55. Матрицы Адамара. (Вторая) конструкция Пэли с квадратичными вычетами при $n = 2p + 2, p = 4m + 1$.

Утверждение (свойства кронекеровского произведения):

1. $(A \otimes B)^T = A^T \otimes B^T$
2. $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$

▲ 1. $C = A \otimes B, D = C^T$. Тогда $d_{pb+q,kb+l} = c_{kb+l,pb+q} = a_{kp}b_{lq} = (A)^T_{pk}(B)^T_{ql} \Rightarrow$ по определению $D = A^T \otimes B^T$

2. Покажем, что это правда для случаев когда размеры A, C и B, D попарно равны и все матрицы квадратные. Тогда можно просто рассмотреть их произведение как блочных матриц.

$$\begin{pmatrix} a_{11}B & \dots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{n1}B & \dots & a_{nn}B \end{pmatrix} \begin{pmatrix} c_{11}D & \dots & c_{1n}D \\ \vdots & \ddots & \vdots \\ c_{n1}D & \dots & c_{nn}D \end{pmatrix} = \begin{pmatrix} R_{11} & \dots & R_{1n} \\ \vdots & \ddots & \vdots \\ R_{n1} & \dots & R_{nn} \end{pmatrix}$$

где $R_{ij} = \sum_{k=1}^n (a_{ik}B)(c_{kj}D)$ (утверждение из Википедии) $= (\sum_{k=1}^n a_{ik}c_{kj})BD = (AC)_{ij}BD$ $\Rightarrow$ по определению получили $(AC) \otimes (BD)$ ■

Лемма:

1. Если $p \equiv 1 (\operatorname{mod} 4)$, то Q_p - симметрична
2. $QQ^T = pE - I$, где I - матрица состоящая полностью из единиц

▲ 1.

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{\frac{4k}{2}} = 1 \Rightarrow \left(\frac{i-j}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{j-i}{p}\right) = \left(\frac{j-i}{p}\right) \Rightarrow Q_{ij} = Q_{ji}$$

2. В первой конструкции Пэли мы показали, что скалярное произведение различных строк Q равно -1. Скалярное произведение строк i, j - это элемент на позиции i, j в QQ^T. Очевидно, что на диагонали будут стоять числа $p - 1$, так как в каждой строке ровно $p-1$ ненулевой элемент, каждый из которых равен ± 1. Таким образом, получается, что $QQ^T = pE - I$ ■

II конструкция Пэли: Пусть $p \equiv 1 (\operatorname{mod} 4)$. Если в матрице

$$A = \begin{pmatrix} 0 & e^T \\ e & Q \end{pmatrix}$$

где e — столбец из единиц размера p, Q - матрица Якобсталя порядка p, заменить 0 на матрицу $M_0 = \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}$, а ± 1 на матрицу $\pm \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \pm M_1$, то получится матрица Адамара порядка $2p + 2$.

▲ Найдем AA^T (пригодится нам в будущем). В левом верхнем углу очевидно будет стоять p, так как просто перемножили столбец из единиц на строку. Остальные элементы первой строки/столбца будут нулями, так как они равны сумме всех символов Лежандра по p. Просто перемножая матрицы заметим, что в оставшемся пространстве у нас получится матрица $I+QQ^T = I+pE-I = pE$ (по пункту 2 леммы). Таким образом, $AA^T = pE$

Пусть H - матрица которая получилась после замен. Тогда так как нули находятся только на главной диагонали

$$H = A \otimes M_1 + E \otimes M_0$$

$$HH^T = (A \otimes M_1 + E \otimes M_0)(A \otimes M_1 + E \otimes M_0)^T = (A \otimes M_1 + E \otimes M_0)(A^T \otimes M_1^T + E \otimes M_0^T)$$

Заметим, что $M_1^T = M_1, M_0^T = M_0, M_1M_0 = -M_0M_1, A = A^T$ (по пункту 1 леммы)

$$HH^T = (A \otimes M_1)(A^T \otimes M_1) + (E \otimes M_0)(A^T \otimes M_1) + (A \otimes M_1)(E \otimes M_0) + (E \otimes M_0)(E \otimes M_0) =$$

$$= (AA^T) \otimes M_1^2 + A^T \otimes (M_0M_1) - A \otimes (M_0M_1) + E \otimes M_0^2$$

Матрицы M_0, M_1 являются матрицами Адамара $\Rightarrow M_i^2 = M_i^T M_i = 2E$

$$HH^T = pE \otimes 2E + E \otimes 2E = (2p+2)E + 2E = (2p+2)E \blacksquare$$