7/4/24

Feb 8th

Last time:

Conference Matrices

$$C = \begin{pmatrix} 0 & & \pm 1 \\ & \ddots & \\ \pm 1 & & 0 \end{pmatrix}$$ and satisfy $CC^T = (n-1)I_n$.

Theorem:

If C is an $n \times n$ conference matrix, (where $n \geq 2$), then one of the following must be true:

(i) $n \equiv 2 \pmod 4$ and C is monomially equivalent to a symmetric matrix, or.

(ii) $n \equiv 0 \pmod 4$ and C is monomially equivalent to a skew-symmetric matrix.

Proof: (Exercise - Sketch)

Take diagonal monomial matrices M_1, M_2 so that:

$$\tilde{C} = M_1 C M_2 = \begin{cases} \begin{pmatrix} 0 & 1 & \cdots & 1 \\ 1 & & & \\ \vdots & & * & \\ 1 & & & \end{pmatrix} & \text{if } n \equiv 2 \pmod 4 \\ \begin{pmatrix} 0 & 1 & \cdots & 1 \\ -1 & & & \\ \vdots & & * & \\ -1 & & & \end{pmatrix} & \text{if } n \equiv 0 \pmod 4 \end{cases}$$

Now check that $\tilde{C} = \pm \tilde{C}^T$:

To do this, look at rows $1, i, j$ of $\tilde{C}$

$$\begin{bmatrix} 0 & 1 & \cdots & 1 \\ \vdots & \vdots & & \vdots \end{bmatrix} \rightarrow 3 \times n \text{ submatrix}$$

The possible columns are:

$$\begin{pmatrix}1\\1\\1\end{pmatrix}, \begin{pmatrix}1\\1\\-1\end{pmatrix}, \begin{pmatrix}1\\-1\\1\end{pmatrix}, \begin{pmatrix}1\\-1\\-1\end{pmatrix}, \begin{pmatrix}0\\c_{ij}\\c_{ji}\end{pmatrix}, \begin{pmatrix}1\\0\\c_{ji}\end{pmatrix}, \begin{pmatrix}1\\c_{ij}\\0\end{pmatrix}.$$

These will be ± 1.

Dot product of rows $= 0 \Rightarrow$ Relationship b/w c_{ij} and c_{ji}
$(c_{ij} = \pm c_{ji})$

$\square$

A conference matrix is standardized if $c_{1j} = 1$ for $j \geq 2$ and $C = \pm C^T$.
If C is standardized the $(n-1) \times (n-1)$ submatrix obtained by deleting the first row and column is called the core.

Theorem:
If C is a skew-symmetric conference matrix, then $I + C$ is a Hadamard matrix.

Proof:
$I + C$ has only ± 1 entries (since the 0's are only on the diagonal).
And:

$$(I+C)(I+C)^T = I + \underbrace{C + C^T}_{=0,\ \text{since } C \text{ skew-symmetric}} + CC^T$$
$$= I_n + (n-1)I_n = nI_n$$

$\square$

Theorem:
If C is a symmetric conference matrix:

$$\left(\begin{array}{c|c} C+I & -(C-I) \\ \hline C-I & C+I \end{array}\right)$$

is a Hadamard matrix.

Note:
This should remind us of complex #'s: $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$.

Proof!
Like the last theorem:

$$\left(\begin{array}{c|c} C+I & -C+I \\ \hline C-I & C+I \end{array}\right)\left(\begin{array}{c|c} C+I & -C+I \\ \hline C-I & C+I \end{array}\right)^T$$

$$= \left(\begin{array}{c|c} C+I & -C+I \\ \hline C-I & C+I \end{array}\right)\left(\begin{array}{c|c} C^T+I & C^T-I \\ \hline -C^T+I & C^T+I \end{array}\right)$$

$= \ldots$ (Exercise!) $\square$.

Theorem:
If an $n \times n$ conference matrix exists and $n \equiv 2 \pmod 4$, then $n-1$ is a sum of 2 squares.

(Example: There is no 22×22 conference matrix, since 21 is not a sum of 2 squares)

Proof:
Since $CC^T = (n-1)I_n \Leftrightarrow C I_n C^T = (n-1)I_n$
$\Rightarrow I_n \approx (n-1)I_n$

~~By~~
Since $n \equiv 2 \pmod 4$, by Witt cancellation, we have that $I_2 \approx (n-1)I_2$
$\Rightarrow$ (By HW Problem 2) $n-1$ is a sum of 2 squares. $\square$

A construction
Let q be a prime power.
Let $a_1, a_2, \ldots, a_q$ be the elements of $GF(q)$ listed in some order.
Let P be the $q \times q$ matrix.

$$P = \begin{cases} 0 & \text{if } i = j \\ 1 & \text{if } a_i - a_j \in GR(q) \\ -1 & \text{o/w} \end{cases}$$

P is called the Paley matrix of $GR(q)$

Theorem:
If q is odd, then P is the core of a standardized conference matrix.
i.e. If $q \equiv 1 \pmod 4$, then

$$\begin{pmatrix} 0 & 1 & \cdots & 1 \\ 1 & & & \\ \vdots & & P & \\ 1 & & & \end{pmatrix}$$ is a symmetric conference matrix

and if $q \equiv 3 \pmod 4$, then

$$\begin{pmatrix} 0 & 1 & \cdots & 1 \\ -1 & & & \\ \vdots & & P & \\ -1 & & & \end{pmatrix}$$ is a skew-symmetric conference matrix.

Proof: Reduce this to a problem of checking facts about quadratic residues. – Similar to stuff we've already done. ☐

What do we have so far?

Any prime power $\longrightarrow$ Conference Matrix $\longrightarrow$ Hadamard Matrix (May be twice as big) $\longleftrightarrow$ Hadamard Design.

$\uparrow$ $q \equiv 3 \pmod 4$ QR Difference Set.

Remark: When $q \equiv 3 \pmod 4$, the two constructions give the same Hadamard matrix.

In Summary:

We can construct $4n \times 4n$ Hadamard matrices when

- (Kronecker Products):
  $4n = m_1 m_2$ and there exist
  $m_1 \times m_1$ and $m_2 \times m_2$ HMs
- $4n-1$ is a prime power (OR difference set)
- $2n-1$ is a prime power
  (If $2n-1 \equiv 1 \pmod 4$, use Paley's matrix)
  (If $2n-1 \equiv 3 \pmod 4$, combine 2 above)

Regular Hadamard Matrices:

A Hadamard matrix H is regular if $H\mathbb{1} = 2h\mathbb{1}$ for some $h \in \mathbb{R}$
(so $\mathbb{1}$ is an eigenvector, and all rows sum to $2h$)

Note: - Any row sum of H is even $\Rightarrow h \in \mathbb{Z}$
- h can be positive or negative

Proposition:

If H is a regular $4n \times 4n$ Hadamard Matrix with $H\mathbb{1} = 2h\mathbb{1}$, then $H^T\mathbb{1} = 2h\mathbb{1}$ and $h^2 = n$.

Proof:

Since $H\mathbb{1} = 2h\mathbb{1}$, $\mathbb{1}$ is an eigenvector of H with eigenvalue $2h$. So, $H^{-1}\mathbb{1} = (2h)^{-1}\mathbb{1}$ (i.e. H^{-1} has $(2h)^{-1}$ as an eigenvalue). But $H^T = (4n)H^{-1} \Rightarrow H^T\mathbb{1} = (4n)H^{-1}\mathbb{1} = \frac{2n}{h}\mathbb{1}$.

Now, compute $\mathbb{1}^T H \mathbb{1} = \mathbb{1}^T H^T \mathbb{1}$ $\Rightarrow 2h = \frac{2n}{h} \Rightarrow$ Both conclusions we want

$\mathbb{1}^T(2h)\mathbb{1} \qquad \mathbb{1}^T\left(\frac{2n}{h}\right)\mathbb{1}$

$\square$.

Feb 12th

Theorem:
If H is a regular Hadamard matrix, then $\frac{J-H}{2}$ is the incidence matrix of a symmetric design called a Menon design, with parameters $(4h^2, 2h^2-h, h^2-h)$, $h \in \mathbb{Z}$.