Codes and Lattices of Hadamard Matrices

Akihiro Munemasa

Graduate School of Information Sciences
Tohoku University

RIMS, Kyoto University
June 12, 2007.

Hadamard Matrix

A Hadamard matrix H is a square matrix of order n with entries ± 1, satisfying

$$HH^T = nI.$$

Hadamard Matrix

A Hadamard matrix H is a square matrix of order n with entries ± 1, satisfying

$$HH^T = nI.$$

Example:

Hadamard Matrix

A Hadamard matrix H is a square matrix of order n with entries ± 1, satisfying

$$HH^T = nI.$$

Example:

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

Normalized Hadamard Matrix

$$\begin{bmatrix} \color{red}{1} & \color{red}{1} & \color{red}{1} & \color{red}{1} & \color{red}{1} & \color{red}{1} & \color{red}{1} & \color{red}{1} \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix}$$

Normalized Hadamard Matrix

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

Normalized if the entries of the first row are all 1.

Code of a Hadamard Matrix

- H : a Hadamard matrix of order n,
- p : an odd prime.

Code of a Hadamard Matrix

- H : a Hadamard matrix of order n,
- p : an odd prime.

$$C_p(H) = \mathbb{F}_p^n H$$

Code of a Hadamard Matrix

- H : a Hadamard matrix of order n,
- p : an odd prime.

$$C_p(H) = \mathbb{F}_p^n H \quad = \{vH \mid v \in \mathbb{F}_p^n\}$$

Code of a Hadamard Matrix

- H : a Hadamard matrix of order n,
- p : an odd prime.

$$C_p(H) = \mathbb{F}_p^n H \quad = \{vH \mid v \in \mathbb{F}_p^n\}$$
$$= \text{row space of } H \text{ over } \mathbb{F}_p \subset \mathbb{F}_p^n$$

Code of a Hadamard Matrix

- H : a Hadamard matrix of order n,
- p : an odd prime.

$$C_p(H) = \mathbb{F}_p^n H \quad = \{vH \mid v \in \mathbb{F}_p^n\}$$
$$= \text{row space of } H \text{ over } \mathbb{F}_p \subset \mathbb{F}_p^n$$

- Fact : If $p||n$, then $C_p(H)$ is self-dual.

Code of a Hadamard Matrix

- H : a Hadamard matrix of order n,
- p : an odd prime.

$$C_p(H) = \mathbb{F}_p^n H \quad = \{vH \mid v \in \mathbb{F}_p^n\}$$
$$= \text{row space of } H \text{ over } \mathbb{F}_p \subset \mathbb{F}_p^n$$

- Fact : If $p||n$, then $C_p(H)$ is self-dual.
- $C_3(H)$ is self-dual for Hadamard matrix H of order 24.

Code of a Hadamard Matrix

- H : a Hadamard matrix of order n,
- p : an odd prime.

$$C_p(H) = \mathbb{F}_p^n H \quad = \{vH \mid v \in \mathbb{F}_p^n\}$$
$$= \text{row space of } H \text{ over } \mathbb{F}_p \subset \mathbb{F}_p^n$$

- Fact : If $p||n$, then $C_p(H)$ is self-dual.
- $C_3(H)$ is self-dual for Hadamard matrix H of order 24.

What if $p = 2$?

Binary Hadamard Matrix

- H : a Hadamard matrix of order n.
- J : the all-ones matrix of order n.

Binary Hadamard Matrix

- H : a Hadamard matrix of order n.
- J : the all-ones matrix of order n.

$$B = \frac{1}{2}(H + J).$$

Binary Hadamard Matrix

- H : a Hadamard matrix of order n.
- J : the all-ones matrix of order n.

$$B = \frac{1}{2}(H + J).$$

$$(-1 \mapsto 0)$$

Binary Hadamard Matrix

- H : a Hadamard matrix of order n.
- J : the all-ones matrix of order n.

$$B = \frac{1}{2}(H + J).$$

$$(-1 \mapsto 0)$$

$$\begin{aligned} C_2(H) &= \mathbb{F}_2^n B = \{vB \mid v \in \mathbb{F}_2^n\} \\ &= \text{row space of } B \text{ over } \mathbb{F}_2 \subset \mathbb{F}_2^n \end{aligned}$$

Binary Hadamard Matrix

- H : a Hadamard matrix of order n.
- J : the all-ones matrix of order n.

$$\color{yellow}{B} = \frac{1}{2}(H + J).$$

$$(-1 \mapsto 0)$$

$$\begin{aligned} C_2(H) &= \mathbb{F}_2^n B = \{vB \mid v \in \mathbb{F}_2^n\} \\ &= \text{row space of } B \text{ over } \mathbb{F}_2 \subset \mathbb{F}_2^n \end{aligned}$$

- Fact : If $n \equiv 8 \pmod{16}$, then $C_2(H)$ is self-dual.

Binary Hadamard Matrix

- H : a Hadamard matrix of order n.
- J : the all-ones matrix of order n.

$$B = \frac{1}{2}(H + J).$$

$$(-1 \mapsto 0)$$

$$\begin{aligned} C_2(H) &= \mathbb{F}_2^n B = \{vB \mid v \in \mathbb{F}_2^n\} \\ &= \text{row space of } B \text{ over } \mathbb{F}_2 \subset \mathbb{F}_2^n \end{aligned}$$

- Fact : If $n \equiv 8 \pmod{16}$, then $C_2(H)$ is self-dual.
- $n = 24$: $C_2(H)$ is self-dual.

Hadamard Matrices of Order 24

H : a Hadamard matrix of order 24. Then

Hadamard Matrices of Order 24

H : a Hadamard matrix of order 24. Then

- $C_3(H)$ has minimum weight 6 or 9

Hadamard Matrices of Order 24

H : a Hadamard matrix of order 24. Then

- $C_3(H)$ has minimum weight 6 or 9
- $C_2(H)$ has minimum weight 4 or 8

Hadamard Matrices of Order 24

H : a Hadamard matrix of order 24. Then

- $C_3(H)$ has minimum weight 6 or 9
- $C_2(H)$ has minimum weight 4 or 8
- There are 60 Hadamard matrices of order 24 up to equivalence. (Ito-Leon-Longyear 1981; and Kimura 1989)

Hadamard Matrices of Order 24

H : a Hadamard matrix of order 24. Then

- $C_3(H)$ has minimum weight 6 or 9
- $C_2(H)$ has minimum weight 4 or 8
- There are 60 Hadamard matrices of order 24 up to equivalence. (Ito-Leon-Longyear 1981; and Kimura 1989)
- Assmus and Key observed (in their book “Designs and Their Codes”):

Hadamard Matrices of Order 24

H : a Hadamard matrix of order 24. Then

- $C_3(H)$ has minimum weight 6 or 9
- $C_2(H)$ has minimum weight 4 or 8
- There are 60 Hadamard matrices of order 24 up to equivalence. (Ito-Leon-Longyear 1981; and Kimura 1989)
- Assmus and Key observed (in their book "Designs and Their Codes"):

$$\min C_2(H) = 8 \iff$$

Hadamard Matrices of Order 24

H : a Hadamard matrix of order 24. Then

- $C_3(H)$ has minimum weight 6 or 9
- $C_2(H)$ has minimum weight 4 or 8
- There are 60 Hadamard matrices of order 24 up to equivalence. (Ito-Leon-Longyear 1981; and Kimura 1989)
- Assmus and Key observed (in their book "Designs and Their Codes"):

$$\min C_2(H) = 8 \iff \min C_3(H^T) = 9$$

Lattice of a Hadamard Matrix

- H : a Hadamard matrix of order 24, $B = \frac{1}{2}(H + J)$.

Lattice of a Hadamard Matrix

- H : a Hadamard matrix of order 24, $B = \frac{1}{2}(H + J)$.
- $\mathbb{Z}^{24}B$

Lattice of a Hadamard Matrix

- H : a Hadamard matrix of order 24, $B = \frac{1}{2}(H + J)$.
- $\mathbb{Z}^{48} \begin{bmatrix} B \\ 4I \end{bmatrix}$

Lattice of a Hadamard Matrix

- H : a Hadamard matrix of order 24, $B = \frac{1}{2}(H + J)$.
- $\mathbb{Z}^{48} \begin{bmatrix} B \\ 4I \\ 2e_1 + \frac{1}{2}\mathbf{1} \end{bmatrix}$

Lattice of a Hadamard Matrix

- H : a Hadamard matrix of order 24, $B = \frac{1}{2}(H + J)$.
- $\mathbb{Z}^{48} \begin{bmatrix} B \\ 4I \\ 2e_1 + \frac{1}{2}\mathbf{1} \end{bmatrix} \times \frac{1}{\sqrt{2}}$

Lattice of a Hadamard Matrix

- H : a Hadamard matrix of order 24, $B = \frac{1}{2}(H + J)$.

- $\mathbb{Z}^{48} \begin{bmatrix} B \\ 4I \\ 2e_1 + \frac{1}{2}\mathbf{1} \end{bmatrix} \times \frac{1}{\sqrt{2}} = \frac{1}{2\sqrt{2}} \mathbb{Z}^{49} \begin{bmatrix} H + J \\ 8I \\ 4e_1 + \mathbf{1} \end{bmatrix}$
  $= \Lambda(H) \subset \mathbb{R}^{24}$.

Lattice of a Hadamard Matrix

- H : a Hadamard matrix of order 24, $B = \frac{1}{2}(H + J)$.

- $$\mathbb{Z}^{48} \begin{bmatrix} B \\ 4I \\ 2e_1 + \frac{1}{2}\mathbf{1} \end{bmatrix} \times \frac{1}{\sqrt{2}} = \frac{1}{2\sqrt{2}} \mathbb{Z}^{49} \begin{bmatrix} H + J \\ 8I \\ 4e_1 + \mathbf{1} \end{bmatrix}$$
  $$= \Lambda(H) \subset \mathbb{R}^{24}.$$

Fact : $\Lambda(H)$ is an even unimodular lattice.

Lattice of a Hadamard Matrix

- H : a Hadamard matrix of order 24, $B = \frac{1}{2}(H+J)$.

- $\mathbb{Z}^{48} \begin{bmatrix} B \\ 4I \\ 2e_1 + \frac{1}{2}\mathbf{1} \end{bmatrix} \times \frac{1}{\sqrt{2}} = \frac{1}{2\sqrt{2}}\mathbb{Z}^{49} \begin{bmatrix} H+J \\ 8I \\ 4e_1 + \mathbf{1} \end{bmatrix}$
  $= \Lambda(H) \subset \mathbb{R}^{24}$.

Fact : $\Lambda(H)$ is an even unimodular lattice.

$\{\|x\|^2 \mid 0 \neq x \in \Lambda(H)\} \subset 2\mathbb{Z}$

Lattice of a Hadamard Matrix

- H : a Hadamard matrix of order 24, $B = \frac{1}{2}(H+J)$.

- $$\mathbb{Z}^{48}\begin{bmatrix} B \\ 4I \\ 2e_1 + \frac{1}{2}\mathbf{1} \end{bmatrix} \times \frac{1}{\sqrt{2}} = \frac{1}{2\sqrt{2}}\mathbb{Z}^{49}\begin{bmatrix} H+J \\ 8I \\ 4e_1 + \mathbf{1} \end{bmatrix}$$
  $= \Lambda(H) \subset \mathbb{R}^{24}$.

Fact : $\Lambda(H)$ is an even unimodular lattice.
$\min\{\|x\|^2 \mid 0 \neq x \in \Lambda(H)\}$
= minimum norm of $\Lambda(H)$

Lattice of a Hadamard Matrix

- H : a Hadamard matrix of order 24, $B = \frac{1}{2}(H + J)$.

- $$\mathbb{Z}^{48} \begin{bmatrix} B \\ 4I \\ 2e_1 + \frac{1}{2}\mathbf{1} \end{bmatrix} \times \frac{1}{\sqrt{2}} = \frac{1}{2\sqrt{2}} \mathbb{Z}^{49} \begin{bmatrix} H + J \\ 8I \\ 4e_1 + \mathbf{1} \end{bmatrix}$$
  $= \Lambda(H) \subset \mathbb{R}^{24}$.

Fact : $\Lambda(H)$ is an even unimodular lattice.
$\min\{\|x\|^2 \mid 0 \neq x \in \Lambda(H)\}$
= minimum norm of $\Lambda(H)$

$= 2$ or 4 .

Lattice of a Hadamard Matrix

- H : a Hadamard matrix of order 24, $B = \frac{1}{2}(H + J)$.

- $\mathbb{Z}^{48} \begin{bmatrix} B \\ 4I \\ 2e_1 + \frac{1}{2}\mathbf{1} \end{bmatrix} \times \frac{1}{\sqrt{2}} = \frac{1}{2\sqrt{2}}\mathbb{Z}^{49} \begin{bmatrix} H + J \\ 8I \\ 4e_1 + \mathbf{1} \end{bmatrix}$
  $= \Lambda(H) \subset \mathbb{R}^{24}$.

Fact : $\Lambda(H)$ is an even unimodular lattice.
$\min\{\|x\|^2 \mid 0 \neq x \in \Lambda(H)\}$
= minimum norm of $\Lambda(H)$
$= 2$ or 4.

Equivalence

Given a Hadamard matrix H of order 24,

Equivalence

Given a Hadamard matrix H of order 24,

	min weight or norm	description
$C_2(H)$	4, 8	Golay
$C_3(H)$	6, 9	QR or Pless symmetry
$\Lambda(H)$	2, 4	Leech

Equivalence

Given a Hadamard matrix H of order 24,

	min weight or norm	description
$C_2(H)$	4, 8	Golay
$C_3(H^T)$	6, 9	QR or Pless symmetry
$\Lambda(H)$	2, 4	Leech

Theorem

Let H be a Hadamard matrix of order 24 whose first row is the all-ones vector. The following statements are equivalent:

(i) $C_2(H)$ has minimum weight 8,

(ii) $C_3(H^T)$ has minimum weight 9,

(iii) $\Lambda(H)$ has minimum norm 4.

Theorem

Let H be a Hadamard matrix of order 24 whose first row is the all-ones vector. The following statements are equivalent:

(i) $C_2(H)$ has minimum weight 8,

(ii) $C_3(H^T)$ has minimum weight 9,

(iii) $\Lambda(H)$ has minimum norm 4.

Proof uses "Neighbors" of $\Lambda(H)$.

Neighbors

$$\frac{1}{2\sqrt{2}}\mathbb{Z}^{49}\begin{bmatrix} H+J \\ 8I \\ 4e_1+\mathbf{1} \end{bmatrix} \qquad \frac{1}{2\sqrt{2}}\mathbb{Z}^{48}\begin{bmatrix} H \\ 8I \end{bmatrix} \qquad \frac{1}{2\sqrt{2}}\mathbb{Z}^{48}\begin{bmatrix} H+J \\ 4I \end{bmatrix}$$

$$\boxed{=\Lambda(H)} \qquad \boxed{=\Lambda'(H)} \qquad \boxed{=\Lambda''(H)}$$

Neighbors

$$\frac{1}{2\sqrt{2}}\mathbb{Z}^{49}\begin{bmatrix} H+J \\ 8I \\ 4e_1+\mathbf{1} \end{bmatrix} \qquad \frac{1}{2\sqrt{2}}\mathbb{Z}^{48}\begin{bmatrix} H \\ 8I \end{bmatrix} \qquad \frac{1}{2\sqrt{2}}\mathbb{Z}^{48}\begin{bmatrix} H+J \\ 4I \end{bmatrix}$$

$$\boxed{=\Lambda(H)} \qquad \boxed{=\Lambda'(H)} \qquad \boxed{=\Lambda''(H)}$$

$$\Lambda_0(H) = \frac{1}{2\sqrt{2}}\mathbb{Z}^{48}\begin{bmatrix} H+J \\ 8I \end{bmatrix}$$

Neighbors

$$\frac{1}{2\sqrt{2}}\mathbb{Z}^{49}\begin{bmatrix} H+J \\ 8I \\ 4e_1+\mathbf{1} \end{bmatrix} \quad \boxed{=\Lambda(H)}$$

$$\frac{1}{2\sqrt{2}}\mathbb{Z}^{48}\begin{bmatrix} H \\ 8I \end{bmatrix} \quad \boxed{=\Lambda'(H)}$$

$$\frac{1}{2\sqrt{2}}\mathbb{Z}^{48}\begin{bmatrix} H+J \\ 4I \end{bmatrix} \quad \boxed{=\Lambda''(H)}$$

$$\begin{tikzcd} \Lambda(H) \arrow[dr, dash, "2"'] & \Lambda'(H) \arrow[d, dash, "2"'] & \Lambda''(H) \arrow[dl, dash, "2"] \\ & \Lambda_0(H) & \end{tikzcd}$$

$$\Lambda_0(H) = \frac{1}{2\sqrt{2}}\mathbb{Z}^{48}\begin{bmatrix} H+J \\ 8I \end{bmatrix}$$

Neighbors

$$\frac{1}{2\sqrt{2}}\mathbb{Z}^{49}\begin{bmatrix} H+J \\ 8I \\ 4e_1+\mathbf{1} \end{bmatrix} \qquad \frac{1}{2\sqrt{2}}\mathbb{Z}^{48}\begin{bmatrix} H \\ 8I \end{bmatrix} \qquad \frac{1}{2\sqrt{2}}\mathbb{Z}^{48}\begin{bmatrix} H+J \\ 4I \end{bmatrix}$$

$$\boxed{=\Lambda(H)} \qquad \boxed{=\Lambda'(H)} \qquad \boxed{=\Lambda''(H)}$$

$\|x\|^2$ even

$\frac{1}{\sqrt{2}}x\cdot\mathbf{1}$ even

$$\Lambda_0(H) = \frac{1}{2\sqrt{2}}\mathbb{Z}^{48}\begin{bmatrix} H+J \\ 8I \end{bmatrix}$$

Neighbors

$$\frac{1}{2\sqrt{2}}\mathbb{Z}^{49}\begin{bmatrix} H+J \\ 8I \\ 4e_1+\mathbf{1} \end{bmatrix} \quad \frac{1}{2\sqrt{2}}\mathbb{Z}^{48}\begin{bmatrix} H \\ 8I \end{bmatrix} \quad \frac{1}{2\sqrt{2}}\mathbb{Z}^{48}\begin{bmatrix} H+J \\ 4I \end{bmatrix}$$

$$\boxed{=\Lambda(H)} \quad \boxed{=\Lambda'(H)} \quad \boxed{=\Lambda''(H)}$$

$\min \Lambda(H)$
$= \min \Lambda_0(H)$

$\|x\|^2$
even

$\frac{1}{\sqrt{2}}x \cdot \mathbf{1}$ even

$$\Lambda_0(H) = \frac{1}{2\sqrt{2}}\mathbb{Z}^{48}\begin{bmatrix} H+J \\ 8I \end{bmatrix}$$

Neighbors

$\min \Lambda(H) \qquad = 2$ or 4

Neighbors

$\min \Lambda(H)$ $= 2$ or 4

$= \min \Lambda_0(H)$

Neighbors

$\min \Lambda(H) \qquad = 2$ or 4

$= \min \Lambda_0(H)$

$= \min\{\|x\|^2 \mid 0 \neq x \in \Lambda'(H) = \frac{1}{2\sqrt{2}}\mathbb{Z}^{48} \begin{bmatrix} H \\ 8I \end{bmatrix},\ \|x\|^2 \text{ even } \}$

Neighbors

$\min \Lambda(H)$ $= 2$ or 4

$= \min \Lambda_0(H)$

$= \min\{\|x\|^2 \mid 0 \neq x \in \Lambda'(H) = \frac{1}{2\sqrt{2}}\mathbb{Z}^{48} \begin{bmatrix} H \\ 8I \end{bmatrix},\ \|x\|^2$ even $\}$

$= \min\{\|x\|^2 \mid 0 \neq x \in \Lambda''(H) = \frac{1}{2\sqrt{2}}\mathbb{Z}^{48} \begin{bmatrix} H + J \\ 4I \end{bmatrix},$

$\frac{1}{\sqrt{2}}x \cdot \mathbf{1}$ even $\}$