НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Модуль 3. Циклические коды

Циклические коды. Порождающий многочлен циклического кода. Корни порождающего многочлена.

Иванов Ф. И.
к.ф.-м.н., доцент

Национальный исследовательский университет
«Высшая школа экономики»

12 июня 2020 г.

Определение циклического кода

Определение

Циклическим кодом называется линейное векторное подпространство $A \subset V$ — пространства всех векторов длины n над полем $GF(q)$, выдерживающее циклический сдвиг компонент своих векторов.

Иными словами, если код циклический, и вектор

$$\mathbf{u} = (u_0, u_1, ..., u_{n-1})$$

принадлежит коду, то и вектор

$$\mathbf{u}^* = (u_{n-1}, u_0, u_1, ..., u_{n-2})$$

также принадлежит коду.

Многочленное представление операций над векторами

$$\mathbf{u} \mapsto u(x) = u_0 + u_1 x + \ldots + u_{n-1} x^{n-1},$$

$$\mathbf{u}^* \mapsto u(x) = u_{n-1} + u_0 x + \ldots + u_{n-2} x^{n-1}.$$

Рассмотрим произведние

$$xu(x) = u_0 x + \ldots + u_{n-2} x^{n-1} + u_{n-1} x^n,$$

тогда $xu(x) = u(x)$ при $x^n = 1$
В связи со сказанным исследуем кольцо $F[x]$ многочленов над $GF(q)$, а вслед за ним — кольцо $F[x]/(x^n - 1)$ классов вычетов многочленов по модулю $x^n - 1$.

Идеалы кольца

Определение

Непустое подмножество $\mathcal{K}$ кольца K само будет кольцом тогда и только тогда, когда:

- *$\mathcal{K}$ — есть подгруппа аддитивной группы кольца, т.е. когда для любых $a, b \in \mathcal{K}: \ a + b \in \mathcal{K}, a - b \in \mathcal{K}$*
- *Для любых $a, b \in \mathcal{K}: \ ab \in \mathcal{K}$*

Среди подколец особую роль играют идеалы.

Определение

Идеалом называется такое подкольцо $\mathcal{K}$ кольца K, что:

$$a \in \mathcal{K}, r \in K \to ar \in \mathcal{K}$$

Циклический код как идеал кольца $F[x]/(x^n-1)$

Теорема

В кольце $F[x]/(x^n-1)$ линейный код A будет циклическим тогда и только тогда, когда он идеал.

Доказательство

Пусть код A циклический. Тогда вместе с вектором $u(x)$ коду принадлежат и все сдвиги $x^i u(x), i = 1,2,\ldots,n-1$, а также все произведения $b_i x^i u(x), b_i \in GF(q)$, и их сумма

$$u(x)\sum_{i=0}^{n-1} b_i x^i,$$

где $\sum_{i=0}^{n-1} b_i x^i = b(x)$ — произвольный элемент кольца $F[x]/(x^n-1)$. Тогда из того, что $u(x) \in A$, $b(x) \in F[x]/(x^n-1)$ следует, что $u(x)b(x) \in A$, а значит A — идеал.
Обратно: если код A — идеал, то вместе с $u(x)$ ему принадлежит и $xu(x)$, а это и означает, что код циклический.

Порождающий многочлен циклического кода

Теорема

Идеал A содержит единственный нормированный многочлен $g(x)$ минимальной степени r.

Доказательство

Предположим противное. Пусть кроме многочлена $g(x)$ в A имеется еще нормированный многочлен $f(x)$ той же степени. Ясно, что $(g(x)f(x)) \in A$, и $deg(g(x)f(x)) < r$, так как старшие коэффициенты обоих многочленов $g(x)$ и $f(x)$ одинаковы. Противоречие.

Следствие

Все многочлены идеала A кратны многочлену $g(x)$.

Доказательство

Действительно, предположим противное, т.е. пусть $f(x) \in A$, но $f(x) = q(x)g(x) + r(x)$. Имеем последовательно: $g(x) \in A$, $q(x)g(x) \in A$, так как A есть идеал; $r(x) = f(x) - q(x)g(x) \in A$. Получается, что $deg\ r(x) < deg\ g(x)$, чего быть не может. Отсюда $r(x) = 0$.

Порождающий и проверочный многочлены циклического кода

Определение

Многочлен $g(x)$ называется порождающим многочленом идеала, т.е. циклического кода.

Теорема

Любой многочлен $g(x)$, порождающий идеал в кольце $F[x]/(x^n - 1)$, делит многочлен $x^n - 1$.

Следствие

Пусть $x^n - 1 = q(x)g(x) + r(x)$, где выполняется нервенство $\deg r(x) < \deg g(x)$. Так как в кольце $F[x]/(x^n - 1)$ многочлен $x^n - 1$ принадлежит нулевому классу вычетов, то в нем $q(x)g(x) + r(x) = 0$, а потому $q(x)g(x) = r(x)$, и $r(x)$ принадлежит идеалу, что может быть только при $r(x) = 0$ из-за соотношения $\deg r(x) < \deg g(x)$.

Определение

Многочлен $h(x) = \frac{x^n - 1}{g(x)}$ называется проверочным многочленом идеала, т.е. циклического кода.

Порождающая матрица циклического кода

Теорема

Если deg $g(x) = r$*, то векторы (многочлены)*

$$g(x), xg(x), ..., x^{n-r-1}g(x)$$

линейно независимы.

Доказательство

Действительно, линейная зависимость означала бы существование такого набора не всех равных нулю элементов $u_i GF(q), i = 0, 1, ..., n-r-1$*, что*

$$\sum_{i=0}^{n-r-1} u_i x^i g(x) = 0$$

чего быть не может, так как многочлен под знаком суммы имеет степень не выше, чем $n-1$*, а потому не может делиться на* $x^n - 1$ *и, следовательно, не может принадлежать нулевому классу вычетов кольца* $F[x]/(x^n - 1)$*.*

Порождающая матрица циклического кода

Порождающая матрица циклического кода над $GF(q)$ длины n с порождающим многочленом $g(x) = g_0 + xg_1 + ... + x^r g_r$ степени r имеет вид:

$$G = \begin{bmatrix} g(x) \\ xg(x) \\ \dots \\ x^{n-r-1}g(x) \end{bmatrix} = \begin{bmatrix} g_0 & g_1 & \dots & g_r & 0 & 0 & \dots & 0 \\ 0 & g_0 & g_1 & \dots & g_r & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & g_0 & g_1 & \dots & g_r \end{bmatrix}$$

Откуда $r = n - k$.

Однако чаще для кодирования используют порождающий многочлен: чтобы закодировать вектор $\mathbf{u} = (u_0, u_1, ...u_{k-1})$ сопоставим $\mathbf{u}$ многочлен $u(x)$ степени не выше $k - 1$ и вычислим $c(x) \in A$ как

$$c(x) = u(x)g(x)$$

Пример

Пример

Положим $g(x) = 1 + x + x^3$ *над* $GF(2)$, $-1 = 1$. *Можно проверить, что* $x^7 - 1 = (1+x)(1+x+x^3)(1+x^2+x^3)$. *Таким образом,* $n = 7, r = 3, k = 4$.

$$G = \begin{bmatrix} 1+x+x^3 \\ x(1+x+x^3) \\ x^2(1+x+x^3) \\ x^3(1+x+x^3) \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}.$$

Порождающий многочлен с заданными свойствами

Пусть элементы

$$\alpha_1, \alpha_2, ..., \alpha_\rho \in GF(q^m),\ m = 1, 2, ...$$

корни порождающего многочлена $g(x)$ над $GF(q)$.
Тогда эти же элементы являются корнями любого многочлена

$$v(x) = v_0 + v_1 x + v_2 x^2 + ... + v_{n-1} x^{n-1},$$

принадлежащего циклическому коду, порождаемому многочленом $g(x)$:

$$v(\alpha_i) = v_0 + v_1 \alpha_i + v_2 \alpha_i^2 + ... + v_{n-1} \alpha_i^{n-1} = 0$$

$$((v_0, v_1, v_2, ... v_{n-1}), (1, \alpha_i, \alpha_i^2, ... \alpha_i^{n-1})) = 0.$$

Проверочная матрица циклического кода

Проверочное соотношение:

$$\big((v_0, v_1, v_2, ...v_{n-1}),(1, \alpha_i, \alpha_i^2, ...\alpha_i^{n-1})\big) = 0$$

Строки проверочной матрицы:

$$(1, \alpha_i, \alpha_i^2, ...\alpha_i^{n-1})$$

Проверочная матрица циклического кода:

$$H = \begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 & \dots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \dots & \alpha_2^{n-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & \alpha_\rho & \alpha_\rho^2 & \dots & \alpha_\rho^{n-1} \end{bmatrix}$$

Построение порождающего многочлена по корням

Задача:

- Дано: набор элементов $\alpha_1, \alpha_2, ..., \alpha_\rho \in GF(q^m)$, которые требуется сделать корнями порождающего многочлена $g(x)$
- Найти: порождающий многочлен $g(x)$ над $GF(q)$

Решение: Многочлен $g(x)$ делится на все минимальные функции $m_i(x)$, $i = 1, 2, ..., \rho$, своих корней $\alpha_1, \alpha_2, ..., \alpha_\rho \in GF(q^m)$. Следовательно, $g(x)$ делится на наименьшее общее кратное $M(m_1(x), m_2(x), ..., m_\rho(x))$:

$$g(x) = M(m_1(x), m_2(x), ..., m_\rho(x)).$$

Длина циклического кода

Теорема

Длина n циклического кода равна наименьшему общему кратному порядков корней порождающего многочлена $g(x)$, т. е. если корни $g(x)$ лежат в поле $GF(q^m)$, то n — делитель $q^m - 1$.

Пример

Пусть корнями порождающего многочлена будут $\alpha, \alpha^3, \alpha^5 \in GF(2^4)$. Элемент α — примитивный. Элементы α^3, α^5 имеют порядки 5 и 3 соответственно. Длина кода $n = 15$. Пусть α — корень многочлена $x^4 + x + 1$. Минимальные функции элементов α^3, α^5 — $x^4 + x^3 + x^2 + x + 1$ и $x^2 + x + 1$. Тогда порождающий многочлен равен:

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

$$g(x) = 1 + x + x^2 + x^4 + x^5 + x^8 + x^{10}, r = 10, k = 5.$$

Порождающая матрица:

$$G = \begin{bmatrix} 111011001010000 \\ 011101100101000 \\ 001110110010100 \\ 000111011001010 \\ 000011101100101 \end{bmatrix}.$$

Пример - продолжение

Проверочная матрица:

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} \\ 1 & \alpha^5 & \alpha^{10} & 1 & \alpha^5 & \alpha^{10} & 1 & \alpha^5 & \alpha^{10} & 1 & \alpha^5 & \alpha^{10} & 1 & \alpha^5 & \alpha^{10} \end{bmatrix}.$$

Или в бинарной форме:

$$H = \begin{bmatrix} 100010011010111 \\ 010011010111100 \\ 001001101011110 \\ 000100110101111 \\ - - - - - - - \\ 100011000110001 \\ 000110001100011 \\ 001010010100101 \\ 011110111101111 \\ - - - - - - - - \\ 101101101101101 \\ 011011011011011 \\ 011011011011011 \\ 000000000000000 \end{bmatrix}$$

Циклический код Хэмминга

Проверочная матрица кода Хэмминга $\mathcal{H}(m)$ состоит из всех $2^m - 1$ различных ненулевых столбцов высоты m. Элементы поля $GF(2^m)$ имеют такое же представление. То есть после подходящей перестановки:

$$\mathbf{H} = \left(1\ \alpha\ \alpha^2 \ldots \alpha^{2^m-2}\right)$$

Если $u(x) \in \mathcal{H}(m)$, то $u(\alpha)\mathbf{H}^T = 0$. Это значит, что любой кодовый вектор делится на минимальную функцию элемента α, а потому:

$$g(x) = m_\alpha(x)$$

и код Хэмминга оказывается циклическим