4S4

Feb 8th

Theorem: For a symmetric (v,k,λ)-design, we have:

$$\underbrace{4n-1}_{\text{Related to Hadamard matrices}} \le v \le \underbrace{n^2+n+1}_{\text{either a projective plane or its complement}}$$

(where $n = k-\lambda$)

Proof:

The upper bound is achieved by projective planes and their complements. (A2GG)

For the lower bound, we have

$$v = 1 + \frac{k(k-1)}{\lambda}.$$

$$\Rightarrow v = 1 + \frac{(n+\lambda)(n+\lambda-1)}{\lambda} = \frac{n^2-n}{\lambda} + 2n + \lambda.$$

Thinking of v as a function of λ with n fixed, v is minimized when the derivative $= 0$:

$$\frac{\partial}{\partial\lambda}\left(\frac{n^2-n}{\lambda} + 2n + \lambda\right) = 0$$

$$\Rightarrow \lambda = \sqrt{n^2-n}.$$

So:

$$v \ge \frac{n^2-n}{\sqrt{n^2-n}} + 2n + \sqrt{n^2-n}.$$

$$= 2\sqrt{n^2-n} + 2n = \underbrace{\sqrt{4n^2-4n}}_{\text{Is this ever a square?}} + 2n.$$

No! Since $4n^2-4n+1 = (2n-1)^2$ is a square.

Proof (cont)

So, we can round the bound up:

$$v \geq \sqrt{4n^2-4n}+2n$$
$$\geq \sqrt{4n^2-4n+1}+2n$$
$$= (2n-1)+2n$$
$$= 4n-1.$$

$\square$

Def'n

A Hadamard design is a symmetric design in which $v=4n-1$.

Proposition:

~~[illegible]~~

The parameters of a Hadamard design are (since $v=4n-1$)

$(v,k,\lambda) = (4n-1, 2n-1, n-1)$

OR $(v,k,\lambda) = (4n-1, 2n, n)$

Proof:

Use $v = 1 + \frac{k(k-1)}{\lambda}$ with $v=4n-1$, $k=n+\lambda$ and solve for λ.

$\square$.

Examples:

(a) The Fano plane is a $(7,3,1)$-design (with $n=2$)

(b) We constructed "projective geometries" (i.e. the design from lines/hyperplanes incidence structure)

This had parameters:

$$\left(\frac{q^{d}-1}{q-1}, \frac{q^{d-1}-1}{q-1}, \frac{q^{d-2}-1}{q-1}\right). \quad q \text{ prime power}$$

Feb 5th

Examples (con't)

(b) If $q=2$, this is a Hadamard design.

Theorem:

If H is a standardized Hadamard matrix (size $4n$-by-$4n$), then:

(a) $$\frac{J+H}{2} = \begin{pmatrix} 1 & \cdots & 1 \\ \vdots & & \\ \vdots & N & \\ 1 & & \end{pmatrix}$$

where N is the incidence matrix of a $(4n-1, 2n-1, n-1)$-design.

(b) $$\frac{J-H}{2} = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & & \\ \vdots & & \\ 0 & & \end{pmatrix}$$

where N is the incidence matrix of a $(4n-1, 2n, n)$ design

These 2 designs are complements

(c) Conversely, if N is the incidence matrix of a $(4n-1, 2n-1, n-1)$-design, then:

$$2\begin{pmatrix} 1 & \cdots & 1 \\ \vdots & N & \\ 1 & & \end{pmatrix} - J$$

is a standardized ~~HM~~. HM.

(d) If N' is the IM of a $(4n-1, 2n, n)$-design, then

$$J - 2\begin{pmatrix} 0 & \cdots & 0 \\ \vdots & & \\ 0 & N' & \end{pmatrix}$$

is a standardized HM.

Proof:

We'll prove (a), the others are similar.

First note:

$$JH^T = \begin{pmatrix} 4n & 0 & \cdots & 0 \\ 4n & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 4n & 0 & \cdots & 0 \end{pmatrix}$$

→ All orthogonal to 1

All rows are the same since all rows of J are the same

Since H is standardized, every row of J is the first row of H. And, the rows of H are orthogonal.

$$HJ = \begin{pmatrix} 4n & \cdots & 4n \\ 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix}$$ (By transpose)

Now, consider:

$$\left(\frac{H+J}{2}\right)\left(\frac{H+J}{2}\right)^T = \frac{HH^T + HJ + JH^T + JJ}{4}.$$

$$\begin{pmatrix} 4n & & 0 \\ & \ddots & \\ 0 & & 4n \end{pmatrix} \leftarrow 4nI + \quad = \frac{4nI + \begin{pmatrix} 4n & \cdots & 4n \\ & 0 & \end{pmatrix} + \begin{pmatrix} 4n & & \\ \vdots & 0 & \\ 4n & & \end{pmatrix} + 4nJ}{4}.$$

$$\rightarrow \begin{pmatrix} 4n & \cdots & 4n \\ \vdots & & \vdots \\ 4n & \cdots & 4n \end{pmatrix}$$

Feb 5th

Proof (cont.):

$$= \begin{pmatrix} 4n & 2n & \cdots & \cdots & 2n \\ 2n & 2n & n & \cdots & n \\ \vdots & n & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & n \\ 2n & n & \cdots & n & 2n \end{pmatrix} = \left(\begin{array}{c|c} 4n & 2n\mathbb{1}^T \\ \hline 2n\mathbb{1} & nI + nJ \end{array}\right).$$

On the other hand:

$$\left(\frac{H+J}{2}\right)\left(\frac{H+J}{2}\right)^T$$

$$= \left(\begin{array}{c|c} 1 & \mathbb{1}^T \\ \hline \mathbb{1} & N \end{array}\right)\left(\begin{array}{c|c} 1 & \mathbb{1}^T \\ \hline \mathbb{1} & N^T \end{array}\right)$$

$$= \left(\begin{array}{c|c} 4n & \mathbb{1}^T + \mathbb{1}^T N^T \\ \hline N\mathbb{1} + \mathbb{1} & J + NN^T \end{array}\right).$$

$$\therefore \left.\begin{array}{l} N\mathbb{1} + \mathbb{1} = 2n\mathbb{1}. \\ \mathbb{1}^T + \mathbb{1}^T N^T = 2n\mathbb{1}^T. \end{array}\right\} \longrightarrow$$ These 2 are just transpose of each other, so one is redundant, we'll ~~t~~ just use the 1st and 3rd eqn.

$$nI + nJ = J + NN^T.$$

③

Proof (con't)

$$\Rightarrow N\mathbb{1} = \underbrace{(2n-1)}_{r}\mathbb{1}$$

$$NN^T = \underbrace{n}_{k-\lambda}I + \underbrace{(n-1)}_{\lambda}J$$

And these are 2 of the 3 equations that N should satisfy.

To get the 3rd equation, consider:

$$\left(\frac{H+J}{2}\right)^T\left(\frac{H+J}{2}\right)$$

and compute this in 2 ways, this will give

$$\mathbb{1}^T N = \underbrace{(2n-1)}_{k}\mathbb{1}^T$$

$$N^T N = \underbrace{n}_{k-\lambda}I + \underbrace{(n-1)}_{\lambda}J$$

Since N is a 0,1-matrix and satisfies the 3 eqs, we're done ∇

Remark:

Since there are many ways to standardize a Hadamard matrix, we get multiple designs from the same HM. These designs may not be isomorphic.

Theorem:

Let $q = 4n-1$ be a prime power (i.e. $q \equiv 3 \pmod 4$)

$$QR(q) = \{x^2 \mid x \in \underbrace{GF(q)^\times}_{\text{units of } GF(q)}\}$$

is a $(4n-1, 2n-1, n-1)$-difference set.

Feb 5th

Corollary:
If $4n-1$ is a prime power, then a $4n \times 4n$ Hadamard matrix exists.

Lemma:
Let $x \in GF(q)^\times$;

$$x \in QR(q) \iff x^{\frac{q-1}{2}} = 1$$

$$x \notin QR(q) \iff x^{\frac{q-1}{2}} = -1.$$

In particular:
- If $q \equiv 1 \pmod 4$, then $x \in QR(q) \iff -x \in QR(q)$
- If $q \equiv 3 \pmod 4$, then $x \in QR(q) \iff -x \notin QR(q)$.

Proof:
$GF(q)^\times$ is a group under multiplication of order $q-1$.
(it is also a cyclic group!)

By Cayley's theorem:
$$x^{q-1} \equiv 1 \quad \forall x \in GF(q)^\times$$
$$\Rightarrow \left(x^{\frac{q-1}{2}}\right)^2 \equiv 1$$

$$\Rightarrow \left(x^{\frac{q-1}{2}}+1\right)\left(x^{\frac{q-1}{2}}-1\right) = 0$$

$$\Rightarrow x^{\frac{q-1}{2}} \equiv \pm 1$$

If $x \in QR(q)$. Then $x = a^2$ for some $a \in GF(q)$, so
$$x^{\frac{q-1}{2}} = (a^2)^{\frac{q-1}{2}} = a^{q-1} \equiv 1$$

$\Leftarrow$

Proof (cont'd) ⊛

Note that $x^{\frac{q-1}{2}} = 1$ is a polynomial eqn of degree $\frac{q-1}{2}$.
Therefore, it can have at most $\frac{q-1}{2}$ solutions.

Claim: $|QR(q)| = \frac{q-1}{2}$

Proof:

The squaring map $\varphi: GF(q)^\times \to QR(q)$ is two-to-one,
$$a \mapsto a^2$$
because $\varphi^{-1}(b) = \{x \in GF(q)^\times \mid x^2 = b\}$

↳ Quadratic, thus has 2 sols, $\pm\sqrt{x}$. □

Since ⊛ has as many solutions as there are quadratic residues, the quadratic residues are the only solutions.

$\therefore$ If $x \notin QR(q)$, then $x^{\frac{q-1}{2}} \not\equiv 1 \Rightarrow x^{\frac{q-1}{2}} \equiv -1$. (since $x^{\frac{q-1}{2}} \equiv \pm 1$)

Finally, if $q \equiv 1 \pmod 4$, then $x^{\frac{q-1}{2}} \equiv (-x)^{\frac{q-1}{2}} \Leftrightarrow x \in QR(q)$

$\Leftrightarrow -x \in QR(q)$

And if $q \equiv 3 \pmod 4$, $x^{\frac{q-1}{2}} \equiv -(-x)^{\frac{q-1}{2}} \Leftrightarrow x \in QR(q)$

$\Leftrightarrow -x \notin QR(q)$

□.

Scanned with CamScanner