Циклические коды

•Относятся к классу линейных, систематических,

•Сумма по модулю 2 двух разрешённых кодовых комбинаций даёт также разрешённую кодовую комбинацию

•Каждый вектор (кодовое слово), получаемый из исходного кодового вектора путём циклической перестановки его символов, также является разрешённым кодовым вектором,

при циклической перестановке символы кодового слова перемещаются слева направо на одну позицию:

Пример1. *Если кодовое слово -* **1101100**, то разрешённой кодовой комбинацией будет и - **0110110**

•Принято описывать циклические коды (ЦК) при помощи порождающих полиномов **G(X)** степени **r = n — k**, где **r** — число проверочных символов в кодовом слове

Пример2. Переведём кодовое слово **Xn = 101100** в полиномиальный вид:

$$Bi(X) = 1 * X^5 + 0 * X^4 + 1 * X^3 + 1 * X^2 + O * X^1 + O * X^0 = X^5 + X^3 + X^2$$

•Операции кодирования и декодирования ЦК сводятся к известным процедурам умножения и деления полиномов

- Действия с кодовыми словами в виде полиномов производятся по правилам арифметики по модулю 2 (вычитание равносильно сложению).

Пример3. Из равенства $\mathbf{X^n - 1 = 0}$ получаем $\mathbf{X^n = 1}$. Прибавив к левой и правой частям по единице, имеем $\mathbf{X^n + 1 = 1 + 1 = 0}$. Таким образом, вместо двучлена $\mathbf{X^n - 1}$ можно ввести бином $\mathbf{X^n + 1}$ или $\mathbf{1 + X^n}$, из чего следует, что $\mathbf{X^n + X^n = X^n (1 + 1) = 0}$

- Приведём далее порядок суммирования (вычитания), умножения и деления полиномов (по модулю 2). В примерах используем вышеприведённые кодовые комбинации

$\mathbf{A_1(X) = X^5 + X^3 + X^2}$ **(101100)** и $\mathbf{A_2(X) = X^4 + X^2 + X}$ **(10110)**.

Суммирование (вычитание):

$\mathbf{A_1(X) + A_2(X) = A_1(X) - A_2(X) = X^5 + X^4 + X^3 + X^2 + X^2 + X = X^5 + X^4 + X^3 + X}$

Или **101100**

10110

$\mathbf{111010 = X^5 + X^4 + X^3 + X}$

- Умножение:

$A_1(X) * A_2(X) = (X^5 + X^3 + X^2) * (X^4 + X^2 + X) = X^9 + X^7 + X^6 + X^7 + X^5 + + X^4 + X^6 + X^4 + X^3 = X^9 + X^5 + X^3 = 1000101000$.

- Деление:

$$\begin{array}{l|l} X^5 + X^3 + X^2 & X^4 + X^2 + X \\ \cline{2-2} X^5 + X^3 + X^2 & X \\ \hline 0 \quad 0 \quad 0 & \end{array}$$

- остаток при делении **R(X) = 0**.

При циклическом сдвиге вправо на один разряд необходимо исходную кодовую комбинацию поделить на X, а умножение на X эквивалентно сдвигу влево на один символ

Порождающие полиномы циклических кодов

- **Формирование разрешённых кодовых комбинаций ЦК B_j *(X)* основано на предварительном выборе порождающего (образующего) полинома G(X), который обладает важным отличительным признаком: все комбинации B_j (X) делятся на порождающий полином G(X) без остатка:**

$$B_j(X) / G(X) = A_j(X) \qquad (1)$$

(при остатке $R(X) = 0$);

Здесь $B_j(X) = Xn$ **- кодовое слово**

$A_j(X) = Xk$ **- информационное слово**

Степень порождающего полинома определяет число проверочных символов $r = n - k$

Из этого свойства следует простой способ формирования разрешенных кодовых слов ЦК — умножение **информационного слова** на порождающий полином **G(X)**:

$$B(X) = A(X)G(X). \qquad (2)$$

Порождающими могут быть только такие полиномы, которые являются делителями двучлена (бинома) X^n+1:

$$(X^n+1)/G(X) = H(X) \qquad (3)$$

при нулевом остатке: **$R(X) = 0$.**

С увеличением максимальной степени порождающих полиномов **r** резко увеличивается их количество: при $r = 3$ имеется всего два полинома, а при $r = 10$ их уже несколько десятков

Пример Найти порождающий многочлен (ПМ) линейного циклического кода длины $n = 15$, который осуществляет кодирование сообщений длины $k = 7$.

Если нам нужен ПМ для кода длины 15 при длине сообщения 7, то нужно найти делитель $x^{15} + 1$ степени $15 - 7 = 8$.

Многочлен $x^{15} + 1$ разлагается на множители (***как? основной вопрос***) :

$$x^{15} + 1 = (1 + x)(1 + x + x^2)(1 + x + x^2 + x^3 + x^4)(1 + x + x^4)(1 + x^3 + x^4),$$

поэтому можно взять $G(x) = (1 + x + x^2 + x^3 + x^4)(1 + x + x^4) = 1 + x^4 + x^6 + x^7 + x^8$

или $(1 + x + x^4)(1 + x^3 + x^4) = \dots$

Степень полин, r	Полином G(X)	Двоичное представ полинома	n	k	Примечание
1	$X+1$	11	3	2	Код с проверкой на чётность (КПЧ)
2	X^2+X+1	111	3	1	Код с повторением
3	X^3+X^2+1 X^3+X+1	1101 1011	7	4	Классический код Хемминга
4	X^4+X^3+1 X^4+X+1 X^4+X^2+X+1 $X^4+X^3+X^2+1$	11001 10011 10111 11101	15 15 7 7	11 11 3 3	Классический код Хемминга, Коды Файра-Абрамсона
5	X^5+X^2+1 X^5+X^3+1	100101 101001	31	26	Классический код Хемминга

Примеры полиномов

r, степень полинома	порождающий полином
2	111
3	1011
4	10011
5	100101, 111101, 110111
6	1000011, 1100111
7	10001001, 10001111, 10011101
8	111100111, 100011101, 101100011

- Два варианта порождающих полиномов кода Хемминга (7,4), с записью по модулю 2 в виде **1101** и **1011**, представляют собой так называемые **двойственные многочлены** (полиномы):весовые коэффициенты одного полинома, зачитываемые слева направо, становятся весовыми коэффициентами двойственного полинома при считывании их справа налево
- Порождающие полиномы кода Хемминга (7,4) являются не только **двойственными**, они также являются **неприводимыми**.
- ***Неприводимые полиномы*** не делятся ни на какой другой полином степени меньше **r**, поэтому их называют ещё **неразложимыми, простыми и примитивными**.
- Порождающий полином **G(X) = X^7 +1** раскладывается на три неприводимых полинома:

$$X^7+1=(X+1)(X^3+X^2+1)(X^3+X+1)=G_1(X)\times G_2(X)\times G_3(X),$$

каждый из которых является порождающим для следующих кодов:

$\mathbf{G_1(X) = X+ 1}$ - код с проверкой на чётность, КПЧ (7, 6);

$\mathbf{G_2(X) = X^3 + X^2+ 1}$ - первый вариант кода Хемминга (7,4);

$\mathbf{G_3(X)} = \mathbf{X^3 + X+ 1}$ - двойственный $G_2(X)$, второй вариант кода Хемминга.

- Различные вариации произведений **$G_{1,2,3}$ (X)** дают возможность получить остальные порождающие полиномы:

$$\mathbf{G_4 (X) = G_1 (X)G_2 (X) = (X + 1)(X^3 + X^2+ 1) = X^4 + X^2+ X +1}$$

- код Абрамсона (7,3);

$$\mathbf{G_5 (X) = G_1 (X)\, G_3 (X) = (X + 1)(X^3 + X+ 1) = X^4 + X^3+ X^2 +1}$$

- двойственный $G_4(X)$;

$$\mathbf{G_6 (X) = G_2 (X)G_3 (X) = (X^3 + X^2+ 1)(X^3 + X+ 1) =}$$

$$\mathbf{= X^6 + X^5 +X^4 + X^3 + X^2+ X +1}$$

- код с повторением (7,1)

- **Порождающая матрица *G*** циклического кода имеет в качестве строк векторы $G(x), xG(x),\dots, x^{k-1}G(x)$:

$$G = \begin{vmatrix} G(x) \\ G(x)/\,x \\ \dots \\ G(x)/\,x^{k-1} \end{vmatrix} = \begin{vmatrix} g_0\ g_1\ g_2\ \dots\ g_r\ \ 0\ \dots & & 0 \\ 0\ \ g_0\ g_1\ g_2\ \dots\ g_r\ 0\ \dots & & 0 \\ & \dots\dots\dots & \\ 0\ \dots & 0\ \ g_0\ g_1\ g_2\ \dots\ g_r \end{vmatrix}$$

где $g_0, \dots, g_r$ - коэффициенты генераторного полинома

Проверочная матрица H кода строится на основе полинома:

$$H(X) = (X^n + 1)/\,G(X) \qquad (4)$$

(сравни с (3))

$$H = \begin{vmatrix} H(x) \\ xH(x) \\ \\ x^{r-1}H(x) \end{vmatrix} = \begin{vmatrix} 0\ \dots & 0\ \ h_k\ \dots & h_2\ h_1\ h_0 \\ 0\ \dots & h_k\ \ h_{k-1}\ \dots & h_1\ h_0\ 0 \\ & \dots\dots\dots & \\ h_k\ \dots & h_1\ \ h_0\ \ 0\ \dots & 0 \end{vmatrix}$$

Справедливо: $G * H^T = 0$ или $H * G^T = 0$ (5)

где h_j - коэффициенты полинома H(X)

Пример 4. Задан ЦК (7,4) дуальными порождающими полиномами **$G(7,4) = X^3+X+1$** и **$\underline{G}$ *(7,4)*= $X^3 + X^2 +1$**. Составить порождающие матрицы кодов.

Решение. Первой строкой в матрице записывается порождающий полином (в двоичном представлении) с домножением его на оператор сдвига **Xr** для резервирования места под запись **r = 3** проверочных символов. Следующие **k - 1** строк матриц получаются путём последовательного циклического сдвига базового кодового слова матриц **G** и **$\underline{G}$** на одну позицию вправо

$$G(7,4) = \begin{matrix} 1011000 \\ 0101100 \\ 0010110 \\ 0001011 \end{matrix} \qquad \underline{G}(7,4) = \begin{matrix} 1101000 \\ 0110100 \\ 0011010 \\ 0001101 \end{matrix}$$

•Для построения порождающей матрицы, формирующей разделимый блочный код, необходимо матрицу преобразовать к каноническому виду путём линейных операций над строками

Каноническая матрица должна в левой части порождающей ЦК матрицы содержать единичную диагональную квадратную подматрицу порядка " **k** " для получения в итоге блочного ЦК.

С этой целью для получения первой строки канонической матрицы **Gк(7,4)** необходимо сложить по *модулю 2* строки с номерами 1, 3 и 4 матрицы **G(7, 4),** а для матрицы **<u>Gк</u>** ***(7,4)*** — строки с номерами 1, 2 и 3 матрицы **<u>G</u>*(7,4)*.** В итоге имеем следующий вид дуальных канонических матриц:

	1000 101	**1+3+4**	
Gк(7,4) =	0100 111	**2+4**	**<u>Gк</u>(7,4) = (самостоят.)**
	0010 110	**3=3**	
	0001 011	**4=4**	

- Проверочная матрица $\mathbf{H_{7,4}}$ размерностью **n x r** может быть получена из порождающей матрицы канонического вида путем дополнения проверочной подматрицы единичной матрицей размерности **r x r**

$$
H_{7,4} = \begin{array}{c} 101 \\ 111 \\ 110 \\ 011 \\ \hline 100 \\ 010 \\ 001 \end{array}
$$

или в канонич. виде:

$$
(H_{7,4})^T = \begin{array}{c|c} 1110 & 100 \\ 0111 & 010 \\ 1101 & 001 \end{array}
$$

Вычисление проверочных символов

- Вычисление символов (**Xr**) кодового слова (**Xn**) чаще всего основывается на **методе деления полиномов**
- Метод позволяет представить разрешенные к передаче кодовые комбинации в виде разделенных информационных **Xk** и проверочных **Xr** символов, т. е. получить блочный код
- Поскольку число проверочных символов равно **r**, то для компактной их записи в последние младшие разряды кодового слова надо предварительно к **Xk** ($\mathbf{A_j(X)}$ - в формуле (1)) справа приписать **r** "нулей", что эквивалентно умножению **Xk** на оператор сдвига ***X*** **r**

при этом имеется возможность представить кодовую комбинацию в виде последовательности информационных и проверочных символов:

$$\mathbf{Xn = Xk \cdot Xr \,||\, R\,(X),} \qquad (6)$$

где **R (X)** — остаток от деления **Xk ·Xr /G(X)** (см. (2)).

- В алгоритме на основе (6) можно выделить три этапа формирования разрешенных кодовых комбинаций в кодере:

1) к комбинации слова **Xk** дописывается справа r нулей, что эквивалентно умножению **Xk** на **Xr** ;

2) произведение **Xk** * **X**r делится на соответствующий порождающий полином **G(X)** и определяется остаток **R(X),** степень которого не превышает **r - 1**, этот остаток и дает группу проверочных символов (**Xr**);

3) вычисленный остаток присоединяется справа к **Xk** .

Пример 5. Рассмотрим процедуру кодирования для при **Xk =1001**, т.е. сформируем кодовое слово циклического кода (7,4).

В заданном ЦК n = 7, k = 4, r = 3, выберем порождающий полином $\mathbf{G(X) = X^3 + X + 1}$ (код Хемминга).

$\mathbf{Xk} = \mathbf{1001} \sim \mathbf{X^3 + 1}$, (знак " ~ " – *тильда* означает соответствие).

1. **Xk ·Xr = (X^3 + 1) · X^3 = X^6 + X^3** ~ **1001000**, (n =7).

2. **Xk ·Xr /G(X) =**

$$\begin{array}{r|l} X^6 + X^3 & X^3 + X + 1 \\ \cline{2-2} X^6 + X^4 + X^3 & X^3 + X \\ \hline X^4 & \\ X^4 + X^2 + X & \\ \hline X^2 + X & \end{array}$$

X^2+ X - остаток ; **R (X) = X^2 + X** ~ **110**.

3. **Xn = Xk ·Xr || R (X) = 1001110** - итоговая комбинация ЦК (кодовое слово).

Пример 6. Показать процедуру формирования кодового слова **Xn** циклического кода, если **Xk =1001** и порождающий полином

G(X) = X^3 + X^2 + 1

Пример 7. Выполнить операции для тех же **G(X)** , если **Xk =1010 и Xk** = **0101** (дома)

Синдромный метод декодирования ЦК

- Основная операция: принятое кодовое слово (**Yn**) нужно поделить на порождающий полином.
- Если **Yn** принадлежит коду, т. е. не искажено помехами, то остаток от деления (**синдром**) будет нулевым.
- Ненулевой остаток свидетельствует о наличии ошибок в принятой кодовой комбинации
- Для исправления ошибки нужно определить **вектор (полином) ошибки En**
- После передачи по каналу с помехами принимается кодовое слово

$$Y_n = X_n + E_n \qquad (7)$$

- При декодировании принятое кодовое слово делится на ***G(X)***:

$$(Y_n)\ /(G(X)) = U,\ S_r \qquad (8)$$

S_r **-** остаток от деления $(Y_n)\ /(G(X))$ **- синдром**

•Всякому ненулевому синдрому соответствует определенное расположение (конфигурация) ошибок: **синдром для ЦК имеет те же свойства, что и для кода Хемминга** (используются при декодировании синдрома)

Пример 7 . Рассмотрим процедуру декодирования сообщения, сформиров-го в примере 5.

Пусть $\mathbf{Y_n}$ =10**1**1110.

1.Выполняем деление в соотв. с (8):

$$\begin{array}{l|l} \mathbf{Y_n / G(X) = X^6 + X^4 + X^3 + X^2 + X} & \mathbf{X^3 + X + 1} \\ \cline{2-2} \quad \underline{\mathbf{X^6 + X^4 + X^3}} & \quad \mathbf{X^3} \\ \qquad\qquad \mathbf{X^2 + X} & \end{array}$$

X2 + X – остаток, $\mathbf{S_r = X^2 + X \sim 110}$

2. Декодирование синдрома – позволяет определить местоположение ошибки : по полученному синдрому 110 в анализаторе синдрома (дешифраторе синдрома) определяем вид вектора $\mathbf{E_n = 0010000}$

3. Исправление ошибки: $\mathbf{Y_n + E_n = 10\underline{1}1110 + 0010000 = 10\underline{0}1110}$