Циклический код. Пример работы алгоритма.

- Множество кодовых комбинаций называется **циклическим кодом**, если циклический сдвиг любой комбинации этого множества на любое число разрядов влево или вправо приводит к комбинации из данного множества.
- Циклические коды относятся к числу групповых кодов, у которых каждая комбинация кодируется самостоятельно в виде блока длиной n. Блок содержит m информационных и k контрольных символов. Длина кодовой комбинации $n=m+k$.
- Если в комбинации кода можно определенно указать позиции, занимаемые информационными и контрольными символами, то код называется **систематическим или разделимым**, в противном случае — несистематическим или неразделимым.

- Исходным кодом для циклического кодирования является двоичный код на все сочетания. Число его комбинаций $M=2^m$. При этом число разрядов m исходного кода определяет число информационных символов.
- При описании циклического кода наиболее удобной является запись его двоичной комбинации в виде многочлена $F(x)$ некот

$$F(x) = b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_1x^1 + b_0x^0$$

где $b_{k-1} \div b_0$ - контрольные символы; $b_{n-1} \div b_k$ - информационные символы.

- Двоичная комбинация исходного кода записывается аналогично в виде многочлена $G(x)$. Например, комбинация исходного кода ***1101*** представляется

$$G(x) = 1 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x^1 + 1 \cdot x^0$$

Или сокращенно

$$G(x) = x^3 + x^2 + 1$$

- В теории циклического кодирования сложение многочленов выполняется как поразрядное сложение по модулю два. При этом $x^i \oplus x^i = 0$, так как $x^i \oplus x^i \rightarrow 1 \oplus 1 = 0$, где $\oplus$ - знак сложения по модулю 2.
- Операция умножения (деления) многочленов включает их перемножение (деление) по обычным правилам с дальнейшим приведением подобных членов по модулю два.

- Построение циклического кода базируется на использовании так называемого **образующего или порождающего** полинома $P(x)$.
- В качестве образующего обычно выбирается *<u>неприводимый</u>* многочлен, т.е. такой, который делится только сам на себя и на единицу.
- Доказано, что полином $P(x)$ порождает циклический код длиной n, если он является сомножителем в разложении двучлена ($x^n + 1$) на неприводимые многочлены.
- Не исключен выбор в качестве образующего полинома произведения двух или более неприводимых многочленов этого разложения. Но тогда циклический код будет обладать худшими параметрами с точки зрения мощности множества кодовых комбинаций.

- Старшая степень образующего полинома определяет число контрольных символов. Например, выбирая для исходного четырехразрядного кода в качестве образующего полинома неприводимый многочлен

$P(x) = x^3 + x + 1$, получим для циклического кода число контрольных символов $k=3$ и длину кодовог

$$H(x) = \frac{(x^n + 1)}{P(x)}$$

Полином

называется проверочным или генераторным полиномом. Высшая степень проверочного полинома равна числу информационных разрядов кода m.

- Кодовые комбинации $F(x)$ циклического кода помимо общих для групповых кодов ограничений удовлетворяют следующим двум условиям:

1. $F(x)/P(x) = 0$, т.е. без остатка делятся на о і полином;
2. $F(x) \cdot H(x) = 0$ по $\mathrm{mod}(x^n + 1)$, т.е. при умножении на проверочный полином дают тождественный нуль по модулю двучлена $(x^n + 1)$.

- Сущность операции умножения по модулю $(x^n + 1)$ состоит в том, что многочлены $F(x)$ и $H(x)$ перемножаются по обычным правилам с приведением подобных членов по модулю 2. Если старшая степень произведения не превышает $(n - 1)$, то оно является результатом умножения по модулю $(x^n + 1)$. В противном случае многочлен произведения делится на двучлен $(x^n + 1)$ и получившийся при этом остаток является результатом умножения по модулю $(x^n + 1)$.
- На названных выше двух свойствах основано обнаружение и исправление ошибок при передаче циклических кодов по каналам связи. Эти же свойства лежат в основе построения циклических последовательностей и технической реализации кодирующих устройств.

- Циклический сдвиг кодовой комбинации F на i шагов влево (вправо) равносилен умножению полинома $F(x)$ на одночлен x^i (x^{-i}) по модулю двучлена (x^n+1).
- Любое слово в циклическом коде $F(x)$ делится на образующий полином. Отсюда следует, что

  $F(x)= U(x)\,P(x)$, где $U(x)$ - частное от деления $F(x)$ на $P(x)$.

При $U(x) = G(x)$ описывает процесс кодирования. Исходные комбинации m-разрядного первичного кода $G=g_{m-1}g_{m-2}\dots g_0$ ($g_i = 0$ или 1) представляются как

- Например, при умножении исходного четырехразрядного информационного полинома $G(x) = x^3 + x^2 + 1$ на образующий полином $P(x) = x^3 + x + 1$ получим кодовую комбинацию в циклическом коде $F(x) = G(x)P(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \rightarrow 1111111$. Такой способ кодирования дает несистематический циклический код, так как в кодовом слове $F(x)$ невозможно указать места информационных символов. Для их выделения на приемной стороне необходимо комбинации циклического кода делить на образующий полином, что затрудняет

- Наиболее целесообразно циклический код представлять в виде разделимого (n, m) кода. Тогда алгоритм кодирования определяется выражением
$F(x)= x^k G(x) + R(x)$, где $R(x)$ - остаток от деления произведения $x^k G(x)$ на образующий пол$R(x) = Rem\left[\frac{x^k G(x)}{P(x)}\right]$но ,
где Rem —обозначение остатка от деления.

Пример

- Пусть n=7, k=3, и $P(x) = x^3+x+1$. Представим в разделимом коде (7,4) информационную комбинацию $1101 \rightarrow G(x) = x^3+x^2+1$. Найдем произведение $x^3\ G(x) = x^6+x^5+x^3 \rightarrow 1101000$.

Умножение на одночлен x^k соответствует сдвигу информационной комбинации G на k разрядов влево, что эквивалентно приписыванию k нулей со стороны младших разрядов. Данная операция позволяет впоследствии на месте этих нулей размещать контрольные символы. Разделим полученное произведение на образующий полином

Пример

$$
\begin{array}{l|l}
x^6+x^5+x^3 & x^3+x+1 \\
\oplus\ \underline{x^6+x^4+x^3} & \hline \\
\quad x^5+x^4 & x^3+x^2+x+1 \\
\quad \oplus\ \underline{x^5+x^3+x^2} & \\
\qquad x^4+x^3+x^2 & \\
\qquad \oplus\ \underline{x^4+x^2+x} & \\
\qquad\quad x^3+x & \\
\qquad\quad \oplus\ \underline{x^3+x+1} & \\
\qquad\quad\ \ 1 & \text{- остаток } R
\end{array}
$$

Отсюда следует $R(x) = 1$ и

$F(x) = x^6+x^5+x^3+1 \rightarrow 1101001$, где 1101 - информационные символы , а 001 - контрольные символы .

- Циклический код компактно описывают с помощью образующей матрицы в канонической форме
  $F_{m,n} = | I_m \ R_{m,k} |$, где I_m —единичная квадратная матрица размерности m, у которой на главной диагонали расположены единицы, а все остальные элементы равны нулю;
  $R_{m,k}$ - матрица контрольных символов размерности $m \times k$.
- Матрица I_m является образующей матрицей первичного m-разрядного кода. Ее строки представляют собой набор линейно-независимых комбинаций первичного кода и определяют вид информационных полиномов $G_j(x) = x^j$, где j - j-я строка единичной матрицы,

- Строки матрицы контрольных символов $R_{m,k}$, соответствуют остаткам $R_j(x)$.
- В целом строки образующей матрицы $F_{m,n}$ представляют собой кодовые полиномы $F_j(x)$, определяемые по алгоритму

$$F(x) = x^k\, G(x) + R(x)$$

Пример

- Составим образующую матрицу для условий примера, когда m=4, k=3, $P(x) = x^3+x+1$. Тогда:

$G_3(x) = x^3$ и $F_3(x) = x^3 G_3(x) + R_3(x) = x^6+x^2+1 \rightarrow 1000101$

$G_2(x) = x^2$ и $F_2(x) = x^3 G_2(x) + R_2(x) = x^5+x^2+x+1 \rightarrow 0100111$

$G_1(x) = x^1$ и $F_1(x) = x^3 G_1(x) + R_1(x) = x^4+x^2+x \rightarrow 0010110$

$G_0(x) = 1$ и $F_0(x) = x^3 G_0(x) + R_0(x) = x^3+x+1 \rightarrow 0001011$

Тогда образующая матрица примет вид

$$F_{4,7} = \begin{vmatrix} F_3(x) \\ F_2(x) \\ F_1(x) \\ F_0(x) \end{vmatrix} = \begin{array}{c} \begin{matrix} b_6 & b_5 & b_4 & b_3 & b_2 & b_1 & b_0 \end{matrix} \\ \begin{vmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{vmatrix} \end{array}$$

- С помощью образующей матрицы могут быть получены все $M = 2^m$ кодовых комбинаций циклического кода путем суммирования строк матрицы $F_{4,7}$ по модулю 2 в различных сочетаниях.
- Образующую матрицу циклического кода можно также построить другим способом. Процесс построения формализуется следующим образом. Исходя из числа информационных разрядов m, составляется единичная матрица I_m. К ней справа приписывают матрицу контрольных символов $R_{m,k}$, которая находится с помощью следующего формального приема. Единица с рядом нулей делится на образующий полином и выписываются m промежуточных остатков деления. Эти остатки, записанные в обратном порядке, образуют матрицу контрольных

Пример

Найдем матрицу контрольных символов для условий примера, когда $P(x) = x^3 + x + 1 \rightarrow 1011.$

Выполним деление

$1000000000\ldots\ldots \;|\; 1011$

$\oplus\ \underline{1011}$

$0110 \rightarrow$ 1й остаток $|\; 1011$

$\oplus\ \underline{0000}$

$1100 \rightarrow$ 2-й остаток

$\oplus\ \underline{1011}$

$1110 \rightarrow$ 3-й остаток

$\oplus\ \underline{1011}$

$1010 \rightarrow$ 4-й остаток

Пример

Выписывая остатки снизу вверх (в обратном порядке), получим матрицу контрольных символов $R_{4,3}$ и образующую матрицу $F_{4,7}$:

$$R_{4,3} = \begin{array}{c} \begin{matrix} b_2 & b_1 & b_0 \end{matrix} \\ \left|\begin{matrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{matrix}\right| \end{array} \quad \text{и}$$

$$F_{4,7} = \begin{vmatrix} F_3(x) \\ F_2(x) \\ F_1(x) \\ F_0(x) \end{vmatrix} = \begin{array}{c} \begin{matrix} b_6 & b_5 & b_4 & b_3 & b_2 & b_1 & b_0 \end{matrix} \\ \left|\begin{matrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{matrix}\right| \end{array}$$

Проверочная матрица

- Циклический код можно описать не только посредством образующей матрицы, но и с помощью проверочной матрицы $H_{k,n}$. Чаще всего на практике применяется циклическая форма этой матрицы. Первая строка такой матрицы зависит от вида проверочного полинома $H(x)$, а остальные строки получают, циклически сдвигая вправо первую строку.
- Вид первой строки проверочной матрицы в циклической форме связан с видом проверочного полинома следующим образом. Полином $H(x)$ представляют в виде кодовой комбинации. Запись этой комбинации в обратном порядке и приписывание к ней справа $k-1$ нулевых символов дает первую строку

Проверочная матрица

- Строки проверочной матрицы дают состав проверок на четность

$$d_{k-j} = \langle \sum_{i=1}^{n} \rangle h_{ij} \cdot b_{n-i}, \qquad j = 1, \ldots, k,$$

где d_{k-j} —результат j-й проверки на четность;

$h_{i,j}$ —элемент j-й строки и i-го столбца проверочной матрицы;

b_{n-i} —разряды комбинации циклического кода;

$< \sum >$ - знак суммирования по модулю 2.

Проверочная матрица

- Идея данной проверки основана на том, что при отсутствии ошибок и при четном числе единиц в кодовой комбинации сумма ее разрядов по модулю два всегда ра

$$d_{k-j} = \langle \sum_{i=1}^{n} \rangle h_{ij} \cdot b_{n-i}, \; j = 1, \ldots, k$$

Отсюда из соотношения при $d_j = 0$ следует соотношение для формирования контро

$$b_{k-j} = \langle \sum_{i=1}^{m+j-1} \rangle h_{ij} \cdot b_{n-i}, \; j = 1, \ldots, k$$

Это соотношение определяет еще один алгоритм построения циклического кода. Двоичная последовательность $D = d_{k-1} d_{k-2} \ldots d_1 d_0$ называется **синдромом** или опознавателем ошибки. Если синдром состоит из одних нулей , то комбинация циклического кода считается безошибочной. Ненулевая величина синдрома ($D \neq 0$) говорит о наличии ошибок.

Пример

- Составим проверочную матрицу для условий старого примера, когда $n=7$, $m=4$, $k=3$ и $P(x) = x^3+x+1$. Проверочный полином:

$$H(x) = \frac{(x^7+1)}{x^3+x+1} = x^4 + x^2 + x + 1 \rightarrow 10111$$

Тогда первая строка проверочной матрицы примет вид 1110100, а в целом проверочная матрица будет иметь форму

$$H_{3,7} = \begin{array}{c|ccccccc} & b_6 & b_5 & b_4 & b_3 & b_2 & b_1 & b_0 \\ \hline d_1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ d_2 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ d_3 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{array}$$

Пример

$$H_{3,7} = \begin{array}{c|ccccccc|c} & b_6 & b_5 & b_4 & b_3 & b_2 & b_1 & b_0 & \\ & 1 & 1 & 1 & 0 & 1 & 0 & 0 & d_1 \\ & 0 & 1 & 1 & 1 & 0 & 1 & 0 & d_2 \\ & 0 & 0 & 1 & 1 & 1 & 0 & 1 & d_3 \end{array}$$

- Соотношения для проверок на четность и уравнения для формирования контрольных символов принимают вид

$$d_1 = b_6 \oplus b_5 \oplus b_4 \oplus b_2 = 0; \quad b_2 = b_6 \oplus b_5 \oplus b_4$$
$$d_2 = b_5 \oplus b_4 \oplus b_3 \oplus b_1 = 0; \quad b_1 = b_5 \oplus b_4 \oplus b_3$$
$$d_3 = b_4 \oplus b_3 \oplus b_2 \oplus b_0 = 0; \quad b_0 = b_4 \oplus b_3 \oplus b_2$$

Построение циклического кода

- Построение циклического кода производится, исходя из разрядности m исходного кода и требуемой от циклического кода корректирующей способности, задаваемой в виде числа обнаруживаемых r и числа исправляемых s ошибок.
- По сути дела построение кода сводится к выбору образующего полинома $P(x)$ и составлению образующей матрицы. Корректирующая способность зависит от кодового расстояния d.

Построение циклического кода

- Под кодовым расстоянием между двумя комбинациями F_1 и F_2 понимают число разрядов, в которых эти комбинации отличаются друг от друга. Кодовое расстояние равно числу единиц (весу) W в сумме двух комбинаций по модулю 2, т.е. $d=W(F_1 \oplus F_2)$.
- Если код должен обнаруживать все ошибки с кратностью r и менее, то $d \geq r+1$. Если код должен исправлять все ошибки с кратностью s и менее, то $d \geq 2s+1$. Если код должен ошибки с кратностью s и менее исправлять, а ошибки с кратностью от $s+1$ до r включительно обнаруживать (причем $r>s$), то

Построение циклического кода

- Старшая степень образующего полинома равна числу контрольных символов. Поэтому первым шагом при выборе образующего полинома является определение числа контрольных разрядов. Это число выбирают на основании ог $\sum_{q=0}^{\frac{d-1}{2}}$ инга:

$$k \geq \log_2 \sum_{q=0}^{q} C_n^q$$ при d нечетном

$$k \geq 1 + \log_2 \sum_{q=0}^{\frac{d}{2}} C_{n-1}^q$$ при d четном

Построение циклического кода

- Образующий полином следует искать по таблицам разложения двучлена $(x^n + 1)$ на неприводимые сомножители. Полином $P(x)$ должен удовлетворять двум условиям :

a) степень полинома равна k;

b) число ненулевых членов больше или равно d.

- Выбранный полином необходимо проверить на соответствие требуемой корректирующей способности. С этой целью единица с нулями делится на образующий полином. Полученные остатки должны удовлетворять следующим условиям :

a) число различных остатков больше или равно m;

b) вес или число единиц каждого остатка больше или равно $(d\text{-}1)$;

c) остатки должны отличаться друг от друга не менее

Пример

- Если требуется закодировать в циклическом коде, исправляющем однократные ошибки ($s=1$), исходные четырехразрядные двоичные слова ($m=4$), то минимальное кодовое расстояние
  $d > 2s+1=3$ и с использованием оценки

$$k \geq \log_2 \sum_{q=0}^{1} C_n^q = \log_2(C_n^0 + C_n^1) = \log_2(1+n) = \log_2(1+m+k)$$

  или с учетом $m=4$: $2^k \geq 1+m+k$

- Этому неравенству удовлетворяет наименьшее значение $k=3$. Тогда общая длина кодовой комбинации $n=m+k=7$.

Пример

- Разложение двучлена степени $n=7$: $x^7+1=(x+1)(x^3+x+1)(x^3+x^2+1)$. В качестве образующего можно выбрать любой из неприводимых многочленов третьей степени, так как каждый из них имеет по три ($d=3$) ненулевых члена. Выберем полином $P(x)=x^3+x+1$. Остатки от деления единицы с нулями на выбранный полином удовлетворяют перечисленным выше требованиям. Таким образом, полином $P(x)=x^3+x+1$ обеспечивает при построении циклического кода $(7,4)$ кодовое расстояние $d=3$.

- В ряде случаев может получиться, что образующий полином имеет требуемые степень k и число членов $\geq d$, но его применение не обеспечивает заданной корректирующей способности, т.е. при делении $1000\ldots$ на $P(x)$ не получаются требуемые остатки. В этом случае нужно повышать степень k (увеличивать число контрольных символов) до тех пор, пока не будет достигнута заданная корректирующая способность.

Задание для выполнения

- Используя образующий полином $P(x) = x^3+x^2+1$ сформируйте 9-разрядный циклический код (Таблица 1).
- Осуществите его декодирование при неискаженном получении сообщения.
- Осуществите декодирование при искажениях в указанном разряде.
- Определите (Таблица 2) десятичное значение передаваемого числа по принятой кодовой комбинации циклического кода с образующим полиномом $P(x) = x^3+x^2+1$.

Таблица 1

№ варианта	Передаваемое число	Искаженные при передаче разряды
1	32	4; 1
2	33	5; 2
3	34	6; 3
4	35	7; 1
5	36	4; 2
6	37	5; 3
7	38	6; 1
8	39	7; 2
9	40	4; 3
10	41	5; 1
11	42	6; 2
12	43	7; 3
13	44	4; 1
14	45	5; 2
15	46	6; 3

Таблица 1

№ варианта	Передаваемое число	Искаженные при передаче разряды
17	48	4; 2
18	49	5; 3
19	50	6; 1
20	51	7; 2
21	52	6; 3
22	53	5; 1
23	54	6; 2
24	55	7; 3
25	56	5; 1
26	57	6; 2
27	58	6; 1
28	59	7; 2
29	60	6; 3
30	61	7; 1

Таблица 2

№ варианта	Принятый циклический код
1	1000000101
2	1000001011
3	1000010111
4	1000010110
5	1000110111
6	1000001010
7	1001110000
8	1000111100
9	1001000000
10	1001001011
11	1001011101
12	1001001000
13	1001000001
14	1000101100
15	1001110111

Таблица 2

№ варианта	Принятый циклический код
17	1010000001
18	1010000000
19	1010000010
20	1010111111
21	1011100110
22	1010101010
23	1010110011
24	1010111000
25	1011001011
26	1011011110
27	1011110100
28	1010011001
29	1011100001
30	1011101111

Соответствия искаженных разрядов и остатков от деления кодового полинома на образующий $P(x) = x^3+x^2+1$

Разряды	7	6	5	4	3	2	1
Остаток	110	011	111	101	100	010	001

Пример

- Задание. Построить 9-разрядный циклический код числа$(30)_{10}$ и осуществить декодирование его при безошибочной передаче и при искажении в седьмом разряде, используя образующий полином $P(x) = x^3+x^2+1.$

a) Так как используется образующий полином 3-ей степени, то количество проверочных разрядов $k = 3.$

b) Число информационных разрядов исходя из заданной 9-значности кода:
$\boldsymbol{m = n - k} = 9 - 3 = 6.$

Пример

c) *Построение информационного полинома.*
Определяем двоичный код передаваемого числа $(30)_{10}=(011110)_2$ для $m = 6$.
Тогда информационный полином
$G(x) = x^4+x^3+x^2+x.$

d) *Определение проверочной комбинации.*
Она определяется как остаток от деления по модулю 2 **сдвинутого на $k = 3$ разряда влево информационного полинома $G(x)$** на образующий полином $P(x)$. Деление по модулю 2 предполагает последовательные сдвиги и поразрядное сложение по модулю 2, т.е. проверку на неравнозначность, что соответствует 0 при равенстве одноименных разрядов и 1 при их отличии.

Пример

$$
\begin{array}{l|l}
011110000 & 1101 \\
\oplus\underline{1101} & \\
\quad 1000 & 010111 \\
\quad \oplus\ \underline{1101} & \\
\quad\quad 1010 & \\
\quad\quad \oplus\ \underline{1101} & \\
\quad\quad\quad 1110 & \\
\quad\quad\quad \oplus\ \underline{1101} & \\
\quad\quad\quad\quad 011 \leftarrow R(x) = x + 1 &
\end{array}
$$

е) *Формирование кодовой комбинации.*

Комбинация циклического кода, соответствующая $(30)_{10}$ 011110011:

$$F = \underbrace{011110}_{m}\ \underbrace{011}_{k}$$

Пример

- Особенность кодовых полиномов, используемых при циклических кодах в том, что полученный полином $F(x)$ делится без остатка на образующий полином $P(x)$. Если у принятого полинома после его проверки остаток отсутствует, то значит кодовая комбинация принята без искажений. Ненулевой остаток указывает на наличие ошибок и их места. Для полинома $P(x) = x^3+x^2+1$ одиночные ошибки в разрядах приводят к образованию остатков в соответствии с Таблицей 3.

Пример

f) Декодирование принятой кодовой комбинации

При неискаженном прохождении полученный код имеет вид F=011110011, проверка правильности сводится к определению остатка от деления по модулю 2 $F(x)$ на $P(x)$:

$$
\begin{array}{l|l}
011110011 & 1101 \\
\oplus\underline{1101} & \\
\quad 1000 & 010111 \\
\quad\oplus\underline{1101} & \\
\quad\quad 1011 & \\
\quad\quad\oplus\underline{1101} & \\
\quad\quad\quad 1101 & \\
\quad\quad\quad\oplus\underline{1101} & \\
\quad\quad\quad\quad 000 \leftarrow R(x)=0 & \text{остаток равен 0, т.е.}
\end{array}
$$

Пример

- Информационный полином $G(x)$ в первых шести (m=6) разрядах $F(x)$ определяет передаваемое число:

$$G(x) = 0 \cdot x^5 + 1 \cdot x^4 + 1 \cdot x^3 + 1 \cdot x^2 + 1 \cdot x^1 + 0 \cdot x^0 =$$
$$= 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 = 30$$

- При искаженной передаче в 7 разряде кодовая комбинация будет иметь вид $F(x)$ =010110011.

Пример

- Проверка принятой комбинации

$$
\begin{array}{l|l}
0101100011 & 1101 \\
\oplus\underline{1101} & \\
\quad 1100 & 011001 \\
\quad\oplus\ \underline{1101} & \\
\qquad 1011 & \\
\qquad\oplus\ \underline{1101} & \\
\qquad\ 110 \leftarrow R(x)= x^2+x. &
\end{array}
$$

- По значению остатка $R(x)=110$ и Таблице 3 можно судить об искажении при передаче в 7 разряде. Для исправления этот разряд надо инвертировать. Информационный полином соответствует первым шести разрядам, тогда

$$G=011110=1\cdot 2^4+1\cdot 2^3+1\cdot 2^2+1\cdot 2^1=30$$

$$F^*=0101110011 \rightarrow F=0111110011$$

Пример 2

- По заданной комбинации циклического кода F^*=1011001 с $P(x) = x^3+x^2+1$ восстановить десятичное значение передаваемого числа.

a) Количество проверочных разрядов: $k=3$.

b) Количество информационных разрядов $\boldsymbol{m = n - k} = 7 - 3 = 4$.

c) Проверка правильности передачи кодовой комбинации:

$$
\begin{array}{l|l}
1011001 & 1101 \\
\oplus\underline{1101} & \\
1100 & 011001 \\
\oplus\ \underline{1101} & \\
101 & \\
\end{array}
$$

$101 \rightarrow R(x)= x^2+1$

Пример

- Вид полученного остатка в соответствии с Таблицей 3 указывает, что ошибка произошла 4 разряде, который надо инвертировать.

d) Исправление кодовой комбинации:

$$F^{*}=1011001 \rightarrow F=1010001$$

(G — выделенная часть F)

e) Выделение информационного полинома и его декодирование:

$$G(x) = 1\cdot x^3+0\cdot x^2+1\cdot x^1+ 0\cdot x^0 =$$

$$=1\cdot 2^3 + 1\cdot 2^1 =8+2=10 \rightarrow$$ Ответ: передано число 10.

Задание для самостоятельной работы

- Написать программу кодирования сообщений с помощью циклического корректирующего кода.
- **Входные данные**:

a) Значность кода n и количество информационных разрядов m;

b) Коэффициенты образующего полинома степени $n-m$;

c) Сообщение длиной m двоичных разрядов;

- **Выходные данные**: кодовая последовательность (m информационных, потом $n-m$ корректирующих разрядов) для