ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ
БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ
им. проф. М. А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)

О. С. Когновицкий
В. М. Охорзин

ТЕОРИЯ ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ

Часть 3

ЦИКЛИЧЕСКИЕ КОДЫ КАК РЕКУРРЕНТНЫЕ ПОСЛЕДОВАТЕЛЬНОСТИ

КОДЫ С МАЛОЙ ПЛОТНОСТЬЮ ПРОВЕРКИ НА ЧЕТНОСТЬ

Учебное пособие

САНКТ-ПЕТЕРБУРГ
2017

УДК 621.391(075.8)
ББК 32.811.7я73
К 57

Рецензенты:
доктор технических наук, профессор
Н. В. Савищенко,
кандидат технических наук
С. С. Владимиров

*Утверждено редакционно-издательским советом СПбГУТ
в качестве учебного пособия*

Когновицкий, О. С.

К 57 Теория помехоустойчивого кодирования. Часть 3. Циклические коды как рекуррентные последовательности. Коды с малой плотностью проверки на четность : учебное пособие / О. С. Когновицкий, В. М. Охорзин ; СПбГУТ. – СПб., 2017. – 94 с.

Рассматривается подход к эквивалентным циклическим кодам как рекуррентным последовательностям. Изложены вопросы теории и практической реализации таких кодов на основе двойственного базиса полей Галуа. Теоретические выкладки иллюстрируются примерами кодирования и декодирования эквивалентных кодов Боуза – Чоудхури – Хоквингема и Рида – Соломона. Также рассмотрены перспективные коды с низкой плотностью проверок на четность Галлагера.

Может быть использовано студентами направлений подготовки 11.03.02, 11.04.02 «Инфокоммуникационные технологии и системы связи», 09.03.01 «Информатика и вычислительная техника», 09.03.04 «Программная инженерия» при изучении дисциплин по теории помехоустойчивого кодирования, а также аспирантами и инженерно-техническими работниками, разрабатывающими современные инфокоммуникационные системы.

УДК 621.391(075.8)
ББК 32.811.7я73

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Настоящее учебное пособие посвящено вопросам повышения эффективности передачи информации по каналам с помехами посредством применения современных помехоустойчивых кодов для борьбы с ошибками. Оно является логическим продолжением изданных ранее учебных пособий по теории и практике помехоустойчивого кодирования, в которых рассматриваются основы теории алгебраических циклических кодов (часть 1) [2], а также сверточных и турбокодов (часть 2) [13].

В настоящем пособии рассматриваются два класса кодов.

В первый класс кодов вошли эквивалентные циклические коды как рекуррентные последовательности, построенные на основе двойственного базиса поля Галуа.

Второй класс – коды с малой плотностью проверок на четность Р. Галлагера.

Теоретические основы этих кодов были известны достаточно давно, но практический интерес к их применению возник с 90-х гг. прошлого века.

Общим для этих кодов является мажоритарный способ декодирования.

Для эквивалентных циклических кодов Боуза – Чоудхури – Хоквингема (БЧХЭ) и Рида – Соломона (РСЭ) мажоритарным способом определяется совокупность информационных элементов кодовой комбинации на основе связей между символами кодовой комбинации циклического кода и коэффициентами двойственного базиса. Декодирование на основе двойственного базиса имеет ряд положительных свойств. Во-первых, при такой процедуре декодирования нет необходимости определять ошибочные позиции кода; во-вторых, сложность реализации существенно проще реализации алгебраических циклических кодов и она практически не зависит от кратности исправляемых ошибок в комбинации; наконец, в-третьих, для хороших каналов с малой вероятностью битовой ошибки процесс декодирования отдельной комбинации может быть завершен еще до окончания приема всей кодовой комбинации. Можно назвать еще одну положительную особенность, состоящую в возможности повышения достоверности передачи данных в канале с повышенной вероятностью битовой ошибки за счет применения децимаций над принятой комбинацией.

Для кодов Галлагера мажоритарным способом исправляются независимые ошибки на основе проверочных соотношений, заложенных в проверочной матрице. Для обеспечения независимости проверочных соотношений автор использует специальную конструкцию проверочной матрицы с малым количеством «единиц». Интерес к кодам Галлагера возник в результате их возможности работать вблизи границы Шеннона, т. е. на скорости, близкой к пропускной способности канала. Технология декодирования

кодов Галлагера близка к технологии декодирования турбокодов, но при этом имеет более простую реализацию. Коды Галлагера нашли применение во многих стандартах цифровой аппаратуры передачи данных космических, спутниковых, мобильных и других систем связи. Алгоритм декодирования кодов Галлагера требует использования демодуляторов с двумя выходными характеристиками принятых сигналов (выходами):

– выход жестких двоичных решений о значении принятых кодовых символов,

– выход мягких решений, пропорциональных логарифмическому отношению правдоподобия принятых кодовых символов.

На основании жестких решений вычисляется синдром ошибки, а на основании заданного числа итераций мягкого декодирования корректируется надежность кодовых символов, входящих в различные проверочные соотношения, т. е. при декодировании используется корректирующая способность кода по жесткому решению и ее уточнение по итеративному мягкому решению. При достаточно большом числе итераций мягкого декодирования удается снизить вероятность ошибочного декодирования по сравнению с жестким декодированием.

1. ЦИКЛИЧЕСКИЕ КОДЫ КАК РЕКУРРЕНТНЫЕ ПОСЛЕДОВАТЕЛЬНОСТИ И ИХ ДЕКОДИРОВАНИЕ С ИСПОЛЬЗОВАНИЕМ ДВОЙСТВЕННОГО БАЗИСА

1.1. Эквивалентное представление циклических кодов рекуррентными последовательностями

Как известно [1, 2], классический способ получения комбинации систематического циклического (n,k)-кода состоит в добавлении к исходной k-элементной комбинации $\varphi(x) = a_0 + a_1x + \ldots + a_{k-1}x^{k-1}$ остатка от деления произведения $x^{n-k}\varphi(x)$ на образующий многочлен $G(x)$степени $(n - k)$, т. е.

$$f(x) = -R(x) + x^{n-k}\varphi(x) = Q(x)G(x).$$

В общем случае комбинация такого кода для простого поля $GF(p)$ имеет длину $n = p^k - 1$, первые k элементов которой являются информационными.

Для двоичных неукороченных циклических кодов имеем $n = 2^k - 1$.

Проверочный многочлен $P(x)$ в этом случае находят как $P(x) = \dfrac{x^n - 1}{G(x)}$.

Из приведенных выражений следуют известные свойства циклических кодов, а именно, любая разрешенная комбинация циклического (n,k)-кода, представленная многочленом $f(x)$, делится на образующий многочлен $G(x)$ без остатка, т. е. $f(x) \equiv 0[\mathrm{mod}G(x)]$, и, во-вторых, произведение $f(x)\cdot P(x)$ делится на двучлен $(x^n - 1)$ без остатка, т. е.

$$f(x)\cdot P(x) = Q(x)\cdot G(x)\cdot\frac{x^n - 1}{G(x)} = Q(x)\cdot\left(x^n - 1\right) \equiv 0 \quad \left[\mathrm{mod}\left(x^n - 1\right)\right].$$

С другой стороны, комбинации такого циклического кода могут быть представлены рекуррентными последовательностями, удовлетворяющими определенному разностному (рекуррентному или возвратному) уравнению. Такой код называют двойственным или дуальным [1]. При этом построение такого циклического (n, k)-кода может быть реализовано с помощью k-элементного регистра сдвига с вынесенными сумматорами, расположение которых задается характеристическим многочленом

$$P(x) = \frac{x^n - 1}{G(x)} = x^{n-k} + p_1x^{n-k-1} + p_2x^{n-k-2} + \ldots + p_{n-k-1}x + p_{n-k}. \quad (1.1)$$

В ячейки регистра записывается параллельным кодом исходная k-элементная комбинация и в течение n тактов на выходе кодера формируется комбинация циклического кода как рекуррентная последовательность.

Пример 1.1. Рассмотрим простой пример эквидистантного циклического кода $(n, k) = (7, 3)$. В качестве характеристического многочлена $P(x)$ выберем примитивный многочлен третьей степени $P(x) = 1 + x + x^3$.

Кодирующее устройство такого систематического циклического (n, k)-кода, как классического циклического кода, строится с помощью регистра сдвига с $(n\text{-}k)$ ячейками и встроенными сумматорами. Цепи обратной связи и расположение сумматоров в регистре задаются образующим многочленом

$$G(x) = \frac{x^7 - 1}{P(x)} = 1 + x + x^2 + x^4.$$

Схема кодирующего устройства для такого циклического кода (7, 3), реализующего деление на образующий многочлен $G(x)$, показана на рис. 1.1, а.

Пусть на вход кодера (рис. 1.1, а) поступает комбинация $(a_0 a_1 a_2) = (001)$, которой соответствует многочлен $\varphi(x) = x^2$. В течение первых трех тактов, пока на вход поступает k-элементная комбинация, ключ находится в положении 1, а затем в течение $(n\text{-}k) = 4$ тактов – в положении 2. Тогда на выходе кодера будет иметь место комбинация (1101001), или в полиномиальном представлении: $f(x) = 1 + x + x^3 + x^6$.

Для рассматриваемого кода (7, 3) схема кодирующего устройства, построенного по второму варианту на основе многочлена

$$P(x) = \frac{x^7 - 1}{G(x)} = x^3 + p_1 x^2 + p_2 x + p_3 = x^3 + x + 1,$$

представлена на рис. 1.1, б.

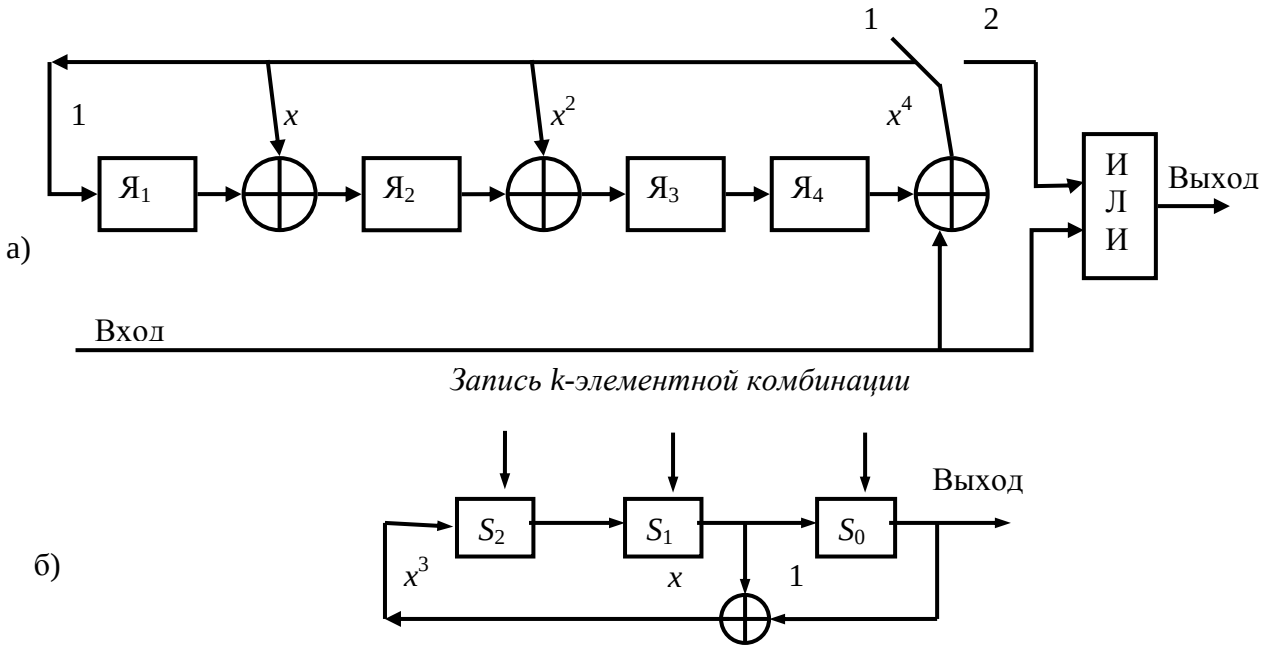

Рис. 1.1. Кодирующее устройство эквидистантного двоичного циклического кода (7, 3) с образующим многочленом $G(x) = 1 + x + x^2 + x^4$ (а) и дуального ему кода на базе многочлена $P(x) = 1 + x + x^3$ (б)

Если в ячейки памяти регистра сдвига с вынесенным сумматором записать параллельным кодом такую же исходную k-элементную информационную комбинацию$(s_2 s_1 s_0)$ = (0 0 1), то на выходе кодера будет сформирована последовательность $(s_6 s_5 s_4 s_3 s_2 s_1 s_0)$ = (1 1 0 1 0 0 1), которая совпадает с последовательностью, сформированной на выходе кодера на рис. 1.1, а.

Очевидно, что сформированная на выходе второго кодера последовательность является линейной возвратной последовательностью, удовлетворяющей рекуррентному уравнению $s_i = s_{i-2} + s_{i-3}$, где $i \geq 3$, в частности, при $i = 4$ имеем $s_4 = s_2 + s_1$. Этому уравнению соответствует характеристический многочлен $P(x)$, который является порождающим для второго метода построения эквидистантного циклического (7, 3)-кода.

Второй вариант циклического кода с порождающим многочленом $P(x)$ является дуальным [1] к коду с образующим многочленом

$$G(x) = \frac{x^7 - 1}{P(x)} = 1 + x + x^3.$$

Таким образом, мы рассмотрели два варианта построения циклического (n, k)-кода. Кодирующие устройства обоих вариантов формируют одинаковые кодовые последовательности, т. е. являются эквивалентными.

Известны различные алгоритмы декодирования циклических кодов, в частности, на основе синдромов (Питерсона – Горенштейна – Цирлера (PGZ), Берлекемпа – Мэсси, алгоритм Евклида), табличный, а также мажоритарное декодирование на основе контрольных проверок [2]. В данном учебном пособии рассматривается мажоритарное декодирование максимального правдоподобия на основе двойственного базиса поля $GF(p^k)$.

Заметим, что все указанные алгоритмы декодирования относятся к системам с «фиксированной» начальной точкой, т. е. с известным началом каждой комбинации циклического (n, k)-кода.

Критериями сравнительной оценки эффективности алгоритмов декодирования циклических кодов могут быть корректирующие способности, задержки, вносимые декодированием, сложность реализации и объем требуемой памяти, необходимой для декодирования.

1.2. Эквивалентные циклические коды БЧХ и их декодирование с использованием двойственного базиса

В табл. 1.1 приведены несколько вариантов двоичных циклических (n, m)-кодов БЧХ, где минимальные многочлены f_0, f_1, f_3, f_5 и f_7 имеют вид

$$
\begin{aligned}
f_0(x) &= (x+\ 1);\\
f_1(x) &= x^4 + x + \ 1;\\
f_3(x) &= x^4 + x^3 + x^2 + x + 1;\\
f_5(x) &= x^2 + x + 1;\\
f_7(x) &= x^4 + x^3 + 1
\end{aligned}
\qquad (1.2)
$$

и входят в разложение на множители двучлена (x^{15}– 1). Первый вариант кода представляет собой простой эквидистантный циклический код типа *M*-последовательности с периодом 15, обладающий наибольшей избыточностью. Последний вариант является обычным кодом Хэмминга с $d_{\min} = 3$.

Таблица 1.1

Циклический (*n*,*m*)-код	Рекурсивный многочлен *P*(*x*)	Степень многочлена *P*(*x*)	Минимальное кодовое расстояние d_{min}	Примечания
(15,4)	f_1	4	8	*M*-последовательность
(15,5)	f_0f_1	5	7	БЧХ
(15,6)	f_1f_5	6	6	БЧХ
(15,7)	$f_0f_1f_5$	7	5	БЧХ
(15,8)	f_1f_7	8	4	БЧХ
(15,10)	$f_1f_3f_5$	10	4	БЧХ
(15,11)	$f_0f_1f_3f_5$	11	3	Код Хэмминга

Другие промежуточные варианты кодов представляют собой примеры классических циклических кодов. Классические циклические коды БЧХ строятся по выбранному образующему многочлену *G*(*x*). Как известно [1], процедура алгебраического декодирования таких кодов БЧХ во временной области состоит из следующих последовательных шагов.

Шаг 1. Принимаемая комбинация циклического (*n*, *m*)-кода БЧХ записывается в буферный накопитель, и параллельно по схеме Горнера вычисляются синдромы. Процедура определения синдромов завершается после приема всей кодовой комбинации.

Шаг 2. Составляется система уравнений (тождества Ньютона), которая решается относительно неизвестных коэффициентов многочлена локаторов ошибок.

Шаг 3. Используя процедуру Ченя, находятся корни многочлена локаторов ошибок, которые и указывают на ошибочные позиции в кодовой комбинации.

Шаг 4. Исправляются ошибки путем добавления к каждой ошибочной позиции единицы по модулю 2 в случае двоичных кодов БЧХ.

Таким образом, особенностями описанной классической процедуры декодирования кодов БЧХ во временной области являются обязательный прием и обработка всей n-элементной кодовой комбинации и исправление каждой из ошибок в отдельности.

Основной трудностью алгебраической процедуры декодирования кодов БЧХ является вычисление детерминантов матрицы, составленной из синдромов. Сложность такой процедуры декодирования растет с увеличением кратности t исправляемых ошибок. Вычисление детерминанта матрицы при $t \geq 4$ является довольно трудоемкой задачей. Поэтому на практике чаще всего применяют коды БЧХ с исправлением $t \leq 3$ ошибок в комбинации. При этом, чем больше кратность исправляемых ошибок, тем сложнее реализация декодера, в связи с чем не прекращаются попытки разработать такие новые алгоритмы декодирования циклических кодов, сложность реализации которых практически мало бы зависела от кратности исправляемых ошибок t. К числу таких новых алгоритмов может быть отнесен алгоритм мажоритарного декодирования циклических кодов как рекуррентных последовательностей на основе двойственного базиса [3].

Рассмотрим алгоритм декодирования кодов БЧХ как рекуррентных последовательностей на основе использования двойственного базиса.

Как показано в [1], циклический (n, m)-код над полем $GF(2^k)$, построенный по рекурсивному многочлену $P(x)$ степени m, является эквивалентным (дуальным) циклическому (n, m)-коду с образующим многочленом $G(x) = (x^n-1)/P(x)$ при $n = 2^k - 1$.

Будем обозначать такие эквивалентные (дуальные) циклические коды БЧХ как коды БЧХЭ.

Обозначим корни характеристического многочлена $P(x)$ через ε_1, ε_2, ε_3, ..., ε_m, где ε_i – элементы поля $GF(2^k)$, образованного первообразным элементом ε. При этом будем считать, что элемент поля ε является корнем некоторого примитивного многочлена степени k, образующего поле $GF(2^k)$. Так как характеристический многочлен $P(x)$ является разложимым на сомножители в виде минимальных многочленов $f_i(x)$, ..., $f_j(x)$, то множеству корней многочлена $P(x)$ ε_1, ε_2, ε_3, ..., ε_m можно поставить в соответствие объединение подмножеств, которые представляют собой циклотомические классы $C(i)$, ...$C(j)$ минимальных многочленов $f_i(x)$, ..., $f_j(x)$ соответственно.

Циклический код БЧХЭ с характеристическим многочленом

$$P(x) = p_0 x^m + p_1 x^{m-1} + \ldots + p_{m-1} x + p_m; \qquad p_i \in GF(2). \tag{1.3}$$

представляет собой множество из 2^m последовательностей $\{s\}=(s_0 s_1 s_2 s_3 \ldots s_{(p^k-2)})$, элементы которых удовлетворяют рекуррентному соотношению (1.4):

$$s_i = -s_{i-1} p_1 - s_{i-2} p_2 - \ldots - s_{i-m} p_m; \;\; i \geq m. \tag{1.4}$$

Таким образом, каждая комбинация $\{s\}$ будет содержать m информационных элементов s_0, s_1, ..., s_{m-1}, которые и порождают ее. Задачей декодирования, как и ранее, является определение информационных элементов s_0, s_1, ..., s_{m-1} по принятой $\{s\}$-последовательности, содержащей в общем случае и ошибки.

Как показано в [3], произвольный элемент s_l последовательности $\{s\}$, удовлетворяющей рекуррентному уравнению (1.4), может быть найден из выражения (1.5):

$$s_n = C_1\varepsilon_1^{\,n} + C_2\varepsilon_2^{\,n} + \ldots + C_m\varepsilon_m^{\,n}, \qquad (1.5)$$

где коэффициенты C_1, C_2, …, C_m принадлежат полю $GF(p^k)$, а их значения зависят от исходных элементов последовательности, а именно, s_0, s_1,..., s_{m-1}.

Учитывая, что характеристический многочлен $P(x)$ степени m, порождающий комбинации циклического кода БЧХЭ как рекуррентные последовательности, является приводимым, то декодирование таких комбинаций может производиться с использованием двойственного базиса в соответствии с методикой, изложенной в разд. 3.3 в [3].

Рассмотрим более детально процедуру декодирования кодов БЧХЭ, как рекуррентных последовательностей, на конкретных примерах.

Пример 1.2. Выберем, в соответствии с обозначениями (1.2), рекурсивный многочлен, состоящий из двух сомножителей:

$$P(x) = f_i(x)\cdot f_j(x) = f_1(x)\cdot f_5(x) = (x^4 + x + 1)(x^2 + x + 1),$$

где степень первого неприводимого многочлена $f_1(x)$·обозначим как $g = 4$, а степень второго неприводимого многочлена – как $v = 2$.

Как было показано в табл. 1.1, с помощью такого рекурсивного многочлена $P(x)$ может быть построен двоичный код БЧХЭ (15,6) с минимальным кодовым расстоянием $d_{\min} = 6$над полем Галуа $GF(2^4)$, т. е. $k = 4$. Очевидно, такой код БЧХЭ может гарантированно исправлять все однократные и двукратные ошибки.

Запишем заданный многочлен $P(x)$ шестой степени в форме (1.3):

$$P(x) = p_0x^6 + p_1x^5 + p_2x^4 + p_3x^3 + p_4x^2 + p_5x + p_6 = x^6 + x^5 + x^4 + x^3 + 1, \qquad (1.6)$$

из которой следует, что

$$p_0 = p_1 = p_2 = p_3 = p_6 = 1 \text{ и} p_4 = p_5 = 0.$$

Тогда, в соответствии с (1.4), рекуррентная последовательность $\{s\}$ на выходе кодирующего устройства рассматриваемого кода БЧХЭ будет удовлетворять рекуррентному уравнению:

$$s_{l+6} \equiv s_{l+5} + s_{l+4} + s_{l+3} + s_l \pmod 2. \qquad (1.7)$$

Теперь, зная коэффициенты p_i многочлена $P(x)$, по методике, изложенной в [3], найдем коэффициенты α_ρ и β_ρ соответственно для минимальных многочленов $f_1(x) = x^4 + x + 1$ и $f_5(x) = x^2 + x + 1$ по формулам:

$$\alpha_\rho = \frac{\sum_{l=0}^{m-\rho} p_{m-\rho-l}\left(\varepsilon^i\right)^l}{p'\left(\varepsilon^i\right)};\ GF(2^4), \tag{1.8}$$

$$\beta_\rho = \frac{\sum_{l=0}^{m-\delta} p_{m-\rho-l}\left(\varepsilon^j\right)^l}{p'\left(\varepsilon^j\right)};\ GF(2^4), \tag{1.9}$$

где числа i и j являются представителями циклоклассов: $C(i)$ – для многочлена $f_i(x) = f_1(x)$степени g =4, $C(j)$ – для многочлена $f_j(x) = f_5(x)$ степени $v = 2$.

При этом корнями минимального многочлена $f_1(x)$ примем первообразные элементы поля $GF(2^4)$: $\varepsilon_1 = \varepsilon$; $\varepsilon_2 = \varepsilon^2$, $\varepsilon_3 = \varepsilon^4$ и $\varepsilon_4 = \varepsilon_g = \varepsilon^{2^{g-1}} = \varepsilon^8$. Тогда, в соответствии с формулой (1.8) и с учетом того, что в этой формуле $\varepsilon^i = \varepsilon$, а $P'(x) = x^4 + x^2$, получим следующие значения коэффициентов α_ρ, где $\rho = \overline{1,6}$:

$$\alpha_1 = \varepsilon^4;\ \alpha_2 = \varepsilon^3;\ \alpha_3 = \varepsilon^2;\ \alpha_4 = 1;\ \alpha_5 = \varepsilon^9;\ \alpha_6 = \varepsilon^5. \tag{1.10}$$

Корнями второго минимального многочлена $f_j(x) = f_5(x)$ соответственно будут элементы поля $GF(2^4)\varepsilon_{g+1} = \varepsilon_5 = \varepsilon^j = \varepsilon^5$ и $\varepsilon_{g+2} = \varepsilon_{g+v} = \varepsilon_6 = \varepsilon^{2j} = \varepsilon^{10}$. Тогда, в соответствии с формулой (1.9), получим коэффициенты β_ρ:

$$\beta_1 = \varepsilon^{10};\ \beta_2 = \varepsilon^5;\ \beta_3 = 1;\ \beta_4 = 0;\ \beta_5 = \varepsilon^{10};\ \beta_6 = 1. \tag{1.11}$$

В общем виде по методике, изложенной в [3], для двух сомножителей многочлена $P(x)$ искомые коэффициенты C_r, $r = 1, 2, \ldots, m$, уравнения (1.5) могут быть найдены по любому m-элементному безошибочному участку $(s_n s_{n+1} \ldots s_{n+m-1})$ принятой рекуррентной последовательности как:

$$C_1 = \varepsilon_1^{-n}\sum_{\rho=1}^{m} s_{n+\rho-1}\alpha_\rho = \sum_{\rho=1}^{m} s_{n+\rho-1}\omega_\rho \tag{1.12}$$

для первого корня $\varepsilon_1 = \varepsilon$ многочлена $f_i(x) = f_1(x)$ и

$$C_{g+1} = \varepsilon_{g+1}^{-n}\sum_{\rho=1}^{m} s_{n+\rho-1}\beta_\rho = \sum_{\rho=1}^{m} s_{n+\rho-1}\upsilon_\rho \tag{1.13}$$

для первого из корней $\varepsilon_{g+1} = \varepsilon^5$ многочлена $f_j(x) = f_5(x)$, где g – степень минимального многочлена $f_i(x)$. Учитывая принятое ранее допущение, что корнями минимального многочлена $f_i(x)$ будут элементы $\varepsilon_1,\varepsilon_2,\varepsilon_3,\ldots,\varepsilon_{g=4}$, для которых справедливо $\varepsilon_2 = \varepsilon_1^2 = \varepsilon^2,\ldots, \varepsilon_g = \varepsilon^{2^{g-1}}$, а также учитывая (1.12), в соответствии с [3] получаем:

$$C_2 = C_1^2; C_3 = C_1^{2^2}, ..., C_g = C_1^{2^{g-1}}.$$

Аналогично, для минимального многочлена $f_j(x)$ степени v имеем

$$C_{g+1}; C_{g+2} = \left(C_{g+1}\right)^2, ..., \left(C_{g+v}\right) = \left(C_{g+1}\right)^{2^{v-1}}.$$

Для большей наглядности в записи формулы (1.5) введем следующие обозначения:

– для многочлена $f_i(x)$:

$$\varepsilon_1 = \varepsilon;\ C_1 = C \in GF(p^k); \tag{1.14}$$

– для многочлена $f_j(x)$:

$$\varepsilon_{g+1} = \mu;\ C_{g+1} = D_1 = D; \quad \in GF(p^k). \tag{1.15}$$

Тогда общее выражение (1.5) для определения произвольного элемента кодовой последовательности s_n перепишется в виде:

$$\begin{aligned} s_n &= C\varepsilon^n + C^2\varepsilon^{2n} + ... + C^{2^{g-1}}\varepsilon^{2^{g-1}n} + D\mu^n + D^2\mu^{2n} + ... + D^{2^{v-1}}\mu^{2^{v-1}n} = \\ &= C\varepsilon^n + \left(C\varepsilon^n\right)^2 + ... + (C\varepsilon^n)^{2^{g-1}} + D\mu^n + \left(D\mu^n\right)^2 + ... + \left(D\mu^n\right)^{2^{v-1}} \end{aligned} \tag{1.16}$$

Как видно из выражения (1.16), элемент s_n будет равен:

$$s_n = T_i\left(C\varepsilon^n\right) + T_j\left(D\mu^n\right), \tag{1.17}$$

где $T_i()$ и $T_j()$ − функции-след относительно минимальных многочленов $f_i(x)$ и $f_j(x)$ соответственно.

Таким образом, можно сформулировать важный вывод, заключающийся в следующем: «*Если рекурсивный многочлен $P(x)$ представляет собой произведение нескольких минимальных многочленов $f_i(x)$, $f_j(x),\ldots, f_z(x)$, то элементы рекуррентной последовательности представляют собой сумму функций-след по этим многочленам, т. е.*

$$s_n = T_i\left(C\varepsilon^n\right) + T_j\left(D\mu^n\right) + ... + T_z\left(E\gamma^n\right), \tag{1.18}$$

где ε, μ, …, γ *корни многочленов* $f_i(x)$, $f_j(x)$, …, $f_z(x)$ *соответственно, а коэффициенты* C, D,…, E *определяются информационными элементами* $(s_0 s_1 s_2 \ldots s_{m-1})$, *которые являются начальными элементами, порождающими рекуррентную последовательность* $\{s\}$».

Рассмотрим теперь процедуру мажоритарного декодирования кода (15,6) с заданным рекурсивным многочленом $P(x)$ в примере (1.2).

Пусть на вход декодера поступает следующая последовательность $\{s\}$ без ошибок:

$$\{s\} = (s_0\, s_1\, s_2 s_3\, s_4\, s_5\, s_6\, s_7\, s_8\, s_9\, s_{10}\, s_{11}\, s_{12}\, s_{13}\, s_{14})$$
$$0\ 1\ 1\ 1\ 1\ 1\ 1\ 0\ 1\ 1\ \ 1\ \ 0\ \ 1\ \ 0\ \ 0$$

По произвольному m-элементному участку, где m − число информационных элементов кодовой комбинации кода $(n, m) = (15,6)$, в соответствии с формулами (1.12) и (1.13) и с учетом обозначений (1.14) и (1.15), найдем коэффициенты C и D. Например, выберем участок

$$(s_l s_{l+1}\, s_{l+2}\, s_{l+3}\, s_{l+4}\, s_{l+5}) = (s_5 s_6 s_7 s_8 s_9 s_{10}) = (110111).$$

Тогда по (1.12), с учетом (1.14) и (1.10), для $l = 5$ найдем:

$$C = \varepsilon^{-l} \sum_{\rho=1}^{m=5} s_{l+\rho-1}\alpha_\rho = \varepsilon^{-5}(\alpha_1 + \alpha_2 + \alpha_4 + \alpha_5 + \alpha_6) =$$

$$= \varepsilon^{-5}(\varepsilon^4 + \varepsilon^3 + 1 + \varepsilon^9 + \varepsilon^5) = \varepsilon^{-5}(\varepsilon + \varepsilon^2) = \varepsilon^{-5}\varepsilon^5 = 1.$$

Аналогично, по(1.13), с учетом (1.15) и (1.11),найдем:

$$D = (\varepsilon^5)^{-l} \sum_{\rho=1}^{m=5} s_{l+\rho-1}\beta_\rho = (\varepsilon^5)\varepsilon^{-5}(\beta_1 + \beta_2 + \beta_4 + \beta_5 + \beta_6) =$$

$$= \varepsilon^5(\varepsilon^{10} + \varepsilon^5 + \varepsilon^{10} + 1) = 1.$$

Возьмем другой m-элементный участок, например, $(s_9 s_{10} s_{11} s_{12} s_{13} s_{14}) =$ $= (110100)$. Тогда коэффициенты C и D будут:

$$C = \varepsilon^{-9}(\alpha_1 + \alpha_2 + \alpha_4) = \varepsilon^{-9}(\varepsilon^4 + \varepsilon^3 + 1) = \varepsilon^{-9}(1\varepsilon + \varepsilon^3 + 1) = \varepsilon^{-9}\varepsilon^9 = 1;$$
$$D = (\varepsilon^5)\varepsilon^{-9}(\beta_1 + \beta_2 + \beta_4) = \varepsilon^0(\varepsilon^{10} + \varepsilon^5) = 1.$$

Таким образом, получились те же значения C и D.

Проследим теперь процесс мажоритарного декодирования последовательности $\{h\}$, в которой содержатся две ошибки (мы умышленно не будем указывать номера ошибочных позиций, чтобы продемонстрировать алгоритм декодирования, который не требует нахождения ошибочных позиций).

Итак, пусть принятый вектор имеет вид:

$$\{h\} = (h_0\, h_1\, h_2\, h_3\, h_4\, h_5\, h_6\, h_7\, h_8\, h_9\, h_{10}\, h_{11}\, h_{12}\, h_{13}\, h_{14})$$
$$0\ 1\ 1\ 1\ 1\ 0\ 1\ 0\ 1\ \ 1\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0$$

Как видно из табл. 1.2, в результате обработки m-элементных участков принятого вектора наибольшее количество совместных значений коэффициентов C_i и D_i равны «1». Таким образом, как и в случае безошибочной последовательности $\{s\}$, будет принято решение, что $C = 1$ и $D = 1$.

Таблица1.2

i	$h_i h_{i+1}\, h_{i+2}\, h_{i+3}\ h_{i+4} h_{i+5}$	$C_i = \varepsilon^{-i} \sum_{\rho=1}^{m=6} h_{i+\rho-1}\alpha_i$	$D_i = (\varepsilon^5)^{-i} \sum_{\rho=1}^{m=6} h_{i+\rho-1}\beta_i$
0	0 1 1 1 1 0	$C_0 = \varepsilon^3 + \varepsilon^2 + 1 + \varepsilon^9 = \varepsilon^{10}$	$D_0 = \varepsilon^5 + 1 + \varepsilon^{10} = 0$
1	1 1 1 1 0 1	$C_1 = \varepsilon^{-1}(\varepsilon^4 + \varepsilon^2 + \varepsilon^3 + 1 + \varepsilon^5) = \varepsilon^2$	$D_1 = \varepsilon^{-5}(\varepsilon^{10} + \varepsilon^5 + 1 + 1) = = \varepsilon^{-5} = \varepsilon^{10}$
2	1 1 1 0 1 0	$C_2 = \varepsilon^{-2}(\varepsilon^4 + \varepsilon^3 + \varepsilon^2 + \varepsilon^9) = \varepsilon^6$	$D_2 = \varepsilon^{-10}(\varepsilon^{10} + \varepsilon^5 + 1 + \varepsilon^{10}) = 1$
3	1 1 0 1 0 1	$C_3 = \varepsilon^{-3}(\varepsilon^4 + \varepsilon^3 + 1 + \varepsilon^5) = 0$	$D_3 = (\varepsilon^{10} + \varepsilon^5 + 1) = 0$
4	1 0 1 0 1 1	$C_4 = \varepsilon^{-4}(\varepsilon^4 + \varepsilon^2 + \varepsilon^9 + \varepsilon^5) = \varepsilon^3$	$D_4 = \varepsilon^{-5}(\varepsilon^{10} + 1 + \varepsilon^{10} + 1) = 0$
5	0 1 0 1 1 0	$C_5 = \varepsilon^{-5}(\varepsilon^3 + 1 + \varepsilon^9) = \varepsilon^{14}$	$D_5 = \varepsilon^{-10}(\varepsilon^5 + \varepsilon^{10}) = \varepsilon^{-10} = \varepsilon^5$
6	1 0 1 1 0 0	$C_6 = \varepsilon^{-6}(\varepsilon^4 + \varepsilon^2 + 1) = \varepsilon^{14}$	$D_6 = 1(\varepsilon^{10} + 1) = \varepsilon^5$
7	0 1 1 0 0 1	$C_7 = \varepsilon^{-7}(\varepsilon^3 + \varepsilon^2 + \varepsilon^5) = \varepsilon^2$	$D_7 = \varepsilon^{-5}(\varepsilon^5 + 1 + 1) = 1$
8	1 1 0 0 1 0	$C_8 = \varepsilon^{-8}(\varepsilon^4 + \varepsilon^3 + \varepsilon^9) = \varepsilon^7$	$D_8 = \varepsilon^{-10}(\varepsilon^{10} + \varepsilon^5 + \varepsilon^{10}) = \varepsilon^{-5} = = \varepsilon^{10}$
9	1 0 0 1 0 0	$C_9 = \varepsilon^{-9}(\varepsilon^4 + 1) = \varepsilon^7$	$D_9 = 1(\varepsilon^{10}) = \varepsilon^{10}$
10	0 0 1 0 0 0	$C_{10} = \varepsilon^{-10}\varepsilon^2 = \varepsilon^7$	$D_{10} = \varepsilon^{-5}(1) = \varepsilon^{10}$
11	0 1 0 0 0 1	$C_{11} = \varepsilon^{-11}(\varepsilon^3 + \varepsilon^5) = 1$	$D_{11} = \varepsilon^{-10}(\varepsilon^5 + 1) = 1$
12	1 0 0 0 1 1	$C_{12} = \varepsilon^{-12}(\varepsilon^4 + \varepsilon^9 + \varepsilon^5) = 1$	$D_{12} = 1(\varepsilon^{10} + \varepsilon^{10} + 1) = 1$
13	0 0 0 1 1 1	$C_{13} = \varepsilon^{-13}(1 + \varepsilon^9 + \varepsilon^5) = 1$	$D_{13} = \varepsilon^{-5}(\varepsilon^{10} + 1) = 1$
14	0 0 1 1 1 1	$C_{14} = \varepsilon^{-14}(\varepsilon^2 + 1 + \varepsilon^9 + \varepsilon^5) = 1$	$D_{14} = \varepsilon^{-10}(1 + \varepsilon^{10} + 1) = 1$

Найдя коэффициенты C и D, мы теперь можем по формуле (1.17) восстановить любой элемент s_i последовательности $\{s\}$. Например, элемент s_5 будет определяться из выражения:

$$s_5 = T_i(C\varepsilon^5) + T_j(D\mu^5) = \sum_{i=0}^{g-1} C^{2^i}\, \varepsilon^{5*2^i} + \sum_{j=0}^{v-1} D^{2^j}\, \mu^{5*2^j},$$

где g – степень многочлена $f_1(x)$, ($g = 4$), а v – степень многочлена $f_5(x)$, ($v = 2$). При этом $\mu = \varepsilon^5$ – корень многочлена $f_5(x)$ с порядком $2^s - 1 = 3$.

Найдем значение функции-след $T_i(C\varepsilon^5)$ при C = 1:

$$T_1(\varepsilon^5) = \varepsilon^5 + (\varepsilon^5)^2 + (\varepsilon^5)^4 + (\varepsilon^5)^8 = \varepsilon^5 + \varepsilon^{10} + \varepsilon^5 + \varepsilon^{10} = 0, \bmod f_1(x).$$

Многочлен $f_5(x) = x^2 + x + 1$ и его корень μ порядка 3 образует подполе $GF(2^2)$ поля $GF(2^4)$. В состав подполя $GF(2^2)$, кроме нуля, входят также ненулевые элементы 1, μ и $\mu^2 = 1 + \mu$ по $\bmod f_5(x)$. Тогда функция-след $T_j(D\mu^5)$ при $D = 1$ равна:

$$T_5(\mu^5) = \mu^5 + (\mu^5)^2 \equiv \mu^2 + \mu \equiv 1 + \mu + \mu = 1, \bmod f_5(x).$$

Таким образом, элемент $s_5 = 0 + 1 = 1$, mod 2.

Сравнивая элемент s_5 и элемент h_5 в принятом векторе $\{h\}$, можно увидеть, что именно элемент h_5 является ошибочным.

Аналогично, определим, например, элемент s_6:

$$s_6 = T_i(C\varepsilon^6) + T_j(D\mu^6) = T_1(\varepsilon^6) + T_5(\mu^6) = 1 + (\mu^6) + (\mu^6)^2 = 1 + 1 + 1 = 1 \pmod 2.$$

Заметим, что ошибки были введены в пятый и десятый разряды комбинации $\{h\}$, т. е. в элементы h_5 и h_{10}.

Пример 1.3. Рассмотрим еще один пример циклического кода БЧХЭ над полем $GF(2^4)$ с рекурсивным многочленом

$$P(x) = f_0(x)f_1(x) = (x + 1)(x^4 + x + 1).$$

Как следует из табл. 1.1, с помощью такого рекурсивного многочлена $P(x)$ может быть построен двоичный код БЧХЭ (15, 5) с $d_{\min} = 7$. Рекуррентная последовательность $\{s\}$ строится по рекуррентному правилу

$$s_l = s_{l-1} + s_{l-3} + s_{l-5} \pmod 2, \quad l = 5,6,7,...,$$

определяемому рекурсивным многочленом $P(x)$ вида (1.3):

$$P(x) = p_0x^5 + p_1x^4 + p_2x^3 + p_3x^2 + p_4x + p_5 = x^5 + x^4 + x^2 + 1,$$

где $p_0 = p_1 = p_3 = p_5 = 1$ и $p_2 = p_4 = 0$.

Найдем теперь коэффициенты α_ρ и β_ρ по формулам (1.8) и (1.9). При этом для построения поля $GF(2^4)$ выберем примитивный многочлен $f_1(x)$. Воспользовавшись формулой (1.8) и подставив в нее коэффициенты p_i многочлена $P(x)$ и значение его корня $\varepsilon_1 = \varepsilon$, а также учитывая, что $P'(\varepsilon) = \varepsilon^4$, получим значения коэффициентов α_ρ, $\rho = \overline{1,m}$ при $m = 5$:

$$\alpha_1 = \varepsilon^{10}; \ \alpha_2 = \varepsilon^9; \ \alpha_3 = \varepsilon; \ \alpha_4 = 1; \ \alpha_5 = \varepsilon^{11}. \qquad (1.19)$$

Корнем второго многочлена первой степени $f_0(x) = (x + 1)$ будет $\varepsilon^0 = 1$. Тогда, воспользовавшись формулой (1.9) и подставив $\varepsilon_j = 1$, получим следующие коэффициенты β_ρ:

$$\beta_1 = 1;\ \beta_2 = 1;\ \beta_3 = 0;\ \beta_4 = 0;\ \beta_5 = 1. \qquad (1.20)$$

Рассмотрим теперь процедуру мажоритарного декодирования рассматриваемого кода БЧХЭ (15,5), представленного рекуррентными последовательностями.

Предположим, что на выход декодера поступает последовательность $\{s\}$ без ошибок, например:

$$\{s\} = (s_0\, s_1\, s_2 s_3\, s_4\, s_5\, s_6\, s_7\, s_8\, s_9\, s_{10}\, s_{11}\, s_{12}\, s_{13}\, s_{14})$$
$$1\ 1\ 0\ 1\ 1\ 0\ 0\ 1\ 0\ 1\ 0\ \ 0\ \ 0\ \ 0\ \ 1$$

Тогда по любому m-элементному участку последовательности $\{s\}$ можно восстановить информационные элементы. Для этого найдем по формулам (1.12) и (1.13), с учетом обозначений (1.14) и (1.15), коэффициенты C и D. Пусть будет выделен участок из $m = 5$ элементов $(s_l s_{l+1}\, s_{l+2}\, s_{l+3}\, s_{l+4}) = (s_6 s_7 s_8 s_9 s_{10}) = (01010)$.

Тогда, по (1.12) для $l = 6$, имеем:

$$C = \varepsilon^{-l} \sum_{\rho=1}^{m=5} s_{l+\rho-1}\alpha_\rho = \varepsilon^{-6}(\alpha_2 + \alpha_4) = \varepsilon,\ GF(2^4).$$

Аналогично, по (1.13), имеем:

$$D = \sum_{\rho=1}^{m=5} s_{l+\rho-1}\beta_\rho = (\beta_2 + \beta_4) = 1,\ GF(2^4).$$

Возьмем, например, $l = 10$ и выделим участок $(s_{10}s_{11}s_{12}s_{13}s_{14}) = (00001)$. Тогда коэффициенты C и D будут определены как:

$$C = \varepsilon^{-10}\alpha_5 = \varepsilon^{-10}\varepsilon^{11} = \varepsilon;$$
$$D = \beta_5 = 1.$$

Таким образом, по любому безошибочному m-элементному участку рекуррентной последовательности $\{s\}$ декодер определяет коэффициенты C и D, что позволяет по формуле (1.17) найти любой заданный элемент последовательности $\{s\}$. Например, элемент s_{11}, будет равен:

$$s_{11} = C\varepsilon^{11} + (C\varepsilon^{11})^2 + (C\varepsilon^{11})^4 + (C\varepsilon^{11})^8 + D\varepsilon^0 = T(C\varepsilon) + D = T(\varepsilon^{12}) + 1.$$

Так как функция-след от элемента поля ε^{12} с образующим многочленом $f_1(x) = x^4 + x + 1$ равна единице и $D = 1$, то $s_{11} = 0$.

Аналогично можно определить начальные m элементов ($s_0s_1s_2s_3s_4$) последовательности $\{s\}$, если они являются искомыми информационными элементами.

В основе мажоритарного декодирования принятой последовательности с ошибками лежит то обстоятельство, что любой безошибочный m-элементный участок рекуррентной последовательности $\{s\}$ однозначно определяет значения коэффициентов C и D. В результате декодирования замкнутой в кольцо n-элементной последовательности, в случае ее полной длины, будет вычислено n значений коэффициентов C и D. Решение об «истинных» коэффициентах C и D принимается по большинству одинаковых парных значений (мажоритарно).

В заключение отметим, что частным случаем циклических кодов БЧХЭ, как рекуррентных последовательностей, являются и M-последовательности.

1.3. Мажоритарное декодирование децимированных комбинаций кода БЧХЭ над полем GF(2k) на основе m-элементных участков с использованием двойственного базиса

В предыдущем разделе был рассмотрен алгоритм мажоритарного декодирования комбинаций (n, m)-кода БЧХЭ по m-элементным участкам последовательности на основе двойственного базиса.

Как видно из (1.18), произвольный элемент кодовой комбинации представляет собой сумму функции-след для каждой из минимальных функций $f_i(x)$. При этом коэффициенты C, D, …, E в выражении (1.18) представляют собой начальные элементы (или фазы) для каждой из рекуррентных подпоследовательностей, образованных минимальными многочленами $f_i(x)$ – сомножителями характеристического многочлена $P(x)$. Конкретные варианты таких кодов и их декодирование рассмотрены в примерах 1.2 и 1.3.

Важным преимуществом декодирования кодов БЧХЭ как рекуррентных последовательностей является то, что корректирующие свойства кода могут быть усилены вследствие применения децимаций.

Рассмотрим декодирование кодов БЧХЭ над полем $GF(2^k)$ как рекуррентных последовательностей с учетом децимаций с индексами $q = 2^i$, $i = 0,1,...,(k-1)$.

Пусть некоторой комбинации(n, m)-кода БЧХЭ, как рекуррентной последовательности $\{s\} = \left(s_0 s_1 s_2 \ldots s_{2^k-2}\right)$, соответствует характеристический

многочлен степени m в виде (1.3).Тогда элементы этой рекуррентной комбинации будут удовлетворять рекуррентному уравнению (1.4), которое для двоичных кодов перепишем в виде:

$$p_0 s_l + p_1 s_{l-1} + p_2 s_{l-2} + \ldots + p_{m-1} s_{l-m+1} + p_m s_{l-m} = 0. \qquad (1.21)$$

Будем считать, что этому уравнению соответствует характеристический многочлен $P(x)$, представляющий собой произведение сомножителей $P(x) = f_i(x) \cdot \ldots \cdot f_j(x)$, где $f_i(x), \ldots, f_j(x)$ − неприводимые полиномы деления круга в разложении двучлена $(x^n - 1)$ на сомножители, у которого $n = 2^k - 1$.

Обозначим корень минимального многочлена $f_i(x)$ как ε_i, а корень минимального многочлена $f_j(x)$ − как ε_j. Тогда, как было показано выше, элемент s_l последовательность $\{s\}$ может быть найден как сумма функций-след:

$$s_l = T\left(C_i \varepsilon_i^l\right) + \ldots + T\left(C_j \varepsilon_j^l\right), \qquad (1.22)$$

где коэффициенты $C_i, \ldots, C_j$ определяют начальные фазы рекуррентных подпоследовательностей, порождаемых неприводимыми многочленами соответственно $f_i(x), \ldots, f_j(x)$.

Для комбинаций кода БЧХЭ как рекуррентных последовательностей справедлива следующая теорема.

Теорема 1.1. *Если рекуррентную последовательность* $\{s\}$ *кода БЧХЭ над полем* $GF(2^k)$*, удовлетворяющую рекуррентному уравнению* (1.21)*, подвергнуть децимации с индексом* $q = 2^i, i = 0,1,...,(k-1)$*, то полученная последовательность* $\{v\}_q = v_0 v_1 v_2 v_3 \ldots v_{2^k-2}$*, где* $v_j = s_{j \cdot q (\mathrm{mod}\, 2^k - 1)}$*, также будет удовлетворять тому же рекуррентному уравнению.*

Для доказательства этой теоремы составим уравнение (1.21) из элементов последовательности $\{v\}_q$ и проверим его на равенство нулю.

Итак, в соответствии с (1.21), запишем сумму

$$p_0 v_l + p_1 v_{l-1} + p_2 v_{l-2} + \ldots + p_{m-1} v_{l-m+1} + p_m v_{l-m}$$

и, подставив в ней $v_j = s_{j \cdot q (\mathrm{mod}\, 2^k - 1)}$, получим:

$$p_0 s_{l \cdot q} + p_1 s_{(l-1) \cdot q} + p_2 s_{(l-2) \cdot q} + \ldots + p_{m-1} s_{(l-m+1) \cdot q} + p_m s_{(l-m) \cdot q}. \qquad (1.23)$$

Выразим теперь каждый из элементов s_j в (1.23) через функции-след в соответствии с (1.22) и получим:

$$p_0\left[T\left(C_i\varepsilon_i^{lq}\right)+\ldots+T\left(C_j\varepsilon_j^{lq}\right)\right]+p_1\left[T\left(C_i\varepsilon_i^{(l-1)q}\right)+\ldots+T\left(C_j\varepsilon_j^{(l-1)q}\right)\right]+\ldots+$$
$$+p_{m-1}\left[T\left(C_i\varepsilon_i^{(l-m+1)q}\right)+\ldots+T\left(C_j\varepsilon_j^{(l-m+1)q}\right)\right]+$$
$$+p_m\left[T\left(C_i\varepsilon_i^{(l-m)q}\right)+\ldots+T\left(C_j\varepsilon_j^{(l-m)q}\right)\right].$$

Подставляя общее выражение для функции-след, а также учитывая, что $\varepsilon_i,\ldots,\varepsilon_j$ – корни характеристического многочлена $P(x)$, получим очевидное равенство нулю выражения (1.23), т. е.

$$\sum_{t=1}^{d_i}C_i^{2^{t-1}}\left[P\left(\varepsilon_i^{2^{t-1}}\right)\right]^q+\ldots+\sum_{t=1}^{d_j}C_j^{2^{t-1}}\left[P\left(\varepsilon_j^{2^{t-1}}\right)\right]^q=0,$$

где $d_i,\ldots,d_j$ – степени сомножителей многочлена $P(x)$.

Таким образом, теорема доказана.

Как видно из (1.22), элементы $C_i,\ldots,C_j\in GF(2^k)$ задают начальную фазу двоичной последовательности $\{s\}$. Поэтому задачей декодирования кода БЧХЭ и будет определение этих элементов $C_i,\ldots,C_j$. Покажем, что в этом случае будет справедлива следующая теорема.

Теорема 1.2. *Если элементы* $C_i,\ldots,C_j\in GF(2^k)$ *однозначно определяют начальную фазу рекуррентной последовательности {s}, то начальная фаза последовательности* $\{v\}_q$*, полученной из {s} путем ее децимации с индексом* $q=2^i, i=0,1,...,(k-1)$*, будет определяться как* $\tilde{C}_i=\sqrt[q]{C_i}$, …, $\tilde{C}_j=\sqrt[q]{C_j}\in GF(2^k)$.

Для доказательства этого запишем, что, в соответствии с доказанной теоремой (1.1) и уравнением (1.22), каждый из элементов v_i последовательности $\{v\}_q$ будет равен

$$v_i=T\left(\tilde{C}_i\varepsilon_i^l\right)+\ldots+T\left(\tilde{C}_j\varepsilon_j^l\right). \tag{1.24}$$

В то же время этот же элемент в последовательности $\{s\}$, в соответствии с (1.22), будет равен

$$v_i=s_{lq}=T\left(C_i\varepsilon_i^{lq}\right)+\ldots+T\left(C_j\varepsilon_j^{lq}\right)=\left[T\left(\sqrt[q]{C_i}\varepsilon_i^l\right)\right]^q+\ldots+\left[T\left(\sqrt[q]{C_j}\varepsilon_j^l\right)\right]^q=$$
$$=T\left(\sqrt[q]{C_i}\varepsilon_i^l\right)+\ldots+T\left(\sqrt[q]{C_j}\varepsilon_j^l\right). \tag{1.25}$$

Приравнивая (1.24) и (1.25), получаем, что

$$\tilde{C}_i=\sqrt[q]{C_i},\ldots,\tilde{C}_j=\sqrt[q]{C_j}\ . \tag{1.26}$$

Таким образом, исходные элементы $C_i, \ldots, C_j$ могут быть определены на основе двойственного базиса путем мажоритарного декодирования m-элементных участков как принятой рекуррентной последовательности $\{s\}$, так и последовательностей $\{v\}_q$, полученных из $\{s\}$ путем децимаций с индексами $q = 2^i, i = 0,1,...,(k-1)$ в соответствии с выражениями:
для $\{s\}$:

$$C_i = \varepsilon_i^{-l} \sum_{t=1}^{m} \alpha_t s_{l+t-1}, \quad \ldots, \quad C_j = \varepsilon_j^{-l} \sum_{t=1}^{m} \beta_t s_{l+t-1}; \tag{1.27}$$

и для $\{v\}_q$:

$$\tilde{C}_i = \varepsilon_i^{-l} \sum_{t=1}^{m} \alpha_t v_{l+t-1}, \quad \ldots, \quad \tilde{C}_j = \varepsilon_j^{-l} \sum_{t=1}^{m} \beta_t v_{l+t-1}. \tag{1.28}$$

Из коэффициентов, найденных по последовательностям $\{v\}_q$, в соответствии с (1.26) находим:

$$C_i = (\tilde{C}_i)^q, \ldots, C_j = (\tilde{C}_j)^q. \tag{1.29}$$

Пример 1.4. Пусть принята комбинация кода БЧХЭ (15, 6) с образующим многочленом $P(x)$ из примера 1.2:

$$\{s\} = (s_0\ s_1\ s_2\ s_3\ s_4\ s_5\ s_6\ s_7\ s_8\ s_9\ s_{10} s_{11} s_{12} s_{13} s_{14}) = (1\ \ 1\ \ 1\ \ 1\ \ 0\ \ 0\ \ 1\ \ 1\ \ 0\ \ 0\ \ 0\ \ 1\ \ 1\ \ 0\ \ 1).$$

Выделим m-элементный участок $(s_0 s_1 s_2 s_3 s_4 s_5) = (1\ \ 1\ \ 1\ \ 0\ \ 1\ \ 0)$, тогда в соответствии с (1.10), (1.11), (1.12) и (1.13), найдем:

$$C = C_i = \alpha_1 + \alpha_2 + \alpha_3 + \alpha_5 = \varepsilon^4 + \varepsilon^3 + \varepsilon^2 + \varepsilon^9 \equiv \varepsilon^8 \left[\mathrm{mod}(1 + x + x^4) \right]$$
$$D = C_j = \beta_1 + \beta_2 + \beta_3 + \beta_5 = \mu^2 + \mu + 1 + \mu^2 \equiv \mu^2 \left[\mathrm{mod}(1 + x + x^2) \right],$$

где $\mu = \varepsilon^5$ – корень многочлена $f_j(x) = 1 + x + x^2$.

Теперь подвергнем последовательность $\{s\}$ децимации с индексом $q = 2$, в результате чего получим последовательность $\{v\}_2$:

$$\{v\}_2 = (v_0\ v_1\ v_2\ v_3\ v_4\ v_5\ v_6\ v_7\ v_8\ v_9 \cdots\ v_{14}) = (s_0\ s_2\ s_4\ s_6\ s_8\ s_{10} s_{12}\ s_{14}\ s_1\ s_3 \ldots s_{14}) =$$
$$= (1\ \ 1\ \ 1\ \ 0\ \ 1\ \ 1\ \ 1\ \ 0\ \ 1\ \ 0\ \ \ldots\ \ 1).$$

Предположим, что в последовательности $\{v\}_2$ выделен m-элементный участок $(v_2\ v_3\ v_4\ v_5\ v_6\ v_7) = (1\ \ 0\ \ 1\ \ 1\ \ 1\ \ 0)$, по которому, в соответствии с (1.28), получим

$$\tilde{C} = \varepsilon^{-2}(\alpha_1 + \alpha_3 + \alpha_4 + \alpha_5) = \varepsilon^{-2}(\varepsilon^4 + \varepsilon^2 + 1 + \varepsilon^9) = \varepsilon^{-2} \cdot \varepsilon^6 = \varepsilon^4;$$
$$\tilde{D} = \mu^{-2}(\beta_1 + \beta_3 + \beta_4 + \beta_5) = \mu^{-2}(\mu^2 + 1 + 0 + \mu^2) = \mu^{-2} = \mu.$$

Откуда, с учетом (1.29), получаем:

$$C = (\tilde{C})^q = (\varepsilon^4)^2 = \varepsilon^8; \quad D = (\tilde{D})^q = (\mu)^2.$$

Аналогично определим элементы C и D из последовательности $\{v\}_q$ с индексом децимации $q = 4$. Пусть был выделен участок

$$(v_1\ v_2\ v_3\ v_4\ v_5\ v_6) = (s_4\ s_8\ s_{12}\ s_1\ s_5\ s_9) = (1\ \ 1\ \ 1\ \ 1\ \ 0\ \ 1),$$

по которому, в соответствии с (1.28), получим

$$\tilde{C} = \varepsilon^{-1}(\alpha_1 + \alpha_3 + \alpha_4 + \alpha_6) = \varepsilon^{-1}(\varepsilon^4 + \varepsilon^3 + \varepsilon^2 + 1 + \varepsilon^5) = \varepsilon^{-1} \cdot \varepsilon^3 = \varepsilon^2;$$
$$\tilde{D} = \mu^{-1}(\beta_1 + \beta_3 + \beta_4 + \beta_6) = \mu^{-1}(\mu^2 + \mu + 1 + 1) = \mu^2.$$

Возведя полученные элементы $\tilde{C}$ и $\tilde{D}$ в степени $q = 4$, на основании (1.29), получим начальные элементы C и D:

$$C = (\tilde{C})^4 = \varepsilon^8\ [\text{mod}\ f_i(x)]; \qquad D = (\mu^2)^4 = \mu^8 = \mu^2\ [\text{mod}\ f_j(x)].$$

Наконец, при индексе децимации $q = 2^{k-1} = 8$ последовательность $\{v\}_8$ примет вид

$$\{v\}_8 = (v_0\ v_1\ v_2\ v_3\ v_4\ v_5\ v_6 \cdots\ v_{14}) = (s_0\ s_8\ s_1\ s_9\ s_2\ s_{10}\ s_3 \ldots\ s_7) =$$
$$= (1\ \ 1\ \ 1\ \ 1\ \ 1\ \ 1\ \ 0\ \ \ldots\ \ 0).$$

Если выделить, например, участок

$$(v_1\ v_2\ v_3\ v_4\ v_5\ v_6) = (s_8\ s_1\ s_9\ s_2\ s_{10}\ s_3) = (1\ \ 1\ \ 1\ \ 1\ \ 1\ \ 0)$$

и обработать его в соответствии с (1.28), то получим

$$\tilde{C} = \varepsilon^{-1}(\alpha_1 + \alpha_3 + \alpha_4 + \alpha_5) = \varepsilon^{-1}(\varepsilon^4 + \varepsilon^3 + \varepsilon^2 + 1 + \varepsilon^9) = \varepsilon;$$
$$\tilde{D} = \mu^{-1}(\beta_1 + \beta_3 + \beta_4 + \beta_5) = \mu^{-1}(\mu^2 + \mu + 1 + 1) = \mu.$$

Возведя полученные элементы в степень $q = 8$, получим:

$$C = (\tilde{C})^8 = \varepsilon^8\ [\text{mod}\ f_i(x)]; \qquad D = (\tilde{D})^8 = \mu^2\ [\text{mod}\ f_j(x)].$$

Таким образом, для декодирования комбинации кода БЧХЭ (15, 6), т. е. для нахождения начальных информационных элементов C и D, мы можем воспользоваться обработкой как рекуррентной последовательности $\{s\}$, так и последовательностей $\{v\}_q$, полученных из $\{s\}$ путем децимаций с индексами $q = 2^i, i = 0,1,...,(k-1)$.

Рассмотрим теперь процедуру мажоритарного декодирования кода БЧХЭ как рекуррентных последовательностей с учетом децимаций.

Пример 1.5. Пусть имеется код БЧХЭ (15, 6) с характеристическим многочленом $P(x)$, соответствующим примеру 1.2. Комбинации такого кода, как рекурсивные последовательности, удовлетворяют рекуррентному выражению $s_i = s_{i-1} + s_{i-2} + s_{i-3} + s_{i-6} \pmod 2$ и имеют $d_{\min} = 6$. Таким образом, этот код будет исправлять гарантированно все однократные и двукратные ошибки ($\sigma_u \le 2$), т. е. $t = 2$.

Пусть принятая комбинация $\{h\}$ с двумя ошибками имеет следующий вид:

$$\{h\} = (h_0\ h_1\ h_2\ h_3\ \ h_4\ \ h_5\ \ h_6\ \ h_7\ h_8\ h_9\ h_{10}\ h_{11}\ h_{12} h_{13} h_{14})$$
$$1\quad 0\quad 1\quad 0\quad 1\quad 0\quad 0\quad 0\quad 1\quad 0\quad 1\quad 1\quad 1\quad 1\quad 0$$

Рассматриваемый алгоритм декодирования, как было показано ранее, не находит ошибочные позиции и значения ошибок, тем не менее укажем, что ошибки введены на второй и десятой позициях, т. е. $h_1 = \bar{s}_1$ и $h_9 = \bar{s}_9$.

Напомним, что коэффициенты α_i и β_i, $i = 1,2,\ldots,6$, найденные для данного характеристического многочлена $P(x)$, будут: $\alpha_1 = \varepsilon^4; \alpha_2 = \varepsilon^3;\ \alpha_3 = \varepsilon^2;$ $\alpha_4 = 1; \alpha_5 = \varepsilon^9; \alpha_6 = \varepsilon^5$ для сомножителя $GF(2^2)$, образующего поле $GF(2^4)$ с первообразным элементом ε – корнем $f_1(x)$, и $\beta_1 = \mu^2; \beta_2 = \mu;\ \beta_3 = 1;$ $\beta_4 = 0; \beta_5 = \mu^2; \beta_6 = 1$ для сомножителя $f_2(x) = 1 + x + x^2$, образующего подполе $GF(2^2)$ с примитивным для данного подполя элементом μ – корнем $f_2(x)$. В составе расширенного поля $GF(2^4)$ этот элемент будет $\mu = \varepsilon^5$.

Выделяя участки длиной $m = 6$ в замкнутой в кольцо последовательности $\{h\}$ и в децимированных последовательностях $\{v\}_q$ с индексами децимаций 2, 4 и 8 и обработав их в соответствии с (1.10), (1.11), (1.12), (1.13), (1.27), (1.28) и (1.29), получим значения коэффициентов C и D. Эти коэффициенты определяют, соответственно, начальные фазы M-последовательностей с периодом 15, генерируемой многочленом $f_1(x)$, и с периодом 3, генерируемой многочленом $f_2(x)$. Значения пар этих коэффициентов, полученных при обработке последовательностей $\{h\}$ и $\{v\}_q$, представлены в табл. 1.3.

Из табл. 1.3 следует, что, после обработки принятой последовательности $\{h\}$ с двумя ошибками и еще хотя бы одной, полученной из нее, последовательности $\{v\}_q$, $q = 2^i, i = 0,1,2,3$, наибольшее количество значений имеет пара коэффициентов $C = \varepsilon^8$ и $D = \mu^2$. Следовательно, путем мажоритарного декодирования кода БЧХЭ (15, 6) будут определены следующие

переданные информационные элементы: (1 0 1 0 1 1). Первые четыре разряда (1 0 1 0) представляют собой исходный элемент $C=\varepsilon^8$ поля $GF(2^4)$ с образующим многочленом $GF(2^2)$, а последние два разряда (1 1) − исходный элемент $D=\mu^2$ подполя $GF(2^2)$ с образующим многочленом $f_2(x)=1+x+x^2$.

Таблица 1.3

$C_i \in GF(2^4)$	$D_i \in GF(2^2)$	Обрабатываемые последовательности каждая в отдельности			
		$\{h\}$	$\{v\}_2$	$\{v\}_4$	$\{v\}_8$
ε^{13}	1	2			
ε^8	μ^2	3	5	7	8
ε^{10}	0	1			
ε^5	μ	1	1		4
ε^{12}	μ^2	1			
ε^7	0	1			
ε	0	2			2
ε^{12}	1	1		1	
ε^9	0	1			
1	μ^2	1			
ε^5	1	1			
ε^5	0		1		
ε^4	μ^2		1		
ε^{11}	μ		1		
0	0		1		
ε^9	μ^2		2		
ε^6	1		3	1	
ε^{14}	0			3	
ε^{12}	μ			1	
ε^{11}	0			2	
0	1				1

Наибольшее накопленное значение (число 23) после обработки всех четырех последовательностей также будет иметь пара элементов $C=\varepsilon^8$ и $D=\mu^2$, что обеспечивает более высокую гарантию правильного декодирования.

Рассмотрим еще один пример того же кода (15, 6) $d_{\min} = 6$ в случае декодирования принятой последовательности $\{h\}$ с трехкратной ошибкой.

Пример 1.6. Пусть была передана рекуррентная комбинация $\{s\}$ кода БЧХЭ (15, 6) соответствующая примеру 1.5. Такой последовательности, как было показано, соответствуют начальные элементы $C = \varepsilon^8 \left[\bmod f_1(x) = 1 + x + x^4 \right]$ и $D = \mu^2 \left[\bmod f_2(x) = 1 + x + x^2 \right]$. Допустим, что в принятой комбинации содержатся три ошибки в первой (h_1), второй (h_2) и девятой (h_9) позициях кода, т. е. принятая комбинация имеет следующий вид:

$$\{h\} = (h_0\ h_1\ h_2\ h_3\ h_4\ h_5\ h_6\ h_7\ h_8\ h_9\ h_{10}\ h_{11}\ h_{12} h_{13} h_{14}) =$$
$$= (1\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 1\ \ 1\ \ 1\ \ 1\ \ 0)$$

Результаты обработки последовательности $\{h\}$ ($q = 1$) и последовательностей $\{v\}_q$, подвергнутых децимациям с индексами 2, 4 и 8, приведены в табл. 1.4.

Таблица 1.4

Выделенные элементы		Количество пар элементов *C* и *D* после обработки последовательности с индексом *q*				Накопленные значения *C* и *D* после обработки последовательностей			
C	*D*	$\{h\}$ $q = 1$	$q = 2$	$q = 4$	$q = 8$	$\{h\}$	$\{h\}$ и $\{v\}_{q=2}$	$\{h\}$, $\{v\}_{q=2}$ и $\{v\}_{q=4}$	$\{h\}, \{v\}_{q=2}$ $\{v\}_{q=4}$ и $\{v\}_{q=8}$
ε^8	μ^2	2	1	5	7	2	3	8	15
ε^{14}	0	2	3	6	2	2	5	11	13
ε	0	3	1	–	–	3	4	4	4
ε^{12}	1	4	–	1	–	4	4	5	5
1	μ	1	–	–	1	1	1	1	2
ε^{10}	0	1	–	–	–	1	1	1	1
ε^5	μ	1	1	–	2	1	2	2	4
ε^{12}	μ^2	1	–	–	–	1	1	1	1
ε^9	μ^2	–	2	–	–	0	2	2	2
ε^5	μ^2	–	2	–	–	0	2	2	2
ε^4	μ^2	–	1	–	1	0	1	1	2
ε^6	μ	–	1	2	–	0	1	3	3
ε^{13}	μ	–	1	–	–	0	1	1	1
ε^6	1	–	1	–	–	0	1	1	1
0	0	–	1	–	–	0	1	1	1
ε^{10}	1	–	–	1	–	0	0	1	1
ε^{11}	1	–	–	–	1	0	0	0	1
ε^2	0	–	–	–	1	0	0	0	1

Из табл. 1.4 видно, что в результате мажоритарного декодирования принятой последовательности $\{h\}$ по наибольшему накопленному значению в результате обработки будет выделена пара коэффициентов: $C = \varepsilon^{12}$ и $D = 1$. После обработки последовательностей $\{h\}$ и $\{v\}_q$ с индексом децимации $q = 2$, а также трех последовательностей $\{h\}$ и $\{v\}_q$ с индексами децимации $q = 2$ и $q = 4$ будут декодированы элементы $C = \varepsilon^{14}$ и $D = 0$. То есть во всех этих случаях будет ошибочное декодирование. Но после обработки последовательности $\{h\}$ и всех трех последовательностей $\{v\}_q$ с индексами децимаций $q = 2$, 4 и 8 будет правильное декодирование, так как наибольшее накопленное значение будет иметь пара коэффициентов $C = \varepsilon^{8}$ и $D = \mu^{2}$, т. е. истинные значения начальных элементов.

Отсюда следует важный и новый вывод, состоящий в том, что код БЧХЭ (15, 6) с $d_{\min} = 6$ позволяет, в результате мажоритарного декодирования с применением децимаций, исправлять определенную долю ошибок кратностью выше, чем $\frac{d_{\min} - 1}{2}$.

Результаты моделирования работы декодера для кода БЧХЭ (15, 6) и с $d_{\min} = 6$, проведенного на компьютере, представлены на рис. 1.2, 1.3 и 1.4, где образующий полином $P(x) = (x^4 + x + 1)(x^2 + x + 1)$.

На рис. 1.2 и 1.3 темным цветом выделены столбцы, соответствующие истинным значениям начальных элементов C и D поля $GF(2^4)$, которые образовали комбинацию $f(x)$. Так, на рис. 1.2 показаны диаграммы декодирования комбинации $h(x) = f(x) + e(x)$, где вектор разрешенной кодовой комбинации $f(x)$ и вектор однократной ошибки $e(x)$, соответственно, имеют вид: $f(x) \rightarrow (100100000110011)$, $e(x) \rightarrow (000001000000000)$. Во всех четырех диаграммах декодирование произведено правильно, а именно, выделена по большинству «голосов» пара элементов $C = \varepsilon$ и $D = \mu^{2}$. Из диаграмм видно, что однократная ошибка при (15, 6) с $d_{\min} = 6$ может быть успешно исправлена и без использования децимаций.

Аналогично, на рис 1.3 показаны результаты декодирования комбинации с тремя ошибками. Вектор разрешенной кодовой комбинации $f(x)$ и вектор трехкратной ошибки $e(x)$, соответственно, имеют вид: $f(x) \rightarrow (101000111111011)$, $e(x) \rightarrow (010011000000000)$. Здесь также по большинству «голосов» выделена истинная пара начальных элементов $C = \varepsilon^{10}$ и $D = \mu$. Однако выделение не такое надежное, как при однократных ошибках. Не все трехкратные ошибки могут быть исправлены. На рис 1.4 показана доля исправляемых ошибок при декодировании комбинаций кода БЧХЭ (15, 6) как без учета децимаций, так и при их учете. Так, доля исправляемых трехкратных ошибок без учета децимаций составляет около 23 %, а при декодировании с учетом всех децимаций – около 63 %.

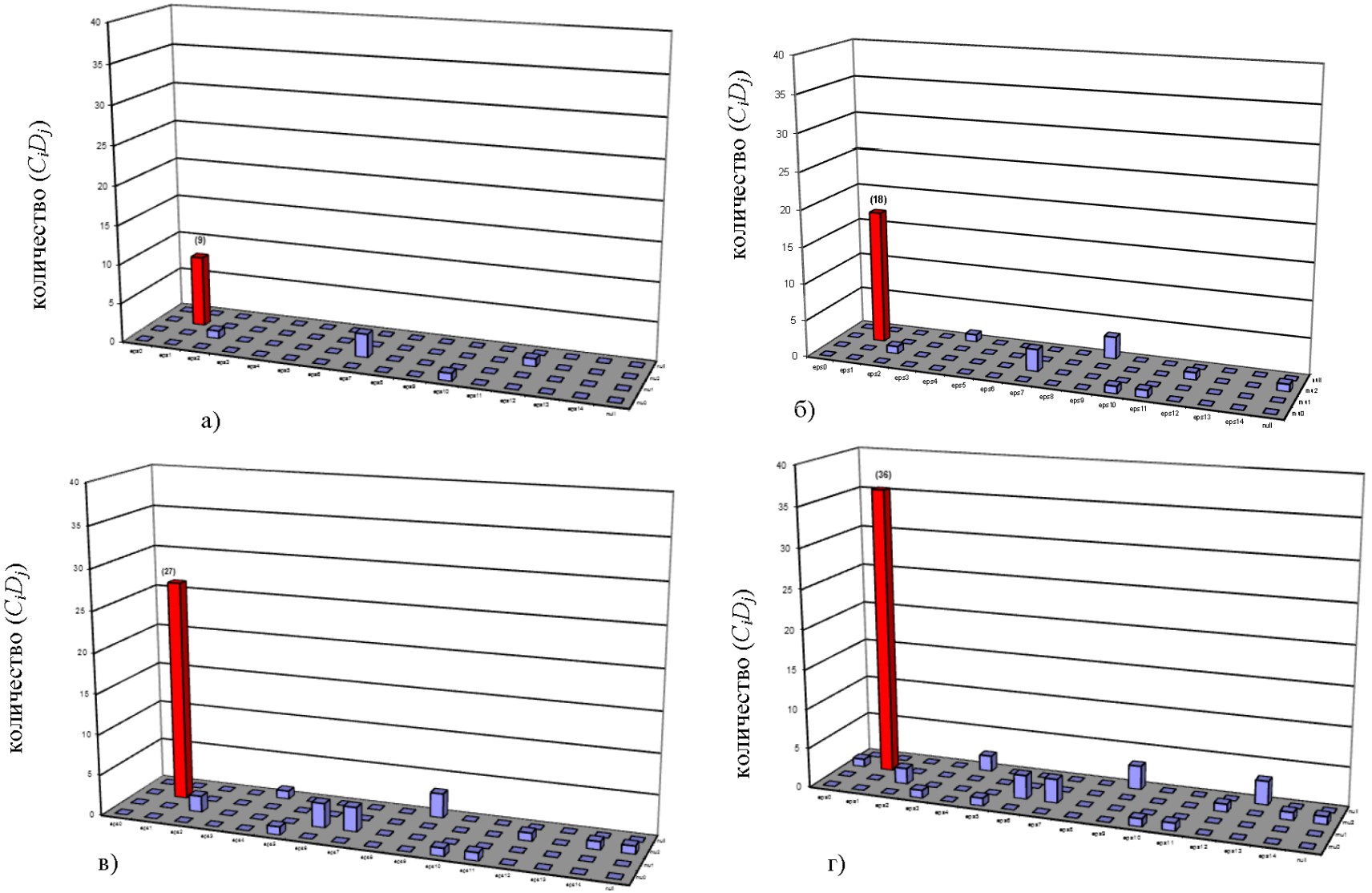

Рис. 1.2. Декодирование комбинации с однократной ошибкой кода БЧХЭ (15, 6):
а) без децимаций; б) с одной децимацией; в) с двумя децимациями; г) с тремя децимациями

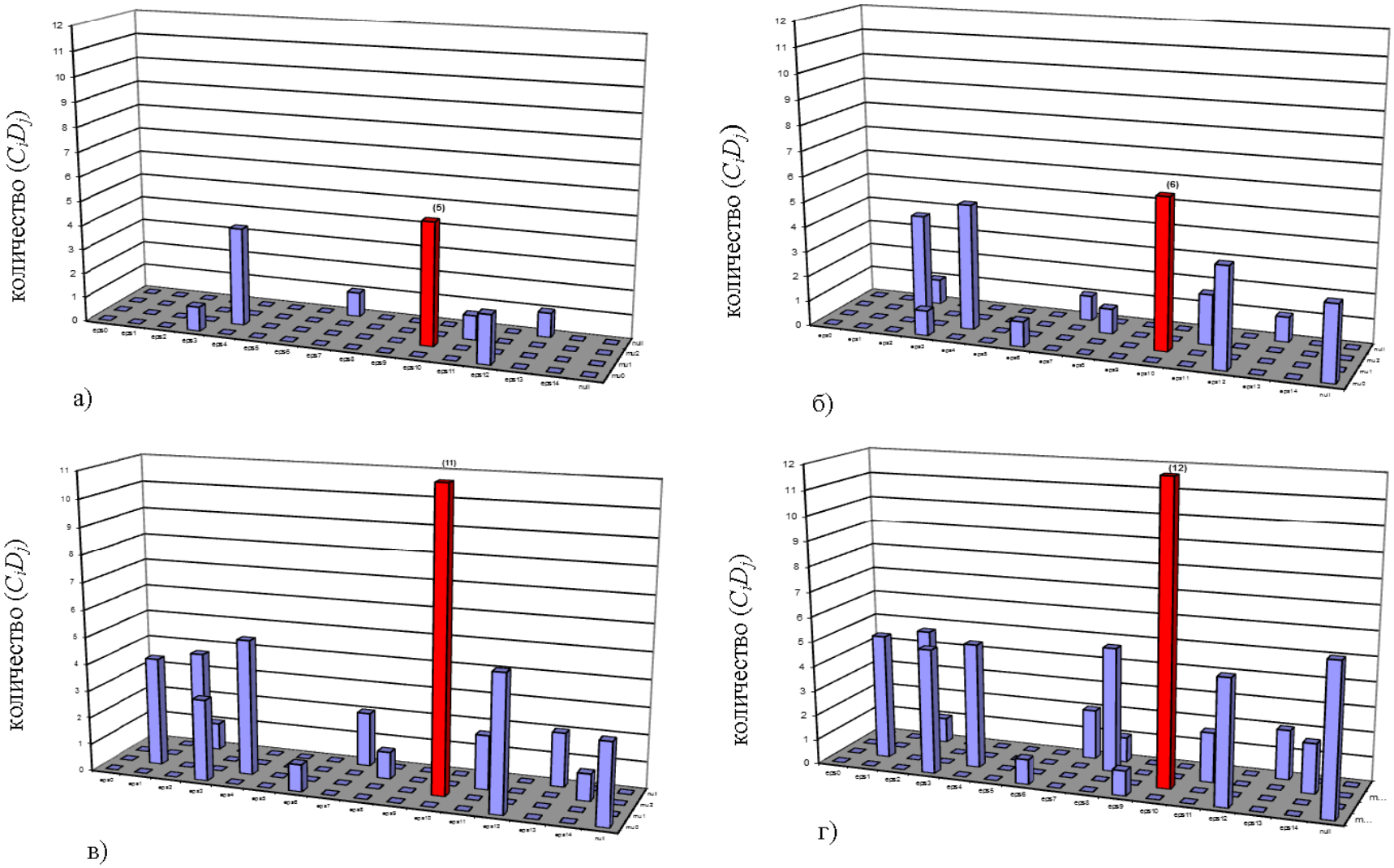

Рис. 1.3. Декодирование комбинации с трехкратной ошибкой кода БЧХЭ (15, 6):
а) без децимаций; б) с одной децимацией; в) с двумя децимациями; г) с тремя децимациями

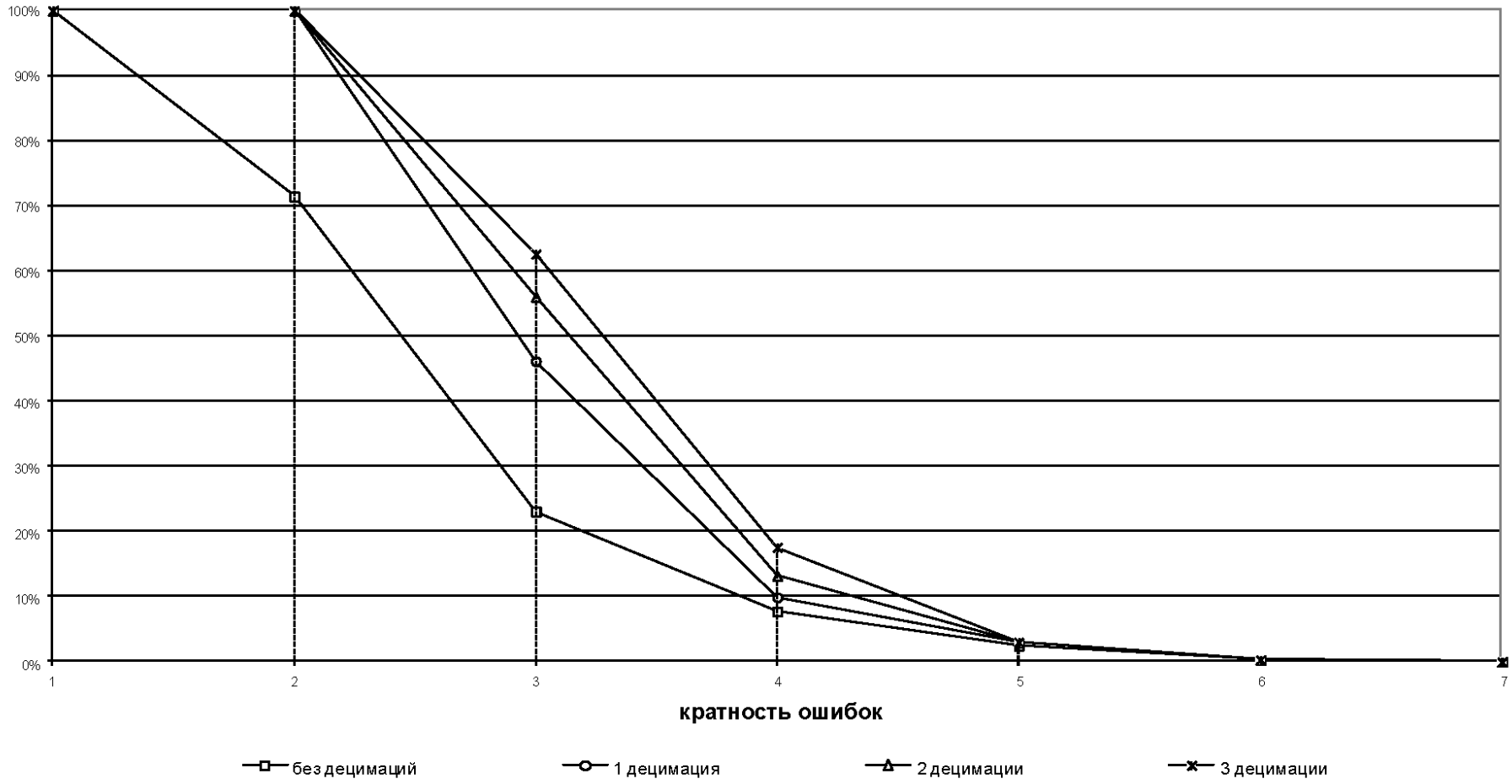

Рис. 1.4. Увеличение доли исправляемых ошибок кодом БЧХЭ (15, 6):
с учетом различного числа децимаций

1.4. Принципы реализации кодирующих и декодирующих устройств кодов БЧХЭ как рекуррентных последовательностей

Построение кодирующих (КУ) и декодирующих (ДКУ) устройств кодов БЧХЭ как рекуррентных последовательностей существенно отличается от классических алгебраических кодеров и декодеров циклических кодов БЧХ, причем в сторону их упрощения. Рассмотрим принципы построения кодирующих и декодирующих устройств кода БЧХЭ как рекуррентных последовательностей с использованием при декодировании двойственного базиса [3].

1.4.1. *Принципы построения кодирующих устройств*

Кодирующее устройство кода БЧХЭ как рекуррентных последовательностей может быть легко реализовано с помощью регистра сдвига с сумматорами, обратные связи в котором определяются рекуррентным уравнением (1.4), задаваемом разложимым характеристическим многочленом $P(x)$ вида (1.3).

Так, для рассматриваемого в примере 1.2 кода БЧХЭ (15, 6) с разложимым характеристическим многочленом (1.6) соответствующее рекуррентное уравнение имеет вид (1.7). Регистр сдвига, построенный по рекуррентному уравнению (1.7), представлен на рис. 1.5.

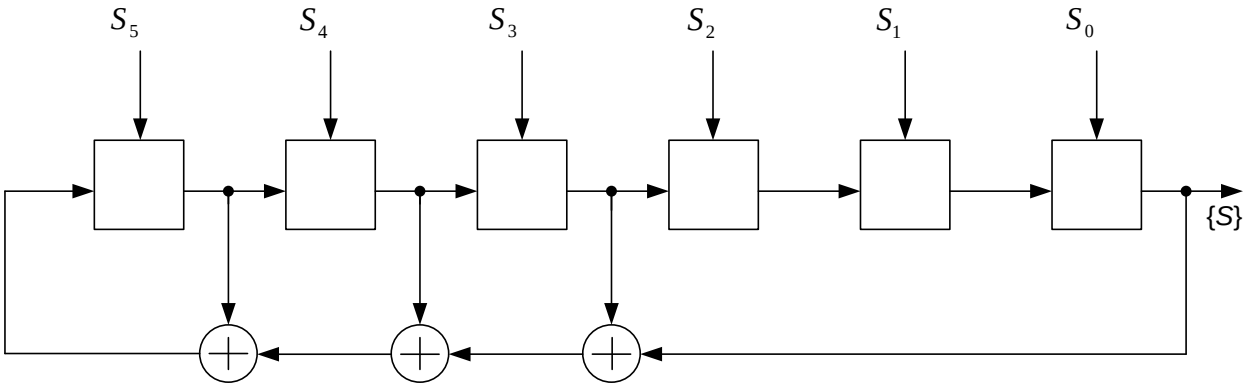

Рис. 1.5. Регистр сдвига с вынесенными сумматорами,
обеспечивающий кодирование для кода БЧХЭ (15, 6)
с характеристическим многочленом $P(x) = x^6 + x^5 + x^4 + x^3 + 1$

Алгоритм кодирования является простым и заключается в следующем: исходные информационные элементы кода ($s_0 s_1 s_2 s_3 s_4 s_5$) записываются параллельно в ячейки регистра, затем включается генератор тактовых импульсов, в течение 15 тактовых интервалов на выходе регистра (с крайней правой ячейки) будет считана кодовая последовательность $\{s\}$, удовлетворяющая рекуррентному соотношению (1.7).

Как следует из структуры комбинации, рассмотренный выше алгоритм кодирования соответствуют систематическому циклическому коду.

Вместе с тем, возможен другой алгоритм кодирования. Действительно, если проанализировать выражение (1.17), то становится понятной идея такого кодирования. Так, для рассматриваемого в примере 1.2 кода БЧХЭ (15, 6) с характеристическим многочленом $P(x) = P_1(x) \cdot P_2(x) = (x^4 + x + 1)(x^2 + x + 1)$, рекуррентная последовательность $\{s\}$, удовлетворяющая рекуррентному уравнению (1.7), может быть сформирована на выходе кодирующего устройства как сумма по модулю 2 двух последовательностей. Одна из них является M_1-последовательностью длиной 15, порождаемой примитивным многочленом $P_1(x) = x^4 + x + 1$, а другая – периодической M_2-последовательностью с периодом 3, порождаемой примитивным многочленом $P_2(x) = x^2 + x + 1$. Как было показано ранее, многочлены $P_1(x)$ и $P_2(x)$ входят в разложение двучлена $(x^{15} + 1)$. Корнями этих многочленов являются элементы поля $GF(2^4)$: $\varepsilon, \varepsilon^2, \varepsilon^4, \varepsilon^8$ – для многочлена $P_1(x)$ и ε^5 и ε^{10} – для многочлена $P_2(x)$. Порядок корней многочлена $P_2(x)$ равен 3, и они образуют вместе с 0 и 1 подполе $GF(2^2)$ в составе поля $GF(2^4)$, построенного по многочлену $P_1(x)$. Отсюда, с учетом (1.17), кодирующее устройство может быть построено на базе двух модулярных регистров, работающих синхронно. Один из модулярных регистров, построенный на базе многочлена $P_1(x)$, формирует M_1-последовательность с элементами в виде функции-след $T(\varepsilon^i)$, где ε – корень многочлена $P_1(x)$. Второй модулярный регистр построен на базе многочлена $P_2(x)$. На выходе этого регистра формируется M_2-последовательность с периодом 3 с элементами в виде функции-след $T(\mu^i)$, где μ – корень многочлена $P_2(x)$. Напомним, что если корень μ рассматривать в составе поля $GF(2^4)$, то $\mu = \varepsilon^5$.

Пусть элемент поля $\varepsilon^i \in GF(2^4)$ имеет общий вид, выраженный через базисные элементы $1, \varepsilon, \varepsilon^2, \varepsilon^3$ как $\varepsilon^i = a_0 + a_1\varepsilon + a_2\varepsilon^2 + a_1\varepsilon^3, \quad a_i \in GF(2)$. Тогда функция-след этого элемента в общем виде будет равна

$$T(\varepsilon^i) = a_0 T(1) + (a_1 + a_2) T(\varepsilon) + a_3 T(\varepsilon^3).$$

Приведя функции-след $T(1)$, $T(\varepsilon)$ и $T(\varepsilon^3)$ по модулю 2 и модулю $P_1(\varepsilon) = \varepsilon^4 + \varepsilon + 1 \equiv 0$, получим, что $T(\varepsilon^i) = a_3$.

Аналогично, функция-след элемента $\mu^i = b_0 + b_1\mu$, принадлежащего полю $GF(2^2)$, будет равна $T(\mu^i) = b_0 T(1) + b_1 T(\mu)$.

Учитывая, что $P_2(\mu) = \mu^2 + \mu + 1 \equiv 0$, получим, что $T(\mu^i) = b_1$.

Таким образом, кодирующее устройство может быть реализовано с помощью двух модулярных регистров, включенных по схеме, показанной на рис. 1.6.

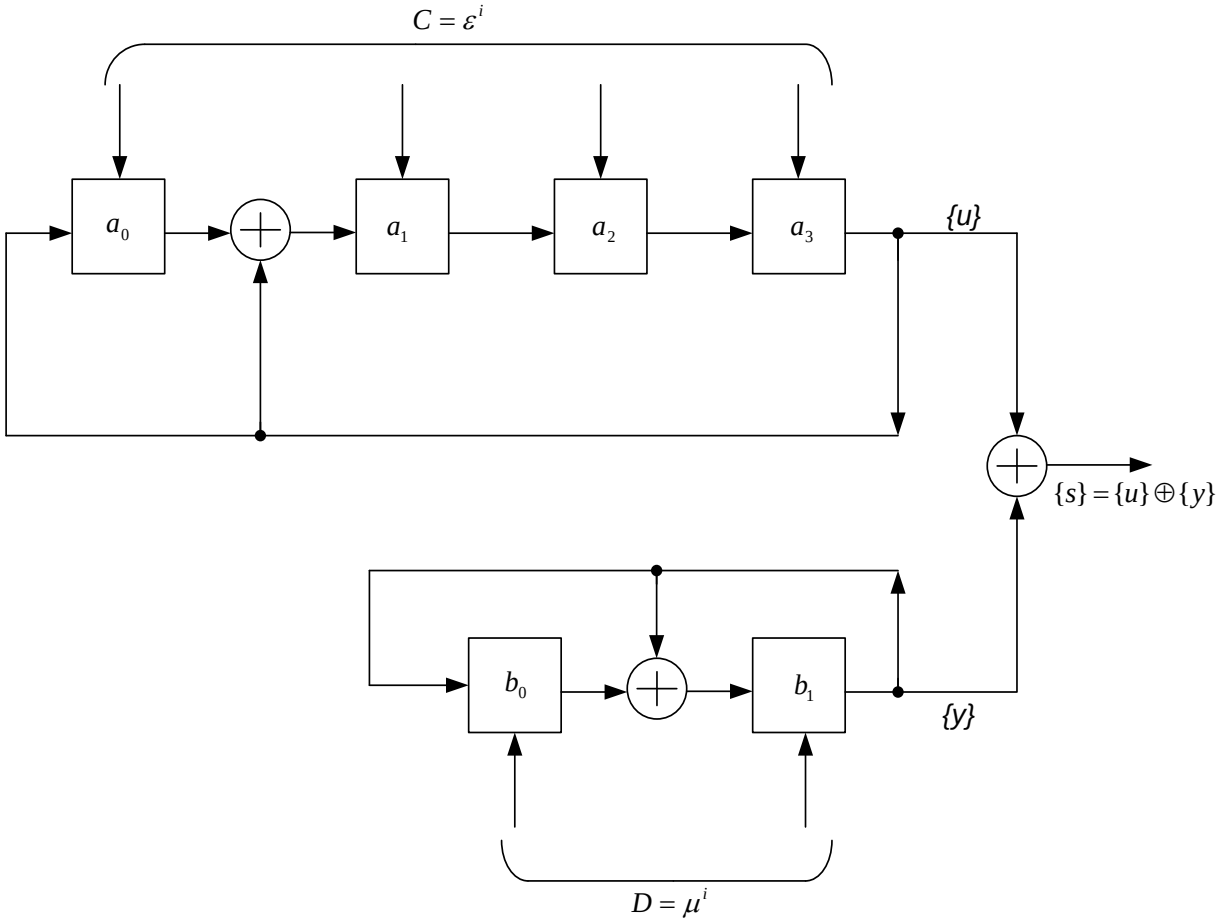

Рис. 1.6. Кодирующее устройство кода БЧХЭ (15, 6)
на базе автономных модулярных регистров

Алгоритм работы кодирующего устройства следующий. Шестиразрядная двоичная кодовая комбинация исходных информационных элементов записывается параллельно в ячейки верхнего регистра в виде элементов $(a_0 a_1 a_2 a_3)$ и в ячейки нижнего регистра в виде элементов $(b_0 b_1)$. В полиномиальном виде вектор $(a_0 a_1 a_2 a_3)$ представляется элементом поля $GF(2^4)$ $C = \varepsilon^i = a_0 + a_1\varepsilon + a_2\varepsilon^2 + a_3\varepsilon^3$, а вектор $(b_0 b_1)$ – в виде элемента поля $GF(2^2)$ $D = b_0 + b_1\mu$.

После записи в ячейки регистров информационных элементов включается генератор сдвигающих тактовых импульсов, который вырабатывает для кода (15, 6) ровно 15 тактов. Таким образом, на выходе верхнего регистра будет сформирована последовательность

$$\{u\} = \{T(\varepsilon^i)T(\varepsilon^{i+1})\ldots T(\varepsilon^{i+14})\} = \{\,T(C)T(C\varepsilon)\ldots T(C\varepsilon^{14})\}\,,$$

а на выходе нижнего модулярного регистра последовательность

$$\{y\} = \left\{T\left(\mu^i\right))T\left(\mu^{i+1}\right)\ldots T\left(\mu^{i+14}\right)\right\} = \left\{\,T(D)T(D\mu)\ldots T\left(D\mu^{14}\right)\right\}.$$

Обе последовательности поэлементно складываются в выходном сумматоре по модулю 2 и образуют требуемую кодовую последовательность $\{s\}$ кода БЧХЭ (15, 6), удовлетворяющую рекуррентному уравнению (1.7).

Так, последовательности $\{s\}$ из примера 1.2

$$\{s\} = (0\quad 1\quad 1\quad 1\quad 1\quad 1\quad 1\quad 0\quad 1\quad 1\quad 1\quad 0\quad 1\quad 0\quad 0)$$

соответствуют исходные коэффициенты $C = 1$ и $D = 1$. Учитывая, что элемент C принадлежит полю $GF(2^4)$ с образующим многочленом $P_1(x)$, а D принадлежит полю $GF(2^2)$ с образующим многочленом $P_2(x)$, можно сделать вывод, что последовательность $\{s\}$ есть поэлементная сумма по mod 2 двух канонических последовательностей $\{u\}$ и $\{y\}$ следующего вида:

$$\{u\} = \left\{T(1)T(\varepsilon)T\left(\varepsilon^2\right)\ldots T\left(\varepsilon^{14}\right)\right\} = \left(0\quad 0\quad 0\quad 1\quad 0\quad 0\quad 1\quad 1\quad 0\quad 1\quad 0\quad 1\quad 1\quad 1\quad 1\right)$$

$$+$$

$$\{y\} = \left\{T(1)T(\mu)T\left(\mu^2\right)T(1)\ldots T\left(\mu^2\right)\right\} = \left(0\quad 1\quad 1\quad 0\quad 1\quad 1\quad 0\quad 1\quad 1\quad 0\quad 1\quad 1\quad 0\quad 1\quad 1\right)$$

$$\{s\} = \left\{\left[T\left(\varepsilon^0\right)\oplus T\left(\mu^0\right)\right],\ldots[T(\varepsilon^{14})\oplus T(\mu^2)]\right\} = \left(0\quad 1\quad 1\quad 1\quad 1\quad 1\quad 1\quad 0\quad 1\quad 1\quad 1\quad 0\quad 1\quad 0\quad 0\right)$$

Итак, мы рассмотрели другой вариант построения, в данном случае, несистематического циклического кода БЧХЭ (15, 6) с $d_{\min} = 6$, комбинации которого удовлетворяют рекуррентному уравнению (1.7).

Пример 1.7. Рассмотрим еще один пример построения двоичного кода БЧХЭ (15, 7) с более сложным разложимым характеристическим многочленом

$$P(x) = f_0(x)\, f_1(x)\, f_5(x) = (x+1)\left(x^4 + x + 1\right)\left(x^2 + x + 1\right) = x^7 + x^3 + x + 1 \,(\mathrm{mod}\, 2).$$

Рассмотрим одну из 2^7 таких последовательностей, например

$$\{s\} = \left(s_0\ s_1\ s_2\ s_3\ s_4\ s_5\ s_6\ s_7\ s_8\ s_9\ s_{10} s_{11} s_{12} s_{13} s_{14}\right) =$$
$$= \left(1\quad 1\quad 1\quad 1\quad 0\quad 0\quad 1\quad 1\quad 0\quad 0\quad 0\quad 1\quad 1\quad 0\quad 1\right)$$

Пусть кодирующее устройство будет построено по рассмотренному выше модулярному принципу, т. е. с помощью трех модулярных регистров.

Исходными информационными элементами, образовавшими кодовую последовательность $\{s\}$, будут $((a_0a_1a_2a_3)(b_0b_1)e_0) = ((0\quad 0\quad 1\quad 1)(0\quad 1)1)$, где

$$C = a_0 + a_1\varepsilon + a_2\varepsilon^2 + a_3\varepsilon^3 = \varepsilon^2 + \varepsilon^3 = \varepsilon^6 \quad \in GF(2^4),$$
$$D = b_0 + b_1\mu = \mu \quad \in GF(2^2),$$
$$E = e_0 = 1 \quad \in GF(2).$$

Покажем, что последовательность $\{s\}$ будет равна сумме по модулю 2 последовательностей $\{u\}$, $\{y\}$ и $\{z\}$, сформированных тремя модулярными регистрами, включенными в соответствии с многочленами $P_1(x)$, $P_2(x)$ и $P_3(x)$ по рис. 1.7.

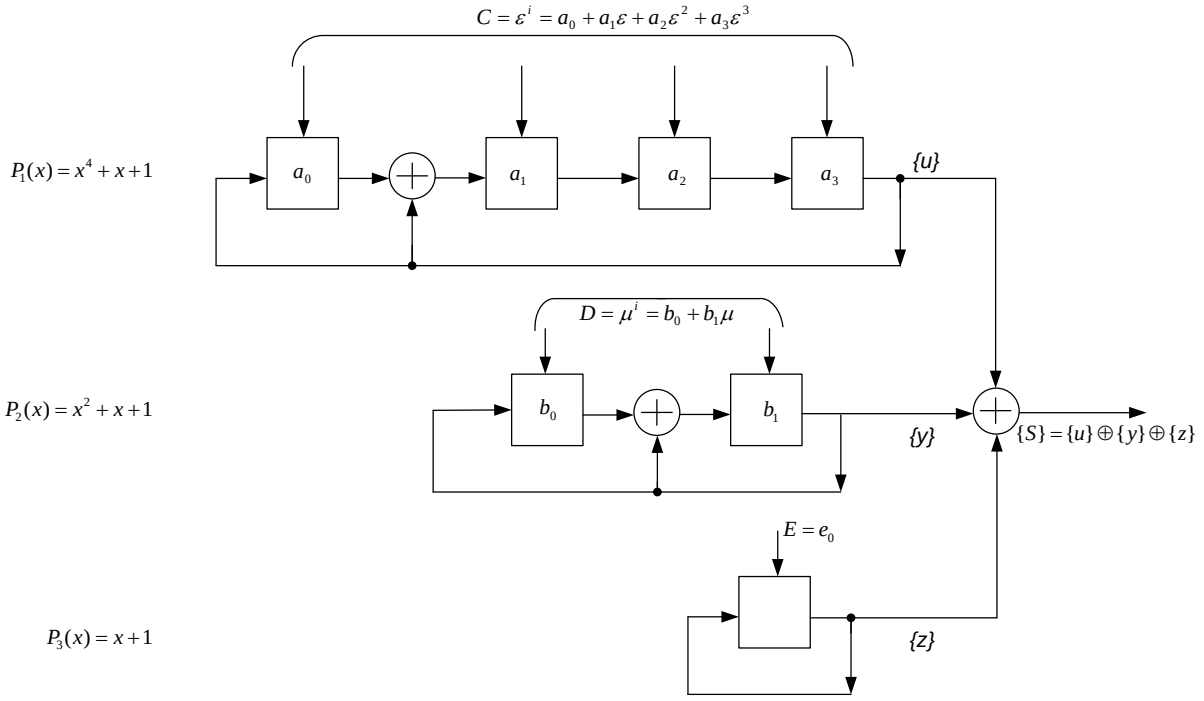

Рис. 1.7. Кодирующее устройство кода БЧХЭ (15, 7)
с характеристическим многочленом $P(x) = x^7 + x^3 + x + 1 = (x^4 + x + 1)(x^2 + x + 1)(x + 1)$

Для начальных значений ячеек регистров $C = \varepsilon^6$, $D = \mu$ и $E = 1$ получим:

$$\{u\} = \{T(C)T(C\varepsilon)\ldots T(\varepsilon^{14})\} = (1\quad 1\quad 0\quad 1\quad 0\quad 1\quad 1\quad 1\quad 1\quad 0\quad 0\quad 0\quad 1\quad 0\quad 0)$$
$$\{y\} = \{T(\mu)T(\mu^2)1\ldots T(\mu^2)\} = (1\quad 1\quad 0\quad 1\quad 1\quad 0\quad 1\quad 1\quad 0\quad 1\quad 1\quad 0\quad 1\quad 1\quad 0)$$
$$\{z\} = \{T(1)T(1)\ldots T(1)\} = (1\quad 1\quad 1\quad 1\quad 1\quad 1\quad 1\quad 1\quad 1\quad 1\quad 1\quad 1\quad 1\quad 1\quad 1)$$
$$\{s\} = (1\quad 1\quad 1\quad 1\quad 0\quad 0\quad 1\quad 1\quad 0\quad 0\quad 0\quad 1\quad 1\quad 0\quad 1)$$

т. е. на выходе кодирующего устройства имеет место выбранная ранее кодовая последовательность.

1.4.2. *Принципы построения декодирующих устройств кода БЧХЭ с разложимым характеристическим многочленом*

Вариант кодирования для кода БЧХЭ с модулярными регистрами позволяет наиболее просто реализовать декодирующее устройство с мажоритарной обработкой принимаемой последовательности. Упрощение реализации достигается тем, что в результате декодирования будут выделены, в качестве информационных элементов, исходные элементы поля *C*, *D*, …, определяющие фазу рекуррентной последовательности. Это, с одной стороны, упрощает процедуру декодирования, а с другой – сокращает время декодирования.

Обобщенная блок-схема декодирующего устройства представлена на рис. 1.8.

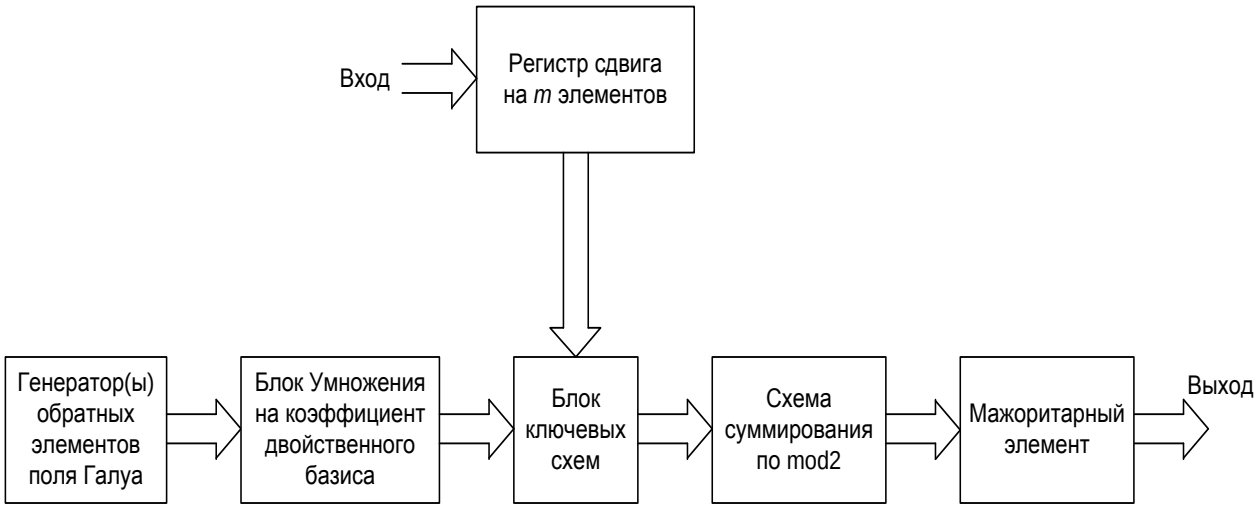

Рис. 1.8. Обобщенная блок-схема декодирующего устройства кода БЧХЭ как рекуррентных последовательностей

Более детальная функциональная схема декодера для рассматриваемого в примере 1.2 кода БЧХЭ (n, m) = (15, 6) с характеристическим многочленом $P(x) = (x^4 + x + 1)(x^2 + x + 1)$ представлена на рис. 1.9.

Декодирование производится с каждым тактом при поступлении нового элемента на вход регистра по m-элементным (m = 6) участкам принимаемой последовательности, находящимся в данный момент в регистре.

Работа декодера происходит следующим образом.

Поступающая на вход из канала последовательность $\{h\}$ проходит через регистр на m = 6 ячеек. Как только первый принятый элемент h_0 достигнет последней правой ячейки регистра, в генераторы обратных элементов поля (ГОЭ) устанавливается единица. Далее, с каждым тактом состояние

верхнего ГОЭ поля $GF(2^4)$ умножается на элемент поля ε^{-1}, а состояние нижнего ГОЭ поля $GF(2^2)$ – на элемент поля μ^{-1}. При этом элемент ε^{-i} поля $GF(2^4)$ с выхода верхнего ГОЭ умножается в блоке умножения (БУ) на коэффициенты α_j, $j=\overline{1,6}$, а элемент μ^{-i} поля $GF(2^2)$ с выхода нижнего ГОЭ умножается на коэффициенты β_j, $j=\overline{1,6}$.

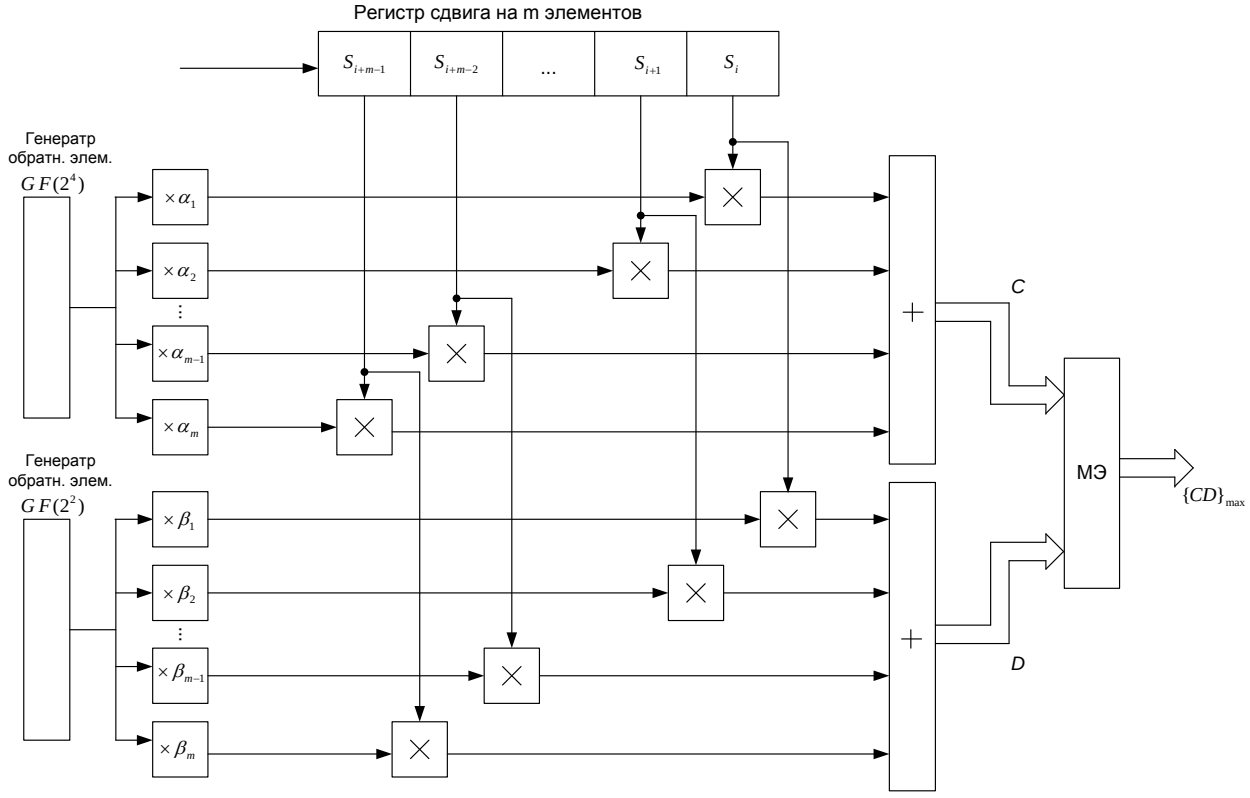

Рис. 1.9. Функциональная схема декодера кода БЧХЭ (*n*, *m*) = (15, 6)

В результате умножения элемента $\varepsilon^{-i}=a_0+a_1\varepsilon+a_2\varepsilon^2+a_3\varepsilon^3\ \alpha_j$, $j=\overline{1,6}$ на коэффициенты α_j, $j=\overline{1,6}$, на выходах умножителей будем иметь следующие вектора:

– после умножения на $\alpha_1=\varepsilon^4:\left(a_0+a_3;\ a_0+a_1+a_3;\ a_1+a_2;\ a_2+a_3\right)$;

– после умножения на $\alpha_2=\varepsilon^3:\left(a_1;\ a_1+a_2;\ a_2+a_3;\ a_0+a_3\right)$;

– после умножения на $\alpha_3=\varepsilon^2:\left(a_2;\ a_1+a_2;\ a_0+a_3;\ a_1\right)$; (1.30)

– после умножения на $\alpha_4=1:\ \ \left(a_0;\ a_1;\ a_2;\ a_3\right)$;

– после умножения на $\alpha_5=\varepsilon^9:\left(a_1+a_3;\ a_0+a_1+a_2+a_3;\ a_1+a_2+a_3;\ a_0+a_2+a_3\right)$;

– после умножения на $\alpha_6=\varepsilon^5:\left(a_2+a_3;\ a_0+a_2;\ a_0+a_1+a_3;\ a_1+a_2\right)$.

Аналогично, в результате умножения элемента $\mu^{-i} = b_0 + b_1\mu$ на коэффициенты β_j, $j = \overline{1,6}$, на выходах умножителей будем иметь следующие вектора:

– после умножения на $\beta_1 = \mu^2 : (b_0 + b_1;\ b_0)$;

– после умножения на $\beta_2 = \mu : (b_1;\ b_0 + b_1)$;

– после умножения на $\beta_3 = 1 : (b_0;\ b_1)$; (1.31)

– после умножения на $\beta_4 = 0 : (0; 0)$;

– после умножения на $\beta_5 = \mu^2 : (b_0 + b_1;\ b_0)$;

– после умножения на $\beta_6 = 1 : (b_0;\ b_1)$.

Полученные векторы через ключевые схемы (КС), которые будут «открыты» или «закрыты» в зависимости от сигнала (1 или 0) на выходе соответствующей ячейки регистра, поэлементно складываются по mod 2 в двух блоках суммирования (БС). На выходе верхнего блока суммирования будут формироваться с каждым тактом вычисленные элементы *C*, а на выходе нижнего БС – элементы *D*. Далее полученные элементы *C* и *D* поступают на мажоритарный элемент (МЭ), который, после обработки всей принятой последовательности $\{h\}$, определит пару элементов *C* и *D*, набравшую максимальное число «голосов». Пусть при декодировании максимальное число «голосов» получили (пример 1.2) элементы:

$$C = 1 = \varepsilon^0 \to (a_0 a_1 a_2 a_3) = (1 \quad 0 \quad 0 \quad 0) \quad \text{и} \quad D = 1 = \mu^0 \to (b_0 b_1) = (1 \quad 0)\ .$$

Тогда исходными информационными элементами, порождающими последовательность $\{s\}$, будут: $(a_0 a_1 a_2 a_3 b_0 b_1) = (1 \quad 0 \quad 0 \quad 0 \quad 1 \quad 0)$.

Аналогичным образом может быть построено декодирующее устройство для каждого из кодов БЧХЭ, характеристические полиномы которых представлены в табл. 1.1.

Так, в примере 1.7 в качестве характеристического многочлена взят многочлен

$$P(x) = f_0(x)\, f_1(x)\, f_5(x) = (x+1)\left(x^4 + x + 1\right)\left(x^2 + x + 1\right) =$$
$$= x^7 + x^3 + x + 1 \left(\mathrm{mod}\, 2\right).$$

В этом случае в составе декодера должны быть генераторы обратных элементов поля $GF(2^4)$, подполя $GF(2^2)$и простого поля $GF(2)$.

В результате декодирования последовательности $\{h\}$ должны быть определены информационные элементы $(a_0 a_1 a_2 a_3 b_0 b_1 e_0)$ как двоичные коэффициенты элементов:

$$C = a_0 + a_1\varepsilon + a_2\varepsilon^2 + a_3\varepsilon^3 \in GF(2^4),$$
$$D = b_0 + b_1\mu \in GF(2^2),$$
$$E = e_0 \in GF(2).$$

Для нахождения элементов C, D и E, порождающих последовательность $\{s\}$, необходимо предварительно вычислить коэффициенты α_i, β_i и $\gamma_i, i = \overline{1,7}$, по формулам (1.8) и (1.9) с подстановкой в нее коэффициентов p_i многочлена $P(x)$ и корней: корня ε многочлена $P_1(x) = f_1(x)$ при вычислении $\alpha_i \in GF(2^4)$; корня $\mu \equiv \varepsilon^5$ многочлена $P_2(x) = f_5(x)$ при вычислении $\beta_i \in GF(2^2)$ и корня $d = \varepsilon^0 = 1$ многочлена $P_3(x) = f_0(x)$ при вычислении $\gamma_i \in GF(2)$.

После соответствующих вычислений получим следующие значения коэффициентов:

$$\begin{array}{lll}
\alpha_1 = 1; & \beta_1 = 1; & \gamma_1 = 1; \\
\alpha_2 = \varepsilon^3; & \beta_2 = \varepsilon^5 = \mu; & \gamma_2 = 0; \\
\alpha_3 = \varepsilon^2; & \beta_3 = 1 = \mu^0; & \gamma_3 = 0; \\
\alpha_4 = \varepsilon^4; & \beta_4 = \varepsilon^5 = \mu; & \gamma_4 = 1; \\
\alpha_5 = \varepsilon^3; & \beta_5 = 1 = \mu^0; & \gamma_5 = 1; \\
\alpha_6 = \varepsilon^3; & \beta_6 = \varepsilon^{10} = \mu^2; & \gamma_6 = 1; \\
\alpha_7 = \varepsilon; & \beta_7 = \varepsilon^5 = \mu; & \gamma_7 = 1.
\end{array} \qquad (1.32)$$

Теперь по m-элементным участкам (m = 7) последовательности $\{h\}$ в декодере будут вычислены элементы C, D и E по формулам (1.12)–(1.15).

При декодировании безошибочной комбинации из примера 1.7 максимальное число «голосов» получили элементы:

$$C = \varepsilon^6 \in GF(2^4);\ D = \varepsilon^5 = \mu \in GF(2^2);\ E = 1 \in GF(2).$$

Таким образом, в результате декодирования последовательности $\{h\}$ будут определены информационные элементы $(a_0 a_1 a_2 a_3 b_0 b_1 e_0) = (0011011)$.

Рассмотрим теперь построение декодера кода БЧХЭ как рекуррентных последовательностей с учетом децимаций над принятой последовательностью $\{h\}$.

Структурная схема реализации декодера рассматриваемого в примере 1.2 кода БЧХЭ (15, 6) представлена на рис. 1.10. Отличие этой схемы от представленной на рис. 1.6 состоит в дополнении блоков возведения вычисляемых элементов C и D в степень, равную индексу децимации $q = 2^i$, i = 0, 1, 2, 3. Кроме того, следует отметить, что в регистре сдвига на m = 6

разрядов должны находиться m-элементные участки децимированных последовательностей $\{V\}_q$. Сам блок формирования децимированных последовательностей $\{V\}_q$ с индексами децимаций $q = 2^i$, $i = 1,\ 2, 3$ на схеме не отображен.

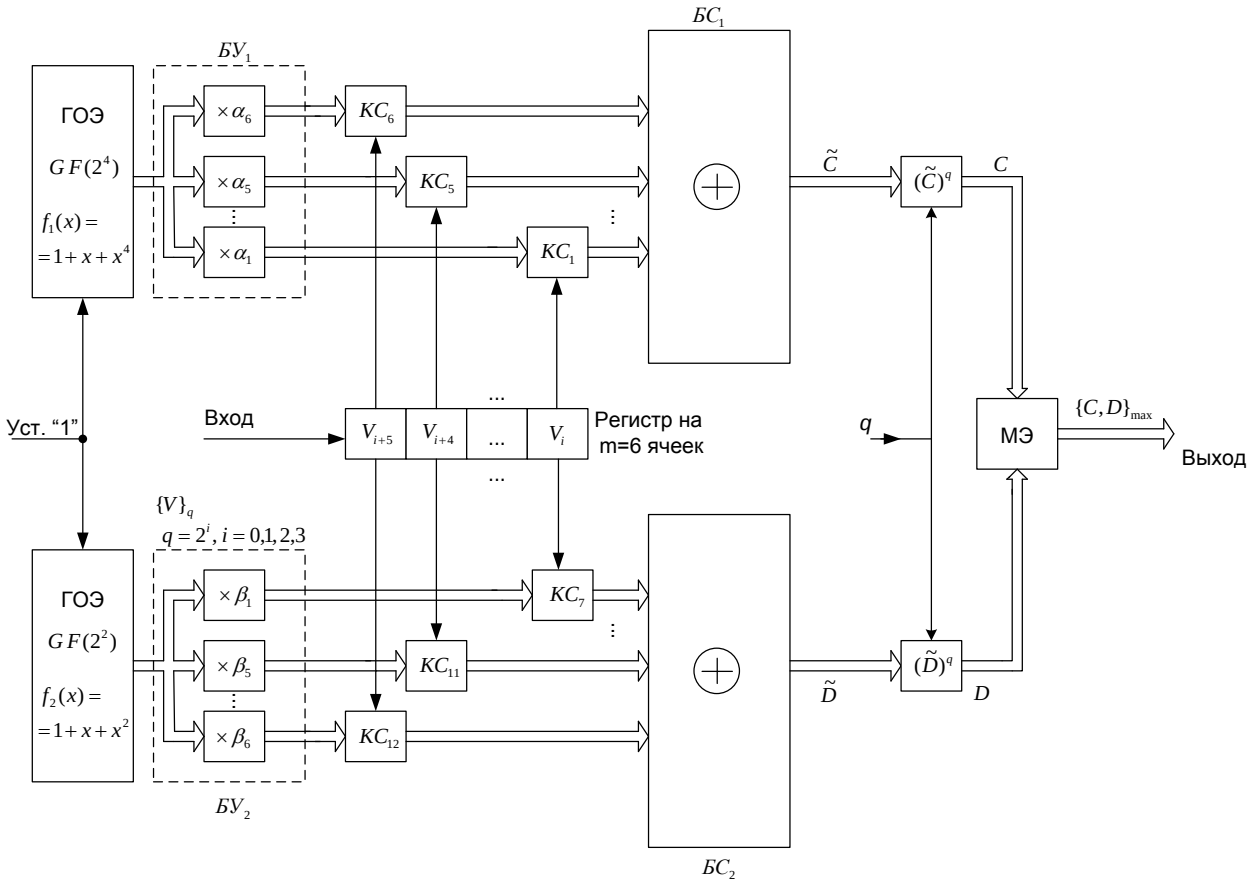

Рис. 1.10. Схема декодирующего устройства кода БЧХЭ (15, 6)
с использованием децимаций

Алгоритм вычисления элементов C и D ничем не отличается от описанного выше для схемы без децимаций (рис. 1.9).

На основании рассмотренных примеров можно сделать общий вывод о том, что реализация декодирующих устройств рекуррентных кодов БЧХЭ с применением двойственного базиса и мажоритарного декодирования (по большинству) является простой как при аппаратной, так и при программной реализации. Так например, в декодере для рассмотренного кода БЧХЭ (15, 6), в соответствии с (1.30) и (1.31), блоки умножения (БУ) легко реализуются с помощью 9 двухвходовых сумматоров по mod 2 для $БУ_1$ и всего лишь одного сумматора по mod 2 для $БУ_2$. Первый блок суммирования $БС_1$ реализуются с помощью 20 двухвходовых сумматоров, а второй $БС_2$ – всего лишь 8 сумматоров по mod 2.

1.5. Дуальные коды Рида – Соломона как рекуррентные последовательности и их декодирование с использованием двойственного базиса

По аналогии с рассмотренными выше эквивалентными кодами БЧХ как рекуррентными последовательностями над простым полем $GF(2)$, могут быть построены эквивалентные (дуальные) коды Рида – Соломона (недвоичные коды БЧХ) над полем $GF(2^k)$ с некоторым порождающим поле многочленом $G(x)$ k-й степени, корнем которого будет в общем случае первообразный элемент $\varepsilon \in GF(2^k)$. Для построения эквивалентного циклического кода Рида – Соломона, в дальнейшем РСЭ выберем образующий многочлен $P(x) = \prod_{i=1}^{m}(x + \varepsilon_i)$, который будет являться характеристическим многочленом

$$P(x) = p_0 x^m + p_1 x^{m-1} + p_2 x^{m-2} + ... + p_{m-1} x + p_m;\ p_i \in GF(2^k), \qquad (1.33)$$

порождающим возвратные рекурсивные последовательности $\{s\} = (s_0 s_1 s_2 s_3 ... s_{2^k-2})$ с периодом $n = 2^k - 1$ и элементами, принадлежащими полю $GF(2^k)$.

В соответствии с видом характеристического многочлена $P(x)$, у которого всегда $p_0 = 1$, любая возвратная последовательность $\{s\}$ будет удовлетворять рекуррентному уравнению:

$$s_i = p_1 s_{i-1} + p_2 s_{i-2} + ... + p_{m-1} s_{i-m+1} + p_m s_{i-m}, \qquad (1.34)$$

где $i \geq m$ и, кроме того, индекс iприводится по модулю $2^k - 1$.

С другой стороны, произвольный элемент возвратной последовательности, как известно, может быть выражен через корни $\varepsilon_1, \varepsilon_2, ..., \varepsilon_m$ характеристического многочлена $P(x)$ и соответствующие корням элементы поля $A, B, \ldots, C$ как

$$s_i = A\varepsilon_1^i + B\varepsilon_2^i + ... + C\varepsilon_m^i. \qquad (1.35)$$

Сами же элементы $A, B, ..., C$ могут быть определены, как это показано при рассмотрении кодов БЧХЭ с разложимым характеристическим многочленом, по любому m-элементному безошибочному участку возвратной последовательности $\{s\}$ в соответствии с выражениями:

$$\begin{aligned} A &= \varepsilon_1^{-i}\left(\alpha_1 s_i + \alpha_2 s_{i+1} + ... + \alpha_m s_{i+m-1}\right); \\ B &= \varepsilon_2^{-i}\left(\beta_1 s_i + \beta_2 s_{i+1} + ... + \beta_m s_{i+m-1}\right); \\ C &= \varepsilon_m^{-i}\left(\gamma_1 s_i + \gamma_2 s_{i+1} + ... + \gamma_m s_{i+m-1}\right). \end{aligned} \qquad (1.36)$$

Постоянные коэффициенты $\alpha_i, \beta_i, ..., \gamma_i \; i = 1, 2, ..., m$, зависят от характеристического многочлена $P(x)$ и определяются по полученным в работе выражениям (1.8), (1.9), через корни и коэффициенты p_j многочлена $P(x)$, а именно, коэффициенты α_i для корня ε_1, β_i – для корня ε_2 и т. д., коэффициенты γ_i – для корня ε_m.

1.5.1. *Принципы построения кодирующих и декодирующих устройств РСЭ*

Исходя из вышеизложенного, кодирующее устройство эквивалентного (дуального) кода Рида – Соломона может строиться по принципу систематического или несистематического кода.

В случае систематического циклического кода РСЭ информационными элементами кода (*n, m*) будут начальные *m* элементов последовательности $\{s\}$, т. е. $s_0 s_1 ... s_{m-1}$. Остальные избыточные элементы кодовой комбинации как рекуррентной последовательности будут находиться по рекуррентной формуле (1.34). Реализуется кодирующее устройство такого систематического кода довольно просто в соответствии с блок-схемой, представленной на рис. 1.11, а.

Другой вариант кодирующего устройства для несистематического циклического кода РСЭ реализуется в соответствии с выражением (1.35). Блок-схема такого кодирующего устройства представлена на рис. 1.11, б. Как видим, реализация кодирующего устройства несистематического кода ничуть не сложнее, чем систематического. Информационные элементы *A, B,…, C*, записанные как исходные в *k*-разрядные ячейки памяти с обратной связью, порождают на выходе последовательность $\{s\}$.

Выбор варианта построения кодирующего устройства следует произвести после анализа сложности реализации декодирующего устройства для обоих вариантов кода. Однако даже без подробного анализа процессов декодирования кодов РСЭ очевидно, что реализация декодирования несистематического кода более проста, чем систематического. Действительно, в результате декодирования систематического кода РСЭ необходимо по принятой комбинации сначала определить элементы *A, B,..., C* по формуле (1.36), а затем, в соответствии с (1.35), найти информационные элементы $s_0, s_1, ..., s_{m-1}$. При декодировании же несистематического кода РСЭ достаточно определить, в соответствии с (1.36), только элементы *A, B,…, C*, которые и являются информационными элементами.

Таким образом, следует рекомендовать применение несистематического кода РСЭ как более простого по реализации.

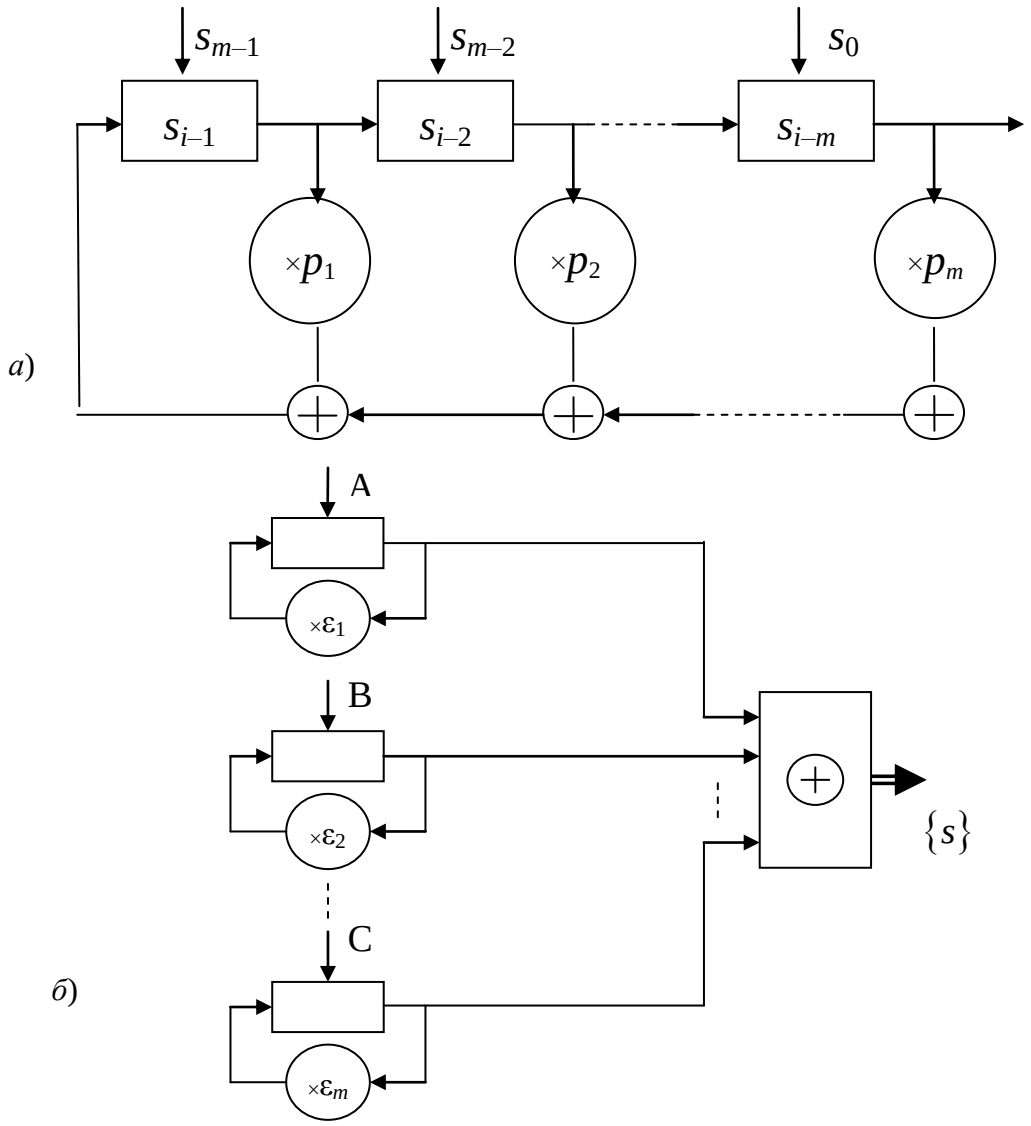

Рис. 1.11. Блок-схема кодирующего устройства систематического (а) и несистематического (б) кода РСЭ

Реализация декодирующего устройства несистематического кода РСЭ мало чем будет отличаться от реализации декодирующего кода БЧХЭ, представленного на рис. 1.8. Отличием является то, что элементы рекуррентной последовательности $\{s\}$ будут принадлежать не простому полю $GF(2)$, а расширенному полю $GF(2^k)$.

Рассмотрим простой пример построения несистематического кода Рида – Соломона, комбинации которого будут рекуррентными последовательностями.

Пример 1.8. Построим циклический несистематический код Рида – Соломона $(n, m) = (7, 3)$ с образующим код многочленом $P(x) = (x+1)(x+\varepsilon)(x+\varepsilon^2)$, который порождает рекуррентную последовательность над расширенным полем $GF(2^3)$.

Пусть полином, образующий поле, имеет вид $G(x)=1+x+x^3$, корнем которого будет первообразный элемент поля ε. После перемножения сомножителей полином $P(x)$ будет иметь следующий вид:

$$P(x)=p_0x^3+p_1x^2+p_2x+p_3=x^3+\varepsilon^5x^2+\varepsilon^6x+\varepsilon^3. \qquad (1.37)$$

Учитывая, что мы рассматриваем несистематический код РСЭ, выберем в качестве информационных элементов произвольные элементы поля $GF(2^3)$, например $A=\varepsilon^5; B=\varepsilon^4; C=0$. При таких начальных элементах, в соответствии с (1.35), будет сформирована следующая рекуррентная последовательность с периодом $(2^3–1) = 7$: $\{s\}=(s_0s_1s_2s_3s_4s_5s_6)=(10\varepsilon\varepsilon^4\varepsilon^6\varepsilon^3\varepsilon^2)$. При этом, корнями многочлена $P(x)$ будут элементы, равные $\varepsilon_1=1;\ \varepsilon_2=\varepsilon;$ $\varepsilon_3=\varepsilon^2$.

Блок-схема кодирующего устройства рассматриваемого несистематического кода будет иметь вид, представленный на рис. 1.12.

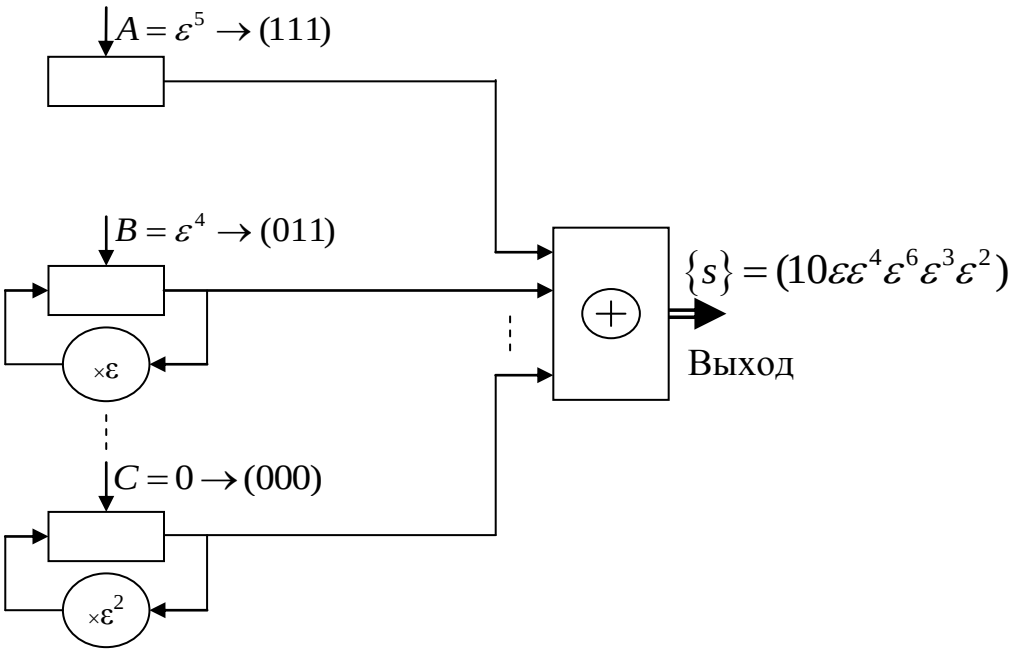

Рис. 1.12. Блок-схема кодирующего устройства несистематического кода РСЭ (7, 3)

Можно проверить, что полученная на выходе последовательность $\{s\}$ будет удовлетворять рекуррентному уравнению, соответствующему характеристическому многочлену $P(x)$ (1.37), т. е.

$$s_i \underset{i\geq 3}{=} p_1s_{i-1}+p_2s_{i-2}+p_3s_{i-3}=\varepsilon^5s_{i-1}+\varepsilon^6s_{i-2}+\varepsilon^3s_{i-3}. \qquad (1.38)$$

Для сравнения приведем схему рекуррентного кодирующего устройства, соответствующего уравнению (1.38) и порождающего такую же кодовую последовательность (рис. 1.13):

Как видно из рис. 1.13, схема кодирующего устройства систематического кода (7, 3) отличается тем, что в ячейки регистра в качестве исходных данных должны быть записаны элементы 1, 0 и ε, которые в данном варианте и будут являться информационными элементами выходной кодовой комбинации.

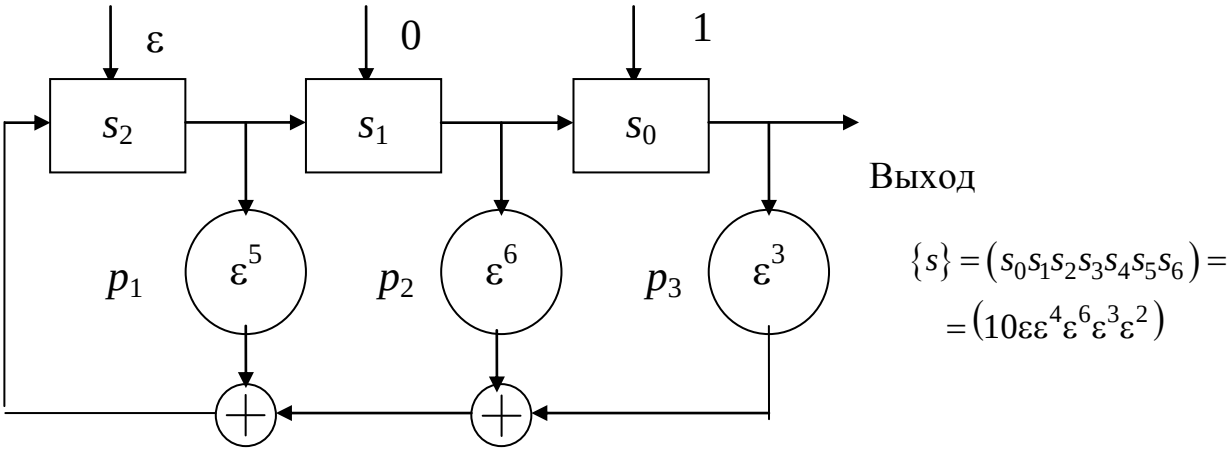

Рис. 1.13. Блок-схема кодирующего устройства
систематического кода РСЭ (7, 3)

Наконец, приведем схему кодирующего устройства классического кода Рида – Соломона (7, 3) над полем $GF(2^3)$ с проверочным многочленом $Q(x) = \dfrac{x^7 - 1}{P(x)} = x^4 + \varepsilon^5 x^3 + \varepsilon^4 x^2 + x + \varepsilon^4$, где ε – первообразный корень образующего поле многочлена $G(x) = 1 + x + x^3$.

Схема кодирующего устройства, реализующего деление многочлена $x^{n-m} f(x) = x^4 f(x)$, где $f(x)$ – многочлен исходных информационных элементов, на проверочный многочлен $Q(x)$ и получение остатка от деления $R(x)$, представлена на рис. 1.14.

Легко проверить, что после подачи на вход исходной комбинации $f(x) = \varepsilon + x^2$ в ячейках регистра деления будет содержаться остаток:

$$R(x) = r_0 + r_1 x + r_2 x^2 + r_3 x^3 = \varepsilon^2 + \varepsilon^3 x + \varepsilon^6 x^2 + \varepsilon^4 x^3.$$

Таким образом, на выходе кодирующего устройства будет сформирована такая же кодовая комбинация: $10\varepsilon\varepsilon^4\varepsilon^6\varepsilon^3\varepsilon^2$.

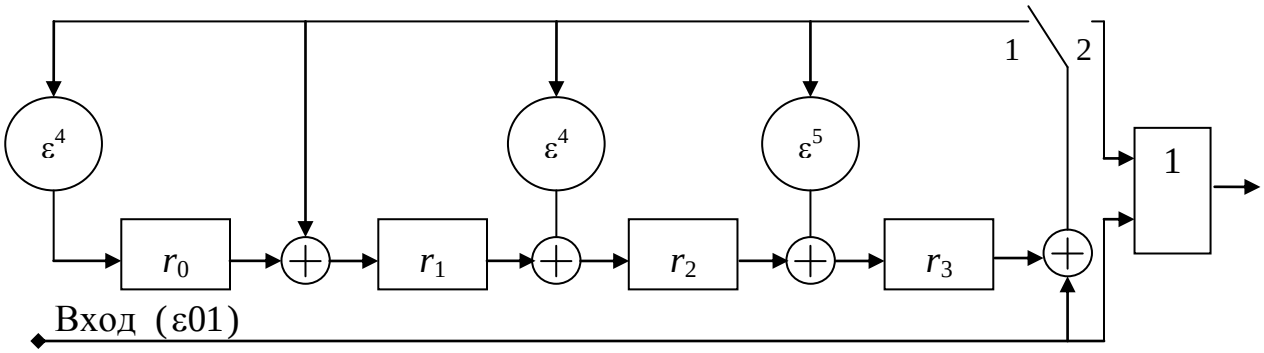

Рис. 1.14. Блок-схема
классического кодирующего устройства кода Рида – Соломона (7, 3)

В результате сравнения с предыдущими вариантами кодирующего устройства можно сделать вывод, что последний вариант имеет более сложную реализацию (так как $n-m>m$).

Задачей декодирования кода РСЭ на основе двойственного базиса является определение информационных элементов *A*, *B* и *C* по *m*-элементным участкам принятой последовательности в соответствии с выражениями (1.36). Для этого необходимо предварительно определить по формулам (1.8), (1.9) постоянные коэффициенты α_i, β_i и γ_i, $i=1,2,3$, соответственно для различных корней $\varepsilon_1=1$, $\varepsilon_2=\varepsilon$ и $\varepsilon_3=\varepsilon^2$ характеристического многочлена:

$$\alpha_1=\varepsilon;\ \alpha_2=\varepsilon^2;\ \alpha_3=\varepsilon^5;$$
$$\beta_1=\varepsilon^2;\ \beta_2=\varepsilon^6;\ \beta_3=1;$$
$$\gamma_1=\varepsilon^5;\ \gamma_2=1;\ \gamma_3=\varepsilon^4.$$

Теперь покажем, что по любому безошибочному *m*-элементному участку последовательности $\{s\}$ будут определены элементы *A, B* и *C*, что и позволяет организовать мажоритарное декодирование.

Пусть был выделен участок $(s_4s_5s_6)=(\varepsilon^6\varepsilon^3\varepsilon^2)$, т. е. $i=4$. Тогда, в соответствии с (1.36), имеем:

$$A=\varepsilon_1^{-4}\left(\alpha_1s_4+\alpha_2s_5+\alpha_3s_6\right)=\varepsilon^5;$$
$$B=\varepsilon_2^{-4}\left(\beta_1s_4+\beta_2s_5+\beta_3s_6\right)=\varepsilon^4;$$
$$C=\varepsilon_3^{-4}\left(\gamma_1s_4+\gamma_2s_5+\gamma_3s_6\right)=0.$$

Возьмем другой участок $\left(s_6s_7s_8\right)=\left(s_6s_0s_1\right)=\left(\varepsilon^210\right)$ замкнутой в кольцо последовательности $\{s\}$, т. е. $i=6$, и так же вычислим элементы *A*, *B* и *C*:

$$A=(\alpha_1s_6+\alpha_2s_0+\alpha_3s_1)=\varepsilon\cdot\varepsilon^2+\varepsilon^2\cdot1=\varepsilon^5;$$

$$B = \varepsilon^{-6}(\beta_1 s_6 + \beta_2 s_0 + \beta_3 s_1) = \varepsilon^{-6}(\varepsilon^2 \cdot \varepsilon^3 + \varepsilon^6 \cdot 1) = \varepsilon^4;$$
$$C = \varepsilon^{-12}(\gamma_1 s_6 + \gamma_2 s_0 + \gamma_3 s_1) = \varepsilon^{-5}(\varepsilon^5 \cdot \varepsilon^2 + 1) = 0.$$

В случае наличия ошибок в принятой комбинации процедура декодирования и сложность реализации не меняется. Результатом декодирования будет совокупность элементов *A, B* и *C*, имеющая наибольшее количество значений, вычисленных по выражениям (1.36).

Корректирующие свойства (*n, m*)-кода Рида–Соломона определяются минимальным кодовым расстоянием $d_{\min}$, которое будет для РС кода равно $d_{\min} = n - m + 1$. Для данного примера кода (7, 3) $d_{\min} = 5$ и поэтому рассматриваемый код РС должен исправлять до двух ошибок.

Используя выражения (1.36) для определения элементов *A, B* и *C* по *m*-элементным участкам комбинации несистематического кода (7, 3), легко убедиться, что данный код с мажоритарным декодированием замкнутой в кольцо рекуррентной последовательности исправляет любую однократную ошибку и часть двукратных. В то же время многие двукратные ошибки, например, в элементах s_i и s_{i+3}, рассматриваемый код в результате декодирования последовательности $\{s\}$ исправить не может.

Для усиления корректирующих свойств кода РСЭ можно, как и в кодах БЧХЭ, использовать децимации с индексами $q = 2^j$, где $j = 1, \ldots, (k-1)$.

Однако возможность применения децимаций по отношению к принятой кодовой последовательности предъявляет определенные требования к характеристическому многочлену $P(x)$, которые можно сформулировать в виде следующего свойства эквивалентного кода Рида – Соломона:

Свойство. *Комбинации циклического кода РСЭ над полем* $GF(p^k)$ *могут быть мажоритарно декодированы с использованием децимаций, если характеристический многочлен* $P(x)$ *представляет собой один или произведение нескольких полиномов* $f_i(x)$*,входящих в разложение двучлена* $(x^{p^k-1} - 1)$ *на неприводимые полиномы деления круга.*

Предположим, что это требование по отношению к многочлену $P(x)$ выполнено. Тогда справедливыми будут две теоремы, одну из которых назовем теоремой идентичности, а другую – теоремой однозначности.

Теорема 1.3. Теорема идентичности.

Если характеристический многочлен $P(x)$ *представляет собой один или произведение нескольких минимальных многочленов, входящих в разложение двучлена* $\left(x^{p^k-1} - 1\right)$*, то исходная рекуррентная последователь-*

ность $\{s\} = \left(s_0 s_1 s_2 s_3 ... s_{p^k-2}\right)$, *образованная по многочлену* $P(x)$, *и последовательности* $\{u\} = (u_0 u_1 u_2 u_3 ... u_{p^k-2})$, *полученные из* $\{s\}$ *путем децимаций с индексом* $q = p^j$, *где* j = 1, 2, ... (k – 1), *будут удовлетворять одному и тому же рекуррентному уравнению (соотношению).*

Доказательство этой теоремы строится по тому же принципу, что и доказательство аналогичной теоремы 1.1 для кодов БЧХЭ с той разницей, что при доказательстве этой теоремы для кодов Рида – Соломона рассматривается расширенное поле $GF(p^k)$ с произвольной характеристикой p простого поля $GF(p)$. Во всем остальном доказательство остается тем же. Поэтому здесь, чтобы не повторяться, более подробное доказательство теоремы идентичности приводить нет необходимости.

Теперь сформулируем и докажем другую теорему.

Теорема 1.4. Теорема однозначности.

Если элементы A, B, C,... $\in GF(p^k)$, *соответствующие сомножителям характеристического многочлена* $P(x)$, *однозначно определяют начальную фазу рекуррентной последовательности* $\{s\}$, *то начальная фаза последовательностей* $\{u\}_q$, *полученных из последовательности* $\{s\}$ *путем ее децимации с индексом* $q = p^j$, *где* j = 1, 2, ... (k – 1), *также будет однозначно определяться теми же элементами A, B, C, ..., но имеющими циклический сдвиг вправо на j шагов.*

Доказательство этой теоремы основано на свойствах p-сопряженных корней. Пусть корнями минимального многочлена $f_i(x)$ будут $\varepsilon_1, \varepsilon_2, ..., \varepsilon_{d-1}, \varepsilon_d$, где d – степень многочлена $f_i(x)$, которая, применительно к полю $GF(p^k)$, будет числом k или его делителем. Если наименьший по степени корень ε_1 равен элементу поля ε^i, то остальными корнями будут элементы $\varepsilon_2 = (\varepsilon^i)^p$; $\varepsilon_3 = (\varepsilon^i)^{p^2}$, $....\varepsilon_{d-1} = (\varepsilon^i)^{p^{d-2}}$, $\varepsilon_d = (\varepsilon^i)^{p^{d-1}}$.

Следовательно, подмножество показателей степени i, ip, ip^2, …, ip^{d-1} представляет собой циклотомический класс с образующим элементом (представителем) i.

Если теперь ряд корней характеристического многочлена $f_i(x)$ возвести каждый в степень p, то, учитывая теорему Ферма, получаем тот же ряд корней, но циклически сдвинутых на один шаг влево, т. е.

$$\left\{\varepsilon_1^p, \varepsilon_2^p, \cdots, \varepsilon_{d-1}^p, \varepsilon_d^p\right\} = \left\{(\varepsilon^i)^p, (\varepsilon^i)^{p^2}, \cdots, (\varepsilon^i)^{p^{d-1}}, (\varepsilon^i)^{p^d}\right\} = \{\varepsilon_2, \varepsilon_3, \cdots, \varepsilon_{d-1}, \varepsilon_d, \varepsilon_1\}.$$

Аналогично, если каждый из ряда корней многочлена $f_i(x)$ возвести в степень p^j, то получим тот же ряд корней с циклическим сдвигом на j шагов влево.

Покажем, что именно такие преобразования происходят в случае применения децимаций. Для упрощения записи примем, что индекс децимации равен $q = p$, т. е. $j = 1$.

Тогда, в результате децимации, из исходной рекуррентной последовательности $\{s\} = \left(s_0 s_1 s_2 s_3 s_4 s_5 ... s_{p^k-2}\right)$ будет получена последовательность

$$\{u\}_p = \left(u_0 u_1 u_2 u_3 u_4 u_5 ... u_{p^k-2}\right) = \left(s_0 s_p s_{2p} s_{3p} s_{4p} ...\right).$$

В соответствии с теоремой 1.3 обе последовательности являются возвратными, удовлетворяющими одному и тому же рекуррентному уравнению. Отличие же между ними состоит в различных начальных участках обеих последовательностей или в различных коэффициентах *A, B,…, C, D,* по которым образуются эти последовательности. Если предположить, что $P(x) = f_i(x)$, то любой произвольный элемент исходной последовательности $\{s\}$ может быть определен как

$$s_n = A\varepsilon_1^n + B\varepsilon_2^n + ... + C\varepsilon_{d-1}^n + D\varepsilon_d^n .$$

Аналогично, элементу u_n последовательности $\{u\}_p$ будет соответствовать выражение

$$u_n = A_p\varepsilon_1^n + B_p\varepsilon_2^n + ... + C_p\varepsilon_{d-1}^n + D_p\varepsilon_d^n . \qquad (1.39)$$

А так как $u_n = s_{np}$, то последнее выражение может быть переписано как:

$$\begin{aligned} u_n = s_{np} &= A\varepsilon_1^{np} + B\varepsilon_2^{np} + ... + C\varepsilon_{d-1}^{np} + D\varepsilon_d^{np} = \\ &= A\left(\varepsilon_1^p\right)^n + B\left(\varepsilon_2^p\right)^n + ... + C\left(\varepsilon_{d-1}^p\right)^n + D\left(\varepsilon_d^p\right)^n . \end{aligned} \qquad (1.40)$$

Выше было показано, что для p-сопряженных корней полинома $f_i(x)$ степени d справедливо следующее: $\varepsilon_1^{\,p} = \varepsilon_2$; $\varepsilon_2^{\,p} = \varepsilon_3$; …; $\varepsilon_{d-1}^p = \varepsilon_d$; $\varepsilon_d^{\,p} = \varepsilon_1$.

Тогда последнее выражение для элемента u_n можно записать как:

$$u_n = D\varepsilon_1^n + A\varepsilon_2^n + B\varepsilon_3^n, ... + C\varepsilon_d^n = A_p\varepsilon_1^n + B_p\varepsilon_2^n + ... + D_p\varepsilon_d^n . \qquad (1.41)$$

Отсюда, коэффициенты $A_p, B_p, ..., D_p$, соответствующие последовательности $\{u\}_p$ с индексом децимации $q = p$, однозначно определяют коэффициенты *A, B, …, C,D,* образующие исходную последовательность $\{s\}$, а именно, $A_p = D, B_p = A, ..., D_p = C$.

Таким образом, коэффициентами $A_p, B_p, ..., D_p$ будут те же коэффициенты *A, B, ..., D*, соответствующие исходной последовательности $\{s\}$, но имеющие циклический сдвиг вправо на один шаг.

Аналогично можно показать, что в общем виде коэффициентам $A_q, B_q, ..., C_q, D_q$, соответствующим последовательности $\{u\}_q$, полученной из $\{s\}$ путем децимаций с индексом $q = p^j$, где j = 1, 2, …, (k – 1), будут соответствовать коэффициенты *A, B, ..., C, D*, имеющие циклический сдвиг вправо на *j* шагов.

Если характеристический многочлен $P(x)$ состоит из произведения нескольких минимальных многочленов, например, $P(x) = f_i(x)...f_j(x)$, то можно также показать, что доказанное выше распространяется и на подмножество других коэффициентов *E*, …, *F*, соответствующих корням других минимальных полиномов, например, $f_j(x)$. При этом, циклическому сдвигу на *j* шагов вправо будут подвергаться подмножества коэффициентов, соответствующих каждому из минимальных полиномов в отдельности.

Таким образом, мы доказали теорему однозначности, по которой в поле $GF(p^k)$ коэффициенты $A_q, B_q, ..., E_q, F_q$, соответствующие рекуррентной последовательности $\{u\}_q$, полученной из исходной последовательности $\{s\}$ путем децимаций с индексом $q = p^j$, где j = 1, 2, …, (k – 1), однозначно определяют коэффициенты *A, B, C, ..., E, F*, образующие исходную рекуррентную последовательность $\{s\}$ над полем $GF(p^k)$.

Именно эта особенность и позволяет усилить корректирующие свойства кода РСЭ при мажоритарном декодировании кодовых комбинаций как рекуррентных последовательностей.

Рассмотрим несколько примеров, поясняющих приведенные выше теоремы и механизм мажоритарного декодирования с применением децимаций.

Пример 1.9. Рассмотрим эквивалентный код Рида – Соломона (7, 3), комбинации которого будут представлять рекуррентные последовательности над полем $GF(2^3)$, удовлетворяющие характеристическому многочлену $P(x) = 1 + x + x^3$. Очевидно, что этот многочлен является минимальным, соответствующие корни его будут $\varepsilon_1 = \varepsilon$, $\varepsilon_2 = \varepsilon^2$, $\varepsilon_3 = \varepsilon^4$. Так как многочлен $P(x)$ является примитивным, то его корни являются первообразными, т. е. имеющими порядок, равный 7.

Наконец, будем считать, что поле $GF(2^3)$ образовано тем же многочленом $G(x) = 1 + x + x^3$. Пусть принята безошибочная комбинация такого

кода, равная $(s_0 s_1 s_2 s_3 s_4 s_5 s_6) = (10\varepsilon 1\varepsilon\varepsilon^3\varepsilon^3)$. Легко проверить, что эта комбинация является рекуррентной и удовлетворяет рекуррентному уравнению $s_i = s_{i-2} + s_{i-3}$, соответствующему заданному характеристическому многочлену $P(x)$.

Блок-схема кодирующего устройства несистематического кода РСЭ (7, 3) представлена на рис. 1.15.

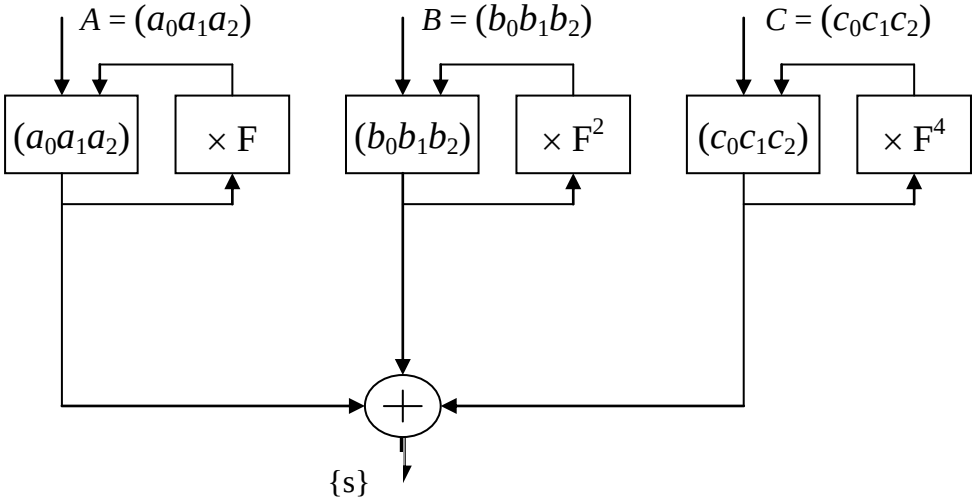

Рис. 1.15. Блок-схема
кодирующего устройства несистематического кода РСЭ (7, 3)

На рис. 1.15 матрицы F, F^2 и F^4имеют вид:

$$F = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}; \quad F^2 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}; \quad F^4 = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}.$$

Схема, как видно, состоит из 3 трехразрядных ячеек памяти, в которые в начальный момент записываются информационные элементы в виде двоичных векторов $A \equiv (a_0 a_1 a_2)$, $B \equiv (b_0 b_1 b_2)$ и $C \equiv (c_0 c_1 c_2)$. Эти векторы затем считываются и поэлементно складываются по mod2 в сумматоре. При этом на выходе сумматора будет сформирован элемент $s_0 \equiv (d_0 d_1 d_2)$.

В цепях обратной связи ячеек памяти кодирующего устройства включены умножители, которые выполняют следующие логические действия:

– умножение на F: $(a_0 a_1 a_2) \cdot F = (a_2, a_0 + a_2, a_1)$;

– умножение на F^2: $(b_0 b_1 b_2) \cdot F^2 = (b_1, b_1 + b_2, b_0 + b_2)$;

– умножение на F^4: $(c_0 c_1 c_2) \cdot F^4 = (c_1 + c_2, c_0 + c_1, c_0 + c_1 + c_2)$.

Сложение полученных векторов в выходном сумматоре в очередной тактовый момент времени формирует следующий элемент $(t_0t_1t_2) = s_1$ кодовой комбинации и т. д.

Рассмотрим процедуру мажоритарного декодирования с использованием двойственного базиса.

Имея характеристический многочлен $P(x) = p_0x^3 + p_1x^2 + p_2x + p_3 = x^3 + x + 1$ $(p_0 = p_2 = p_3 = 1, p_1 = 0)$, воспользуемся формулой (1.8) и найдем коэффициенты $\{\alpha_1, \alpha_2, \alpha_3\}$ как двойственный базис поля $GF(2^3)$ по отношению к левому степенному базису $\{1, \varepsilon, \varepsilon^2\}$: $\alpha_1 = 1$, $\alpha_2 = \varepsilon^2$, $\alpha_3 = \varepsilon$; $GF(2^3)$.

Зная коэффициенты α_1, α_2 и α_3, можно теперь по любому m-элементному участку (m = 3) последовательности определить информационные элементы A, B и C несистематического (7, 3)-кода.

Например, если выделен начальный участок $(s_0s_1s_2) = (10\varepsilon)$, i = 0, то коэффициенты A, B и C, с учетом формулы (1.36), будут равны:

$$A = 1 \cdot \alpha_1 + \varepsilon \cdot \alpha_3 = 1 + \varepsilon^2 = \varepsilon^6;$$
$$B = 1 \cdot \alpha_1^2 + \varepsilon \cdot \alpha_3^2 = 1 + \varepsilon^3 = \varepsilon;$$
$$C = 1 \cdot \alpha_1^4 + \varepsilon \cdot \alpha_3^4 = 1 + \varepsilon^5 = \varepsilon^4.$$

Возьмем другой участок, например, $(s_6s_7s_8) = (s_6s_0s_1) = (\varepsilon^3 10)$. Тогда, аналогично, по формуле (1.36), имеем:

$$A = \varepsilon_1^{-6}\left(\varepsilon^3\alpha_1 + \alpha_2\right) = \varepsilon^{-6}\left(\varepsilon^3 + \varepsilon^2\right) = \varepsilon^{-1} = \varepsilon^6;$$
$$B = \varepsilon_2^{-6}\left(\varepsilon^3\alpha_1^2 + \alpha_2^2\right) = \varepsilon^{-5}\left(\varepsilon^3 + \varepsilon^4\right) = \varepsilon;$$
$$C = \varepsilon_3^{-6}\left(\varepsilon^3\alpha_1^4 + \alpha_2^4\right) = \varepsilon^{-3}\left(\varepsilon^3 + \varepsilon\right) = \varepsilon^4.$$

Покажем теперь, что те же коэффициенты можно получить, обработав последовательность, подвергнутую децимациям с индексами $q = 2^j$, где j = 1, 2.

Пусть j = 1, т. е. $q = p = 2$. Тогда, из исходной последовательности $\{s\}$ получим последовательность $\{u\}_2$:

$$\{u\}_2 = \left(s_0s_2s_4s_6s_1s_3s_5\right) = \left(u_0u_1u_2u_3u_4u_5u_6\right) = \left(1\varepsilon\varepsilon\varepsilon^3 01\varepsilon^3\right).$$

Выберем, например, участок $(u_1u_2u_3) = (\varepsilon\varepsilon\varepsilon^3)$. Тогда, в соответствии с теоремой 1.4 (однозначности), для j = 1 получаем:

$$A_2 = \varepsilon_1^{-1}\left(\varepsilon\alpha_1 + \varepsilon\alpha_2 + \varepsilon^3\alpha_3\right) = \varepsilon^{-1}\left(\varepsilon + \varepsilon^3 + \varepsilon^4\right) = \varepsilon^4 = C;$$

$$B_2 = \varepsilon_2^{-1}\left(\varepsilon\alpha_1^2 + \varepsilon\alpha_2^2 + \varepsilon^3\alpha_3^2\right) = \varepsilon^{-2}\left(\varepsilon + \varepsilon^5 + \varepsilon^5\right) = \varepsilon^6 = A;$$
$$C_2 = \varepsilon_3^{-1}\left(\varepsilon\alpha_1^4 + \varepsilon\alpha_2^4 + \varepsilon^3\alpha_3^4\right) = \varepsilon^{-4}\left(\varepsilon + \varepsilon^2 + 1\right) = \varepsilon = B.$$

Таким образом, мы имеем те же коэффициенты *A*, *B* и *C*, но только сдвинутые циклически на $j = 1$ шаг.

Наконец, продемонстрируем обработку последовательности $\{u\}_q$, полученную из $\{s\}$ путем ее децимации с индексом $q = 2^j$, где $j = 2$:

$$\{u\}_4 = \left(s_0 s_4 s_1 s_5 s_2 s_6 s_3\right) = \left(u_0 u_1 u_2 u_3 u_4 u_5 u_6\right) = \left(1\varepsilon 0\varepsilon^3\varepsilon\varepsilon^3 1\right).$$

Выделим произвольный *m*-элементный участок, например, $(u_1 u_2 u_3) = (\varepsilon 0\varepsilon^3)$. Тогда, аналогично предыдущему примеру, получим:

$$A_4 = \varepsilon_1^{-1}\left(\varepsilon\alpha_1 + \varepsilon^3\alpha_3\right) = \varepsilon^{-1}\left(\varepsilon + \varepsilon^4\right) = \varepsilon = B;$$
$$B_4 = \varepsilon_2^{-1}\left(\varepsilon\alpha_1^2 + \varepsilon^3\alpha_3^2\right) = \varepsilon^{-2}\left(\varepsilon + \varepsilon^5\right) = \varepsilon^4 = C;$$
$$C_4 = \varepsilon_3^{-1}\left(\varepsilon\alpha_1^4 + \varepsilon^3\alpha_3^4\right) = \varepsilon^{-4}(\varepsilon + 1) = \varepsilon^6 = A.$$

Как видим, получены те же значения информационных элементов *A*, *B* и $C \in GF(2^3)$, но циклически сдвинутых на $j = 2$ шага.

Покажем теперь, что мажоритарное декодирование как основной последовательности с ошибками $\{h\} = \{s\} + \{e\}$, так и ее децимаций, усиливает корректирующие свойства кода.

Как следует из теории кодов Рида – Соломона, код (7, 3) имеет минимальное кодовое расстояние $d_{\min} = 5$ и поэтому такой код может исправлять до двух ошибочных элементов в кодовой комбинации.

Пусть в переданной кодовой комбинации $\{s\}$ возникли две ошибки в элементах s_0 и s_3, при этом принятая комбинация $\{h\}$ с ошибками будет иметь вид: $\{h\} = (h_0 h_1 h_2 h_3 h_4 h_5 h_6) = (\varepsilon^5 0\varepsilon\varepsilon^5\varepsilon\varepsilon^3\varepsilon^3)$.

Обработав по *m*-элементным участкам ($m = k = 3$) последовательность $\{h\}$ и две ее децимированные последовательности с индексами децимации $q = 2$ и $q = 4$ так, как показано выше, получим коэффициенты *A*, *B* и *C*, значения которых приведены в табл. 1.5.

Анализ данных таблицы показывает, что обработка только одной последовательности $\{h\}$ без децимаций не позволяет правильно определить коэффициенты *A*, *B* и *C*. В то же время, после обработки всех трех последовательностей по большинству правильно определяются информационные элементы: $A = \varepsilon^6$; $B = \varepsilon$ и $C = \varepsilon^4$.

Таблица 1.5

Значения коэффициентов			Количество сочетаний *A*, *B*, *C* при обработке рекуррентных последовательностей с индексом децимации *q*			Суммарное количество сочетаний коэффициентов *A*, *B*, *C*
A	*B*	*C*	$q=1$ ($j=0$)	$q=2$ ($j=1$)	$q=4$ ($j=2$)	
ε^6	ε	ε^4	1	2	3	6
1	ε^4	ε	1	1	1	3
ε^3	ε^2	0	2			2
ε	ε^2	1	1			1
ε	0	ε^5	2			2
ε^2	1	ε		2		2
ε^6	ε^2	ε^2		1		1
ε^5	ε^3	1		1		1
0	0	1			1	1
1	ε^5	ε^3			1	1
ε^4	ε	1			1	1

Пример 1.10. Рассмотрим другой пример кода РСЭ (15, 4), элементы которого принадлежат полю $GF(2^4)$, образованному примитивным многочленом $G(x)=1+x+x^4$. Будем представлять комбинации такого кода как рекуррентные последовательности с характеристическим многочленом $P(x)=G(x)$, т. е. характеристический многочлен будет минимальным многочленом с первообразными корнями.

Тогда, в соответствии с выбранным $P(x)$, элементы кодовой комбинации $(s_0 s_1 s_2 ... s_{13} s_{14})$ будут удовлетворять рекуррентному уравнению $s_i = s_{i-3} + s_{i-4}$; $GF(2^4)$. При этом, индексы i при s_i приводятся по модулю 15.

Многочлен $P(x)$ имеет своими сопряженными корнями элементы $\varepsilon_1=\varepsilon$; $\varepsilon_2=\varepsilon^2$; $\varepsilon_3=\varepsilon^4$ и $\varepsilon_4=\varepsilon^8$. Следовательно, по аналогии с предыдущим примером, схема кодирующего устройства будет иметь вид, представленный на рис. 1.16.

Если в 4-разрядные ячейки памяти записать исходные информационные элементы, как показано на рис. 1.16, $A=\varepsilon^7$, $B=\varepsilon^{11}$, $C=\varepsilon^5$ и $D=\varepsilon$, то на выходе будет сформирована следующая рекуррентная кодовая последовательность:

$$\{s\}=\left(s_0 s_1 s_2 s_3 s_4 s_5 s_6 s_7 s_8 s_9 s_{10} s_{11} s_{12} s_{13} s_{14}\right)=\left(1\varepsilon^3\varepsilon 0\varepsilon^{14}\varepsilon^9\varepsilon\varepsilon^{14}\varepsilon^4\varepsilon^3\varepsilon^7\varepsilon^9\varepsilon^7\varepsilon^4 1\right).$$

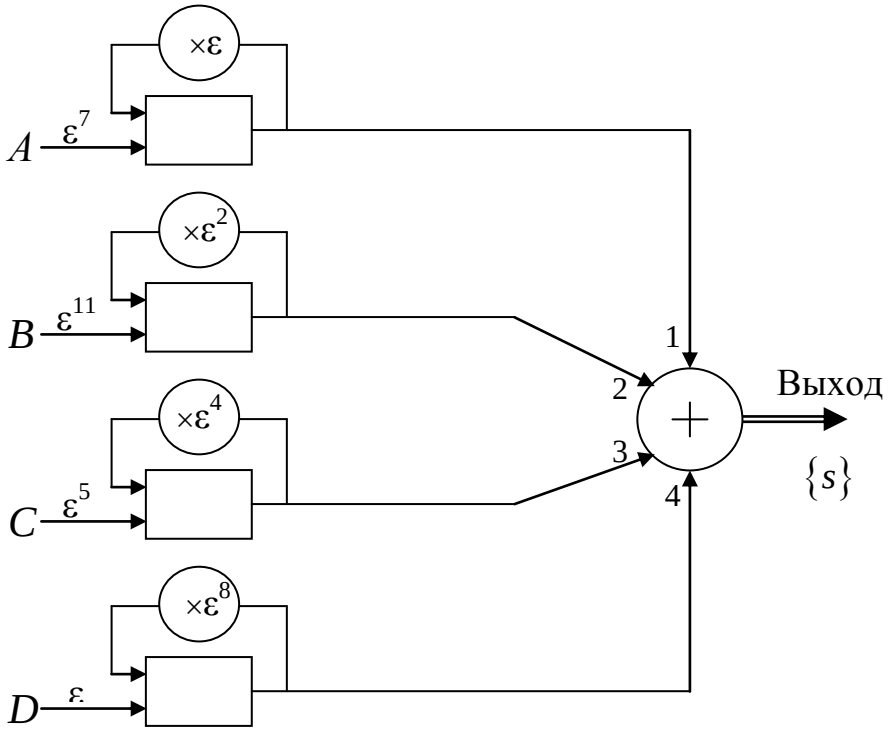

Рис. 1.16. Кодирующее устройство для кода РСЭ (15, 4)

Таблица 1.6

Входы сумматора				
1	ε^7	ε^8	ε^9	ε^{10}
2	ε^{11}	ε^{13}	1	ε^2
3	ε^5	ε^9	ε^{13}	ε^2
4	ε	ε^9	ε^2	ε^{10}
Выход сумматора	1 s_0	ε^3 s_1	ε s_2	0 s_3

Формирование первых элементов (s_0, s_1, s_2 и s_3) показано в табл. 1.6.

Рассмотрим теперь процедуру мажоритарного декодирования. Как следует из теории кодов Рида–Соломона, код (15, 4) имеет $d_{\min} = 12$ и поэтому он должен исправлять 5 и менее ошибок в комбинации.

Пусть была передана кодовая комбинация $\{s\}$, указанная выше, а принятая комбинация имеет вид:

$$\{h\} = (h_0 \overline{h_1} h_2 h_3 h_4 \overline{h_5} h_6 h_7 \overline{h_8} h_9 \overline{h_{10}} h_{11} h_{12} \overline{h_{13}} h_{14}) = (10\varepsilon 0\varepsilon^{14} 0\varepsilon\varepsilon^{14} 0\varepsilon^3 0\varepsilon^9\varepsilon^7 01).$$

Видим, что в принятой комбинации $\{h\}$ ошибки имеют место в элементах h_1, h_5, h_8, h_{10} и h_{13} (для наглядности над этими элементами поставлены черточки).

Декодирование будем вести по m-элементным ($m = k = 4$) участкам последовательности в соответствии с выражением (1.36). При этом, как было показано ранее, двойственный базис многочлена $P(x)$ равен:

$$\alpha_1 = \varepsilon^{14},\ \alpha_2 = \varepsilon^2,\ \alpha_3 = \varepsilon \text{ и } \alpha_4 = 1.$$

Проведя декодирование последовательности $\{h\}$ и ее трех децимированных последовательностей с индексами децимации $q = 2^j$, где j = 1, 2, 3, установим, что истинные информационные элементы *A*, *B*, *C* и *D* в совокупности появятся 6 раз, пять других сочетаний появятся по 3 раза каждое, еще шесть других сочетаний по 2 раза каждое и еще 27 сочетаний по одному разу. Как видим, из общего числа обработанных *m*-элементных участков, равного 60, наибольшее число раз появятся правильные информационные элементы: $A = \varepsilon^7$, $B = \varepsilon^{11}$, $C = \varepsilon^5$ и $D = \varepsilon$.

Таким образом, принятая комбинация $\{h\}$ кода (15, 4) с пятикратной ошибкой будет декодирована правильно по большинству выделенной совокупности элементов *A*, *B*, *C* и *D*.

Заметим, что в данном примере обработка по *m*-элементным участкам только одной последовательности $\{h\}$ не даст вообще ни одного сочетания правильных элементов *A*, *B*, *C* и *D*.

Рассмотрим теперь более общий пример, когда характеристический многочлен $P(x)$ кода РСЭ будет состоять из произведения нескольких минимальных многочленов, а элементы рекуррентной последовательности $\{s\}$ будут принадлежать расширенному полю $GF(p^k)$ с характеристикой p простого поля большей 2.

Пример 1.11. Рассмотрим процедуры кодирования и мажоритарного декодирования комбинаций кода РСЭ (8, 4) над полем $GF(3^2)$.

Выберем для построения поля примитивный многочлен $G(x) = x^2 + x + 2$, корнями которого будут сопряженные элементы поля ε и ε^3.

Построим циклический код РСЭ (8, 4) по характеристическому многочлену $P(x)$, равному произведению двух минимальных функций $f_1(x) = x^2 + x + 2$ и $f_2(x) = x^2 + 1$, т. е.

$$P(x) = f_1(x) f_2(x) = \left(x^2 + x + 2\right)\left(x^2 + 1\right) =$$
$$= p_0 x^4 + p_1 x^3 + p_2 x^2 + p_3 x + p_4 = x^4 + x^3 + x + 2.$$

Корнями многочлена $P(x)$ являются сопряженные корни минимального многочлена $f_1(x)$ – элементы $\varepsilon_1 = \varepsilon$; $\varepsilon_2 = \varepsilon^3$, и сопряженные корни минимального многочлена $f_2(x)$ – элементы поля $\varepsilon_3 = \varepsilon^2$ и $\varepsilon_4 = \varepsilon^6$

Тогда кодирующее устройство несистематического циклического кода РСЭ (8, 4) над полем $GF(3^2)$ (схема абсолютно аналогична схемам в рассмотренных примерах1.15 и 1.16) будет формировать на выходе сумматора по mod 3 комбинации $\{s\}$, элементы которых удовлетворяют уравнению:

$$p_0 s_i + p_1 s_{i-1} + p_2 s_{i-2} + p_3 s_{i-3} + p_4 s_{i-4} = 0.$$

Из уравнения следует, что произвольный элемент замкнутой в кольцо последовательности $\{s\}$ удовлетворяет, в соответствии с полиномом $P(x)$, рекуррентной формуле:

$$s_i = -\frac{p_1}{p_0}s_{i-1} - \frac{p_2}{p_0}s_{i-2} - \frac{p_3}{p_0}s_{i-3} - \frac{p_4}{p_0}s_{i-4}. \qquad (1.42)$$

Учитывая, что значения коэффициентов многочлена $P(x)$ равны $p_0 = p_1 = p_3 = 1;\ p_2 = 0;\ p_4 = 2$, рекуррентное уравнение принимает вид:

$$s_i = -s_{i-1} - s_{i-3} - 2s_{i-4} = 2s_{i-1} + 2s_{i-3} + s_{i-4}. \qquad (1.43)$$

С другой стороны, произвольный элемент s_i последовательности $\{s\}$ будет удовлетворять уравнению:

$$s_i = A\varepsilon_1^i + B\varepsilon_2^i + C\varepsilon_3^i + D\varepsilon_4^i, \quad GF\left(3^2\right), \qquad (1.44)$$

где A, B, C и D – информационные элементы, порождающие последовательность $\{s\}$.

Пусть информационные элементы имеют вид: $A = 1;\ B = 1;\ C = \varepsilon^7;$ $D = \varepsilon^2$.

Тогда на выходе кодирующего устройства будет сформирована следующая последовательность $\{s\}$:

$$\{s\} = \left(s_0 s_1 s_2 s_3 s_4 s_5 s_6 s_7\right) = \left(1\varepsilon 1\varepsilon^2 0\varepsilon^6 1\varepsilon^5\right).$$

Легко проверить, что элементы последовательности удовлетворяют рекуррентному уравнению (1.43).

Например, элемент $s_7 = 2s_6 + 2s_4 + s_3 = 2 + \varepsilon^2 = 2 + 1 + 2\varepsilon = 2\varepsilon = \varepsilon^5$

или $s_1 = 2s_0 + 2s_{-2} + s_{-3} = 2s_0 + 2s_6 + s_5 = 2 + 2 + \varepsilon^6 = 1 + 2 + \varepsilon = \varepsilon$.

Теперь рассмотрим процедуру декодирования по m-элементным участкам (m – степень многочлена $P(x)$). Для этого найдем коэффициенты двойственного базиса из выражения (1.8) в зависимости от значения коэффициентов многочлена $P(x)$ и его корней.

Так для корня $\varepsilon_1 = \varepsilon$ имеем:

$$\alpha_4 = \frac{p_0}{P'(\varepsilon)} = \varepsilon^3;\ \alpha_3 = \frac{p_1}{P'(\varepsilon)} + \alpha_4\varepsilon = \varepsilon^2;\ \alpha_2 = \frac{p_2}{P'(\varepsilon)} + \alpha_3\varepsilon = \varepsilon^3;$$

$$\alpha_1 = \frac{p_3}{P'(\varepsilon)} + \alpha_2\varepsilon = \varepsilon^2.$$

Для корня $\varepsilon_2 = \varepsilon^3$ коэффициенты α_i' равны соответственно коэффициентам α_i возведенным в степень $p = 3$.

Коэффициенты для корня $\varepsilon_3 = \varepsilon^2$, вычисленные из того же выражения, имеют значения: $\beta_1 = \varepsilon^5$; $\beta_2 = 2$; $\beta_3 = \varepsilon^2$; $\beta_4 = \varepsilon^7$.

Для второго сопряженного корня $\varepsilon_4 = \varepsilon^6$ коэффициенты β_i' являются коэффициентами β_i, возведенными в степень $p = 3$.

Покажем, что по любому m-элементному безошибочному участку рекурсивной последовательности $\{s\}$ можно определить информационные элементы.

Пусть будет выделен участок $(s_4 s_5 s_6 s_7) = (0\varepsilon^6 1\varepsilon^5)$. Тогда информационные элементы будут равны:

– для $\varepsilon_1 = \varepsilon$:

$$A = \varepsilon^{-4}\left(0 \cdot \alpha_1 + \varepsilon^6\alpha_2 + 1 \cdot \alpha_3 + \varepsilon^5\alpha_4\right) = \varepsilon^4\left(\varepsilon + \varepsilon^2 + 1\right) = 2 \cdot 2 = 1;$$

– для $\varepsilon_2 = \varepsilon^3$:

$$B = \left(\varepsilon^3\right)^{-4}\left(0 \cdot \alpha_1' + \varepsilon^6\alpha_2' + 1 \cdot \alpha_3' + \varepsilon^5\alpha_4'\right) = \varepsilon^{-4}\left(\varepsilon^6 \cdot \varepsilon + 1 \cdot \varepsilon^6 + \varepsilon^5 \cdot \varepsilon\right) = 1;$$

– для $\varepsilon_3 = \varepsilon^2$:

$$C = \left(\varepsilon^2\right)^{-4}\left(0 \cdot \beta_1 + \varepsilon^6\beta_2 + 1 \cdot \beta_3 + \varepsilon^5\beta_4\right) =$$

$$= 2\varepsilon^6 + \varepsilon^2 + \varepsilon^4 = 1 + 2\varepsilon + 1 + 2\varepsilon + 2 = 1 + \varepsilon = \varepsilon^7;$$

– для $\varepsilon_4 = \varepsilon^6$:

$$D = (\varepsilon^6)^{-4}(0 \cdot \beta_1' + \varepsilon^6\beta_2' + 1 \cdot \beta_3' + \varepsilon^5\beta_4') = 2 \cdot \varepsilon^6 + \varepsilon^6 + \varepsilon^2 = \varepsilon^2.$$

Подвергнем последовательность $\{s\}$ децимации с индексом $q = p = 3$ и получим последовательность:

$$\{u\}_3 = (u_0 u_1 u_2 u_3 u_4 u_5 u_6 u_7) = (s_0 s_3 s_6 s_1 s_4 s_7 s_2 s_5) = (1\varepsilon^2 1\varepsilon 0\varepsilon^5 1\varepsilon^6).$$

Возьмем m-элементный участок $(u_1 u_2 u_3 u_4) = (\varepsilon^2 1\,\varepsilon 0)$ и найдем по нему коэффициенты A', B', C' и D':

– для $\varepsilon_1 = \varepsilon$:

$$A' = \varepsilon^{-1}\left(\varepsilon^2\alpha_1 + 1 \cdot \alpha_2 + \varepsilon\alpha_3\right) = \varepsilon^{-1}\left(\varepsilon^4 + \varepsilon^3 + \varepsilon^3\right) = 1 = B;$$

– для $\varepsilon_2 = \varepsilon^3$:

$$B' = \varepsilon^{-3}\left(\varepsilon^2\alpha_1' + 1\alpha_2' + \varepsilon\alpha_3'\right) = \varepsilon^5\left(1 + \varepsilon + \varepsilon^7\right) = \varepsilon^5 \cdot \varepsilon^3 = 1' = A;$$

– для $\varepsilon_3 = \varepsilon^2$:

$$C' = \varepsilon^{-2}\left(\varepsilon^2\beta_1 + 1\cdot\beta_2 + \varepsilon\beta_3\right) = \varepsilon^{-2}\left(\varepsilon^7 + 2 + \varepsilon^3\right) = 2\varepsilon^6 = 1 + 2\varepsilon = \varepsilon^2 = D;$$

– для $\varepsilon_4 = \varepsilon^6$:

$$D' = \varepsilon^{-6}\left(\varepsilon^2\beta_1' + 1\cdot\beta_2' + \varepsilon\beta_3'\right) = \varepsilon^2\left(\varepsilon + 2 + \varepsilon^7\right) = 2\varepsilon^3 = 1 + \varepsilon = \varepsilon^7 = C.$$

Как видим, пара элементов A' и B' является циклически сдвинутыми на один шаг элементами A и B, т. е. $A' = B;\ B' = A$.

Аналогично пара элементов C' и D' является также циклически сдвинутыми на один шаг элементами C и D, т. е. $C' = D;\ D' = C$.

Таким образом, применение децимации приводит к усилению корректирующих свойств кода при мажоритарном декодировании принятой последовательности $\{h\}$ циклического кода РСЭ над полем $GF(p^k)$

Представление комбинаций циклических кодов рекуррентными последовательностями над полем $GF(p^k)$ и применение децимаций с индексами $q = p^j$, где j = 1, 2, …. (k – 1), позволяют осуществить мажоритарное декодирование с простой реализацией декодера. При этом сложность реализации декодера практически не зависит от кратности исправляемых ошибок.

ВЫВОДЫ

1. Дуальные циклические коды БЧХ и Рида – Соломона (недвоичные коды БЧХ) могут быть представлены линейными рекуррентными последовательностями $\{s\}$ над полем $GF(p^k)$ с характеристическим многочленом $P(x)$ степени m.

2. Представление комбинаций циклических кодов БЧХЭ и РСЭ рекуррентными последовательностями длины $n = p^k - 1$ позволяет использовать для их декодирования двойственный базис.

3. Обработка комбинаций циклических кодов БЧХЭ и РСЭ по m-элементным участкам позволяет реализовать мажоритарный принцип декодирования.

4. Для кодов РСЭ, так же как и для кодов БЧХ, можно выбрать такой характеристический многочлен $P(x)$, что децимированные комбинации кода, как рекуррентные последовательности, будут сохранять исходные свойства рекуррентности.

5. Применение децимаций над рекуррентной последовательностью $\{s\}$ и обработка децимированных последовательностей с помощью двойственного базиса обеспечивают более высокую степень достоверности по сравнению с традиционными алгоритмами декодирования, в том числе и по алгоритму Мэттсона – Соломона.

6. Кодирующие и декодирующие устройства циклических кодов БЧХЭ и РСЭ наиболее рационально строить на базе модулярных регистров сдвига с обратными связями.

7. Систематические циклические коды, представленные рекуррентными последовательностями, могут быть построены как укороченные комбинации, для мажоритарного декодирования которых применим двойственный базис.

Контрольные вопросы по разделу 1

1. Охарактеризуйте особенности эквивалентных циклических кодов БЧХ и Рида – Соломона.

2. Дайте определения степенному и двойственному базисам поля $GF(2^m)$.

3. Что собой представляет функция-след элемента поля ε^i в поле $GF(p^k)$?

4. Какой многочлен $p(x)$ степени m является примитивным над полем $GF(2^m)$?

5. Какую степень будет иметь примитивный многочлен $p(x)$ над полем $GF(2^4)$?

6. Одним из корней примитивного многочлена $p(x)$ будет элемент ε^3, принадлежащий полю $GF(2^4)$. Назовите другие элементы поля, являющиеся корнями многочлена $p(x)$, и их степень.

7. Пусть рекуррентная последовательность $\{s\} = (s_0.\ s_1.\ s_2.\ldots\ s_{N-1})$ с периодом $N = 2^4 - 1$ удовлетворяет рекуррентному уравнению $s_i + s_{i-3} + s_{i-4} = 0 \pmod 2$. Определите характеристический многочлен, порождающий последовательность $\{s\}$.

8. Задан характеристический примитивный многочлен $p(x) = p_0\ x^4 + p_1x^3 + p_2x^2 + p_3x + p_4 = x^4 + x^3 + 1$. Составить один полный период рекуррентной последовательности и записать соответствующее ей рекуррентное уравнение.

9. Какой принцип мажоритарного декодирования циклических кодов БЧХЭ и РСЭ на основе двойственного базиса над полем $GF(p^k)$?

10. Какие индексы децимации комбинации циклического кода как рекуррентной последовательности $\{s\} = (s_0.\ s_1.\ s_2.\ldots.\ s_{N-1})$ длины $N = 2^4 - 1$ можно выбрать для мажоритарного декодирования кода на основе двойственного базиса?

11. Дайте характеристику двоичному эквидистантному циклическому коду с длиной комбинации $n = 15$.

12. Пусть начальный элемент s_0 двоичной комбинации как рекуррентной последовательности циклического эквидистантного кода (15.4), равен функции-след от элемента поля ε^3, т. е., $s_0 = \mathrm{T}(\varepsilon^3)$, где ε – первообразный элемент поля и корень порождающего поле и рекуррентную последовательность примитивного многочлена $p(x) = p_0 x^4 + p_1 x^3 + p_2 x^2 + p_3 x + p_4 = x^4 + x + 1$. Сформируйте по заданному начальному элементу поля $GF(2^4)$ всю кодовую комбинацию длины $n = 15$.

13. Сформулируйте пошаговый алгоритм мажоритарного декодирования циклических кодов на основе двойственного базиса.

14. Поясните, нужно ли при мажоритарном декодировании комбинаций циклических кодов БЧХЭ и РСЭ как рекуррентных последовательностей на основе двойственного базиса, определять номера ошибочных позиций для исправления ошибок в комбинации.

2. КОДЫ С МАЛОЙ ПЛОТНОСТЬЮ ПРОВЕРОК НА ЧЕТНОСТЬ

2.1. Определение кода с малой плотностью проверок на четность и его основные свойства

В 1962 г. Роберт Галлагер [5] предложил новый класс линейных кодов с исправлением ошибок, названный им «low – density parity – check codes», что в русском переводе было представлено как «коды с малой плотностью проверок на четность». Этот класс кодов известен специалистам как коды Галлагера. В данном учебном пособии для этого класса кодов используется название МППЧ коды. По мнению Галлагера разработанный им метод кодирования приближает решение задачи поиска метода кодирования, о котором говорится в теореме кодирования для канала с шумами, сформулированной К. Э. Шенноном в 1948 г., а именно – предлагаемый ансамбль кодов обеспечит получение высоких скоростей передачи и сколь угодно малые вероятности ошибки и при этом уменьшит большое время вычислений, требуемых для декодирования принятой при наличии шума информации и сократит сложность оборудования.

Автор представил МППЧ коды как (n, J, K) коды, являющиеся нулевым пространствомпроверочной матрицы $\boldsymbol{H}$ размерности $(n - k) \times n$, в которой каждый столбец содержит J единиц, а каждая строка – K единиц.

Галлагер предполагал, что число единиц в столбцах и строках проверочной матрицы $\boldsymbol{H}$ должно быть небольшим (J и K намного меньше n). Поскольку $K(n - k) = Jn$. то скорость передачи кода R задается равенством

$$R = 1 - J/K. \qquad (2.1)$$

В проводимых им исследованиях использовались коды с длиной блока, равной 126, 252, 504, 1008 бит с значениями $J = 3$ или 4, $K = 6$ или 9 при скости передачи кода $k/n = 1/3, 1/2, 2/3$.

Для МППЧ кодов принято оценивать корректирующие свойства не для конкретного кода, а для всего ансамбля (n, J, K) кодов. Галлагером было доказано, что минимальное кодовое расстояние МППЧ кодов растет линейно с длиной кода. В более поздних исследованиях МППЧ кодов показано, что МППЧ коды могут быть так же близки к пределу Шеннона, как и турбокоды, а нерегулярные МППЧ коды могут превосходить турбокоды при примерно одинаковых длинах кодовых блоков.

Нерегулярными названы такие МППЧ коды, у которых параметры J и K – непостоянны. Известно [7], что лучший среди двоичных кодов скорости 1/2 с длиной блока 10 000 000 есть код МППЧ, достигший 0,0045 дБ от предела Шеннона для случая передачи сигналов по каналу с АБГШ, который определяет граничное значение отношения энергии бита к спектральной плотности помехи $E_b/N_0 = 1/\log_2 e = 0{,}693 = -1{,}59$ дБ, меньше которого

невозможно исправление ошибок с использованием помехоустойчивых кодов. Высокая эффективность кодов МППЧ привела к их использованию вместо турбокодов в стандартах спутниковой передачи данных для цифрового ТВ и в стандартах для цифрового наземного ТВ вещания, а также в высокоскоростных системах мобильной связи.

Процедуры кодирования и декодирования для введенного класса кодов Галлагер строит на основе проверочных соотношений, заложенных в строках проверочной матрицы. Для исправления ошибок Галлагер применяет мажоритарный метод декодирования, предложенный в 1954 г. Ридом. Обеспечение высокой эффективности мажоритарного метода исправления ошибок достигается высокой степенью независимости проверок и их развитостью (многоярусностью). Это потребовало большого разноса элементов кодовых блоков, охваченных проверочным соотношением по длине блока, и увеличения длин кодовых блоков, что и вызвало малое число единиц в строках проверочной матрицы при увеличении их длин. При этом важной характеристикой проверочной матрицы является отсутствие в ней циклов определенного размера. Под циклом длины 4 понимают образование в проверочной матрице прямоугольника, в углах которого находятся единицы. Циклы большей длины (6, 8, 10 и т. д.) можно выявить, если в проверочной матрице можно построить граф, вершинами которого являются единицы, а ребра – горизонтальные и вертикальные линии, соединяющие вершины. Наличие циклов отражает связность, т. е. зависимость проверочных векторов, составляющих строки проверочной матрицы. Отсутствие цикла длины 4 проверяют по результату вычисления каждого попарного скалярного произведения столбцов (или строк) проверочной матрицы. Если скалярное произведение каждой пары столбцов (или строк) проверочной матрицы дает результат не более 1, то циклы длины 4 отсутствуют. Наличие циклов большей длины определяется минимальной длиной цикла при представлении проверочной матрицы кода МППЧ в виде графа Таннера. Известны методы поиска и удаления циклов минимальных длин в проверочных матрицах МППЧ кодов. На рис. 2.1 приводится проверочная матрица кода Хемминга (7, 4) с указанием циклов длины 4.

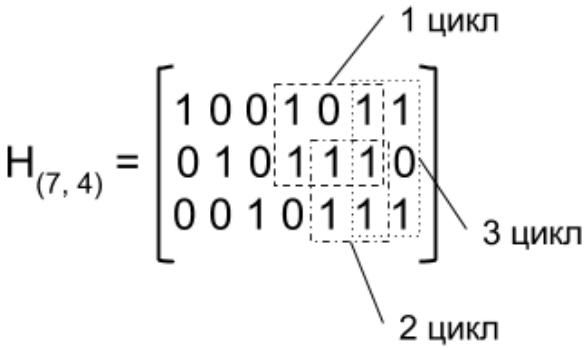

Рис. 2.1. Проверочная матрица кода Хемминга (7, 4)
с указанием циклов длины 4

2.2. Процедуры декодирования для кодов МППЧ

Галлагер разработал две процедуры декодирования для кодов МППЧ:

– итеративное декодирование с жестким решением – алгоритм с перевертыванием бита;

– итеративное вероятностное декодирование – алгоритм распространения доверия.

2.2.1. *Итеративное декодирование с жестким решением – алгоритм с перевертыванием бита*

Декодирование производится посимвольно мажоритарным методом с использованием проверочных соотношений, представленных строками проверочной матрицы. В соответствии с правилом формирования проверочной матрицы каждый символ кодовой комбинации МППЧ кода присутствует ровно в J проверочных соотношениях, каждое из которых охватывает K символов кодовой комбинации, при общем числе проверочных соотношений равном $n - k$. Для каждой совокупности K символов из J проверочных соотношений только один кодовый символ входит в каждое проверочное соотношение, а остальные $K - 1$ символов – различные, выбранные из различных частей кодовой комбинации. Связь между кодовыми символами и проверочными множествами Галлагер отобразил в виде дерева проверочных множеств кода (рис. 2.2).

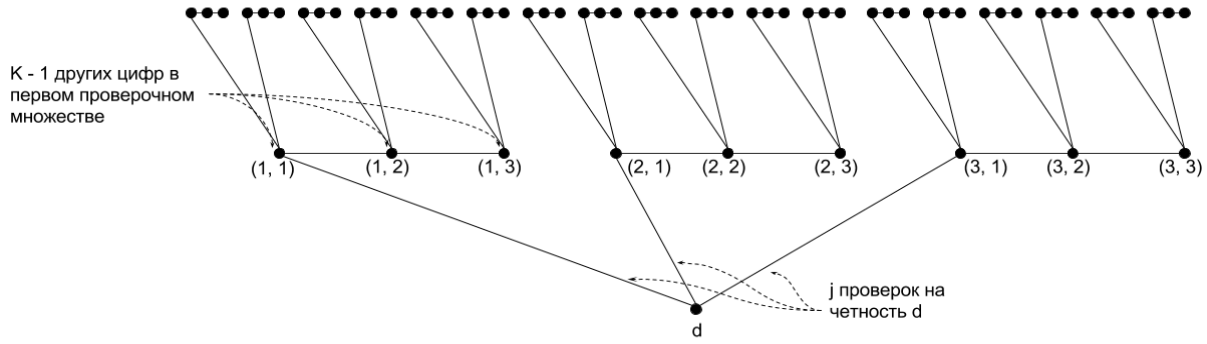

Рис. 2.2. Дерево проверочных множеств кода

Процедура мажоритарного декодирования выполняется следующим образом. Анализируется совокупность J проверочных соотношений, связанных с первым символом принятой кодовой комбинации. Из каждого проверочного соотношения вычисляется значение первого символа и по большинству совпадений результатов вычислений определяется значение первого символа в декодируемой комбинации. Последующие вычисления выполняются с использованием вновь полученных значений символов. Аналогичным образом вычисляются значения всех остальных символов

кодовой комбинации. Процедура декодирования продолжается до тех пор, пока в последних n вычислениях не будет сделано никаких изменений. При большом числе J и в зависимости от качества канала можно вводить порог числа совпадений вычисленных значений анализируемого символа для принятия решения по его значению. Порог может меняться на каждом этапе из n вычислений процедуры декодирования [8].

Пример 2.1. В работе Галлагера приводится проверочная матрица кода (20, 5) с $J = 3$ и $K = 4$, представленная на рис. 2.3, на основе которой можно проиллюстрировать выполнение процедуры мажоритарного декодирования. Пусть кодер выдал в канал кодовую комбинацию $E = (e_1, e_2, \ldots e_{20})$ кода (20, 5), состоящую из одних нулей, а в декодер поступила кодовая комбинация с ошибками в первых четырех символах. Выполним процедуру декодирования этой комбинации с применением алгоритма перевертывания бита. В соответствии с алгоритмом декодирования процедура декодирования содержит $n + \Delta$ шагов. Предполагается, что для исправления ошибок потребуется Δ шагов, необходимых для исправления анализируемых символов, после чего выполняется еще n шагов, подтверждающих завершение процедуры исправления ошибок. На каждом шаге выполняется 3 вычисления анализируемого символа, на основе которых принимается мажоритарное решение о его значении.

$$\begin{pmatrix}
1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1\\
-&-&-&-&-&-&-&-&-&-&-&-&-&-&-&-&-&-&-&-\\
1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&0&0&0&0\\
0&1&0&0&0&1&0&0&0&1&0&0&0&0&0&0&1&0&0&0\\
0&0&1&0&0&0&1&0&0&0&0&0&0&1&0&0&0&1&0&0\\
0&0&0&1&0&0&0&0&0&0&1&0&0&0&1&0&0&0&1&0\\
0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1\\
-&-&-&-&-&-&-&-&-&-&-&-&-&-&-&-&-&-&-&-\\
1&0&0&0&0&1&0&0&0&0&0&1&0&0&0&0&0&1&0&0\\
0&1&0&0&0&0&1&0&0&0&1&0&0&0&0&1&0&0&0&0\\
0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&0&1&0\\
0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&1&0&0&0\\
0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1
\end{pmatrix}$$

Рис. 2.3. Проверочная матрица кода (20, 5) с $J = 3$ и $K = 4$

Ход процедуры декодирования представлен в табл. 2.1.

Таблица 2.1

Шаги итерации	Анализи-руемые символы	Проверочные соотношения	Результаты вычислений	Решение декодера
1	e_1	$e_1 = e_2 + e_3 + e_4$ (1-я строка)	1	0
		$e_1 = e_5 + e_9 + e_{13}$ (6-я строка)	0	
		$e_1 = e_6 + e_{12} + e_{18}$ (11-я строка)	0	
2	e_2	$e_2 = e_1 + e_3 + e_4$ (1-я строка)	0	0
		$e_2 = e_6 + e_{10} + e_{17}$ (7-я строка)	0	
		$e_2 = e_7 + e_{11} + e_{16}$ (12-я строка)	0	
3	e_3	$e_3 = e_1 + e_2 + e_4$ (1-я строка)	1	0
		$e_3 = e_7 + e_{14} + e_{18}$ (8-я строка)	0	
		$e_3 = e_8 + e_{13} + e_{19}$ (13-я строка)	0	
4	e_4	$e_4 = e_1 + e_2 + e_3$ (1-я строка)	0	0
		$e_4 = e_{11} + e_{15} + e_{19}$ (9-я строка)	0	
		$e_4 = e_9 + e_{14} + e_{17}$ (19-я строка)	0	
5	e_5	$e_5 = e_6 + e_7 + e_8$ (2-я строка)	0	0
		$e_5 = e_1 + e_9 + e_{13}$ (6-я строка)	0	
		$e_5 = e_{10} + e_{15} + e_{20}$ (20-я строка)	0	

Из табл. 2.1 и условия решаемой в данном примере задачи видно, что исправление ошибок завершилось на третьем шаге декодирования, т. е. $\Delta = 3$. В соответствии с алгоритмом декодирования декодер выполнит еще $n = 20$ шагов, которые подтвердят отсутствие изменений в анализе значений остальных и уже исправленных символов принятой кодовой комбинации.

2.2.2. *Итеративное декодирование с мягким решением – алгоритм распространения доверия*

Процедура декодирования основывается на последовательном повышении надежности принятых канальных значений символов кодового слова. Предположим, что кодовые комбинации (n, J, K) кода равновероятны. Пользуясь обозначениями рис. 2.2 Галлагер построил итерационный процесс вычисления вероятности того, что значение некоторого символа d принятой кодовой комбинации на некоторой итерации равно 1 при условии того, что известны все принятые символы на рассматриваемой итерации $\{y\}$ и произошло событие S, заключающееся в том, что принятые символы

удовлетворяют J проверочным соотношениям, контролирующим символ d. Эта вероятность обозначена

$$P_r[x_d = 1/\{y\}, S\,].$$

Процедура декодирования при рассмотренных условиях основывается на следующей теореме, сформулированной и доказанной Р. Галлагером.

Теорема Галлагера. Пусть P_d есть вероятность того, что переданный символ в позиции d равен 1 при условии, что известен принятый символ в той же позиции, и пусть P_{il} – такая же вероятность для l-го символа i-го проверочного множества первого яруса рис. 2.2. Пусть символы независимы, а событие S состоит в том, что символы удовлетворяют J проверочным соотношениям, контролирующим символ d. Тогда

$$\frac{P_r\left[x_d = 0/\{y\}, S\right]}{P_r\left[x_d = 1/\{y\}, S\right]} = \frac{1-P_d}{P_d}\prod_{i=1}^{j-1}\left[\frac{1+\prod_{l=1}^{k-1}\left(1-2P_{il}\right)}{1-\prod_{l=1}^{k-1}\left(1-2P_{il}\right)}\right]. \qquad (2.2)$$

Комментарий к теореме

1. По определению условных вероятностей имеем

$$\frac{P_r\left[x_d = 0/\{y\}, S\right]}{P_r\left[x_d = 1/\{y\}, S\right]} = \left(\frac{1-P_d}{P_d}\right)\left(\frac{\Pr\left(S/x_d = 0, \{y\}\right)}{\Pr\left(S/x_d = 1, \{y\}\right)}\right).$$

2. $P_r\left(S/x_d = 0, \{y\}\right) = \prod_{i=1}^{j}\frac{1+\prod_{l=1}^{k-1}\left(1-2P_{il}\right)}{2}$.

3. $P_r\left(S/x_d = 1, \{y\}\right) = \prod_{i=1}^{j}\frac{1-\prod_{l=1}^{k-1}\left(1-2P_{il}\right)}{2}$.

4. В первом произведении берется $J-1$сомножителей, поскольку проверочное множество, содержащее символ d, не используется.

Процедура декодирования формулируется следующим образом.

Для каждого символа и каждого из $J-1$ проверочных множеств, содержащих этот символ, вычисляется по выражению (2.2) вероятность того, что передана 1 при условии того, что известны принятые символы в $(J-1)$-м проверочном множестве. Таким образом, каждому символу соответствует J различных вероятностей, каждая из которых не учитывает одно проверочное множество. Эти вероятности затем используются в выражении (2.2) для

вычисления совокупности вероятностей второго порядка. Вероятность, связываемая с некоторым символом при вычислении вероятности символа d, должна быть величиной, найденной на первой итерации, и не должна учитывать проверочное множество, содержащее символ d.

При успешном декодировании вероятности, соответствующие каждому символу, стремятся либо к 1, либо к 0. Метод справедлив, пока используются итерации, для которых не нарушается предположение о независимости проверок. Это предположение нарушается, когда в дереве образуются петли, характеризуемые циклами в проверочной матрице. Можно, однако, пренебречь отсутствием независимости, сделав предположение, что зависимости ничтожны и до некоторой степени компенсируют друг друга. Для практического вычисления вероятностей в сформулированной теореме ее автор преобразовал равенство (2.2) с помощью логарифмических отношений правдоподобий:

$$\ln\frac{1-P_d}{P_d}=\alpha_d\beta_d,$$

$$\ln\frac{1-P_{il}}{P_{il}}=\alpha_{il}\beta_{il},$$

$$\ln\frac{\Pr\left[x_d=0/\{y\},S\right]}{\Pr\left[x_d=1/\{y\},S\right]}=\alpha'_d\beta'_d,$$

где $\alpha-$ знак, а $\beta-$ абсолютная величина логарифмического отношения правдоподобий. После некоторых преобразований выражение (2.2) принимает следующий вид:

$$\alpha'_d\beta'_d=\alpha_d\beta_d+\sum_{i=1}^{j}\left\{\left(\prod_{l=1}^{k-1}\alpha_{il}\right)f\left[\sum_{l=1}^{k-1}f\left(\beta_{il}\right)\right]\right\}, \qquad (2.3)$$

где $f(\beta)=\ln\dfrac{e^{\beta}+1}{e^{\beta}-1}$.

Данное выражение в современной редакции вычисляется через гиперболический котангенс.

Исходными данными для расчетов по формуле (2.3) являются логарифмические отношения правдоподобий α и β, поступающие на вход декодера от демодулятора для каждого принятого символа, по которым декодер вычисляет значение $f(\beta)$, т. е. выполняет самую правую операцию в равенстве (2.3). Все остальные вычисления выполняются последовательно, справа налево. Вычисления логарифмических отношений правдоподобий могут выполняться параллельно. Современная процедура итеративного декодирования кодов Галлагера выполняется на основе работ Р. Таннера и Д. Маккая [7]. Для любого линейного (n, k) кода существует двудольный

граф, определяемый видом проверочной матрицы **H**. Этот граф известен как граф Таннера. Вершины графа Таннера для некоторого линейного (n, k) кода ассоциируются с переменными двух типов:

– n *кодовых* (*символьных*) *вершин*, т. е. вершин соответствующих символам кодовой комбинации;

– $n–k$ *проверочных вершин*, соответствующих проверочным уравнениям. Введение вершин-состояний превращает граф Таннера в фактор-граф, т. е. графическую вероятностную модель декодера, в которой зависимости между случайными величинами представлены в виде графа, вершины которого соответствуют случайным переменным, а ребра – вероятностным связям между случайными величинами.

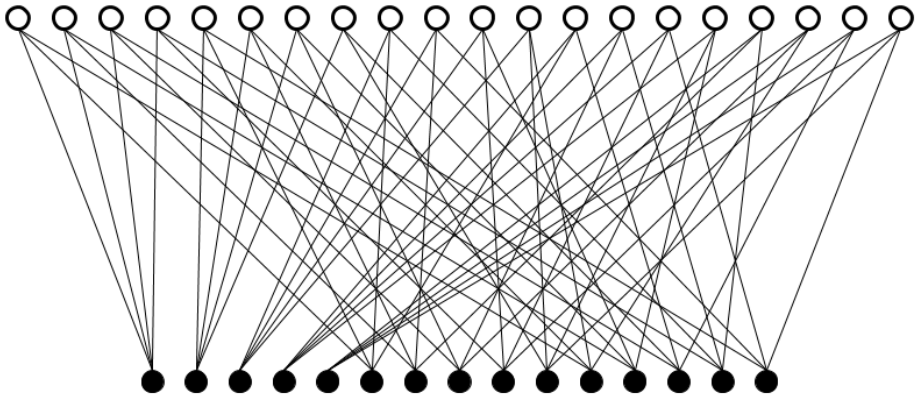

Рис. 2.4. Двудольный граф Таннера для кода (20, 5).
Здесь верхние узлы – символьные,
а нижние – проверочные

Описание алгоритма распространения доверия

Задача декодирования – максимизировать условную вероятность

$$P(C_m/Y),$$

где C_m – кодовое слово, Y – блок символов, поступающих с выхода канала на вход декодера. Процедура декодирования изложена в соответствии с работой [12].

Начальные установки

Каждому принятому символу l приписывается логарифмическое отношение правдоподобия $L(c_l) = \lg \dfrac{P\left(c_l = 0 / Y\right)}{P\left(c_l = 1 / Y\right)}$ соответствующих символов принятого мягкого слова. Затем декодер осуществляет итерации, каждая из которых состоит из трех шагов.

Шаг 1. Пересчет проверочных узлов (горизонтальная проверка).

Для каждого ненулевого элемента проверочной матрицы вычислить логарифмическое отношение правдоподобия, формируемое проверочным соотношением (узлом), к которому принадлежит данный символ

$$L\left(r_{m,l}\right) = 2\text{th}^{-1}\left(\prod_{l'\in\xi(m)\setminus l} th\left(\frac{1}{2}L\left(q_{m,l'}\right)\right)\right), \qquad (2.4)$$

где $r_{m,l}$ – вероятность того, что m-е проверочное соотношение, в котором участвует символ l, удовлетворяется,

$\zeta(m)$ – множество символов, участвующих в m-й проверке,

запись $l' \in \zeta(m) \setminus l$ означает, что l' изменяется по всему множеству $\zeta(m)$ кроме номера l,

$q_{m,l}$ – вероятность того, что значение символа l удовлетворяется по всем $\mu(l)$ проверочным соотношениям, в которых участвует этот символ,

$th(x)$ – гиперболический тангенс, $th(–x) = –th(x)$.

Для первой итерации $L(q_{m,l})$ инициализируется как $L(c_l)$.

Шаг 2. Пересчет символьных узлов (вертикальная проверка).

Для каждого ненулевого элемента проверочной матрицы вычислить

$$\left(q_{m,l}\right) = L\left(c_l\right) + \sum_{m'\in\mu(l)\setminus m} L\left(r_{m,l}\right). \qquad (2.5)$$

Запись $m' \in \mu(l) \setminus m$ означает, что суммирование выполняется по всему множеству проверочных соотношений $\mu(l)$, кроме соотношения с номером m.

Шаг 3.Выполнение пробного декодирования.

Для каждого принятого символа вычислить

$$L\left(Q_{m,l}\right) = L\left(c_l\right) + \sum_{m\in\mu(l)} L\left(r_{m,l}\right). \qquad (2.6)$$

На основе полученных мягких решений $L(Q_{m,l})$ принимаются жесткие решения:

$c_l = 0$, если $L(Q_{m,l}) > 0$ или

$c_l = 1$, если $L(Q_{m,l}) < 0$.

Если все проверки выполняются, то декодирование заканчивается. В противном случае следует вернуться к шагу 1.Таким образом, рассмотренная процедура декодирования представляется как итеративный обмен сообщениями (message passing метод) между символьными и проверочными узлами графа кода.

Пример 2.2. Пусть переданная комбинация рассмотренного выше кода (20, 5) $E = (e_1, e_2, \ldots e_{20},)$ состоит из одних нулей. Для простоты изложения сути метода декодирования с *итеративным распространением доверия* последовательность вычисленных декодером отношений правдоподобия $L(l_i)$ принятых символов мягкого кодового слова $E_м$ имеет вид: $L(l_1) = L(l_2) = –0{,}86$, а для всех остальных $i = 3,\ldots, 20$ величина $L(l_i) = 0{,}86$. Затем декодер осуществляет итеративное декодирование, которое начинается с инициализации (начальная установка) и последовательности итераций, каждая итерация состоит из трех шагов.

Начальные установки

Каждому принятому символу l приписывается логарифмическое отношение правдоподобия $L(c_l) = \lg \dfrac{P(c_l = 0 / Y)}{P(c_l = 1 / Y)}$ соответствующих символов принятого мягкого слова, т. е. $L(l_1) = L(l_2) = –0{,}86$, а для всех остальных $i = 3,\ldots, 20$ величина $L(l_i) = 0{,}86$.

Итерация 1.

Шаг 1. Пересчет проверочных узлов

Для каждого ненулевого элемента проверочной матрицы l вычисляется сообщение, посылаемое m-м проверочным узлом об оценке того, что m-е проверочное соотношение, в котором участвует символ l, удовлетворяется. Расчет производится по формуле (2.4). В этой формуле значение $th(1/2L(\pm 0{,}86)) = \pm 0{,}41$, а оценка $L(r_{m,l}) = \pm 28{,}58$. Значения $L(r_{m,l})$ для каждого ненулевого символа проверочной матрицы приводятся в табл. 2.2, где указан лишь знак $L(r_{m,l})$.

Таблица 2.2

Вычисление $L(r_{m,l})$

1 строка	1 –	2 –	3 +	4 +
2 строка	5 +	6 +	7 +	8 +
3 строка	9 +	10 +	11 +	12 +
4 строка	13 +	14 +	15 +	16 +
5 строка	17 +	18 +	19 +	20 +
6 строка	1 +	5 –	9 –	13 –
7 строка	2 +	6 –	10 –	17 –
8 строка	3 +	7 +	14 +	18 +
9 строка	4 +	11 +	15 +	19 +
10 строка	8 +	12 +	16 +	20 +
11 строка	1 +	6 –	12 –	18 –
12 строка	2 +	7 –	11 –	16 –
13 строка	3 +	8 +	13 +	19 +
14 строка	4 +	9 +	14 +	17 +
15 строка	5 +	10 +	15 +	20 +

Шаг 2. Пересчет символьных узлов.

Для каждого ненулевого элемента проверочной матрицы вычисляется сообщение, посылаемое l-м символьным узлом к m-му проверочному, как сумма всех сообщений, поступивших от других проверочных узлов, и канального решения для кодового символа $L\left(q_{m,l}\right)=L\left(c_l\right)+\sum_{m'\in\mu(l)\setminus m} L\left(r_{m,l}\right)$.

Результаты расчетов представлены в табл. 2.3, где для каждого ненулевого элемента проверочной матрицы приводится лишь значение $\sum_{m'\in\mu(l)\setminus m} L(r_{m,l})$, в виде двух слагаемых, а величина $L(c_l)$ опущена в силу ее малого значения. В табл. 2.3 знаками «+» и «–» обозначены те же самые значения $L(r_{m,l})$, что и в табл. 2.2.

Таблица 2.3

Вычисление $L(q_{m,l})$

1 строка	1 + +	2 + +	3 + +	4 + +
2 строка	5 – +	6 – –	7 + –	8 + +
3 строка	9 – +	10 – +	11 + –	12 + –
4 строка	13 – +	14 + +	15 ++	16 + –
5 строка	17 – +	18 + –	19 ++	20 + +
6 строка	1 – +	5 + +	9 + +	13 + +
7 строка	2 – +	6 + –	10 + +	17 + +
8 строка	3 + +	7 + –	14 + +	18 + –
9 строка	4 + +	11 + –	15 + +	19 + +
10 строка	8 + +	12 + –	16 + –	20 + +
11 строка	1 – +	6 + –	12 + +	18 + +
12 строка	2 – +	7 + +	11 + +	16 + –
13 строка	3 + +	8 + +	13 + –	19 + +
14 строка	4 + +	9 + –	14 + +	17 + +
15 строка	5 + –	10 + –	15 + +	20 + +

Шаг 3. Выполнение пробного декодирования.

Для каждого принятого символа необходимо вычислить итоговый результат декодирования итерации: $L\left(Q_{m,l}\right)=L\left(c_l\right)+\sum_{m\in\mu(l)} L\left(r_{m,l}\right)$.

Итоговые результаты декодирования по итерации 1 представлены в табл. 2.4. в том же виде, что и в табл. 2.1, 2.2, 2.3.

Таблица 2.4

Вычисление $L(Q_{m,l})$

1 – + +	2 – + +	3 + + +	4 + + +
5 + – +	6 + – –	7 + + –	8 + + +
9 + – +	10 + – +	11 + + –	12 + + –
13 + – +	14 + + +	15 +++	16 + + –
17 + – +	18 + + –	19 + ++	20 + + +

Вычисленное жесткое решение по сформированным мягким в табл. 2.4 дает следующее значение принятой комбинации: (00000100000000000000). Проверка на соответствие полученной последовательности кодовой комбинации кода (20, 5) покажет, что сформированная двоичная последовательность не является кодовым словом данного кода, так как не будут выполняться проверочные соотношения, связанные с шестым символом, и декодер, сохранив вычисленные значения $L(l_i)$,$L(r_{m,l})$, $L(q_{m,l})$, приступит к выполнению следующей итерации декодирования.

Процесс обмена сообщениями между символьными и проверочными узлами повторяется многократно, несколько десятков или даже сотен раз. После последней итерации, когда, наконец, удовлетворяются все проверочные соотношения для каждого символа кодовой комбинации, знак итогового значения $L(Q_{m,l})$ определяет жесткое решение значения принятого символа, а его абсолютное значение является его надежностью.

2.2.3. *Модификация алгоритма распространения доверия – алгоритм «сумма наименьших»*

Декодирование по *алгоритму распространения доверия* является эффективным для каналов с мягким (непрерывным) выходом. Однако его сложность значительно выше, чем сложность жесткого декодирования. Сложность данного алгоритма в основном определяется сложностью формирования сообщений от проверочных узлов к символьным, так как требует выполнения достаточно сложных расчетов, связанных с гиперболическим тангенсом, гиперболическим котангенсом и умножением. А при формировании сообщений от символьных узлов к проверочным используются только операции сложения. При практической реализации декодера МППЧ кодов стремятся использовать алгоритмы, обладающие приемлемым качеством декодирования при простой реализации. К числу таких алгоритмов относят *алгоритм* «*сумма наименьших*» (min-sum). Алгоритм «сумма наименьших» использует те же шаги декодирования, что и алгоритм распространения доверия. Разница заключается только в том, что при вычислении сообщений от проверочных узлов к символьным используется более простое выражение:

$$L\left(r_{m,l}\right)=\prod_{l'\in\xi(m)\setminus l} signL\left(q_{m,l'}\right)\cdot\min_{l'\in\xi(m)\setminus l}\left|L\left(q_{m,l'}\right)\right|. \qquad (2.7)$$

Здесь $signL(q_{m,l'})$ – знак сообщения от l-го символа для m-й проверки, $\left|L(q_{m,l'})\right|$ – модуль (абсолютное значение) сообщения от l-го символа для m-й проверки. Остальные обозначения пояснялись выше. Выражение (2.7) является упрощенным представлением второго слагаемого выражения (2.3) в котором сумма $\sum_{l=1}^{K-1} f(\beta_{ij})$ представлена минимальным по абсолютному значению слагаемым, входящим в эту сумму. Суть алгоритма декодирования кода МППЧ «сумма наименьших» иллюстрируется двумя примерами [14].

Пример 2.3.

Для передачи сообщений используется код (8, 4) с минимальным кодовым расстоянием равным 3 и проверочной матрицей

$$\mathrm{H}=\begin{bmatrix}1&1&1&0&0&0&0&0\\0&0&0&1&1&1&0&0\\1&0&0&1&0&0&1&0\\0&1&0&0&1&0&0&1\end{bmatrix}.$$

Матрица H рассматриваемого кода (8, 4) содержит в каждой строке по 3 единицы, а число единиц в столбцах – различно, от одного до двух, т. е. данный код – нерегулярный. По каналу связи передается блок данных (10101111) двухполюсным сигналом (–1 1 –1 1 –1 –1 –1 –1). Помеха в канале представляет собою АБГШ с дисперсией $\sigma^2 = 0{,}5$. Принятый блок с мягкими значениями символов на выходе демодулятора имеет вид: (–0.8 0.7–0.9 0.7 0.5–1.5–2.4–1.2). LLR представление принятого блока равно: (–3.2 2.8 –3.6 2.8 2.0 –6.0 –9.6 –4.8), так как связь между значением сигнала на выходе демодулятора $\boldsymbol{y}$ и его *LLR* представлением в рассматриваемом случае имеет вид $L(y) = 2y/\sigma^2$. Пятый символ в блоке искажен.

Граф Таннера для рассматриваемого кода изображен на рис. 2.5. Процедура декодирования принятого блока в *LLR* представлении по алгоритму «сумма наименьших» приведена на рис. 2.6.

На рис. 2.5 граф Таннера для кода (8,4) представлен в общепринятом виде. На рис. 2.6 в графе Таннера для кода (8,4) в проверочных узлах графически представлены связи между символами блока данных, определенные содержанием проверочных соотношений, заложенных в строках матрицы *H*.

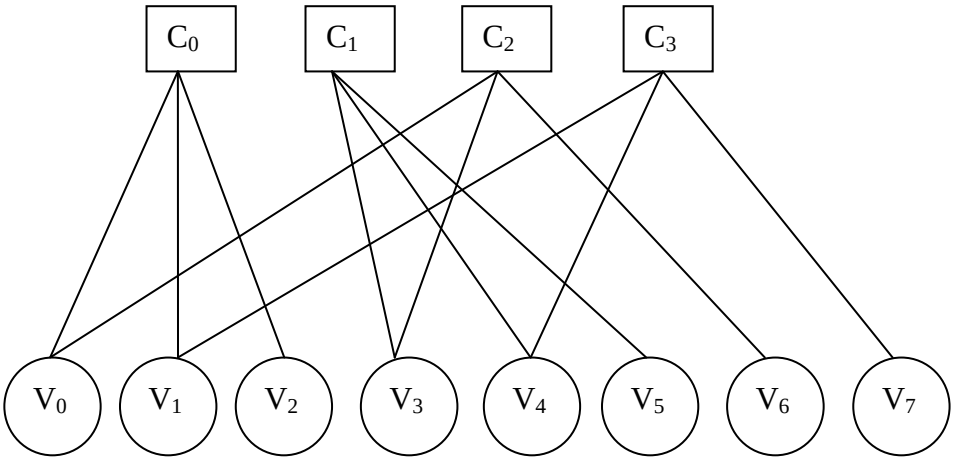

Рис. 2.5. Граф Таннера для кода (8, 4)

Декодирование выполнено за одну итерацию. На этапе ***инициализации*** выполняются начальные установки значений символьных узлов по значениям вычисленных *LLR* представлений принятых сигналов.

Первый шаг итерации – пересчет проверочных узлов на основе горизонтальных проверок, определяемых содержанием проверочных соотношений, заложенных в строках матрицы *H*.

Суть пересчета проверочных узлов заключается в формировании для каждого из *K* символов, входящего в некоторую горизонтальную проверку, нового внешнего по отношению к содержащемуся в мягком значении принятого сигнала априорного значения переданного символа, определяемого значениями остальных *K*–1 символов, входящих в данное проверочное соотношение. Так, например, в проверочном узле C_0, отображающем проверочное соотношение, соответствующее первой строке матрицы *H*:

$$V_0 + V_1 + V_2 = 0,$$

вычисляются новые внешние априорные значения для каждого из символов, входящих в эту проверку:

для V_0: $L(r_{00}) = -\min(|L(c_1)|, |L(c_2)|) = -\min(2.8, 3.6) = -2.8$;

для V_1: $L(r_{01}) = +\min(|L(c_0)|, |L(c_2)|) = +\min(3.2, 3.6) = +3.2$;

для V_2: $L(r_{02}) = -\min(|L(c_0)|, |L(c_1)|) = -\min(3.2, 2.8) = -2.8$.

На рис. 2.6 процедура вычисления $\min(a,b)$ обозначена как $\}a,b\{$. Подобный пересчет произведен на каждом проверочном узле C_i, а результаты пересчета отражены в фигурных скобках для каждого символьного узла V_j, связанного с проверочным узлом C_i.

Переданная комбинация	1	0	1	0	1	1	1	1
LLR представление принятых сигналов	-3,2	2,8	-3,6	2,8	2	-6	-9,6	-4,8
Инициализация (начальные установки)	-3,2	2,8	-3,6	2,8	2	-6	-9,6	-4,8
Пересчет проверочных узлов (горизонтальная проверка) Пересылка $C_i \rightarrow V_i$ Формула (2.7)	-3,2 2,8 -3,6	2,8 2 -6	-3,2 2,8 -9,6	2,8 2 -4,8				
Пересчет символьных узлов (вертикальная проверка) Пересылка $V_i \rightarrow C_i$ Формула (2.5)	C_0:-3,2-2,8=-6 C_2:-3,2-2,8=-6	C_0:2,8-2=0,8 C_3:2,8+3,2=6	C_0:-3,6+0=-3,6	C_1:2,8+3,2=6 C_2:2,8-2=0,8	C_1:2-2,8=-0,8 C_3:2-2,8=-0,8	C_1:-6+0=-6	C_2:-9,6+0=-9,6	C_3:-4,8+0=-4,8
Пробное декодирование а) Результирующее значение символа Формула (2.6)	-3,2-2,8-2,8= =-8,8	2,8-2+3,2= =4	-3,6-2,8=-6,4	2,8+3,2-2= 4	2-2,8-2,8=-3,6	-6+2=-4	-9,6-2,8=-12,4	-4,8+2=-2,8
б) Двоичное значение выхода декодера	1	0	1	0	1	1	1	1
в) Проверка на соответствие	Декодированная комбинация удовлетворяет проверочной матрице кода. Декодирование завершается							

Рис. 2.6. Процедура декодирования блока данных кода (8, 4)

На каждом шаге итерации процедуры декодирования готовятся данные для выполнения следующего шага итерации. Этот факт нашел отражение в понятии пересылки сообщений на каждом шаге итерации между уровнями графа Таннера как модели процесса декодирования. С этой точки зрения завершающим этапом пересчета проверочных узлов является пересылка от проверочных узлов к символьным новых априорных данных о значении символьных узлов. Данный процесс на рисунке отражен линиями, идущими вниз от проверочных узлов к символьным. ***Второй шаг итерации*** – пересчет символьных узлов на основе вертикальных проверок, определяемых единицами в столбцах проверочной матрицы H. На этом шаге повышается надежность оценки значения символьного узла за счет учета его значения по результатам всех проверочных соотношений, в которые входит каждый символ принятого блока данных. Так символьный узел V_0 входит в проверочные соотношения, определяемые первой и третьей строками матрицы H (проверочные узлы C_0 и C_2) и на основе сообщений от этих узлов определяется два значения узла V_0: по сообщению от C_0: $L(q_{00}) = L(c_0) + L(r_{00}) = -3{,}2 - 2{,}8 = -6$, по сообщению от C_2: $L(q_{20}) = L(c_0) + L(r_{20}) = -3{,}2 - 2{,}8 = -6$.

Подобный пересчет произведен для каждого символьного узла V_j, который участвует в двух различных проверках, т. е. кроме V_0 – для V_1, V_3 и V_4. Результаты выполненных расчетов рассматриваются как сообщения от символьных узлов к проверочным для выполнения последующих итераций декодирования, что подробнее будет рассмотрено в следующем примере, а также в последнем шаге декодирования данного примера – пробном декодировании. ***Третий шаг итерации*** – выполнение пробного декодирования. Этот шаг включает несколько этапов обработки сообщений, накопленных к данному моменту на каждом символьном узле о значении символа, соответствующего данному узлу. Содержание этапов: вычисление окончательного для данной итерации апостериорного мягкого значения сигнала для соответствующего символа блока данных, преобразование мягкого выхода в жесткое решение, проверка на соответствие последовательности битов сформированного блока данных проверочной матрице кода, принятие решения о завершении или продолжении процедуры декодирования. Выходное (апостериорное) мягкое значение каждого принятого символа $L(V_l)$ определяется по формуле (2,6) как сумма входного значения $L(c_l)$ и вычисленных на шаге горизонтальной проверки внешних априорных значений $L(r_{m,l})$ от всех проверочных узлов, с которыми связан рассматриваемый символ. Для символа V_0 мягкий выход равен: $-3{,}2 - 2{,}8 - 2{,}8 = -8{,}8$. Остальные значения $L(V_l)$ приведены на рис. 2.6.

По результатам горизонтальной и вертикальной проверок удалось повысить надежность оценки правдоподобия для всех символов блока данных, кроме V_5 и V_7. Надежность отношения правдоподобия для символа V_4 повысилась за счет внешних дополнений от остальных символов, входящих в проверки C_1 и C_3, что привело к исправлению ошибки. В свою очередь ошибочное значение V_4 повлияло на итоговые значения символов V_3 и V_5 (проверочное соотношение C_1), а также V_1 и V_7 (проверочное соотношение C_3). Символы V_5 и V_7 входят только в одну из горизонтальных проверок вместе с V_4, и вертикальная проверка никак не повлияла на их итоговое значение. Символы V_1 и V_3 входят в две горизонтальных проверки: в одну из них входит V_4, а в другую V_4 не входит. В следствие этого вертикальная проверка за счет внешних дополнений несколько повысила надежность оценки правдоподобия символов V_1 и V_3.

На основе полученных мягких решений $L(V_l)$ принимаются жесткие решения: $V_l = 0$, если $V_{ll}) > 0$, или $V_l = 1$, если $L(V_l) < 0$. Двоичное представление принятого блока данных представлено на рисунке и полностью соответствует переданному блоку. Соответствие исправленного блока коду проверяется вычислением синдрома. Синдром вычисляется суммированием столбцов проверочной матрицы, соответствующих единицам проверяемого блока:

$$S = \begin{pmatrix}1\\0\\1\\0\end{pmatrix} + \begin{pmatrix}1\\0\\0\\0\end{pmatrix} + \begin{pmatrix}0\\1\\0\\1\end{pmatrix} + \begin{pmatrix}0\\1\\0\\0\end{pmatrix} + \begin{pmatrix}0\\0\\1\\0\end{pmatrix} + \begin{pmatrix}0\\0\\0\\1\end{pmatrix} = \begin{pmatrix}0\\0\\0\\0\end{pmatrix} = 0.$$

Нулевой синдром свидетельствует о соответствии блока данных на выходе декодера используемому коду. Декодирование завершено.

В рассмотренном примере потребовалась всего одна итерация для выполнения процедуры декодирования. Представляет интерес процесс перехода от итерации к итерации. Для этого рассмотрим схожий пример с более простым кодом, в котором декодирование выполняется за две итерации.

Пример 2.4.

Для передачи сообщений используется код (7, 4) с проверочной матрицей

$$H = \begin{bmatrix}1 & 1 & 0 & 1 & 0 & 0 & 0\\0 & 0 & 1 & 1 & 1 & 0 & 0\\0 & 0 & 0 & 1 & 0 & 1 & 1\end{bmatrix}.$$

Матрица *H* рассматриваемого кода (7, 4) с минимальным кодовым расстоянием, равным 2, содержит в каждой строке по 3 единицы, а число единиц в столбцах – различно, от одного до двух, т. е. данный код – нерегулярный как и код предыдущего примера. По каналу связи передается блок данных (1011001) двухполюсным сигналом (–1 1 –1 –1 1 1 –1). Помеха в канале, как и в предыдущем примере, представляет собою АБГШ с дисперсией $\sigma^2 = 0{,}5$. *LLR* представление принятого блока имеет вид: (–8 –6 –11 –5 8 9 –12). Второй символ в блоке искажен.

Граф Таннера для рассматриваемого кода изображен на рис. 2.7. Процедура декодирования принятого блока в *LLR* представлении по алгоритму «сумма наименьших» приведена на рис. 2.8.

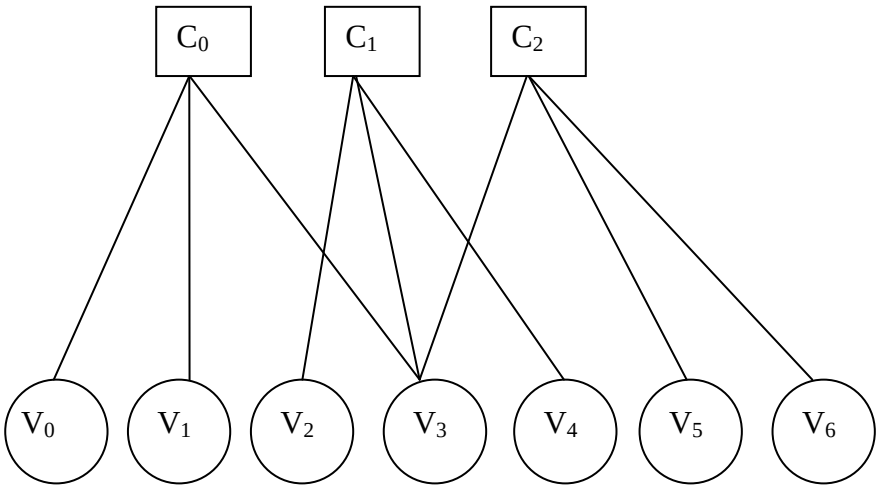

Рис. 2.7. Граф Таннера для кода (7, 4)

Как и в предыдущем примере на **этапе инициализации** вычисленные *LLR* значения принятых символов блока данных присваиваются соответствующим символьным узлам. Эти *LLR* значения являются исходными данными для выполнения **шага 1 итерации 1**. Пересчет проверочных узлов происходит по выражению (2.7) аналогично выполненному в предыдущем примере. Новые вычисленные априорные значения изображены как выходные сигналы от проверочных узлов к символьным. Как показано на рис. 2.8, внешние дополнения для всех символьных узлов, кроме V_3, поступают только от одного из проверочных узлов, а к узлу V_3 – от всех трех проверочных узлов.

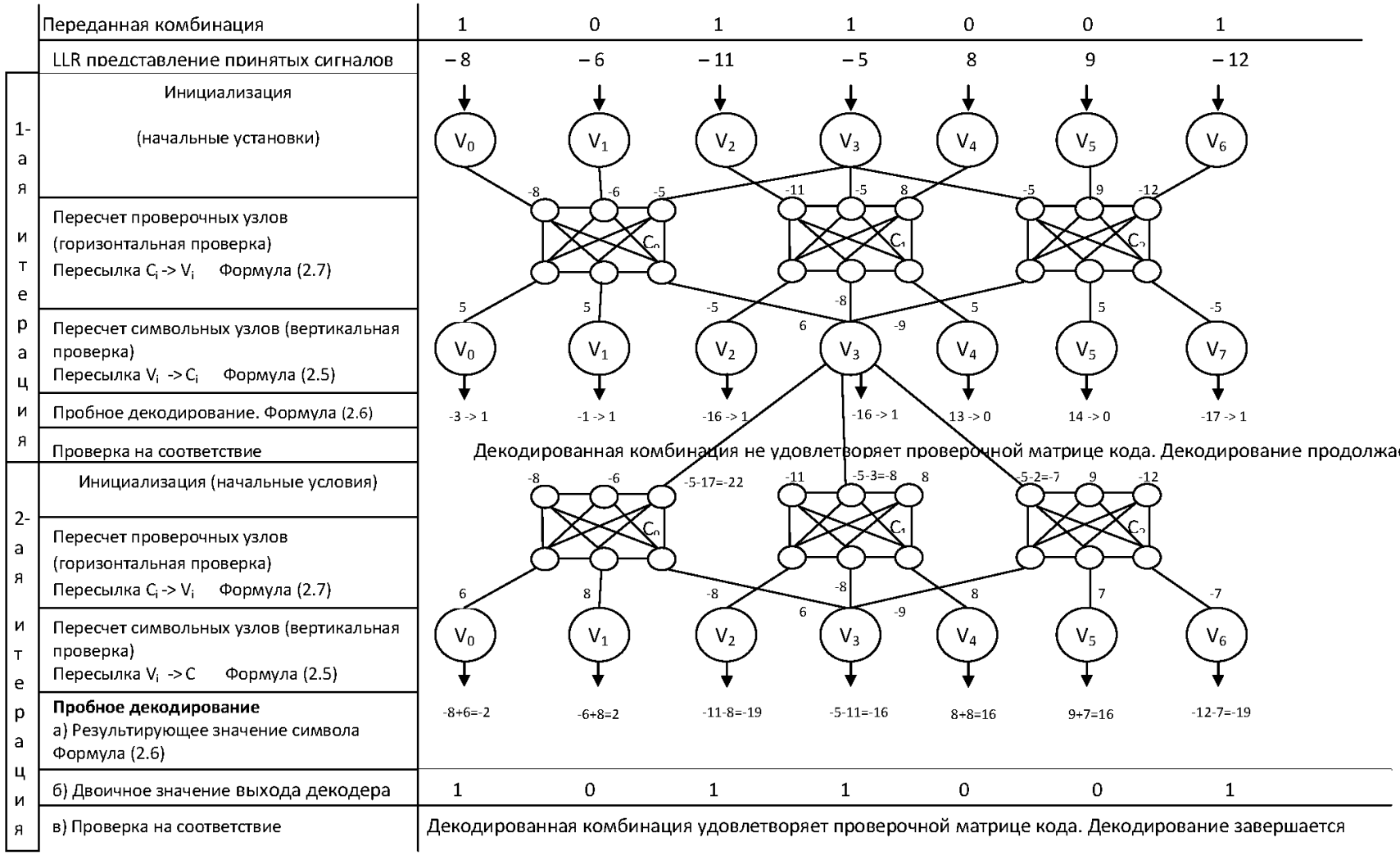

Рис. 2.8. Процедура декодирования блока данных кода (7, 4)

На **шаге 2 итерации 1** производится пересчет *LLR* значений символьных узлов. Здесь выполняется два вида расчетов: для выполнения следующей итерации по формуле (2.5); для пробного декодирования по формуле (2.6). Шесть символьных узлов V_0, V_1, V_2, V_4, V_5 и V_6 входят только в одну из горизонтальных проверок и внешние дополнения к ним от других горизонтальных проверок отсутствуют, в соответствии с (2.5). Указанные узлы начнут итерацию 2 с первоначальными значениями *LLR*, как на шаге 1 итерации 1. Значения *LLR* для символьного узла V_3 изменятся, и при этом в каждом из проверочных узлов они будут различными.

Дополнением к исходному значению (–5) узла V_3 в проверочном узле C_0 будет сумма внешних дополнений от узлов C_1 и C_2: (–8 – 9 = –17). В проверочном узле C_1 к значению (–5) узла V_3 добавится сумма внешних дополнений от узлов C_0 и C_2: (6 – 9 = –3), а в узле C_2 к значению (–5) узла V_3 добавится сумма внешних дополнений от узлов C_0 и C_1 (6 – 8 = –2).

Для **пробного декодирования** по результатам **итерации 1** мягкие значения символов блока данных формируются согласно (2.6), т. е. учитывают все внешние дополнения: (–3 –1 –16 –16 13 14 –17). По значениям символов полученного после итерации 1 блока данных видно, что ошибка во втором символе сохранилась и декодер переходит к следующей итерации декодирования.

Итерация 2 начинается при следующих LLR значениях символьных узлов: $V_0 = -8$, $V_1 = -6$, $V_2 = -11$, $V_{30} = -5 - 17 = -22$, $V_{31} = -5 - 3 = -8$, $V_{32} = -5 - 2 = -7$, $V_4 = 8$, $V_5 = 9$ и $V_6 = -12$. Вторая цифра i в подстрочном индексе V_{3i} указывает номер проверочного узла, для которого это значение рассчитано. Результаты **шага 1** и исходные данные для **пробного декодирования итерации 2** получены в соответствии с процедурами, использованными при расчетах на итерации 1, и представлены на рис. 2.8. *Двоичное значение блока данных,* представленное для пробного декодирования и также изображенное на рис. 2.8, *удовлетворяет* используемому коду:

$$(1011001) \times \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix} = (000).$$

Примеры 2.3 и 2.4 подтверждают высокую эффективность мягкого декодирования МППЧ кодов по критерию минимального кодового расстояния.

2.3. Способы построения МППЧ кодов

Р. Галлагер первоначально использовал псевдослучайную конструкцию предложенных им МППЧ кодов. Он использовал следующий алгоритм формирования проверочной матрицы.

Первоначально строится матрица H_0 небольшого размера с заданными характеристиками либо случайным способом, либо на основе некоторой алгебраической конструкции (например, Т. Ричардсон предложил в качестве H_0 использовать проверочную матрицу кода с проверкой на четность (2001 г.), К. Зигангиров – проверочную матрицу кода Хемминга (1999 г.), И. Джорджевич – проверочную матрицу кода Рида – Соломона (2003 г.), У. Уай – проверочную матрицу кода БЧХ (2005 г.), Е. Габидулин (2006 г.) – матрицы перестановок). Затем матрица H_0 многократно дублируется для получения требуемой длины кода МППЧ. В полученной матрице требуемых размеров производится случайная перестановка строк и столбцов. В итоге получается требуемая проверочная матрица H.

Построение кодов МППЧ на основе алгебраических конструкций позволяют детерминировать их основные характеристик, как то: минимальная длина цикла и минимальное кодовое расстояние.

В настоящем учебном пособии рассматриваются конструкции проверочной матрицы кода МППЧ, основанные на тройках Штейнера и матрицах перестановок, а также на мультипликативных группах полей Галуа, описанные в работах В. В. Зяблова, Ф. И. Иванова и В. Г. Потапова [10, 11].

2.3.1. *Детерминированный способ построения проверочных матриц для кодов МППЧ*

Для построения проверочных матриц кодов МППЧ авторы [10, 11] используют матрицы перестановок $H_0 = P_\sigma$. Напомним, что матрица перестановок – квадратная двоичная матрица. в каждой строке и в каждом столбце которой содержится только одна 1 [4]. Каждая матрица перестановок размеров $m \times m$ является матричным представлением перестановки порядка m. Пусть задана некоторая перестановка порядка m:

$$\begin{pmatrix} 1 & 2 & \dots & m \\ \sigma_1 & \sigma_2 & \dots & \sigma_m \end{pmatrix}.$$

Ей соответствует матрица размеров $m \times m$

$$P_\sigma = \begin{pmatrix} E_{\sigma 1} \\ E_{\sigma 2} \\ \dots \\ E_{\sigma m} \end{pmatrix},$$

где E_i – двоичная последовательность длины m, содержащая 1 только на позиции, соответствующей числу σ_i отображаемой перестановки.

Например, перестановке $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$ соответствует матрица перестановок $P = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$.

Известно, что матрицы перестановок образуют циклическую группу [4]. Действительно, матрицы перестановок можно умножать:

$$P_\sigma \times P_\beta = P_{\sigma * \beta}.$$

где * – операция умножения двух перестановок $\pi(\sigma)*\pi(\beta)$, т. е. произведение матриц перестановок есть матрица перестановок, равная произведению отображаемых перестановок. Для каждой матрицы перестановок существует обратная по операции умножения: $P_\sigma^{-1} = \mathrm{P}_\sigma^{\mathrm{T}}$. так как $P_\sigma \times P_\sigma^{\mathrm{T}} = I$, где P_σ^{T} есть транспонированная матрица P_σ, а I – единичная матрица тех же размеров, что и P_σ.

Пусть m, l, n_0 – целые положительные числа, причем $n_0 > l$, $m! > ln_0$. Рассмотрим группу $\mathbf{P}_m$ матриц перестановок размера $m \times m$. Выберем ln_0 случайных матриц $\{P_{ij}\}$ из группы $\mathbf{P}_m$ и составим матрицу $\mathbf{H}$ размера $l \times n_0$ таким образом, чтобы на каждой позиции в каждой строке и каждом столбце матрицы $\mathbf{H}$ находились различные матрицы из набора $\{P_{ij}\}$. Предложенный способ построения матрицы $\mathbf{H}$ гарантирует, что все матрицы P_{ij} в каждой строке и в каждом столбце будут различны. Так как P_{ij} квадратная матрица размера $m \times m$, то размер $\mathbf{H}$ равен $ml \times mn_0$. Построенные подобным способом проверочные матрицы $\mathbf{H}$ определяют семейство (l, n_0) – регулярных (с постоянным весом столбца l и спостоянным весом строки n_0) МППЧ кодов $(n_0m, n_0m–lm)$, получивших название *МППЧ кодов, основанных на матрицах перестановок*. Проверочная матрица семейства $(n_0m, n_0m–lm)$ кодов МППЧ имеет вид:

$$\mathbf{H} = \begin{bmatrix} P_{11} & P_{12} & P_{13} & \dots & P_{1n_0} \\ P_{21} & P_{22} & P_{23} & \dots & P_{2n_0} \\ \dots & \dots & \dots & \dots & \dots \\ P_{l1} & P_{l2} & P_{l3} & \dots & P_{\ln_0} \end{bmatrix}, \qquad (2.8)$$

где P_{ij} – матрицы перестановок, выбранные без возвращений из группы матриц перестановок P_m размера $m \times m$.

Известны граничные значения для характеристик рассматриваемого семейства МППЧ кодов:

– минимальное кодовое расстояние

$$\mathrm{d_c} \le 2\mathrm{m}, \qquad (2.9)$$

– нижняя оценка скорости кода

$$R > 1 - l/n_0.$$

2.3.2. *Коды МППЧ, основанные на тройках Штейнера и матрицах перестановок*

Якоб Штейнер – швейцарский математик (1796–1863). Система Штейнера [6] $S(v, k, t)$ – это пара (X, B), где X – множество из v элементов, а B – семейство k подмножеств X, называемых блоками. Каждое t – подмножество множества X, содержится ровно в одном блоке семейства B. Система $S(v, k = 3, t = 2)$ называется системой троек Штейнера. Систему $S(v, 3, 2)$ будем обозначать $STS(v)$. Если под элементами понимать целые положительные числа, то система $S(v, 3, 2)$ представляет собою совокупность неупорядоченных троек чисел, сформированных из набора v чисел, в которой каждая неупорядоченная пара чисел встречается только один раз. Известно [6], что для существования системы $STS(v)$ необходимо и достаточно, чтобы $v \equiv 1, 3 \pmod 6$. Для $v = 3, 7, 9$ получаем решения

$v = 3$: 123; $v = 7$: 123 145 167 246 257 347 356;
$v = 9$: 123 145 168 179 249 256 278 348 357 369 467 589.

Из литературных источников [10] известно, что кодовые комбинации веса 3 кода Хемминга с m избыточными символами образуют систему троек Штейнера $STS(2^m - 1)$. Например, для кода Хемминга (7, 4) с $m = 3$ система троек Штейнера представлена в табл. 2.5.

В [10] для получения требуемых троек Штейнера из комбинаций кода Хемминга используется следующий прием.

Таблица 2.5

Тройки Штейнера
на основе комбинаций Хемминга (7, 4)

Номера позиций кодовой комбинации кода Хемминга (7, 4)	Тройки Штейнера *STS* (7)
1234567	
1101000	124
0110100	235
0011010	346
0001101	457
1000110	156
0100011	267
1010001	137

Все комбинации веса 3 представляются в виде $c(x) = x^a + x^b + x^c$, где $0 \le a < b < c \le 2^m - 2$. Комбинация $c(x)$ выбирается так, чтобы все $2^m - 2$ циклических сдвига ее символов были различны. Так как $c(x)$ имеет вес 3 то $c^2(x)$, $c^4(x)$, $c^8(x)$, …. $c^l(x)$, где $l = 2^{p-1}$ – различные комбинации веса 3. Очевидно, что $p \le m$. Ниже приводится таблица значений p для некоторых циклических кодов Хемминга. На основании рассмотренного способа и данных таблицы можно построить системы троек Штейнера *STS* (2^m – 1) с различными значениями m.

Таблица 2.6

Таблица значений p

m	$c(x)$	p
4	$x^4 + x + 1$	2
5	$x^5 + x^2 + 1$	5
6	$x^6 + x + 1$	6
7	$x^7 + x + 1$	7

Таким образом, кодовое слово $c(x)$ веса 3 циклического кода Хемминга порождает $N_3(c(x))$ двоичных последовательностей длины $2^m - 1$ веса 3. Если общее число кодовых слов веса 3 в коде Хемминга длины $2^m - 1$ равно [9]:

$$B^3_{2^m-1} = \frac{C^2_{2^m-1}}{3} = \frac{(2^m-1)(2^m-2)}{6},$$

то существует $N_3(\tilde{c}(x)) = B^3_{2^m-1}/N_3(c(x)) = \dfrac{2^{m-1}-1}{3m}$ [10] кодовых слов $\tilde{c}_i(x)$, каждое из которых порождает $p(2^m - 1)$ кодовых слов веса 3.

Составим квадратную матрицу S_i размера $(2^m-1) \times (2^m-1)$, столбцы которой представляют набор из $p(2^m - 1)$ кодовых слов, порождаемых кодовым словом $\tilde{c}_i(x)$. Вес любой строки и любого столбца матрицы S_i равен 3, так как каждая из трех степеней многочлена $c(x)$ независимо от других

принимает значения из полного набора вычетов по модулю $(2^m - 1)$. Для простых (а в ряде случаев и непростых) $2^m - 1$ можно получить $p = m$ матриц S_i. Из полной совокупности матриц S_i построим матрицу $\tilde{H} = [S_0 \ldots S_{p-1}]$ размеров $(2^m - 1) \times p(2^m - 1)$. Вес каждой строки матрицы $\tilde{H}$ равен $3p$, а вес каждого столбца составляет 3. Размер матрицы $\tilde{H}$ может быть увеличен, если заменить в матрице $\tilde{H}$ каждую единицу на произвольную матрицу перестановок P_{ij} размерами $t \times t$, а каждый из нулей – на нулевую $t \times t$ матрицу. В результате таких преобразований будет получена разреженная матрица $\hat{H}$ размерами $t(2^m - 1) \times pt(2^m - 1)$ с весом каждой строки $3p$ и весом каждого столбца 3. Матрица $\hat{H}$ может быть использована для построения ансамбля МППЧ кодов. С этой целью, задаваясь некоторым целым k, из диапазона $1 < k \leq p$ выбираем из состава $[S_0 \ldots S_{p-1}]$ некоторое упорядоченное подмножество $< S_{i_1} \ldots . S_{i_k} >$, из которого формируем матрицу H. Матрица H имеет размеры $t(2^m - 1) \times kt(2^m - 1)$ с весом каждой строки $3k$ и весом каждого столбца 3. Таким образом, для некоторых произвольных целых $m > 3$, $2 \leq k \leq p$, а так же $3k(2^m - 1)$ случайных $t \times t$ матриц перестановок, $t > 1$, существует ансамбль регулярных $(3,3k)$ кодов с малой плотностью проверок на четность длины $n = kt(2^m - 1)$.

Этот ансамбль в [10] обозначен через $E_{STS}(m, k, t)$, а произвольный код из этого ансамбля назван *кодом с малой плотностью проверок на четность, основанным на матрицах перестановок и* $STS(2^m - 1)$.Основные свойства ансамбля $E_{STS}(m, k, t)$:

1) скорость кода лежит в пределах : $½ \leq R \leq 1 - 1/m$,
2) минимальное кодовое расстояние :$d_{\min} \geq 4$,
3) минимальная длина цикла g в проверочной матрице H: $g \geq 6$.

2.3.3. *Коды МППЧ, основанные на полях Галуа*

Квазициклические коды

Рассмотренный в п. 2.3.1. ансамбль кодов МППЧ, на основе матриц перестановок может быть расширен способами построения матриц перестановок P_{ij} и способом формирования из этих матриц проверочной матрицы H кода МППЧ. Критерием выбора способа формирования матрицы H кода МППЧ является отсутствие циклов длины 4, т. е. речь идет о создании таких кодовых конструкций, которые гарантируют требуемое свойство. Этим свойством при определенных условиях обладает ансамбль так называемых *квазициклических* МППЧ кодов. В основе построения ансамбля квазициклических кодов лежит возможность отображения элементов циклической

группы расширенного поля Галуа $GF^*(2^m)$ на элементы циклической группы перестановок. Рассмотрим пример, иллюстрирующий возможность такого отображения.

Пример 2.5. Рассмотрим $GF^*(2^2) = \{x, x + 1, 1\} = \{\alpha, \alpha^2, \alpha^3 = 1\}$, где $\alpha = x$ – примитивный элемент поля. Известно, что для отображения элементов поля на группу матриц перестановок достаточно найти отображение примитивного элемента поля, т. е. построить перестановку π_α, тогда $\pi_{\alpha^2} = \pi_\alpha^2$, $\pi_{\alpha^3} = \pi_\alpha^3 = e$, где e – единичная перестановка. Отобразим каждый из элементов группы $GF^*(2^2)$ на двоичный вектор и его десятичное представление:

$$\alpha \to (1\ 0) \to 2,$$
$$\alpha^2 \to (1\ 1) \to 3,$$
$$\alpha^3 \to (0\ 1) \to 1.$$

Табличное изображение перестановки π_α имеет вид:

$$\pi_\alpha = \begin{pmatrix} \alpha^3 & \alpha & \alpha^2 \\ \alpha & \alpha^2 & \alpha^3 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Полученная перестановка является циклической. Действительно, отображение π_α на соответствующую матрицу перестановки имеет вид:

$$\pi_\alpha \to P_\alpha = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix},\ \pi_{\alpha^2} \to P^2{}_\alpha = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},\ \pi_{\alpha^3} \to P^3{}_\alpha = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Обобщая этот пример на произвольную степень расширения m поля Галуа, для примитивного элемента циклической группы расширенного поля Галуа $GF^*(2^m)$ табличное изображение перестановки π_α имеет вид:

$$\pi_\alpha = \begin{pmatrix} 1 & 2 & 3 & \dots & q^m - 2 & q^m - 1 \\ 2 & 3 & 4 & \dots & q^m - 1 & 1 \end{pmatrix}$$

и, следовательно,

$$P_\alpha = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & 0 & \dots & 0 & 0 \end{pmatrix}. \qquad (2.10)$$

Матрицу P_α и все ее степени называют *циклическими матрицами перестановки*. Пусть α – примитивный элемент поля Галуа $GF(2^m)$ и $\alpha_{ij} = \alpha^{r_{ij}} \in GF^*(2^m)$. Отобразим каждый α_{ij} на циклическую матрицу перестановки $P_{\alpha_{ij}}$. Выберем целые положительные l, n_0, $n_0 > l$. Тогда проверочная матрица

$$H = \begin{pmatrix} P_{\alpha_{11}} & P_{\alpha_{12}} & \dots & P_{\alpha_{1n_0}} \\ P_{\alpha_{21}} & P_{\alpha_{22}} & \dots & P_{\alpha_{2n_0}} \\ \dots & \dots & \dots & \dots \\ P_{\alpha_{l1}} & P_{\alpha_{l2}} & \dots & P_{\alpha_{ln_0}} \end{pmatrix} \qquad (2.11)$$

определяет ансамбль регулярных двоичных МППЧ кодов длины $n = (2^m - 1)n_0$. Элементы проверочной матрицы (2.11) получаются путем равновероятного выбора (с возвращением) элементов мультипликативной группы $GF^*(2^m)$, отображаемых степенями матрицы P_α (2.10). Произвольный код из этого ансамбля называют ***квазициклическим*** кодом. Эти коды достаточно хорошо изучены [11]. Их преимущество перед случайными кодами заключается в том, что необходимо хранить не ln_0 произвольных матриц перестановок, а ln_0 чисел, являющихся степенями матрицы (2.10). Если представить элементы матрицы (2.11) в виде $P_\alpha^{r_{ij}} = P^{r_{ij}}$, то отсутствие в матрице H циклов длины 4 формулируется в следующем виде: матрица H не содержит циклов длины 4, когда для любой ее подматрицы $\begin{pmatrix} P^{r_{i_1 j_1}} & P^{r_{i_1 j_2}} \\ P^{r_{i_2 j_1}} & P^{r_{i_2 j_2}} \end{pmatrix}$ справедливо соотношение $r_{i_2 j_1} - r_{i_1 j_1} \neq r_{i_1 j_2} - r_{i_1 j_2}$.

Коды, основанные на поле Галуа

Полученные выше результаты могут быть обобщены на более широкий класс МППЧ кодов, основанных на свойствах элементов полей Галуа $GF(2^m)$, проверочные матрицы которых составляются из более сложных конструкций, чем циклические сдвиги единичных матриц, как это принято в квазициклических МППЧ кодах.

Рассмотрим способ построения отображения элементов мультипликативной группы поля Галуа $GF^*(2^m)$ порядка $2^m - 1 = \prod_{i=1}^{z} p_i^{c_i}$ на элементы некоторой подгруппы η симметрической группы перестановок S_h, где $h = \sum_{i=1}^{z} p_i^{c_i}$, для любого элемента γ из состава $GF^*(2^m)$:

$$\varphi(\gamma) = \pi_{\beta_1}^{r_1} \pi_{\beta_2}^{r_2} ... \pi_{\beta_z}^{r_z}, \qquad (2.12)$$

где β_i – образующая циклической подгруппы $GF^*(2^m)$ порядка $p_i^{c_i}$, а значения $r_i < p_i^{c_i}$ являются решениями уравнения

$$1 = \sum_{i=1}^{z} r_i \frac{2^m - 1}{p_i^{c_i}} \bmod(2^m - 1). \qquad (2.13)$$

Очевидно, что матрица P_γ, соответствующая перестановке $\varphi(\gamma)$, будет циклической только тогда, когда $2^m - 1$ – простое число. В противном случае P_γ будет иметь вид:

$$P_\gamma = \begin{pmatrix} I_{r_1} & 0 & ... & 0 \\ 0 & I_{r_2} & ... & 0 \\ ... & ... & ... & ... \\ 0 & ... & 0 & I_{r_z} \end{pmatrix}, \qquad (2.14)$$

а выражение (2.12) – являться произведением независимых циклов $\pi_{\beta_i}^{r_i}$.

Уравнение (2.13) есть результат применения китайской теоремы об остатках [4], которая утверждает, что *любое неотрицательное целое число r, не превышающее каждого из взаимно простых множителей модуля* $M = \prod_{i=1}^{z} m_i$ *можно однозначно восстановить, если известны его остатки по этим модулям*, к показателям степеней β_i в представлении отображаемого элемента γ на элементы подгруппы η симметрической группы перестановок S_h:

$$\gamma = \prod_{i=1}^{z} \beta_i^{r_i}. \qquad (2.15)$$

Так как $\gamma = \alpha^s, \beta_i = \alpha^{\frac{2^m - 1}{p_i^{c_i}}}$, то выражение (2.12) может быть записано:

$$\alpha^s = \prod_{i=1}^{z} \alpha^{r_i \frac{2^m - 1}{p_i^{c_i}}}$$

или

$$s = \sum_{i=1}^{z} r_i \frac{2^m - 1}{p_i^{c_i}} \bmod\left(2^m - 1\right). \qquad (2.16)$$

Для отображения элементов $GF^*(2^m)$ на элементы подгруппы η симметрической группы перестановок S_h достаточно определить отображение примитивного элемента $GF^*(2^m)$, т. е. принять в (2.16) $s = 1$, что и приводит к выражению (2.13).

Пример 2.6.

Рассмотрим мультипликативную группу $GF^*(2^4)$. Так как $2^4 - 1 = 3 \cdot 5$, то существуют две подгруппы с образующими $\beta_1 = \alpha^5$ – для циклической подгруппы порядка 3: $< \alpha^5, \alpha^{10}, \alpha^{15} >$ и $\beta_2 = \alpha^3$ – для циклической подгруппы порядка 5: $<\alpha^3, \alpha^6, \alpha^9, \alpha^{12}, \alpha^{15}>$, где α примитивный элемент поля $GF(2^4)$. Найдем отображение $\varphi : GF^*(2^4) \mapsto S_8$.

Прежде всего определим, куда переходят β_1 и β_2. Для этих подгрупп существуют отображения φ_1 и φ_2 на симметрические группы перестановок S_3 и S_5 соответственно. В соответствии с алгоритмом, выработанным по результатам примера 1, строим отображения

$$\varphi_1(\beta_1) = \pi_{\beta_1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \text{ и } \varphi_2(\beta_2) = \pi_{\beta_2} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}.$$

Для того, чтобы π_{β_1} и π_{β_2} являлись независимыми циклами, а их произведение принадлежало группе S_8, достаточно в перестановке π_{β_2} сделать переобозначения переставляемых элементов:

$$\pi_{\beta_2} = \begin{pmatrix} 4 & 5 & 6 & 7 & 8 \\ 5 & 6 & 7 & 8 & 4 \end{pmatrix}.$$

В результате

$$\pi_{\beta_1}^{r_1} \pi_{\beta_2}^{r_2} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^{r_1} \begin{pmatrix} 4 & 5 & 6 & 7 & 8 \\ 5 & 6 & 7 & 8 & 4 \end{pmatrix}^{r_2} \tag{2.17}$$

есть произведение независимых циклов при любых целых положительных r_1 и r_2. Для того, чтобы найти перестановку π_α. входящую в S_8 и соответствующую примитивному элементу α поля $GF(2^4)$, необходимо в выражении (2.17) вычислить r_1 и r_2. Для этого достаточно решить сравнение: $5\, r_1 + 3\, r_2 = 1 \bmod 15$. Решением являются числа $r_1 = r_2 = 2$ и значит

$$\pi_\alpha = \pi_{\beta_1}^2 \pi_{\beta_2}^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^2 \begin{pmatrix} 4 & 5 & 6 & 7 & 8 \\ 5 & 6 & 7 & 8 & 4 \end{pmatrix}^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 4 & 5 & 6 & 7 & 8 \\ 6 & 7 & 8 & 4 & 5 \end{pmatrix}. \tag{2.18}$$

В матричной форме выражение (2.18) имеет вид:

$$P_\alpha = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}.$$

Матрица P_α имеет структуру, соответствующую выражению (2.14):

$$P_\alpha = \begin{pmatrix} I_{r_1} & 0 \\ 0 & I_{r_2} \end{pmatrix}.$$

При этом

$$I_{r_1} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

и

$$I_{r_2} = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

в точности соответствуют выражению (2.18), и легко проверить, что порядок P_α равен 15. Рассмотренный пример подводит [11] к определению ансамбля *регулярных двоичных МППЧ GF-кодов*.

Определение. Пусть $\alpha_{ij} = \alpha^{s_{ij}} \in GF^*(q^m)$, где α – примитивный элемент поля. Представим $q^m - 1$ в каноническом виде: $q^m - 1 = \prod_{i=1}^{z} p_i^{c_i}$. Отобразим каждый элемент α_{ij} на матрицу перестановки $P_{\alpha_{ij}}$ размерности $\prod_{i=1}^{z} p_i^{c_i}$. Выберем целые положительные l, n_0, $n_0 > l$. Тогда проверочная матрица

$$H = \begin{pmatrix} P_{\alpha_{11}} & P_{\alpha_{12}} & \dots & P_{\alpha_{1n_0}} \\ P_{\alpha_{21}} & P_{\alpha_{22}} & \dots & P_{\alpha_{2n_0}} \\ \dots & \dots & \dots & \dots \\ P_{\alpha_{l1}} & P_{\alpha_{l2}} & \dots & P_{\alpha_{\ln_0}} \end{pmatrix} \qquad (2.19)$$

определяет ансамбль регулярных двоичных МППЧ кодов длины

$$n = n_0 \prod_{i=1}^{z} p_i^{c_i}.$$

Элементы проверочной матрицы $P_{\alpha_{ij}}$ получаются путем равновероятного выбора с возвращением элементов мультипликативной группы $GF^*(q^m)$.

Произвольный код из этого ансамбля называют ***МППЧ кодом, основанным на поле Галуа или GF-кодом***.

Каждая матрица $P_{\alpha_{ij}}$ может быть представлена в виде

$$P_{\alpha_{ij}} = P_{\alpha}^{s_{ij}} = \begin{pmatrix} I_{r_1} & 0 & \dots & 0 \\ 0 & I_{r_2} & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & I_{r_z} \end{pmatrix}^{s_{ij}} = \begin{pmatrix} I_{r_1}^{s_{ij}} & 0 & \dots & 0 \\ 0 & I_{r_2}^{s_{ij}} & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & I_{r_z}^{s_{ij}} \end{pmatrix}.$$

GF-код является квазициклическим кодом, если $q^m - 1$ является простым числом. Для *GF*-кодов, как и для квазициклических кодов, формулируется признак отсутствия циклов длины 4: проверочная матрица *GF*-кода (2.19) не имеет циклов длины 4, если любая ее подматрица вида

$$H_1 = \begin{pmatrix} P_{i_1 j_1} & P_{i_1 j_2} \\ P_{i_2 j_1} & P_{i_2 j_2} \end{pmatrix}$$

не имеет циклов длины 4.

Контрольные вопросы по разделу 2

1. Предназначение кодов МППЧ по замыслу автора.
2. Какова структура проверочной матрицы кодов МППЧ?
3. Какие требования предъявляются к проверочной матрице кодов МППЧ?

4. Как принято оценивать корректирующие свойства кодов МППЧ?

5. На основе чего строятся процедуры кодирования и декодирования кодов МППЧ?

6. К чему приводит наличие циклов различной длины в составе проверочной матрицы кодов МППЧ?

7. В чем состоит сущность жесткого декодирования кодов МППЧ?

8.В чем состоит сущность мягкого декодирования кодов МППЧ?

9. Что такое двудольный граф Таннера. Как он строится?

10. Как используется граф Таннера в процедуре мягкого декодирования кодов МППЧ?

11. Перечислите основные процедуры алгоритма декодирования «распространение доверия».

12. В чем состоит сущность построения проверочной матрицы кодов МППЧ по замыслу автора?

13. В чем состоит сущность детерминированного способа построения проверочной матрицы кодов МППЧ?

14. Что называют перестановкой и матрицей перестановок?

15. Как выполняется умножение перестановок и какими свойствами обладают перестановки по операции умножения?

16. Что такое система троек Штейнера?

17. Как можно построить систему троек Штейнера на основе весового спектра кода Хемминга?

18. Перечислите свойства ансамбля кодов МППЧ, основанных на матрицах перестановок.

19. Как строятся квазициклические коды МППЧ?

20. Перечислите сходство и отличия квазициклических кодов и кодов, основанных на полях Галуа.

Список литературы

1. *Кларк, Дж. К. мл.* Кодирование с исправлением ошибок в системах цифровой связи / Дж. К. Кларк, мл., Дж. Б. Кейн ; пер. с англ. – М. : Радио и связь, 1987. – 392 с.

2. *Когновицкий, О. С.* Теория помехоустойчивого кодирования. Часть 1. Циклическин коды : учеб. пособие / О. С. Когновицкий, В. М. Охорзин ; СПбГУТ. – СПб., 2013. – 94 с.

3. *Когновицкий, О. С.* Двойственный базис и его применение в телекоммуникациях / О. С. Когновицкий. – СПб. : Линк, 2009. – 423 с.

4. *Кострикин, А. И.* Введение в алгебру / А. И. Кострикин. – М. : Наука, 1977. – 496 с.

5. *Галлагер, Р.* Коды с малой плотностью проверки на четность / Р. Галлагер ; пер с англ. – М. : Мир, 1966. – 144 с.

6. *Холл, М.* Комбинаторный анализ / М. Холл ; пер. с англ. – М. : ИЛЛ, 1963. – 98 с.

7. *Морелос-Сарагоса, Р.* Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение / Р. Морелос-Сарагоса ; пер. с англ. – М. : Техносфера, 2005. – 320 с.

8. *Питерсон, У.* Коды, исправляющие ошибки / У. Питерсон, Э. Уэлдон ; пер. с англ. – М. : Мир, 1976. – 594 с.

9. *Ерош, С. Л.* Статистические характеристики систем передачи дискретных сообщений / С. Л. Ерош, В. М. Охорзин. – Л. : ВАС, 1974. – 107 с.

10. *Иванов, Ф. И.* Коды с малой плотностью проверок на четность, основанные на тройках Штейнера и матрицах перестановок / Ф. И. Иванов, В. В. Зяблов // Проблемы передачи информации. – том 49. – вып. 4. – С.41–56.

11. *Иванов, Ф. И.* Коды с малой плотностью проверок на четность, основанные на полях Галуа и матрицах перестановок / Ф. И. Иванов, В. В. Зяблов, В. Г. Потапов // Информационные процессы. – том 12. – № 1. – С. 68–83.

12. *Важенин, Н. А.* Оценка статистических характеристик функционирования LPDC-декодера на имитационной модели / Н. А. Важенин, И. А. Кирьянов // Электронный журнал «Труды МАИ». – вып. 59. – С. 1–14

13. *Когновицкий, О. С.* Теория помехоустойчивого кодирования. Часть 2. Сверточные коды. Турбокоды : учеб. пособие / О. С. Когновицкий, В. М. Охорзин, И. А. Небаев ; СПбГУТ. – СПб., 2015. – 64 с.

14. *Arijit Mondal.* Design of a min-sum LPDC decoder for error correction.Departament of electronic systems engineering Indian Institute of Since. Bangalore. India, 2014. – 59 p.

Когновицкий Олег Станиславович
Охорзин Виктор Михайлович

ТЕОРИЯ ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ

ЧАСТЬ 3

Циклические коды как рекуррентные последовательности
Коды с малой плотностью проверки на четность

Учебное пособие

Редактор *Л. К. Паршина*

План издания 2017 г., п. 46

Подписано к печати 27.06.2017
Объем 6,0 усл.-печ. л. Тираж 28 экз. Заказ 765

Редакционно-издательский отдел СПбГУТ
191186 СПб., наб. р. Мойки, 61

Отпечатано в СПбГУТ