Алгебра. Глава 12. Основы теории кодирования

Кодовое расстояние.

Введение в теорию кодирования

Основные понятия

- 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 $F : \Sigma_1^* \to \Sigma_2^*$, которое называется **кодирующим отображением** или просто **кодированием**.

Основные задачи теории кодирования

- **Шифрование данных:** требуется, чтобы вычисление обратного отображения F^{-1} было значительно более трудоёмким, 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.

Помехоустойчивое кодирование

- 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 $c : \Sigma_1^k \to \Sigma_2^n$, которая будет называться **схемой кодирования**.
- В первую очередь нас будет интересовать множество кодовых слов $C := \mathrm{Im}(c) = \{x \in \Sigma_2^n \mid \exists u \in \Sigma_1^k (c(u) = x)\}$, которое мы будем называть просто кодом.
- Как правило, мы будем считать, что $\Sigma_1 = \Sigma_2 = \Sigma$ и $k < n$.

Типы ошибок

- Пусть $x = x_1 \dots x_n \in \Sigma^n$. Ошибки при передаче слова x могут быть трёх 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 называется

$$d(x, y) := |\{i \in [1..n] \mid x_i \neq y_i\}|.$$

- 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

$$B_r(x) := \{y \in \Sigma^n \mid d(x, y) \leq r\}.$$

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

Определение

- Пусть $C \subset \Sigma^n$ — произвольный код. **Кодовое расстояние** кода C — это

$$d(C) := \min\{d(x, y) \mid x, y \in C, x \neq y\}.$$

- **Кодовое расстояние** схемы кодирования $c : \Sigma^k \to \Sigma^n$ — это $d(c) := d(\mathrm{Im}(c))$.

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 $d \leq 2r$.
     - Заменим 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 $z \in B_r(x) \cap B_r(y)$.

Пример

- 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

$$c(u) = u_1 \dots u_1 \; u_2 \dots u_2 \dots u_k \dots u_k.$$

- Разумеется, такая схема очень неэкономна.

Линейные коды. Параметры. Кодовое расстояние линейного кода.

Линейные коды

Определение

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

Линейный код

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

Кодирование

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

Эквивалентность кодов

- Линейные коды C_1 и C_2 эквивалентны, если они отличаются перестановкой координат.
- У эквивалентных кодов все кодовые параметры одинаковы.

Кодовое расстояние линейного кода

Определение

- Пусть $x = (x_1, x_2, \ldots, x_n) \in F_q^n$. Весом Хэмминга $w(x)$ вектора x называется число его ненулевых координат (то есть, $w(x) = |\{i \in [1..n] : x_i \neq 0\}|$).
- Пусть $x, y \in F_q^n$. Тогда $d(x, y) = w(x - y)$.

Лемма 1

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

Доказательство

- Пусть $\min\{w(x) \mid x \in C \setminus \{0\}\} = d'$.
- Нужно доказать, что $d = d'$.
  - $d \geq d'$. Рассмотрим такие векторы $x, y \in F_q^n$, что $d(x, y) = d$. Тогда $d = d(x, y) = w(x - y) \geq d'$.
  - $d \leq d'$. Рассмотрим вектор $s \in F_q^n$, такой, что $w(s) = d'$. Тогда $d \leq d(s, 0) = w(s - 0) = d'$.

Скалярное произведение и ортогональное дополнение в F_q^n.

Скалярное произведение и ортогональное дополнение в F_q^n

Определение

- Пусть $x = (x_1, x_2, \ldots, x_n), y = (y_1, y_2, \ldots, y_n) \in F_q^n$.
- Тогда **скалярным произведением** векторов x и y будем называть величину

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

- Векторы $x, y \in F_q^n$ **ортогональны**, если $\langle x, y \rangle = 0$.
- Пусть C — линейное подпространство F_q^n. Тогда **ортогональным дополнением** к C называется множество

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

Теорема 2

1. $C^\perp < F_q^n$. Если $\dim(C) = k$, то $\dim(C^\perp) = n - k$.
2. $(C^\perp)^\perp = C$.

Доказательство

1. - Пусть $g_1, g_2, \ldots, g_k$ — базис C.
   - Тогда $y \in C^\perp \iff \langle g_1, y \rangle = \langle g_2, y \rangle = \cdots = \langle g_k, y \rangle = 0$.
   - Рассмотрим матрицу G, строками которой являются векторы $g_1, g_2, \ldots, g_k$. Её элементы будем обозначать g_{ij}.
   - Это означает, что вектор y является решением ОСЛУ $yG = 0$.
   - Пространство решений этой ОСЛУ (а это $C^\perp$) — линейное подпространство F_q^n размерности

$$n - \mathrm{rk}(G) = n - k.$$

2. - Из определения очевидно, что $C \subset (C^\perp)^\perp$.
   - С другой стороны,

$$\dim((C^\perp)^\perp) = n - (n - k) = k = \dim(C),$$

   следовательно, $C = (C^\perp)^\perp$.

Порождающая и проверочная матрицы линейного кода

Порождающая матрица линейного кода

Определение

- Пусть C — линейный q-значный $[n, k]$-код. **Порождающей** матрицей кода C называется матрица $G \in M_{k,n}(F_q)$ (с k строками и n столбцами), строки которой образуют базис C.
- Из определения очевидно, что у любого линейного кода есть порождающая матрица и её строки линейно независимы (т.е. $\mathrm{rk}(G) = k$).
- Понятно, что порождающая матрица неединственна.

Схема кодирования

- Порождающая матрица G задаёт схему кодирования. Действительно, пусть $g_1, g_2, \ldots, g_k$ — строки G и $u \in F_q^k$.
- Тогда отображение c можно определить следующим образом:

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

- Это же отображение задаётся формулами $c(u) = uG$ или $c(u)^T = G^T u^T$.
- Любая схема кодирования должна переводить стандартный базис пространства F_q^k в некоторый базис подпространства C.
- Следовательно, любая схема кодирования представляется в описанном выше виде для некоторой порождающей матрицы кода C.

Проверочная матрица линейного кода

Определение

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

$$\forall x \in F_q^n \ (x \in C \iff Hx^T = 0).$$

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

Следствие 1

- У любого линейного q-значного кода C есть проверочная матрица.

Доказательство

- Пусть H — матрица, строки которой образуют базис подпространства $C^\perp$.
- Поскольку $\dim(C^\perp) = n - k$, матрица H имеет размеры $(n-k) \times n$.
- Векторы, удовлетворяющие условию $Hx^T = 0$, — это в точности векторы, принадлежащие подпространству $(C^\perp)^\perp = C$.

Теорема о столбцах проверочной матрицы. Граница Синглтона.

Теорема о столбцах проверочной матрицы

Теорема 3

- Пусть H — проверочная матрица линейного кода C. Тогда код 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 $h_1, h_2, \ldots, h_n$ — столбцы матрицы H.
- Существует вектор $a = (a_1, a_2, \ldots, a_n) \in C \setminus \{0\}$ с $w(a) = d$.
- Пусть $a_{i_1}, a_{i_2}, \ldots, a_{i_d}$ — все ненулевые координаты a. Тогда

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

- Следовательно, столбцы $h_{i_1}, h_{i_2}, \ldots, h_{i_d}$ линейно зависимы.
- Наоборот, если столбцы $h_{i_1}, h_{i_2}, \ldots, h_{i_s}$ линейно зависимы, то найдётся такой вектор $a \in F_q^n \setminus \{0\}$, что $Ha^T = 0$ и $w(a) \leq s$ (ненулевые коэффициенты у a могут быть только среди $a_{i_1}, a_{i_2}, \ldots, a_{i_s}$).
- Следовательно, $s \geq d$.

Граница Синглтона

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,

$$\mathrm{rk}(H) \leq n - k.$$

- 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 и код Хэмминга.

Граница Хэмминга

Теорема 4

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

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

Доказательство

- Для каждого кодового слова $x \in C$ рассмотрим шар радиуса r с центром в x:

$$B_r(x) = \{y \in F_q^n \mid d(x, y) \leq r\}.$$

- 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.

Совершенные коды

- Коды, для которых достигается граница Хэмминга, называются совершенными или плотно упакованными.

Двузначный код Хэмминга

Определение

- Пусть $q = 2$ и $n = 2^m - 1$, где $m \in \mathbb{N}$.
- Рассмотрим линейный код, задаваемый проверочной матрицей $H_m \in M_{m,n}(F_2)$, 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 младший разряд должен оказаться в нижней строчке.)

Пример

- H_3:

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

Свойства

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

Циклические коды. Теорема об идеале.

Циклические коды

Определение

- Линейный код C длины n называется циклическим, если

$$\forall x_1, x_2, \ldots, x_n \; ((x_1, x_2, \ldots, x_n) \in C \implies (x_2, \ldots, x_n, x_1) \in C).$$

- Циклические коды удобно представлять при помощи многочленов.
- Будем использовать в качестве алфавита конечное поле F_p.
- Пусть $a = (a_0, a_1, \ldots, a_{n-1}) \in F_p^n$ — некоторое сообщение.
- Поставим ему в соответствие многочлен

$$a(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \in F_p[x].$$

- Такие многочлены удобно рассматривать по модулю многочлена $x^n - 1$.
- То есть мы будем смотреть на сообщение a как на класс вычетов $\overline{a(x)} \in F_p[x]/(x^n - 1)$.
- 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 $C \subset F_p[x]/(x^n - 1)$.

Циклические коды и идеалы

Теорема 5

- Подмножество $C \subset F_p[x]/(x^n - 1)$ является циклическим кодом, если и только если C — идеал.

Доказательство

- В кольце $F_p[x]/(x^n - 1)$ циклический сдвиг коэффициентов многочлена происходит при домножении на x.
- А именно, если $c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} \in F_p[x]$, то

$$xc(x) = c_0x + c_1x^2 + \cdots + c_{n-1}x^n \equiv c_{n-1} + c_0x + \cdots + c_{n-2}x^{n-1} \pmod{x^n - 1}.$$

Прямое доказательство ($\Leftarrow$)

- Пусть C — идеал в $F_p[x]/(x^n - 1)$.
- Тогда C — линейное подпространство в $F_p[x]/(x^n - 1)$.
- Так как $c(x) \in C \implies xc(x) \in C$, C — циклический код.

Обратное доказательство ($\Rightarrow$)

- Пусть C — циклический код.
- Тогда $0 \in C$. Если $f(x), g(x) \in C$, то $f(x) \pm g(x) \in C$ и $xf(x) \in C$.
- Из этого следует, что C — идеал.

Порождающий многочлен циклического кода

Порождающий многочлен циклического кода

Теорема 6

- Пусть $C \subset F_p[x]/(x^n - 1)$ — циклический код, а r — минимальная степень ненулевого многочлена из C. Тогда:
  1. В C есть ровно один унитарный многочлен $g(x)$ степени r.
  2. $x^n - 1 \vdots g(x)$.
  3. $C = (g) = \{ga : a \in F_p[x], \deg(a) < n - r\}$.

Доказательство

1. - Пусть $g_1, g_2 \in C$, $\deg(g_1) = \deg(g_2) = r$ и g_1, g_2 унитарны.
   - Тогда $g_1 - g_2 \in C$ 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 $s(x) \in C$, следовательно, $s(x) = 0$, то есть $x^n - 1 \vdots g(x)$.
3. - Пусть $c \in C$. Напомним, что $\deg(c) < n$.
   - Если $c(x) = g(x)a(x) + s(x)$, где $\deg(s) < \deg(g)$, то $s(x) \in C$, откуда $s(x) = 0$.
   - Значит, $c(x) = g(x)a(x)$. Очевидно, $\deg(a) < n - r$.

Определение

- Определённый выше многочлен $g(x)$ называется порождающим многочленом циклического кода C.

Следствие 3

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

Доказательство

- Рассмотрим идеал $C := (g)$ в кольце $F_p[x]/(x^n - 1)$.
- Нужно доказать, что g имеет наименьшую степень среди всех ненулевых элементов этого идеала.
- Пусть $\deg(g) = r$.
- Рассмотрим многочлен $f \in C$. Тогда $f = g(x)a(x)$, где $a \in F_p[x]$.
- Поделим с остатком $f = g(x)a(x)$ на $x^n - 1$:

$$g(x)a(x) = (x^n - 1)q(x) + s(x).$$

- Тогда $s(x) \in C$. Следовательно, $s(x) \vdots g(x)$, а значит, либо $s = 0$, либо $\deg(s) \geq \deg(g) = r$.

Теорема о размерности циклического кода. Порождающая матрица циклического кода.

Теорема 7

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

Доказательство

- Пусть $k = n - r$ и

$$a(x) = a_0 + a_1 x + \cdots + a_{k-1}x^{k-1}.$$

- Тогда

$$g(x)a(x) = a_0 \cdot g(x) + a_1 \cdot xg(x) + \cdots + a_{k-1} \cdot x^{k-1}g(x),$$

  — линейная комбинация многочленов $g(x), xg(x), \ldots, x^{k-1}g(x)$.
- По пункту 3 Теоремы 6 все многочлены из C представляются в виде таких линейных комбинаций. Таким образом, $g(x), xg(x), \ldots, x^{k-1}g(x)$ — порождающая система в C.
- Докажем, что $g(x), xg(x), \ldots, x^{k-1}g(x)$ — линейно независимы.
- Если это не так, существует такой многочлен $a \neq 0$, $\deg(a) \leq k$, что

$$g(x)a(x) = a_0 \cdot g(x) + a_1 \cdot xg(x) + \cdots + a_{k-1} \cdot x^{k-1}g(x) = 0$$

  в $F_p[x]/(x^n - 1)$. Это означает, что $g(x)a(x) \vdots x^n - 1$.
- Но $\deg(g(x)a(x)) < \deg(x^n - 1)$, поэтому $g(x)a(x) \not\vdots x^n - 1$. Противоречие.
- Таким образом, $g(x), xg(x), \ldots, x^{k-1}g(x)$ — базис в C, откуда $\dim(C) = k$.

Порождающая матрица циклического кода

Теорема 8

- Пусть $g(x) = g_0 + g_1 x + \cdots + g_r x^r$ — порождающий многочлен циклического кода C. Тогда матрица

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

  является порождающей матрицей кода 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 C: строка номер i соответствует многочлену $x^{i-1}g(x)$.
- Строки G — линейно независимы. Действительно, $g_r = 1$, поэтому последние $n - r$ столбцов G образуют нижнетреугольную матрицу с единицами на главной диагонали.

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

Проверочный многочлен и проверочная матрица циклического кода.

Проверочный многочлен циклического кода

Определение

- Проверочный многочлен циклического кода C — это такой многочлен $h(x) \in F_p[x]$, что $g(x)h(x) = x^n - 1$ (где g — порождающий многочлен кода C).
- Легко видеть, что $\deg(h) = n - r = k$, где $r = \deg(g)$ и $k = \dim(C)$.

Лемма 2

- Пусть $c \in F_p[x]$, $\deg(c) < n$. Тогда $c \in C$, если и только если $h(x)c(x) \vdots x^n - 1$.

Доказательство

- ($\Rightarrow$) Пусть $c \in C$. Тогда $c(x) = g(x)a(x)$, где $a \in F_p[x]$.
  - 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 $f \in F_p[x]$.
  - Тогда $h(x)c(x) = (x^n - 1)f(x) = h(x)g(x)f(x)$, откуда

$$c(x) = g(x)f(x) \in C.$$

Проверочная матрица циклического кода

Теорема 9

- Пусть $h(x) = h_0 + h_1 x + \cdots + h_k x^k$ — проверочный многочлен циклического кода C. Тогда матрица

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

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

Доказательство

- Все строки матрицы линейно независимы, поскольку $h_k = 1$.
- Пусть $c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} \in C$.
- 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 $f \in F_p[x], \deg(f) \leq k - 1$.
- Значит, $ch = f \cdot x^n - f$. 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,

$$\sum_{i=0}^{k+t} c_i h_{k+t-i} = 0 \quad \text{при } t \in [0..r-1].$$

- Но написанная выше сумма — это скалярное произведение вектора c на $(r-t)$-ю строку матрицы H.
- Таким образом, для любого $c \in C$ вектор из коэффициентов c ортогонален всем строкам матрицы H.
- Следовательно, строки H — это $n - r$ линейно независимых векторов из $C^\perp$.
- Это означает, что строки H — это базис $C^\perp$.
- По Следствию 1 тогда H — проверочная матрица кода C.

Методы кодирования и декодирования циклического кода.

Циклические коды: кодирование

Несистематический кодер

- Пусть $a(x) = a_0 + a_1 x + \dots + a_{k-1} x^{k-1}$ — исходное сообщение.
- Есть два способа закодировать его в сообщение $c(x) \in C$.
- Пусть $g(x)$ — порождающий многочлен кода C.

1. **Несистематический кодер**: $c(x) := a(x)g(x) \in C$.
   - 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.

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

$$-s(x) = \lambda_0 + \lambda_1 x + \dots + \lambda_{r-1} x^{r-1}.$$

- Поскольку $\deg(s) < r$, все коэффициенты многочлена $a(x)$ являются коэффициентами многочлена $c(x)$. А именно, $a_i = c_{i+r}$.

Декодирование циклического кода

Основные понятия

- Пусть:
  - $a(x)$ — исходное сообщение;
  - $c(x)$ — кодированное сообщение;
  - $c'(x)$ — принятое сообщение (возможно, содержит ошибки);
  - $\varepsilon(x) := c'(x) - c(x)$ — вектор ошибки.

Свойства

- 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.

Нули циклического кода.

Определение

- Пусть $p \in P$. Мы будем рассматривать циклические коды над полем 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 F_q.
- Нулями циклического кода C называются корни его порождающего многочлена.

Теорема 10

- Пусть C — циклический код над F_p длины $n = p^m - 1$, $q = p^m$, $g(x)$ — порождающий многочлен кода C, $\deg(g) = r$, а $\beta_1, \beta_2, \ldots, \beta_r \in F_q$ — все нули C. Пусть $f(x) \in F_p[x]$, $\deg(f) < n$. Тогда:

$$f \in C \iff f(\beta_1) = f(\beta_2) = \cdots = f(\beta_r) = 0.$$

Доказательство

- $(\Rightarrow)$
  - По Теореме 6, $f = g \cdot a$, где $a \in F_p[x]$.
  - Следовательно, $f(\beta_i) = g(\beta_i) \cdot a(\beta_i) = 0$ при всех $i \in [1..r]$.
- $(\Leftarrow)$
  - Разделим f на g с остатком: $f = g \cdot a + s$, где $\deg(s) < r$.
  - Тогда $s(\beta_i) = f(\beta_i) - g(\beta_i) \cdot a(\beta_i) = 0$ 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 $f(x) = g(x) \cdot a(x) \in C$.

Граница БЧХ.

Теорема 11

- Пусть C — p-значный циклический код длины n, $\alpha \in F_{p^n}$ — примитивный элемент, а $g(x)$ — порождающий многочлен кода C. Пусть $b, \delta \in \mathbb{Z}$ таковы, что $b \geq 0$, $\delta > 1$ и

$$g(\alpha^b) = g(\alpha^{b+1}) = \cdots = g(\alpha^{b+\delta-2}) = 0.$$

Тогда кодовое расстояние $d(C) \geq \delta$.

Доказательство

- Предположим противное: пусть в C есть ненулевой элемент, вес Хэмминга которого меньше δ.
- Этому элементу соответствует многочлен

$$f(x) = c_1 x^{k_1} + c_2 x^{k_2} + \cdots + c_{\delta-1} x^{k_{\delta-1}} \in C,$$

где $c_1, c_2, \ldots, c_{\delta-1} \in F_p$ — не все нули.

- По Теореме 10,

$$f(\alpha^b) = f(\alpha^{b+1}) = \cdots = f(\alpha^{b+\delta-2}) = 0.$$

- Получаем следующие равенства:

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

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

$$0 = \begin{vmatrix} \alpha^{k_1 b} & \alpha^{k_2 b} & \ldots & \alpha^{k_{\delta-1} b} \\ \alpha^{k_1 (b+1)} & \alpha^{k_2 (b+1)} & \ldots & \alpha^{k_{\delta-1} (b+1)} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{k_1 (b+\delta-2)} & \alpha^{k_2 (b+\delta-2)} & \ldots & \alpha^{k_{\delta-1} (b+\delta-2)} \end{vmatrix} = \alpha^{(k_1+k_2+\cdots+k_{\delta-1})b} \begin{vmatrix} 1 & 1 & \ldots & 1 \\ \alpha^{k_1} & \alpha^{k_2} & \ldots & \alpha^{k_{\delta-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{k_1 (\delta-2)} & \alpha^{k_2 (\delta-2)} & \ldots & \alpha^{k_{\delta-1} (\delta-2)} \end{vmatrix}. = \alpha^{(k_1+k_2+\cdots+k_{\delta-1})b}$$

- 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.

Коды БЧХ

Определение

- Кодом БЧХ над полем F_p длины $n = p^m - 1$ с конструктивным расстоянием $\delta > 1$ называется циклический код с порождающим многочленом наименьшей степени, корнями которого являются элементы $\alpha^b, \alpha^{b+1}, \ldots, \alpha^{b+\delta-2}$, где α — примитивный элемент поля 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 $d \in \mathbb{N}$ — минимальное такое, что $\alpha^{p^d s} = \alpha^s$.
  - По Теореме 10.13 имеем:

$$M^{(s)}(x) = \prod_{i=0}^{d-1} (x - \alpha^{p^i s}), \quad \deg(M^{(s)}) = d \leq m.$$

- Тогда код БЧХ над полем F_p длины $n = p^m - 1$ с конструктивным расстоянием $\delta > 1$ — это циклический код с порождающим многочленом:

$$g(x) := \operatorname{lcm}(M^{(b)}(x), M^{(b+1)}(x), \ldots, M^{(b+\delta-2)}(x)),$$

где $b \in \mathbb{Z}, b \geq 0$.

Следствие 4

- Код БЧХ C над полем F_p длины $n = p^m - 1$ с конструктивным расстоянием $\delta > 1$ имеет параметры:

$$d \geq \delta, \quad k \geq n - (\delta - 1)m.$$

Доказательство

- По Теореме 11, $d \geq \delta$.
- Рассмотрим порождающий многочлен:

$$g(x) = \operatorname{lcm}(M^{(b)}(x), M^{(b+1)}(x), \ldots, M^{(b+\delta-2)}(x))$$

кода C.
- Заметим, что по доказанному выше:

$$\deg(g) \leq \deg(M^{(b)}) + \deg(M^{(b+1)}) + \cdots + \deg(M^{(b+\delta-2)}) \leq (\delta - 1)m.$$

- Тогда:

$$k = n - \deg(g) \geq n - (\delta - 1)m.$$

Коды Рида-Соломона

Определение

- Пусть $p \in P, m \in \mathbb{N}, q = p^m > 2, \alpha$ — примитивный элемент поля F_q.
- Код Рида-Соломона — это код БЧХ длины $q - 1$ над полем F_p с порождающим многочленом:

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

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

Следствие 5

- Код Рида-Соломона имеет параметры:

$$n = q - 1, \quad k = n - \delta + 1, \quad d = \delta = n - k + 1.$$

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.