Глава 1

Корректирующие коды, код Хемминга

(Конспект: А. Рязанов)

1.1 Общие определения

Кодируется последовательность бит. При **непрерывном коде** кодируется вся последовательность, при **блочном** последовательность разбивается на блоки по k бит и каждый блок кодируется отдельно.

Определение 1.1. Инъективное отображение $f : K \to \{0,1\}^n$, $K \subset \{0,1\}^k$ называется кодом. Образ любого слова из $\{0,1\}^k$ называется кодовым словом или кодом. Множество $C = f(\{0,1\}^k)$ также называется кодом.

Определение 1.2. Код называется раздельным, если $[n] = A \cup B$, $A \cap B = \emptyset$, $|A| = k$ и $\forall x \in K\colon f(x)|_A = x$, то есть, для некоторого подмножества бит кода оно совпадает с прообразом как строка. Биты множества A называются информационными, а из множества B — проверочными.

Определение 1.3. Код называется линейным, если соответствующее отображение f линейно.

Определение 1.4. Раздельный код называется систематическим, если проверочные символы являются линейной комбинацией информационных. То же самое, что раздельный линейный код.

Определение 1.5. Два кода f и g назовем эквивалентными, если $g(x) = f(\pi(x))$, где $\pi(x)$ — это x под действием некоторой перестановки π.

Определение 1.6. Скорость кода $C \subset \{0,1\}^n$ — это величина $R = \frac{1}{n}\log_2|C|$. При $|C| = 2^k$ имеет место $R = \frac{k}{n}$.

Избыточность кода — это величина $1 - R$

1.2 Расстояние Хемминга и исправление ошибок

Определение 1.7. Расстоянием Хемминга между строками $x, y \in \{0,1\}^n$ будем называть величину

$$d(x,y) = |\{i\colon x_i \neq y_i\}|$$

Определение 1.8. $d(C) = \min\limits_{\substack{x,y\in C\\ x\neq y}} d(x,y)$ — кодовое расстояние кода C.

Обозначение: (n,k,d)-код, код с длиной кодируемого слова k, кодового слова n и минимальным кодовым расстоянием d. $[n,K,d]$-код — код с длиной кодового слова n, количеством слов K и минимальным кодовым расстоянием d.

Определение 1.9. Код обнаруживает ошибки в r битах, если существует отображение $g : \{0,1\}^n \to \{0,1\}$, такое, что $\forall x \in \{0,1\}^k, |z| \le r\colon g(f(x) \oplus z) = 1$

Определение 1.10. Код исправляет ошибки в r битах, если существует отображение $g : \{0,1\}^n \to \{0,1\}^k$, такое, что $\forall x \in \{0,1\}^k, |z| \le r\colon g(f(x) \oplus z) = x$

Теорема 1.1. *Для того, чтобы код C позволял обнаружить ошибки в r битах, необходимо и достаточно, чтобы $d(C) \ge r + 1$*

Теорема 1.2. *Для того, чтобы код C позволял исправить ошибки в r битах, необходимо и достаточно, чтобы* $d(C) \geq 2r+1$

Доказательство. $\Leftarrow$

$g(x) = \arg\min\limits_{y\in\{0,1\}^k} d(x, f(y))$. Пусть $x = f(y)+z$ и $|z| \leq r$ и $g(x) \neq y$. Тогда $d(f(g(x)), x) \leq r$, а, значит $d(f(y), f(g(x))) \leq d(x, f(y)) + d(x, f(g(x))) \leq 2r$. Противоречие.

$\Rightarrow$

Рассмотрим $x, y \in C$ такие, что $d(x,y) \leq 2r$. Тогда легко видеть, что существует z, такое, что $d(x,z) \leq r$ и $d(y,z) \leq r$. Тогда, как бы мы не определили $g(z)$, мы получим противоречие с x или y. □

1.3 Граница Хемминга

Определение 1.11. Шаром радиуса r с центром в x назовем множество точек

$$B_r(x) = \{y \colon d(x,y) \leq r\}$$

Количество вершин в шаре в пространстве $\{0,1\}^n$ обозначим $S_r(n)$

Замечание 1.1. $S_r(x) = \sum\limits_{i=0}^{r} C_n^i$.

Доказательство. $S_r(n) = |B_r(0)|$. Строки в $B_r(0)$ — это строки с не более чем r единичными битами. □

Определение 1.12. Энтропией дискретной случайной величины ξ принимающей значения $1, \dots n$ с вероятностями $p_1, \dots, p_n$ называется

$$H(\xi) = -\sum_{i=1}^{n} p_i \log_2(p_i)$$

Лемма 1.1.

$$\frac{1}{n+1} 2^{nH(\frac{r}{n})} \leq C_n^r \leq 2^{nH(\frac{r}{n})}$$

Доказательство. По формуле Стирлинга

$$C_n^r \simeq \frac{\sqrt{2\pi n}}{\sqrt{2\pi k}\sqrt{2\pi(n-k)}} \cdot \frac{n^n}{k^k(n-k)^{n-k}}$$

С другой стороны

$$2^{nH(\frac{r}{n})} = 2^{n\left(-\frac{r}{n}\log_2\frac{r}{n} - (1-\frac{r}{n})\log_2(1-\frac{r}{n})\right)} = \frac{\left(\frac{r}{n}\right)^{-r}}{\left(1-\frac{r}{n}\right)^{n-r}} = \frac{n^n}{r^r(n-r)^{n-r}}$$

Тогда для достаточно больших n достаточно показать

$$\frac{1}{n+1} \leq \frac{\sqrt{2\pi n}}{\sqrt{2\pi k}\sqrt{2\pi(n-k)}} \leq 1$$

Второе неравенство очевидно, поскольку в знаменателе квадратичная зависимость.

$$\frac{\sqrt{2\pi n}}{\sqrt{2\pi k}\sqrt{2\pi(n-k)}} = \sqrt{\frac{n}{k(n-k)}}\frac{1}{\sqrt{2\pi}}$$

$k(n-k) \leq \frac{n^2}{4}$, тогда имеем

$$\frac{\sqrt{2\pi n}}{\sqrt{2\pi k}\sqrt{2\pi(n-k)}} \geq \frac{2}{\sqrt{2\pi n}}$$

для достаточно больших n последнее $\geq \frac{1}{n+1}$ □

Теорема 1.3. *Для достаточно больших n и при условии $0 < r \leq \frac{n}{2}$ верно*

$$\frac{\log_2 S_r(n)}{n} = H(\frac{r}{n}) + O(\frac{\log_2 n}{n})$$

где $H(\frac{r}{n})$ — энтропия случайной величины, принимающей значения 0 и 1 с вероятностями $\frac{r}{n}$ и $1 - \frac{r}{n}$.

Доказательство. Покажем, что при $r \leq \frac{n}{2}$ наибольшим слагаемым будет C_n^r.

$$\frac{C_n^i}{C_n^{i+1}} = \frac{n!(i+1)!(n-i-1)!}{n!i!(n-i)!} = \frac{i+1}{n-i}$$

Возрастание C_n^i равносильно $\frac{C_n^i}{C_n^{i+1}} \leq 1 \iff i+1 \leq n-i \iff 2i \leq n-1$. То есть C_n^i больше предыдущего сочетания, если $2(i-1) \leq n-1$ то есть $i \leq \frac{n+1}{2}$. Тогда имеем

$$C_n^r \leq S_r(n) \leq (r+1)C_n^r$$

Воспользуемся леммой, прологарифмируем формулу оттуда:

$$-\log_2(n+1) + nH(\frac{r}{n}) \leq \log_2 S_r(n) \leq \log_2(r+1) + nH(\frac{r}{n})$$

Поделим три части на n

$$-\frac{\log_2(n+1)}{n} + H(\frac{r}{n}) \leq \frac{\log_2 S_r(n)}{n} \leq \frac{\log_2(r+1)}{n} + H(\frac{r}{n})$$

Тогда получили, что требовалось,

$$\frac{\log_2 S_r(n)}{n} = H(\frac{r}{n}) + \underbrace{c}_{|.|\leq 1}\frac{\log_2(r+1)}{n}$$

□

Теорема 1.4. *(Граница Хемминга) Для любого (n,k)-кода, исправляющего r ошибок верно*

$$n - k \geq \log_2\Big(\sum_{i=0}^{r} C_n^i\Big)$$

Доказательство. Рассмотрим прообразы исправляющей функции g. $g^{-1}(y)$. По определению $|g^{-1}(y)| \geq S_r(n)$ и $y_1 \neq y_2 \implies g^{-1}(y_1) \cap g^{-1}(y_2) = \emptyset$. Тогда для завершения доказательства достаточно расписать

$$2^n = |\{0,1\}^n| = \Big|\bigcup_{y\in\{0,1\}^k} g^{-1}(y)\Big| \geq \sum_{y\in\{0,1\}^k} S_r(k) = 2^k S_r(n)$$

□

Теорема 1.5. *Если $n - k \geq \log_2(n+1)$, то существует $(n,k,3)$ код, то есть, граница Хемминга достигается.*

Доказательство. Построим явно такой линейный код. $C = \{Hx = 0\}$, где H — матрица $(n-k) \times n$. Пусть H_ij — это i-й бит числа j $(1 \leq i \leq n-k$; $1 \leq j \leq n)$. Заметим, что в условиях теоремы в матрице нет двух одинаковых столбцов, то есть, ее ранг не меньше 2. Пусть существуют $x, y \in C$, такие, что $d(x,y) \leq 2$ тогда $d(0, x \oplus y) \leq 2$. То есть $x \oplus y$ имеет не более двух единиц в двоичной записи $H(x \oplus y) = H_{j_1} \oplus H_{j_2} = 0$, что противоречит выводу о ранге. Тогда кодовое расстояние полученного кода равно 3. □

Пример 1.1. Построим систематический (n,k) код Хемминга.

Пусть $a \in \{0,1\}^k$; $b \in \{0,1\}^n$. Кодирующее преобразование $E(a) = b$. Наложим следующие ограничения:

$$\begin{cases} b_i = a_i & i \leq k \\ b_{i+k} = (\Gamma_i, a) & i \leq n-k \end{cases}$$

То есть $b = a(E_k|\Gamma^T)$. То есть, мы построили порождающую матрицу кодирующей функции. Построим теперь проверочную матрицу:

$$b_{i+k} = (\Gamma_i, (b_1, \ldots, b_k)) \iff b_{i+k} \oplus (\Gamma_i, (b_1, \ldots, b_k)) = 0$$

То есть, $H = (\Gamma | E_{n-k})$. Условие $Hb = 0$ является необходимым и достаточным для того, чтобы b являлось кодом, поскольку образом такого b является $(b_1, \ldots, b_k)$.

Если стоблцы матрицы H различны, то по 1.5 мы можем исправлять одну ошибку. Давайте построим явно исправляющую функцию.

Пусть $b' = b \oplus e_i$, где $e_i = (\underbrace{0, \ldots, 0}_{i-1}, 1, 0, \ldots, 0)$. Тогда $Hb' = H_i - i -$ столбец матрицы H. Так как все столбцы различны, мы можем узнать, в каком бите была ошибка. Hb' называется *синдромом* вектора b'.

1.4 Граница Варшамова-Гильберта

Теорема 1.6. *Существует (n,k)-код с минимальным расстоянием d, такой, что*

$$n - k \leq \log_2 S_{d-1}(n)$$

Доказательство. Выберем точку c_1. Рассмотрим $B_{d-1}(c_1)$ и пометим точки в нем. Пока есть непомеченные точки будем выбирать c_i и помечать точки в шаре $B_{d-1}(C_i)$. Так мы построим последовательность точек $c_1, \ldots, c_K$, такую, что $i \neq j \implies d(c_i, d_j) \geq d$. Все точки $\{0,1\}^n$ покрыты хотя бы одним шаром, то есть $K \cdot S_{d-1}(n) \geq 2^n$. $K \geq 2$, если $d - 1 < n$, так как $d((0, \ldots, 0), (1, \ldots, 1)) = n$. Выберем $k = \lceil \log_2 K \rceil$, тогда $2^k S_{d-1}(n) \geq 2^n \implies S_{d-1}(n) \geq 2^{n-k}$. □

Следствие 1.1. *Существует (n,k)-код, исправляющий r ошибок и удовлетворяющий*

$$n - k \leq \log_2(S_{2r}(n))$$

Замечание 1.2. Мы получили верхнюю границу на количество исправляющих символов. Граница Хемминга — нижняя граница, то есть

$$\log_2 S_r(n) \leq n - k \leq \log_2 S_{2r}(n)$$

1.5 Граница Плоткина

Теорема 1.7. *Для $[n, K, d]$-кода выполнено $d \leq \frac{n \cdot \frac{K}{2}}{K-1}$. В частности, для (n,k,d)-кода верно $d \leq \frac{n 2^{k-1}}{2^k - 1}$*

Доказательство. Рассмотрим $D = \sum\limits_{x,y \in C} d(x,y)$. С одной стороны

$$D \geq 2^2_K d = K(K-1)d$$

С другой стороны, нассмотрим каждый бит строк и обозначим

$$d_i(x,y) = \begin{cases} 0 & x_i = y_i \\ 1 & x_i \neq y_i \end{cases}$$

Тогда $d(x,y) = d_1(x,y) + \ldots + d_n(x,y)$. Тогда

$$D = \sum_{i=1}^{n} \underbrace{\sum_{x,y \in C} d_i(x,y)}_{D_i}$$

Заметим, что

$$D_i = 2|\{x \in C \colon x_i = 0\}| \cdot |\{x \in C \colon x_i = 1\}|$$

Тогда $D_i \leq 2\left(\frac{K}{2}\right)^2$, а, значит

$$D \leq \frac{nK^2}{2}$$

Таким образом,

$$\frac{nK^2}{2} \geq K(K-1)d \iff \frac{nK}{K-1} \geq d$$

□

Теорема 1.8. *Если существует, (n,k)-код C, такой, что $d(C) \geq \frac{n}{2}$, то*

$$k \leq \log_2(2n) \iff \frac{\overbrace{K}^{2^k}}{2} \leq n$$

Доказательство. Рассмотрим преобразование

$$\underbrace{(b_1, \ldots, b_n)}_{\in\{0,1\}^n} \mapsto ((-1)^{b_1}, \ldots, (-1)^{b_n})$$

Пусть $v^{(1)}, \ldots, v^{(K)}$ — векторы, полученные этим преобразованием из векторов кода. $d(b^{(i)}, b^{(j)}) \geq \frac{n}{2} \iff (v^{(i)}, v^{(j)}) \leq 0$.

Пусть $\frac{K}{2} > n$, тогда покажем, что не может существовать набора $v^{(1)}, \ldots, v^{(K)}$ с требуемым свойством. Рассмотрим $x \in \mathbb{R}^n$, такой, что $(x, v^{(i)}) \neq 0$ для всех i. Например, можно рассмотреть $(1, 0, \ldots, 0)$.

Тогда $(x, v^{(i)}) > 0$ для не менее чем $\frac{K}{2}$ векторов, либо $(x, v^{(i)}) < 0$ для не менее чем $\frac{K}{2}$ векторов. НУО верно первое иначе рассмотрим $-x$.

Тогда у нас есть набор из $\frac{K}{2} > n$ векторов, таких, что $(x, v^{(i)}) > 0$ для всех i. Количество векторов превышает n, тогда

$$\exists \lambda\colon \sum_{i=1}^{n+1} \lambda_i v^{(i)} = 0$$

НУО $\exists \lambda_i > 0$, иначе поменяем знак всем λ, тогда обозначим $I = \{i\colon \lambda_i > 0\} \neq \emptyset$. Можем записать

$$\sum_{i=1}^{n+1} \lambda_i v^{(i)} = \underbrace{\sum_{i\in I} \lambda_i v^{(i)}}_{z} + \sum_{i \notin I} \lambda_i v^{(i)} = 0$$

- $z \neq 0$. Тогда $(z, z) > 0$, с другой стороны

$$(z, 0 - z) = \Big(\sum_{i\in I} \lambda_i v^{(i)}, -\sum_{i\notin I} \lambda_i v^{(i)}\Big) = -\sum_{\substack{i \in I \\ j \notin I}} \underbrace{\lambda_i}_{>0} \underbrace{\lambda_j}_{<0} \overbrace{(v^{(i)}, v^{(j)})}^{<0} \leq 0$$

  Получаем противоречие

- $z = 0$. Тогда $(z, x) = 0$, но

$$(z, x) = \Big(\sum_{i\in I} \lambda_i v^{(i)}, x\Big) = \sum_{i \in I} \underbrace{\lambda_i}_{>0} \underbrace{(v^{(i)}, x)}_{>0} > 0$$

□

Теорема 1.9. *Для (n,k) кода, такого, что $n \geq 2d(C)$ выполнено*

$$n - k \geq 2d(C) - \log_2 4d(C)$$

Доказательство. При $n = 2d$ воспользуемся 1.8 и получим $-k \geq -\log_2(2n)$ и прибавим к обеим частям $n = 2d$

При $n > 2d$ обозначим $n = 2d + t$ и рассмотрим два случая:

1. $t \geq k$. Тогда сразу $n \geq 2d + k$ и теорема доказана

2. $t < k$. Тогда выберем в коде t информационных символов I_0 тогда рассмотрим код $C' = \{x|_{[n]\setminus I_0}\colon x \in C \wedge x|_{I_0} = a\}$ для произвольного $a \in \{0,1\}^t$. Кодовое расстояние этого кода не менее d, поскольку мы вычеркивали одинаковые символы, $n' = 2d$. Тогда $k - t \leq \log_2(2n')$. Тогда

$$n - k = 2d - (k - t) \geq 2d - \log_2(4d)$$

□

1.6 Асимптотика границ

$R = \frac{k}{n}$ — скорость кода.

Обозначим $\delta(C) = \frac{d(C)}{n}$ — относительное кодовое расстояние.

Обозначим $\mathcal{U} = \{(R, \delta)\} \subset [0,1] \times [0,1]$ множество пар, таких, что существует последовательность (n_i, k_i, d_i) кодов, таких, что

$$n_i \underset{i\to\infty}{\to} \infty$$
$$\frac{k_i}{n_i} \underset{i\to\infty}{\to} R$$
$$\frac{d_i}{n_i} \underset{i\to\infty}{\to} \delta$$

Оценим величину $\bar{R}(\delta) = \sup\{R\colon (R,\delta) \in \mathcal{U}\}$

Замечание 1.3. При $\delta > \frac{1}{2}$ $\bar{R}(\delta) = 0$

Доказательство.

$$d \le \frac{n2^{k-1}}{2^k - 1} \implies \delta + \frac{O(1)}{n} \le \frac{2^{k-1}}{2^k - 1}$$

При $n \to \infty$ получим (пользуясь $2\delta - 1 > 0$) $2^k \le \frac{2\delta}{2\delta - 1}$, тогда $k \le \log_2 \frac{2\delta}{2\delta-1}$, и значит $R = \frac{k}{n} \to 0$ □

Утверждение 1.1. $\bar{R}(\delta) \le 1 - H(\frac{\delta}{2})$

Доказательство. $n - k \ge \log_2 S_{\lfloor \frac{d(C)-1}{2} \rfloor}(n)$ известно из теоремы о границе Хемминга. $d(C) = \lfloor \delta n \rfloor$ имеем

$$1 - \frac{k}{n} \ge \frac{\log_2 S_{\lfloor \frac{\lfloor n\delta \rfloor - 1}{2} \rfloor}(n)}{n}$$

По следствию

$$\frac{\log_2 S_r(n)}{n} = H(\frac{r}{n}) + O(\frac{\log_2 n}{n})$$

тогда

$$1 - R \ge O(\frac{\log_2 n}{n}) + H(\lfloor \frac{\lfloor n\delta \rfloor - 1}{2} \rfloor)$$

пренебрегая округлениями

$$R + O(\frac{\log_2 n}{n}) \le 1 - H(\frac{\delta}{2})$$

и при $n \to \infty$

$$\bar{R}(\delta) \le 1 - H(\frac{\delta}{2})$$

□

Утверждение 1.2. $\bar{R}(\delta) \ge 1 - H(\delta)$ *при* $\delta \le \frac{1}{2}$

Доказательство. Из теоремы о границе Варшамова-Гильберта знаем, что

$$n - k \le \log_2 S_{d-1}(n)$$

в нашем случае

$$1 - \frac{k}{n} \le \frac{\log_2 S_{\lfloor n\delta \rfloor - 1}(n)}{n}$$

по следствию из теоремы о границе Хемминга

$$1 - \frac{k}{n} \le H(\frac{\lfloor n\delta \rfloor - 1}{n}) - O(\frac{\log_2 n}{n})$$

тогда при $n \to \infty$ получаем требуемое. □

Утверждение 1.3. $\bar{R}(\delta) \le 1 - 2\delta$ *при* $\delta \le \frac{1}{2}$

Доказательство. Из последней теоремы о границе Плоткина

$$n - k \ge 2n\delta - \log_2(4n\delta)$$

можно переписать как

$$\frac{k}{n} \le 1 - 2\delta + \frac{\log_2 4n\delta}{n}$$

тогда при $n \to \infty$ имеем $\bar{R} \le 1 - 2\delta$ □

Глава 2

Матрицы и коды Адамара

(Конспект: А. Рязанов)

2.1 Матрицы и коды Адамара, общее представление

Определение 2.1. Матрицей Адамара называется матрица $H \in \{-1,1\}^{n\times n}$, такая, что $H \cdot H^T = nE_n$.

Матрица адамана в нормализованном виде — это матрица, у которой первая строка и первый столбец состоят из единиц.

Двоичная матрица Адамара, это матрица, полученная из матрицы Адамара заменой -1 на 1 а 1 на 0.

Утверждение 2.1. *Умножение строчки или столбца матрицы Адамара на -1 переводит ее в матрицу Адамара.*

Доказательство. Умножение строчки или столбца на единицу, это доножение слева или справа на матрицу $d = diag(1,\ldots,1,-1,1,\ldots,1)$. Тогда в первом случае

$$(dH)\cdot(dH)^T = dHH^Td^T = d(nE)d^T = nEdd^T = nE$$

а во стором

$$(Hd)\cdot(Hd)^T = Hdd^TH^T = HH^T = nE$$

$\square$

Теорема 2.1. *Если существует матрица Адамара порядка n, то $n \in \{1,2\} \cup \{4k\}$*

Доказательство. Пусть $n \geq 3$ и существует H. Тогда представим ее в нормализованном виде и разделим столбцы на четыре типа:

1. Начинается с $(1,1,1)$ — i штук
2. Начинается с $(1,1,-1)$ — j штук
3. Начинается с $(1,-1,1)$ — k штук
4. Начинается с $(1,-1,-1)$ — l штук

Запишем условия ортогональности строк $(1,2)$, $(2,3)$ и $(1,3)$:

$$\begin{cases} i+j-k-l=0 \\ i-j+k-l=0 \\ i-j-k+l=0 \end{cases}$$

Тогда $i=j=k=l$, тогда $n=4i$ $\square$

Утверждение 2.2. *Если H — матрица Адамара, то*

$$\begin{pmatrix} H & H \\ H & -H \end{pmatrix}$$

— тоже матрица Адамара.

Доказательство.

$$\begin{pmatrix} H & H \\ H & -H \end{pmatrix} \cdot \begin{pmatrix} H^T & H^T \\ H^T & -H^T \end{pmatrix} = \begin{pmatrix} HH^T + HH^T & HH^T - HH^T \\ HH^T - HH^T & HH^T + HH^T \end{pmatrix} = 2nE_{2n}$$

□

Такие матрицы Адамара называются матрицами Сильвестра.

Определение 2.2. Симплексным кодом Адамара называется $[K-1, K, \frac{K}{2}]$-код, состоящий из строк двоичной матрицы Адамара из которой удален первый столбец.

Утверждение 2.3. *Для симплексного кода Адамара выполнено* $K = \frac{2d}{2d-n}$.

Доказательство. Очевидно. □

Замечание 2.1. Если матрица Адамара, построена по способу Сильвестра, то симплексный код, построенный по ней, линеен.

2.2 Построение матрицы Адамара по способу Пэли

Определение 2.3. Пусть $p \in \mathbb{P}\backslash\{2\}$. $\{a \in \{0, \dots, p-1\} \colon \exists b \colon b^2 = a\}$ называется множеством квадратичных вычетов.

Определение 2.4. Функция

$$\chi(i) = \begin{cases} 0 & i \text{ кратно } p \\ 1 & i \mod p \text{ вычет} \\ -1 & i \mod p \text{ невычет} \end{cases}$$

называется символом Лежандра.

Теорема 2.2. $\forall c \neq 0 \mod p$ *выполнено* $\sum\limits_{b=0}^{p-1} \chi(b)\chi(b+c) = -1$

Конструкция 2.1. Матрица Джекобстола. $Q = \{q_{ij}\}_{p \times p}$. $q_{ij} = \chi(j-i)$.

Лемма 2.1. $Q \cdot Q^T = pE - \mathbf{1}_{p\times p}$
$Q\mathbf{1}_{p\times p} = \mathbf{1}_{p\times p}Q = 0$

Доказательство. $Q\mathbf{1}_{p\times p} = \mathbf{1}_{p\times p}Q = 0$, так как по модулю p существует $\frac{p-1}{2}$ вычетов и $\frac{p-1}{2}$ невычетов.

Рассмотрим $P = \{p_{ij}\} = Q \cdot Q^T$. Тогда

$$\begin{aligned} p_{ii} &= \sum_{k=0}^{p-1} q_{ik}^2 = p \\ p_{ij} &= \sum_{k=0}^{p-1} q_{ik}q_{jk} \end{aligned}$$

$$p_{ij} = \sum_{k=0}^{p-1} \chi(i-k)\chi(j-k) = \sum_{k=0}^{p-1} \chi(i-k) + \chi((i-k)+(j-i)) = -1$$

□

Лемма 2.2. *Пусть*

$$H = \begin{pmatrix} 1 & \mathbf{1}_p \\ \mathbf{1}_p & Q-E \end{pmatrix}$$

Тогда H — матрица Адамара

Доказательство.

$$H \cdot H^T = \begin{pmatrix} 1 & \mathbf{1}_p \\ \mathbf{1}_p & Q-E \end{pmatrix} \cdot \begin{pmatrix} 1 & \mathbf{1}_p \\ \mathbf{1}_p & Q^T-E \end{pmatrix} = \begin{pmatrix} p+1 & \mathbf{0}_p \\ \mathbf{0}_p & \mathbf{1}_{p\times p} + (Q-E)(Q^T-E) \end{pmatrix}$$

Распишем

$$\mathbf{1}_{p\times p} + (Q-E)(Q^T-E) = \mathbf{1}_{p\times p} + QQ^T - Q - Q^T + E\mathbf{1}_{p\times p} + QQ^T - Q - Q^T + E$$

заметим, что $q_{ij} = \chi(i-j) = \chi(-1)\chi(j-i) = -\chi(j-i)$, тогда $Q^T = -Q^T$, тогда

$$\mathbf{1}_{p\times p} + QQ^T - Q - Q^T + E = \mathbf{1}_{p\times p} + QQ^T + E = (p+1)E$$

□

Глава 3

Линейные коды

(Конспект: А. Рязанов)

3.1 Базовые факты, коды Адамара

Определение 3.1. Код называется линейным, если множество кодовых слов C является линейным подпространством $\{0,1\}^n$.

Определение 3.2. Весом Хэмминга $a \in \{0,1\}^n$ назовем $w(a) = \{i\colon a_i = 1\}$

Замечание 3.1. $d(a,b) = w(a \oplus b)$

Лемма 3.1. *Пусть C — линейный код. Тогда* $d(C) = \min\limits_{\substack{x \in C \\ x \neq 0}} w(x)$

Доказательство. $d(C) = \min\limits_{a \neq b \in C} d(a,b) = \min\limits_{a \neq b \in C} w(a \oplus b) = \min\limits_{\substack{x \in C \\ x \neq 0}} w(x)$ □

Определение 3.3. Пусть C — некоторый линейный код с порождающей матрицей G и проверочной матрицей H. Тогда дуальным к нему называется код $C^\perp$ с порождающей матрицей H и проверочной матрицей G.

Если C являлся (n,k)-кодом, то $C^\perp$ будет $(n, n-k)$-кодом.

Теорема 3.1. *Дуальный код Хэмминга* $(2^m - 1, 2^m - 1 - m)$ *является кодом Адамара с матрицей Сильвестра.*

Доказательство. Будем доказывать по индукции.

База: $m = 2$. Тогда $n = 2^m - 1 = 3$, $k = 2^m - 1 - m = 1$. Тогда проверочная матрица такого кода Хемминга имеет вид $\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$ Тогда все векторы дуального кода выглядят как: $\begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$. Этот код совпадает с соответствующим кодом Адамара.

Переход: пусть доказано для $n = 2^{m-1} - 1$. Пусть $\bar{H} \in \{0,1\}^{(m-1) \times 2^{m-1}}$ — проверочная матрица для кода Хэмминга $(2^{m-1} - 1, 2^{m-1} - 1 - (m-1))$.

Покажем, что матрица

$$H = \begin{pmatrix} 0 \dots 0 & 1 & 1 \dots 1 \\ \bar{H} & \mathbf{0}_{m-1} & \bar{H} \end{pmatrix}$$

является проверочной матрицей кода Хэмминга $(2^m - 1, 2^m - 1 - m)$. Это почти очевидно, достаточно заметить, что столбцы матрицы различны и ее размерность $m \times (2^m - 1)$ (следует из того же свойства для $\bar{H}$ и отсутствия в $\bar{H}$ нулевого столбца.

По индукционному предположению матрица $\bar{H}$ порождает строки матрицы $\mathcal{A}'$ — усеченной бинарной матрицы Адамара размера $2^{m-1} \times 2^{m-1} - 1$. Тогда матрица $(\bar{H}|\mathbf{0}_{m-1}|\bar{H})$ порождает строки матрицы $(\mathcal{A}'|\mathbf{0}_{2^{m-1}}|\mathcal{A}')$.

Добавим в $(\bar{H}|\mathbf{0}_{m-1}|\bar{H})$ первую строку H_1, чтобы получить матрицу H. Тогда можно сделать вывод, что матрица H порождает все строки матрицы $(\mathcal{A}'|\mathbf{0}_{2^{m-1}}|\mathcal{A}')$ и строки, полученные из них прибавлением H_0. Тогда в итоге мы получим коды

$$\begin{pmatrix} \mathcal{A}' & \mathbf{0}_{2^{m-1}} & \mathcal{A}' \\ \mathcal{A}' & \mathbf{1}_{2^{m-1}} & \mathbf{1} - \mathcal{A}' \end{pmatrix}$$

Припишем слева столбец из нулей и получим, что новая матрица — это в точности матрица, полученная из $(\mathbf{0}_{2^{m-1}}|\mathcal{A}')$ по правилу Сильвестра. Таким образом, теорема доказана.

□

Следствие 3.1. *Код Адамара с матрицей Сильвестра является линейным.*

Теорема 3.2. *Пусть C — линейный код, H — его проверочная матрица.*

1. *В проверочной матрице H любые $d-1$ столбцов линейно независимы $\iff$ $d(C) \geq d$*

2. *Если любые $d-1$ столбцов матрицы H линейно независимы и существуют d линейно зависимых столбцов, то $d(C) = d$*

Доказательство. $\Rightarrow$

По лемме $d(C) = \min\limits_{x \in C} w(x)$. Пусть существует $x \in C$ такое, что $w(x) < d$. $Hx = 0$. Пусть $i_1, \ldots, i_r$ — номера ненулевых компонент x ($r < d$). Тогда $H_{i_1} \oplus H_{i_2} \oplus \ldots \oplus H_{i_r} = 0$, но это противоречит условию линейной независимости столбцов.

$\Leftarrow$

Если $H_{i_1} \oplus \ldots \oplus H_{i_r} = 0$, то рассмотрим вектор $x = \{x_j\}$, $x_j = \begin{cases} 0 & \exists l \colon j = i_l \\ 1 & \text{иначе} \end{cases}$, Для такого вектора $Hx = 0$, но $w(x) = r < d$.

Пункт 2 непосредственно следует из пункта 1. □

3.2 Смежные классы и декодирование по синдрому

Определение 3.4. Смежным классом группы G по подгруппе C называется множество вида

$$\begin{array}{ll} Cb = \{xb \colon x \in C\} & \text{правый} \\ bC = \{bx \colon x \in C\} & \text{левый} \end{array}$$

Определение 3.5. Синдром вектора x относительно линейного кода C с проверочной матрицей H называется вектор Hx

Теорема 3.3. *Пусть $x, y \in \{0,1\}^n$. Тогда $x, y \in Cz$ для некоторого $z \iff Hx = Hy$*

Доказательство. $\Rightarrow x = a + z$, $y = b + z$, $a, b \in C$. Тогда

$$Hx = Ha + Hz = Hz = Hb + Hz = Hy$$

$\Leftarrow Hx = Hy \implies H(x+y) = 0$, тогда $x, y \in Cx$. □

Пусть $b \in C$, $b' = b + e$, где e — вектор ошибок. Тогда $Hb' = He$, то есть, ошибку для b' нужно искать в его смежном классе по C.

Лидер — это слово наименьшего веса в смежном классе. Лидер является наиболее вероятным вектором ошибок.

Утверждение 3.1. *Будем полагать вектором ошибок лидера соответствующего смежного класса. Составим матрицу $A = \{A_{ij}\}_{2^{n-k} \times 2^k}$, $A_{i,0}$ — лидер смежного класса i, $A_{0,i} \in C$ и $A_{ij} = A_{i,0} \oplus A_{0,j}$.*

1. *Исправим все ошибки, являющиеся лидерами*

2. *Для любого слова A_{ij} слово $A_{0,j}$ является ближайшим к A_{ij} кодовым словом.*

Доказательство. 1. Очевидно

2. $A_{ij} = A_{0,j} + A_{i,0}$. $A_{i,0}$ — лидер. $d(A_{ij}, A_{0,j}) = w(A_{i,0})$.

   Рассмотрим другое кодовое слово $A_{0,j'}$.

$$d(A_{ij}, A_{0,j'}) = w(A_{ij} \oplus A_{0,j'})$$

$$A_{ij} \oplus A_{0,j'} = A_{i,0} \oplus \underbrace{A_{0,j} \oplus A_{0,j'}}_{\in C}$$

   Тогда $A_{ij} \oplus A_{0,j'}$ лежит в смежном классе i, значит $w(A_{ij} \oplus A_{0,j'}) \geq w(A_{i,0})$, что и требовалось.

□

3.3 Полиномиальные коды

Определение 3.6. Установим взаимно однозначной соответствие между многочленами степени $< n$ и двоичными векторами из $\{0,1\}^n$.

$$\sum_{i=0}^{n-1} g_i x^i \mapsto (x_0, \dots, x_{n-1}) \mapsto \sum_{i=0}^{n-1} g_i x^i$$

. Тогда рассмотрим некоторый многочлен $g(x)$, тогда кодовые многочлены получаются по правилу $b(x) = a(x)g(x)$, где $deg(a(x)) < k$. Тогда, если $deg(g(x)) = n - k$, то получается (n,k) код.

Пример 3.1. $(6,4)$ код, с порождающим многочленом $1 + x + x^2$

$$\begin{array}{lcl} 0001 & \xrightarrow{x^3} & 000111 \\ 0010 & \xrightarrow{x^2} & 001110 \\ 0100 & \xrightarrow{x} & 011100 \\ 1000 & \xrightarrow{1} & 111000 \end{array}$$

3.4 Совершенные линейные коды

Определение 3.7. Линейный (n,k)-код, исправляющий r ошибок называется совершенным, если для него достигается граница Хэмминга:

$$2^{n-k} = S_r(n)$$

Замечание 3.2. Для нелинейных кодов граница Хэмминга имеет вид

$$K = \frac{2^n}{S_r(n)}$$

Пример 3.2. $(2m+1,1)$ код. Кодовые слова $\begin{pmatrix} 0 & \dots & 0 \\ 1 & \dots & 1 \end{pmatrix}$. Этот код исправляет m ошибок.

$$S_m(2m+1) = \sum_{i=0}^{m} C_{2m+1}^i = \frac{1}{2}\sum_{i=0}^{m}(C_{2m+1}^i + C_{2m+1}^{2m+1-i}) = 2^{2m}$$

Тогда $2^{2m+1-1} = 2^{2m} = S_m(2m+1)$, что и требуется по определению.

Пример 3.3. Код Хэмминга с $n = 2^m - 1$, $k = 2^m - 1 - m$, $m \geq 2$. Код исправляет одну ошибку, $S_1(n) = 1 + n = 2^m$. Тогда

$$2^{n-k} = 2^{2^m - 1 - (2^m - 1 - m)} = 2^m = S_1(n)$$

Теорема 3.4. *Следующие условия равносильны*

1. *Существует двоичный совершенный код C в $\{0,1\}^n$, который исправляет одну ошибку*

2. *$n = 2^m - 1$*

Доказательство. 2 $\implies$ 1 Должно выполняться $K = \frac{2^n}{n+1}$. K может быть целым, только если $n + 1 = 2^m$ для некоторого m.

1 $\implies$ 2 Доказали в примере 3.3. □

Пример 3.4. $(23,12)$-код Голея, исправляющий 3 ошибки. $S_3(23) = 1 + 23 + C_{23}^2 + C_{23}^3 = 2048 = 2^{11}$. Тогда $2^{23} = S_3(23) \cdot 2^{12}$.

3.5 Двоичные циклические коды

Определение 3.8. Линейный код C называется циклическим, если $\forall b \in C$: $b^{(1)} \in C$, где $(b_0, \dots, b_{n-1})^{(1)} = (b_{n-1}, b_0, \dots, b_{n-2})$

Аналогично обозначим $b^{(j)} = (b^{(j-1)})^{(1)}$ — сдвиг на j позиций вправо.

Определение 3.9. Кодовым многочленом, соответствующим $b \in C$ назовем многочлен $\sum\limits_{i=0}^{n-1} b_i x^i$

Теорема 3.5. $b^{(j)}(x) = x^j b(x) \mod (x^n+1)$

Доказательство. Распишем $x^j b(x)$:

$$x^j b(x) = \sum_{i=0}^{n-j-1} b_i x^{i+j} + \sum_{i=n-j}^{n-1} b_i x^{i+j} = \sum_{i=0}^{n-j-1} b_i x^{i+j} + x^n \underbrace{\sum_{i=n-j}^{n-1} b_i x^{i+j-n}}_{q(x)}$$

Рассмотрим многочлен $q(x) = b_{n-j} + b_{n-j+1}x + \ldots + b_{n-1}x^{j-1}$ и прибавм его дважды к $x^j b(x)$ $(q(x)+q(x)=0)$:

$$x^j b(x) = \underbrace{b_{n-j} + b_{n-j+1}x + \ldots + b_{n-1}x^{j-1}}_{q(x)} + b_0 x^j + \ldots + b_{n-j-1}x^{n-1} + x^n q(x) + q(x)$$

Тогда по модулю x^n+1 получаем $b^{(j)}(x)$ □

Теорема 3.6. *В циклическом коде существует только один ненулевой многочлен минимальной степени.*

Доказательство. Пусть есть два таких многочлена $q_1(x) = x^m + \ldots$; $q_2(x) = x^m + \ldots$. Тогда из линейности кода $q_1(x) + q_2(x) \in C(x)$. Но

$$(q_1+q_2)(x) = \underbrace{x^m + x^m}_{=0} + \underbrace{\ldots}_{deg<m}$$

тогда q_1 и q_2 не минимальны по степени. противоречие. □

Определение 3.10. Кодовый многочлен $g(x)$ минимальной степери среди многочленов $C(x)$ называется порождающим многочленом C.

Теорема 3.7. *Свободный член $g(x)$ — порождающего многочлена циклического кода, равен* 1.

Доказательство. Пусть $g_0 = 0$, тогда $g_1 + g_2x + \ldots + g_{n-1}x^{n-2} \in C(x)$, но его степень меньше, чем у g. Противоречие. □

Теорема 3.8. *Пусть $g(x)$ — порождающий многочлен для циклического кода длины n. Тогда $b(x) \in C(x) \iff b(x)$ кратно $g(x)$.*

Доказательство. $\Leftarrow$ Пусть $b(x) = g(x)\cdot a(x)$. $deg(a) \le n-m-1$, тогда

$$b(x) = g(x)\sum_{i=0}^{n-m-1} a_i x^i = \sum_{i=0}^{n-m-1} a_i \underbrace{g(x)x^i}_{=g^{(i)}(x)}$$

таким образом, $b(x)$ представлен в виде линейной комбинации циклических сдвигов $g(x)$, то есть $b(x) \in C(x)$

$\Rightarrow$ Пусть $b(x) \in C(x)$. Можно записать $b(x) = g(x)\cdot q(x) + r(x)$. Нужно показать, что $r(x) = 0$

$$r(x) = \underbrace{b(x)}_{\in C(x)} + \underbrace{g(x)q(x)}_{\in C(x)}$$

Тогда $r(x) \in C(x)$. $deg(r(x)) < deg(g(x))$, тогда по теореме 3.6 $r(x) = 0$. □

Теорема 3.9. *Пусть код порождается многочленом $g(x)$. Тогда следующие условия равносильны*

1. *C является циклическим*
2. *$g(x)$ — делитель x^n+1*

Доказательство. $1 \implies 2$ Рассмотрим $b \in C$. По теореме 3.5 имеем $b(x)x^j = b^{(j)}(x) + (x^n+1)q(x)$. Выберем j так, чтобы $deg(b(x)x^j) = n$, тогда $q(x) = 1$. Тогда

$$\exists j \in \{0, \dots, n-1\} \colon x^j b(x) = b^{(j)}(x) + (x^n + 1)$$

Так как C циклический и порождается $g(x)$, то $b^{(j)}(x) = g(x)a_j(x)$. Тогда

$$\underbrace{x^j b(x)}_{\text{кратно } g(x)} = \underbrace{b^{(j)}(x)}_{\text{кратно } g(x)} + (x^n + 1)$$

Тогда и $x^n + 1$ кратно $g(x)$.

$2 \implies 1$ Снова запишем

$$x^j b(x) = b^{(j)}(x) + (x^n + 1)q(x)$$

Тогда

$$b^{(j)}(x) = \underbrace{x^j b(x)}_{\text{кратно } g(x)} + \underbrace{(x^n + 1)}_{\text{кратно } g(x)} q(x)$$

Таким образом, код циклический. $\square$