Московский физико-технический институт
Физтех-школа прикладной математики и информатики

БОЛЬШОЕ НАЗВАНИЕ КУРСА

V СЕМЕСТР

Лектор: *Иван Иванович Иванов*

h\nu

Автор: *Павел Дуров*
Репозиторий на Github

осень 2022

Содержание

1 Матрицы Адамара

Определение 1.1. Матрицей Адамара называется матрица A, если и только если

$$[A]_{ij} \in \{1, -1\}$$

И ее строчки попарно отрогональны (то есть скалярное произведение любых двух строк равно 0)

Пример. 1. $n = 1$ — очев

2. $n = 2$:

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

3. $n = 2$:

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

Замечание. $n \geqslant 2 \Rightarrow n = 2k$

Доказательство. Очевидно, т.к. если мы перемножим любые две строчки, то тогда в скалярном произведении придется сложить нечетное количество ± 1, тогда эта сумма точно не будет равна 0. $\square$

Утверждение 1.1. *Если у матрицы попарно ортогональны сторчки, то и столбцы — тоже*

Определение 1.2. Нормальная форма матрицы Адамара: когда $A_1 = A^1 = (1, 1, \dots 1)$

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & \pm 1 & \dots & \pm 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \pm 1 & \dots & \pm 1 \end{pmatrix}$$

Замечание. Любую матрицу адамара можно привести к нормальному виду путем домножения строк и столбцов на -1.

Теорема 1.1. $n > 2 \Rightarrow n = 4k$

Доказательство. Приведем матрицу Адамара к нормальному виду. Теперь переставим столбцы, чтобы вторая строчка была вида

$$(\underbrace{1, 1 \dots 1,}_{\frac{n}{2}}, \underbrace{-1, -1, \dots -1}_{\frac{n}{2}})$$

А третья строка была вида

$$(\underbrace{1, 1 \dots 1}_{x} \underbrace{1, -1, -1, \dots -1}_{\frac{n}{2} - x}, \underbrace{1, 1 \dots 1,}_{\frac{n}{2} - x} \underbrace{-1, -1, \dots -1}_{x})$$

Тогда скалярное произведение второй и третьей будет равно

$$x - \left(\frac{n}{2} - x\right) - \left(\frac{n}{2} - x\right) + x = 4x - n = 0$$

Тогда $x \vdots 4$ □

Теорема 1.2. *(Гипотеза Адамара) Если $n = 4k$, то матрица Адамара существует.*

Доказательство. Не доказана □

Определение 1.3. Кронекеровское произведение матриц $A * B = C \Rightarrow$

$$C = \begin{pmatrix} a_{11}B & \dots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{n1}B & \dots & a_{nn}B \end{pmatrix} \in M_{mn \times mn}$$

Утверждение 1.2. *Кронекеровское произведение двух матриц Адамара есть матрица Адамара*

Доказательство. Скалярное произведение двух строк равняется

$$\sum_{k=1}^{n} \left(\sum_{s=1}^{m} a_{ik} a_{jk} b_{i's} b_{j's} \right) = \sum_{k=1}^{n} a_{ik} a_{jk} \left(\sum_{s=1}^{m} b_{i's} b_{j's} \right) = (B_{i'}, B_{j'}) \left(\sum_{k=1}^{n} a_{ik} a_{jk} \right) = (B_{i'}, B_{j'})(A_i, A_j) \neq 0$$

□

Теорема 1.3 (Пэли)**.** *Пусть $p = 4k + 3$ — простое число. Тогда $\exists$ матрица Адамара порядка $p + 1$.*

Доказательство. Рассмотрим матрицу порядка p, такую, что $A_{ab} = \left(\frac{a-b}{p}\right)$ (символ Лежандра). Тогда произведение любых двух строк i, j равно

$$\sum_{b=1}^{p} \left(\frac{i-b}{p}\right) \left(\frac{j-b}{p}\right)$$

$c = i - b$.

$$\sum_{c=1}^{p} \left(\frac{c}{p}\right) \left(\frac{c-i+j}{p}\right)$$

Причем, $c = p \Rightarrow \left(\frac{c}{p}\right) = 0$

$$\sum_{c=1}^{p-1} \left(\frac{c}{p}\right) \left(\frac{c-i+j}{p}\right) = \sum_{c=1}^{p-1} \left(\frac{c}{p}\right) \left(\frac{c(1+c^{-1}(i-j))}{p}\right) = \sum_{c=1}^{p-1} \left(\frac{1+c^{-1}(i-j)}{p}\right)$$

При этом, $i - j, c^{-1} \not\equiv_p 0 \Rightarrow$ выражение $1 + c^{-1}(i - j)$ пробегает все остатки $\mod p$, кроме

1. Но тогда итоговая сумма равна $0 - \left(\frac{1}{p}\right) = -1$. Тогда рассмотрим такую матрицу:

$$C = \left(\begin{array}{c|ccc} 1 & 1 & \dots & 1 \\ \hline 1 & & & \\ \vdots & & A & \\ 1 & & & \end{array}\right)$$

Где все нули в A заменены на -1 (получится матрица A', причем замены произойдут только на главной диагонали). Докажем, что она подходит. Заметим, что в матрице A' поровну 1 и -1. Тогда скалярное произведение с первой строчкой точно будет 0. Возьмем строчки i, j в матрице A'. В их скалярном произведении добавилась $(-1)\left(\frac{i-j}{p}\right) + (-1)\left(\frac{j-i}{p}\right) = 0$. Теперь посчитаем скалярное произведение любых двух строк, к нему просот добавится 1 за счет первого столбца. Тогда это будет матрицей Адамара. $\square$

Теорема 1.4 (Пэли)**.** *Пусть $p = 4k+1$ — простое число. Тогда $\exists$ матрица Адамара порядка $2(p+1)$.*

Теорема 1.5 (б/д)**.** $\forall \varepsilon > 0 \exists n_0 : \forall n > n_0$ *на отрезке* $[n, (1 + (1+\varepsilon)n)]$ *есть порядок матрицы Адамара*

Теорема 1.6 (переформулировка, тоже б/д)**.** $\exists f : f(n) = o(n)$*, такая, что на отрезке* $[n, n + f(n)]$ *есть порядок матрицы Адамара*

2 Коды, исправляющие ошибки

Представим ситуацию: разговариваем с бабушкой. Еще мы с ней общаемся азбукой морзе (отправляем ей 0 или 1) и передаем ей сообщения длины n. Известно, что бабушка неправильно услышит не более чем k циферок. Как тогда с ней общаться?

Определение 2.1. Расстояние Хэмминга между словами — количество несовпадающих координат

Тогда нам, по сути, надо расположить непересекающиеся "шары" радиуса k, состоящие из слов. В таком случае мы сможем определить, какое слово мы передали, т.к. оно будет лежать не более, чем в одном шаре.

Определение 2.2. (n, M, d)-код — такой словарь, в котором M слов, каждое из которых имеет длину n и минимальное расстояние между любями двумя словами равно d.

Теорема 2.1 (Граница Плоткина)**.** *Пусть дан (n, M, d)-код, где $2d > n$. Тогда $M \leqslant \frac{2d}{2d-n}$.*

Доказательство неулучшаемости оценки. Рассмотрим матрицу Адамара:

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & \pm1 & \dots & \pm1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \pm1 & \dots & \pm1 \end{pmatrix}$$

И зачеркнем в ней первый столбец. Будем рассматривать строки как слова. Тогда расстояние Хэмминга между ними равно $\frac{n}{2}$ (т.к. скалярное произведение любых двух равно 0). Тогда получили $\left(n-1, n, \frac{n}{2}\right)$. Но тогда плоткин дает результат $\frac{2\frac{n}{2}}{2\frac{n}{2}-(n-1)} = n$, т.е. мы нашли пример, который точно подходит под оценку. $\square$