Полиномиальные и циклические блоковые коды.

Полиномиальное представление двоичных комбинаций

Любая двоичная комбинация может быть представлена в полиномиальном виде путем введения фиктивной переменной x в степени, соответствующей весу двоичного символа в комбинации. Например, двоичная информационная 4-разрядная комбинация $I_1 = 1101$ в полиномиальном виде будет иметь следующий вид:

$$I_1(X) = 1 \cdot X^3 + 1 \cdot X^2 + 0 \cdot X^1 + 1 \cdot X^0 = X^3 + X^2 + 1$$

А двоичная информационная комбинация $I_2 = 0001$ в полиномиальном виде будет представлена как

$$I_2(X) = 0 \cdot X^3 + 0 \cdot X^2 + 0 \cdot X^1 + 1 \cdot X^0 = 1$$

Образующий (порождающий) полином кода G(X)

Полином, на который без остатка делятся все разрешенные кодовые полиномы кода, называется образующим (порождающим) полиномом G(X). Старшая степень образующего полинома соответствует числу проверочных символов в кодовом полиноме.

Примеры образующих (порождающих) полиномов G(X)

Старшая степень полинома (соответствует числу проверочных разрядов r в кодовом слове)	Вид образующего полинома G(X)	Двоичное представление полинома G(X)	Десятичное представление полинома G(X)
2	X^2+X+1	111	7
3	X^3+X+1	1011	11
4	X^4+X+1 $X^4+X^3+X^2+X+1$	10011 11111	19 31
5	$X^5+X^4+X^3+X^2+1$	111101	61
6	X^6+X+1 X^6+X^3+1 $X^6+X^5+X^2+X+1$	1000011 1001001 1100111	67 73 103
7	X^7+X+1 $X^7+X^4+X^3+X^2+1$	10000011 10011101	131 157
…	…	…	…

Арифметические действия над полиномами

Сложение полиномов

$$\begin{array}{rrrrr} & X^4+ & +X^3 & & +1 \\ \oplus\ X^6+ & & +X^3 & +X & +1 \\ \hline X^6+ & +X^4 & & +X & \end{array}$$

Умножение полиномов

$$\begin{array}{rrrrr} & & X^3+ & & +1 \\ \times & & X^3+ & +X & +1 \\ \hline & & X^3+ & & +1 \\ & X^4+ & & +X & \\ X^6+ & & X^3 & & \\ \hline X^6+ & +X^4 & & +X & +1 \end{array}$$

Деление полиномов

$$\begin{array}{rrrrr|l} X^6+ & & +X^3 & & & X^3+ +X +1 \\ X^6+ & +X^4 & +X^3 & & & \\ \hline & X^4+ & & & & X^3+ +X \\ & X^4+ & & +X^2 & +X & \text{частное} \\ \hline & & & X^2 & +X & \text{остаток} \end{array}$$

Примеры полиномиальных кодов

Код (6,3,3) (нециклический), $G(X)= X^3 + X + 1$

Пример получения кодовой комбинации путем деления информационного полинома Q(X) на образующий полином G(X)

Увеличение степени информационного полинома I(X)

$$Q(X) = I(X) \cdot X^3 = (X^2 + X + 1) \cdot X^3 = X^5 + X^4 + X^3$$

Деления расширенного информационного полинома Q(X) на образующий полином G(X)

$$\begin{array}{rrrrr|l} X^5+ & +X^4 & +X^3 & & & X^3+ +X +1 \\ X^5+ & & +X^3 & +X^2 & & \\ \hline & X^4+ & & +X^2 & & X^2+ +X \\ & X^4+ & & +X^2 & +X & \\ \hline & & & & X & \end{array}$$

Кодовый полином C(X) получается путем добавления остатка от деления Q(X) на G(X) к расширенному информационному полиному Q(X). В нашем случае: $C(X) = X^5 + X^4 + X^3 + X$

Информационная комбинация	Информационный полином I(X)	Расширенный информационный полином $Q(X)=I(X)\cdot X^3$	Остаток от деления Q(X) на образующий полином G(X)	Кодовый полином C(X)	Кодовый полином в двоичном представлении	Метрика Хемминга
000	0	0	0	0	000000	
001	1	X^3	X+1	X^3+X+1	001011	3
010	X	X^4	X^2+X	X^4+X^2+X	010110	3
011	X+1	X^4+X^3	X^2+1	$X^4+X^3+X^2+1$	011101	4
100	X^2	X^5	X^2+X+1	X^5+X^2+X+1	100111	4
101	X^2+1	X^5+X^3	X^2	$X^5+X^3+X^2$	101100	3
110	X^2+X	X^5+X^4	1	X^5+X^4+1	110001	3
111	X^2+X+1	$X^5+X^4+X^3$	X	$X^5+X^4+X^3+X$	111010	4

Код (7,3,4) (расширенный код (6,3,3)) (циклический), $G(X)= (X + 1)\cdot(X^3 + X + 1) = X^4 + X^3 + X^2 + 1$

Информационная комбинация	Информационный полином I(X)	Расширенный информационный полином $Q(X)=I(X)\cdot X^4$	Остаток от деления Q(X) на образующий полином G(X)	Кодовый полином C(X)	Кодовый полином в двоичном представлении	Метрика Хемминга
000	0	0	0	0	0000000	
001	1	X^4	X^3+X^2+1	$X^4+X^3+X^2+1$	0011101	4
010	X	X^5	X^2+X+1	X^5+X^2+X+1	0100111	4
011	X+1	X^5+X^4	X^3+X	$X^5+X^4+X^3+X$	0111010	4
100	X^2	X^6	X^3+X^2+X	$X^6+X^3+X^2+X$	1001110	4
101	X^2+1	X^6+X^4	X+1	X^6+X^4+X+1	1010011	4
110	X^2+X	X^6+X^5	X^3+1	$X^6+X^5+X^3+1$	1101001	4
111	X^2+X+1	$X^6+X^5+X^4$	X^2	$X^6+X^5+X^4+X^2$	1110100	4

Код (7,4,3) (циклический), $G(X)= X^3 + X + 1$

Информационная комбинация	Информационный полином I(X)	Расширенный информационный полином $Q(X)=I(X)\cdot X^3$	Остаток от деления Q(X) на образующий полином G(X)	Кодовый полином C(X)	Кодовый полином в двоичном представлении	Метрика Хемминга
0000	0	0	0	0	0000000	
0001	1	X^3	X+1	X^3+X+1	0001011	3
0010	X	X^4	X^2+X	X^4+X^2+X	0010110	3
0011	X+1	X^4+X^3	X^2+1	$X^4+X^3+X^2+1$	0011101	4
0100	X^2	X^5+X^2	X+1	X^5+X^2+X+1	0100111	4
0101	X^2+1	X^5+X^3	X^2	$X^5+X^3+X^2$	0101100	3
0110	X^2+X	X^5	X^4+1	X^5+X^4+1	0110001	3
0111	X^2+X+1	$X^5+X^4+X^3$	X	$X^5+X^4+X^3+X$	0111010	4
1000	X^3	X^6	X^2+1	X^6+X^2+1	1000101	3
1001	X^3+1	X^6+X^3	X^2+X	$X^6+X^3+X^2+X$	1001110	4
1010	X^3+X	X^6+X^4	X+1	X^6+X^4+X+1	1010011	4
1011	X^3+X+1	$X^6+X^4+X^3$	0	$X^6+X^4+X^3$	1011000	3
1100	X^3+X^2	X^6+X^5	X	X^6+X^5+X	1100010	3
1101	X^3+X^2+1	$X^6+X^5+X^3$	1	$X^6+X^5+X^3+1$	1101001	4
1110	X^3+X^2+X	$X^6+X^5+X^4$	X^2	$X^6+X^5+X^4+X^2$	1110100	4
1111	X^3+X^2+X+1	$X^6+X^5+X^4+X^3$	X^2+X+1	$X^6+X^5+X^4+X^3+X^2+X+1$	1111111	7

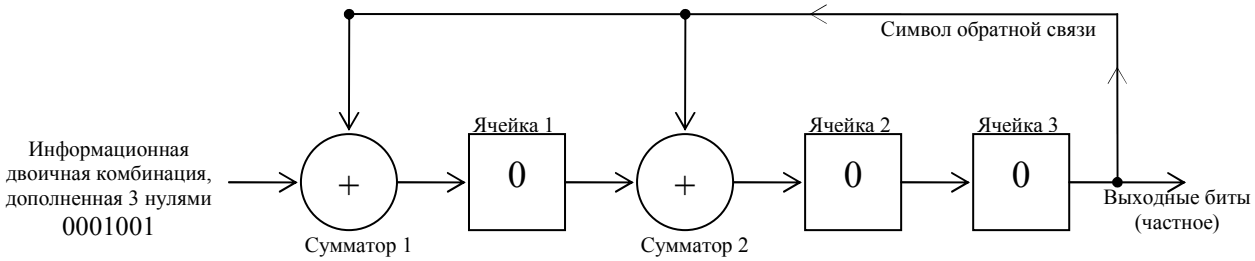
Код (5,2,3) (укороченный код (7,4,3)) (нециклический), $G(X)= X^3 + X + 1$

Инф. комбинация, k=2	Инф. комбинация, k=4	Информационный полином I(X)	Расширенный информационный полином $Q(X)=I(X)\cdot X^3$	Остаток от деления Q(X) на образующий полином G(X)	Кодовый полином C(X)	Кодовый полином в двоичном представлении	Метрика Хемминга
00	0000	0	0	0	0	~~00~~ 00000	
01	0001	1	X^3	X+1	X^3+X+1	~~00~~ 01011	3
10	0010	X	X^4	X^2+X	X^4+X^2+X	~~00~~ 10110	3
11	0011	X+1	X^4+X^3	X^2+1	$X^4+X^3+X^2+1$	~~00~~ 11101	4

Реализация кодеров полиномиальных кодов на регистрах сдвига

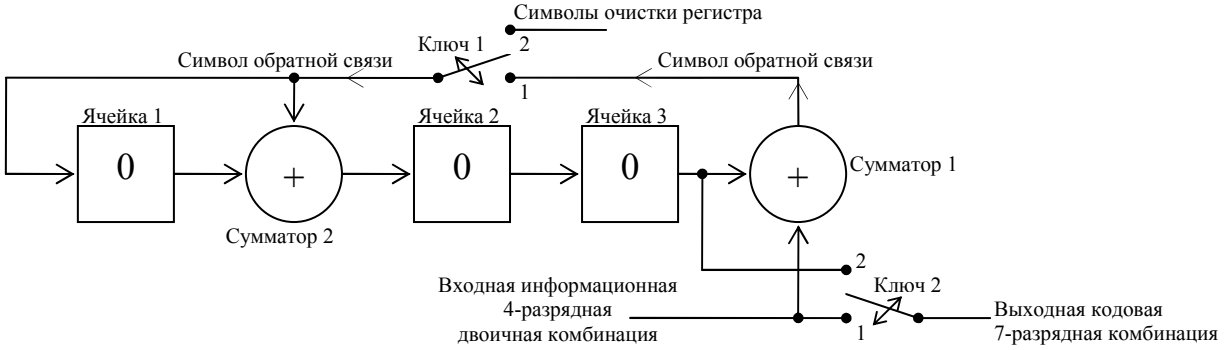
Кодер циклического кода (7,4,3)

1. Базовый вариант



№ итерации	Входная очередь	Сумматор 1	Сумматор 2	Ячейка 1	Ячейка 2	Ячейка 3	Символ обратной связи (выходной бит)
0	0001001	-	-	0	0	0	-
1	000100	1⊕..0=1	0⊕..0=0	..1	..0	0	0
2	00010	0⊕..0=0	1⊕..0=1	..0	..1	0	0
3	0001	0⊕..0=0	0⊕..0=0	..0	..0	1	0
4	000	1⊕..1=0	0⊕..1=1	..0	..1	0	1
5	00	0⊕..0=0	0⊕..0=0	..0	..0	1	0
6	0	0⊕..1=1	0⊕..1=1	..1	..1	0	1
7	-	0⊕..0=0	1⊕..0=1	***..0***	***..1***	***1***	0

2. Усложненный вариант



№ итерации	Входная очередь	Сумматор 1	Символ обратной связи	Сумматор 2	Ячейка 1	Ячейка 2	Ячейка 3	Выходные биты
0	1001	-	-	-	0	0	0	-
1	100	1⊕..0=1	..1	..1⊕0=1	..1	..1	0	1
2	10	0⊕..0=0	..0	..0⊕1=1	..0	..1	1	0
3	1	0⊕..1=1	..1	..1⊕0=1	..1	..1	1	0
4	-	1⊕..1=0	..0	..0⊕1=1	..0	..1	1	1
5	-	-	0	0⊕0=0	0	0	1	1
6	-	-	0	0⊕0=0	0	0	0	1
7	-	-	0	0⊕0=0	0	0	0	0

Пояснения к работе ключа 1 и 2.

Такты 1-4:

Ключ 1 замкнут на позицию 1, позволяя циркуляцию символов в регистре сдвига;

Ключ 2 замкнут на позицию 1 и пропускает все входные символы на выход для формирования информационной части систематической кодовой комбинации.

Такты 5-7:

Ключ 1 замкнут на позицию 2, позволяя символам очистки регистра заполнить ячейки регистра сдвига, готовя кодер к кодированию новой информационной комбинации;

Ключ 2 замкнут на позицию 2 и пропускает на выход символы, содержащиеся в ячейках регистра сдвига (остаток от деления) для формирования проверочной части кодовой комбинации.

Декодирование полиномиальных кодов

Пример декодирования кодового полинома $C(X) = X^6 + X^3 + X^2 + X$ кода (7,4,3)

Декодирование осуществляется путем деления кодового полинома C(X) на образующий полином G(X)

$$\begin{array}{llllll|lll} X^6+ & & +X^3 & +X^2 & +X & & X^3+ & +X & +1 \\ X^6+ & +X^4 & +X^3 & & & & X^3+ & +X & \\ \hline & X^4+ & & +X^2 & +X & & & & \\ & X^4+ & & +X^2 & +X & & & & \\ \hline & & & & 0 & & & & \end{array}$$

Остаток от деления (синдром) C(X) на G(X), равный 0, означает отсутствие ошибок в процессе передачи кодовой комбинации. Информационная комбинация получается путем отбрасывания составляющих полинома C(X), меньших X^3 и делением оставшихся составляющих на X^3. В нашем случае, $C(X) = X^6 + X^3 + X^2 + X$; $Q(X) = X^6 + X^3$; $I(X) = X^3 + 1$. I(X) в двоичном представлении – комбинация 1001

Декодирование с исправлением (обнаружением) ошибок на основе определения соответствия между остатками от деления при декодировании (синдромами ошибок) и векторами ошибок.

Пример декодирования разных кодовых комбинаций кода (6,3,3) с одинаковым вектором ошибок

$C_1(X) = X^5+X^4+X^3+X$, $E(X)=X^4$, $C_1^*(X) = X^5+X^3+X$

$$\begin{array}{llll|lll} X^5+ & & +X^3 & +X & X^3+ & +X & +1 \\ X^5+ & & +X^3 & +X^2 & & X^2 & \\ \hline & & & \mathbf{X^2+} & \mathbf{+X} & & \end{array}$$

$C_2(X) = X^3+X+1$, $E(X)=X^4$, $C_1^*(X) = X^4+X^3+X+1$

$$\begin{array}{llllll|lll} X^4+ & +X^3 & & +X & +1 & & X^3+ & +X & +1 \\ X^4+ & & +X^2 & +X & & & & X+ & +1 \\ \hline & X^3+ & +X^2 & & +1 & & & & \\ & X^3+ & & +X & +1 & & & & \\ \hline & & \mathbf{X^2+} & \mathbf{+X} & & & & & \end{array}$$

Таблица соответствия синдромов ошибок и векторов ошибок нулевого и первого порядка для кода (6,3,3)

Вектор ошибок порядка 0 или 1	Полином E(X), соответствующий вектору ошибок порядка 0 или 1	Остаток от деления кодового полинома C(X) на образующий полином G(X)
000000	0	0
000001	1	1
000010	X	X
000100	X^2	X^2
001000	X^3	X+1
010000	X^4	X^2+X
100000	X^5	X^2+X+1

Таблица соответствия синдромов ошибок и векторов ошибок нулевого, первого и второго порядков для кода (7,3,4)

Вектор ошибок порядка 0, 1 или 2	Полином E(X), соответствующий вектору ошибок порядка 0, 1 или 2	Остаток от деления кодового полинома C(X) на образующий полином G(X)
0000000	0	0
0000001	1	1
0000010	X	X
0000100	X^2	X^2
0001000	X^3	X^3
0010000	X^4	X^3+X^2+1
0100000	X^5	X^2+X+1
1000000	X^6	X^3+X^2+X
0000011	X+1	X+1
0000101	X^2+1	X^2+1
0000110	X^2+X	X^2+X
0001001	X^3+1	X^3+1
0001010	X^3+X	X^3+X
0001100	X^3+X^2	X^3+X^2
0010001	X^4+1	X^3+X^2
0010010	X^4+X	X^3+X^2+X+1
0010100	X^4+X^2	X^3+1
0011000	X^4+X^3	X^2+1
0100001	X^5+1	X^2+X
0100010	X^5+X	X^2+1
0100100	X^5+X^2	X+1
0101000	X^5+X^3	X^3+X^2+X+1
0110000	X^5+X^4	X^3+X
1000001	X^6+1	X^3+X^2+X+1
1000010	X^6+X	X^3+X
1000100	X^6+X^2	X^3+X^2
1001000	X^6+X^3	X^2+X
1010000	X^6+X^4	X+1
1100000	X^6+X^5	X^3+1

Таблица соответствия синдромов ошибок и векторов ошибок нулевого и первого порядков для кода (7,4,3)

Вектор ошибок порядка 0 или 1	Полином E(X), соответствующий вектору ошибок порядка 0 или 1	Остаток от деления кодового полинома C(X) на образующий полином G(X)
0000000	0	0
0000001	1	1
0000010	X	X
0000100	X^2	X^2
0001000	X^3	X+1
0010000	X^4	X^2+X
0100000	X^5	X^2+X+1
1000000	X^6	X^2+1

Таблица соответствия синдромов ошибок и векторов ошибок нулевого и первого порядков для кода (5,2,3)

Вектор ошибок порядка 0 или 1	Полином E(X), соответствующий вектору ошибок порядка 0 или 1	Остаток от деления кодового полинома C(X) на образующий полином G(X)
00000	0	0
00001	1	1
00010	X	X
00100	X^2	X^2
01000	X^3	X+1
10000	X^4	X^2+X

Декодирование циклических кодов путем сведения к известному синдрому

Предположим, что в процессе передачи кодовой комбинации, соответствующей кодовому полиному $C(X) = X^6 + X^3 + X^2 + X$, возникла однократная ошибка, соответствующая вектору ошибок 0000100. В полиномиальном виде вектор ошибок может быть представлен как полином $E(X) = X^2$. Сложение кодового полинома C(X) с полиномом ошибок E(X) даст нам "искаженный шумами" кодовый полином $C^*(X) = X^6 + X^3 + X$. Выполним деление $C^*(X)$ на G(X)

$$\begin{array}{llll|l} x^6+ & & +x^3 & +x & x^3+ \quad +x \quad +1 \\ x^6+ & +x^4 & +x^3 & & x^3+ \quad +x \\ \hline & x^4+ & & +x & \\ & x^4+ & +x^2 & +x & \\ \hline & & x^2 & & \end{array}$$

Полученный остаток от деления (синдром), отличный от нуля, означает наличие ошибки в кодовом полиноме. Из таблицы соответствия синдромов ошибок и векторов ошибок известно, что остаток от деления, равный 1 соответствует вектору ошибок 0000001. Для исправления ошибки будем выполнять циклические сдвиги (в данном случае выбран правый циклический сдвиг) на одну позицию кодового полинома $C^*(X)$ и выполнять повторное деление $C^*(X)$ на G(X) до тех пор, пока не будет найден интересующий нас остаток, равный 1. После этого ошибка может быть исправлена.

Правый циклический сдвиг кодового полинома $C^*(X) = X^6 + X^3 + X$ (в двоичном представлении 1001010) приведет к появлению кодового полинома $C_1^*(X) = X^5 + X^2 + 1$ (в двоичном представлении 0100101). Выполним деление $C_1^*(X)$ на G(X)

$$\begin{array}{llll|l} x^5+ & & +x^2 & +1 & x^3+ \quad +x \quad +1 \\ x^5+ & +x^3 & +x^2 & & \quad x^2+ \quad +1 \\ \hline & x^3+ & & +1 & \\ & x^3+ & +x & +1 & \\ \hline & & x & & \end{array}$$

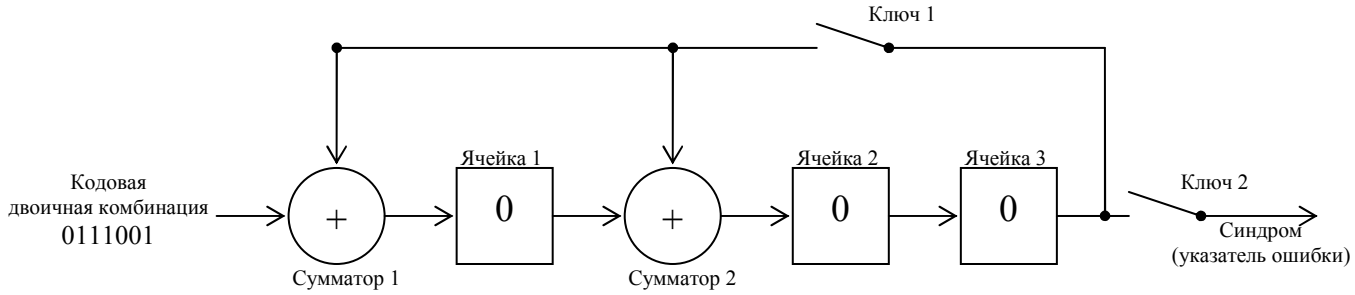
Остаток от деления X не совпадает с интересующим нас остатком, равным 1, поэтому необходимо произвести еще один правый циклический сдвиг, на этот раз полинома $C_1^*(X)$. В результате появится кодовый полином $C_2^*(X) = X^6 + X^4 + X$ (в двоичном представлении 1010010). Выполним деление $C_2^*(X)$ на G(X)

$$\begin{array}{llll|l} x^6+ & +x^4 & & +x & x^3+ \quad +x \quad +1 \\ x^6+ & +x^4 & +x^3 & & x^3+ \quad +1 \\ \hline & & x^3+ & +x & \\ & & x^3+ & +x \quad +1 & \\ \hline & & & 1 & \end{array}$$

Наконец, вес остатка от деления равен 1, а это означает, что позиция ошибки обнаружена и мы можем осуществить ее исправление. Для этого сначала генерируется начальный корректирующий вектор 0000001, который соответствует полиному $Cr_0(X) = 1$. Далее выполняются левые циклические сдвиги полинома Cr(X), соответствующие числу правых циклических сдвигов при нахождении остатка от деления, равного 1. В данном примере необходимо выполнить два левых циклических сдвига полинома $Cr_0(X)$ для получения корректирующего полинома $Cr(X) = X^2$, который складывается с кодовым полиномом $C^*(X)$ и исправляет содержащуюся в нем ошибку: $X^6 + X^3 + X + X^2 = X^6 + X^3 + X^2 + X$. Информационная комбинация получается путем отбрасывания составляющих полинома C(X), меньших X^3 и делением оставшихся составляющих на X^3. В нашем случае, $C(X) = X^6 + X^3 + X^2 + X$; $Q(X) = X^6 + X^3$; $I(X) = X^3 + 1$. I(X) в двоичном представлении – комбинация 1001.

Реализация декодеров полиномиальных кодов на регистрах сдвига

1. Декодирование при отсутствии ошибок



№ итерации	Входная очередь	Сумматор 1	Сумматор 2	Ячейка 1	Ячейка 2	Ячейка 3	Символ обратной связи
0	0111001	-	-	0	0	0	-
1	011100	1⊕..0=1	0⊕..0=0	..1	..0	0	0
2	01110	0⊕..0=0	1⊕..0=1	..0	..1	0	0
3	0111	0⊕..0=0	0⊕..0=0	..0	..0	1	0
4	011	1⊕..1=0	0⊕..1=1	..0	..1	0	1
5	01	1⊕..0=1	0⊕..0=0	..1	..0	1	0
6	0	1⊕..1=0	1⊕..1=0	..0	..0	0	1
7	-	0⊕..0=0	0⊕..0=0	***..0***	***..0***	***0***	0

По виду синдрома 000 определяем, что ошибок в процессе передачи не возникло, что позволяет отбросить проверочные разряды и получить исходную информационную комбинацию 1001

2. Декодирование при наличии однократной ошибки

№ итерации	Входная очередь	Сумматор 1	Сумматор 2	Ячейка 1	Ячейка 2	Ячейка 3	Символ обратной связи
0	0101001	-	-	0	0	0	-
1	011100	1⊕..0=1	0⊕..0=0	..1	..0	0	0
2	01110	0⊕..0=0	1⊕..0=1	..0	..1	0	0
3	0111	0⊕..0=0	0⊕..0=0	..0	..0	1	0
4	011	1⊕..1=0	0⊕..1=1	..0	..1	0	1
5	01	0⊕..0=0	0⊕..0=0	..0	..0	1	0
6	0	1⊕..1=0	0⊕..1=0	..0	..1	0	1
7	-	0⊕..0=0	0⊕..0=0	***..0***	***..0***	***1***	0

По виду синдрома определяем наличие ошибок в принятой кодовой комбинации. Далее можно осуществить поиск соответствия полученного синдрома определенному вектору ошибок, а можно выполнить циклический сдвиг принятой кодовой комбинации для сведения остатка от деления к известному синдрому. После исправления ошибки восстановление информационной комбинации можно осуществить путем отбрасывания проверочных разрядов.