



Циклические коды

В теории и на практике

Сидоренков Олег, БПИ204



Циклические коды. Теория

Рассмотрим поле F_q^n , которое содержит q элементов, $q = p^n$, где p - это простое число.

Линейный код $C \subseteq F_q^n$, является циклическим, если $(c_0, c_1, \dots, c_{n-2}, c_{n-1}) \in C \Rightarrow (c_{n-1}, c_0, \dots, c_{n-3}, c_{n-2}) \in C$

Пусть $(x^n - 1)$ - это главный идеал кольца многочленов $F_q[x]$, порождённый многочленом $x^n - 1$

Тогда $F_q[x]/(x^n - 1)$ - факторкольцо многочленов по идеалу $(x^n - 1)$

Данное факторкольцо изоморфно пространству F_q^n , а сам изоморфизм имеет вид:

$$(c_0, c_1, \dots, c_{n-2}, c_{n-1}) \Leftrightarrow c_0 + c_1 \cdot x + \dots + c_{n-2} \cdot x^{n-2} + c_{n-1} \cdot x^{n-1}$$

Получается, для сдвига можно просто умножить многочлен на x :

$$\begin{aligned} (c_0 + c_1 \cdot x + \dots + c_{n-2} \cdot x^{n-2} + c_{n-1} \cdot x^{n-1}) \cdot x &= c_0 \cdot x + c_1 \cdot x^2 + \dots + c_{n-2} \cdot x^{n-1} + c_{n-1} \cdot x^n = \\ &= c_0 \cdot x + c_1 \cdot x^2 + \dots + c_{n-2} \cdot x^{n-1} + c_{n-1} \cdot (x^n - 1 + 1) = c_0 \cdot x + c_1 \cdot x^2 + \dots + c_{n-2} \cdot x^{n-1} + c_{n-1} \cdot (0 + 1) = \\ &= c_0 \cdot x + c_1 \cdot x^2 + \dots + c_{n-2} \cdot x^{n-1} + c_{n-1} = c_{n-1} + c_0 \cdot x + c_1 \cdot x^2 + \dots + c_{n-2} \cdot x^{n-1} \end{aligned}$$



Циклические коды. Теория

Линейный код C является циклическим $\Leftrightarrow C$ является идеалом $F_q[x]/(x^n - 1)$

\Leftarrow Если C является идеалом и $(c_0, \dots, c_n) \in C$, то:

$$(c_0 + \dots + c_{n-1} \cdot x^{n-1}) \cdot x = (c_{n-1}, \dots, c_{n-2}) \in C$$

\Rightarrow Так как $(c_0, \dots, c_{n-1}) \in C \rightarrow (c_{n-1}, \dots, c_{n-2}) \in C$, то $\forall c(x), i \in C : x^i \cdot c(x) \in C$

Тогда $\forall b(x) : b(x) \cdot c(x) \in C \Rightarrow C$ is I



Циклические коды. Теория

C - это циклический код длины n . Пусть $g(x) \in C$ - неприводимый многочлен наименьшей степени, $\deg(g(x)) = d$.

Тогда: $C = \{c(x) = q(x) \cdot g(x), q(x) \in F[x]_{n-d}\}$

Докажем от противного. Если утверждение неверно - тогда $\exists c(x) \in C$, который не делится на $g(x)$, тогда:

$$c(x) = g(x) \cdot q(x) + r(x)$$

$$r(x) = c(x) - g(x) \cdot q(x)$$

Так как $c(x) \in C$ и $g(x) \cdot q(x) \in C$, то $r(x) \in C$. Но $\deg(r(x)) < \deg(g(x)) = d$. Противоречие.



Циклические коды. Теория

$C = (g(x))$ - идеал $F_q[x]/(x^n - 1)$.

Тогда: $g(x) \mid (x^n - 1)$

Докажем от противного. Пусть $g(x)$ не делит $x^n - 1$.

$$x^n - 1 = g(x) \cdot h(x) + s(x)$$

$$s(x) \equiv (-h(x)) \cdot g(x) \pmod{x^n - 1}$$

Так как $(-h(x)) \cdot g(x) \in C$, то и $s(x) \in C$. Однако $\deg(s(x)) < \deg(g(x)) = d$. Противоречие.

Рассмотрим циклический код C . Тогда многочлен $g(x)$ называется порождающим многочленом кода C , а многочлен $h(x) = (x^n - 1)/g(x)$ называется проверочным многочленом кода C .



Циклические коды. Теория

Построение циклического кода: $C = \left\{ c(x) = r(x) \cdot g(x), r(x) \in F_q[x] \right\}, \deg(r(x)) < \deg(g(x))$

Пусть степень порождающего многочлена $\deg(g(x)) = n - d$, тогда размерность кода - d .

В циклических кодах кодированием является умножение слова (многочлена) на $g(x)$.

$h(x)$ называется проверочным многочленом $c(x) \in C \Leftrightarrow c(x) \cdot h(x) = 0 \pmod{x^n - 1}$

Соответственно, если $c(x) \cdot h(x) \neq 0 \pmod{x^n - 1}$, то при передаче сообщения произошла ошибка.



Циклические коды. Теория

$g(x) = g_0 + \dots + g_{n-d} \cdot x^{n-d}$ - порождающий многочлен циклического кода C .

$$h(x) = (x^n - 1) / g(x)$$

Многочлены $x \cdot g(x), \dots, x^{d-1} \cdot g(x)$ образуют базис C , тогда порождающая матрица имеет вид:

$$G = \begin{pmatrix} g_0 & g_1 & g_2 & \dots & g_{n-d} & 0 & 0 & \dots & 0 \\ 0 & g_0 & g_1 & \dots & \dots & g_{n-d} & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & g_0 & g_1 & g_2 & \dots & \dots & \dots & g_{n-d} \end{pmatrix}$$

$h(x) = h_0 + \dots + h_d \cdot x^d$ - проверочный многочлен циклического кода C .

Проверочная матрица имеет вид:

$$H = \begin{pmatrix} 0 & \dots & \dots & \dots & 0 & h_d & h_{d-1} & \dots & h_0 \\ 0 & \dots & \dots & 0 & h_d & h_{d-1} & \dots & h_0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ h_d & h_{d-1} & \dots & h_0 & 0 & \dots & \dots & \dots & 0 \end{pmatrix}$$



Примеры циклических кодов

Общий вид:

Код (n, r, k) , n - длина итогового сообщения, r - количество проверочных символов (степень порождающего полинома), k - количество информационных символов (длина исходного сообщения).

Код повторений:

$\{(0, \dots, 0), (1, \dots, 1)\}$, код - $(n, 1, n)$

Пространство:

F_2^n , код - $(n, n, 1)$

Разложим многочлен $(x^7 - 1)$ на неприводимые множители.

$$(x^7 - 1) = (x + 1) \cdot (x^3 + x + 1) \cdot (x^3 + x^2 + 1)$$

Многочлен $g(x) = x^3 + x^2 + 1$ порождает циклический код с проверочным многочленом $h(x) = x^4 + x^3 + x^2 + 1$

$\deg(g(x)) = 7 - 4 = 3$, получается, что размерность кода - 4.



Примеры циклических кодов

Рассмотрим бинарный код $(7, 3, 4)$

Разложим многочлен $(x^7 - 1)$ на неприводимые множители:

$$(x^7 - 1) = (x + 1) \cdot (x^3 + x + 1) \cdot (x^3 + x^2 + 1)$$

Многочлен $g(x) = x^3 + x^2 + 1$ порождает циклический код, который будет иметь длину $n = 7$, а число проверочных символов $r = 3$ (степень порождающего многочлена), число информационных символов $k = 4$

Проверяющий многочлен: $h(x) = x^4 + x^3 + x^2 + 1$

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}; H = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}$$

$$G \cdot H^T = 0$$



Декодирование циклических кодов

Рассмотрим декодирование на примере сообщения 0011010

Порождающий многочлен: $g(x) = 1101$

Пусть ошибка будет на 4 разряде, то есть, получили сообщение $c(x) = 0010010$

Определяем синдром ошибки в крайнем правом разряде как остаток от деления вектора ошибки $e_6 = 0000001$ на $g(x)$

Получился синдром $s_6 = 1$

Теперь нужно делить $c(x)$ на $g(x)$ до получения s_6

Нужно было дописать четыре нуля \Rightarrow ошибка на 4 позиции слева.

Получаем исходное сообщение.

Если при делении пришлось добавить n нулей, а остаток так и не был найден, то исправить ошибку не удастся.

0	0	1	0	0	1	0		1	1	0	1
		1	1	0	1			?			
		1	0	0	0						
		1	1	0	1						
		1	0	1				0			
		1	1	0	1						
		1	1	1				0			
		1	1	0	1						
			1	1				0	0		
			1	1	0	1					
										1	

Коды Голея

Швейцарский астроном и математик, был профессором Женевского университета и восьмым директором Женевской обсерватории с 1956 по 1992 год. Голей был членом Международного астрономического союза и президентом нескольких его комиссий, включая «Звездную классификацию» и «Астрономическую фотометрию и поляриметрию». В 1991 году Базельский университет присвоил ему звание почетного профессора. Его именем назван астероид 3329 Голей.



Марсель Жюль Эдуард Голей

1902-1989гг.





Коды Голея. Примеры

Бинарный (23, 17, 2) циклический код C :

$$g(x) = x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1$$

$$h(x) = (x^{23} - 1)/g(x) = x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^5 + x^2 + 1$$

$$x^{23} - 1 = (x - 1) \cdot (x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1) \cdot (x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1)$$

Тернарный (11, 6, 5) циклический код C :

$$g(x) = x^5 + x^4 - x^3 + x^2 - 1$$

$$h(x) = (x^{11} - 1)/g(x) = x^6 - x^5 - x^4 - x^3 + x^2 - 1$$

$$x^{11} - 1 = (x - 1) \cdot (x^5 - x^3 + x^2 - x - 1) \cdot (x^5 + x^4 - x^3 + x^2 - 1)$$

Источники



- https://en.wikipedia.org/wiki/Cyclic_code
- https://en.wikipedia.org/wiki/Binary_Golay_code
- http://www.opds.spbsut.ru/data_uploaded/mu/teor_kod/vlss19-ppk-cycle-prakt.pdf
- http://informkod.narod.ru/5_6item.htm
- https://libeldoc.bsuir.by/bitstream/123456789/488/2/Salomatin_cikl.pdf



НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
УНИВЕРСИТЕТ

Спасибо за внимание!