Теория кодирования

МФТИ, осень 2013

Александр Дайняк

www.dainiak.com

Матрицы Адамара (J. Hadamard)

Матрица Адамара — это квадратная матрица из $\{-1, 1\}^{n \times n}$, в которой любые две строки ортогональны.

Примеры:

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

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

Теорема Адамара

Матрицы Адамара берут начало от следующей теоремы:

Теорема. (J. Hadamard)
Если $A = \left(a_{ij}\right)_{1\le i,j\le n} \in \mathbb{R}^{n\times n}$ и $\left|a_{ij}\right| \le 1$ для любых i, j, то тогда

$$|\det A| \le n^{n/2}$$

Доказательство:

- $|\det A|$ — это объём параллелепипеда, построенного на векторах-строках матрицы A
- Объём максимален, когда длины сторон максимальны (максимум равен $\sqrt{n}$ при $\left|a_{ij}\right| = 1$) и углы между сторонами прямые (т.е. векторы ортогональны).

Матрицы Адамара

Если H — матрица Адамара, то

- Матрица, полученная из H перестановками строк/столбцов, тоже является матрицей Адамара.
- Матрица, полученная из H умножением строк/столбцов на -1, тоже является матрицей Адамара.

Матрицы Адамара, получаемые друг из друга такими преобразованиями, *эквивалентны*.

Матрицы Адамара

Любую матрицу Адамара умножением строк/столбцов на -1 можно привести к виду

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & & & \\ \vdots & & & \\ 1 & & & \end{pmatrix}$$

Такая матрица Адамара называется *нормализованной*.

Порядок матриц Адамара

Утверждение.

Если $H \in \{-1, 1\}^{n\times n}$ — матрица Адамара, и $n > 2$, то $4|n$.

Доказательство:

От матрицы H перейдём к эквивалентной матрице, в которой первые три строки такие:

$$\underbrace{\begin{matrix}1 & 1 & \cdots & 1\\ 1 & 1 & \cdots & 1\\ 1 & 1 & \cdots & 1\end{matrix}}_{i}\ \underbrace{\begin{matrix}1 & 1 & \cdots & 1\\ 1 & 1 & \cdots & 1\\ -1 & -1 & \cdots & -1\end{matrix}}_{j}\ \underbrace{\begin{matrix}1 & 1 & \cdots & 1\\ -1 & -1 & \cdots & -1\\ 1 & 1 & \cdots & 1\end{matrix}}_{k}\ \underbrace{\begin{matrix}1 & 1 & \cdots & 1\\ -1 & -1 & \cdots & -1\\ -1 & -1 & \cdots & -1\end{matrix}}_{l}$$

Отсюда

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

Решение этой системы: $i = j = k = l = n/4$.

Порядок матриц Адамара

Гипотеза Адамара (не доказана).
Матрицы Адамара порядка n существуют(?) для *всех* натуральных n, кратных четырём.

Наименьший порядок, для которого пока не доказано существование матрицы Адамара, равен 668.

Конструкция Сильвестра

Утверждение.
Матрица Адамара порядка n существует для любого $n = 2^k$.

Доказательство: (J. J. Sylvester)

Заметим, что если H — матрица Адамара, то матрицей Адамара будет и такая: $\begin{pmatrix} H & H \\ H & -H \end{pmatrix}$.

Утверждение теперь следует по индукции из того факта, что $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ — матрица Адамара.

Матрицы Адамара

Теорема. (R. E. A. C. Paley ’1933)
Если p простое и $4|(p^m+1)$, то существует матрица Адамара порядка (p^m+1).

(Конструкция Пэли на основе квадратичных вычетов.)

Квадратичные вычеты

Элемент $a \in \mathbb{F}_q \setminus \{0\}$ называется *квадратичным вычетом*, если $a = x^2$ для некоторого $x \in \mathbb{F}_q$.

Остальные элементы из $\mathbb{F}_q \setminus \{0\}$ называются *квадратичными невычетами*.

Например, в $\mathbb{Z}_7$ элементы $1,2,4$ — к.в.,
а $3,5,6$ — к.н.

Квадратичные вычеты

Утверждение.

- Если λ — примитивный элемент $\mathbb{F}_q$, то элементы вида λ^{2t} являются к.в., а вида λ^{2t+1} — к.н.
- Если $q = p^m$ и $p > 2$, то ровно половина элементов из $\mathbb{F}_q \setminus \{0\}$ являются к.в., а половина — к.н.

<u>Везде далее будем предполагать, что $p > 2$.</u>

Символ Лежандра

Символ Лежандра $\chi(a)$ определяется так:

$$\chi(a) = \begin{cases} 0, \text{если } a = 0 \\ 1, \text{если } a \text{ к. в.} \\ -1, \text{если } a \text{ к. н.} \end{cases}$$

Утверждение.
Для любых $a, b \in \mathbb{F}_q$ имеет место равенство

$$\chi(a) \cdot \chi(b) = \chi(ab)$$

Квадратичные вычеты

Утверждение.

Для любого $c \in \mathbb{F}_q \setminus \{0\}$ имеет место равенство

$$\sum_{b \in \mathbb{F}_q} \chi(b) \cdot \chi(b+c) = -1$$

Доказательство:

Т.к. *ровно* половина элементов $\mathbb{F}_q \setminus \{0\}$ квадратичными вычетами, то $\sum_{a \in \mathbb{F}_q} \chi(a) = 0$.

Также заметим, что

$$\sum_{b \in \mathbb{F}_q} \chi(b) \cdot \chi(b+c) = \sum_{b \in \mathbb{F}_q \setminus \{0\}} \chi(b) \cdot \chi(b+c)$$

Квадратичные вычеты

С учётом замеченного, получаем

$$\sum_{b\in\mathbb{F}_q\setminus\{0\}} \chi(b)\cdot\chi(b+c) = \sum_{b\in\mathbb{F}_q\setminus\{0\}} \chi(b)\cdot\chi\big(b\cdot b^{-1}(b+c)\big) =$$

$$= \sum_{b\in\mathbb{F}_q\setminus\{0\}} \big(\chi(b)\big)^2\cdot\chi\big(b^{-1}(b+c)\big) = \sum_{b\in\mathbb{F}_q\setminus\{0\}} \chi\big(b^{-1}(b+c)\big) =$$

$$= \sum_{b\in\mathbb{F}_q\setminus\{0\}} \chi(1+b^{-1}c) = \sum_{a\in\mathbb{F}_q\setminus\{1\}} \chi(a) = \sum_{a\in\mathbb{F}_q} \chi(a) - \chi(1) = -1$$

Матрица Якобшталя (E. Jacobsthal)

Рассмотрим матрицу $\left(t_{a,b}\right)_{a,b\in\mathbb{F}_q} \in \{-1,0,1\}^{q\times q}$, в которой $t_{a,b} \coloneqq \chi(a-b)$.

Скалярное произведение любых двух различных строк $\left(t_{a',b}\right)_{b\in\mathbb{F}_q}$ и $\left(t_{a'',b}\right)_{b\in\mathbb{F}_q}$ равно

$$\sum_{b\in\mathbb{F}_q} \chi(a'-b)\cdot\chi(a''-b) = \sum_{b\in\mathbb{F}_q} \chi(b)\cdot\chi\big(b+(a''-a')\big) = -1$$

«Подправленная» матрица Якобшталя

Рассмотрим матрицу $\left(t'_{a,b}\right)_{a,b\in\mathbb{F}_q} \in \{-1,1\}^{q\times q}$, в которой $t'_{a,b} = \chi(a-b)$, если $a \neq b$ и $t'_{a,b} = -1$ иначе.

Скалярное произведение различных строк $\left(t'_{a',b}\right)_{b\in\mathbb{F}_q}$ и $\left(t'_{a'',b}\right)_{b\in\mathbb{F}_q}$ равно

$$\left(\sum_{b\in\mathbb{F}_q} \chi(a'-b)\cdot\chi(a''-b)\right) - \chi(a'-a'') - \chi(a''-a') =$$

$$= -1 - \chi(a'-a'') - \chi(a''-a')$$

Если (-1) является квадратичным *не*вычетом в $\mathbb{F}_q$, то

$$\chi(a''-a') = \chi(-1)\cdot\chi(a'-a'') = -\chi(a'-a''),$$

и скалярное произведение получается равным -1.

«Подправленная» и «дополненная» матрица Якобшталя

$T' \coloneqq \left(t'_{a,b}\right)_{a,b\in\mathbb{F}_q} \in \{-1,1\}^{q\times q}$,

где $t'_{a,b} = \chi(a-b)$, если $a \neq b$, и $t'_{a,b} = -1$ иначе.

Если (-1) является квадратичным невычетом в $\mathbb{F}_q$, то скалярное произведение любых двух строк матрицы T' равно -1. Тогда матрица

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & & & \\ \vdots & & T' & \\ 1 & & & \end{pmatrix}$$

является нормализованной матрицей Адамара.

Матрицы Адамара

Утверждение. (Без доказательства)
При $4|(q+1)$ элемент (-1) является квадратичным невычетом в $\mathbb{F}_q$.

Следствие.
Если p простое и $4|(p^m+1)$, то существует матрица Адамара порядка (p^m+1).

Коды Адамара

Введены R. C. Bose, S. S. Shrikhande ’1959.

Идея:
В матрице Адамара любые две строки $\boldsymbol{a}, \boldsymbol{b}$ ортогональны. Т.к. $a, b \in \{-1, 1\}^n$, это значит, что ровно половина координат у них совпадает, а половина противоположны.

Заменяем координаты $-1 \to 0$ и получаем из строк матрицы двоичный код с большим кодовым расстоянием.

Коды Адамара

Пусть $A \in \{0,1\}^{n \times n}$ — матрица, полученная из нормализованной матрицы Адамара заменой элементов -1 на 0.

- Множество строк матрицы A с отброшенной первой координатой образует двоичный $\left(n-1, n, \frac{n}{2}\right)$-код
- Множество строк матрицы A и их дополнений образует $\left(n, 2n, \frac{n}{2}\right)$-код

Оптимальность кодов Адамара

Граница Плоткина (в двоичном случае)

Если $N < 2d$, то для любого (N, M, d)-кода

$$M \leq \frac{2d}{2d - N}$$

Коды Адамара с параметрами $\left(n-1, n, \frac{n}{2}\right)$ достигают границы Плоткина, имея максимально число слов при заданных длине и кодовом расстоянии.

Каскадные коды
(предложены G. D. Forney ’1966)

Пусть

- C_{internal} — $(n, m, d)_q$-код (*внутренний код*)
- C_{external} — $(N, M, D)_m$-код (*внешний код*)

Символам алфавита кода C_{ext} сопоставим слова кода C_{int}.

Тогда кодовым словам кода C_{ext} соответствуют слова длины Nn в алфавите кода C_{int}.

Получаем *каскадный* $(Nn, M, d')_q$-код, где $d' \geq Dd$.

Каскадные коды (линейный двоичный случай)

Пусть

- C_{int} — $[n, k, d]$-код (*внутренний код*)
- C_{ext} — $[N, K, D]_{2^k}$-код (*внешний код*)

Элементам $\mathbb{F}_{2^k}$ сопоставим слова кода C_{int}, так, чтобы линейная комбинация элементов $\mathbb{F}_{2^k}$ соответствовала линейной комбинации слов кода C_{int}.

Тогда кодовым словам кода C_{ext} соответствуют слова длины Nn в алфавите кода C_{int}.

Получаем каскадный $[Nn, kK, dD]$-код.

Коды Форни

В качестве внешнего кода удобно взять оптимальный (например, MDS) код над алфавитом большой (не слишком) мощности.

В качестве внутреннего кода можно взять близкий к оптимальному код с не очень большим числом кодовых слов.

Сможем получить асимптотически хорошее семейство линейных кодов, для которых есть полиномиальный алгоритм декодирования.

Асимптотически хорошие коды

Пусть задано семейство двоичных кодов

$$\tilde{C} \coloneqq \{C_n\}_{n=1}^{\infty}$$

Асимптотической скоростью семейства $\tilde{C}$ называется величина

$$\mathrm{rate}\left(\tilde{C}\right) \coloneqq \varliminf_{n\to\infty} \frac{\log_2|C_n|}{n}$$

Асимптотическим относительным кодовым расстоянием семейства $\tilde{C}$ называется величина

$$\delta\left(\tilde{C}\right) \coloneqq \varliminf_{n\to\infty} \frac{d(C_n)}{n}$$

Асимптотически хорошие коды

$$\mathrm{rate}(\tilde{C}) \coloneqq \varliminf_{n\to\infty} \frac{\log_2|C_n|}{n}$$
$$\delta(\tilde{C}) \coloneqq \varliminf_{n\to\infty} \frac{d(C_n)}{n}$$

Семейство кодов называется *асимптотически хорошим*, если для него $\mathrm{rate}(\tilde{C}) > 0$ и $\delta(\tilde{C}) > 0$

До кодов Форни было неизвестно, существуют ли асимптотически хорошие семейства кодов с полиномиальными алгоритмами декодирования.

Теорема Варшамова—Гилберта

Теорема. (Р. Р. Варшамов, E. N. Gilbert)
Пусть натуральные числа n, k, d' таковы, что

$$\sum_{j=0}^{d'-1} \binom{n-1}{j} < 2^{n-k}$$

Тогда существует $[n, k, d]$-код, где $d > d'$.

Следствие.
Если $\delta < 0.5$ и ρ таковы, что $H(\delta) \leq 1 - \rho$, то *существует* семейство линейных кодов $\tilde{C}$, для которого $\mathrm{rate}(\tilde{C}) \geq \rho$ и $\delta(\tilde{C}) \geq \delta$.

Теорема Варшамова—Гилберта (асимптотическая версия)

Доказательство следствия:
Если n, k, d' таковы, что $H(d'/n) \leq 1 - \frac{k}{n}$, то

$$\sum_{j=0}^{d'-1} \binom{n-1}{j} < 2^{n \cdot H\left(d'/n\right)} \leq 2^{n-k},$$

то есть условия теоремы В.—Г. выполнены, и существует линейный $[n, k, d]$-код, где $d > d'$.

Если $H(\delta) \leq 1 - \rho$, то берём для каждого n
$k \coloneqq \lfloor \rho n \rfloor$, $d' \coloneqq \lfloor \delta n \rfloor$, и получаем требуемое.

Цель

Теорема Варшамова—Гилберта не даёт полиномиальных (по длине кодовых слов) алгоритмов построения кода и декодирования.

А хочется следующего:

- Для каждого n строить порождающую или проверочную матрицу некоторого линейного кода с длиной слов, размерностью и кодовым расстоянием $\Omega(n)$. И всё за полиномиальное от n время.
- Исправлять $\Omega(n)$ ошибок в кодовых словах за полиномиальное от n время.

Каскадный код Форни на основе конструкции В.—Г. и кода Р.—С.

Пусть $t \in \mathbb{N}$, и пусть $\delta < 0.5$ — произвольное фиксированное число.

По теореме В.—Г., существует линейный код с параметрами

$$\left[\frac{t}{1-H(\delta)}, t, \frac{\delta t}{1-H(\delta)}\right]$$

Возьмём этот код в качестве внутреннего.

В качестве внешнего возьмём RS-код с параметрами $[2^t, 2^{t-1}, 2^{t-1}+1]_{2^t}$.

Получаем каскадный $[n, k, d]$-код, для которого

$$n = \frac{t \cdot 2^t}{1 - H(\delta)}, \quad k = \frac{t \cdot 2^t}{2}, \quad d > \frac{\delta t \cdot 2^t}{2\big(1 - H(\delta)\big)}$$

Каскадный код Форни на основе конструкции В.—Г. и кода Р.—С.

Получаем каскадный $[n, k, d]$-код, для которого

$$n = \frac{t \cdot 2^t}{1 - H(\delta)}, \quad k = \frac{t \cdot 2^t}{2}, \quad d > \frac{\delta t \cdot 2^t}{2\big(1 - H(\delta)\big)}$$

Этот код является асимптотически хорошим, т.к. $\frac{d}{n} \geq \frac{\delta}{2\left(1-H(\delta)\right)} > 0$ и $\frac{k}{n} \geq \frac{1}{2\left(1-H(\delta)\right)} > 0$.

Каскадный код Форни на основе конструкции В.—Г. и кода Р.—С.

Получаем каскадный $[n, k, d]$-код, для которого

$$n = \frac{t \cdot 2^t}{1 - H(\delta)}, \quad k = \frac{t \cdot 2^t}{2}, \quad d > \frac{\delta t \cdot 2^t}{2\big(1 - H(\delta)\big)}$$

Вычислить порождающую матрицу кода можно при каждом t за полиномиальное время, т.к.

- коды Р.—С. строятся за полиномиальное время от своих параметров,
- проверочная матрица кода в теореме В.—Г. строится хотя и перебором, но параметры этого кода логарифмичны по n.

Каскадный код Форни на основе конструкции В.—Г. и кода Р.—С.

Получаем каскадный $[n, k, d]$-код, для которого

$$n = \frac{t \cdot 2^t}{1 - H(\delta)}, \quad k = \frac{t \cdot 2^t}{2}, \quad d > \frac{\delta t \cdot 2^t}{2\big(1 - H(\delta)\big)}$$

Существует «почти тривиальный» полиномиальный алгоритм, декодирующий кодовые слова, принятые с не более чем $\frac{\delta t \cdot 2^t}{8\left(1 - H(\delta)\right)}$ ошибками.

Тривиальный алгоритм декодирования кодов Форни

Каждое слово кода Форни имеет вид

$$\boldsymbol{c} = \boldsymbol{a}_1 \boldsymbol{a}_2 \dots \boldsymbol{a}_{2^t}$$

где $\boldsymbol{a}_i$ — слова кода В.—Г. длины $\frac{t}{1-H(\delta)}$.

Если в слове $\boldsymbol{c}$ произошло $\leq \frac{\delta t \cdot 2^t}{8\left(1-H(\delta)\right)}$ ошибок, и в результате принято слово $\tilde{\boldsymbol{c}} = \tilde{\boldsymbol{a}}_1 \tilde{\boldsymbol{a}}_2 \dots \tilde{\boldsymbol{a}}_{2^t}$, то слово $\boldsymbol{c}$ восстанавливаем в два шага:

- Для каждого $\tilde{\boldsymbol{a}}_i$ перебором ищем ближайшее к нему слово кода В.—Г. При этом неверно восстановленных слов может быть не более $\frac{\delta t \cdot 2^t}{8\left(1-H(\delta)\right)} / \frac{\delta t}{2\left(1-H(\delta)\right)} = 2^{t-2}$.
- Кодовое расстояние внешнего кода равно $(2^{t-1} + 1)$, поэтому даже 2^{t-2} ошибок он успешно исправит.

Пояснения к алгоритму декодирования кодов Форни

Пусть слово $\boldsymbol{c} = \boldsymbol{a}_1 \boldsymbol{a}_2 \ldots \boldsymbol{a}_{2^t}$ исказилось в s разрядах и перешло в слово $\tilde{\boldsymbol{c}} = \widetilde{\boldsymbol{a}}_1 \widetilde{\boldsymbol{a}}_2 \ldots \widetilde{\boldsymbol{a}}_{2^t}$.

$\boldsymbol{a}_i$ — слова кода В.—Г. с расстоянием d_{int}.

Пусть $I = \left\{ i \mid d(\widetilde{\boldsymbol{a}}_i, \boldsymbol{a}_i) \geq \frac{d_{\text{int}}}{2} \right\}$, где $|I| \leq \frac{2s}{d_{\text{int}}}$.

Т.к. на первом шаге проблемы с исправлением могут быть только у слов $\widetilde{\boldsymbol{a}}_i$, у которых $i \in I$, то на втором шаге, рассматривая каждое $\widetilde{\boldsymbol{a}}_i$ как один элемент поля $\mathbb{F}_{2^t}$, мы получаем задачу восстановления слова кода Р.—С. с ошибками не более чем в $\frac{2s}{d_{\text{int}}}$ разрядах.