Critical cases of circulant partial Hadamard matrices

R. Craigen
Dept of Mathematics
University of Manitoba

PMDW 2016

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

Circulant partial Hadamard matrices

Circulant partial Hadamard matrices

A matrix $A \in \mathbb{R}^{m \times n}$ is **circulant** if each row after the first is a right cyclic shift of its predecessor by 1 position.

Circulant partial Hadamard matrices

A matrix $A \in \mathbb{R}^{m \times n}$ is **circulant** if each row after the first is a right cyclic shift of its predecessor by 1 position.

EG: Writing $A = \mathrm{circ}_m(a_1, \ldots, a_n)$

Circulant partial Hadamard matrices

A matrix $A \in \mathbb{R}^{m \times n}$ is **circulant** if each row after the first is a right cyclic shift of its predecessor by 1 position.

EG: Writing $A = \mathrm{circ}_m(a_1, \ldots, a_n)$,

$$\mathrm{circ}_2(a, b, c) = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}$$

Circulant partial Hadamard matrices

A matrix $A \in \mathbb{R}^{m \times n}$ is **circulant** if each row after the first is a right cyclic shift of its predecessor by 1 position.

EG: Writing $A = \mathrm{circ}_m(a_1, \dots, a_n)$,

$$\mathrm{circ}_2(a, b, c) = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}, \mathrm{circ}_3(a, b) = \begin{pmatrix} a & b \\ b & a \\ a & b \end{pmatrix}$$

Circulant partial Hadamard matrices

A matrix $A \in \mathbb{R}^{m \times n}$ is **circulant** if each row after the first is a right cyclic shift of its predecessor by 1 position.

EG: Writing $A = \mathrm{circ}_m(a_1, \ldots, a_n)$,

$$\mathrm{circ}_2(a, b, c) = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}, \mathrm{circ}_3(a, b) = \begin{pmatrix} a & b \\ b & a \\ a & b \end{pmatrix}$$

A *circulant partial Hadamard matrix* is a (rectangular) circulant matrix $H \in \{\pm 1\}^{k \times n}$

Circulant partial Hadamard matrices

A matrix $A \in \mathbb{R}^{m \times n}$ is **circulant** if each row after the first is a right cyclic shift of its predecessor by 1 position.

EG: Writing $A = \mathrm{circ}_m(a_1, \ldots, a_n)$,

$$\mathrm{circ}_2(a, b, c) = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}, \mathrm{circ}_3(a, b) = \begin{pmatrix} a & b \\ b & a \\ a & b \end{pmatrix}$$

A *circulant partial Hadamard matrix* is a (rectangular) circulant matrix $H \in \{\pm 1\}^{k \times n}$ satisfying

$$HH^\top = nI_k.$$

Circulant partial Hadamard matrices

A matrix $A \in \mathbb{R}^{m \times n}$ is **circulant** if each row after the first is a right cyclic shift of its predecessor by 1 position.

EG: Writing $A = \mathrm{circ}_m(a_1, \ldots, a_n)$,

$$\mathrm{circ}_2(a, b, c) = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}, \mathrm{circ}_3(a, b) = \begin{pmatrix} a & b \\ b & a \\ a & b \end{pmatrix}$$

A *circulant partial Hadamard matrix* is a (rectangular) circulant matrix $H \in \{\pm 1\}^{k \times n}$ satisfying

$$HH^\top = nI_k.$$

A third parameter r gives the sum along the first row of H.

Circulant partial Hadamard matrices

A matrix $A \in \mathbb{R}^{m \times n}$ is **circulant** if each row after the first is a right cyclic shift of its predecessor by 1 position.

EG: Writing $A = \mathrm{circ}_m(a_1, \ldots, a_n)$,

$$\mathrm{circ}_2(a, b, c) = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}, \mathrm{circ}_3(a, b) = \begin{pmatrix} a & b \\ b & a \\ a & b \end{pmatrix}$$

A *circulant partial Hadamard matrix* is a (rectangular) circulant matrix $H \in \{\pm 1\}^{k \times n}$ satisfying

$$HH^\top = nI_k.$$

A third parameter r gives the sum along the first row of H.

We denote such H by r-$H(k \times n)$.

Examples

The title slide displays a 0-$H(7 \times 16)$

Examples

The title slide displays a $0\text{-}H(7 \times 16)$

$0\text{-}H(2 \times 4)$:

Examples

The title slide displays a 0-$H(7 \times 16)$

0-$H(2 \times 4)$: $\quad \mathrm{circ}_{2\times 4}(11--) = \begin{pmatrix} 1 & 1 & - & - \\ - & 1 & 1 & - \end{pmatrix}$

Examples

The title slide displays a 0-$H(7 \times 16)$

0-$H(2 \times 4)$: $\mathrm{circ}_{2\times 4}(11--) = \begin{pmatrix} 1 & 1 & - & - \\ - & 1 & 1 & - \end{pmatrix}$

0-$H(3 \times 8)$:

Examples

The title slide displays a 0-$H(7 \times 16)$

0-$H(2 \times 4)$: $\mathrm{circ}_{2\times 4}(11--) = \begin{pmatrix} 1 & 1 & - & - \\ - & 1 & 1 & - \end{pmatrix}$

0-$H(3 \times 8)$: $\mathrm{circ}_{3\times 8}(111-1---)$

Examples

The title slide displays a 0-$H(7 \times 16)$

0-$H(2 \times 4)$: $\mathrm{circ}_{2\times 4}(11--) = \begin{pmatrix} 1 & 1 & - & - \\ - & 1 & 1 & - \end{pmatrix}$

0-$H(3 \times 8)$: $\mathrm{circ}_{3\times 8}(111-1---)$

2-$H(4 \times 8)$:

Examples

The title slide displays a 0-$H(7 \times 16)$

0-$H(2 \times 4)$: $\mathrm{circ}_{2\times 4}(11--) = \begin{pmatrix} 1 & 1 & - & - \\ - & 1 & 1 & - \end{pmatrix}$

0-$H(3 \times 8)$: $\mathrm{circ}_{3\times 8}(111-1---)$

2-$H(4 \times 8)$: $\mathrm{circ}_{4\times 8}(1-1111--)$

Examples

The title slide displays a 0-$H(7 \times 16)$

0-$H(2 \times 4)$: $\mathrm{circ}_{2\times 4}(11--) = \begin{pmatrix} 1 & 1 & - & - \\ - & 1 & 1 & - \end{pmatrix}$

0-$H(3 \times 8)$: $\mathrm{circ}_{3\times 8}(111-1---)$

2-$H(4 \times 8)$: $\mathrm{circ}_{4\times 8}(1-1111--)$

4-$H(4 \times 8)$:

Examples

The title slide displays a 0-$H(7 \times 16)$

0-$H(2 \times 4)$: $$\mathrm{circ}_{2\times4}(11--) = \begin{pmatrix} 1 & 1 & - & - \\ - & 1 & 1 & - \end{pmatrix}$$

0-$H(3 \times 8)$: $$\mathrm{circ}_{3\times8}(111-1---)$$

2-$H(4 \times 8)$: $$\mathrm{circ}_{4\times8}(1-1111--)$$

4-$H(4 \times 8)$: $$\mathrm{circ}_{4\times8}(-111-111)$$

Applications

The study of CPHs arose out of a basic question in stream cypher cryptography

Applications

The study of CPHs arose out of a basic question in stream cypher cryptography

An application has arisen in relation to study of fMRI technology (Lin et al 2017, Statistica Sinica

Ryser's Conjecture about circulant Hadamard matrices

Obs: If $k = n$, then $H = r\text{-}H(k \times n)$

Ryser's Conjecture about circulant Hadamard matrices

Obs: If $k = n$, then $H = r\text{-}H(k \times n) = r\text{-}H(n \times n)$

Ryser's Conjecture about circulant Hadamard matrices

Obs: If $k = n$, then $H = r\text{-}H(k \times n) = r\text{-}H(n \times n)$ would be a *circulant* Hadamard matrix of order n

Ryser's Conjecture about circulant Hadamard matrices

Obs: If $k = n$, then $H = r\text{-}H(k \times n) = r\text{-}H(n \times n)$ would be a *circulant* Hadamard matrix of order n, $H = H(n)$.

Ryser's Conjecture about circulant Hadamard matrices

Obs: If $k = n$, then $H = r\text{-}H(k \times n) = r\text{-}H(n \times n)$ would be a *circulant* Hadamard matrix of order n, $H = H(n)$.

Conjecture(Ryser): If $n > 4$ then there is no circulant $H(n)$.

Ryser's Conjecture about circulant Hadamard matrices

Obs: If $k = n$, then $H = r\text{-}H(k \times n) = r\text{-}H(n \times n)$ would be a *circulant* Hadamard matrix of order n, $H = H(n)$.

Conjecture(Ryser): If $n > 4$ then there is no circulant $H(n)$.

Verified to $n = 548,964,900$

Ryser's Conjecture about circulant Hadamard matrices

Obs: If $k = n$, then $H = r\text{-}H(k \times n) = r\text{-}H(n \times n)$ would be a *circulant* Hadamard matrix of order n, $H = H(n)$.

Conjecture(Ryser): If $n > 4$ then there is no circulant $H(n)$.

Verified to $n = 548,964,900$ and for $n < 10^{11}$ with at most 3 exceptions (Schmidt).

Ryser's Conjecture about circulant Hadamard matrices

Obs: If $k = n$, then $H = r\text{-}H(k \times n) = r\text{-}H(n \times n)$ would be a *circulant* Hadamard matrix of order n, $H = H(n)$.

Conjecture(Ryser): If $n > 4$ then there is no circulant $H(n)$.

Verified to $n = 548,964,900$ and for $n < 10^{11}$ with at most 3 exceptions (Schmidt).

There is a circulant $H(n, 4)$

Ryser's Conjecture about circulant Hadamard matrices

Obs: If $k = n$, then $H = r\text{-}H(k \times n) = r\text{-}H(n \times n)$ would be a *circulant* Hadamard matrix of order n, $H = H(n)$.

Conjecture(Ryser): If $n > 4$ then there is no circulant $H(n)$.

Verified to $n = 548,964,900$ and for $n < 10^{11}$ with at most 3 exceptions (Schmidt).

There is a circulant $H(n, 4)$

$$H = \mathrm{circ}(-111) = \begin{pmatrix} - & 1 & 1 & 1 \\ 1 & - & 1 & 1 \\ 1 & 1 & - & 1 \\ 1 & 1 & 1 & - \end{pmatrix}$$

Row sum $r = 2$.

Ryser's Conjecture about circulant Hadamard matrices

Obs: If $k = n$, then $H = r\text{-}H(k \times n) = r\text{-}H(n \times n)$ would be a *circulant* Hadamard matrix of order n, $H = H(n)$.

Conjecture(Ryser): If $n > 4$ then there is no circulant $H(n)$.

Verified to $n = 548,964,900$ and for $n < 10^{11}$ with at most 3 exceptions (Schmidt).

There is a circulant $H(n,4)$

$$H = \mathrm{circ}(-111) = \begin{pmatrix} - & 1 & 1 & 1 \\ 1 & - & 1 & 1 \\ 1 & 1 & - & 1 \\ 1 & 1 & 1 & - \end{pmatrix}$$

Row sum $r = 2$. So this is a $2\text{-}H(4 \times 4)$.

Heuristic approach to Ryser's conjecture

- $H = H(n)$, circulant

Heuristic approach to Ryser's conjecture

- $H = H(n)$, circulant with row-sum r

Heuristic approach to Ryser's conjecture

- $H = H(n)$, circulant with row-sum r
  $\Rightarrow \forall k \leq n$,

Heuristic approach to Ryser's conjecture

- $H = H(n)$, circulant with row-sum r
  $\Rightarrow \forall k \leq n, r\text{-}H(k \times n)$ exists

Heuristic approach to Ryser's conjecture

- $H = H(n)$, circulant with row-sum r
  $\Rightarrow \forall k \leq n, r\text{-}H(k \times n)$ exists (in particular $k = \frac{n}{2}$)

Heuristic approach to Ryser's conjecture

- $H = H(n)$, circulant with row-sum r
  $\Rightarrow \forall k \leq n, r\text{-}H(k \times n)$ exists (in particular $k = \frac{n}{2}$)
- Easy to show: $r = \sqrt{n}$.

Heuristic approach to Ryser's conjecture

- $H = H(n)$, circulant with row-sum r
  $\Rightarrow \forall k \leq n, r\text{-}H(k \times n)$ exists (in particular $k = \frac{n}{2}$)
- Easy to show: $r = \sqrt{n}$.
- So circulant $H(n)$

Heuristic approach to Ryser's conjecture

- $H = H(n)$, circulant with row-sum r
  $\Rightarrow \forall k \leq n, r\text{-}H(k \times n)$ exists (in particular $k = \frac{n}{2}$)
- Easy to show: $r = \sqrt{n}$.
- So circulant $H(n) \Rightarrow \sqrt{n}\text{-}H(\frac{n}{2} \times n)$.

Heuristic approach to Ryser's conjecture

- $H = H(n)$, circulant with row-sum r
  $\Rightarrow \forall k \leq n, r\text{-}H(k \times n)$ exists (in particular $k = \frac{n}{2}$)
- Easy to show: $r = \sqrt{n}$.
- So circulant $H(n) \Rightarrow \sqrt{n}\text{-}H(\frac{n}{2} \times n)$. **(Necessary condition)**

Heuristic approach to Ryser's conjecture

- $H = H(n)$, circulant with row-sum r
  $\Rightarrow \forall k \leq n, r\text{-}H(k \times n)$ exists (in particular $k = \frac{n}{2}$)
- Easy to show: $r = \sqrt{n}$.
- So circulant $H(n) \Rightarrow \sqrt{n}\text{-}H(\frac{n}{2} \times n)$. **(Necessary condition)**
- How common are $r\text{-}H(\frac{n}{2} \times n)$?

Heuristic approach to Ryser's conjecture

- $H = H(n)$, circulant with row-sum r
  $\Rightarrow \forall k \leq n, r\text{-}H(k \times n)$ exists (in particular $k = \frac{n}{2}$)
- Easy to show: $r = \sqrt{n}$.
- So circulant $H(n) \Rightarrow \sqrt{n}\text{-}H(\frac{n}{2} \times n)$. **(Necessary condition)**
- How common are $r\text{-}H(\frac{n}{2} \times n)$? And can we have $r \approx \sqrt{n}$?

Heuristic approach to Ryser's conjecture

- $H = H(n)$, circulant with row-sum r
  $\Rightarrow \forall k \leq n, r\text{-}H(k \times n)$ exists (in particular $k = \frac{n}{2}$)
- Easy to show: $r = \sqrt{n}$.
- So circulant $H(n) \Rightarrow \sqrt{n}\text{-}H(\frac{n}{2} \times n)$. **(Necessary condition)**
- How common are $r\text{-}H(\frac{n}{2} \times n)$? And can we have $r \approx \sqrt{n}$?
- Infinitely many $2\text{-}H(\frac{n}{2} \times n)$ are known.

Heuristic approach to Ryser's conjecture

- $H = H(n)$, circulant with row-sum r
  $\Rightarrow \forall k \leq n, r\text{-}H(k \times n)$ exists (in particular $k = \frac{n}{2}$)
- Easy to show: $r = \sqrt{n}$.
- So circulant $H(n) \Rightarrow \sqrt{n}\text{-}H(\frac{n}{2} \times n)$. **(Necessary condition)**
- How common are $r\text{-}H(\frac{n}{2} \times n)$? And can we have $r \approx \sqrt{n}$?
- Infinitely many $2\text{-}H(\frac{n}{2} \times n)$ are known. $(n = 2(p^t + 1))$

Heuristic approach to Ryser's conjecture

- $H = H(n)$, circulant with row-sum r
  $\Rightarrow \forall k \leq n, r\text{-}H(k \times n)$ exists (in particular $k = \frac{n}{2}$)
- Easy to show: $r = \sqrt{n}$.
- So circulant $H(n) \Rightarrow \sqrt{n}\text{-}H(\frac{n}{2} \times n)$. **(Necessary condition)**
- How common are $r\text{-}H(\frac{n}{2} \times n)$? And can we have $r \approx \sqrt{n}$?
- Infinitely many $2\text{-}H(\frac{n}{2} \times n)$ are known. $(n = 2(p^t + 1))$
- There are three known $4\text{-}H(\frac{n}{2} \times n)$.

Heuristic approach to Ryser's conjecture

- $H = H(n)$, circulant with row-sum r
  $\Rightarrow \forall k \leq n, r\text{-}H(k \times n)$ exists (in particular $k = \frac{n}{2}$)
- Easy to show: $r = \sqrt{n}$.
- So circulant $H(n) \Rightarrow \sqrt{n}\text{-}H(\frac{n}{2} \times n)$. **(Necessary condition)**
- How common are $r\text{-}H(\frac{n}{2} \times n)$? And can we have $r \approx \sqrt{n}$?
- Infinitely many $2\text{-}H(\frac{n}{2} \times n)$ are known. $(n = 2(p^t + 1))$
- There are three known $4\text{-}H(\frac{n}{2} \times n)$. $(n = 8, 12, 28)$

Heuristic approach to Ryser's conjecture

- $H = H(n)$, circulant with row-sum r
  $\Rightarrow \forall k \leq n, r\text{-}H(k \times n)$ exists (in particular $k = \frac{n}{2}$)
- Easy to show: $r = \sqrt{n}$.
- So circulant $H(n) \Rightarrow \sqrt{n}\text{-}H(\frac{n}{2} \times n)$. **(Necessary condition)**
- How common are $r\text{-}H(\frac{n}{2} \times n)$? And can we have $r \approx \sqrt{n}$?
- Infinitely many $2\text{-}H(\frac{n}{2} \times n)$ are known. $(n = 2(p^t + 1))$
- There are three known $4\text{-}H(\frac{n}{2} \times n)$. $(n = 8, 12, 28)$
- Thus far no $r\text{-}H(\frac{n}{2} \times n)$ are known with $r > 4$.

Heuristic approach to Ryser's conjecture

- $H = H(n)$, circulant with row-sum r
  $\Rightarrow \forall k \leq n, r\text{-}H(k \times n)$ exists (in particular $k = \frac{n}{2}$)
- Easy to show: $r = \sqrt{n}$.
- So circulant $H(n) \Rightarrow \sqrt{n}\text{-}H(\frac{n}{2} \times n)$. **(Necessary condition)**
- How common are $r\text{-}H(\frac{n}{2} \times n)$? And can we have $r \approx \sqrt{n}$?
- Infinitely many $2\text{-}H(\frac{n}{2} \times n)$ are known. $(n = 2(p^t + 1))$
- There are three known $4\text{-}H(\frac{n}{2} \times n)$. $(n = 8, 12, 28)$
- Thus far no $r\text{-}H(\frac{n}{2} \times n)$ are known with $r > 4$.
- Much empirical evidence suggests that, for large n,

Heuristic approach to Ryser's conjecture

- $H = H(n)$, circulant with row-sum r
  $\Rightarrow \forall k \leq n, r\text{-}H(k \times n)$ exists (in particular $k = \frac{n}{2}$)
- Easy to show: $r = \sqrt{n}$.
- So circulant $H(n) \Rightarrow \sqrt{n}\text{-}H(\frac{n}{2} \times n)$. **(Necessary condition)**
- How common are $r\text{-}H(\frac{n}{2} \times n)$? And can we have $r \approx \sqrt{n}$?
- Infinitely many $2\text{-}H(\frac{n}{2} \times n)$ are known. $(n = 2(p^t + 1))$
- There are three known $4\text{-}H(\frac{n}{2} \times n)$. $(n = 8, 12, 28)$
- Thus far no $r\text{-}H(\frac{n}{2} \times n)$ are known with $r > 4$.
- Much empirical evidence suggests that, for large n, $r \ll \sqrt{n}$

Heuristic approach to Ryser's conjecture

- $H = H(n)$, circulant with row-sum r
  $\Rightarrow \forall k \leq n, r\text{-}H(k \times n)$ exists (in particular $k = \frac{n}{2}$)
- Easy to show: $r = \sqrt{n}$.
- So circulant $H(n) \Rightarrow \sqrt{n}\text{-}H(\frac{n}{2} \times n)$. **(Necessary condition)**
- How common are $r\text{-}H(\frac{n}{2} \times n)$? And can we have $r \approx \sqrt{n}$?
- Infinitely many $2\text{-}H(\frac{n}{2} \times n)$ are known. $(n = 2(p^t + 1))$
- There are three known $4\text{-}H(\frac{n}{2} \times n)$. $(n = 8, 12, 28)$
- Thus far no $r\text{-}H(\frac{n}{2} \times n)$ are known with $r > 4$.
- Much empirical evidence suggests that, for large n, $r \ll \sqrt{n}$
- Since we apparently cannot even approach the above necessary condition,

Heuristic approach to Ryser's conjecture

- $H = H(n)$, circulant with row-sum r
  $\Rightarrow \forall k \leq n, r\text{-}H(k \times n)$ exists (in particular $k = \frac{n}{2}$)
- Easy to show: $r = \sqrt{n}$.
- So circulant $H(n) \Rightarrow \sqrt{n}\text{-}H(\frac{n}{2} \times n)$. **(Necessary condition)**
- How common are $r\text{-}H(\frac{n}{2} \times n)$? And can we have $r \approx \sqrt{n}$?
- Infinitely many $2\text{-}H(\frac{n}{2} \times n)$ are known. $(n = 2(p^t + 1))$
- There are three known $4\text{-}H(\frac{n}{2} \times n)$. $(n = 8, 12, 28)$
- Thus far no $r\text{-}H(\frac{n}{2} \times n)$ are known with $r > 4$.
- Much empirical evidence suggests that, for large n, $r \ll \sqrt{n}$
- Since we apparently cannot even approach the above necessary condition, failure of Ryser's conjecture is unlikely

Heuristic approach to Ryser's conjecture

- $H = H(n)$, circulant with row-sum r
  $\Rightarrow \forall k \leq n, r\text{-}H(k \times n)$ exists (in particular $k = \frac{n}{2}$)
- Easy to show: $r = \sqrt{n}$.
- So circulant $H(n) \Rightarrow \sqrt{n}\text{-}H(\frac{n}{2} \times n)$. **(Necessary condition)**
- How common are $r\text{-}H(\frac{n}{2} \times n)$? And can we have $r \approx \sqrt{n}$?
- Infinitely many $2\text{-}H(\frac{n}{2} \times n)$ are known. $(n = 2(p^t + 1))$
- There are three known $4\text{-}H(\frac{n}{2} \times n)$. $(n = 8, 12, 28)$
- Thus far no $r\text{-}H(\frac{n}{2} \times n)$ are known with $r > 4$.
- Much empirical evidence suggests that, for large n, $r \ll \sqrt{n}$
- Since we apparently cannot even approach the above necessary condition, failure of Ryser's conjecture is unlikely—even a near counterexample is improbable!

A relation between r, k, n

A relation between r, k, n

Theorem: $r\sqrt{k} \leq n$

A relation between r, k, n

Theorem: $r\sqrt{k} \leq n$
Sketch: $c_1, \ldots, c_n$ columns of H.

A relation between r, k, n

Theorem: $r\sqrt{k} \leq n$
Sketch: $c_1, \ldots, c_n$ columns of H.

Sum of entries: $c_1 + \cdots + c_n = E_k H E_n^\top = rk$.

A relation between r, k, n

Theorem: $r\sqrt{k} \leq n$
Sketch: $c_1, \ldots, c_n$ columns of H.

Sum of entries: $c_1 + \cdots + c_n = E_k H E_n^\top = rk$.

Examine row sums of $HH^\top = kI$ two ways, gives $\sum c_i^2 = kn$

A relation between r, k, n

Theorem: $r\sqrt{k} \leq n$
Sketch: $c_1, \ldots, c_n$ columns of H.

Sum of entries: $c_1 + \cdots + c_n = E_k H E_n^\top = rk$.

Examine row sums of $HH^\top = kI$ two ways, gives $\sum c_i^2 = kn$

Cauchy-Schwartz inequality to vectors $(1\ 1\ \cdots\ 1)_k H$ and $(1\ 1\ \cdots\ 1)_n$ gives the relation. $\square$

Easy to show: If $r\sqrt{k} = n$ then $k|n$ and $H = (K \mid K \mid \cdots \mid K)$

A relation between r, k, n

Theorem: $r\sqrt{k} \leq n$
Sketch: $c_1, \ldots, c_n$ columns of H.

Sum of entries: $c_1 + \cdots + c_n = E_k H E_n^\top = rk$.

Examine row sums of $HH^\top = kI$ two ways, gives $\sum c_i^2 = kn$

Cauchy-Schwartz inequality to vectors $(1\ 1\ \cdots\ 1)_k H$ and $(1\ 1\ \cdots\ 1)_n$ gives the relation. $\square$

Easy to show: If $r\sqrt{k} = n$ then $k|n$ and $H = (K \mid K \mid \cdots \mid K)$ ($\frac{n}{k}$ copies of a circulant $H(k)$).

A relation between r, k, n

Theorem: $r\sqrt{k} \leq n$
Sketch: $c_1, \ldots, c_n$ columns of H.

Sum of entries: $c_1 + \cdots + c_n = E_k H E_n^\top = rk$.

Examine row sums of $HH^\top = kI$ two ways, gives $\sum c_i^2 = kn$

Cauchy-Schwartz inequality to vectors $(1\ 1\ \cdots\ 1)_k H$ and $(1\ 1\ \cdots\ 1)_n$ gives the relation. $\square$

Easy to show: If $r\sqrt{k} = n$ then $k|n$ and $H = (K \mid K \mid \cdots \mid K)$ ($\frac{n}{k}$ copies of a circulant $H(k)$).

So modulo Ryser's conjecture, equality is impossible, $k > 4$.

A relation between r, k, n

Theorem: $r\sqrt{k} \leq n$
Sketch: $c_1, \ldots, c_n$ columns of H.
Sum of entries: $c_1 + \cdots + c_n = E_k H E_n^\top = rk$.
Examine row sums of $HH^\top = kI$ two ways, gives $\sum c_i^2 = kn$
Cauchy-Schwartz inequality to vectors $(1\ 1\ \cdots\ 1)_k H$ and $(1\ 1\ \cdots\ 1)_n$ gives the relation. $\square$

Easy to show: If $r\sqrt{k} = n$ then $k|n$ and $H = (K \mid K \mid \cdots \mid K)$ ($\frac{n}{k}$ copies of a circulant $H(k)$).

So modulo Ryser's conjecture, equality is impossible, $k > 4$.

So $k \leq \left(\frac{n}{r}\right)^2$. What if $c = \frac{n}{r}$, $k = c^2 - 1$?

A relation between r, k, n

Theorem: $r\sqrt{k} \leq n$
Sketch: $c_1, \ldots, c_n$ columns of H.

Sum of entries: $c_1 + \cdots + c_n = E_k H E_n^\top = rk$.

Examine row sums of $HH^\top = kI$ two ways, gives $\sum c_i^2 = kn$

Cauchy-Schwartz inequality to vectors $(1\ 1\ \cdots\ 1)_k H$ and $(1\ 1\ \cdots\ 1)_n$ gives the relation. $\square$

Easy to show: If $r\sqrt{k} = n$ then $k|n$ and $H = (K \mid K \mid \cdots \mid K)$ ($\frac{n}{k}$ copies of a circulant $H(k)$).

So modulo Ryser's conjecture, equality is impossible, $k > 4$.

So $k \leq \left(\frac{n}{r}\right)^2$. What if $c = \frac{n}{r}$, $k = c^2 - 1$?

Theorem If $H = r$-$H((c^2-1) \times cr)$, then the only possible column sums of H are:

A relation between r, k, n

Theorem: $r\sqrt{k} \leq n$
Sketch: $c_1, \ldots, c_n$ columns of H.

Sum of entries: $c_1 + \cdots + c_n = E_k H E_n^\top = rk$.

Examine row sums of $HH^\top = kI$ two ways, gives $\sum c_i^2 = kn$

Cauchy-Schwartz inequality to vectors $(1\ 1\ \cdots\ 1)_k H$ and $(1\ 1\ \cdots\ 1)_n$ gives the relation. $\square$

Easy to show: If $r\sqrt{k} = n$ then $k|n$ and $H = (K \mid K \mid \cdots \mid K)$ ($\frac{n}{k}$ copies of a circulant $H(k)$).

So modulo Ryser's conjecture, equality is impossible, $k > 4$.

So $k \leq \left(\frac{n}{r}\right)^2$. What if $c = \frac{n}{r}$, $k = c^2 - 1$?

Theorem If $H = r\text{-}H((c^2 - 1) \times cr)$, then the only possible column sums of H are: $c - 1$ $(\frac{r(c+1)}{2} \times)$

A relation between r, k, n

Theorem: $r\sqrt{k} \leq n$
Sketch: $c_1, \ldots, c_n$ columns of H.
Sum of entries: $c_1 + \cdots + c_n = E_k H E_n^\top = rk$.
Examine row sums of $HH^\top = kI$ two ways, gives $\sum c_i^2 = kn$
Cauchy-Schwartz inequality to vectors $(1\ 1\ \cdots\ 1)_k H$ and $(1\ 1\ \cdots\ 1)_n$ gives the relation. $\square$

Easy to show: If $r\sqrt{k} = n$ then $k|n$ and $H = (K \mid K \mid \cdots \mid K)$ ($\frac{n}{k}$ copies of a circulant $H(k)$).

So modulo Ryser's conjecture, equality is impossible, $k > 4$.

So $k \leq \left(\frac{n}{r}\right)^2$. What if $c = \frac{n}{r}$, $k = c^2 - 1$?

Theorem If $H = r\text{-}H((c^2-1) \times cr)$, then the only possible column sums of H are: $c - 1$ ($\frac{r(c+1)}{2}\times$) and $c + 1$ ($\frac{r(c-1)}{2}\times$)

What if $\frac{n}{r}$ is not an integer?

What if $\frac{n}{r}$ is not an integer?

The case

$$n = cr, k = c^2 - 1, c \in \mathbb{Z}$$

gives special structure

What if $\frac{n}{r}$ is not an integer?

The case

$$n = cr, k = c^2 - 1, c \in \mathbb{Z}$$

gives special structure because it approaches the bound $r\sqrt{k} \leq n$.

What if $\frac{n}{r}$ is not an integer?

The case

$$n = cr, k = c^2 - 1, c \in \mathbb{Z}$$

gives special structure because it approaches the bound $r\sqrt{k} \leq n$.

The condition $c \in \mathbb{Z}$ is constricting

What if $\frac{n}{r}$ is not an integer?

The case

$$n = cr, k = c^2 - 1, c \in \mathbb{Z}$$

gives special structure because it approaches the bound $r\sqrt{k} \leq n$.

The condition $c \in \mathbb{Z}$ is constricting.

Can't we just say $|k - c^2| \leq 1$?

What if $\frac{n}{r}$ is not an integer?

The case

$$n = cr, k = c^2 - 1, c \in \mathbb{Z}$$

gives special structure because it approaches the bound $r\sqrt{k} \leq n$.

The condition $c \in \mathbb{Z}$ is constricting.

Can't we just say $|k - c^2| \leq 1$?

But there is a sensitive balance in how parameters force exactly two column sums.

What if $\frac{n}{r}$ is not an integer?

The case

$$n = cr, k = c^2 - 1, c \in \mathbb{Z}$$

gives special structure because it approaches the bound $r\sqrt{k} \leq n$.

The condition $c \in \mathbb{Z}$ is constricting.

Can't we just say $|k - c^2| \leq 1$?

But there is a sensitive balance in how parameters force exactly two column sums.

Could there be <u>other</u> exact conditions on c, r, n approaching $r\sqrt{k} \leq n$ and forcing similar structure?

What if $\frac{n}{r}$ is not an integer?

The case

$$n = cr, k = c^2 - 1, c \in \mathbb{Z}$$

gives special structure because it approaches the bound $r\sqrt{k} \leq n$.

The condition $c \in \mathbb{Z}$ is constricting.

Can't we just say $|k - c^2| \leq 1$?

But there is a sensitive balance in how parameters force exactly two column sums.

Could there be <u>other</u> exact conditions on c, r, n approaching $r\sqrt{k} \leq n$ and forcing similar structure?

Initial attempts proved fruitless.

A successful approach

Parity turns out to be a critical issue in locating cases with threshold behaviour

A successful approach

Parity turns out to be a critical issue in locating cases with threshold behaviour

Suppose $\exists r\text{-}H(k \times n)$.

A successful approach

Parity turns out to be a critical issue in locating cases with threshold behaviour

Suppose $\exists r\text{-}H(k \times n)$.

Write

$$\frac{kr}{n} = m + \delta$$

A successful approach

Parity turns out to be a critical issue in locating cases with threshold behaviour

Suppose $\exists r\text{-}H(k \times n)$.

Write

$$\frac{kr}{n} = m + \delta$$

where

1. $m \in \mathbb{Z}$

A successful approach

Parity turns out to be a critical issue in locating cases with threshold behaviour

Suppose $\exists r\text{-}H(k \times n)$.

Write

$$\frac{kr}{n} = m + \delta$$

where

1. $m \in \mathbb{Z}$;
2. m and k have opposite parity

A successful approach

Parity turns out to be a critical issue in locating cases with threshold behaviour

Suppose $\exists r\text{-}H(k \times n)$.

Write

$$\frac{kr}{n} = m + \delta$$

where

1. $m \in \mathbb{Z}$;
2. m and k have opposite parity; and
3. $\delta \in [-1, 1)$.

A successful approach

Parity turns out to be a critical issue in locating cases with threshold behaviour

Suppose $\exists r\text{-}H(k \times n)$.

Write

$$\frac{kr}{n} = m + \delta$$

where

1. $m \in \mathbb{Z}$;
2. m and k have opposite parity; and
3. $\delta \in [-1, 1)$.

Observe:

1. m and δ are uniquely determined by r, k, n

A successful approach

Parity turns out to be a critical issue in locating cases with threshold behaviour

Suppose $\exists r\text{-}H(k \times n)$.

Write

$$\frac{kr}{n} = m + \delta$$

where

1. $m \in \mathbb{Z}$;
2. m and k have opposite parity; and
3. $\delta \in [-1, 1)$.

Observe:

1. m and δ are uniquely determined by r, k, n;
2. If $\frac{n}{r} = c \in \mathbb{Z}$, $k = c^2 - 1$ then $m = c, \delta = \frac{1}{c}$

A successful approach

Parity turns out to be a critical issue in locating cases with threshold behaviour

Suppose $\exists r\text{-}H(k \times n)$.

Write

$$\frac{kr}{n} = m + \delta$$

where

1. $m \in \mathbb{Z}$;
2. m and k have opposite parity; and
3. $\delta \in [-1, 1)$.

Observe:

1. m and δ are uniquely determined by r, k, n;
2. If $\frac{n}{r} = c \in \mathbb{Z}$, $k = c^2 - 1$ then $m = c, \delta = \frac{1}{c}$ (except when $c = 1$ which is impossible if $k > 1$)

Column sum relations

For $i \in \{-k, -k+1, \ldots, k-1, k\}$:

put b_i for # of columns of H with sum i.

Column sum relations

For $i \in \{-k, -k+1, \ldots, k-1, k\}$:
put b_i for # of columns of H with sum i.

For $1 \leq i \leq k$ write $a_i = b_i + b_{-i}$ and $a_0 = b_0$.

Column sum relations

For $i \in \{-k, -k+1, \ldots, k-1, k\}$:

put b_i for $\#$ of columns of H with sum i.

For $1 \leq i \leq k$ write $a_i = b_i + b_{-i}$ and $a_0 = b_0$.Then

$$\sum_{i=0}^{k} a_i = n$$

Column sum relations

For $i \in \{-k, -k+1, \ldots, k-1, k\}$:

put b_i for # of columns of H with sum i.

For $1 \leq i \leq k$ write $a_i = b_i + b_{-i}$ and $a_0 = b_0$.Then

$$\sum_{i=0}^{k} a_i = n, \tag{A}$$

and our sum of column squares result may be written

Column sum relations

For $i \in \{-k, -k+1, \ldots, k-1, k\}$:

put b_i for $\#$ of columns of H with sum i.

For $1 \leq i \leq k$ write $a_i = b_i + b_{-i}$ and $a_0 = b_0$.Then

$$\sum_{i=0}^{k} a_i = n, \tag{A}$$

and our sum of column squares result may be written

$$\sum_{i=0}^{k} i^2 a_i = nk \tag{B}$$

Column sum relations

For $i \in \{-k, -k+1, \ldots, k-1, k\}$:

put b_i for # of columns of H with sum i.

For $1 \leq i \leq k$ write $a_i = b_i + b_{-i}$ and $a_0 = b_0$.Then

$$\sum_{i=0}^{k} a_i = n, \tag{A}$$

and our sum of column squares result may be written

$$\sum_{i=0}^{k} i^2 a_i = nk \tag{B}$$

Note: - column sums must have the same parity as k

Column sum relations

For $i \in \{-k, -k+1, \ldots, k-1, k\}$:

put b_i for # of columns of H with sum i.

For $1 \leq i \leq k$ write $a_i = b_i + b_{-i}$ and $a_0 = b_0$.Then

$$\sum_{i=0}^{k} a_i = n, \tag{A}$$

and our sum of column squares result may be written

$$\sum_{i=0}^{k} i^2 a_i = nk \tag{B}$$

Note: - column sums must have the same parity as k

- Therefore if $i \not\equiv k \pmod 2$, then $a_i = 0$

Column sum relations

For $i \in \{-k, -k+1, \ldots, k-1, k\}$:

put b_i for # of columns of H with sum i.

For $1 \leq i \leq k$ write $a_i = b_i + b_{-i}$ and $a_0 = b_0$.Then

$$\sum_{i=0}^{k} a_i = n, \tag{A}$$

and our sum of column squares result may be written

$$\sum_{i=0}^{k} i^2 a_i = nk \tag{B}$$

Note: - column sums must have the same parity as k

- Therefore if $i \not\equiv k \pmod 2$, then $a_i = 0$

- This will be important later.

A column sum inequality

The sum of the entries of H is

A column sum inequality

The sum of the entries of H is

$$(b_1 - b_{-1}) + 2(b_2 - b_{-2}) + \cdots + k(b_k - b_{-k}) = rk.$$

A column sum inequality

The sum of the entries of H is

$$(b_1 - b_{-1}) + 2(b_2 - b_{-2}) + \cdots + k(b_k - b_{-k}) = rk.$$

Now clearly, $a_i \geq b_i - b_{-i}$

A column sum inequality

The sum of the entries of H is

$$(b_1 - b_{-1}) + 2(b_2 - b_{-2}) + \cdots + k(b_k - b_{-k}) = rk.$$

Now clearly, $a_i \geq b_i - b_{-i}$

We infer that

$$a_1 + 2a_2 + \cdots + ka_k = \sum_{i=0}^{k} ia_i \geq rk. \tag{C}$$

A column sum inequality

The sum of the entries of H is

$$(b_1 - b_{-1}) + 2(b_2 - b_{-2}) + \cdots + k(b_k - b_{-k}) = rk.$$

Now clearly, $a_i \geq b_i - b_{-i}$

We infer that

$$a_1 + 2a_2 + \cdots + ka_k = \sum_{i=0}^{k} ia_i \geq rk. \tag{C}$$

This is a <u>very</u> crude approximation

A column sum inequality

The sum of the entries of H is

$$(b_1 - b_{-1}) + 2(b_2 - b_{-2}) + \cdots + k(b_k - b_{-k}) = rk.$$

Now clearly, $a_i \geq b_i - b_{-i}$

We infer that

$$a_1 + 2a_2 + \cdots + ka_k = \sum_{i=0}^{k} ia_i \geq rk. \tag{C}$$

This is a <u>very</u> crude approximation

but it suffices to force threshold column-sum behaviour.

Getting a bound on k when $\frac{kr}{n} = m + \delta$

Getting a bound on k when $\frac{kr}{n} = m + \delta$

Consider
$$(m^2 - 1)(A) + (B) - 2m(C)$$

Getting a bound on k when $\frac{kr}{n} = m + \delta$

Consider

$$(m^2 - 1)(A) + (B) - 2m(C)$$

That is,

$$(m^2 - 1)\left(\sum a_i = n\right) + \left(\sum i^2 a_i = nk\right) - 2m\left(\sum i a_i \geq rk\right)$$

Getting a bound on k when $\frac{kr}{n} = m + \delta$

Consider

$$(m^2 - 1)(A) + (B) - 2m(C)$$

That is,

$$(m^2 - 1)\left(\sum a_i = n\right) + \left(\sum i^2 a_i = nk\right) - 2m\left(\sum i a_i \geq rk\right)$$

which simplifies to:

$$\sum \left[(m-i)^2 - 1\right] a_i$$

Getting a bound on k when $\frac{kr}{n} = m + \delta$

Consider

$$(m^2 - 1)(A) + (B) - 2m(C)$$

That is,

$$(m^2 - 1)\left(\sum a_i = n\right) + \left(\sum i^2 a_i = nk\right) - 2m\left(\sum i a_i \geq rk\right)$$

which simplifies to:

$$\sum \left[(m-i)^2 - 1\right] a_i \qquad \leq n\left(m^2 - 1 + k - 2m\frac{rk}{n}\right)$$

Getting a bound on k when $\frac{kr}{n} = m + \delta$

Consider

$$(m^2 - 1)(A) + (B) - 2m(C)$$

That is,

$$(m^2 - 1)\left(\sum a_i = n\right) + \left(\sum i^2 a_i = nk\right) - 2m\left(\sum i a_i \geq rk\right)$$

which simplifies to:

$$\begin{aligned} \sum \left[(m-i)^2 - 1\right] a_i &\leq n\left(m^2 - 1 + k - 2m\frac{rk}{n}\right) \\ &= n\left[\left(m - \frac{rk}{n}\right)^2 + k - 1 - \left(\frac{rk}{n}\right)^2\right] \end{aligned}$$

Getting a bound on k when $\frac{kr}{n} = m + \delta$

Consider

$$(m^2 - 1)(A) + (B) - 2m(C)$$

That is,

$$(m^2 - 1)\left(\sum a_i = n\right) + \left(\sum i^2 a_i = nk\right) - 2m\left(\sum i a_i \geq rk\right)$$

which simplifies to:

$$\begin{aligned}\sum \left[(m-i)^2 - 1\right] a_i &\leq n\left(m^2 - 1 + k - 2m\frac{rk}{n}\right) \\ &= n\left[\left(m - \frac{rk}{n}\right)^2 + k - 1 - \left(\frac{rk}{n}\right)^2\right]\end{aligned}$$

Now $m - \frac{rk}{n} = \delta$ ...

Getting a bound on k (cont.)

So finally we have

$$\sum \left[(m-i)^2 - 1\right] a_i \le n\left[\delta^2 + k - 1 - \left(\frac{kr}{n}\right)^2\right]. \qquad (*)$$

Getting a bound on k (cont.)

So finally we have

$$\sum \left[(m-i)^2 - 1\right] a_i \leq n\left[\delta^2 + k - 1 - \left(\frac{kr}{n}\right)^2\right]. \qquad (*)$$

- Recall m was chosen to have opposite parity to k

Getting a bound on k (cont.)

So finally we have

$$\sum \left[(m-i)^2 - 1\right] a_i \leq n \left[\delta^2 + k - 1 - \left(\frac{kr}{n}\right)^2\right]. \qquad (*)$$

- Recall m was chosen to have opposite parity to k
- So when i, k have the same parity, $m - i$ is odd.

Getting a bound on k (cont.)

So finally we have

$$\sum \left[(m-i)^2 - 1\right] a_i \leq n\left[\delta^2 + k - 1 - \left(\frac{kr}{n}\right)^2\right]. \qquad (*)$$

- Recall m was chosen to have opposite parity to k
- So when i, k have the same parity, $m - i$ is odd.
- Recall when i, k have opposite parity, $a_i = 0$.

Getting a bound on k (cont.)

So finally we have

$$\sum \left[(m-i)^2 - 1\right] a_i \leq n \left[\delta^2 + k - 1 - \left(\frac{kr}{n}\right)^2\right]. \qquad (*)$$

- Recall m was chosen to have opposite parity to k
- So when i, k have the same parity, $m - i$ is odd.
- Recall when i, k have opposite parity, $a_i = 0$.
- Therefore LHS ≥ 0

Getting a bound on k (cont.)

So finally we have

$$\sum \left[(m-i)^2 - 1\right] a_i \leq n\left[\delta^2 + k - 1 - \left(\frac{kr}{n}\right)^2\right]. \qquad (*)$$

- Recall m was chosen to have opposite parity to k
- So when i, k have the same parity, $m - i$ is odd.
- Recall when i, k have opposite parity, $a_i = 0$.
- Therefore LHS ≥ 0 (another very crude estimate!)

Getting a bound on k (cont.)

So finally we have

$$\sum \left[(m-i)^2 - 1\right] a_i \leq n \left[\delta^2 + k - 1 - \left(\frac{kr}{n}\right)^2\right]. \qquad (*)$$

- Recall m was chosen to have opposite parity to k
- So when i, k have the same parity, $m - i$ is odd.
- Recall when i, k have opposite parity, $a_i = 0$.
- Therefore LHS ≥ 0 (another very crude estimate!)
- Therefore $\delta^2 + k - 1 - \left(\frac{kr}{n}\right)^2 \geq 0$

and so

$$\left(\frac{rk}{n}\right)^2 + 1 \leq k + \delta^2.$$

Getting a bound on k (cont.)

Which may be arranged as a quadratic inequality in k:

Getting a bound on k (cont.)

Which may be arranged as a quadratic inequality in k:

$$\left(\frac{r}{n}\right)^2 k^2 - k + (1 - \delta^2) \leq 0$$

(a concave-up parabola)

Getting a bound on k (cont.)

Which may be arranged as a quadratic inequality in k:

$$\left(\frac{r}{n}\right)^2 k^2 - k + (1 - \delta^2) \leq 0$$

(a concave-up parabola) so k cannot exceed the larger root:

Getting a bound on k (cont.)

Which may be arranged as a quadratic inequality in k:

$$\left(\frac{r}{n}\right)^2 k^2 - k + (1 - \delta^2) \leq 0$$

(a concave-up parabola) so k cannot exceed the larger root:

$$k \leq \frac{1 + \sqrt{1 + (\delta^2 - 1)\left(\frac{2r}{n}\right)^2}}{2\left(\frac{r}{n}\right)^2},$$

Getting a bound on k (cont.)

Which may be arranged as a quadratic inequality in k:

$$\left(\frac{r}{n}\right)^2 k^2 - k + (1 - \delta^2) \leq 0$$

(a concave-up parabola) so k cannot exceed the larger root:

$$k \leq \frac{1 + \sqrt{1 + (\delta^2 - 1)\left(\frac{2r}{n}\right)^2}}{2\left(\frac{r}{n}\right)^2},$$

yielding an upper bound on k.

Getting a bound on k (cont.)

Which may be arranged as a quadratic inequality in k:

$$\left(\frac{r}{n}\right)^2 k^2 - k + (1 - \delta^2) \le 0$$

(a concave-up parabola) so k cannot exceed the larger root:

$$k \le \frac{1 + \sqrt{1 + (\delta^2 - 1)\left(\frac{2r}{n}\right)^2}}{2\left(\frac{r}{n}\right)^2},$$

yielding an upper bound on k.

The case of equality makes the RHS of (*) equal to 0:

$$0 \le \sum \left[(m-i)^2 - 1\right] a_i \le n\left[\delta^2 + k - 1 - \left(\frac{kr}{n}\right)^2\right] = 0.$$

Getting a bound on k (cont.)

Which may be arranged as a quadratic inequality in k:

$$\left(\frac{r}{n}\right)^2 k^2 - k + (1-\delta^2) \leq 0$$

(a concave-up parabola) so k cannot exceed the larger root:

$$k \leq \frac{1+\sqrt{1+(\delta^2-1)\left(\frac{2r}{n}\right)^2}}{2\left(\frac{r}{n}\right)^2},$$

yielding an upper bound on k.

The case of equality makes the RHS of (*) equal to 0:

$$0 \leq \sum \left[(m-i)^2 - 1\right] a_i \leq n\left[\delta^2 + k - 1 - \left(\frac{kr}{n}\right)^2\right] = 0.$$

Note $m - i \neq \pm 1$ implies $(m-i)^2 - 1 > 0$

Getting a bound on k (cont.)

Which may be arranged as a quadratic inequality in k:

$$\left(\frac{r}{n}\right)^2 k^2 - k + (1-\delta^2) \leq 0$$

(a concave-up parabola) so k cannot exceed the larger root:

$$k \leq \frac{1+\sqrt{1+(\delta^2-1)\left(\frac{2r}{n}\right)^2}}{2\left(\frac{r}{n}\right)^2},$$

yielding an upper bound on k.

The case of equality makes the RHS of (*) equal to 0:

$$0 \leq \sum \left[(m-i)^2 - 1\right] a_i \leq n\left[\delta^2 + k - 1 - \left(\frac{kr}{n}\right)^2\right] = 0.$$

Note $m - i \neq \pm 1$ implies $(m-i)^2 - 1 > 0$, which forces $a_i = 0$.

Threshold necessary conditions

So H has only two possible column sums, $i = m \pm 1$

Threshold necessary conditions

So H has only two possible column sums, $i = m \pm 1$.
From our basic relations it is easy to work out how many of each.

Threshold necessary conditions

So H has only two possible column sums, $i = m \pm 1$.
From our basic relations it is easy to work out how many of each.
We summarize.

Threshold necessary conditions

So H has only two possible column sums, $i = m \pm 1$.
From our basic relations it is easy to work out how many of each.
We summarize.

Theorem (Threshold necessary conditions)

Suppose $\exists$ r-$H(k \times n)$, and m, δ are as described. Then

1. $\left(\frac{rk}{n}\right)^2 + 1 \leq k + \delta^2$;
2. $k \leq \frac{1+\sqrt{1+(\delta^2-1)\left(\frac{2r}{n}\right)^2}}{2\left(\frac{r}{n}\right)^2}$.
3. *If $\left(\frac{rk}{n}\right)^2 + 1 = k + \delta^2$ then all column sums are equal to $m \pm 1$; further there are*
   (a) $a_{m-1} = n\frac{1-\delta}{2}$ *columns having sum $m-1$, and*
   (b) $a_{m+1} = n\frac{1+\delta}{2}$ *columns having sum $m+1$.*

An awkward inequality

An awkward inequality

$k \leq \frac{1+\sqrt{1+(\delta^2-1)\left(\frac{2r}{n}\right)^2}}{2\left(\frac{r}{n}\right)^2}$ looks problematic as δ depends on k.

An awkward inequality

$k \le \frac{1+\sqrt{1+(\delta^2-1)\left(\frac{2r}{n}\right)^2}}{2\left(\frac{r}{n}\right)^2}$ looks problematic as δ depends on k.

Regard this as an upper bound for k among cases with constant δ.

An awkward inequality

$k \leq \frac{1+\sqrt{1+(\delta^2-1)\left(\frac{2r}{n}\right)^2}}{2\left(\frac{r}{n}\right)^2}$ looks problematic as δ depends on k.

Regard this as an upper bound for k among cases with constant δ.

That is, among each residue class modulo $\frac{2n}{\gcd(r,2n)}$

An awkward inequality

$k \leq \frac{1+\sqrt{1+(\delta^2-1)\left(\frac{2r}{n}\right)^2}}{2\left(\frac{r}{n}\right)^2}$ looks problematic as δ depends on k.

Regard this as an upper bound for k among cases with constant δ.

That is, among each residue class modulo $\frac{2n}{\gcd(r,2n)}$

So more than one k value may produce a threshold case!

An awkward inequality

$k \leq \frac{1+\sqrt{1+(\delta^2-1)\left(\frac{2r}{n}\right)^2}}{2\left(\frac{r}{n}\right)^2}$ looks problematic as δ depends on k.

Regard this as an upper bound for k among cases with constant δ.

That is, among each residue class modulo $\frac{2n}{\gcd(r,2n)}$

So more than one k value may produce a threshold case!

We examine a few test cases.

Examination of 12-$H(k \times 36)$ for threshold cases

$(n, r) = (36, 12)$; $k_{\max} = 8$

k	m	δ	Threshold inequality
1	0	$\frac{1}{3}$	Equality
2	1	$-\frac{1}{3}$	Satisfied
3	1	-1	Satisfied
4	1	$\frac{1}{3}$	Satisfied
5	2	$-\frac{1}{3}$	Satisfied
6	3	-1	Satisfied
7	2	$\frac{1}{3}$	Satisfied
8	3	$-\frac{1}{3}$	Equality
9	4	-1	Equality
10	3	$-\frac{1}{3}$	Violated

Examination of 10-$H(k \times 40)$ for threshold cases

$(n, r) = (40, 10)$
$k_{\max} = 13$

k	m	δ	Threshold inequality
1	0	$\frac{1}{4}$	Equality
2	1	$-\frac{1}{2}$	Satisfied
3	0	$\frac{3}{4}$	Satisfied
4	1	0	Satisfied
5	2	$-\frac{3}{4}$	Satisfied
6	1	$\frac{1}{2}$	Satisfied
7	2	$-\frac{1}{4}$	Satisfied
8	3	-1	Satisfied
9	2	$\frac{1}{4}$	Satisfied
10	3	$-\frac{1}{2}$	Satisfied
11	2	$\frac{3}{4}$	Satisfied
12	3	0	Satisfied
13	4	$-\frac{3}{4}$	Satisfied
14	3	$\frac{1}{2}$	Satisfied
15	4	$-\frac{1}{4}$	Equality
16	5	-1	Equality
17	4	$\frac{1}{4}$	Violated

Examination of 12-$H(k \times 40)$ for threshold cases

$(n, r) = (40, 12)$; $k_{\max} = 10$

k	m	δ	Threshold inequality
1	0	$\frac{3}{10}$	Equality
2	1	$-\frac{2}{5}$	Satisfied
3	0	$\frac{9}{10}$	Satisfied
4	1	$\frac{1}{5}$	Satisfied
5	2	$-\frac{1}{2}$	Satisfied
6	1	$\frac{4}{5}$	Satisfied
7	2	$\frac{1}{10}$	Satisfied
8	3	$-\frac{3}{5}$	Satisfied
9	2	$\frac{7}{10}$	Satisfied
10	3	0	Equality
11	4	$-\frac{7}{10}$	Violated

Thanks for listening!

References

R. Craigen, G. Faucher, R. Low and T. Wares, *Circulant partial Hadamard matrices*, LAA **439** (2013) pp. 3307–3317.

R. Low, M. Stamp, R. Craigen and G. Faucher, *Unpredictable binary strings*, Congr. Numer. **177** (2005) 65?75.

H.J. Ryser, *Combinatorial Mathematics*, Carus Math. Monogr., v. **14**, MAA/John Wiley and Sons, 1963.

B. Schmidt, *Towards Ryser's Conjecture*, Proceedings of the Third European Congress of Mathematics (Birkhuser, Boston, 2001) 533-541.

Y-L. Lin, F. K. H Phoa and M-H. Kao, *CPH Matrices: Construction via general difference sets and its application to FMRI Experiments*, Statistica Sinica **27**, 1715-1724.