



Лекция № 6

«Методы кодирования»

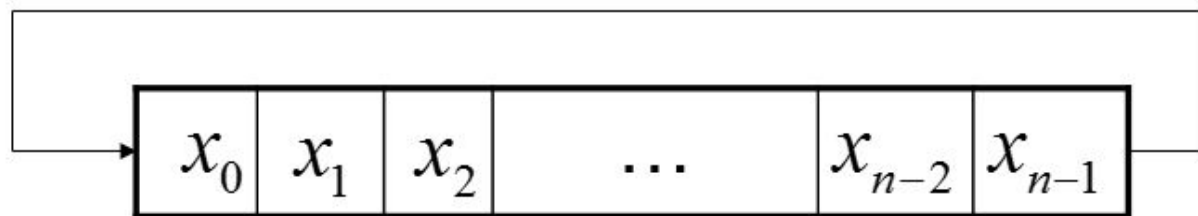
Циклический код.

Ведущий преподаватель: канд. техн. наук, доцент кафедры ИУТС Альчаков Василий Викторович

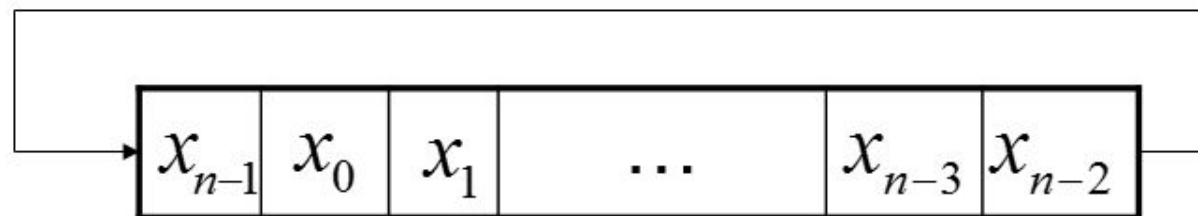
2 ЦИКЛИЧЕСКИЕ КОДЫ

Основные свойства циклических кодов

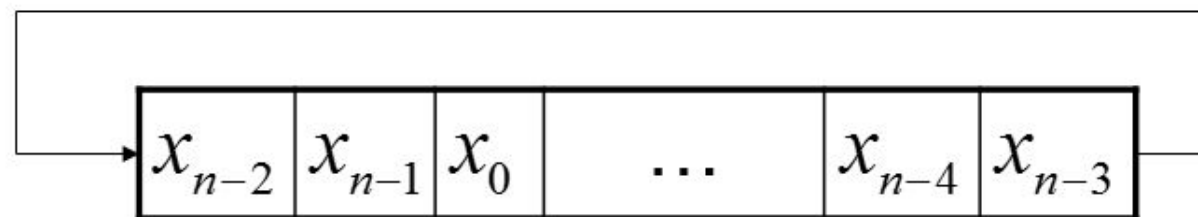
Если некоторая кодовая комбинация принадлежит циклическому коду, то комбинация, полученная циклической перестановкой исходной комбинации (циклическим сдвигом), также принадлежит данному коду



$$(x_0, x_1, x_2, \boxtimes, x_{n-2}, x_{n-1})$$



$$(x_{n-1}, x_0, x_1, x_2, \boxtimes, x_{n-2})$$



$$(x_{n-2}, x_{n-1}, x_0, x_1, x_2, \boxtimes, x_{n-3})$$

Вторым свойством всех разрешенных комбинаций циклических кодов является их делимость без остатка на некоторый выбранный полином, называемый **производящим** или **образующим**.

Характеристика циклических кодов

Циклический код относится к систематическим блочным (n, k) – кодам, в которых k первых разрядов представляют собой комбинация первичного кода, а последующие $(n-k)$ разрядов являются проверочными.

В основе построения циклических кодов лежит операция деления передаваемой кодовой комбинации на порождающий неприводимый полином степени r .

Остаток от деления используется при формировании проверочных разрядов. При этом операции деления предшествует операция умножения, осуществляющая сдвиг влево k –разрядной информационной кодовой комбинации на r разрядов.

При декодировании принятой n –разрядной кодовой комбинации опять производится деление на порождающий (производящий, образующий) полином.

4 ЦИКЛИЧЕСКИЕ КОДЫ

Способность исправлять ошибки

Пусть общее число бит в блоке равно n , из них полезную информацию несут в себе m бит, тогда в случае ошибки имеется возможность исправить s бит. Зависимость s от m и n для кодов можно представить в виде таблицы.

Зависимость общего числа разрядов комбинаций от количества информационных и исправляемых разрядов

| Общее число битов, n | Число полезных битов, m | Число исправляемых битов, s |
|------------------------|---------------------------|-------------------------------|
| 31 | 26 | 1 |
| | 21 | 2 |
| | 16 | 3 |
| 63 | 57 | 1 |
| | 51 | 2 |
| | 45 | 3 |
| 127 | 120 | 1 |
| | 113 | 2 |
| | 106 | 3 |

5 ЦИКЛИЧЕСКИЕ КОДЫ

Представление в виде многочленов

$$A_{n-1}(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \boxtimes + a_1x + a_0$$

$$a_{n-1} = \{0, 1\}$$

$$x^5 + x^3 + x^2 + 1 \Leftrightarrow 101101$$

7 ЦИКЛИЧЕСКИЕ КОДЫ

Неприводимые многочлены

Идея построения циклических кодов базируется на использовании **неприводимых многочленов**.

Неприводимым называется многочлен, который не может быть представлен в виде произведения многочленов низших степеней, т.е. делится только на самого себя или на единицу и не делится ни на какой другой многочлен.

На такой многочлен делится без остатка двучлен

$$(x^n + 1)$$

Неприводимые многочлены в теории циклических кодов играют роль **порождающих** полиномов.

Порождающий полином

Требования к порождающим полиномам

- 1) $P(x)$ должен быть ненулевым;
- 2) Вес $P(x)$ не должен быть меньше минимального кодового расстояния $V(P(x)) \geq d_{\min}$;
- 3) $P(x)$ должен иметь максимальную степень k , где k – число избыточных элементов в коде;
- 4) $P(x)$ должен быть делителем полинома $(x^n + 1)$.

Циклический код – это код, все рабочие комбинации которого делятся на порождающий полином без остатка

$$r \geq \log_2(n + 1)$$

Порождающие полиномы

Примеры порождающих полиномов

| Степень полинома r | Порождающий полином $P(x)$ |
|----------------------|---------------------------------|
| 2 | 111 |
| 3 | 1011 |
| 4 | 10011 |
| 5 | 100101, 111101, 110111 |
| 6 | 1000011, 1100111 |
| 7 | 10001001, 10001111, 10011101 |
| 8 | 111100111, 100011101, 101100011 |

10 ЦИКЛИЧЕСКИЕ КОДЫ

Алгоритм кодирования

$$P(x) = a_{r-1}x^r + a_{r-2}x^{r-1} + \boxtimes + 1$$

$$A_m(x)$$

1. Исходная кодовая комбинация представляется в виде $A_m(x)$

$$1101 \rightarrow A_m(x) = x^3 + x^2 + 1$$

2. Многочлен $A_m(x)$ умножают на x^r . Степень порождающего полинома r равна значению старшего разряда исходной кодовой комбинации. $A_m(x) \cdot x^r$

$r = 3$ – число контрольных символов

$$A_m(x) \cdot x^r = (x^3 + x^2 + 1)x^3 = x^6 + x^5 + x^3 \Rightarrow 1101000$$

11 ЦИКЛИЧЕСКИЕ КОДЫ

Алгоритм кодирования

3. Определяют проверочные разряды, дополняющие исходную кодовую комбинацию до разрешенной, как остаток от деления полученного в предыдущем пункте многочлена на образующий полином.

Выбираем образующий полином степени $r = 3$

$$P(x) = x^3 + x + 1$$

Необходимо вычислить

$$\frac{A_m(x) \cdot x^r}{P(x)}$$

| | | | | | |
|----------|-------------------|--|---------------------|---|--------|
| \oplus | $x^6 + x^5 + x^3$ | | $x^3 + x + 1$ | | |
| | $x^6 + x^4 + x^3$ | | $x^3 + x^2 + x + 1$ | | |
| | <hr/> | | | | |
| \oplus | $x^5 + x^4$ | | | | |
| | $x^5 + x^3 + x^2$ | | | | |
| | <hr/> | | | | |
| \oplus | $x^4 + x^3 + x^2$ | | | | |
| | $x^4 + x^2 + x$ | | | | |
| | <hr/> | | | | |
| \oplus | $x^3 + x$ | | | | |
| | $x^3 + x + 1$ | | | | |
| | <hr/> | | | | |
| | | | | 1 | = R(x) |

12 ЦИКЛИЧЕСКИЕ КОДЫ

Алгоритм кодирования

4. Окончательно разрешенная кодовая комбинация циклического кода определяется как $A_{n-1}(x) = A_m(x)x^r + R(x)$

$$x^6 + x^5 + x^3 + 1 \Rightarrow 1101001$$

Если разделить $\frac{A_{n-1}(x)}{P(x)}$ в результате получится нулевой

остаток.

13 ЦИКЛИЧЕСКИЕ КОДЫ

Алгоритм декодирования

1. Выявляем факт наличия ошибки

Получаем остаток от деления принятой кодовой комбинации на образующий полином. Остаток от деления обозначаем

$$\frac{A_{n-1}(x)}{P(x)} = R_0(x)$$

| | | | | | | | |
|---|---|---|---|---|---|---|-----------------------------|
| 1 | 1 | 0 | 1 | 0 | 0 | 1 | исходная кодовая комбинация |
| 1 | 1 | 0 | 0 | 0 | 0 | 1 | |
| 1 | 1 | 0 | 0 | 0 | 0 | 1 | |
| 1 | 0 | 1 | 1 | | | | |
| | 1 | 1 | 1 | 0 | | | |
| | 1 | 0 | 1 | 1 | | | |
| | | 1 | 0 | 1 | 0 | | |
| | | 1 | 0 | 1 | 1 | | |
| | | | 0 | 1 | 1 | | ненулевой остаток |

15 ЦИКЛИЧЕСКИЕ КОДЫ

Алгоритм декодирования

1. Принятая комбинация делится на образующий многочлен $P(x)$. Если остаток $R(x) \neq 0$, то определяется вес остатка w . Если вес остатка равен или меньше числа исправляемых ошибок t ($w \leq t$), то принятую комбинацию складывают по модулю 2 с остатком и получают исправленную комбинацию.
2. Если $w > t$, то производится циклический сдвиг принятой кодовой комбинации на один символ влево и полученная после такого сдвига комбинация снова делится на образующий многочлен. Если вес полученного остатка $w \leq t$, то циклически сдвинутую комбинацию складывают с остатком и затем после сложения циклически сдвигают в обратную сторону вправо на один символ (возвращают на прежнее место). В результате получаем исправленную комбинацию.
3. Если после циклического сдвига на один символ по-прежнему $w > t$, то производят дополнительные циклические сдвиги влево. При этом после каждого сдвига осуществляется деление сдвинутой комбинации на $P(x)$ и проверяется вес остатка. При $w \leq t$ сдвинутую комбинацию складывают с остатком и производят обратных циклических сдвигов вправо столько, сколько было сделано влево.

