Last time we showed:

$\forall n \in \mathbb{Z}_{\geq 1}$, $\exists$ a Hurwitz quaternion $N$ such that $NN^T = nI_4$.

Corollary (Lagrange's 4-square theorem)

For every $n \in \mathbb{Z}_{\geq 0}$, $\exists\ a,b,c,d \in \mathbb{Z}$ s.t. $n = a^2+b^2+c^2+d^2$.

Proof:

If $N$ has integer coeffs, i.e.

$$N = \begin{pmatrix} a & — \\ b & — \\ c & — \\ d & — \end{pmatrix}, \text{ then } NN^T = nI_4 \Leftrightarrow a^2+b^2+c^2+d^2 = n$$

and we're done.

However, if $N$ has $\mathbb{Z}+\frac{1}{2}$ coeffs then this only gives us $n = a^2+b^2+c^2+d^2$, where $a,b,c,d \in \mathbb{Z}+\frac{1}{2}$.

Let:

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

(and is also a Hurwitz quaternion)

Note that $\frac{1}{2}H \in lA$, $HH^T = 4I_4$, so $UU^T = I_4$, so $U$ is an orthogonal matrix.

$U$. $\Rightarrow$ Can check that $U$ is a unit in $lA$ and $U^6 = 1$. (so $U^{-1} = U^5$).

Exercise: Check that if $A \in lA$, then at least one of the matrices $A$, $\frac{1}{2}HA$, $\frac{1}{2}H^TA$ has integer coefficients.

all have same modulus since $U = \frac{1}{2}H$ is orthogonal.

Now, use whichever matrix has integer coeffs. $\square$.

# Hadamard Matrices and Designs:

**Defn:** A Hadamard Matrix $H$ is an $n \times n$ matrix such that $HH^T = nI_n$, and all entries of $H$ are in $\{1, -1\}$.

**Remark:** $HH^T = nI_n \iff H^TH = nI_n$

(so $H$ will be normal).

**Examples:**

(1) ~~Not very interesting~~ (1-by-1 matrix)

$\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$ ~~2×2 matrix~~

$H_4$ as defined before.

$\begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix}$ is also a Hadamard matrix.

**Defn:** A monomial matrix $M$ is an $n \times n$ matrix with entries in $\{0, -1, 1\}$ such that there is exactly one non-zero entry in each row/column.

**Note:** We can produce more Hadamard matrices by permuting rows/cols or multiplying by $-1$.

→ Since $HH^T \Rightarrow$ rows of $H$ are orthogonal, so the negative of a row is still orthogonal and similarly with $H^TH$ and cols.

Monomial matrices encode this exactly)

Example (Menonical matrix)

$$\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \end{bmatrix}$$

If $H$ is an $n \times n$ Hadamard matrix and $M_1, M_2$ are $n \times n$ menonical matrices, then $M_1 H M_2$ is also a Hadamard matrix. We say that $H$ and $M_1 H M_2$ are menonically equivalent.

Example:

Let $H_1 = \begin{pmatrix} -1 & 1 \\ 1 & -1 \end{pmatrix}$ and $H_2 = \begin{pmatrix} 1 & -1 & -1 & -1 \\ 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \end{pmatrix}$ as defined before

Then, we can get from $H_1 \to H_2$ by:

1) Multiply 1st row by $-1$
2) Cyclically permute cols 2, 3, 4.

We write this:

$$H_2 = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} H_1 \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$M_1$ $M_2$

Remark: The smallest $n$ for which there exist 2 $n \times n$ Hadamard matrices which are not menonically equivalent is $n = 16$.

**Proposition:**
Every Hadamard matrix is monomially equivalent to one in which every entry in the first row and first column is 1.

**Proof:**
Multiplying the first row by -1 if necessary we can assume that $H_{1x} = 1$.
Now, multiply row $i$ by $H_{i1}$ and multiply col $j$ by $H_{1j}$ for $i = 2, \ldots, m$, $j = 2, \ldots, m$.

A Hadamard matrix in this form is said to be standardized.

Note: Every Hadamard matrix is monomially equivalent to many standardized matrices.

**Theorem:**
If $H$ is an $m \times m$ Hadamard matrix, then $m=1$, $m=2$ or $m = 4n$.

**Proof:**
Assume that $m \geq 3$, and $H$ is standardized. Look at the first 3 rows of $H$.

$$\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & * & * & \cdots & * \\ 1 & * & * & \cdots & * \end{bmatrix}$$ ← 3 rows

There are only 4 possible cols.

$$\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ -1 \end{pmatrix}.$$

→

Proof: (cont'd)

Suppose the number of each type is a, b, c, and d respectively. The dot product of any 2 rows of a HM is 0

$$(\text{row } 1) \cdot (\text{row } 2) = a+b-c-d = 0$$
$$(\text{row } 1) \cdot (\text{row } 3) = a-b+c-d = 0$$
$$(\text{row } 2) \cdot (\text{row } 3) = a-b-c+d = 0.$$

$\Rightarrow a=b=c=d$

and we also know that $a+b+c+d = m$. (from $(\text{row } 1)(\text{row } 1)^T$)

and so we see that $m=4a$. □

Remark: More generally, if $Q$ is a $k \times m$ matrix ($k \geq 3$) with $\pm 1$ entries and $QQ^T = mI_k$, then $m = 4n$. (the proof is the same).

Kronecker Products of Matrices:

Def'n: If $A$, $B$ are matrices, the Kronecker Product $A \otimes B$ is the block matrix obtained by replacing $A_{ij}$ with block $A_{ij}B$

Properties:

- Entries of $A \otimes B$ are all possible products of an entry in $A$ with an entry in $B$.
- Non-commutative, but $A \otimes B$ and $B \otimes A$ are related by permuting rows and columns.

- Associative: $A \otimes (B \otimes C) = (A \otimes B) \otimes C$.
- Bilinear:
$$A \otimes (sB + tC) = sA \otimes B + tA \otimes C$$
$$(sA + tB) \otimes C = sA \otimes C + tB \otimes C.$$
- $(A \otimes B)^T = A^T \otimes B^T$.
- $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$, if RHS makes sense.
Special Case: If $x, y$ are column vectors (i.e. $m \times 1$ matrices), then:
$$(A \otimes B)(x \otimes y) = (Ax) \otimes (By).$$
- If $A, B$ are square matrices then
$$\operatorname{tr}(A \otimes B) = \operatorname{tr}(A)\operatorname{tr}(B)$$
(and $A \otimes B$ is also square).

Theorem:
If $H_1$ and $H_2$ are Hadamard matrices, then $H_1 \otimes H_2$ is a Hadamard matrix.

Proof:
$H_1 \otimes H_2$ has $\pm 1$ entries (since the entries are products of $\pm 1$).
To see that it is Hadamard:
$$(H_1 \otimes H_2)(H_1 \otimes H_2)^T$$
$$= (H_1 \otimes H_2)(H_1^T \otimes H_2^T)$$
$$= (H_1 H_1^T) \otimes (H_2 H_2^T)$$
$$= (m_1 I_{m_1}) \otimes (m_2 I_{m_2})$$
$$= m_1 m_2 (I_{m_1} \otimes I_{m_2})$$
$$= m_1 m_2 I_{m_1 m_2}.$$
□.