Циклические коды

В теории и на практике

Выполнил: Сидоренков Олег, БПИ204
Преподаватель: Куреев Алексей Андреевич

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 $\left(c_0,\, c_1,\, \ldots,\, c_{n-2},\, c_{n-1}\right) \in C \Rightarrow \left(c_{n-1},\, c_0,\, \ldots,\, c_{n-3},\, c_{n-2}\right) \in C$

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

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

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

$$\left(c_0,\, c_1,\, \ldots,\, c_{n-2},\, c_{n-1}\right) \Leftrightarrow c_0 + c1 \cdot x + \ldots + c_{n-2} \cdot x^{n-2} + c_{n-1} \cdot x^{n-1}$$

Получается, для сдвига можно просто умножить многочлен на x:

$$(c_0 + c1 \cdot x + \ldots + c_{n-2} \cdot x^{n-2} + c_{n-1} \cdot x^{n-1}) \cdot x = c_0 \cdot x + c1 \cdot x^2 + \ldots + c_{n-2} \cdot x^{n-1} + c_{n-1} \cdot x^n =$$

$$= c_0 \cdot x + c1 \cdot x^2 + \ldots + c_{n-2} \cdot x^{n-1} + c_{n-1} \cdot (x^n - 1 + 1) = c_0 \cdot x + c1 \cdot x^2 + \ldots + c_{n-2} \cdot x^{n-1} + c_{n-1} \cdot (0 + 1) =$$

$$= c_0 \cdot x + c1 \cdot x^2 + \ldots + c_{n-2} \cdot x^{n-1} + c_{n-1} = c_{n-1} + c_0 \cdot x + c1 \cdot x^2 + \ldots + c_{n-2} \cdot x^{n-1}$$

Циклические коды. Теория

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

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

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

$\Rightarrow$Так как $\left(c_0,\ \ldots,\ c_{n-1}\right) \in C \to \left(c_{n-1},\ \ldots,\ c_{n-2}\right) \in C$, 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, $deg\left(g(x)\right) = d$.

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

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 $deg\left(r(x)\right) < deg\left(g(x)\right) = d$. Противоречие.

Циклические коды. Теория

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

Тогда: $g(x) \mid \left(x^n - 1\right)$

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

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

$s(x) \equiv \left(-h(x)\right) \cdot g(x) \mod x^n - 1$

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

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

Циклические коды. Теория

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

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

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

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

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

Циклические коды. Теория

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

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

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

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

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

Проверочная матрица имеет вид:

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

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:

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

Пространство:

F_2^n, код - $(n,\ n,\ 1)$

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

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

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

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

Примеры циклических кодов

Рассмотрим бинарный код $(7,\ 3,\ 4)$

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

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

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.

$$
\begin{array}{ccccccc|cccc}
0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\
\cline{8-11}
 & & 1 & 1 & 0 & 1 & & ? & & & \\
\cline{3-6}
 & & & 1 & 0 & 0 & 0 & & & & \\
 & & & 1 & 1 & 0 & 1 & & & & \\
\cline{4-7}
 & & & & 1 & 0 & 1 & \boxed{0} & & & \\
 & & & & 1 & 1 & 0 & 1 & & & \\
\cline{5-8}
 & & & & & 1 & 1 & 1 & \boxed{0} & & \\
 & & & & & 1 & 1 & 0 & 1 & & \\
\cline{6-9}
 & & & & & & & 1 & 1 & \boxed{0} & \boxed{0} \\
 & & & & & & & 1 & 1 & 0 & 1 \\
\cline{8-11}
 & & & & & & & & & & \boxed{1}
\end{array}
$$

Коды Голея

Швейцарский астроном и математик , был профессором Женевского университета и восьмым директор 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 $(23,\ 17,\ 2)$ код:

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

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

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

Тернарный $(11,\ 6,\ 5)$ код:

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

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

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

Расширенный бинарный $(24,\ 12,\ 8)$ код:

Кодирует 12 бит информации 24 бит кода, в котором любые ошибки не длиннее 3-х бит могут быть исправлены, а не длиннее 7-и бит могут быть обнаружены

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
- https://www.studmed.ru/view/morelos-saragosa-r-iskusstvo-pomehoustoychivogo-kodirovaniya-metody-algortmy-primenenie_431f14e652a.html

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Спасибо за внимание!