Криптография и корректирующее кодирование

13 января 2017 г.

Оглавление

Глава 1

Корректирующие коды, код Хемминга

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 $\forall x \in \{0,1\}^k, |z| \leq r\colon g(f(x) \oplus z) = 1$

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

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

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 $1, \ldots n$ с вероятностями $p_1, \ldots, p_n$ 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* $0 < r \le \frac{n}{2}$ *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 $r \le \frac{n}{2}$ 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 $\frac{C_n^i}{C_n^{i+1}} \le 1 \iff i+1 \le n-i \iff 2i \le n-1$. То есть C_n^i больше предыдущего сочетания, если $2(i-1) \le n-1$ то есть $i \le \frac{n+1}{2}$. Тогда имеем

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

Воспользуемся леммой, прологарифмируем формулу оттуда:

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

Поделим три части на n

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

Тогда получили, что требовалось,

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

□

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

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

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

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

□

Теорема 1.5. *Если* $n - k \ge \log_2(n+1)$*, 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 ($1 \le i \le n-k$; $1 \le j \le n$). 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 $d(x,y) \le 2$ тогда $d(0, x\oplus y) \le 2$. 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:

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

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 $(b_1, \dots, b_k)$.

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 $e_i = (\underbrace{0, \dots, 0}_{i-1}, 1, 0, \dots, 0)$. 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*

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

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 $c_1, \dots, c_K$, такую, что $i \ne j \implies d(c_i, d_j) \ge d$. Все точки $\{0,1\}^n$ покрыты хотя бы одним шаром, то есть $K \cdot S_{d-1}(n) \ge 2^n$. $K \ge 2$, если $d - 1 < n$, так как $d((0, \dots, 0), (1, \dots, 1)) = n$. Выберем $k = \lceil \log_2 K \rceil$, тогда $2^k S_{d-1}(n) \ge 2^n \implies S_{d-1}(n) \ge 2^{n-k}$. □

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

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

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

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

1.5 Граница Плоткина

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

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

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

С другой стороны, нассмотрим каждый бит строк и обозначим

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

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

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

Таким образом,

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

□

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 $C' = \{x|_{[n]\setminus I_0}\colon x \in C \land x|_{I_0} = a\}$ 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.

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

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

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

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

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

По следствию

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

тогда

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

пренебрегая округлениями

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

и при $n \to \infty$

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

□

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

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

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

в нашем случае

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

по следствию из теоремы о границе Хемминга

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

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

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

Доказательство. Из последней теоремы о границе Плоткина

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

можно переписать как

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

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

Глава 2

Матрицы и коды Адамара

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 $d = diag(1, \dots, 1, -1, 1, \dots, 1)$. Тогда в первом случае

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

а во стором

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

□

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 $n = 4i$ □

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 $p \in \mathbb{P} \backslash \{2\}$. $\{a \in \{0, \ldots, p-1\} \colon \exists b \colon b^2 = a\}$ 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

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 $w(a) = \{i : a_i = 1\}$

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.

$\square$

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. $\square$

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 $x, y \in Cx$. $\square$

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.

$\square$

3.3 Полиномиальные коды

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

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

. 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 $1 + x + x^2$

$$\begin{array}{lcl} 0\,0\,0\,1 & \xrightarrow{x^3} & 0\,0\,0\,1\,1\,1 \\ 0\,0\,1\,0 & \xrightarrow{x^2} & 0\,0\,1\,1\,1\,0 \\ 0\,1\,0\,0 & \xrightarrow{x} & 0\,1\,1\,1\,0\,0 \\ 1\,0\,0\,0 & \xrightarrow{1} & 1\,1\,1\,0\,0\,0 \end{array}$$

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 $\begin{pmatrix} 0 & \ldots & 0 \\ 1 & \ldots & 1 \end{pmatrix}$. 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

3.5.1 Свойства циклического кода

Определение 3.8. Линейный код C называется циклическим, если $\forall b \in C\colon b^{(1)} \in C$, 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 $g_1 + g_2 x + \ldots + g_{n-1}x^{n-2} \in C(x)$, 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. □

3.5.2 Порождающая и проверочная матрицы циклического кода

Пусть C — циклический код с порождающим многочленом $g(x) = 1 + g_1x + \ldots + g_{r-1}x^{r-1} + x^r$. Тогда все кодовые многочлены имеют вид

$$b(x) = g(x) \underbrace{a(x)}_{deg=k-1} = a_0g(x) + a_1xg(x) + \ldots + a_{k-1}x^{k-1}g(x)$$

То есть, любой кодовый многочлен представляется как линейная комбинация многочленов $x^jg(x)$. Тогда порождающая матрица имеет вид:

$$G = \begin{pmatrix} 1 & g_1 & g_2 & \dots & g_{r-1} & 1 & 0 & \dots & 0 \\ 0 & 1 & g_1 & \dots & g_{r-2} & g_{r-1} & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \\ 0 & \dots & \dots & 1 & g_1 & \dots & & g_{r-1} & 1 \end{pmatrix}$$

Теперь построим проверочную матрицу. Рассмотрим $h(x)$, такой, что $x^n+1 = h(x)g(x)$. Тогда рассмотрим произвольный кодовый многочлен $b(x) = q(x)g(x)$.

$$b(x)h(x) = q(x)g(x)h(x) = q(x)(x^n+1) = q(x) + x^na(x)$$

Заметим, что $deg(a(x)) \le k-1$, а мономы $x^na(x)$ имеют степень не менее n тогда коэффициенты $b(x)h(x)$ при $x^k, x^{k+1}, \dots, x^{n-1}$ равны нулю. Давайте выразим эти коэффициенты через коэффициенты b и h:

$$\begin{array}{l} \sum\limits_{i=0}^{k} b_ih_{k-i} = 0 \\ \sum\limits_{i=0}^{k} b_{i+1}h_{k-i} = 0 \\ \dots \end{array}$$

Тогда в матричном виде это выглядит как:

$$H = \begin{pmatrix} h_k & h_{k-1} & h_{k-2} & \dots & h_1 & h_0 & 0 & \dots & 0 \\ 0 & h_k & g_{k-1} & \dots & h_2 & h_1 & h_0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \\ 0 & \dots & \dots & h_k & g_{k-1} & \dots & & h_1 & h_0 \end{pmatrix}$$

Замечание 3.3. Строки в G и H линейно независимы, поскольку у каждой строки есть компонент, отсутствующий во всех строках с большими номерами. Формально можно доказать по индукции.

Замечание 3.4. Порождающим многочленом дуального кода, порожденного многочленом $g(x)$ с проверочным многочленом $h(x)$ является многочлен $x^k h(x^{-1})$.

Доказательство. Многочлен $x^k h(x^{-1}) = h_k + x h_{k-1} + \ldots + x^{k-1} h_1 + x^k h_0$, то есть, это многочлен $h(x)$ с развернутыми коэффициентами. Тогда порождающая матрица для этого многочлена совпадает с проверочной для кода, порожденного C. □

3.6 Модификации линейных кодов

Определение 3.11. $(n+1,k)$-код, полученный из (n,k)-кода добавлением одного контрольного бита (иначе говоря, дополнительной переменной), называется *расширенным кодом (extended code).*

Вообще говоря, добовлять можем любой бит, но это не всегда имеет смысл.

Утверждение 3.2. *Любой (n,k,d)-код с нечётным кодовым расстоянием можно расширить до $(n+1,k,d+1)$-кода добавлением бита проверки чётности.*

Доказательство. Если между двумя словами было расстояние d, то одно из них имеет чётный вес, а другое нечётный, т.к. d нечётно. Тогда очевидно, что добавление бита проверки чётности увеличит расстояние между ними. □

Определение 3.12. $(n-1,k)$-код, полученный из (n,k)-кода удалением одного из контрольных битов (удалением переменной), называется *проколотым кодом (punctured code).*

Если расширим код, а затем уменьшим его на тот же контрольный бит, на который увеличивали, получим исходный код.

Если удаляемый бит принимает значение 1 в кодовом слове минимального веса, то минимальное кодовое расстояние уменьшается.

Определение 3.13. Код, полученный удалением информационных битов, называется *укороченным кодом (shortened code).*

Это значит удаление строки из порождающей матрицы и удаление столбца из проверочной. Т.е. (n,k)-код превращается в $(n-1,k-1)$-код.

Определение 3.14. Код, полученный добавлением информационного бита, называется *удлинённым кодом (lengthened code).*

Это значит, что мы добавили строку в порождающую матрицу и столбец в проверочную. Т.е. (n,k)-код превращается в $(n+1,k+1)$-код.

Утверждение 3.3. *При удлинении и при укорочении минимальное кодовое расстояние не меняется.*

Доказательство.

1. При удлинении очевидно.

2. При укорочении происходит следующее: из G вычёркивается строка и соответствующий её столбец *единичной подматрицы.* Соответственно, вычёркивается столбец из проверочной матрицы.
   Любая линейная комбинация строк G имеет вес как минимум d.

   $$a_1 g_1 + \ldots + a_n g_n \geq d, \ \forall \{a_i\}$$

   Вычёркивание i-ой строки и соответствующего ей столбца — это линейная комбинация с $a_i = 0$.

□

Определение 3.15. Код, полученный удалением некоторых кодовых слов, называется *суженным кодом (expurgated code).*

Возможно построить суженный код так, чтобы он оставался линейным.

Минимальное кодовое расстояние может увеличиться.

Определение 3.16. Код, полученный добавлением новых кодовых слов, называется *дополненным кодом (augmented code)*.

Пример 3.5. $(7,4)$-код Хэмминга.

Построим расширенный код двум способами: начиная с проверочной матрицы и начиная с порождающей. Новая переменная — дополнительная проверка чётности для всех битов.

1. Проверочная матрица

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & |0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & |0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & |0 \\ \overline{1} & \overline{1} & \overline{1} & \overline{1} & \overline{1} & \overline{1} & \overline{1} & 1 \end{bmatrix}$$

   Последняя строка соответствует уравнению $\sum\limits_{i=0}^{6} x_i = x_7$, то есть x_7 — бит проверки четности.

   Линейными преобразованиями получим

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{bmatrix}$$

   Ей соответствует порождающая матрица

$$G = \begin{bmatrix} 1 & 0 & 1 & |1| & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & |0| & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & |1| & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & |1| & 0 & 0 & 0 & 1 \end{bmatrix}$$

   соответствующая начальной порождающей, к которой добавили 1 столбец (4-ый).

2. Порождающая матрица

$$G = \begin{bmatrix} 1 & 0 & 1 & |?| & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & |?| & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & |?| & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & |?| & 0 & 0 & 0 & 1 \end{bmatrix}$$

   . Добавим такой столбец, что количество единиц в каждой строке чётно. Легко видеть, что это тот же столбец, который мы получили в первом случае и других быть не может.

   Почему появляется условие чётности по строкам? Вспомним,$G = (\Gamma^t|E)\,, H = (E|\Gamma)$. От H хотим, чтобы линейными преобразованиями над строками можно было получить строку из всех единиц. Поскольку в H есть единичная подматрица, единственный способ это сделать — просуммировать все строки с коэффициентами 1. Тогда нам необходимо, чтобы все столбцы Γ были веса 1, то есть чтобы все строки Γ^t были веса 1. Следовательно, все строки G должны иметь вес 0.

3.7 Бинарные коды Голея

Чтобы бинарный (n,k,d)-код был совершенным, необходимо выполнение условия плотной упаковки:

$$2^k \sum_{k=0}^{\lfloor \frac{d-1}{2} \rfloor} C_n^k = 2^n$$

Голей нашел два возможных кандидата: $(23,12,7)$ и $(90,78,5)$.

Теорема 3.10. *Не существует бинарного* $(90,78,5)$*-кода.*

Доказательство. Предположим, что существует C — $(90,78,5)$-код. Не умаляя общности можем считать, что $0 \in C$ (иначе выберем любой вектор C и прибавим его ко всем векторам кода).

Пусть $Y = \{y \in \{0,1\}^{90} \colon y_0 = y_1 = 1 \wedge w(y) = 3\}$. Очевидно, $|Y| = 88$. Так как C — совершенный код, каждому $y \in Y$ соответствует единственный $x \in C$ причем $d(x,y) = 2$. Тогда $1 \le w(x) \le 5$, но $d(x,0) \ge 5$ и тогда мы можем заключить, что $w(x) = 5$. Тогда $y \subset x$, то есть $y_i = 1 \implies x_i = 1$.

Пусть $X = \{x \in C \colon x_0 = x_1 = 1 \wedge w(x) = 5\}$. Каждому $y \in Y$ соответствует единственный $\phi(y) = x \in X$, такой, что $d(x,y) = 2$. С другой стороны, рассмотрим $x \in X$. Заменяя две из трех единиц, стоящих на позициях $\{2,\ldots,89\}$ на нули мы получим три различных $y_1, y_2, y_3 \in Y$, при этом $d(x,y_1) = d(x,y_2) = d(x,y_3) = 2$, тогда $\phi(y_1) = \phi(y_2) = \phi(y_3) = x$. Для любых других $y \in Y$ $d(x,y) > 2$. Тогда все элементы Y должны разбиться на тройки по значению $\phi(y)$. Но 88 не делится на 3. Противоречие. □

Определение 3.17. Расширенным кодом Голея назовем $(24,12)$-код, построенный с помощью порождающей матрицы $G = (E_{12}|A)$, где A — фиксированная матрица 12×12, обладающая следующими свойствами:

- $A = A^T$
- $i \neq j \implies A_i \perp A_j$ (где A_i, A_j — строки матрицы A)

Утверждение 3.4. *Так построенный код обладает кодовым расстоянием 8 и исправляет три ошибки.*

Замечание 3.5. Удалив один проверочный бит из $(24,12,8)$-кода получим $(23,12,7)$-код — совершенный код Голея.

Утверждение 3.5. *Код Голея самодуален, то есть $G^\perp = G$*

Доказательство. Заметим, что строки матрицы G ортогональны. Это следует из того, что строки E ортогональны и строки A ортогональны. Тогда $G \subset G^\perp$. Но размерности G и $G^\perp$ равны 12, тогда $G = G^\perp$ □

3.8 Бинарные CRC-коды

Определение 3.18. CRC-код — это циклический код, используемый для *обнаружения* ошибок. Пусть порождающий многочлен нашего кода — $g(x)$. Тогда будем производить кодирование по правилу

$$c(x) = x^k m(x) + (x^k m(x) \mod g(x)$$

Будем проверять наличие ошибок в $\bar{c}(x)$ следующим образом:

$$\begin{cases} \text{ошибка} & \text{если } \bar{c}(x) \neq 0 \\ \text{принимаем} & \text{если } \bar{c}(x) = 0 \end{cases}$$

Обозначим $e(x) = \bar{c}(x) + c(x)$.

Замечание 3.6. В одну сторону наша проверка корректна, если ошибки нет, то мы точно примем вектор. Но мы можем принять и вектор с ошибкой.

Определение 3.19. Вектор ошибок содержит пакет ошибок длины B, если расстояние между первой и поледней ошибкой равно B, то есть, существует i, такое, что

$$e(x) = x^i(1 + e_1 x + \ldots + x^{B-1})$$

Утверждение 3.6. *Верны следующие утверждения*

1. *Ошибка $e(x) = x^i$ для $i \in \{0,\ldots,n-1\}$ будет найдена*
2. *Если $g(x) = (1+x)\bar{g}(x)$, то $\forall e(x) \colon w(e) \mod 2 = 1$ будет найдена*
3. *Если $e(x)$ содержит пакет ошибок длины $n-k$, то такая ошибка будет найдена*
4. *Если $e(x)$ содержит пакет ошибок длины $n-k+1$, то она не будет найдена только если $e(x) = x^i g(x)$*
5. *Вероятность, что ошибка с блоком длины $l > n-k+1$ не будет найдена равна 2^{k-n}*

Доказательство. 1. $g(x) = 1 + \ldots + x^r$. $r > 0$. Рассмотрим произвольный многочлен $a(x) = x^{d_l} + \ldots + x^{d_r}$. Тогда $g(x)a(x) = x^{d_l} + \ldots + x^{r+d_r}$. Следовательно, так как $d_l < r + d_r$, x^i не может делиться на $g(x)$

2. $$c(x) = (1+x)\bar{g}(x)m(x) = (1+x)\Big(\sum_{i=0}^{n-2} t_i x^i\Big) = t_0 + x(t_0+t_1) + \ldots + t_{n-2}x^{n-1}$$

   Посчитаем сумму коэффициентов: $t_0 + (t_0+t_1) + (t_1+t_2) + \ldots + t_{n-2} = 2(\sum_{i=0}^{n-2} t_i) = 0$. То есть, если ошибка содержит нечетное число единиц, то она не поделится на $g(x)$

3. Пусть $e(x)$ содержит пакет ошибок длины $n-k$. Тогда

   $$e(x) = x^i(1 + e_1 x + \ldots + x^{n-k-1})$$

   $i \in \{0, \ldots, k\}$. Пусть $e(x) = f(x)g(x)$.

   $$deg(f) = deg(e) - deg(g) = (i + n - k - 1) - (n-k) = i - 1$$

   Тогда вспомним, что g не кратно x^j ни для каких j. Таким образом f кратно x^i, но $deg(f) < i$. Значит, $e(x)$ не делится на $g(x)$ и мы обнаружим такую ошибку.

4. Если $e(x) = x^i(1 + e_1 x + \ldots + x^{n-k})$, тогда ошибка может не распознаться только если $e(x) = x^i g(x)$

5. Пусть $e(x)$ содержит пакет ошибок длины $l > n-k+1$. Тогда можем записать $e(x) = x^i a(x)g(x)$, опять исходя из факта, что g не кратно x^j для всех $j > 0$. Тогда $deg(a) = l - (n-k) - 1$ и свободный член a равен 1. Тогда возможных вариантов выбора a существует $2^{l-n+k-2}$.

   Будем считать e равномерно распределенным по всем возможным ошибкам с блоком длины l. Тогда вероятность того, что такая ошибка поделится на $g(x)$ равна

   $$\frac{\overbrace{(n-l+1)}^{\text{выбор } i} 2^{l-n+k-2}}{2^{l-2}(n-l+1)} = 2^{k-n}$$

□

Глава 4

Регистры сдвига и линейная сложность

4.1 Регистры сдвига с линейной обратной связью

Хотим генерировать поток битов из некоторого начального конечного количества. Рассмотрим следующий алгоритм:

Алгоритм 4.1. Имеем $s_0, s_1, \ldots, s_{l-1}$, где l будем называть длиной регистра сдвига. Пусть $f : \{0,1\}^l \to \{0,1\}$. Тогда будем генерировать дальнейшие биты по рекуррентному соотношению $s_i = f(s_{i-1}, s_{i-2}, \ldots, s_{i-l})$.

f будем называть функцией обратной связи.
s_i — выход регистра на шаге i.

Рассмотрим регистр сдвига с линейной функцией обратной связи (РСЛОС)

Определение 4.1. Если $f(x_0, \ldots, x_{l-1}) = \sum\limits_{i=0}^{l-1} c_i x_i$, то многочлен, ассоциированный с РСЛОС: $c(x) = 1 + c_0 x + \ldots + c_{l-1} x^l$.

Определение 4.2. Периодом регистра называется число $\min\{N \in \mathbb{N} \colon \forall i \geq N\; S_{N+i} = S_i\}$

Свойства:

1. $s_0 = \ldots = s_{l-1} = 0 \implies \forall i \colon s_i = 0$
2. Период регистра конечен.

   Доказательство. Если
   $$\begin{cases} s_i & = s_j \\ s_{i+1} & = s_{j+1} \\ \ldots & \ldots \\ s_{i+l-1} & = s_{j+l-1} \end{cases}$$
   То $s_{i+l} = s_{j+l}$ по определению. Тогда $\forall k \geq 0 \colon s_{i+k} = sj + k$. Таким образом $(s_i, s_{i+1}, \ldots) = (s_j, s_{j+1}, \ldots)$. Но тогда существует не более 2^l различных типов таких последовательностей.

   □

3. $T \leq 2^l - 1$. Непосредственно следует из доказательства предыдущего пункта.
4. $c_{l-1} = 0 \implies$ период начинается не с начала последовательности (c_T не всегда равно c_0)
5. $c_{l-1} = 1 \implies c_T = c_0$
6. $c(x)$ неприводим над $\mathbb{F}_2 \implies 2^l - 1$ кратно T
7. $c(x)$ примитивный над $\mathbb{F}_2 \implies T = 2^l - 1$

Утверждение 4.1. *Пусть известны $s_i, \ldots, s_{i+2l-1}$ и известно, что регистр имеет длину l. Тогда можно найти регистр сдвига, порождающий такую последовательность.*

Доказательство. Составим систему уравнений, относительно c_i:

$$\begin{cases} s_{i+l} &= c_0 s_{i+l-1} + c_1 s_{i+l-2} + \ldots + c_{l-1} s_0 \\ s_{i+l+1} &= c_0 s_{i+l} + c_1 s_{i+l-1} + \ldots + c_{l-1} s_1 \\ \ldots &= \ldots \\ s_{i+2l-1} &= c_0 s_{i+2l-2} + c_1 s_{i+2l-3} + \ldots + c_{l-1} s_{i+l-1} \end{cases}$$

Система совместна по построению s_i, тогда решение — подходящий регистр сдвига. Если уранения линейно-независимы, регистр сдвига определяется однозначно. □

4.2 Линейная сложность, алгоритм Берлекэмпа-Мэсси

Определение 4.3. Регистр сдвига порождает последовательность s, если для начальных значений $s_0, \ldots, s_{l-1}$ регистр выдает последовательность s.

Определение 4.4. Линейной сложностью последовательности бит (конечной или бесконечной) s назовем

- 0, если $s = (0, 0, \ldots)$
- ∞, если $\nexists$ РСЛОС, порождающего s.
- Длина минимального регистра сдвига, порождающего s.

Обозначим $L(s)$.

Определение 4.5. Пусть s — последовательность бит. Тогда пусть

$$L_N = L(s_0, \ldots, s_{N-1})$$

Последовательность $L_1, L_2, \ldots$ назовем профилем линейной сложности последовательности s.

Утверждение 4.2. *Верны следующие утверждения*

1. $j > i \implies L_j \geq L_i$
2. $L_N \leq \frac{N}{2} \implies L_{N+1} > L_N$
3. $L_{N+1} > L_N \implies L_N + L_{N+1} = N + 1$

Сам алгоритм базируется на этих трех утверждениях. *[Можно его дописать сюда].*

4.3 Порождение симплексного кода с помощью регистра сдвига

Определение 4.6. Рассмотрим C_m, $(2^m - 1, 2^m - m - 1)$-код Хэмминга. Дуальный к нему код S_m является кодом Адамара с матрицей Сильвестра — симплексным кодом.

Замечание 4.1. S_m является циклическим кодом с проверочным многочленом

$$h(x) = 1 + h_1 x + \ldots + h_{m-1} x^{m-1} + x^m$$

Тогда, вспоминая структуру проверочной матрицы циклического кода, можем записать условия на то, что $(s_0, \ldots, s_{2^m-2}) \in S_m$:

$$\forall i \in \{0, \ldots 2^m - 2 - m\} \colon s_{i+m} = s_i + s_{i+1} h_{m-1} + \ldots + s_{i+m-1} h_1$$

Тогда каждое кодовое слово $s \in S_m$ порождается регистром сдвига с характеристическим многочленом $h(x)$ и начальными входами $s_0, \ldots, s_{m-1}$.

Глава 5

Булевы функции

5.1 Определения. Алгебраическая нормальная форма

5.1.1 Алгебраическая нормальная форма

Определение 5.1. Функция $f : \{0,1\}^m \to \{0,1\}$ называется булевой функцией

Мы поймем, что *любую* булеву функцию можно представить в виде многочлена от m переменных в $\mathbb{F}_2$ и даже выведем явную формулу.

С помощью таблицы истинности можно легко заметить, что для любой булевой функции f верно

$$f(v_1, \ldots, v_m) = \bigvee_{i_1,\ldots,i_m \in \{0,1\}} f(i_1, \ldots, i_m)(w_1^{i_1} \wedge \ldots \wedge w_m^{i_m})$$

Где $w_i^1 = v_i$ и $w_i^0 = \neg v_i$.

Это просто функция в дизъюнктивной нормальной форме.

Определение 5.2. Будем обозначать $x \le y$ для $x, y \in \{0,1\}^n$, если $x_i \le y_i$ для всех $i \in \{1, \ldots, n\}$

Теорема 5.1. *Любая булева функция f может быть записана как*

$$f(v_1, \ldots, v_m) = \sum_{a \in \{0,1\}^m} g(a) v_1^{a_1} \ldots, v_m^{a_m}$$

где $g(a) = \sum_{b \le a} f(b_1, \ldots, b_m)$

Здесь и далее, если не указано иное, все суммы в $\mathbb{F}_2$

Доказательство. Зафиксируем набор значений $v_1, \ldots, v_m$ и проверим, что получается то, что нужно. Пусть $A = \{i \colon v_i = 1\} = \{\alpha_1, \ldots, \alpha_k\}$; $B = \{i \colon v_i = 0\}$.

Во-первых, можно выбросить слагаемые, где $a_i = 1$ для $i \in B$, так как они обращаются в ноль.

$$\sum_{a \le \mathbf{1}_A} g(a) v_1^{a_1} \ldots, v_m^{a_m} = \sum_{a \le \mathbf{1}_A} g(a)$$

Здесь $\mathbf{1}_A$ — характеристический вектор A, он равен $(v_1, \ldots, v_m)$.

Так как во всех остальных слагаемых $v_1^{a_1} \ldots, v_m^{a_m} = 1$. Тогда, подставляя $g(a)$, получаем

$$= \sum_{a \le \mathbf{1}_A} \sum_{b \le a} f(b_1, \ldots, b_m)$$

Давайте поймем, сколько раз каждое слагаемое входит в сумму:

$$= \sum_{b \le \mathbf{1}_A} \sum_{\mathbf{1}_A \ge a \ge b} f(b_1, \ldots, b_m)$$

Осталость посчитать сколько бывает таких a. Легко видеть, что их количество равно $2^{w(a)-w(b)}$ и тогда все слагаемые, кроме $b = \mathbf{1}_A = (v_1, \dots v_m)$ по четности обращаются в ноль

$$= f(v_1, v_2, \dots, v_m)$$

$\square$

Определение 5.3. Представление

$$f(v_1, \dots, v_m) = \sum_{a \in \{0,1\}^m} g(a) v_1^{a_1} \dots, v_m^{a_m}$$

называется *алгебраической нормальной формой* функции f.

5.1.2 Быстрое преобразование Мёбиуса

Определение 5.4. Пусть $f \in \{0,1\}^{2^n}$. Поставим вектору f в соответствие будеву функцию $\in \mathrm{Map}(\{0,1\}^n, \{0,1\})$ следующим образом

$$f \mapsto (\underbrace{x}_{\in\{0,1\}^n} \mapsto f_x)$$

где f_x — компонента вектора f с номером, соответствующим двоичной записи x. Мы будем отождествлять вектор f и соответствующую ему функцию и записывать $f(x) = f_x$.

Отображение $\mu : \{0,1\}^{2^n} \to \{0,1\}^{2^n}$ называется *преобразованием Мёбиуса*, если выполнено:

$$f \mapsto g \iff \forall a \colon g(a) = \bigoplus_{b \le a} f(b)$$

Вычисление преобразования Мёбиуса по определению требует 3^n операций (это количество пар $x, y \in \{0,1\}^n : x \le y$). Но можно выполнить его оптимальнее, используя $2^n \cdot n$ операций.

Действительно, рассмотрим f и $g = \mu(f)$.

$$g(a_1, \dots, a_n) = \bigoplus_{b \le a} f(b_1, \dots, b_n) = \bigoplus_{\substack{b \le a \\ b_1 = 0}} f(b_1, \dots, b_n) \oplus \bigoplus_{\substack{b \le a \\ b_1 = 1}} f(b_1, \dots, b_n)$$

Теперь разберем два случая: $a_1 = 0$ и $a_1 = 1$:

$$g(0, a_2, \dots, a_n) = \bigoplus_{\substack{b \le a \\ b_1 = 0}} f(b_1, \dots, b_n)$$

в этом случае второе слагаемое обращается в ноль, поскольку $b_1 = 1 \implies b \nleq a$.

$$g(1, a_2, \dots, a_n) = \bigoplus_{\substack{b \le a \\ b_1 = 0}} f(b_1, \dots, b_n) \oplus \bigoplus_{\substack{b \le a \\ b_1 = 1}} f(b_1, \dots, b_n)$$

Заметим, что теперь в обоих случаях условие $b \le a \iff (b_2, \dots, b_n) \le (a_2, \dots, a_n)$. Это дает нам возможность рассмотреть функции $f_0(a') = f(0, a'_1, \dots, a'_{n-1})$ и $f_1(a') = f(0, a'_1, \dots, a'_{n-1})$ и, используя прошлые рассуждения, записать

$$g(0, a_2, \dots, a_n) = \mu(f_0)(a_2, \dots, a_n)$$

и

$$g(1, a_2, \dots, a_n) = \mu(f_0)(a_2, \dots, a_n) \oplus \mu(f_1)(a_2, \dots, a_n))$$

Таким образом, мы свели задачу нахождения преобразования Мёбиуса для вектора из $\{0,1\}^{2^n}$ к двум задачам нахождения преобразования Мёбиуса для вектора из $\{0,1\}^{2^{n-1}}$ тогда время работы нашего алгоритма равно $T(n) = 2^n + 2T(n-1)$. Из этого соотношения легко видеть, что $T(n) = 2^n \cdot n$.

5.2 Коды Рида-Маллера

Определение 5.5. Для произвольного $r \in \{0, \dots, m\}$ двоичный код Рида-Маллера $\mathscr{R}(r, m)$ порядка r и длины 2^m определяется как

$$Lin\{v_{\alpha_1} \cdot \ldots \cdot v_{\alpha_p} : p \leq r;\ 1 \leq \alpha_i \leq m\}$$

то есть линейная оболочка мономов степени $\leq r$ или, что то же самое, множество всех многочленов от m переменных над $\mathbb{F}_2$ степени не больше r.

Собственно кодами будут характеристические векторы этих многочленов.

Очевидно, что этот код является линейным. Значит, можно говорить о его размерности.

Замечание 5.1. Размерность $\mathscr{R}(r, m)$ равна $\sum\limits_{k=0}^{r} C_m^k$

Доказательство. Из теоремы 5.1 все мономы линейно независимы, а количество мономов степени $\leq r$ равно $\sum\limits_{k=0}^{r} C_m^k$ □

5.2.1 Взаимосвязь кодов Рида-Маллера разных порядков

Теорема 5.2.

$$\mathscr{R}(r+1, m+1) = \{|u|u+v| : u \in \mathscr{R}(r+1, m),\ v \in \mathscr{R}(r, m)\}$$

Здесь $|x|y|$ — конкатенация x и y

Лемма 5.1. *Пусть $f(v_1, \dots, v_m)$ — булева функция с характеристическим вектором ϕ. Тогда характеристические векторы функций $g(v_1, \dots, v_{m+1}) = f(v_1, \dots, v_m)$ и $h(v_1, \dots, v_{m+1}) = v_{m+1} f(v_1, \dots, v_m)$ равны, соответственно $|\phi|\phi|$ и $|\mathbf{0}|\phi|$*

Доказательство. Здесь $m+1$ считается старшей степенью. Тогда левой части соответствуют те значения переменных где $v_{m+1} = 0$, а правой — те, где $v_{m+1} =$. Тогда в обеих частях характеристического вектора f будет вектор ϕ. Левой части характеристического вектора h будет соответствовать тождественный 0, поскольку мы умножили на 0. □

Доказательство. Рассмотрим $f \in \mathscr{R}(r+1, m+1)$. Давайте запишем

$$f(v_1, \dots, v_{m+1}) = \underbrace{g(v_1, \dots, v_m)}_{deg \leq r+1} + v_{m+1} \underbrace{h(v_1, \dots, v_m)}_{deg \leq r}$$

Вспомним лемму и заметим, что характеристические векторы слагаемых этой формулы равны $|\mathbf{1}_g|\mathbf{1}_g|$ и $|\mathbf{0}|\mathbf{1}_h|$ соответственно. Тогда характеристический вектор их суммы равен $|\mathbf{1}_g|\mathbf{1}_g + \mathbf{1}_h|$. □

Замечание 5.2. Похоже на формулу для биномиальных коэффициентов.

Теперь мы готовы к тому, чтобы найти расстояние между кодовыми словами в коде Рида-Маллера.

Теорема 5.3. *Минимальное расстояние между словами в коде $\mathscr{R}(r, m)$ равно 2^{m-r}*

Доказательство. Индукция по m. При $m = 0$ существует один код Рида Миллера: $\mathscr{R}(0, 0)$. Он состоит из слов 0 и 1, расстояние между ними равно 1.

Пусть для всех $m < m_0$ доказано, докажем для m_0. Из прошлой теоремы $\mathscr{R}(r, m) = \mathscr{R}(r, m-1) + \mathscr{R}(r-1, m-1)$. Рассмотрим $a_1, a_2 \in \mathscr{R}(r, m)$. Они имеют вид $|u_1|u_1 + v_1|$ и $|u_2|u_2 + v_2|$ соответственно. Тогда

$$d(a_1, a_2) = d(u_1, u_2) + d(u_1 + v_1, u_2 + v_2) \geq d(u_1, u_2) + |\underbrace{d(u_1, u_2)}_{\geq 2^{m-r-1}} - \underbrace{d(v_1, v_2)}_{\geq 2^{m-r}}|$$

Поймём, что это неравенство действительно верно (здесь сумма вещественных чисел):

$$d(u_1 + v_1, u_2 + v_2) = \sum_{i=1}^{2^m} d_i(u_1 + v_1, u_2 + v_2)$$

где $d_i(x, y) = 1$, если i-е символы x и y различаются и 0, если совпадают. Теперь разбором случаев можно доказать, что $d_i(a + b, c + d) \leq |d_i(a, c) - d_i(b, d)|$:

a	b	c	d	$d_i(a+b,c+d)$	$d_i(a,c)$	$d_i(b,d)$	$\|\dots\|$
0	0	0	0	0	0	0	0
0	0	0	1	1	0	1	1
0	0	1	0	1	1	0	1
0	0	1	1	0	1	1	0

Здесь можно считать $a = b = 0$, так как иначе можно перейти к $a \to a + a$; $b \to b + b$; $c \to c + a$; $d \to d + b$, не изменив обе части формулы и обратив a, b в ноль. Таким образом можем записать

$$\sum_{i=1}^{2^m} d_i(u_1+v_1, u_2+v_2) \le \sum_{i=1}^{2^m} |d_i(u_1,u_2) - d_i(v_1,v_2)| \le |\sum_{i=1}^{2^m} \big(d_i(u_1,u_2) - d_i(v_1,v_2)\big)| = |d(u_1,u_2) - d(v_1,v_2)|$$

Теперь нужно разобрать два случая:

- $d(u_1,u_2) \ge d(v_1,v_2)$. Тогда $d(a_1,a_2) \ge 2^{m-r} + |\dots| \ge 2^{m-r}$
- $d(v_1,v_2) > d(u_1,u_2)$. Тогда $d(a_1,a_2) \ge d(u_1,u_2) + d(v_1,v_2) - d(u_1,u_2) = d(v_1,v_2) \ge 2^{m-r}$

$\square$

5.2.2 Выколотые коды Рида-Маллера

Определение 5.6. Для произвольного $r \in \{0, \dots, m-1\}$ **выколотый** двоичный код Рида-Маллера $\mathscr{R}^*(r,m)$ порядка r и длины 2^m определяется как

$$\{x_1 x_2 \dots x_{2^m-1} \colon x \in \mathscr{R}(r,m)\}$$

то есть, получается из $\mathscr{R}(r,m)$ вычеркиванием элемента вектора, соответствующего $v_1 = \dots = v_m = 0$

Очевидно, что $\mathscr{R}^*(r,m)$ имеет длину $2^m - 1$, минимальное расстояние $2^{m-r} - 1$.

Утверждение 5.1. *Для $r < m$ верно $dim(\mathscr{R}^*(r,m)) = \sum\limits_{k=0}^{r} C_m^k$*

Доказательство. То есть, нужно доказать, что размерность равна размерности кода до выкалывания. Заметим, что по лемме о рандомизации, в каждой строке порождающей матрицы четное количество единиц (так как $r < m$ и строки, соответствующей $v_1 \cdot \ldots \cdot v_m$, где только одна единица, в матрице нет).

Тогда сложим все столбцы, кроме первого, и получим столбец вида $(1, 0, \dots, 0)^T$.

Таким образом, размерность линейной оболочки всех столбцов $\mathscr{R}(r,m)$ равна размерности линейной оболочки всех столбцов, кроме первого, то есть $dim(\mathscr{R}^*(r,m))$ $\square$

5.2.3 Декодирование кода $\mathscr{R}(1,m)$

Рассмотрим на примере $m = 3$. Порождающая матрица $\mathscr{R}(1,m)$ будет иметь размер $(m+1) \times 2^m$ и будет состоять из векторов $\mathbf{1}, \mathbf{1}_{x_1}, \mathbf{1}_{x_2}, \mathbf{1}_{x_3}$:

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Кодирование, как и в любом линейном коде — домножение кодируемой строки на порождающую матрицу.

Все возможные 16 кодов получаются линейными комбинациями строк матрицы:

$$A = \mathscr{R}(1,3) = \begin{pmatrix} 0&0&0&0&0&0&0&0\\ 1&1&1&1&1&1&1&1\\ 0&1&0&1&0&1&0&1\\ 1&0&1&0&1&0&1&0\\ 0&0&1&1&0&0&1&1\\ 1&1&0&0&1&1&0&0\\ 0&1&1&0&0&1&1&0\\ 1&0&0&1&1&0&0&1\\ 0&0&0&0&1&1&1&1\\ 1&1&1&1&0&0&0&0\\ 0&1&0&1&1&0&1&0\\ 1&0&1&0&0&1&0&1\\ 0&0&1&1&1&1&0&0\\ 1&1&0&0&0&0&1&1\\ 0&1&1&0&1&0&0&1\\ 1&0&0&1&0&1&1&0 \end{pmatrix}$$

Закодируем какое-нибудь слово. Например $y = (1,0,0,1)$. $z = yG = (1,1,1,1,0,0,0,0)$. Кодовое расстояние равно $2^{3-1} = 4$. Поэтому код способен исправить только одну ошибку. Тогда пусть $z' = (0,1,1,1,0,0,0,0)$. Преобразуем матрицу A так, чтобы можно посчитать расстояния от декодируемого вектора до всех кодовых слов. $H_{ij} = 2A_{ij} - 1$. Можно заметить, что H — это две матрицы Адамара, поставленные друг на друга. Преобразуем z' тем же образом: $z''_i = 2z'_i - 1$.

Рассмотрим $H(z'')^T$. i-й компонент этого вектора равен $(2^m - d(H_i, z')) - d(H_i, z') = 2^m - 2d(H_i, z')$. Тогда вектор с минимальным расстоянием соответствует максимуму среди компонент $H(z'')^T$.

$$H = \begin{pmatrix} -1&-1&-1&-1&-1&-1&-1&-1\\ 1&1&1&1&1&1&1&1\\ -1&1&-1&1&-1&1&-1&1\\ 1&-1&1&-1&1&-1&1&-1\\ -1&-1&1&1&-1&-1&1&1\\ 1&1&-1&-1&1&1&-1&-1\\ -1&1&1&-1&-1&1&1&-1\\ 1&-1&-1&1&1&-1&-1&1\\ -1&-1&-1&-1&1&1&1&1\\ 1&1&1&1&-1&-1&-1&-1\\ -1&1&-1&1&1&-1&1&-1\\ 1&-1&1&-1&-1&1&-1&1\\ -1&-1&1&1&1&1&-1&-1\\ 1&1&-1&-1&-1&-1&1&1\\ -1&1&1&-1&1&-1&-1&1\\ 1&-1&-1&1&-1&1&1&-1 \end{pmatrix}$$

Тогда

$$H(z'')^T = (2, -2, 2, -2, 2, -2, 2, -2, -6, 6, 2, -2, 2, -2, 2, -2)^T$$

Максимальная компонента соответсвтует 10-й строке матрицы, а это и есть вектор $(1,1,1,1,0,0,0,0)$, который мы шифровали.

5.3 Преобразование Фурье и Уолша-Адамара для булевых функций

Определение 5.7. *Экспонента* булевой функцииexp $f(x) = (-1)^{f(x)}$

Т.е. $\exp f : V_n \xrightarrow{f} \{0,1\} \longrightarrow \{-1,1\}$

Определение 5.8. *Дискретная функция Уолша*

$$v(a,x) : = (-1)^{\langle a,x \rangle}, \; a, x \in V_n$$

$$v : \{0,1\}^n \times \{0,1\}^n \longrightarrow \{1,-1\}$$

На a и x мы смотрим одновременно и как на двоичные векторы из $\{0,1\}^n$, и как на целые числа, двоичная запись которых, дополненная при необходимости слева нулями, совпадает с этими векторами.

Свойства функции Уолша:

1. $v(a,x) = v(x,a)$
2. $|v(a,x)| = 1$
3. $v(0,x) = v(x,0) = 1$
4. E линейное подпространство $\{0,1\}^n$
   $a \notin E^{\perp}$
   Тогда
   $$\sum_{x \in E} v(a,x) = 0$$

   Доказательство. $E_0 := \{x \in E : \langle a,x \rangle = 0\}, E_1 := \{x \in E : \langle a,x \rangle = 1\}$

   Покажем, что $|E_0| = |E_1|$, тогда число +1 и -1 в сумме будет одинаково.

   $a \notin E^{\perp} \Rightarrow \exists x \in E : \langle a,x \rangle \neq 0 \Rightarrow E_1 \neq \emptyset$ $\left(E^{\perp} = \{u \in \{0,1\}^n : \langle u,x \rangle = 0, \forall x \in E\}\right)$

   Пусть $y \in E_1$. Рассмотрим равенство $x + y = z$. Скалярно домножив на a получим
   $$\langle a,x \rangle + \underbrace{\langle a,y \rangle}_{1} = \langle a,z \rangle$$

   То есть если $x \in E_1$, то $z \in E_0$. И наоборот, если $x \in E_0$, то $z \in E_1$. Отсюда легко видеть, что, прибавляя y ко всем элементам E_1, получим элементы E_0. Значит, $E_1 + y \subset E_0 \Rightarrow |E_1| \leq |E_0|$. Так же прибавляя y ко всем элементам E_0, получим элементы E_1. Значит, $E_0 + y \subset E_1 \Rightarrow |E_0| \leq |E_1|$. □

Следствие 5.1. *Т.к.* $\{0,1\}^{n\perp} = \{0\}$,
$$\sum_{x \in \{0,1\}^n} v(a,x) = \delta_0(a)\, 2^n$$
где
$$\delta_0(a) = \begin{cases} 1, & \textit{если } a = 0 \\ 0, & \textit{если } a \neq 0 \end{cases}$$

Определение 5.9. *Преобразованием Фурье* булевой функции f называется целочисленная функция на $\{0,1\}^n$, определяемая следующим равенством
$$F_f(u) = \sum_{x \in \{0,1\}^n} f(x)\, v(x,u)$$

Для каждого $u \in \{0,1\}^n$ значение $F_f(u)$ называется *коэффициентом Фурье.*

Определение 5.10. *Преобразованием Уолша-Адамара* булевой функции f называется целочисленная функция на $\{0,1\}^n$, определяемая следующим равенством
$$W_f(u) = F_f(\exp f(u)) = \sum_{x \in \{0,1\}^n} \exp f(x)\, v(x,u) =$$
$$= \sum_{x \in \{0,1\}^n} (-1)^{f(x)} (-1)^{\langle x,u \rangle} = \sum_{x \in \{0,1\}^n} (-1)^{f(x) \oplus \langle x,u \rangle} =$$
$$= \sum_{x \in \{0,1\}^n} \exp\left(f(x) \oplus \langle x,u \rangle\right)$$

Для каждого $u \in \{0,1\}^n$ значение $W_f(u)$ называется *коэффициентом Уолша-Адамара.*

Уолш: от функции Уолша.

Адамар: функцию Уолша можно получить из матрицы Адамара. Рекурсивно умеем формировать матрицы Адамара размера 2^n (мы полученные таким спобом матрицы матрицами Сильвестра).

$$H_{new} = \begin{bmatrix} H & H \\ H & -H \end{bmatrix}$$

Тогда строчки — функции Уолша. То есть x соответствует номеру столбца, a соответствует номеру строки. Элемент $H_{a,x} = v(a, x)$.

Пример 5.1.

$$H_4 = \left[\begin{array}{r|cccc} & \underline{x_1 = 00} & \underline{x_2 = 01} & \underline{x_3 = 10} & \underline{x_4 = 11} \\ a_1 = 00 & 1 & 1 & 1 & 1 \\ a_2 = 01 & 1 & -1 & 1 & -1 \\ a_3 = 10 & 1 & 1 & -1 & -1 \\ a_4 = 11 & 1 & -1 & -1 & 1 \end{array}\right]$$

Определение 5.11. Часто коэффициенты Фурье и коэффициенты Уолша-Адамара называются *спектральными коэффициентами.*

Теорема 5.4. *Коэффициенты Фурье и Уолша-Адамара связаны соотношением*

$$W_f(u) = 2^n \delta_0(u) - 2F_f(u)$$

Доказательство.

$$W_f(u) = \sum_{x \in \{0,1\}^n} \exp f(x)\, v(x, u) = \sum_{x \in \operatorname{Supp} f} \underbrace{\exp \underbrace{f(x)}_{1}}_{-1} v(x, u) + \sum_{x \in \{0,1\}^n \setminus \operatorname{Supp} f} \underbrace{\exp \underbrace{f(x)}_{0}}_{1} v(x, u) =$$

$$= - \sum_{x \in \operatorname{Supp} f} v(x, u) + \sum_{x \in \{0,1\}^n \setminus \operatorname{Supp} f} v(x, u)$$

По замечанию к 4-ому свойству

$$\sum_{x \in \{0,1\}^n} v(a, x) = \delta_0(a)\, 2^n$$

$$\sum_{x \in \{0,1\}^n \setminus \operatorname{Supp} f} v(x, u) = \underbrace{\sum_{x \in \{0,1\}^n} v(x, u)}_{=\delta_0(u)2^n} - \sum_{x \in \operatorname{Supp} f} v(x, u)$$

Кроме того

$$F_f(u) = \sum_{x \in \{0,1\}^n} f(x)\, v(u, x) = \sum_{x \in \operatorname{Supp} f} v(u, x)$$

Итого

$$W_f(u) = \delta_0(u)\, 2^n - 2 \sum_{x \in \operatorname{Supp} f} v(x, u) = \delta_0(u)\, 2^n - 2F_f(u)$$

$\square$

Теорема 5.5 (формула обращения)**.** *Для преобразования Уолша-Адамара справедлива формула обращения.*

$$\exp f(x) = 2^{-n} \sum_{u \in \{0,1\}^n} W_f(u)\, v(x, u)$$

Доказательство.

$$2^{-n} \sum_{u \in \{0,1\}^n} W_f(u)\, v(x, u) = 2^{-n} \sum_{u \in \{0,1\}^n} \sum_{y \in \{0,1\}^n} (-1)^{f(y)} \underbrace{(-1)^{\langle y,u \rangle} (-1)^{\langle x,u \rangle}}_{(-1)^{\langle x \oplus y, u \rangle} = v(x \oplus y, u)} =$$

$$= 2^{-n} \sum_{y\in\{0,1\}^n} (-1)^{f(y)} \sum_{u\in\{0,1\}^n} v\left(x \oplus y, u\right) =$$

$$\sum_{u\in\{0,1\}^n} v\left(x \oplus y, u\right) = \begin{cases} 2^n, & x \oplus y = 0 \\ 0, & x \oplus y \neq 0 \end{cases}$$

Т.е. от всех сумм останется только одно слагаемое при $y = x$

$$= 2^{-n} \left(-1\right)^{f(x)} 2^n = \exp f\left(x\right)$$

□

Таким образом, коэффициенты Уолша-Адамара однозначно определяют булеву функцию. Вместе с тем, не любой набор из 2^n чисел может быть набором коэффициентов Уолша-Адамара некоторой булевой функции.

Задачи 2.38, 2.39.

Теорема 5.6 (равенство Парсеваля)**.** *Коэффициенты Уолша-Адамара удовлетворяют соотношению:*

$$\sum_{u\in\{0,1\}^n} W_f^2\left(u\right) = 2^{2n}$$

Доказательство.

$$\sum_{u\in\{0,1\}^n} W_f^2\left(u\right) = \sum_{u\in\{0,1\}^n} \left(\sum_{x\in\{0,1\}^n} (-1)^{f(x)\oplus\langle x,u\rangle} \right)^2 = \sum_{u\in\{0,1\}^n} \left(\sum_{x\in\{0,1\}^n} (-1)^{f(x)\oplus\langle x,u\rangle} \right) \left(\sum_{y\in\{0,1\}^n} (-1)^{f(y)\oplus\langle y,u\rangle} \right) =$$

$$= \sum_{u\in\{0,1\}^n} \sum_{x,y\in\{0,1\}^n} (-1)^{f(x)\oplus\langle x,u\rangle\oplus f(y)\oplus\langle y,u\rangle} = \sum_{x,y\in\{0,1\}^n} (-1)^{f(x)\oplus f(y)} \underbrace{\sum_{u\in\{0,1\}^n} (-1)^{\langle x\oplus y,u\rangle}}_{=0,\text{ при } x\neq y} = \sum_{x\in\{0,1\}^n} \sum_{x\in\{0,1\}^n} (-1)^{\overbrace{f\left(x\right)\oplus f\left(x\right)}^{0}} =$$

$$= 2^{2n}$$

□

Утверждение 5.2. *Коэффициенты алгебраический нормальной формы $g_f\left(u\right)$ выражаются через коэффициенты Уолша-Адамара следующим образом:*

$$g_f\left(u\right) = 2^{wt(u)-1} - 2^{wt(u)-n-1} \sum_{\alpha\preccurlyeq u\oplus 1} W_f\left(\alpha\right)$$

Доказательство. Подставим формулу для коэффициентов Уолша-Адамара:

$$g_f(u) = 2^{wt(u)-1} - 2^{wt(u)-n-1} \sum_{\alpha\leq u\oplus\mathbf{1}} \sum_{x\in\{0,1\}^n} \exp(f(x)\oplus\langle x,\alpha\rangle) = 2^{wt(u)-1} - 2^{wt(u)-n-1} \sum_{x\in\{0,1\}^n} \exp(f(x)) \sum_{\alpha\leq u\oplus\mathbf{1}} \exp(\langle x,\alpha\rangle)$$

Величина $\sum\limits_{\alpha\leq u\oplus\mathbf{1}} \exp(\langle x,\alpha\rangle)$ обращается в 0 при x не ортогональном $\{y \leq u \oplus \mathbf{1}\}$ и равна $2^{n-wt(u)}$ при $x \perp \{y \leq u \oplus \mathbf{1}\} \iff x \in \{y \leq u\}$.

$$= 2^{wt(u)-1} - 2^{wt(u)-n-1} \sum_{x\leq u} \exp(f(x)) 2^{n-wt(u)} = \frac{1}{2} 2^{wt(u)} - \frac{1}{2} \sum_{x\leq u} \exp(f(x)) = \frac{1}{2} \sum_{x\leq u} \underbrace{(1 - \exp(f(x)))}_{=2f(x)} = \sum_{x\leq u} f(x)$$

□

5.4 Быстрое вычисление коэффициентов Уолша-Адамара

Коэффициенты Уолша-Адамара — это коэффициенты Фурье для функции $\exp f$, поэтому достаточно научиться вычислять коэффициенты Фурье. Будем действовать аналогично вычислению преобразования Мёбиуса. Пусть $u \in \{0,1\}^n$. Обозначим $u' = (u_2, \dots, u_n)$, аналогично для $x \in \{0,1\}^n$ обозначим $x' = (x_2, \dots, x_n)$

$$F_f(u) = \sum_{x \in \{0,1\}^n} f(x_1, x') \exp(x_1 v_1 + \langle x', u' \rangle) = \sum_{x \in \{0,1\}^{n-1}} f(0,x) \exp(\langle x, u' \rangle) + f(1,x) \exp(u_1) \exp(\langle x, u' \rangle)$$

Пусть $f_0(x) = f(0,x)$ и $f_1(x) = f(1,x)$, тогда

$$F_f(u) = F_{f_0}(u') + \exp u_1 F_{f_1}(u')$$

Таким образом, мы свели задачу преобразования Фурье для вектора $\in \{0,1\}^{2^n}$ к задаче вычисления преобразования Фурье для двух векторов из $\{0,1\}^{2^{n-1}}$. Аналогично вычислению преобразования Мёбиуса, имеем время работы $T(n) = 2^n + 2T(n-1) = 2^n \cdot n$

5.5 Производная булевой функции по направлению

Определение 5.12. Производной булевой функции f по направлению $u \in \{0,1\}^n$ называется булева функция

$$D_u f(x) = f(x \oplus u) \oplus f(x)$$

Определение 5.13. Производной булевой функции f по направлению подпространства $L \subset \{0,1\}^n$ называется функция

$$D_u f(x) = \bigoplus_{u \in F} f(x \oplus u)$$

Замечание 5.1. Если $L = \langle u_1, \dots, u_k \rangle$, то $D_L f = D_{u_k} D_{u_{k-1}} \dots D_{u_1} f$

Доказательство. Индукция по k. Для $k = 1$ очевидно. Пусть $L = Lin(u, L')$, докажем, что $D_L f(x) = D_u D_{L'}(x)$.

$$D_u D_{L'}(x) = D_u \bigoplus_{v \in L'} f(x \oplus v) = \bigoplus_{v \in L'} f(x \oplus v) \oplus \bigoplus_{v \in L'} f(x \oplus v \oplus u) = \bigoplus_{v \in L} f(x \oplus v)$$

□

Утверждение 5.3. *Верны следующие утверждения*

1. $\forall L \subset \{0,1\}^n$ *подпространства* $\forall f \in \mathrm{Map}(\{0,1\}^n, \{0,1\})$, $u \in L$, $x \in \{0,1\}^n$ *верно*

$$D_L f(x) = D_L f(x \oplus u)$$

2. $\forall f, g \in \mathrm{Map}(\{0,1\}^n, \{0,1\})$, $\forall$ *подпространства* $L \subset \{0,1\}^n$

$$D_L(f \oplus g) = D_L f \oplus D_L g$$

3. $\forall f \in \mathrm{Map}(\{0,1\}^n, \{0,1\})$, $\forall u, v, x \in \{0,1\}^n$

$$D_{u \oplus v} f(x) = D_u f(x) \oplus D_v f(x \oplus u)$$

4. $\forall u, x \in \{0,1\}^n$ $D_u f(x) = 0 \iff f = const$

5. $\forall u \in \{0,1\}^n$ $D_u f = const \iff \exists \alpha \in \{0,1\}^n, \beta \in \{0,1\} \colon f = \langle \alpha, x \rangle \oplus \beta$ *то есть* f *— аффинная.*

Доказательство.

1. $D_L f(x) = \bigoplus_{v \in L} f(x \oplus v) = \bigoplus_{v \in L} f(x \oplus (u \oplus v)) = \bigoplus_{v \in L} f((x \oplus u) \oplus v) = D_L f(x \oplus u)$

2. $D_L(f \oplus g)(x) = \bigoplus_{u \in L} f(x \oplus u) \oplus g(x \oplus v) = D_L f(x) \oplus D_L g(x)$

3. $D_u f(x) \oplus D_v f(x \oplus u) = f(u \oplus x) \oplus f(x) \oplus f(x \oplus u \oplus v) \oplus f(x \oplus u) = f(x) \oplus f(x \oplus u \oplus v) = D_{u \oplus v} f(x)$

4. Очевидно по определению

5. $D_u f(x) = \alpha_u \implies f(x) \oplus f(x \oplus u) = \alpha_u$ Тогда $f(u) = f(0) + \alpha_u$, тогда $f(x) \oplus f(y) = \alpha_{x \oplus y} = f(0) \oplus f(x \oplus y)$. Тогда $\sum\limits_{i=1}^{k} f(x_i) = f(\sum\limits_{i=1}^{k} x_i) + kf(0)$. Пусть $e_1, \ldots, e_n$ — единичные векторы. Тогда

$$f(x) = \langle (f(e_1), \ldots, f(e_n)), x \rangle \oplus (w(x) \mod 2 \oplus 1) f(0) = \langle (f(e_1), \ldots, f(e_n)) + (f(0), \ldots, f(0)), x \rangle \oplus f(0)$$

□

Глава 6

Криптографические свойства булевых функций

6.1 Нелинейность

Определение 6.1. Нелинейностью булевой функции $f : \{0,1\}^n \to \{0,1\}$ называется число

$$\mathcal{N}_f = \min_{g \in \mathscr{A}_n} d(f,g)$$

где $\mathscr{A}_n$ — пространство афинных функций (имеющих как многочлены степень не более 1) и $d(f,g) = |\{x\colon f(x) \neq g(x)\}|$

Замечание 6.1. Легко видеть, что для любой $f \in \mathscr{A}_n$ существует $u \in \{0,1\}^n$ и $b \in \{0,1\}$ такой, что $f(x) = (u,x) \oplus b$

Теорема 6.1.

$$\mathcal{N}_f = 2^{n-1} - \frac{1}{2} \max_{u \in \{0,1\}^n} |W_f(u)|$$

Доказательство.

$$W_f(u) = \sum_{x \in \{0,1\}^n} \exp f(x) v(x,u) = \sum_{x \in \{0,1\}^n} (-1)^{f(x) \oplus (u,x)} =$$

$$\sum_{x \in \{0,1\}^n} \exp(f \oplus (u,x))(x) \underbrace{v(x,0)}_{=1} = W_{f \oplus u}(0) = |\{x\colon f(x) \oplus (u,x) = 0\}| - |\{x\colon f(x) \oplus (u,x) = 1\}|$$

$$= (2^n - d(f(x),(u,x))) - d(f(x),(u,x)) = 2^n - 2d(f(x),(u,x))$$

Выражая из этой формулы расстояние

$$d(f(x),(u,x)) = 2^{n-1} - \frac{1}{2} W_f(u)$$

теперь выразим расстояние до функции $(u,x) \oplus 1$

$$d(f(x),(u,x) \oplus 1)) = 2^n - (2^{n-1} - \frac{1}{2} W_f(u)) = 2^{n-1} + \frac{1}{2} W_f(u)$$

Тогда

$$\min\{d(f(x),(u,x)), d(f(x),(u,x) \oplus 1)\} = 2^{n-1} - \frac{1}{2}|W_f(u)|$$

и, наконец

$$\mathcal{N}_f = \min_{g \in \mathscr{A}_n} d(f,g) = \min_{\substack{u \in \{0,1\}^n \\ b \in \{0,1\}}} d(f,(u,x) \oplus b) = \min_{u \in \{0,1\}^n} \left|2^{n-1} - \frac{1}{2}|W_f(u)|\right| =$$

$$= 2^{n-1} - \frac{1}{2} \max_{u \in \{0,1\}^n} |W_f(u)|$$

□

6.2 Автокорреляция

Определение 6.2. Пусть $f, g \in \mathscr{F}_n = \mathrm{Map}(\{0,1\}^n, \{0,1\})$. Определим функцию $\Delta_{f,g} : \{0,1\}^n \to \mathbb{Z}$ следующим образом:

$$\Delta_{f,g}(u) = \sum_{x \in \{0,1\}^n} \exp(f(x) \oplus g(x \oplus u))$$

Назовем эту функцию *функцей взаимной корреляции.*

Утверждение 6.1. $\forall u \in \{0,1\}^n, \forall f, g \in \mathscr{F}_n \colon \Delta_{f,g}(u) = \Delta_{g,f}(u)$

Определение 6.3. Для $f \in \mathscr{F}_n$ функция $\Delta_f(u) = \Delta_{f,f}(u)$ называется функцией автокорреляции.

Замечание 6.1. Автокорреляция f в точке $u \in \{0,1\}^n$ равна нулевому коэффициенту Уолша-Адамара производной f по направлению u:

$$\Delta_f(u) = W_{D_u f}(0)$$

Доказательство.

$$W_{D_f u}(0) = \sum_{x \in \{0,1\}^n} \exp(D_u f(x)) = \sum \exp(f(x+u) + f(x)) = \Delta_f(u)$$

□

Замечание 6.2. Не любой набор из 2^n чисел может быть набором значений автокорреляции.

Теорема 6.2. *Пусть $f, g \in \mathscr{F}_n$. Тогда*

$$(\Delta_{f,g}(0), \ldots, \Delta_{f,g}(2^n - 1))H_n = (W_f(0) \cdot W_g(0), \ldots, W_f(2^n - 1) \cdot W_g(2^n - 1))$$

где H_n — матрица Сильвестра размера $2^n \times 2^n$

Доказательство. Без доказательства □

Следствие 6.1. *Пусть $f \in \mathscr{F}_n$ тогда*

$$(\Delta_f(0), \ldots, \Delta_f(2^n - 1))H_n = (W_f^2(0), \ldots, W_f^2(2^n - 1))$$

или

$$\sum_{x \in \{0,1\}^n} \Delta_f(x) \exp(\langle x, u \rangle) = W_f^2(u)$$

для всех $u \in \{0,1\}^n$.

Теорема 6.3. *Определим $h \in \mathscr{F}_{n+m}$ как $h(x,y) = f(x) + g(y)$, где $f \in \mathscr{F}_n$, $g \in \mathscr{F}_m$. Тогда*

$$\forall \alpha \in \{0,1\}^n, \beta \in \{0,1\}^m \colon \Delta_h(\alpha, \beta) = \Delta_f(\alpha)\Delta_g(\beta)$$

Доказательство.

$$\Delta_h(\alpha, \beta) = \sum_{\substack{x \in \{0,1\}^n \\ y \in \{0,1\}^m}} \exp(h(x,y) \oplus h(x+\alpha, y+\beta)) =$$

$$\sum_{\substack{x \in \{0,1\}^n \\ y \in \{0,1\}^m}} \exp(f(x) \oplus g(y) \oplus f(x+\alpha) \oplus g(y+\beta)) = \Delta_f(\alpha)\Delta_g(\beta)$$

□

Следствие 6.2. $\forall f \in \mathscr{F}_n$ *выполнено* $|\operatorname{Supp} \Delta_f| \cdot |\operatorname{Supp} W_f| \geq 2^n$, *где* $\operatorname{Supp} \Delta_f = \{x \colon \Delta_f(x) \neq 0\}$; $\operatorname{Supp} W_f = \{x \colon W_f(x) \neq 0\}$.

6.3 Уравновешенность, устойчивость и корреляционная имунность

6.3.1 Уравновешенность

Определение 6.4. Функция $f : \{0,1\}^n \to \{0,1\}$ называется, уравновешенной, если для

$$|\{x\colon f(x) = 0\}| = 2^{n-1}$$

, то есть, если она принимает значение 0 ровно в половине случаев.

Если функция уравновешена, то она наиболее оптимально сужает множество возможных прообразов, то есть, сообщает ровно 1 бит информации о прообразе.

Утверждение 6.2. *f уравновешенна $\iff$ $W_f(0^n) = 0$, где F_f — преобразование Фурье функции f.*

Доказательство. $W_f(0^n) = \sum\limits_{x\in\{0,1\}^n} (-1)^{f(x)} \underbrace{v(x, 0^n)}_{=1} = \sum\limits_{x\in\{0,1\}^n} (-1)^{f(x)} = |\{x\colon f(x) = 0\}| - |\{x\colon f(x) = 1\}|$

Так как $\{x\colon f(x) = 0\} \cap \{x\colon f(x) = 1\} = \emptyset$, получили, что требовалось. □

6.3.2 Корелляционная имунность

Определение 6.5. Пусть $f : \{0,1\}^n \to \{0,1\}$, $1 \le i_1 < \ldots < i_m \le n$, $a_1, \ldots, a_m \in \{0,1\}$. Тогда обозначим $f^{a_i \ldots, a_m}_{i_1,\ldots,i_m}$ функцию из $\{0,1\}^{n-m}$ полученную как сужение функции f на множество $\{x\colon x_{i_k} = a_k\}$ с введением естественных координат.

Определение 6.6. Пусть $f : \{0,1\}^n \to \{0,1\}$. f называется корелляционно-имунной, если для любых $1 \le i_1 < \ldots < i_m \le n$, $a_1, \ldots, a_m \in \{0,1\}$ выполнено

$$w(f^{a_i \ldots, a_m}_{i_1,\ldots,i_m}) = \frac{w(f)}{2^m}$$

6.3.3 Устойчивость

Определение 6.7. Функция $f : \{0,1\}^n \to \{0,1\}$ называется m-устойчивой, если для любых $1 \le i_1 < \ldots < i_m \le n$ и любых $a_1, \ldots, a_m \in \{0,1\}$ функция, полученная из f сужением на множество $\{x\colon x_{i_k} = a_k\}$ уравновешенна.

Вспомним несколько свойств преобразования Уолша-Адамара.

Утверждение 6.3. *Пусть E — линейное подпространство $\{0,1\}^n$. Тогда $F_{\mathbf{1}_E} = |E|\mathbf{1}_{E^\perp}$*

Определение 6.8. Обозначим $\mathscr{F}(f) = W_f(0)$

Определение 6.9. Бинарной производной функции $f : \{0,1\}^n \to \{0,1\}$ называется функция $D_b f(x) = f(x) \oplus f(x+b)$

Утверждение 6.4. *Для бинарной f выполняется $W_f^2(u) = \sum\limits_{b\in\{0,1\}^n} \mathscr{F}(D_b(f))(-1)^{(u,b)}$*

Доказательство. Распишем правую часть:

$$\sum_{b\in\{0,1\}^n} \mathscr{F}(D_b(f))(-1)^{(u,b)} = \sum_{b\in\{0,1\}^n} \sum_{g\in\{0,1\}^n} (-1)^{f(g)\oplus f(g+b)}(-1)^{(u,b)}$$

поменяем обозначения

$$\sum_{h\in\{0,1\}^n} \sum_{g\in\{0,1\}^n} (-1)^{f(g)\oplus f(h)}(-1)^{(u,g\oplus h)}$$

и по линейности скалярного произведения получаем

$$\left(\sum_{h\in\{0,1\}^n} (-1)^{f(h)}(-1)^{(u,h)}\right) \cdot \left(\sum_{g\in\{0,1\}^n} (-1)^{f(g)}(-1)^{(u,g)}\right) = W_f^2(u)$$

□

Теорема 6.4. *$f: \{0,1\}^n \to \{0,1\}$ является m-устойчивой $\iff$ $\forall u\colon w(u) \le m$ выполняется $W_f(u) = 0$*

Уравновешенные функции являются 0-устойчивыми и для них мы эту теорему уже доказали.

Лемма 6.1. *Пусть E и E' — подпространства $\{0,1\}^n$ такие, что $\underbrace{E + E'}_{\text{прямая сумма}} = \{0,1\}^n$ и $E \cap E' = \{0\}$. Пусть h_a — сужение f на сдвинутое подпространство $E + a$. Тогда выполняется*

$$\sum_{u\in E^\perp} W_f^2(u) = |E^\perp| \sum_{a\in E'} W_{h_a}^2(0)$$

Доказательство.

$$\sum_{u\in E^\perp} W_f^2(u) =$$

по второму утверждению

$$\sum_{u\in E^\perp} \sum_{b\in\{0,1\}^n} \mathscr{F}(D_b f)(-1)^{(u,b)} =$$

поменяем местами суммы

$$\sum_{b\in\{0,1\}^n} \mathscr{F}(D_b f) \underbrace{\sum_{u\in E^\perp} (-1)^{(u,b)}}_{F_{\mathbf{1}_{E^\perp}}(b)} =$$

по первому утверждению

$$\sum_{b\in\{0,1\}^n} \mathscr{F}(D_b f)|E^\perp|\mathbf{1}_E(b) = |E^\perp| \sum_{b\in E} \mathscr{F}(D_b f)$$

теперь, так как $\{0,1\}^n$ является прямой суммой E и E' можно записать $f = \sum\limits_{e\in E'} h_e$

$$|E^\perp| \sum_{b\in E} \mathscr{F}\big(D_b \sum_{e\in E'} h_e\big)$$

производная и преобразование Уолша-Адамара линейны, поэтому вынесем сумму по e вовне

$$= |E^\perp| \sum_{e\in E'} \big(\sum_{b\in E} \mathscr{F}(D_b h_e)\big)$$

теперь применим второе утверждение еще раз, пользуясь тем, что E — линейное пространство

$$|E^\perp| \sum_{e\in E'} \mathscr{F}^2(D_e f)$$

□

Доказательство. Рассмотрим произвольное множество $I \subset \{1,\dots,n\}$ такое, что $|I| = m$. Обозначим $E = \{x\colon \forall i \in I\, x_i = 0\}$. Тогда легко видеть, что $E^\perp = \{x\colon \forall i \notin I\, x_i = 0\}$. Прямая сумма E и $E^\perp$ дает всё $\{0,1\}^n$.

Тогда можем записать утверждение леммы

$$\sum_{u\in E^\perp} W_f^2(u) = |E^\perp| \sum_{a\in E^\perp} W_{h_a}^2(0)$$

Левая часть равна нулю тогда и только тогда, когда для всех $u \in E^\perp$ верно $W_f(u) = 0$, вторая часть равна нулю тогда и только тогда, когда для всех $a \in E^\perp$ верно $W_{h_a}(0) = 0$, что, в свою очередь, равносильно уравновешенности h_a. Здесь h_a — сужение на сдвинутое подпространство $a + E$, то есть сужение из определения устойчивости.

Так как эта равносильность выполнена для любых I, теорема доказана.

□

6.4 Бент-Функции

6.4.1 Определение и базовые свойства

Определение 6.10. Функция $f \in \mathscr{F}_n$ называется *максимально нелинейной* если $f = \arg\max_{f \in \mathscr{F}_n} \mathcal{N}_f$

Определение 6.11. Функция $f \in \mathscr{F}_n$ называется бент-функцией, если

$$\forall u \in \{0,1\}^n : W_f(u) \in \{2^{\frac{n}{2}}, -2^{\frac{n}{2}}\}$$

Замечание 6.3. Бент-функции существуют только для четных n, поскольку $W_f(u) \in \mathbb{Z}$

Замечание 6.4. Если n четно, то f бент-функция $\iff$ f максимально нелинейна.

Доказательство. Вспомним, что $\mathcal{N}_f = 2^{n-1} - \frac{1}{2} \max_{u \in \{0,1\}^n} |W_f(u)|$. Кроме того, по неравенству Парсеваля

$$\sum_{x \in \{0,1\}^n} W_f^2(x) = 2^{2n}.$$

Тогда

$$\sum_{x \in \{0,1\}^n} W_f^2(x) \le 2^n \max_{x \in \{0,1\}^n} W_f^2(x) \implies \max_{x \in \{0,1\}^n} W_f^2(x) \ge 2^n \implies \mathcal{N}_f \le 2^{n-1} - \frac{1}{2} 2^{\frac{n}{2}}$$

Тогда на бент-функциях достигается максимум нелинейности, а это и требовалось показать. □

ок

Теорема 6.5. *$f \in \mathscr{F}_{2n}$ является максимально нелинейной тогда и только тогда, когда $Q = \left\{\frac{1}{2^n} W_f(\alpha \oplus \beta)\right\}_{\alpha,\beta \in \{0,1\}^{2n}}$ является матрицей Адамара.*

Доказательство. Все элементы матрицы принадлежат $\{1, -1\}$, осталось проверить ортогональность строк:

$$\langle Q_\alpha, Q_\beta \rangle = \sum_{x \in \{0,1\}^{2n}} \frac{1}{2^{2n}} W_f(x \oplus \alpha) W_f(x \oplus \beta) = \frac{1}{2^{2n}} \sum_{x' \in \{0,1\}^{2n}} W_f(x') W_f(x' \oplus \alpha \oplus \beta)$$

теперь по свойству ортогональности коэффициентов Уолша-Адамара имеем

$$\langle Q_\alpha, Q_\beta \rangle = \begin{cases} 0 & \text{если } \alpha \ne \beta \\ 2^{2n} & \text{иначе} \end{cases}$$

Тогда Q — матрица Адамара.

В обратную сторону аналогично. □

6.4.2 Дуальная функция

Определение 6.12. Пусть $f \in \mathscr{F}_{2n}$ — максимально нелинейная булева функция. Тогда $\widetilde{f} \in \mathscr{F}_{2n}$ называется *дуальной к f*, если $W_f(\alpha) = 2^n (-1)^{\widetilde{f}(\alpha)}$

Пример 6.1. Имея пример максимально-нелинейной функции легко построить дуальную к ней:

x	f	$\exp f$		W_f	$\widetilde{f}$
00	1	-1	0	2	0
01	0	1	2	-2	1
10	0	1	-2	-2	1
11	0	1	0	-2	1

Теорема 6.6. *Пусть $f \in \mathscr{F}_{2n}$ является бент-функцией, то $\widetilde{f}$ тоже является бент-функцией.*

Доказательство. Воспользуемся формулой обращения преобразования Уолша-Адамара (5.5):

$$\exp f(x) = \frac{1}{2^{2n}} \sum_{u \in \{0,1\}^{2n}} W_f(u) \exp\langle x, u\rangle$$

Рассмотрим преобразование Уолша-Адамара для $\widetilde{f}$:

$$W_{\widetilde{f}}(u) = \sum_{x \in \{0,1\}^{2n}} \exp(\widetilde{f}(x) \oplus \langle x, u\rangle)$$

По определению дуальной функции $\exp \widetilde{f}(x) = \frac{1}{2^n} W_f(x)$, тогда, подставляя в предыдущую формулу:

$$W_{\widetilde{f}}(u) = \frac{1}{2^n} \sum_{x \in \{0,1\}^{2n}} W_f(x) \exp(\langle x, u\rangle) = 2^n \exp f(x) \in \{2^n, -2^n\}$$

А это и значит, что $\widetilde{f}$ является бент-функцией. □

Замечание 6.5. $\widetilde{\widetilde{f}} = f$. Следует из теоремы об обращении преобразования Уолша-Адамара.

6.4.3 Критерий Ротхауза

Теорема 6.7 (критерий Ротхауза)**.** *$f \in \mathscr{F}_{2n}$ является бент-функцией тогла и только тогда, когда*

$$\forall u \in \{0,1\}^{2n} \setminus \{0\} \colon D_u f \text{ уравновешенна}$$

.

Доказательство. Вспомним теорему 6.5 о связи бент-функции с матрицей Адамара. Мы поняли, что

$$\left\{\frac{1}{2^n} W_f(a \oplus b)\right\}_{a,b \in \{0,1\}^{2n}}$$

является матрицей Адамара. Запишем это условие для функции $\widetilde{f}$, учитывая

$$W_{\widetilde{f}}(u) = 2^n \exp f(u).$$

Скалярное произведение двух строк матрицы $Q = \left\{\frac{1}{2^n} W_{\widetilde{f}}(a \oplus b)\right\}_{a,b \in \{0,1\}^{2n}}$:

$$\langle Q_{\mathbf{0}}, Q_\alpha\rangle = \sum_{x \in \{0,1\}^{2n}} \frac{1}{2^{2n}} W_{\widetilde{f}}(x) W_{\widetilde{f}}(x \oplus \alpha) = \sum_{x \in \{0,1\}^{2n}} \exp(f(x) \oplus f(x \oplus \alpha)) = \sum_{x \in \{0,1\}^{2n}} \exp D_\alpha f(x)$$

Тогда $\alpha = 0 \iff D_\alpha f$ уравновешенна. Мы записываем только произведения с первой строкой, поскольку $\langle Q_a, Q_b\rangle = \langle Q_0, Q_{a \oplus b}\rangle$ □

6.4.4 Конструкция Мэйорана — Мак-Фарланда

Теорема 6.8. *Пусть $\pi : \{0,1\}^n \to \{0,1\}^n$ — перестановка (биекция). $\psi \in \mathscr{F}_n$.*
Тогда

$$f \in \mathscr{F}_2 n : \ f(x,y) = \langle \pi(y), x\rangle \oplus \psi(y)$$

является бент-функцией.

Доказательство. Воспользуемся критерием Ротхауза (6.7) об уравновешенности производных.

$$D_u f(x,y) = f(x \oplus u_1, y \oplus u_2) \oplus f(x,y) = \langle \pi(y + u_2), x + u_1\rangle \oplus \psi(x \oplus u_2) \oplus \langle \pi(y), x\rangle \oplus \psi(y)$$

Чтобы доказать уравновешенность, достаточно вычислить нулевой коэффициент Уолша-Адамара для $D_u f(x,y)$:

$$W_{D_u f}(0) = \sum_{v_1, v_2 \in \{0,1\}^n} \exp(\langle \pi(v_2 + u_2), v_1 + u_1\rangle \oplus \psi(v_2 \oplus u_2) \oplus \langle \pi(v_2), v_1\rangle \oplus \psi(v_2))$$

Распишем по линейности скалярного произведения и вынесем за скобки всё, зависящее только от v_2:

$$\ldots = \sum_{v_2 \in \{0,1\}^n} \exp(\langle \pi(v_2 \oplus u_2), u_1 \rangle \oplus \psi(v_2) \oplus \psi(v_2 \oplus u_2)) \sum_{v_1 \in \{0,1\}^n} \exp(\langle \pi(v_2 \oplus u_2) \oplus \pi(v_2), v_1 \rangle)$$

Из свойств функции Уолша знаем, что

$$\sum_{v_1 \in \{0,1\}^n} \exp(\langle \pi(v_2 \oplus u_2) \oplus \pi(v_2), v_1 \rangle) = \begin{cases} 0 & \text{если } \pi(v_2 \oplus u_2) \oplus \pi(v_2) \neq 0 \iff u_2 \neq 0 \\ 2^n & \text{иначе} \end{cases}$$

Тогда можем переписать сумму как

$$\ldots = 2^n \cdot \begin{cases} 0 & \text{если } u_2 \neq 0 \\ \sum\limits_{v_2 \in \{0,1\}^n} \exp(\langle \pi(v_2), u_1 \rangle \oplus \underbrace{\psi(v_2) \oplus \psi(v_2)}_{=0}) & \text{если } u_2 = 0 \end{cases}$$

Тогда, из тех же соображений, можем записать

$$W_{D_u f}(0) = \begin{cases} 0 & u \neq 0 \\ 2^{2n} & u = 0 \end{cases}$$

Это доказывает условие критерия Ротхауза и завершает доказательство теоремы. □

Определение 6.13. Класс функций, построенных по теореме выше, называется классом Мэйорана — Мак-Фарланда и обозначается $\mathcal{M}$.

Утверждение 6.5. $|\mathcal{M}| = (2^n)! \cdot 2^{2^n}$

Доказательство. Любая функция из $\mathcal{M}$ однозначно задается поответствующими π и ψ. Пусть существует π_1, π_2 и ψ_1, ψ_2, такие, что

$$\langle \pi_1(y), x \rangle \oplus \psi_1(y) \equiv \langle \pi_2(y), x \rangle \oplus \psi_2(y)$$

тогда

$$\langle \pi_1(y) \oplus \pi_2(y), x \rangle \equiv \psi_1(y) \oplus \psi_2(y)$$

Но левая часть зависит от x, а правая не зависит, положив $x = 0$ получаем $\psi_1 \equiv \psi_2$ и тогда сразу $\pi_1 \equiv \pi_2$. □

Утверждение 6.6. *Пусть* $f(x, y) = \langle \pi(y), x \rangle \oplus \psi(y)$. *Тогда*

$$\widetilde{f}(x, y) = \langle y, \pi^{-1}(x) \rangle \oplus \psi(\pi^{-1}(x))$$

для $x, y \in \{0,1\}^n$

Доказательство. Нужно проверить $W_f(\alpha) = 2^n(-1)^{\widetilde{f}(\alpha)}$:

$$W_f(\alpha_1, \alpha_2) = \sum_{x,y \in \{0,1\}^n} \exp(\langle \pi(y), x \rangle \oplus \psi(y) \oplus \langle \alpha_1, x \rangle \oplus \langle \alpha_2, y \rangle) = \sum_{y \in \{0,1\}^n} \exp(\psi(y) \oplus \langle \alpha_2, y \rangle) \sum_{x \in \{0,1\}^n} \exp(\langle \pi(y) \oplus \alpha_1, x \rangle)$$

По свойству функции Уолша

$$\sum_{x \in \{0,1\}^n} \exp(\langle \pi(y) \oplus \alpha_1, x \rangle) = \begin{cases} 2^n & \pi(y) = \alpha_1 \\ 0 & \text{иначе} \end{cases}$$

Тогда в итоге получаем

$$W_f(\alpha) = 2^n \exp(\langle \alpha_2, \pi^{-1}(\alpha_1) \rangle \oplus \psi(\pi^{-1}(\alpha_1))) = 2^n \exp(\widetilde{f}(\alpha))$$

□

Утверждение 6.7. *На множестве* $\mathscr{F}_{2n}$ *существуют бент-функции степеней* $2, 3, \ldots, n$.

Доказательство. Рассмортим $f(x, y) = \langle \pi(y), x \rangle \oplus \psi(y)$.

Второе слагаемое зависит только от y. Пусть $\forall y \colon \pi(y) = y$. Тогда

$$f(x, y) = x_1 y_1 \oplus \ldots \oplus x_n y_n \oplus \psi(y)$$

$deg(\psi) \in \{0, \ldots, n\}$, кроме того, он не содержит мономов $x_i y_i$, то есть, коэффициенты при них в f равны 1. Тогда $deg f \in \{2, \ldots, n\}$. □