Binary codes of t-designs and Hadamard matrices

Akihiro Munemasa[1]

[1] Graduate School of Information Sciences
Tohoku University

November 8, 2013
JSPS-DST Asian Academic Seminar 2013
Discrete Mathematics and Its Applications
The University of Tokyo

Overview

R. C. Bose (1901–1987)

- Combinatorial design theory
  association schemes, symmetric (square) designs,
  Hadamard designs
- Algebraic coding theory
  BCH code Dijen Ray-Chaudhuri (1933–)
- Finite geometries

In this talk, I will connect codes and Hadamard matrices directly, present an answer to a question of Assmus–Key (1992), and try to reveal the theory behind (integral lattices).

Analytic characterization of Hadamard matrices

The function

$$f : \det(x_{ij}) : [-1,1]^{n^2} \to \mathbb{R}.$$

satisfies Hadamard's inequality,

$$f(x) \le n^{n/2}$$

equality is achieved (if? and) only if $n = 1, 2$ or $n \equiv 0 \pmod 4$.

Conjecture: "if and only if."
Amounts to finding a square matrix H of order n with entries in $\{\pm 1\}$ such that $HH^\top = nI$. The smallest unsettled case is $n = 668$.

Hadamard matrices

Definition

A Hadamard matrix of order n is an $n \times n$ matrix with entries in $\{\pm 1\}$, such that rows are pairwise orthogonal:

$$HH^\top = nI.$$

Example

The Hadamard matrix of Sylvester type, where $n = 2^v$:

$$H \otimes \cdots \otimes H,$$

where

$$H = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

Existence of Hadamard matrices

A Hadamard matrix of order n exists for

$$n = 1, 2, 4, 8, 12, 16, \ldots \text{(multiples of } 4\text{)}, \ldots, 664, 672, \ldots$$

Except $n = 1, 2$, the existence of a Hadamard matrix of order n implies $n \equiv 0 \pmod 4$:

$$\begin{array}{cccc} 1 \cdots 1 & 1 \cdots 1 & 1 \cdots 1 & 1 \cdots 1 \\ 1 \cdots 1 & 1 \cdots 1 & -1 \cdots -1 & -1 \cdots -1 \\ 1 \cdots 1 & -1 \cdots -1 & 1 \cdots 1 & -1 \cdots -1 \end{array}$$

Conjecture

A Hadamard matrix of order n exists for any $n \equiv 0 \pmod 4$.

Classification of Hadamard matrices

If H is a Hadamard matrix, then so is $H^\top$.

Definition

Two Hadamard matrices H_1, H_2 are said to be equivalent if

$$\exists P, Q,\ PH_1Q = H_2,$$

where P and Q are signed permutation matrices.

The numbers of equivalence classes of Hadamard matrices are known for orders up to 32.

order	1	2	4	8	12	16	20	24	28	32
number	1	1	1	1	1	5	3	60	487	13,710,027

$16, 20$: Hall; 24: Ito–Leon–Longyear, Kimura; 28: Kimura, Spence; 32: Kharaghani and Tayfeh-Rezaie (2012).

Invariants of Hadamard matrices

- Combinatorial invariants by counting
- Algebraic invariants (linear algebra over finite fields)

Given a Hadamard matrix H, consider the linear span of its row vectors.
$\rightarrow$ nonsense for $\mathbb{Q}$ or any field $\mathbb{F}$ of characteristic 0, or characteristic p with $(p, n) = 1$.
Otherwise, it is a proper subspace of $\mathbb{F}^n$.

Definition

If $\mathbb{F}$ is a finite field, then a vector subspace of $\mathbb{F}^n$ is called a (linear) code of length n.
For $\mathbb{F} = \mathbb{F}_2$, binary code. For $\mathbb{F} = \mathbb{F}_3$, ternary code.

But in $\mathbb{F}_2$, $1 = -1$, so the linear span is again a nonsense. . . .

Normalized and binary Hadamard matrices

Every Hadamard matrix is equivalent to the one with 1 everywhere in the first row:

$$H = \begin{bmatrix} 1 & 1 \cdots 1 \\ & \cdots \\ & \pm 1 \\ & \cdots \end{bmatrix}$$

Such a Hadamard matrix H is said to be normalized (we assume always in what follows). The binary Hadamard matrix associated to H is

$$B = \frac{1}{2}(H + J) = \begin{bmatrix} 1 & 1 \cdots 1 \\ & \cdots \\ & 1 \text{ or } 0 \\ & \cdots \end{bmatrix}$$

where J is the all-one matrix.

The code of a Hadamard matrix

Definition

The binary code of a Hadamard matrix H is defined as the linear span over $\mathbb{F}_2$ of any binary Hadamard matrix associated to H.

It is non-trivial to check that this is well-defined.

Definition

The ternary code of a Hadamard matrix H is defined as the linear span over $\mathbb{F}_3$ of H.

This is simply $\mathbb{F}_3^n$ if H has order n and $3 \nmid n$.

Weight

For $x = (x_1, \ldots, x_n) \in \mathbb{F}^n$, we write

$$\begin{aligned} \mathrm{supp}(x) &= \{i \mid 1 \le i \le n,\ x_i \ne 0\}, \\ \mathrm{wt}(x) &= |\,\mathrm{supp}(x)|. \end{aligned}$$

For a code $C \subset \mathbb{F}^n$, its minimum weight is

$$\min\{\mathrm{wt}(x) \mid 0 \ne x \in C\}.$$

The minimum weight of the binary (ternary) code is an invariant of a Hadamard matrix.

Assmus and Key (1992)

Fact

Let H be a Hadamard matrix of order 24. The following are equivalent.

- The binary code of H has minimum weight 8 (largest).
- The ternary code of $H^\top$ has minimum weight 9 (largest).

- The binary code of H has dimension 12, and the minimum weight is 4 or 8.
- The ternary code of $H^\top$ has dimension 12, and the minimum weight is 6 or 9.
- There are two (up to equivalence) Hadamard matrices H satisfying the above equivalent conditions.

Verification using MAGMA

There are 60 Hadamard matrices of order 24 up to equivalence. Database is available in MAGMA computer algebra system.

```
DB:=HadamardDatabase();
NumberOfMatrices(DB,24) eq 60;
H24s:=[Matrix(DB,24,i):i in [1..60]];
normalize:=func<H|H*DiagonalMatrix(Eltseq(H[1]))>;
J:=Matrix(Integers(),24,24,[1:i in [1..24^2]]);
bH:=func<H|Parent(H)![x div 2:x in Eltseq(normalize(H)+J)]>
bC:=func<H|LinearCode(ChangeRing(bH(H),GF(2)))>;
tCT:=func<H|LinearCode(ChangeRing(Transpose(H),GF(3)))>;
[i:i in [1..60]|MinimumWeight(bC(H24s[i])) eq 8] eq [3,9];
[i:i in [1..60]|MinimumWeight(tCT(H24s[i])) eq 9] eq [3,9];

Total time: 0.290 seconds, Total memory usage: 32.09MB
```

Assmus and Key (1992)

Fact

Let H be a Hadamard matrix of order 24. The following are equivalent.

- The binary code of H has minimum weight 8 (largest).
- The ternary code of $H^\top$ has minimum weight 9 (largest).

- Why are the behavior modulo 2 and modulo 3 related? (Intuitively speaking, this is unusual. cf. Chinese Remainder Theorem).
- Why transpose?

Ternary codes of H

If C is a code of length n over $\mathbb{F}$, then the dual code of C is defined as

$$C^{\perp} = \{x \in \mathbb{F}^n \mid x \cdot y = 0 \ (\forall y \in C)\}.$$

where

$$x \cdot y = \sum_{i=1}^{n} x_i y_i.$$

Then $\dim C^{\perp} = n - \dim C$. The code C is said to be self-orthogonal if $C \subset C^{\perp}$ and self-dual if $C = C^{\perp}$.

$C =$ the ternary code of a Hadamard matrix H.

$$HH^{\top} = nI \text{ and } 3|n \implies HH^{\top} \equiv 0 \pmod 3 \implies C \subset C^{\perp}.$$

The ternary code of H is self-dual

Lemma

Let n be an integer divisible by 4. If $3|n$ and $9 \nmid n$, then the ternary code of a Hadamard matrix of order n is self-dual.

In particular, for $n = 24$, the ternary code C_3 of $H^\top$, (H: a Hadamard matrix of order 24) is self-dual.

$$C_3 = \text{ span of rows of } H^\top \; = \text{ span of columns of } H$$
$$C_3^\perp = (\text{ span of columns of } H\ )^\perp = \text{ left kernel of } H$$

$$\begin{aligned} C_3 = C_3^\perp &= \text{left kernel of } H \\ &= \{v \mid vH = 0\}. \end{aligned}$$

The binary code of H is doubly even self-dual

A binary code C is said to be doubly even if

$$\mathrm{wt}(x) \equiv 0 \pmod 4 \quad (\forall x \in C).$$

Lemma

Let C be the binary code of a Hadamard matrix of order n.

- If $n \equiv 8 \pmod{16}$, then C is doubly even self-dual.

In particular, for $n = 24$, the binary code C_2 of H, (H: a Hadamard matrix of order 24) is doubly even self-dual.

H: a Hadamard matrix of order 24

- C_3: the ternary code of $H^\top$.
- $C_3 = C_3^\perp$, C_3 has only weights divisible by 3.
- C_2: the binary code of H.
- $C_2 = C_2^\perp$, C_2 has only weights divisible by 4 (doubly even).

Fact (Assmus–Key, 1992)

The following are equivalent:

- C_2 has minimum weight 8 (largest).
- C_3 has minimum weight 9 (largest).

It turns out C_3 has no vectors of weight 3 for any H.

H: a Hadamard matrix of order 24

Theorem

The following are equivalent.

1. C_2 has weight 4.
2. C_3 has weight 6.

Proof.

$$\begin{array}{ccc}
\frac{1}{\sqrt{3}}v \in \frac{1}{\sqrt{3}}\mathbb{Z}^{24} & \xrightarrow{\text{isometry } \frac{1}{\sqrt{24}}H} & \frac{1}{\sqrt{2}}u = \frac{1}{\sqrt{2}}\frac{1}{6}vH \in \frac{1}{\sqrt{2}}\mathbb{Z}^{24} \\
\text{lift}\uparrow & & \downarrow \bmod 2 \\
v \in C_3,\ \mathrm{wt} = 6 & & u \in C_2,\ \mathrm{wt} = 4
\end{array}$$

$v \in C_3 =$ left kernel of $H \implies vH \equiv 0 \pmod 3$ (In fact, $vH \equiv 0 \pmod 6$). Moreover, $2 = \|\frac{1}{\sqrt{3}}v\|^2 = \|\frac{1}{\sqrt{2}}u\|^2$. □

Unimodular lattices

$$\frac{1}{\sqrt{3}}v \in \frac{1}{\sqrt{3}}\mathbb{Z}^{24} \xrightarrow{\text{isometry } \frac{1}{\sqrt{24}}H} \frac{1}{\sqrt{2}}u = \frac{1}{\sqrt{2}}\frac{1}{6}vH \in \frac{1}{\sqrt{2}}\mathbb{Z}^{24}$$

The idea behind this is that, the isometry $\frac{1}{\sqrt{24}}H$ maps the unimodular lattice

$$\frac{1}{\sqrt{3}}C_3 + \sqrt{3}\mathbb{Z}^{24}$$

to a “neighbor” of the unimodular lattice

$$\frac{1}{\sqrt{2}}C_2 + \sqrt{2}\mathbb{Z}^{24}$$

and $\frac{1}{\sqrt{3}}v$, $\frac{1}{\sqrt{2}}u$ are “roots” of these.

H: a Hadamard matrix of order 48

Similarly, one can consider a code over $\mathbb{Z}/4\mathbb{Z}$, the ring of integers modulo 4. The Euclidean weight of a vector $v \in (\mathbb{Z}/4\mathbb{Z})^n$ is

$$\mathrm{wt}(v) = \sum_{i=1}^{n} v_i^2,$$

where we regard $v_i \in \{0, \pm 1, 2\} \subset \mathbb{Z}$.

Theorem (Munemasa–Tamura, 2012)

- C_4: the code over $\mathbb{Z}/4\mathbb{Z}$ with generator matrix $B = \frac{1}{2}(H + J)$.
- C_3: the ternary code of $H^\top$.

Then both C_4 and C_3 are self-dual. Moreover, the following are equivalent:

- C_4 has minimum Euclidean weight 24 (largest).
- C_3 has minimum weight 15 (largest).

H: a Hadamard matrix of order 48

Theorem (Munemasa–Tamura, 2012)

- C_4: the code over $\mathbb{Z}/4\mathbb{Z}$ with generator matrix $B = \frac{1}{2}(H+J)$.
- C_3: the ternary code of $H^\top$.

Then both C_4 and C_3 are self-dual. Moreover, the following are equivalent:

- C_4 has minimum Euclidean weight 24 (largest).
- C_3 has minimum weight 15 (largest).

$$\begin{array}{ccc} \frac{1}{\sqrt{3}}v \in \frac{1}{\sqrt{3}}\mathbb{Z}^{24} & \xrightarrow{\text{isometry } \frac{1}{\sqrt{48}}H} & \frac{1}{2}u = \frac{1}{2}\frac{1}{6}vH \in \frac{1}{2}\mathbb{Z}^{24} \\ \text{lift}\uparrow & & \downarrow \bmod 4 \\ v \in C_3,\ \mathrm{wt} = 12 & & u \in C_2,\ \mathrm{wt} = 16 \end{array}$$

This is not sufficient; one must also consider smaller weights.

Hadamard matrices of order 48 and ternary codes

Theorem

If C is a ternary self-dual code of length 48 and minimum weight 15 (largest possible), then C is the ternary code of a Hadamard matrix.

Unlike the case $n = 24$, the following problem is still open.

Problem

- classify ternary self-dual codes of length 48 with minimum weight 15, or
- classify Hadamard matrices of order 48 whose ternary code has minimum weight 15.