

Алгебра. Глава 12. Основы теории кодирования

Д. В. Карпов

2024

- Для конечного алфавита Σ через Σ^* обозначается множество всех слов в этом алфавите — конечных последовательностей элементов Σ .
- Пусть Σ_1 и Σ_2 — два конечных алфавита. Сообщение — произвольное слово $u \in \Sigma_1^*$.
- Мы хотим закодировать сообщение u в алфавите Σ_2 , то есть поставить ему в соответствие слово $F(u) \in \Sigma_2^*$, которое будет передаваться по каналам связи.
- Для этого нам нужно задать отображение $F : \Sigma_1^* \rightarrow \Sigma_2^*$, которое называется кодирующим отображением или просто кодированием.

• Требования к отображению F зависят от того, какую задачу мы решаем. Основные задачи теории кодирования таковы:

— **шифрование данных:** требуется, чтобы вычисление обратного отображения F^{-1} было значительно более трудоемким, чем вычисление F ;

— **помехоустойчивое кодирование:** требуется, чтобы исходное сообщение u можно было восстановить даже в том случае, если при передаче $F(u)$ произошли ошибки (при условии, что ошибок было не слишком много);

— **сжимающие отображения:** требуется, чтобы длина кодированного сообщения была как можно меньше.

— В большинстве случаев, важным требованием является возможность однозначного декодирования (то есть F должно быть инъекцией). Но это требуется не всегда. Например, сжатие с потерей качества не предполагает однозначного декодирования.

- Мы обсудим вопросы, связанные с помехоустойчивым кодированием.
- Мы будем рассматривать **блочное** или **равномерное** кодирование, при котором сообщение $u \in \Sigma_1^*$ разбивается на блоки длины k , каждый из которых будет закодирован словом длины n в алфавите Σ_2 .
- Для этого нам нужно задать инъекцию $c : \Sigma_1^k \rightarrow \Sigma_2^n$, которая будет называться **схемой кодирования**.
- В первую очередь нас будет интересовать множество кодовых слов $C := \text{Im}(c) = \{x \in \Sigma_2^n \mid \exists u \in \Sigma_1^k (c(u) = x)\}$, которое мы будем называть просто **кодом**.
- Как правило, мы будем считать, что $\Sigma_1 = \Sigma_2 = \Sigma$ и $k < n$.
- Пусть $x = x_1 \dots x_n \in \Sigma^n$. Ошибки при передаче слова x могут быть трех типов:
 - **замещение разряда**: вместо символа x_i приняли другой символ x'_i ;
 - **выпадение разряда**: символ x_i не был распознан;
 - **вставка разряда**: между x_i и x_{i+1} прочитали “лишний” символ y .
- Мы будем рассматривать только ошибки типа замещения.

Кодовое расстояние

Определение

Пусть Σ — конечный алфавит, $n \in \mathbb{N}$ и

$$x = x_1 \dots x_n, y = y_1 \dots y_n \in \Sigma^n.$$

• **Расстоянием Хэмминга** между словами x и y — это $d(x, y) := |\{i \in [1..n] : x_i \neq y_i\}|$.

• Очевидно, выполнено неравенство треугольника:

$$d(x, y) \leq d(x, z) + d(z, y).$$

• Пусть $x \in \Sigma^n$ и $r \in \mathbb{N}_0$. **Шар** с центром x и радиусом r — это множество $B_r(x) := \{y \in \Sigma^n : d(x, y) \leq r\}$.

• Очевидно, $|B_r(x)| = \sum_{i=0}^r C_n^i (q-1)^i$, где $q = |\Sigma|$.

Определение

• Пусть $\mathcal{C} \subset \Sigma^n$ — произвольный код. **Кодовое расстояние** кода $\mathcal{C}$ — это $d(\mathcal{C}) := \min\{d(x, y) \mid x, y \in \mathcal{C}, x \neq y\}$.

• **Кодовое расстояние** схемы кодирования $c : \Sigma^k \rightarrow \Sigma^n$ — это $d(c) := d(\text{Im}(c))$.

Теорема 1

Пусть при передаче сообщения длины n возникает не более r ошибок типа замещения, а для кодирования сообщений используется схема c . Тогда:

- 1) схема кодирования c обеспечивает гарантированное обнаружение ошибки, если и только если $d(c) > r$;
- 2) схема кодирования c обеспечивает гарантированное исправление всех ошибок, если и только если $d(c) > 2r$.

Доказательство. • Заметим, что при передаче слова x , результат может оказаться любым словом из $B_r(x)$.

1) Для гарантированного обнаружения ошибки необходимо и достаточно, чтобы никакое кодовое слово не лежало в шаре радиуса r с центром в другом кодовом слове. Но это и означает, что $d(c) > r$.

2) • Для гарантированного исправления всех ошибок необходимо и достаточно, чтобы шары радиуса r с центрами в кодовых словах не пересекались.

• Докажем, что это эквивалентно тому, что $d(c) > 2r$.

⇐. Пусть $z \in B_r(x) \cap B_r(y)$. Тогда

$d(x, y) \leq d(x, z) + d(z, y) \leq r + r = 2r$. Противоречие.

⇒. • Пусть $d(x, y) \leq 2r$.

• Рассмотрим те разряды, в которых слово x отличается от слова y . Пусть таких разрядов $d \leq 2r$.

• Заменяем в слове x какие-нибудь $\lfloor d/2 \rfloor$ из рассматриваемых разрядов на соответствующие разряды слова y .

• Получим слово z , такое, что $d(x, z) \leq r$ и $d(z, y) \leq r$. То есть $z \in B_r(x) \cap B_r(y)$. □

• Простейшим примером схемы кодирования с кодовым расстоянием d является схема, при которой каждый символ повторяется d раз.

• То есть слово $u = u_1 u_2 \dots u_k$ кодируется как

$$c(u) = \underbrace{u_1 \dots u_1}_d \underbrace{u_2 \dots u_2}_d \dots \underbrace{u_k \dots u_k}_d.$$

• Разумеется, такая схема очень неэкономна.

Линейные коды

- Пусть q — степень простого числа p и $\Sigma = \mathbb{F}_q$.
- Множество $\mathbb{F}_q^n$ всех слов длины n в этом алфавите является векторным пространством размерности n над $\mathbb{F}_q$.

Определение

- Линейное подпространство $\mathcal{C}$ пространства $\mathbb{F}_q^n$ называется **линейным q -значным кодом длины n** .
- В случае $q = 2$ линейный такой код называется **двоичным**.
- Линейный код $\mathcal{C}$ имеет следующие параметры:
 - **длина** кода n (количество символов в каждом кодовом слове);
 - **размерность** кода $k = \dim(\mathcal{C})$ (как линейного пространства над $\mathbb{F}_q$);
 - **кодированное расстояние** d .
- Код $\mathcal{C}$ в этом случае мы будем также называть **$[n, k, d]$ -кодом**. Иногда мы будем опускать параметр d и говорить об **$[n, k]$ -кодах**.

- Пусть дан линейный q -значный $[n, k, d]$ -код $\mathcal{C}$.
- Тогда кодовые слова представляются как векторы вида $x = (x_1, x_2, \dots, x_n)$, где $x_i \in \mathbb{F}_q$.
- Поскольку $\dim_{\mathbb{F}_q} \mathcal{C} = k$, очевидно, что $|\mathcal{C}| = q^k$.
Исходные сообщения также можно представлять как векторы вида $u = (u_1, u_2, \dots, u_k)$, где $u_i \in \mathbb{F}_q$.
- Схемой кодирования тогда будет линейное отображение $c : \mathbb{F}_q^k \rightarrow \mathbb{F}_q^n$.
- Нам нужно, чтобы отображение c было инъекцией, что равносильно $\ker(c) = \{0\}$.

Определение

Линейные коды $\mathcal{C}_1$ и $\mathcal{C}_2$ **эквивалентны**, если они отличаются перестановкой координат.

- У эквивалентных кодов все кодовые параметры одинаковы.

Определение

Пусть $x = (x_1, x_2, \dots, x_n) \in \mathbb{F}_q^n$. **Весом Хэмминга $w(x)$** вектора x называется число его ненулевых координат. (То есть, $w(x) = |\{i \in [1..n] : x_i \neq 0\}|$.)

• Пусть $x, y \in \mathbb{F}_q^n$. Тогда $d(x, y) = w(x - y)$.

Лемма 1

Пусть $\mathcal{C}$ — линейный q -значный код с кодовым расстоянием d . Тогда $d = \min\{w(x) \mid x \in \mathcal{C} \setminus \{0\}\}$.

Доказательство. • Пусть $\min\{w(x) \mid x \in \mathcal{C} \setminus \{0\}\} = d'$.

Нужно доказать, что $d = d'$.

$d \geq d'$. Рассмотрим такие векторы $x, y \in \mathbb{F}_q^n$, что $d(x, y) = d$. Тогда $d = d(x, y) = w(x - y) \geq d'$.

$d \leq d'$. Рассмотрим вектор $s \in \mathbb{F}_q^n$, такой, что $w(s) = d'$. Тогда $d \leq d(s, 0) = w(s - 0) = d'$. □

Скалярное произведение и ортогональное дополнение в $\mathbb{F}_q^n$

Определение

- Пусть $x = (x_1, x_2, \dots, x_n), y = (y_1, y_2, \dots, y_n) \in \mathbb{F}_q^n$.

Тогда **скалярным произведением** векторов x и y будем

называть величину $\langle x, y \rangle := \sum_{i=1}^n x_i y_i$.

- Векторы $x, y \in \mathbb{F}_q^n$ **ортогональны**, если $\langle x, y \rangle = 0$.

- Пусть $\mathcal{C}$ — линейное подпространство $\mathbb{F}_q^n$. Тогда **ортогональным дополнением** к $\mathcal{C}$ называется множество

$$\mathcal{C}^\perp := \{y \in \mathbb{F}_q^n \mid \forall x \in \mathcal{C} (\langle x, y \rangle = 0)\}.$$

Теорема 2

- 1) $\mathcal{C}^\perp < \mathbb{F}_q^n$. Если $\dim(\mathcal{C}) = k$, то $\dim(\mathcal{C}^\perp) = n - k$.
- 2) $(\mathcal{C}^\perp)^\perp = \mathcal{C}$.

Доказательство. 1) • Пусть $g_1, g_2, \dots, g_k$ — базис $\mathcal{C}$.

- Тогда $y \in \mathcal{C}^\perp \iff \langle g_1, y \rangle = \langle g_2, y \rangle = \dots = \langle g_k, y \rangle = 0$.
- Рассмотрим матрицу G , строками которой являются векторы $g_1, g_2, \dots, g_k$. Её элементы будем обозначать g_{ij} .
- Это означает, что вектор y является решением ОСЛУ $yG = 0$.
- Пространство решений этой ОСЛУ (а это $\mathcal{C}^\perp$) — линейное подпространство $\mathbb{F}_q^n$ размерности $n - \text{rk}(G) = n - k$.

2) • Из определения очевидно, что $\mathcal{C} \subset (\mathcal{C}^\perp)^\perp$.

- С другой стороны,
 $\dim(\mathcal{C}^\perp)^\perp = n - (n - k) = k = \dim(\mathcal{C})$, следовательно,
 $\mathcal{C} = (\mathcal{C}^\perp)^\perp$.



Порождающая матрица линейного кода

Определение

Пусть $\mathcal{C}$ — линейный q -значный $[n, k]$ -код. **Порождающей матрицей** кода $\mathcal{C}$ называется матрица $G \in M_{k,n}(\mathbb{F}_q)$ (k строк и n столбцов), строки которой образуют базис $\mathcal{C}$.

- Из определения очевидно, что у любого линейного кода есть порождающая матрица и её строки ЛНЗ (т. е. $\text{rk} G = k$).

Понятно, что порождающая матрица неединственна.

- Порождающая матрица G задает схему кодирования. Действительно, пусть $g_1, g_2, \dots, g_k$ — строки G и $u \in \mathbb{F}_q^k$.

- Тогда отображение c можно определить следующим

образом: $c(u) := \sum_{i=1}^k g_i u_i$.

- Это же отображение задается формулами $c(u) = uG$ или $c(u)^T = G^T u^T$.

- Любая схема кодирования должна переводит стандартный базис пространства $\mathbb{F}_q^k$ в некоторый базис подпространства $\mathcal{C}$.

- Следовательно, любая схема кодирования представляется в описанном выше виде для некоторой порождающей матрицы кода $\mathcal{C}$.

Проверочная матрица линейного кода

Определение

Проверочной матрицей кода $\mathcal{C}$ называется матрица H размером $(n - k) \times n$, удовлетворяющая следующему условию:

$$\forall x \in \mathbb{F}_q^n (x \in \mathcal{C} \iff Hx^T = 0).$$

- В отличие от порождающей матрицы, существование проверочной матрицы не является очевидным. Это следует из Теоремы 2.

Следствие 1

У любого линейного q -значного кода $\mathcal{C}$ есть проверочная матрица.

Доказательство. Пусть H — матрица, строки которой образуют базис подпространства $\mathcal{C}^\perp$.

- Поскольку $\dim(\mathcal{C}^\perp) = n - k$, матрица H имеет размеры $(n - k) \times n$.
- Векторы, удовлетворяющие условию $Hx^T = 0$ — это в точности векторы, принадлежащие подпространству $(\mathcal{C}^\perp)^\perp = \mathcal{C}$.



Теорема о столбцах проверочной матрицы

Теорема 3

Пусть H — проверочная матрица линейного кода $\mathcal{C}$. Тогда код $\mathcal{C}$ имеет кодовое расстояние d , если и только если любые $d - 1$ столбцов матрицы H линейно независимы и найдутся d линейно зависимых столбцов.

Доказательство. • Пусть $h_1, h_2, \dots, h_n$ — столбцы матрицы H .

• Существует вектор $a = (a_1, a_2, \dots, a_n) \in \mathcal{C} \setminus \{0\}$ с $w(a) = d$.

• Пусть $a_{i_1}, a_{i_2}, \dots, a_{i_d}$ — все ненулевые координаты a . Тогда

$$\sum_{j=1}^d a_{i_j} h_{i_j} = Ha^T = 0.$$

• Следовательно, столбцы $h_{i_1}, h_{i_2}, \dots, h_{i_d}$ линейно зависимы.

• Наоборот, если столбцы $h_{i_1}, h_{i_2}, \dots, h_{i_s}$ линейно зависимы, то найдется такой вектор $a \in \mathbb{F}_q^n \setminus \{0\}$, что $Ha^T = 0$ и $w(a) \leq s$ (ненулевые коэффициенты у a могут быть только среди $a_{i_1}, a_{i_2}, \dots, a_{i_s}$).

• Следовательно, $s \geq d$.



Следствие 2

(R. C. Singleton, 1964.) Для любого линейного кода C с параметрами $[n, k, d]$ выполнено соотношение $n - k \geq d - 1$.

Доказательство. • Пусть H — проверочная матрица C .

- В этой матрице $n - k$ строк, следовательно, $\text{rk}(H) \leq n - k$.
- Тогда любые $n - k + 1$ столбцов матрицы H линейно зависимы.
- По Теореме 3 (о столбцах проверочной матрицы) получаем, что $d \leq n - k + 1$. □
- Существуют коды, для которых граница Синглтона достигается. Они называются **MDS-кодами** (maximum distance separable).

Граница Хэмминга

Теорема 4

Пусть $A_q(n, d)$ — наибольшая мощность q -значного кода длины n с кодовым расстоянием d и $r = \lfloor \frac{d-1}{2} \rfloor$. Тогда

$$A_q(n, d) \leq \frac{q^n}{\sum_{i=0}^r C_n^i (q-1)^i}.$$

Доказательство. • Для каждого кодового слова $x \in \mathcal{C}$ рассмотрим шар радиуса r с центром в x :

$$B_r(x) = \{y \in \mathbb{F}_q^n : d(x, y) \leq r\}.$$

• Такие шары не могут пересекаться.

Утверждение

$$|B_r(x)| = \sum_{i=0}^r C_n^i (q-1)^i.$$

Доказательство. • Для каждого i от 0 до $r-1$ можно C_n^i способами выбрать i координат вектора x , которые будут изменены.

- Каждую координату можно изменить на $q-1$ другую. □
- Утверждение теоремы очевидно следует из доказанного. □
- Коды, для которых достигается граница Хэмминга называются **совершенным** или **плотно упакованными**.

Двузначный код Хэмминга

- Пусть $q = 2$ и $n = 2^m - 1$, где $m \in \mathbb{N}$.
- Рассмотрим линейный код, задаваемый проверочной матрицей $H_m \in M_{m,n}(\mathbb{F}_2)$, столбцы которой — все $2^m - 1$ ненулевые векторы длины m .
- (i -й столбец представляет из себя двоичную запись числа i из m разрядов, в случае необходимости, в её начало дописывается нужное число нулей. Разряды записываются “сверху вниз” — самый младших разряд должен оказаться в нижней строчке.)

- Пример: $H_3 = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$

- Поскольку все столбцы различны, $d = 3$. Получился линейный двузначный код с параметрами $[2^m - 1, 2^m - m - 1, 3]$.
- Линейный код, заданный определенной выше проверочной матрицей H_m , называется **кодом Хэмминга**.
- Код Хэмминга является совершенным кодом.
- Действительно, $|B_1(u)| = n + 1 = 2^m$ и $2^n / |B_1(u)| = 2^k$.

Циклические коды

Определение

Линейный код $\mathcal{C}$ длины n называется **циклическим**, если

$$\forall x_1, x_2, \dots, x_n ((x_1, x_2, \dots, x_n) \in \mathcal{C} \Rightarrow (x_2, \dots, x_n, x_1) \in \mathcal{C}).$$

- Циклические коды удобно представлять при помощи многочленов
- Будем использовать в качестве алфавита конечное поле $\mathbb{F}_p$.
- Пусть $a = (a_0, a_1, \dots, a_{n-1}) \in \mathbb{F}_p^n$ — некоторое сообщение.
- Поставим ему в соответствие многочлен $a(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1} \in \mathbb{F}_p[x]$.
- Такие многочлены удобно рассматривать по модулю многочлена $x^n - 1$.
- То есть мы будем смотреть на сообщение a как на класс вычетов $\overline{a(x)} \in \mathbb{F}_p[x]/(x^n - 1)$.
- Для обозначения этого класса вычетов мы, как правило, будем использовать многочлен $a(x)$, степень которого меньше n (в каждом классе вычетов по модулю $x^n - 1$ есть ровно один такой многочлен).
- Далее мы будем считать, что $\mathcal{C} \subset \mathbb{F}_p[x]/(x^n - 1)$.

Теорема 5

Подмножество $\mathcal{C} \subset \mathbb{F}_p[x]/(x^n - 1)$ является циклическим кодом, если и только если $\mathcal{C}$ — идеал.

Доказательство. • В кольце $\mathbb{F}_p[x]/(x^n - 1)$ циклический сдвиг коэффициентов многочлена происходит при домножении на x .

• А именно, если $c(x) = c_0 + c_1x + \dots + c_{n-1}x^{n-1} \in \mathbb{F}_p[x]$, то $xc(x) = c_0x + c_1x^2 + \dots + c_{n-1}x^n \equiv c_{n-1} + c_0x + \dots + c_{n-2}x^{n-1} \pmod{x^n - 1}$.

$\Leftarrow$. • Пусть $\mathcal{C}$ — идеал в $\mathbb{F}_p[x]/(x^n - 1)$.

• Тогда $\mathcal{C}$ — линейное подпространство в $\mathbb{F}_p[x]/(x^n - 1)$.

• Так как $c(x) \in \mathcal{C} \implies xc(x) \in \mathcal{C}$, $\mathcal{C}$ — циклический код.

$\Rightarrow$. • Пусть $\mathcal{C}$ — циклический код.

• Тогда $0 \in \mathcal{C}$. Если $f(x), g(x) \in \mathcal{C}$, то $f(x) \pm g(x) \in \mathcal{C}$ и $xf(x) \in \mathcal{C}$.

• Из этого следует, что $\mathcal{C}$ — идеал.



Порождающий многочлен циклического кода

Теорема 6

Пусть $\mathcal{C} \subset \mathbb{F}_p[x]/(x^n - 1)$ — циклический код, а r — минимальная степень ненулевого многочлена из $\mathcal{C}$. Тогда:

- 1) в $\mathcal{C}$ есть ровно один унитарный многочлен $g(x)$ степени r ;
- 2) $x^n - 1 \div g(x)$;
- 3) $\mathcal{C} = (g) = \{ga : a \in \mathbb{F}_p[x], \deg(a) < n - r\}$.

Доказательство. 1) • Пусть $g_1, g_2 \in \mathcal{C}$, $\deg(g_1) = \deg(g_2) = r$ и g_1, g_2 унитарны.

• Тогда $g_1 - g_2 \in \mathcal{C}$ и $\deg(g_1 - g_2) < r$. Следовательно, $g_1 = g_2$.

2) • Пусть $x^n - 1 = g(x)h(x) + s(x)$, где $\deg(s) < \deg(g) = r$.

• Тогда $s(x) \in \mathcal{C}$, следовательно, $s(x) = 0$, то есть $x^n - 1 \div g(x)$.

3) • Пусть $c \in \mathcal{C}$. Напомним, что $\deg(c) < n$.

• Если $c(x) = g(x)a(x) + s(x)$, где $\deg(s) < \deg(g)$, то $s(x) \in \mathcal{C}$, откуда $s(x) = 0$.

• Значит, $c(x) = g(x)a(x)$. Очевидно, $\deg(a) < n - r$. □

Определение

Определенный выше многочлен $g(x)$ называется

порождающим многочленом циклического кода $\mathcal{C}$.

Следствие 3

Любой унитарный делитель $g(x)$ многочлена $x^n - 1$ является порождающим многочленом некоторого циклического кода длины n .

Доказательство. • Рассмотрим идеал $\mathcal{C} := (g)$ в кольце $\mathbb{F}_p[x]/(x^n - 1)$.

- Нужно доказать, что g имеет наименьшую степень среди всех ненулевых элементов этого идеала.
- Пусть $\deg(g) = r$.
- Рассмотрим многочлен $f \in \mathcal{C}$. Тогда $f = g(x)a(x)$, где $a \in \mathbb{F}_p[x]$.
- Поделим с остатком $f = ga$ на $x^n - 1$:

$$g(x)a(x) = (x^n - 1)q(x) + s(x).$$
- Тогда $s(x) \in \mathcal{C}$. Следовательно, $s(x) \div g(x)$, а значит, либо $s = 0$, либо $\deg(s) \geq \deg(g) = r$. □

Теорема 7

Пусть $\mathcal{C} \subset \mathbb{F}_p[x]/(x^n - 1)$ — циклический код с порождающим многочленом g и $\deg(g) = r$. Тогда $\dim(\mathcal{C}) = n - r$.

Доказательство. • Пусть $k = n - r$ и $a(x) = a_0 + a_1x + \dots + a_{k-1}x^{k-1}$.

• Тогда

$g(x)a(x) = a_0 \cdot g(x) + a_1 \cdot xg(x) + \dots + a_{k-1} \cdot x^{k-1}g(x)$ — линейная комбинация многочленов $g(x), xg(x), \dots, x^{k-1}g(x)$.

• По пункту 3 Теоремы 6 все многочлены из $\mathcal{C}$ представляются в виде таких линейных комбинаций. Таким образом, $g(x), xg(x), \dots, x^{k-1}g(x)$ — порождающая система в $\mathcal{C}$.

• Докажем, что $g(x), xg(x), \dots, x^{k-1}g(x)$ — ЛНЗ.

• Если это не так, существует такой многочлен $a \neq 0$, $\deg(a) \leq k$, что

$g(x)a(x) = a_0 \cdot g(x) + a_1 \cdot xg(x) + \dots + a_{k-1} \cdot x^{k-1}g(x) = 0$
в $\mathbb{F}_p[x]/(x^n - 1)$. Это означает, что $ga \vdots x^n - 1$.

• Но $\deg(ga) < \deg(x^n - 1)$, поэтому $ga \nmid x^n - 1$. Противоречие.

• Таким образом, $g(x), xg(x), \dots, x^{k-1}g(x)$ — базис в $\mathcal{C}$, откуда $\dim(\mathcal{C}) = k$.

Теорема 8

Пусть $g(x) = g_0 + g_1x + \dots + g_rx^r$ — порождающий многочлен циклического кода $\mathcal{C}$. Тогда матрица

$$G = \begin{pmatrix} g_0 & g_1 & g_2 & \dots & g_r & 0 & 0 & \dots & 0 \\ 0 & g_0 & g_1 & g_2 & \dots & g_r & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & g_0 & g_1 & g_2 & \dots & g_r & 0 \\ 0 & 0 & \dots & 0 & g_0 & g_1 & g_2 & \dots & g_r \end{pmatrix}$$

является порождающей матрицей кода $\mathcal{C}$. (Матрица имеет размеры $(n - r) \times n$: в каждой её строке стоят $r + 1$ коэффициент многочлена g и $n - r - 1$ нулей.)

Доказательство. • Все строки матрицы принадлежат $\mathcal{C}$: строка номер i соответствует многочлену $x^{i-1}g(x)$.

• Строки G — ЛНЗ. Действительно, $g_r = 1$, поэтому последние $n - r$ столбцов G образуют нижнетреугольную матрицу с единицами на главной диагонали.

• Поскольку $\dim(\mathcal{C}) = n - r$, строки G образуют базис в $\mathcal{C}$.



Определение

Проверочный многочлен циклического кода $\mathcal{C}$ — это такой многочлен $h(x) \in \mathbb{F}_p[x]$, что $g(x)h(x) = x^n - 1$ (где g — порождающий многочлен кода $\mathcal{C}$).

- Легко видеть, что $\deg(h) = n - r = k$, где $r = \deg(g)$ и $k = \dim(\mathcal{C})$.

Лемма 2

Пусть $c \in \mathbb{F}_p[x]$, $\deg(c) < n$. Тогда $c \in \mathcal{C}$, если и только если $h(x)c(x) \vdots x^n - 1$.

Доказательство. $\Rightarrow$.

- Пусть $c \in \mathcal{C}$. Тогда $c(x) = g(x)a(x)$, где $a \in \mathbb{F}_p[x]$.

- Следовательно,

$$h(x)c(x) = h(x)g(x)a(x) = (x^n - 1)a(x) \vdots x^n - 1.$$

$\Leftarrow$. • Пусть $h(x)c(x) = (x^n - 1)f(x)$, где $f \in \mathbb{F}_p[x]$.

- Тогда $h(x)c(x) = (x^n - 1)f(x) = h(x)g(x)f(x)$, откуда $c(x) = g(x)f(x) \in \mathcal{C}$. □

Теорема 9

Пусть $h(x) = h_0 + h_1x + \dots + h_kx^k$ — проверочный многочлен циклического кода $\mathcal{C}$. Тогда матрица

$$H = \begin{pmatrix} 0 & 0 & \dots & 0 & h_k & \dots & h_2 & h_1 & h_0 \\ 0 & \dots & 0 & h_k & \dots & h_2 & h_1 & h_0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & h_k & \dots & h_2 & h_1 & h_0 & 0 & \dots & 0 \\ h_k & \dots & h_2 & h_1 & h_0 & 0 & \dots & 0 & 0 \end{pmatrix}$$

является проверочной матрицей кода $\mathcal{C}$. (Матрица имеет размеры $(n - r) \times n$ (напомним, что $n - r = k$), в каждой её строке стоят $k + 1$ коэффициент многочлена h и $r - 1$ нулей.)

Доказательство. • Все строки матрицы ЛНЗ, поскольку $h_k = 1$.

- Пусть $c(x) = c_0 + c_1x + \dots + c_{n-1}x^{n-1} \in \mathcal{C}$.
- По Лемме 2, $c(x)h(x) \vdots x^n - 1$. При этом, $\deg(ch) < n + k$.

Утверждение

Коэффициенты при $x^k, x^{k+1}, \dots, x^{n-1}$ многочлена ch равны нулю.

Доказательство. • По Лемме 2, $c(x)h(x) \vdots x^n - 1$. При этом, $\deg(ch) < n + k$.

- Тогда $ch = f \cdot (x^n - 1)$, где $f \in \mathbb{F}_p[x]$, $\deg(f) \leq k - 1$.
- Значит, $ch = f \cdot c - x^n - f$. Непосредственным вычитанием легко убедиться, что все коэффициенты этого многочлена степеней от $\deg(f) + 1 \leq k$ до $n - 1$ равны 0. □
- Заметим, что коэффициент при x^{k+t} многочлена ch равен $\sum_{i=0}^{k+t} c_i h_{k+t-i}$. Таким образом, $\sum_{i=0}^{k+t} c_i h_{k+t-i} = 0$ при $t \in [0..r - 1]$.
- Но написанная выше сумма — это скалярное произведение вектора c на $(r - t)$ -ю строку матрицы H .
- Таким образом, для любого $c \in \mathcal{C}$ вектор из коэффициентов c ортогонален всем строкам матрицы H .
- Следовательно, строки H — это $n - r$ ЛНЗ векторов из $\mathcal{C}^\perp$.
- Это означает, что строки H — это базис $\mathcal{C}^\perp$.
- По Следствию 1 тогда H — проверочная матрица кода $\mathcal{C}$. □

Циклические коды: кодирование

- Пусть $a(x) = a_0 + a_1x + \dots + a_{k-1}x^{k-1}$ — исходное сообщение.
- Есть два способа закодировать его в сообщение $c(x) \in \mathcal{C}$.
- Пусть $g(x)$ — порождающий многочлен кода $\mathcal{C}$.

1. Несистематический кодер. $c(x) := a(x)g(x) \in \mathcal{C}$.

- Этот кодер **несистематический** в том смысле, что коэффициенты многочлена $a(x)$ не обязаны присутствовать среди коэффициентов многочлена $c(x)$. Тем не менее, способ часто оказывается удобным из-за простоты кодирования.

2. Систематический кодер. $c(x) = x^r a(x) - s(x)$, где $s(x)$ — остаток от деления $x^r a(x)$ на $g(x)$.

- При таком кодировании мы заменяем вектор $(a_0, a_1, \dots, a_k)$ на вектор $(\lambda_0, \dots, \lambda_{r-1}, a_0, a_1, \dots, a_k)$, где $-s(x) = \lambda_0 + \lambda_1x + \dots + \lambda_{r-1}x^{r-1}$.
- Поскольку $\deg(s) < r$, все коэффициенты многочлена $a(x)$ являются коэффициентами многочлена $c(x)$. А именно, $a_i = c_{i+r}$.

- Пусть
 - $a(x)$ — исходное сообщение;
 - $c(x)$ — кодированное сообщение;
 - $c'(x)$ — принятое сообщение (возможно, содержит ошибки);
 - $\varepsilon(x) := c'(x) - c(x)$ — вектор ошибки.
- Тогда $\varepsilon(x) \equiv c'(x) \pmod{g(x)}$.
- Мы знаем, что количество ошибок невелико (ограничение на количество ошибок соответствует параметрам кода).
- Тогда $w(\varepsilon(x))$ мал (не превосходит количества ошибок).
- Следовательно, многочлен $\varepsilon(x)$ можно найти перебирая все векторы малого веса.

- Пусть $p \in \mathbb{P}$. Мы будем рассматривать циклические коды над полем $\mathbb{F}_p$ длины $n = p^m - 1$, где $m \in \mathbb{N}$.
- Тогда $(x^n - 1)x = x^q - x$, где $q = p^m$. Следовательно, многочлен $x^n - 1$ не имеет кратных корней и его корнями являются все ненулевые элементы поля $\mathbb{F}_q$.

Определение

Нулями циклического кода $\mathcal{C}$ называются корни его порождающего многочлена.

Теорема 10

Пусть $\mathcal{C}$ — циклический код над $\mathbb{F}_p$ длины $n = p^m - 1$, $q = p^m$
 $g(x)$ — порождающий многочлен кода $\mathcal{C}$, $\deg(g) = r$, а
 $\beta_1, \beta_2, \dots, \beta_r \in \mathbb{F}_q$ — все нули $\mathcal{C}$. Пусть $f(x) \in \mathbb{F}_p[x]$,
 $\deg(f) < n$. Тогда

$$f \in \mathcal{C} \iff f(\beta_1) = f(\beta_2) = \dots = f(\beta_r) = 0.$$

Доказательство. $\Rightarrow$. • По Теореме 6, $f = ga$, где $a \in \mathbb{F}_p[x]$.

• Следовательно, $f(\beta_i) = g(\beta_i)a(\beta_i) = 0$ при всех $i \in [1..r]$.

$\Leftarrow$. • Разделим f на g с остатком: $f = ga + s$, где $\deg(s) < r$.

• Тогда $s(\beta_i) = f(\beta_i) - g(\beta_i)a(\beta_i) = 0$ при всех $i \in [1..r]$.

• Таким образом, многочлен $s(x)$ имеет r различных корней и при этом $\deg(s) < r$.

• Следовательно, $s = 0$. Тогда $f(x) = g(x)a(x) \in \mathcal{C}$. □

Теорема о границе БЧХ (Боуз-Чоудхури-Хоквингем)

Теорема 11

Пусть $\mathcal{C}$ — p -значный циклический код длины n , $\alpha \in \mathbb{F}_{p^n}$ — примитивный элемент, а $g(x)$ — порождающий многочлен кода $\mathcal{C}$. Пусть $b, \delta \in \mathbb{Z}$ таковы, что $b \geq 0$, $\delta > 1$ и $g(\alpha^b) = g(\alpha^{b+1}) = \dots = g(\alpha^{b+\delta-2}) = 0$. Тогда кодовое расстояние $d(\mathcal{C}) \geq \delta$.

Доказательство. • Предположим противное: пусть в $\mathcal{C}$ есть ненулевой элемент, вес Хэмминга которого меньше δ .

• Этому элементу соответствует многочлен $f(x) = c_1x^{k_1} + c_2x^{k_2} + \dots + c_{\delta-1}x^{k_{\delta-1}} \in \mathcal{C}$ где $c_1, c_2, \dots, c_{\delta-1} \in \mathbb{F}_p$ — не все нули.

• По Теореме 10, $f(\alpha^b) = f(\alpha^{b+1}) = \dots = f(\alpha^{b+\delta-2}) = 0$.

• Получаем следующие равенства:

$$\begin{cases} c_1\alpha^{k_1b} & + & c_2\alpha^{k_2b} & + \dots + & c_{\delta-1}\alpha^{k_{\delta-1}b} & = & 0 \\ c_1\alpha^{k_1b+k_1} & + & c_2\alpha^{k_2b+k_2} & + \dots + & c_{\delta-1}\alpha^{k_{\delta-1}b+k_{\delta-1}} & = & 0 \\ \dots & & & & & & \\ c_1\alpha^{k_1b+k_1(\delta-2)} & + & c_2\alpha^{k_2b+k_2(\delta-2)} & + \dots + & c_{\delta-1}\alpha^{k_{\delta-1}b+k_{\delta-1}(\delta-2)} & = & 0. \end{cases}$$

- На эти равенства можно смотреть как на ОСЛУ, в которой $c_1, c_2, \dots, c_{\delta-1}$ — неизвестные, а степени α — коэффициенты.
- Так как эта ОСЛУ имеет нетривиальное решение, матрица системы — вырожденная. Следовательно,

$$\begin{aligned}
 0 &= \begin{vmatrix} \alpha^{k_1 b} & \alpha^{k_2 b} & \dots & \alpha^{k_{\delta-1} b} \\ \alpha^{k_1 b + k_1} & \alpha^{k_2 b + k_2} & \dots & \alpha^{k_{\delta-1} b + k_{\delta-1}} \\ \vdots & \vdots & & \vdots \\ \alpha^{k_1 b + k_1(\delta-2)} & \alpha^{k_2 b + k_2(\delta-2)} & \dots & \alpha^{k_{\delta-1} b + k_{\delta-1}(\delta-2)} \end{vmatrix} = \\
 &= \alpha^{(k_1 + k_2 + \dots + k_{\delta-1})b} \begin{vmatrix} 1 & 1 & \dots & 1 \\ \alpha^{k_1} & \alpha^{k_2} & \dots & \alpha^{k_{\delta-1}} \\ \vdots & \vdots & & \vdots \\ \alpha^{k_1(\delta-2)} & \alpha^{k_2(\delta-2)} & \dots & \alpha^{k_{\delta-1}(\delta-2)} \end{vmatrix} = \\
 &= \alpha^{(k_1 + k_2 + \dots + k_{\delta-1})b} \prod_{i < j} (\alpha^{k_i} - \alpha^{k_j}) \neq 0.
 \end{aligned}$$

- Последнее из написанных выше равенств — это определитель Вандермонда.
- Выражение в правой части не может быть равно нулю, так как $\alpha^{k_i} \neq \alpha^{k_j}$ — ведь α — примитивный элемент поля.
- Полученное противоречие завершает доказательство.

Определение

Кодом БЧХ над полем $\mathbb{F}_p$ длины $n = p^m - 1$ с **конструктивным расстоянием** $\delta > 1$ называется циклический код с порождающим многочленом наименьшей степени, корнями которого являются элементы $\alpha^b, \alpha^{b+1}, \dots, \alpha^{b+\delta-2}$, где α — примитивный элемент поля $\mathbb{F}_{p^m}$ и $b \in \mathbb{Z}$ — некоторое неотрицательное число.

- Это определение можно эквивалентно переформулировать следующим образом.

- Обозначим через $M^{(s)}(x)$ минимальный многочлен α^s .
- Пусть Пусть $d \in \mathbb{N}$ — минимальное такое, что $\alpha^{p^d s} = \alpha^s$.

- По Теореме 10.13 имеем $M^{(s)}(x) = \prod_{i=0}^{d-1} (x - \alpha^{p^i s})$ и

$$\deg(M^{(s)}) = d \leq m.$$

- Тогда код БЧХ над полем $\mathbb{F}_p$ длины $n = p^m - 1$ с конструктивным расстоянием $\delta > 1$ — это циклический код с порождающим многочленом

$$g(x) := [M^{(b)}(x), M^{(b+1)}(x), \dots, M^{(b+\delta-2)}(x)], \text{ где } b \in \mathbb{Z}, b \geq 0.$$

Коды Рида-Соломона

- Пусть $p \in \mathbb{P}$, $m \in \mathbb{N}$, $q = p^m > 2$, α — примитивный элемент поля $\mathbb{F}_q$.

Определение

Код Рида-Соломона — это код БЧХ длины $q - 1$ над полем $\mathbb{F}_p$ с порождающим многочленом

$$g(x) = (x - \alpha^b)(x - \alpha^{b+1}) \dots (x - \alpha^{b+\delta-2}),$$

где $b, \delta \in \mathbb{Z}$, $b \geq 0$ и $\delta > 1$.

Следствие 5

Код Рида-Соломона имеет параметры $n = q - 1$, $k = n - \delta + 1$ и $d = \delta = n - k + 1$.

Доказательство. • $k = n - \deg(g) = n - \delta + 1$.

- $d \geq \delta$ по Теореме 11 (о границе БЧХ).
- Вспомним, что $n - k \geq d - 1$ по Следствию 2 (о границе Синглтона). Следовательно, $d \leq \delta$.
- Таким образом, $d = \delta$. □

- Код Рида-Соломона является MDS-кодом: он достигает границу Синглтона.