

С учетом найденных значений корней $\Lambda(x)$ вычисляем:

$$Y_0 = (\alpha^6 + \alpha^5) / \alpha^5 = \alpha / \alpha^5 = \alpha^3,$$
$$Y_4 = (\alpha^6 + \alpha^5\alpha^3) / \alpha^5 = (\alpha^6 + \alpha) / \alpha^5 = \alpha^5 / \alpha^5 = 1.$$

Полученные результаты полностью совпадают с исходными.

Пример 2. Кодирование

Возьмем тот же самый код РС (7,3) с порождающим многочленом $g(x) = \alpha^3 + \alpha x + x^2 + \alpha^3x^3 + x^4$ и выполним кодирование информационной последовательности $K(x) = \alpha^0x^4$. Для решения поставленной задачи воспользуемся способностью кодов РС исправлять до $n - k$ стираний. Под стиранием понимают ошибку с известным местоположением, т. е. локатором.

Полагая стертые избыточные элементы кодовой комбинации с известной информационной частью $f'(x) = K(x) = \alpha^0x^4$ равными нулю $f_0' = f_1' = f_2' = f_3' = 0$, поставим задачу методом быстрого декодирования восстановить значение неизвестных избыточных элементов и тем самым сформировать искомую кодовую комбинацию $f(x)$, т. е. выполнить процедуру кодирования.

Как и в предыдущем примере, первым шагом процедуры кодирования является вычисление синдромного многочлена: $S(x) = \alpha^4+\alpha x+ \alpha^5x^2+\alpha^2x^3$.

Знание расположения избыточных элементов, т. е. локаторов стираний, позволяет на следующем шаге найти многочлен локаторов стираний $\Gamma(x)$ тем же способом, как в предыдущем примере был вычислен многочлен локаторов ошибок $\Lambda(x)$:

$$\Gamma(x) = (1 + x)(1 + \alpha x)(1 + \alpha^2x)(1 + \alpha^3x) = 1 + \alpha^2x + \alpha^5x^2 + \alpha^5x^3 + \alpha^6x^4.$$

Корнями $\Gamma(x)$ являются $x_1 = 1, x_2 = \alpha^6, x_3 = \alpha^5, x_4 = \alpha^4$. Производная $\Gamma(x)$ имеет вид: $\Gamma'(x) = \alpha^2 + \alpha^5x^2$.

Теперь можно вычислить многочлен значений стираний:

$$\Omega(x) = S(x) * \Gamma(x)(\mathrm{mod}\, x^{2t}) = (\alpha^4 + \alpha x + \alpha^5x^2 + \alpha^2x^3)(1 + \alpha^2x + \alpha^5x^2 + \\ + \alpha^5x^3 + \alpha^6x^4)(\mathrm{mod}\, x^4) = \alpha^4 + \alpha^5x + \alpha^2x^3.$$

Значения стираний определяем по приведенной выше формуле с заменой $\Lambda'(x)$ на $\Gamma'(x)$: $Y_i = \alpha^{i(1-m)} \dfrac{\Omega(x=\alpha^{-i})}{\Gamma'(x=\alpha^{-i})}$.

Расчеты дают следующие значения избыточных элементов:

$Y_0 = (\alpha^4 + \alpha^5 + \alpha^2) / (\alpha^2 + \alpha^5) = \alpha^6 / \alpha^3 = \alpha^3$,

$Y_1 = (\alpha^4 + \alpha^4 + \alpha^6) / (\alpha^2 + \alpha^3) = \alpha^6 / \alpha^5 = \alpha$,

$Y_2 = (\alpha^4 + \alpha^3 + \alpha^3) / (\alpha^2 + \alpha) = \alpha^4 / \alpha^4 = 1$,

$Y_3 = (\alpha^4 + \alpha^2 + \alpha^0) / (\alpha^2 + \alpha^6) = \alpha^3 / \alpha^0 = \alpha^3$.

Результатом выполненной процедуры кодирования является следующая комбинация РС кода (7,3): $f(x) = \alpha^3 + \alpha x + x^2 + \alpha^3 x^3 + x^4$. Данная комбинация нам известна как порождающий многочлен рассматриваемого кода.

Перейдем к рассмотрению реализации процедур кодирования и декодирования кодов Рида–Соломона на основе решения ключевого уравнения по алгоритму Евклида [2].

Алгоритм Евклида. Алгоритм Евклида представляет собой рекуррентный метод нахождения наибольшего общего делителя (НОД) двух целых чисел или двух многочленов. В основе этого алгоритма лежит следующее утверждение. Пусть a и b – два целых числа или многочлена, причем $a \geq b$, если это числа, и $\deg(a) \geq \deg(b)$, если это многочлены (значок deg означает степень). Разделим a на b. Если остаток от деления r равен 0, то $d = b$ является наибольшим общим делителем. Если остаток не равен 0, заменим a на b, b на r и повторим деление. Рассмотрим пример, показывающий, что изложенный алгоритм приводит к НОД.

Пример. Найти НОД целых чисел $a = 186$ и $b = 66$.

Действуя по алгоритму Евклида, получаем:

итерация 1: $186 = 66 \times 2 + 54$,

итерация 2: $66 = 54 \times 1 + 12$,

итерация 3: $54 = 12 \times 4 + 6$,

итерация 4: $12 = 6 \times 2 + 0$.

Поскольку $d = 6$ делит 186 и 66, оно должно делить и 54. Поскольку d делит 66 и 54, оно должно делить и 12. Наконец, поскольку оно делит 54 и 12, оно должно делить 6 и поэтому является НОД. В процессе нахождения НОД согласно алгоритму Евклида вычисляются два числа f и g (или многочлена $f(x)$ и $g(x)$), для которых $fa + gb = d$.

Для алгоритма Евклида полезными являются промежуточные результаты. При каждой итерации вычисляются числа (многочлены) f_i, g_i, такие, что $f_i a + g_i b = r_i$.

Существуют рекуррентные соотношения между f_i, g_i и r_i на различных итерациях. Для их установления выполним следующие преобразования с итерациями нахождения НОД. Цель преобразований – привести содержание шагов итераций к виду $f_i a + g_i b = r_i$.

Суть преобразований:

Шаг 1. Приводим уравнение итерации 1 к требуемой форме:

$$1\times186 - 2\times66 = 54.$$

Шаг 2. Из уравнения итерации 2 находим: 54 = 66 – 12, подставляем найденное значение для 54 в уравнение итерации 1 и получаем

$$(-1)\times186 + 3\times66 = 12.$$

Шаг 3. Найденные выражения для чисел 54 и 12 подставляем в уравнение итерации 3 и получаем

$$5\times186 - 14\times66 = 6.$$

Шаг 4. Найденные выражения для чисел 12 и 6 подставляем в уравнение итерации 4 и получаем

$$(-11)\times186 + 31\times66 = 0.$$

Поставленная задача решена. Анализ полученных выражений показывает, что уравнение каждого шага получается из двух предыдущих по формуле $E_i = E_{i-2} - q_i E_{i-1}$, где E_i определяет значения f_i, g_i и r_i на различных шагах итераций, а q_i – отношение двух предыдущих остатков: $q_i = [r_{i-2}/r_{i-1}]$, здесь [] означает целую часть дроби r_{i-2}/r_{i-1}.

Для подтверждения этого вывода введем два формальных шага.

Шаг(–1). $1\times186 + 0\times66 = 186$,

Шаг 0. $0\times186 + 1\times66 = 66$.

Теперь процесс нахождения НОД(186,66) можно представить в табличном виде (табл. 2.5).

Таблица 2.5

Шаг i	f_i	g_i	d_i	q_i	$f_i \cdot a + g_i \cdot b = d_i$
–1	1	0	186	–	$1\cdot186 + 0\cdot66 = 186$
0	0	1	66	–	$0\cdot186 + 1\cdot66 = 66$
1	1	–2	54	[186/66]=2	$1\cdot186 - 2\cdot66 = 54$
2	–1	3	12	[66/54]=1	$-1\cdot186 + 3\cdot66 = 12$
3	5	–14	6	[54/12]=4	$5\cdot186 - 14\cdot66 = 6$
4	–11	31	0	[12/6]=2	$-11\cdot186 + 31\cdot66 = 0$

Выполненные преобразования используются при быстром декодировании кодов БЧХ для решения ключевого уравнения по алгоритму Евклида. Поскольку процедура декодирования кодов БЧХ выполняется для многочленов, повторим вышеприведенные рассуждения применительно к многочленам.

Известно, если существует наибольший общий делитель $d(x)$ двух многочленов $a(x)$ и $b(x)$, то существуют многочлены $f(x)$ и $g(x)$ такие, что справедливо: $a(x)f(x)+b(x)g(x)= d(x)$.

Многочлен $d(x)$ может быть найден по алгоритму Евклида, который состоит в последовательном делении с остатком $a(x)$ на $b(x)$, затем $b(x)$ на первый остаток $r_1(x)$, затем $r_1(x)$ на второй остаток $r_2(x)$ и т. д.

Пример. Найти наибольший общий делитель $d(x)$ двух многочленов $a(x)=x^3+1$ и $b(x)=x^2+1$, а также многочлены $f(x)$ и $g(x)$, для которых выполняется: $a(x)f(x)+b(x)g(x)= d(x)$ в двоичном поле. Результаты расчетов представим в виде табл. 2.6.

Таблица 2.6

Функция	Шаг итерации i			
	–1	0	1	2
$f_i(x)$	1	0	1	$x+1$
$g_i(x)$	0	1	x	x^2+x+1
$r_i(x)$	x^3+1	x^2+1	$x+1$	0
$q_i(x)$	–	–	x	$x+1$

Искомое значение $d(x)$ определяется последним ненулевым значением $r_i(x)$, т. е. $d(x) = r_1(x) = x + 1$. Многочлены $f(x)$ и $g(x)$ найдены на шаге 2 при нулевом значении остатка $r_i(x)$. Обратим внимание на то, что с ростом шага итерации степени многочленов $f_i(x)$ и $g_i(x)$ возрастают, а степень многочлена $r_i(x)$, что вполне ожидаемо, уменьшается.

При декодировании кодов БЧХ интересуются не конечным результатом алгоритма Евклида, а промежуточными результатами, которые можно представить в виде: $a(x)f_i(x) + b(x)g_i(x) = r_i(x)$.

У. Сугияма и его соавторы использовали этот результат для решения ключевого уравнения следующим образом: $b(x)g_i(x) = r_i(x)(\mathrm{mod}\ a(x))$, полагая, $a(x) = x^{2t}$, $b(x) = S(x)$, $g_i(x) = \Lambda_i(x)$, $r_i(x) = \Omega_i(x)$.

При этом используется свойство алгоритма Евклида:

$$\deg[g_i(x)] + \deg[r_{i-1}(x)] = \deg[a(x)].$$

Если $a(x) = x^{2t}$, то $\deg[\Lambda_i(x)] + \deg[\Omega_{i-1}(x)] = 2t$,

$$\deg[\Lambda_i(x)] + \deg[\Omega_i(x)) < 2t.$$

При появлении $v \le t$ ошибок имеем: $\deg[\Omega_i(x)] < \deg[\Lambda_i(x)] \le t$.

Существует единственный с точностью до постоянного множителя (элемента поля) многочлен $\Lambda_i(x)$ степени $\le t$, удовлетворяющий ключевому уравнению:

$$\Omega_i(x) = S(x)\,\Lambda_i(x) \pmod{x^{2t}}.$$

Кроме того, если $\deg[\Omega_{i-1}(x)] \ge t$ при $\deg[\Lambda_i(x)] \le t$ и $\deg[\Omega_i(x)] < t$, то $\deg[\Lambda_{i+1},(x)] > t$.

Поэтому промежуточные результаты на i-м шаге дают единственное интересующее нас решение ключевого уравнения.

Таким образом, для решения ключевого уравнения следует применять алгоритм Евклида до тех пор, пока не будет выполнено условие $\deg[\Omega_i(x)] < t$.

Итак, алгоритм Евклида решения ключевого уравнения по методу У. Сугиямы и др. сводится к следующему.

1. Применить алгоритм Евклида к $a(x) = x^{2t}$ и $b(x) = S(x)$.

2. Использовать начальные условия: $\Lambda_{-1}(x)=0$, $\Lambda_0(x)=1$, $\Omega_{-1}(x) = x^{2t}$, $\Omega_0(x) = S(x)$.

3. Остановиться, если $\deg[\Omega_i(x)] < t$.

4. Положить $\Lambda(x) = \Lambda_i(x)$ и $\Omega(x) = \Omega_i(x)$.

При вычислении значений $\Lambda_i(x)$ и $\Omega_i(x)$ следует использовать свойство алгоритма Евклида: каждое из значений $\Lambda_i(x)$ и $\Omega_i(x)$ получается из двух предшествующих значений по следующей общей формуле:

$E_i(x)=E_{i-2}(x)+q_iE_{i-1}(x)$, где $q_i(x)=\left[\dfrac{\Omega_{i-2}(x)}{\Omega_{i-1}(x)}\right]_0^{\infty}$ – частное от деления указанных многочленов без учета остатка, т. е. многочлен степени 0 и более.

2.4.4. Кодирование

Кодирование комбинации $K(x)$ реализуется как исправление стираний, размещенных на местах избыточных элементов кодовой комбинации, информационные элементы которой известны. Таким образом, локаторы стираний известны, а стертые элементы принимаются нулевыми по значению. Схема кодирования по алгоритму Евклида имеет вид, представленный на рис. 2.1, где подстрочные индексы у символов многочленов значения ошибок $\Omega_i(x)$, и локаторов стираний $\Gamma_i(x)$ указывают их принадлежность к начальным условиям итеративной процедуры, реализующей алгоритм Евклида. Из рис. 2.1 можно сделать вывод, что вся процедура кодирования по алгоритму Евклида осуществляется на стадии формирования начальных условий, т. е. ограничена шагами: –1 и 0. Введение специального символа $T(x)$ для обозначения многочлена значения стираний, наряду с $\Omega_i(x)$, обозначающим многочлен значения ошибок, заимствовано из общего случая процедуры декодирования на основе алгоритма Евклида с исправлением ошибок и стираний [2], который в данной работе не предусмотрен.

Рис. 2.1. Схема кодирования по алгоритму Евклида

Для кода (7,3) информационные элементы имеют локаторы α^4, α^5, α^6. Избыточные элементы неизвестны и подлежат определению при выполнении процедуры кодирования. Удобно принять значения избыточных элементов, равными нулю.

Таким образом, кодируемая комбинация принимает вид многочлена $f'(x)=f_4x^4+f_5x^5+f_6x^6$. Проверочные элементы f_0, f_1, f_2 и f_3 имеют локаторы α^0, α^1, α^2 и α^3 соответственно.

Для описания стираний используются:

1) многочлен локаторов стираний:

$$\Gamma(x)=\prod_{i=1}^{v}(1-xX_i),$$

имеющий корни X_i^{-1}, i = 1,..., v взаимные к локаторам стираний, т. е. $X_i^{-1}\alpha^l=1$. Поскольку локаторы стираний известны, известен и многочлен локаторов стираний $\Gamma(x)=(1+\alpha^0x)\cdot(1+\alpha^1x)\cdot(1+\alpha^2x)\cdot(1+\alpha^3x)$.

Корни многочлена локаторов стираний:

α^0 соответствует локатору α^0,

α^6 соответствует локатору α^1,

α^5 соответствует локатору α^2,

α^4 соответствует локатору α^3;

2) многочлен значений стираний $T(x)$ (видоизмененный синдромный многочлен): $T(x)=\Gamma(x)\cdot S(x)\bmod(x^{2t})$, где $t=2$ – кратность гарантийно исправляемых кодом ошибок;

3) вид синдромного многочлена $S(x)$ зависит от кодовой комбинации $f'(x)$, поступившей на вход кодера. Общий вид синдромного многочлена $S(x)=S_1+S_2x^1+S_3x^2+S_4x^3$, где S_1, S_2, S_3, S_4 определяются подстановкой значений корней порождающего многочлена в $f'(x)$.

Результаты расчетов $\Gamma(x)$ и $T(x)$ представлены в табл. 2.7 на позициях шагов –1 и 0 в качестве исходных данных процедуры кодирования, которая завершается вычислением значений стираний на позициях избыточных элементов.

Таблица 2.7

Функция	Шаг	
	–1	0
$\Gamma(x)$	0	$\Gamma(x)=(1+\alpha^0x)\cdot(1+\alpha^1x)\cdot(1+\alpha^2x)\cdot(1+\alpha^3x)$
$\Omega(x)$	x^4	$\Omega_0(x)=T(x)=\Gamma(x)\cdot S(x)\bmod(x^4)$

Для определения значений стираний используется алгоритм Форни.

1. Вычисляется производная многочлена локаторов стираний $\Gamma'(x)$.

2. Значения корней X_l^{-1} многочлена локаторов стираний $\Gamma(x)$ уже известны из начальных условий, так как они обратны локаторам стираний в кодовой последовательности.

3. Вычисляются значения стираний (которые соответствуют искомым избыточным элементам) по формуле:

$$Y_l = \frac{\Omega_0(X_l^{-1})}{\Gamma'(X_l^{-1})}.$$

Таким образом, находятся избыточные элементы и этим процедура кодирования завершается.

2.4.5. Декодирование

Декодирование комбинации представляет собой исправление ошибок. При этом локаторы ошибок заранее неизвестны.

Алгоритм процедуры декодирования по алгоритму Евклида имеет вид, представленный на рис. 2.2.

Для описания ошибок используются:

1) многочлен локаторов ошибок: $\Lambda(x) = \prod_{i=1}^{v}(1 - xX_i)$, где $X_i = \alpha^i$ – локатор ошибки. Многочлен локаторов ошибок имеет корни X_i^{-1}, i = 1,..., v, взаимные к локаторам ошибок, т. е. $X_i^{-1}\alpha^i = 1$;

2) многочлен значений ошибок $\Omega(x)$:

$$\Omega(x) = S(x)\Lambda(x) \pmod{x^{2t}},$$

где t – кратность гарантийно исправляемых кодом ошибок (для рассматриваемого кода РС (7,3) t = 2). Предварительно для формирования начальных условий вычисляются значения многочленов локаторов и значений ошибок на – 1-м и 0-м шагах.

Предполагается, что $\Lambda_{-1}(x) = 0$, $\Lambda_0(x) = 1$, $\Omega_{-1}(x) = x^{2t} = x^4$, $\Omega_0(x) = S(x)$. Вид синдромного многочлена $S(x)$ зависит от кодовой комбинации $f'(x)$, поступившей на вход декодера. Напомним общий вид синдромного многочлена: $S(x) = S_1 + S_2x^1 + S_3x^2 + S_4x^3$, где S_1, S_2, S_3, S_4 определяются подстановкой значений корней порождающего многочлена в $f'(x)$. Процедура декодирования отображается содержимым табл. 2.8. Значения $\Lambda_i(x)$ и $\Omega_i(x)$ вычисляются итеративно на основе схемы рис. 2.2.

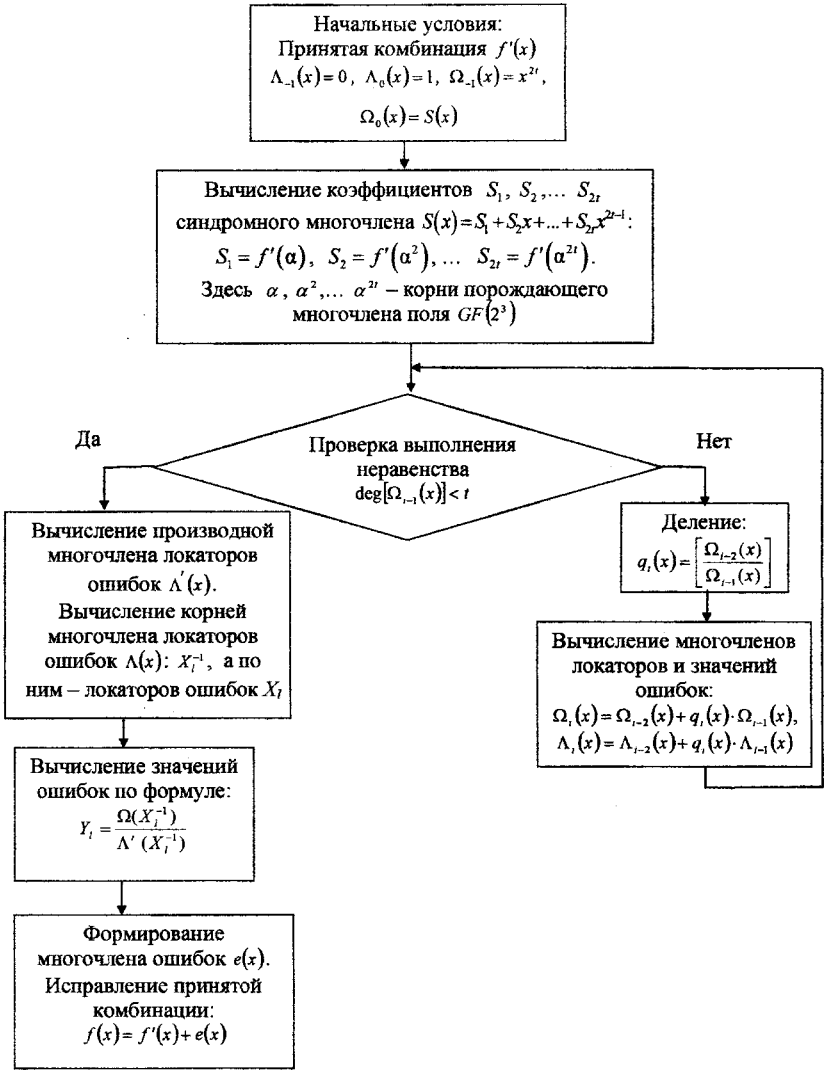


Рис. 2.2. Схема декодирования по алгоритму Евклида

Таблица 2.8

Функция	Шаг				
	–1	0	1	…	i
$\Lambda_i(x)$	0	1	$\Lambda_1(x)=\Lambda_{-1}(x)+q_1(x)\cdot\Lambda_0(x)$	…	$\Lambda_i(x)=\Lambda_{i-2}(x)+q_i(x)\cdot\Lambda_{i-1}(x)$
$\Omega_i(x)$	x^{2t}	$S(x)$	$\Omega_1(x)=\Omega_{-1}(x)+q_1(x)\cdot\Omega_0(x)$	…	$\Omega_i(x)=\Omega_{i-2}(x)+q_i(x)\cdot\Omega_{i-1}(x)$
$q_i(x)$	–	–	$\left[\frac{\Omega_{-1}(x)}{\Omega_0(x)}\right]$	…	$\left[\frac{\Omega_{i-2}(x)}{\Omega_{i-1}(x)}\right]$

На шагах «–1» и «0» записываются исходные данные процедуры декодирования в соответствии с первым блоком схемы рис. 2.2.

Каждый последующий шаг начинается с вычисления $q_i(x)$. Значения $\Lambda_i(x)$ и $\Omega_i(x)$ вычисляются в соответствии с выражениями $\Lambda_i(x)=\Lambda_{i-2}(x)+q_i(x)\cdot\Lambda_{i-1}(x)$ и $\Omega_i(x)=\Omega_{i-2}(x)+q_i(x)\cdot\Omega_{i-1}(x)$.

При реализации процедуры декодирования после завершения очередного шага проверяется условие $\deg[\Omega_i(x)]< t$.

Если степень $\Omega_i(x)$ меньше t (в рассматриваемом коде t=2), то процедура вычисления значений $\Lambda(x)$ и $\Omega(x)$ завершается и дальнейшее значение $q_i(x)=\left[\frac{\Omega_{i-2}(x)}{\Omega_{i-1}(x)}\right]$ не вычисляется.

После того, как многочлены локаторов и значений ошибок найдены, многочлен ошибки вычисляется по алгоритму Форни.

Для этого выполняются следующие операции.

1. Вычисляется производная многочлена локаторов ошибок $\Lambda'(x)$.

2. Вычисляются значения корней X_l^{-1} многочлена локаторов ошибок $\Lambda(x)$. Затем вычисляются локаторы ошибок X_l как величины, обратные корням X_l^{-1} многочлена локаторов ошибок X_l.

3. Вычисляются значения ошибок по формуле: $Y_l=\frac{\Omega(X_l^{-1})}{\Lambda'(X_l^{-1})}$.

4. Формируется многочлен ошибок $e(x)$, коэффициентами которого являются значения ошибок Y_l, а степенями слагаемых являются локаторы ошибок.

5. Исправление ошибок осуществляется посредством сложения принятой кодовой комбинации и многочлена ошибки $f(x)=f'(x)+e(x)$.

2.4.6. Примеры использования алгоритма Евклида для решения ключевого уравнения

В качестве примера использования алгоритма Евклида рассмотрим кодирование комбинации $K(x)=\alpha^0 x^4$ и декодирование комбинации $f'(x)=\alpha^0 x^1$.

Кодирование информационной последовательности

Процедура кодирования этой информационной последовательности в общем виде была рассмотрена во втором примере п. 2.4.3.2. Здесь рассматриваются особенности этой процедуры применительно к решению ключевого по алгоритму Евклида.

Итак, информационная часть кодируемой комбинации на входе кодера имеет следующий вид: $K(x)=\alpha^0 x^4$.

1	0	0
0	0	0
0	0	0

Избыточные элементы считаем стертыми и на их позициях записываем нулевые символы. Таким образом, кодируемая комбинация имеет вид $f'(x)=\alpha^0 x^4$:

0	0	0	0	1	0	0
0	0	0	0	0	0	0
0	0	0	0	0	0	0

В результате выполнения процедуры кодирования должны быть определены значения стираний, расположенных на местах избыточных разрядов. Процедура кодирования начинается с вычисления синдромного многочлена $S(x) = S_1 x^0 + S_2 x^1 + S_3 x^2 + S_4 x^3$.

Для вычисления S_i подставляем корни порождающего многочлена в $f'(x)$:

для корня α^1: $S_1 = f'(\alpha^1) = \alpha^0 (\alpha^1)^4 = \alpha^4$.

для корня α^2: $S_2 = f'(\alpha^2) = \alpha^0 (\alpha^2)^4 = \alpha^1$.

для корня α^3: $S_3 = f'(\alpha^3) = \alpha^0 (\alpha^3)^4 = \alpha^5$.

для корня α^4: $S_4 = f'(\alpha^4) = \alpha^0 (\alpha^4)^4 = \alpha^2$.

Синдромный многочлен имеет вид: $S(x) = \alpha^4 + \alpha x + \alpha^5 x^2 + \alpha^2 x^3$.

Многочлен локаторов стираний вычисляем по известным локаторам избыточных элементов:

$$\Gamma(x) = (1+\alpha^0 x)\cdot(1+\alpha^1 x)\cdot(1+\alpha^2 x)\cdot(1+\alpha^3 x) = \alpha^0 + \alpha^2 x + \alpha^5 x^2 + \alpha^5 x^3 + \alpha^6 x^4.$$

Видоизмененный синдромный многочлен имеет вид:

$$T(x)=\Gamma(x)\cdot S(x)\bmod(x^4)=\left(\alpha^4+\alpha x+\alpha^5x^2+\alpha^2x^3\right)\times$$

$$\times\left(\alpha^0+\alpha^2x+\alpha^5x^2+\alpha^5x^3+\alpha^6x^4\right)\bmod(x^4)=\alpha^4+\alpha^5x+\alpha^2x^3.$$

Полученные данные заносим в табл. 2.9, которая формируется по форме табл. 2.7.

Таблица 2.9

Функция	Шаг	
	–1	0
$\Gamma(x)$	0	$\alpha^0+\alpha^2x+\alpha^5x^2+\alpha^5x^3+\alpha^6x^4$
$\Omega(x)$	x^4	$\alpha^4+\alpha^5x^2+\alpha^2x^3$

Производная многочлена локаторов стираний имеет вид:

$$\Gamma'(x)=\alpha^2+\alpha^5x^2.$$

Расчет значений стираний:

для локатора α^0: $Y_0=\dfrac{\Omega_0(\alpha^0)}{\Gamma'(\alpha^0)}=\dfrac{\alpha^6}{\alpha^3}=\alpha^3$,

для локатора α^1: $Y_1=\dfrac{\Omega_0(\alpha^6)}{\Gamma'(\alpha^6)}=\dfrac{\alpha^6}{\alpha^5}=\alpha^1$,

для локатора α^2: $Y_2=\dfrac{\Omega_0(\alpha^5)}{\Gamma'(\alpha^5)}=\dfrac{\alpha^4}{\alpha^4}=\alpha^0$,

для локатора α^3: $Y_3=\dfrac{\Omega_0(\alpha^4)}{\Gamma'(\alpha^4)}=\alpha^3$.

Таким образом, сформированные избыточные разряды имеют вид:

$$r(x)=\alpha^3+\alpha^1x+\alpha^0x^2+\alpha^3x^3.$$

Комбинация на выходе кодера:

$$f(x)=f'(x)+r(x)=\alpha^3+\alpha^1x+\alpha^0x^2+\alpha^3x^3+\alpha^0x^4.$$

1	0	1	1	1	0	0
1	1	0	1	0	0	0
0	0	0	0	0	0	0

Рассмотренная процедура кодирования полностью совпадает с процедурой кодирования в п. 2.4.3.2. Отличие состоит в использовании табл. 2.9 для представления исходных данных для алгоритма Форни.

Декодирование

Процедура декодирования выполняется в соответствии со схемой рис. 2.2. Весь процесс декодирования отображается в табл. 2.6. Пусть комбинация на входе декодера имеет вид $f'(x)=\alpha^0 x^1$.

0	1	0	0	0	0	0
0	0	0	0	0	0	0
0	0	0	0	0	0	0

Процедура декодирования начинается с формирования начальных условий.

Для вычисления компонентов синдромного многочлена подставляем корни порождающего многочлена в $f'(x)$:

для корня α^1: $S_1=f'(\alpha^1)=\alpha^0\alpha^1=\alpha^1$,

для корня α^2: $S_2=f'(\alpha^2)=\alpha^0\alpha^2=\alpha^2$,

для корня α^3: $S_3=f'(\alpha^3)=\alpha^0\alpha^3=\alpha^3$,

для корня α^4: $S_4=f'(\alpha^4)=\alpha^0\alpha^4=\alpha^4$.

Синдромный многочлен имеет вид: $S(x)=\alpha^1+\alpha^2x+\alpha^3x^2+\alpha^4x^3$.

Результаты заносим в табл. 2.10, формируемую по типу табл. 2.8. Выполненные расчеты позволяют заполнить ячейки для $\Lambda_i(x)$ и $\Omega_i(x)$ на -1-м и 0-м шагах итерации.

Далее вычисляем $q_1(x)=\left[\dfrac{\Omega_{-1}(x)}{\Omega_0(x)}\right]=\dfrac{x^4}{\alpha+\alpha^2x+\alpha^3x^2+\alpha^4x^3}=\alpha^2+\alpha^3x^1$.

Теперь можно вычислить $Q_1(x)$ и $\Lambda_1(x)$.

Таблица 2.10

Функция	Шаг		
	–1	0	1
$\Lambda_i(x)$	0	1	$\alpha^2+\alpha^3x^1$
$\Omega_i(x)$	x^4	$\alpha^1+\alpha^2x+\alpha^3x^2+\alpha^4x^3$	α^3
$q_i(x)$	–	–	$\alpha^2+\alpha^3x^1$

$$\Omega_1(x)=\Omega_{-1}(x)+q_1(x)\cdot\Omega_0(x)=x^4+(\alpha^2+\alpha^3x^1)(\alpha^1+\alpha^2x+\alpha^3x^2+\alpha^4x^3)=\alpha^3.$$

$$\Lambda_1(x)=\Lambda_{-1}(x)+q_1(x)\cdot\Lambda_0(x)=0+(\alpha^2+\alpha^3x^1)\cdot 1=\alpha^2+\alpha^3x^1.$$

Поскольку степень $\Omega_1(x)$ меньше 2, процедура нахождения $\Omega(x)$ и $\Lambda(x)$ заканчивается на первом шаге.

Далее производится вычисление корней $\Lambda(x)$ и локаторов ошибок.

Многочлен локаторов ошибок имеет только один корень $-\alpha^6$, соответственно локатор ошибки равен $1/\alpha^6=\alpha^1$. Производная многочлена локаторов ошибок имеет вид: $\Lambda'(x)=\alpha^3$.

Расчет значения ошибки на позиции, определяемой локатором α^1:

$$Y_1=\frac{\Omega_0(\alpha^6)}{\Lambda'(\alpha^6)}=\frac{\alpha^3}{\alpha^3}=\alpha^0=1.$$

Таким образом, многочлен ошибок имеет вид: $e(x)=\alpha^0 x$.

Комбинация на выходе декодера: $f(x)=f'(x)+e(x)=\alpha^0 x+\alpha^0 x=0$.

Для того чтобы выявить одну важную особенность решения ключевого уравнения на основе алгоритма Евклида, повторим декодирование принятой комбинации из первого примера п. 2.4.3.2 с помощью алгоритма Евклида. Пусть на вход декодера поступила комбинация $f'(x) = \alpha x + x^2 + \alpha^3 x^3$. Декодер работает в соответствии со схемой рис. 2.2, а результаты расчетов представляем в виде табл. 2.11.

Таблица 2.11

Функция	Шаг			
	–1	0	1	2
$\Lambda_i(x)$	0	1	$\alpha^2 x+\alpha^6$	$\alpha^3 x^2+\alpha^4 x+\alpha^6$
$\Omega_i(x)$	x^4	$\alpha^6+x+\alpha^2 x^2+\alpha^5 x^3$	$\alpha^4 x^2+\alpha^5 x+\alpha^5$	$\alpha^4 x+\alpha^5$
$q_i(x)$	–	–	$\alpha^2 x+\alpha^6$	$\alpha x+\alpha^3$

Шаг 1. Значение многочлена локаторов ошибок $\Lambda_{-1}(x) = 0$. Значение синдромного многочлена $\Omega_{-1}(x)=x^4$. Значение $q_{-1}(x)$ не вычисляется.

Шаг 0. Значение многочлена локаторов ошибок $\Lambda_0(x) = 1$. Значение синдромного многочлена берем из первого примера п. 2.4.3.2: $\Omega_0(x)=S(x)=\alpha^6+x+\alpha^2x^2+\alpha^5x^3$. Значение $q_0(x)$ не вычисляется.

Шаг 1. Делением x^4 на $S(x)=\alpha^6+x+\alpha^2x^2+\alpha^5x^3$ находим значение $q_1(x) = \alpha^2 x + \alpha^6$. Используя выражение $\Lambda_i(x)=\Lambda_{i-2}(x)+q_i(x)\cdot\Lambda_{i-1}(x)$, вычисляем $\Lambda_1(x)=\alpha^2x+\alpha^6$.

Используя выражение $\Omega_i(x)=\Omega_{i-2}(x)+q_i(x)\cdot\Omega_{i-1}(x)$, вычисляем $\Omega_1(x) = \alpha^4x^2 + \alpha^5x + \alpha^5$. Значение степени многочлена $\Omega_1(x)$ показывает необходимость продолжения процедуры декодирования, так как процедура декодирования завершается, если степень $\Omega_i(x)$ меньше t (в нашем случае t равно двум).

Шаг 2. Вычисляем $q_2(x)= \alpha x + \alpha^3$ как частное от деления $\Omega_0(x) = S(x)= \alpha^6 + x + \alpha^2x^2+ \alpha^5x^3$ на $\Omega_1(x) = \alpha^4x^2 + \alpha^5x + \alpha^5$. Используя выражение $\Lambda_i(x)=\Lambda_{i-2}(x)+q_i(x)\cdot\Lambda_{i-1}(x)$, вычисляем $\Lambda_2(x) = 1 + (\alpha x + \alpha^3)(\alpha^2x + \alpha^6) =$

$= \alpha^3 x^2 + \alpha^4 x + \alpha^6$. Используя выражение $\Omega_i(x) = \Omega_{i-2}(x) + q_i(x) \cdot \Omega_{i-1}(x)$, вычисляем $\Omega_2(x) = \alpha^4 x + \alpha^5$. Теперь степень $\Omega_2(x)$ меньше t, что указывает на завершение процедуры декодирования.

Представляет интерес сравнить полученные многочлены $\Lambda_2(x)$ и $\Omega_2(x)$ с вычисленными в п. 2.4.3.2 многочленами $\Lambda(x)$ и $\Omega(x)$. Сравнение показывает их отличие на один и тот же постоянный множитель – элемент поля, над которым эти многочлены построены, т. е. декодирование на основе алгоритма Евклида позволяет вычислить многочлены $\Lambda(x)$ и $\Omega(x)$ с точностью до постоянного множителя [2]. При этом корни $\Lambda(x)$ из первого примера и $\Lambda_2(x)$ совпадают. Также совпадают и значения ошибок, вычисленные по алгоритму Форни: $Y_i = \alpha^{i(1-m)} \frac{\Omega(x = \alpha^{-i})}{\Lambda'(x = \alpha^{-i})}$. Так, в рассматриваемом случае корнями $\Lambda_2(x) = \alpha^3 x^2 + \alpha^4 x + \alpha^6$ являются:

Первый корень $x_1 = 1$: $\Lambda_2(x = 1) = \alpha^3 + \alpha^4 + \alpha^6 = 0$.

Локатор ошибки: $1/1 = 1 = X_0$.

Второй корень $x_2 = \alpha^3$: $\alpha^3 \alpha^6 + \alpha^4 \alpha^3 + \alpha^6 = \alpha^2 + \alpha^0 + \alpha^6 = 0$.

Локатор ошибки: $1/\alpha^3 = \alpha^4 = X_4$.

Производная от $\Lambda_2(x) = \alpha^3 x^2 + \alpha^4 x + \alpha^6$ равна α^4.

Значения ошибок:

$Y_0 = (\alpha^4 + \alpha^5) / \alpha^4 = \alpha^3$,

$Y_4 = (\alpha^4 \alpha^3 + \alpha^5) / \alpha^4 = 1$.

Таким образом, вычислен многочлен ошибок: $e(x) = \alpha^3 + x^4$.

Переданная комбинация имеет вид

$$f(x) = f'(x) + e(x) = \alpha^3 + \alpha x + x^2 + \alpha^3 x^3 + x^4.$$

Этот результат декодирования полностью совпадает с полученным выше.

Контрольные вопросы

1. Найти наибольший общий делитель (НОД) чисел 405 и 75, т. е. НОД(405,75).

2. Представить результат, полученный в п. 1, в виде $fa + gb = d$, где $a = 405$, $b = 75$, $d = $ НОД (a, b).

3. Дайте определение кода Рида–Соломона.

4. Почему коды Рида–Соломона широко используются для защиты от ошибок?

5. Какие методы кодирования и декодирования для кодов Рида–Соломона вы знаете?

6. В каких случаях целесообразно использовать аппаратные методы реализации кодов Рида–Соломона, а в каких – программные?

7. Сформулируйте свойство алгоритма Евклида, используемое в процедуре декодирования: $E_i(x)=E_{i-2}(x)+q_iE_{i-1}(x)$, где $q_i=\left[\frac{\Omega_{i-2}(x)}{\Omega_{i-1}(x)}\right]$.

8. Что нужно знать для построения кодера кода Рида–Соломона на основе регистра сдвига с обратными связями?

9. Что нужно знать для начала процедуры кодирования кода Рида–Соломона?

10. Что нужно знать для начала процедуры декодирования кода Рида–Соломона?

11. Определите вид порождающего многочлена кода Рида–Соломона (7,5) над полем $GF(2^3)$.

2.5. Порядок выполнения работы

1. По известной информационной части кодовой комбинации (согласно варианту задания) определить значения избыточных элементов для кода (7,3) над полем $GF(2^3)$. Представить комбинацию на входе кодера в виде многочлена.

2. Для комбинации на входе декодера определить локаторы и значения ошибок, используя алгоритм Евклида для кода (7,3) над полем $GF(2^3)$. Представить комбинацию на выходе декодера в виде многочлена.

3. Сравнить результаты своих вычислений с результатами работы программы AE (запускается двойным щелчком с рабочего стола).

Кодирование

- перейти по ссылке «Кодирование»;
- представить информационную часть кодовой комбинации $K(x)$ и закодированную последовательность в двоичном виде и занести значения элементов в таблицы размерности 3×3 и 3×7 соответственно (один щелчок левой клавиши мыши инвертирует значение кнопки). Информацию о том, как представить многочлен в двоичном виде и другие подсказки можно найти, перейдя по ссылке «Информация»;
- нажать кнопку «Закодировать и проверить»;
- результаты кодирования представлены в таблице размерности 3×7, а результат сравнения с введенными данными отображается под таблицей.

Декодирование

- перейти по ссылке «Декодирование»;
- повторить шаги кодирования, но занести исходную информацию в таблицу размерности 3×7, а результат получить в таблице размерности 3×3.

2.6. Содержание отчета

1. Исходные данные на входе кодера/декодера в виде многочлена и в виде таблицы из нулей и единиц.

2. Синдромные и видоизмененный синдромный (только для кодирования) многочлены.

3. Таблицы расчетов многочленов локаторов и значений ошибок и стираний.

4. Расчет значений ошибок (для декодирования) и стираний (для кодирования).

5. Многочлен ошибок (для декодирования) и многочлен стираний (для кодирования).

6. Итоговые комбинации на выходе кодера/декодера в виде многочлена и в виде таблицы из нулей и единиц.

7. Вывод о целесообразности использования алгоритма Евклида для реализации процедур кодирования и декодирования.

Список литературы

1. *Блейхут*, Р. Теория и практика кодов, контролирующих ошибки / Р. Блейхут. – М. : Мир, 1986. – 576 с.

2. *Кларк*, Дж., мл. Кодирование с исправлением ошибок в системах цифровой связи / Дж., мл. Кларк, Дж. Кейн. – М. : Радио и связь, 1987. – 392 с.

Практическое занятие 1

ПОЛЯ ГАЛУА ПРОСТЫЕ И РАСШИРЕННЫЕ. ДВОЙСТВЕННЫЙ БАЗИС. ДВОЙНОЕ РАСШИРЕНИЕ

Основные алгебраические системы, используемые в теории кодирования [3].

Построение простых и расширенных полей Галуа [1, 3].

Базисы расширенных полей Галуа [1, 2].

Двойственный базис и его применение [2].

Двойное расширение полей Галуа [1].

Темы рефератов

1. Рекуррентные последовательности и их обработка с использованием двойственного базиса.
2. Минимальные многочлены в полях с двойным расширением.

Список литературы

1. *Стародубцев*, В. Г. Помехоустойчивые коды в телекоммуникационных и информационных системах. Вып. 1. / В. Г. Стародубцев, О. А Павлов. – СПб. : ВКА, 2003. – 255 с.

2. *Когновицкий*, О. С. Двойственный базис и его применение в телекоммуникациях / О. С. Когновицкий. – СПб. : Линк, 2009. – 424 с.

3. *Охорзин*, В. М. Циклические коды. Практикум /В. М. Охорзин ; СПбГУТ. – СПб., 2010. – 56 с.

Цель. Изучить методы построения простых и расширенных полей Галуа и их базисов. Получить навыки в решении задач по теме занятия.

Задачи

1. Определить вид минимальных многочленов для всех ненулевых элементов поля $GF(2^4)$ с коэффициентами из поля $GF((2^2)^2)$.
2. Сколько различных полей $GF(2^3)$ существует? Построить эти поля.
3. Сколько различных полей $GF(2^4)$ существует? Построить эти поля.
4. Построить генератор элементов поля $GF(2^3)$.
5. Построить генератор элементов поля $GF(2^4)$.
6. Построить генератор элементов поля $GF(2^4)$ с коэффициентами из поля $GF((2^2)^2)$.
7. Построить генератор обратных элементов поля $GF(2^4)$.

8. Построить генератор последовательности максимальной длины (ПМД) периода 15 с элементами из поля $GF(2)$ и получить один период этой последовательности.

9. Построить генератор ПМД периода 15 с элементами из поля $GF(2^2)$ и получить один период этой последовательности.

10. Вычислить значения функции-след, отображающей элементы поля $GF(2^4)$ в элементы поля $GF(2)$.

11. Вычислить значения функции-след, отображающей элементы поля $GF(2^4)$ в элементы поля $GF(2^2)$.

12. Построить декодер для кода (15,2) с кодовыми комбинациями в виде многочленов над полем $GF((2^2)^2)$ [2].

13. Построить ПМД периода 15 с элементами из поля $GF(2^2)$ как последовательность функций-след, отображающей элементы поля $GF(2^4)$ в элементы поля $GF((2^2)$ с начальной фазой последовательности 11.

Примеры решения задач

Задача 14. Определить вид минимального многочлена $m(x)$ для элемента поля $GF(2^4)$ ε^1 с коэффициентами из поля $GF(2^2)$.

Решение. Строим циклотомический класс для ε^1:$\{\varepsilon^1, \varepsilon^4\}$. Выражаем искомый многочлен через его корни: $m(x) = (x + \varepsilon^1)(x + \varepsilon^4) = x^2 + x + a$ [1].

Задача 15. Для декодера кода БЧХЭ (15,2) с характеристическим многочленом $P(x) = x^2 + x + a$ вычислить коэффициенты двойственного базиса α_1 и α_2.

Решение. Напомним, что коэффициенты двойственного базиса вычисляются по формуле: $\alpha_i = \dfrac{\sum_{r=0}^{m=k-i} p_{1-r}\varepsilon^r}{P^I(\varepsilon)}$,

где k – степень характеристического многочлена $P(x)$, p_i – его коэффициенты и $P'(x)$ – производная.

Находим коэффициенты характеристического многочлена $P(x)$:

$$p_0=1, p_1=1, p_2=a.$$

Вычисляем: $\alpha_1 = \dfrac{\sum_{r=0}^{1} p_{1-r}\varepsilon^r}{P^I(\varepsilon)} = \varepsilon^0 + \varepsilon^1 = \varepsilon^4;$

$$\alpha_2 = \frac{\sum_{r=0}^{0} p_{1-r}\varepsilon^r}{P^I(\varepsilon)} = \varepsilon^0.$$

Задача 16. Построить генератор ПМД периода 15 с элементами из поля $GF(2^2)$ с характеристическим многочленом, один из корней которого равен ε^1, и получить один период этой последовательности.

Решение. Вид требуемого характеристического многочлена найден в решении задачи 14: $p(x) = x^2 + x + a$. Соответствующий ему генератор ПМД изображен на рис. 1.1, а первый пятнадцатиэлементный период ПМД с начальной фазой 01 изображен в строке r_1 табл. 1.1.

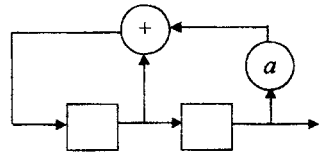


Рис. 1.1

Таблица 1.1

Такты i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
r_0	1	1	a^2	1	0	a	a	1	a	0	a^2	a^2	a	a^2	0
r_1	0	1	1	a^2	1	0	a	a	1	a	0	a^2	a^2	a	a^2

Задача 17. Построить ПМД периода 15 из задачи 16 с элементами из поля $GF(2^2)$ как последовательность функций-след, отображающей элементы поля $GF(2^4)$ в элементы поля $GF(2^2)$ с начальной фазой последовательности 10.

Решение. Для решения задачи используем табл. 1.2, заимствованную из [1].

Таблица 1.2

Формы представления элементов поля $GF((2^2)^2)$				Минимальные многочлены
степенная	полиномиальная	векторная		
		$GF(2^2)$	$GF(2)$	
$\varepsilon^{-\infty}$	0	00	0 0 0 0	z
ε^0	1	10	1 0 0 0	$z+1$
ε^1	x	01	0 0 1 0	z^2+z+a
ε^2	$a+x$	$a1$	0 1 1 0	z^2+z+a^2
ε^3	$a+a^2x$	aa^2	0 1 1 1	z^2+a^2z+1
ε^4	$1+x$	11	1 0 1 0	z^2+z+a
ε^5	a	$a0$	0 1 0 0	$z+a$
ε^6	ax	$0a$	0 0 0 1	z^2+az+1
ε^7	a^2+ax	a^2a	1 1 0 1	z^2+az+a

Окончание табл. 1.2

Формы представления элементов поля $GF((2^2)^2)$				Минимальные многочлены
степенная	полиномиальная	векторная		
		$GF(2^2)$	$GF(2)$	
ε^8	a^2+x	$a^2 1$	1 1 1 0	z^2+z+a^2
ε^9	$a+ax$	aa	0 1 0 1	z^2+az+1
ε^{10}	a^2	$a^2 0$	1 1 0 0	$z+a^2$
ε^{11}	a^2x	$0a^2$	0 0 1 1	$z^2+a^2z+a^2$
ε^{12}	$1+a^2x$	$1a^2$	1 0 1 1	z^2+a^2z+1
ε^{13}	$1+ax$	$1a$	1 0 0 1	z^2+az+a
ε^{14}	a^2+a^2x	a^2a^2	1 1 1 1	$z^2+a^2z+a^2$

ПМД с начальной фазой С, сформированной с помощью функции-след, имеет вид [2]: $\{s\}=\{T(C), T(C\varepsilon), T(C\varepsilon^2),..., T(C\varepsilon^{13}), T(C\varepsilon^{14})\}$. По условию задачи С=10. Из табл. 1.1 находим, что $C = \varepsilon^0$. Находим $T(C) = 1 + 1 = 0$, $T(C\varepsilon) = \varepsilon^1 + \varepsilon^4 = 1$, $T(C\varepsilon^2) = \varepsilon^2 + \varepsilon^8 = 1$, $T(C\varepsilon^3) = \varepsilon^3 + \varepsilon^{12} = a^2$ и т. д., что полностью совпадает с результатом решения задачи 16.

Задача 18. Определить число порождающих многочленов минимальной степени для кода БЧХ длины 15 с коэффициентами из поля $GF(2^2)$, способного исправить ошибки кратности до 3 включительно.

Указание. Использовать данные табл. 1.2 о значении минимальных ногочленов для элементов поля $GF((2^2)^2)$.

Ответ: минимальная степень порождающего многочлена, удовлетворяющего условию задачи – 8.

Существует 3 таких многочлена над полем $GF(2^2)$. Это многочлены, имеющие в составе своих корней 6 подряд идущих степеней примитивного элемента поля $GF((2^2)^2)$: $\{\varepsilon^0,\varepsilon^1,\varepsilon^2,\varepsilon^3,\varepsilon^4,\varepsilon^5\}$, $\{\varepsilon^5,\varepsilon^6,\varepsilon^7,\varepsilon^8,\varepsilon^9,\varepsilon^{10}\}$ и $\{\varepsilon^{10},\varepsilon^{11},\varepsilon^{12},\varepsilon^{13},\varepsilon^{14},\varepsilon^{15=0}\}$. Полученный код имеет параметры – (15,7). Заметим, что код БЧХ (15,7) над $GF(2^2)$ может исправить ошибки кратности только до 2.

Задача 19. Вычислить порождающий многочлен кода (15,7) из условия задачи 18, среди корней которого имеются элементы поля $GF((2^2)^2)$: $\{\varepsilon^5,\varepsilon^6,\varepsilon^7,\varepsilon^8,\varepsilon^9,\varepsilon^{10}\}$.

Ответ: $g(x) = (z + a)(z^2 + az + 1)(z^2 + az + a)(z^2 + z + a^2)(z + a^2)$.

Практическое занятие 2

КОДЫ РИДА–СОЛОМОНА. ПРОЦЕДУРЫ КОДИРОВАНИЯ И ДЕКОДИРОВАНИЯ. АЛГОРИТМ БЕРЛЕКЭМПА–МЕССИ РЕШЕНИЯ КЛЮЧЕВОГО УРАВНЕНИЯ

Коды Рида–Соломона как частный случай кодов БЧХ [2, 3].

Методы кодирования и декодирования кодов Рида–Соломона [2, 3].

Алгоритм Берлекэмпа–Месси решения ключевого уравнения [1–3].

Блок-схема алгоритма Берлекэмпа–Месси [1–3].

Применение алгоритма Берлекэмпа–Месси для исправления ошибок и стираний в кодах Рида–Соломона [2, 3].

Темы рефератов

1. Коды Рида–Соломона в современных телекоммуникационных системах.
2. Быстрое декодирование кодов БЧХ.
3. Интерпретация ключевого уравнения с помощью регистра сдвига с обратной связью как математическое обоснование алгоритма Берлекэмпа–Месси.

Список литературы

1. *Берлекэмп*, Э. Р. Алгебраическая теория кодирования / Э. Р. Берлекэмп. – М. : Мир, 1971. – 490 с.

2. *Блейхут*, Р. Э. Теория и практика кодов, контролирующих ошибки / Р. Э. Блейхут ; пер. с. англ. – М. : Мир, 1986. – 576 с.

3. *Кларк*, Дж. мл. Кодирование с исправлением ошибок в системах цифровой связи / Дж. мл. Кларк, Дж. Кейн. – М. : Радио и связь, 1987. – 392 с.

4. *Охорзин*, В. М. Построение каскадных кодов на основе кодов Рида–Соломона и Боуза–Чоудхури–Хоквингема : учебное пособие / В. М. Охорзин, Д. С. Кукунин, М. С. Новодворский ; СПбГУТ. – СПб., 2004. – 58 с.

Цель. Изучить методы построения кодов Рида–Соломона и метод их декодирования с использованием алгоритма Берлекэмпа–Мееси.

Задачи

1. Вычислить порождающий многочлен для кода Рида–Соломона (15,9) над полем $GF(2^4)$.Определить характеристики этого кода.

2. Вычислить порождающий многочлен для кода Рида–Соломона (15,9) над полем $GF((2^2)^2)$.

3. Построить порождающую и проверочную матрицы для кода из задачи 1.

4. Построить порождающую и проверочную матрицы для кода из задачи 2.

5. Необходимо вычислить избыточные элементы кодовой комбинации кода Рида–Соломона (15,9) из задачи 1 по ее информационным элементам, заданным многочленом $\kappa(x) = \alpha^0 x^6 + \alpha^0 x^7 + \alpha^0 x^8 + \alpha^0 x^9 + \alpha^0 x^{10} + \alpha^0 x^{11} + \alpha^0 x^{12} + + \alpha^0 x^{13} + \alpha^0 x^{14}$. Вычислить синдромный многочлен и многочлен локаторов стираний, расположенных на позициях избыточных элементов.

6. Пусть от передатчика в канал передана комбинация кода Рида–Соломона (15,9) из задачи 1 $f(x) = 0$. Приемник принял комбинацию $C(x) = = \alpha x^7 + \alpha^5 x^5 + \alpha^{11} x^2 = e(x)$. Вычислить синдромный многочлен.

Примеры решения задач

Задача 7. По вычисленному в условиях задачи 6 синдромному многочлену $S(x) = \alpha^{11} x^6 + \alpha^0 x^5 + \alpha^{13} x^4 + \alpha^{14} x^3 + \alpha^0 x^2 + \alpha^{12} x^1$, используя приведенную ниже блок-схему алгоритма Берлекэмпа–Месси, вычислить многочлены локаторов ошибок и значений ошибок.

Решение. Результаты вычислений в соответствии с алгоритмом Берлекэмпа–Месси представлены в приведенной ниже табл. 2.1.

Таблица 2.1

r	S_r	Δr	$M(x)$	$B(x)$	$\Lambda(x)$	L	$\Omega(x)$	$A(x)$
0				1	1	0	0	1
1	a^{12}	a^{12}	$1+a^{12}x$	a^3	$1+a^{12}x$	1	a^{12}	0
2	a^0	a^7	$1+a^3x$	a^3x	$1+a^3x$	1	a^{12}	0
3	a^{14}	a^0	$1+a^3x+a^3x^2$	$1+a^3x$	$1+a^3x+a^3x^2$	2	a^{12}	$a^{12}x$
4	a^{13}	a^0	$1+a^{14}x$	$x+a^3x^2$	$1+a^{14}x$	2	$a^{12}+a^{12}x$	$a^{12}x$
5	a^0	a^{11}	$1+a^{14}x+ +a^{11}x^2+a^{14}x^3$	a^4+a^3x	$1+a^{14}x+a^{11}x^2+a^{14}x^3$	3	$a^{12}+a^{12}x+ +a^8x^2$	ax^3
6	a^{11}	0	$1+a^{14}x+ +a^{11}x^2+a^{14}x^3$	$a^4x+a^3x^2$	$1+a^{14}x+ a^{11}x^2+a^{14}x^3$	3	$a^{12}+a^{12}x+ +a^8x^2$	ax^4

Задача 8. По вычисленным в условиях задачи 5 синдромному многочлену $S(x) = x^5 + \alpha^6 x^3 + x^2 + \alpha^3 x + \alpha^9$ и многочлену локаторов стираний, расположенных на позициях избыточных элементов $\Gamma(x) = x^6 + \alpha^4 x^5 + \alpha^2 x^4 + + \alpha x^3 + \alpha^{12} x^2 + \alpha^9 x + 1$, найти значения избыточных элементов.

Решение. Вычисление многочлена значений искажений (стираний):

$$\Omega(x)=S(x)\cdot\Gamma(x)=(\alpha^9+\alpha^3x+x^2+\alpha^6x^3+x^5)(1+\alpha^9x+\alpha^{12}x^2+$$
$$+\alpha x^3+\alpha^2x^4+\alpha^4x^5+x^6)=\alpha^4x^4+\alpha^1x^2+\alpha^9.$$

Здесь в $\Omega(x)$ степени равные и старшие $N - K = 6$ отбрасываются. Вычисление производной многочлена локаторов стираний:

$$\Gamma'(x)=\alpha^4x^4+\alpha^1x^2+\alpha^9.$$

Вычисление значений стираний (избыточных символов): $Y_l=\dfrac{\Omega(X_l^{-1})}{\Gamma'(X_l^{-1})}$

при l = 0, 1, 2, 3, 4, 5, где $X_l=\alpha^l$ – локатор стираний, дают результат: $Y_0 = Y_1 = Y_2 = Y_3 = Y_4 = Y_5 = 1$, т. е. кодируемая комбинация имеет вид

$$f(x)=1+x+x^2+x^3+x^4+x^5+x^6+x^7+x^8+x^9+x^{10}+x^{11}+x^{12}+x^{13}+x^{14}.$$

Примечание. При сложении элементов поля $GF(2^4)$ можно использовать векторное представление элементов поля $GF((2^2)^2)$, приведенное в табл. 1.2 практического занятия 1. Это возможно в силу того, что в каждом из этих полей ненулевые элементы являются степенями одного и того же корня двучлена $x^{15}+1$. В поле $GF(2^4)$ – это корень многочлена $x^4 + x + 1$, а в поле $GF((2^2)^2)$ – это корень многочлена $x^2 + x + a$, который в поле $GF((2^2)^2)$ является делителем многочлена $x^4 + x + 1$.

Задача 9. Пусть по каналу связи передается нулевая комбинация кода (15,7) из условия задачи 19 практического занятия 1. При этом на вход декодера поступила комбинация $f(z) = a + z^5 + z^{10}$. Декодер вычислил синдромный многочлен: $S(z) = a^2 + az + a^2z^2 + a^2z^3 + az^4 + a^2z^5$. Проверить правильность его значения.

Решение. На основании общего выражения для синдромного многочлена $S_i = f(z = \varepsilon^i)$ находим: $S_1 = f(z = \varepsilon^5) = a + (\varepsilon^5)^5 + (\varepsilon^5)^{10} = a + \varepsilon^{10} + \varepsilon^5 = a + a + a^2 = a^2$, $S_2 = f(z = \varepsilon^6) = a + (\varepsilon^6)^5 + (\varepsilon^6)^{10} = a + \varepsilon^0 + \varepsilon^0 = a + 1 + 1 = a$. Остальные значения S_i студенты могут вычислить самостоятельно.

Задача 10. Для принятой комбинации кода (15,7) из условия задачи 9 найти значения ошибок, используя алгоритмы Евклида и Форни.

Решение. Задача решается на основании результатов пп. 2.4.5 и 2.4.6 лабораторной работы 2. Поиск значений $\Lambda_i(z)$ в $\Omega_i(z)$ по алгоритму Евклида, удовлетворяющих приведенным выше критериям, представим в виде табл. 2.2.

Таблица 2.2

i	–1	0	1	2	3
$\Lambda_i(x)$	0	1	$1+az$	$1+z+az^2$	$a+az^3$
$\Omega_i(x)$	z^6	$S(z)$	$a^2+a^2z+az^3+a^2z^4$	$a^2+z+a^2z^3$	$1+a^2z+z^2$
$q_{i(x)}$	–	–	$[x^6/S(z)]=1+az$	z	a^2+z

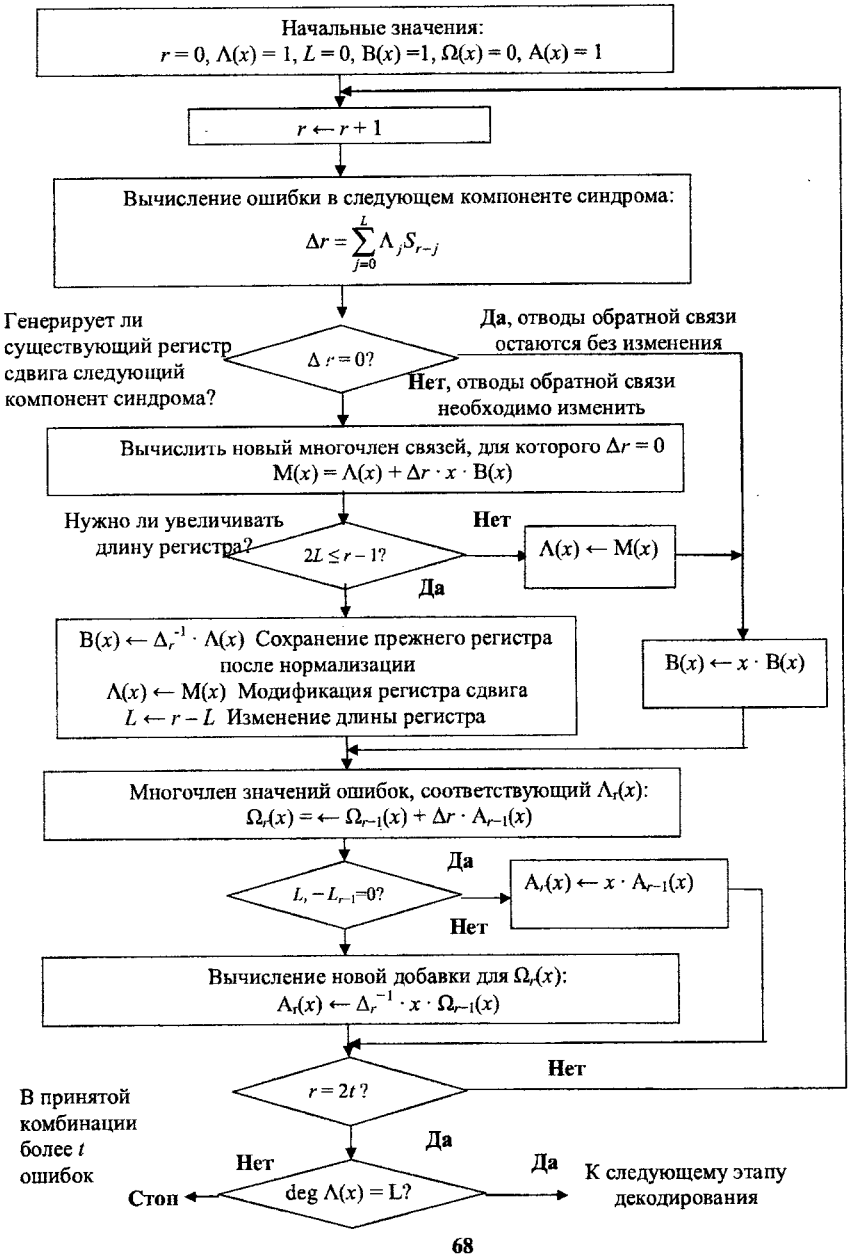
Находим корни $\Lambda_i(z)$. Полагаем $a + az^3 = 0$, тогда $z_1 = \varepsilon^0 = 1/X_0$, $z_2 = \varepsilon^5 = 1/X_{10}$, $z_3 = \varepsilon^{10} = 1/X_5$. Это значит, что локаторы ошибок равны $X_0 = \varepsilon^0$, $X_5 = \varepsilon^5$, $X_{10} = \varepsilon^{10}$.

В соответствии с алгоритмом Форни вычисляем значения ошибок:

$$Y_i = \varepsilon^{i(1-m)} \frac{\Omega(z=\varepsilon^{-i})}{\Lambda'(z=\varepsilon^{-i})}.$$

В результате получим $Y_0 = a$, $Y_5 = 1$, $Y_{10} = 1$. Суммируя вычисленные значения ошибок со значениями соответствующих коэффициентов принятой комбинации $f(z) = a + z^5 + z^{10}$, находим истинное значение принятой кодовой комбинации – $f(z) = 0$.

Алгоритм Берлекэмпа-Месси



Когновицкий Олег Станиславович
Охорзин Виктор Михайлович

ТЕОРИЯ ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ

ПРАКТИКУМ

Редактор *Л. А. Медведева*

План 2013 г., п. 14

Подписано к печати 19.06.2013
Объем 4,25 усл.-печ. л. Тираж 100 экз. Зак. 355

РИЦ СПбГУТ. 191186 СПб., наб. р. Мойки, 61
Отпечатано в СПбГУТ


08000127