Помехоустойчивое кодирование

Циклические коды – подкласс линейных кодов

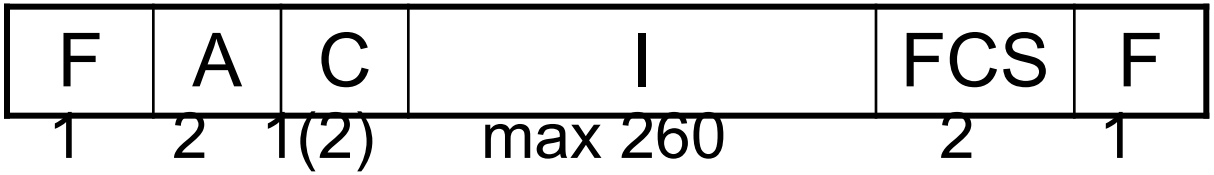
Примеры использования линейных кодов

- Пример 1. Протокол передачи данных по телефонному каналу ISDN-D, в котором используется формат передачи данных LAPD.

1	2	1(2)	max 260	2	1
F	A	C	I	FCS	F

Примеры использования линейных кодов

- F=01111110 (flag)
- A – поле адреса (address)
- C поле команд (control)
- I –информационное поле (information)
- FCS – проверочные разряды (frame check sequence)
- Общая длина 266x8=21128 бит, проверочных – 16 бит



Примеры использования линейных кодов

- Пример 2. Протокол передачи данных в 802.3 CSMA/CD для передачи данных в локальных сетях связи (LAN)

Преамбула	7
Разделитель	1
Адрес получателя	2(6)
Адрес источника	2(6)
Данные	65-1518
Контроль четности	4

Линейные циклические коды

Циклические коды интенсивно изучаются, так как:

- Циклические коды обладают богатой алгебраической структурой, что используется в различных приложениях.
- Для циклических кодов чрезвычайно кратко формулируются технические требования (спецификации).
- Циклические коды легко реализуются с помощью *сдвиговых регистров.*
- Многие практически важные коды являются циклическими.

Линейные циклические коды

Линейный *(n,k)*-код *C* называется *циклическим,* если *циклический сдвиг* любого кодового слова из *C* также принадлежит *C:*

$$\chi = \begin{bmatrix} x_0 \\ x_1 \\ \dots \\ x_{n-2} \\ x_{n-1} \end{bmatrix} \Rightarrow \chi^{(1)} = \begin{bmatrix} x_{n-1} \\ x_0 \\ \dots \\ x_{n-3} \\ x_{n-2} \end{bmatrix}$$

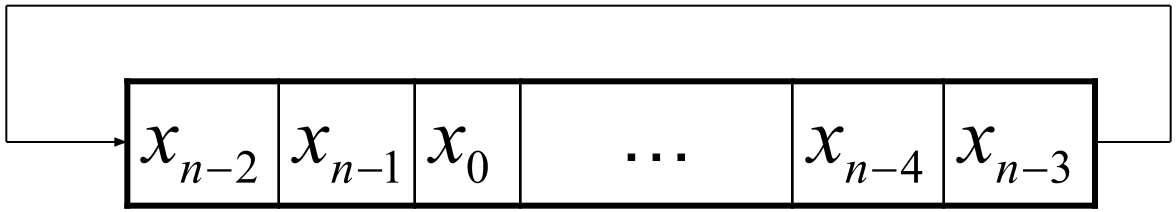
Реализация циклического сдвига

Циклический сдвиг реализуется с помощью *регистра сдвига* длины *n* с обратной связью:

Реализация циклического сдвига

Регистр сдвига на такте 1

Регистр сдвига на такте 2



Замечания

- Для задания произвольного кода из 2^k слов длины n необходимо выписать все 2^k кодовых слов длины n.
- Для задания линейного кода из 2^k слов длины n достаточно выписать базисных слов длины n (порождающая матрица).
- Для задания линейного циклического кода из 2^k слов длины n достаточно выписать *одно* кодовое слово.

Представление кодовых слов в виде кодовых многочленов

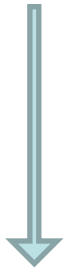
$$\alpha = \begin{bmatrix} a_0 \\ a_1 \\ \dots \\ a_{n-2} \\ a_{n-1} \end{bmatrix} \Rightarrow a(x) = a_0 \oplus a_1 x \oplus \dots \oplus a_{n-1} x^{n-1}$$

Представление кодовых слов в виде многочленов

Кодовое слово	Многочлен
0000	0
1010	$1+x^2$
0101	$x+x^3$
1111	$1+x+x^2+x^3$

Действие циклического сдвига на многочлен

$$a(x) = a_0 \oplus a_1 x \oplus \ldots \oplus a_{n-1} x^{n-1}$$



$$a^{(1)}(x) = a_{n-1} \oplus a_0 x \oplus \ldots \oplus a_{n-3} x^{n-2} \oplus a_{n-2} x^{n-1}$$

Сложение и умножение многочленов по модулю

$$1 = x^n \pmod{x^n \oplus 1}$$

Пример

$$a(x) = 1 \oplus x \oplus x^3, \quad n = 7 \Rightarrow$$

$$\Rightarrow 1101000$$

Пример

$$(1 \oplus x \oplus x^4)a(x) = (1 \oplus x \oplus x^4)(1 \oplus x \oplus x^3) =$$

$$= 1 \oplus x \oplus x^4 \oplus x \oplus x^2 \oplus x^5 \oplus x^3 \oplus x^4 \oplus x^7 =$$

$$1 \oplus x^2 \oplus x^3 \oplus x^5 \oplus x^7 = 1 \oplus x^2 \oplus x^3 \oplus x^5 \oplus 1 \,(\mathrm{mod}\, x^7 \oplus 1) =$$

$$= x^2 \oplus x^3 \oplus x^5 \bmod(x^7 \oplus 1)$$

Пример

$$(1 \oplus x \oplus x^4)a(x) = (1 \oplus x \oplus x^4)(1 \oplus x \oplus x^3) =$$

$$1101000 \quad \oplus$$

$$0110100 \quad \oplus$$

$$1000110 \quad =$$

$$0011010 \Rightarrow x^2 \oplus x^3 \oplus x^5$$

Действие циклического сдвига на многочлен

$$a(x) = a_0 \oplus a_1 x \oplus \ldots \oplus a_{n-1} x^{n-1}$$

$$a^{(1)}(x) = a_{n-1} \oplus a_0 x \oplus \ldots \oplus a_{n-3} x^{n-2} \oplus a_{n-2} x^{n-1} =$$

$$= a_0 x \oplus \ldots \oplus a_{n-3} x^{n-2} \oplus a_{n-2} x^{n-1} \oplus a_{n-1} x^n (\mathrm{mod}\, x^n \oplus 1) =$$

$$= x \cdot a(x) (\mathrm{mod}\, x^n \oplus 1)$$

Циклический сдвиг многочлена на *i* позиций

$$\alpha^{(i)} = \begin{bmatrix} a_{n-i} \\ a_{n-i+1} \\ \dots \\ a_{n-i-2} \\ a_{n-i-1} \end{bmatrix} \Rightarrow x^i \cdot a(x) (\mathrm{mod}\, x^n \oplus 1)$$

- Пространство слов длины *n* – множество многочленов степени $\leq n$

- Циклический код длины *n* – подмножество многочленов степени $\leq n-1$

Важные теоремы

- *Теорема 1.* Циклический код содержит единственный кодовый многочлен минимальной степени.
- *Теорема 2.*Если $g(x)$ – кодовый многочлен минимальной степени, то его младший коэффициент $g_0 = 1.$
- *Теорема 3.*Пусть $g(x)$-кодовый многочлен минимальной степени. Многочлен $a(x)$ является кодовым многочленом тогда и только тогда, когда он кратен $g(x).$

Порождающий многочлен

Пусть $g(x)$ -кодовый многочлен минимальной степени, этот многочлен называется *порождающим многочленом.*

Базис *(n,k)*- кода: *к* базисных многочлена

$$\left\{g(x), x \cdot g(x), x^2 \cdot g(x), ..., x^{k-1} \cdot g(x)\right\}$$

Степень порождающего многочлена

$$\deg g(x) = n - k$$

Теоремы о порождающем многочлене

- *Теорема1*. Порождающий многочлен циклического кода $g(x)$ делит без остатка многочлен $x^n \oplus 1.$.
- *Теорема 2*. Если некоторый многочлен $g(x)$ - степени *n-k* делит многочлен $x^n \oplus 1$ без остатка, то $g(x)$ порождает циклический *(n,k)*-код.

Пример

Разложение

$$x^7 \oplus 1 = (x \oplus 1)(1 \oplus x \oplus x^3)(1 \oplus x^2 \oplus x^3)$$

Различные циклические коды

$$g(x) = 1$$

$$g(x) = 1 \oplus x$$

$$g(x) = 1 \oplus x \oplus x^3$$

$$g(x) = 1 \oplus x^2 \oplus x^3$$

$$g(x) = (1 \oplus x)(1 \oplus x \oplus x^3)$$

$$g(x) = (1 \oplus x)(1 \oplus x^2 \oplus x^3)$$

$$g(x) = (1 \oplus x \oplus x^3)(1 \oplus x^2 \oplus x^3)$$

$$g(x) = (1 \oplus x)(1 \oplus x \oplus x^3)(1 \oplus x^2 \oplus x^3)$$

Кодирование

- Кодирование циклического кода – умножение информационного многочлена на порождающий многочлен

Циклический (7,4)-код Хэмминга

- $g(x) = 1 \oplus x \oplus x^3$

инф.сл.	кодовое сл.	многочлен
0000	0000000	$0 \cdot g(x)$
1000	1101000	$\mathbf{1 \cdot g(x)}$
0100	0110100	$\mathbf{x \cdot g(x)}$
1100	1011100	$(1 \oplus x) \cdot g(x)$
0010	0011010	$\mathbf{x^2 \cdot g(x)}$
1010	1110010	$(1 \oplus x^2) \cdot g(x)$
0110	0101110	$(x \oplus x^2) \cdot g(x)$
1110	1000110	$(1 \oplus x \oplus x^2) \cdot g(x)$
0001	0001101	$\mathbf{x^3 \cdot g(x)}$
1001		
0101		
1101		Заполните самостоятельно
0011		
1011		
0111		
1111		

Циклический (7,4)-код

- Минимальный вес (7,4)-кода равен 3, код исправляет 1 ошибку

Замечания (1)

- По сравнению с линейными, циклические коды редки. Например, существует порядка 300000 линейных двоичных (7,3)-кодов, но только два из них являются циклическими.

Замечания (2)

- Тривиальные двоичные циклические коды.
- *Код без информации* – код из нулевого слова.
- *Код с повторением* – код состоящий из двух слов: 00…0 и 11…1.
- *Код с проверкой на четность* – код из слов четного веса.
- *Код без проверки* – код из всех слов длины n.
- В некоторых случаях (например $n = 19$), не существуют циклические коды, кроме описанных выше четырех кодов.

Порождающая матрица циклического кода

$$G^{T}_{k\times n} = \begin{pmatrix} 1 & g_1 & g_2 & \dots & g_{n-k-1} & 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & g_1 & \dots & g_{n-k-2} & g_{n-k-1} & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & \dots & \dots & g_{n-k-1} & 1 & \dots & \square \\ \square & \square & \square & \square & \square & \square & \square & \square & \square & 0 \\ 0 & \dots & \dots & 0 & 1 & g_1 & g_2 & \dots & g_{n-k-1} & 1 \end{pmatrix}$$

Проверочный многочлен циклического кода

- Так как порождающий многочлен циклического кода $g(x)$ делит без остатка многочлен $x^n \oplus 1$, то

$$x^n \oplus 1 = h(x) \cdot g(x)$$

- Многочлен *h(x) – проверочный многочлен*

Проверочная матрица циклического кода

- Всякое кодовое слово можно представить как $c(x) = a(x) \cdot g(x), \quad \deg a(x) \le k-1$
- Тогда $$c(x) \cdot h(x) = a(x) \cdot g(x) \cdot h(x) = a(x) \cdot (1 \oplus x^n) = a(x) \oplus a(x) \cdot x^n$$
- поэтому $\deg c(x) \cdot h(x) \le k-1$

Проверочная матрица циклического кода

- Поэтому коэффициенты при степенях *x* старше *k-1* равны 0.
- Тогда

$$c_0 \cdot h_k \oplus c_1 \cdot h_{k-1} \oplus \ldots \oplus c_k \cdot h_0 = 0$$

$$c_1 \cdot h_k \oplus c_2 \cdot h_{k-1} \oplus \ldots \oplus c_{k+1} \cdot h_0 = 0$$

$$c_2 \cdot h_k \oplus c_3 \cdot h_{k-1} \oplus \ldots \oplus c_{k+2} \cdot h_0 = 0$$

$$\boxtimes$$

$$c_{n-k-1} \cdot h_k \oplus c_{n-k} \cdot h_{k-1} \oplus \ldots \oplus c_{n-1} \cdot h_0 = 0$$

Проверочная матрица циклического кода

$$\underset{(n-k)\times n}{H} = \begin{pmatrix} h_k & h_{k-1} & h_{k-2} & \dots & h_1 & h_0 & 0 & 0 & \dots & 0 \\ 0 & h_k & h_{k-1} & \dots & h_2 & h_1 & h_0 & 0 & \dots & 0 \\ 0 & 0 & h_k & \dots & \dots & \dots & h_1 & h_0 & \dots & \square \\ \square & \square & \square & \square & \square & \square & \square & \square & \square & 0 \\ 0 & \dots & \dots & 0 & h_k & h_{k-1} & h_{k-2} & \dots & h_1 & h_0 \end{pmatrix}$$

Порождающий многочлен дуального кода

$$h^*(x) = h_k + h_{k-1}x + \ldots + h_0 x^k$$

$$h^*(x) = x^k \cdot h(x^{-1})$$

Параметры циклического кода Хэмминга

- Длина кода $n = 2^m - 1$
- Число информационных символов

$$k = n - m = 2^m - 1 - m$$

- Минимальное расстояние - 3
- Число исправляемых ошибок - 1