Binary and Ternary Codes of Hadamard Matrices*

Akihiro Munemasa

February 18, 2007

Abstract

Let H be a Hadamard matrix of order 24. In this note, we show that the extremality of the binary code of H is equivalent to the extremality of the ternary code of H^T. This fact has been observed by Assmus and Key [1], as a result of the complete classification of Hadamard matrices of order 24. Our proof is a consequence of more general results on the minimum weight of the dual code of the code of a Hadamard matrix, and does not depend on the classification of Hadamard matrices of order 24.

1 Introduction

A Hadamard matrix is a square matrix H of order n with entries ± 1 satisfying $HH^T = nI$. If p is an odd prime such that $n \equiv 0 \pmod{p}$ and $n \not\equiv 0 \pmod{p^2}$, then the row vectors of a Hadamard matrix of order n generate a self-dual code of length n over $\mathbb{F}_p$. In particular, every Hadamard matrix of order 24 generates a ternary self-dual code length 24. A ternary self-dual code of length 24 is called extremal if its minimum weight is 9. Such codes have been classified, and there are exactly two extremal ternary self-dual codes of length 24, up to equivalence. It is known that, from the classification of Hadamard matrices of order 24, there are exactly two Hadamard matrices,

*A talk given at Kunitachi One Day Seminar on Design Theory, Hitotsubashi University, February 19, 2007.

up to equivalence, which generate extremal ternary self-dual codes. One is the Paley matrix, and the other is the matrix $H58$.

For a Hadamard matrix H, the matrix $B = \frac{1}{2}(H + J)$ is called the binary Hadamard matrix associated to H. A Hadamard matrix H is said to be normalized if all the entries of its first row are 1. For a normalized Hadamard matrix H, the binary code generated by the binary Hadamard matrix associated to H is called the binary code of H. It is not difficult to check that if H, H' are equivalent normalized Hadamard matrices, then the binary codes of H, H' are equivalent. The binary code of a Hadamard matrix of order n is self-dual if $n \equiv 8 \pmod{16}$ (see [2, Section 17.3]). In particular, the binary code of every normalized Hadamard matrix of order 24 is a binary doubly even self-dual code length 24. A binary doubly even self-dual code length 24 is called extremal if its minimum weight is 8. The extended binary Golay code is the unique extremal binary doubly even self-dual code length 24. It is known that, from the classification of Hadamard matrices of order 24, there are exactly two normalized Hadamard matrices, up to equivalence, whose binary codes are equivalent to the extended binary Golay code. One is the Paley matrix, and the other is the matrix $H8$.

Among the sixty equivalence classes of Hadamard matrices of order 24, only two correspond to extremal ternary self-dual codes, and also only two correspond to extremal binary doubly even self-dual codes. Somewhat remarkable fact [1] was that, apart from the Paley matrix which is common to the ternary and the binary cases, the transpose of the Hadamard matrix $H58$ is equivalent to the matrix $H8$. Since the Paley matrix is equivalent to its transpose, this phenomenon makes one wonder if there is any reason why the extremality of the ternary code of a Hadamard matrix is equivalent to the extremality of the binary code of its transpose. The purpose of this note is to give a theoretical explanation of this phenomenon, which does not depend on the classification of Hadamard matrices of order 24.

2 Rank of Hadamard matrices

Lemma 1. *For a prime p and a matrix $A \in M_n(\mathbb{Z})$, we have*

$$\mathrm{rank}_p(A) + v_p(\det A) \geq n.$$

Proof. Let $d_1|d_2|\ldots|d_n$ be the elementary divisors of A, so that

$$PAQ = \mathrm{diag}(d_1, \ldots, d_n)$$

for some matrices $P, Q \in GL(n, \mathbb{Z})$. Set

$$r = \max\{i \mid d_i \not\equiv 0 \pmod{p}\}.$$

Then

$$\begin{aligned}
\operatorname{rank}_p(A) + v_p(\det A) &= \operatorname{rank}_p(PAQ) + v_p(\prod_{i=1}^{n} d_i) \\
&= \operatorname{rank}_p(\operatorname{diag}(d_1, \ldots, d_n)) + \sum_{i=1}^{n} v_p(d_i) \\
&= r + \sum_{i=r+1}^{n} v_p(d_i) \\
&\geq r + \sum_{i=r+1}^{n} 1 \\
&= n.
\end{aligned}$$

□

Lemma 2. *Let p be a prime, and let $A \in M_n(\mathbb{Z})$ be a matrix of which the greatest common divisor of the row sums is d. If $d \equiv 0 \pmod{p}$, then*

$$\operatorname{rank}_p(A) + v_p(\det A) \geq n + v_p(d) - 1.$$

Proof. Let $r_1, \ldots, r_n$ be the row sums of A. Then there exists a matrix $P \in GL(n, \mathbb{Z})$ such that

$$P \begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{pmatrix} = \begin{pmatrix} d \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

This implies

$$PA \begin{pmatrix} 1 & & & \\ 1 & 1 & & \\ \vdots & & \ddots & \\ 1 & & & 1 \end{pmatrix} = \begin{pmatrix} d & * \\ 0 & A' \end{pmatrix}$$

for some $A' \in M_{n-1}(\mathbb{Z})$. Since $d \equiv 0 \pmod{p}$, Lemma 1 implies

$$\begin{aligned}\operatorname{rank}_p(A) + v_p(\det A) &= \operatorname{rank}_p(A') + v_p(\det A') + v_p(d) \\ &\geq (n-1) + v_p(d).\end{aligned}$$

□

Lemma 3. *Let H be a Hadamard matrix of order n, p a prime such that $v_p(n) = 1$. Then the row vectors of H generate a self-dual code of length n over $\mathbb{F}_p$.*

Proof. Let C be the code over $\mathbb{F}_p$ generated by the row vectors of H. Clearly, C is self-orthogonal. Since

$$\begin{aligned}\dim C &= \operatorname{rank}_p H \\ &\geq n - v_p(\det H) && \text{(by Lemma 1)} \\ &= n - v_p(n^{n/2}) \\ &= n - \frac{n}{2} v_p(n) \\ &= \frac{n}{2} \\ &\geq \dim C,\end{aligned}$$

we have $\dim C = \frac{n}{2}$, hence C is self-dual. □

Lemma 4. *Let H be a Hadamard matrix of order n, normalized in such a way that the entries of its first row are all 1. Let B be the binary Hadamard matrix associated to H. Then*

$$\det B = \pm \frac{n^{n/2}}{2^{n-1}}.$$

Proof. Since

$$\begin{aligned}BB^T &= \frac{1}{4}(H+J)(H^T+J) \\ &= \frac{1}{4}\left(nI + nJ + \begin{pmatrix} n & \cdots & n \\ & & \\ & 0 & \end{pmatrix} + \begin{pmatrix} n & & \\ \vdots & & 0 \\ n & & \end{pmatrix}\right)\end{aligned}$$

$$= \frac{n}{4} \begin{pmatrix} 4 & 2 & \cdots & 2 \\ 2 & 2 & & 1 \\ \vdots & & \ddots & \\ 2 & 1 & & 2 \end{pmatrix},$$

we have

$$\begin{aligned} (\det B)^2 &= \det BB^T \\ &= \left(\frac{n}{4}\right)^n \det \begin{pmatrix} 4 & 2 & \cdots & 2 \\ 2 & 2 & & 1 \\ \vdots & & \ddots & \\ 2 & 1 & & 2 \end{pmatrix} \\ &= \left(\frac{n}{4}\right)^n \det \begin{pmatrix} 4 & 0 & \cdots & 0 \\ 2 & 1 & & 0 \\ \vdots & & \ddots & \\ 2 & 0 & & 1 \end{pmatrix} \\ &= \frac{n^n}{4^{n-1}}, \end{aligned}$$

and the result follows. □

Lemma 5. *Let H be a Hadamard matrix of order $n \equiv 8 \pmod{16}$, normalized in such a way that the entries of its first row are all 1. Let B be the binary Hadamard matrix associated to H. Then the row vectors of B generate a binary doubly even self-dual code of length n.*

Proof. Let C be the binary code generated by the row vectors of B. Since $n \equiv 0 \pmod 8$, C is doubly even. Since H is normalized, the row sums of B are $n, n/2, \ldots, n/2$ whose greatest common divisor is $n/2$. Since

$$\begin{aligned} \dim C &= \operatorname{rank}_2 B \\ &\geq n - v_2(\det B) + v_2(\frac{n}{2}) - 1 && \text{(by Lemma 2)} \\ &= n - v_2\left(\frac{n^{n/2}}{2^{n-1}}\right) + 1 && \text{(by Lemma 4)} \\ &= 2n - v_2(n^{n/2}) \\ &= 2n - \frac{n}{2} v_2(n) \end{aligned}$$

$$
\begin{aligned}
&= 2n - \frac{3n}{2} \\
&= \frac{n}{2} \\
&\geq \dim C,
\end{aligned}
$$

we have $\dim C = \frac{n}{2}$, hence C is self-dual. □

3 Minimum weight of codes of Hadamard matrices

Lemma 6. *Let H be a Hadamard matrix of order n, C the ternary code generated by the rows of H. Then $C^\perp$ has no codeword of weight 3.*

Proof. Suppose that $C^\perp$ has a codeword of weight 3. Then there exists a set $\{\boldsymbol{h}_1, \ldots, \boldsymbol{h}_3\}$ of three columns of H and $\varepsilon_1, \varepsilon_2, \varepsilon_3 \in \{\pm 1\}$ such that

$$\sum_{j=1}^{3} \varepsilon_j \boldsymbol{h}_j \equiv 0 \pmod 3.$$

But this forces $\varepsilon_1 \boldsymbol{h}_1 = \varepsilon_2 \boldsymbol{h}_2 = \varepsilon_3 \boldsymbol{h}_3$, which contradicts $(\boldsymbol{h}_1, \boldsymbol{h}_2) = 0$. □

Lemma 7. *Let $\boldsymbol{b} = (b_1, \ldots, b_m) \in \mathbb{F}_2^m$. Then $\mathrm{wt}(\boldsymbol{b})$ is even if and only if $\sum_{i=1}^m (-1)^{b_i} \equiv m \pmod 4$.*

Proof. This is immediate from $\sum_{i=1}^m (-1)^{b_i} = m - 2\,\mathrm{wt}(\boldsymbol{b})$. □

Lemma 8. *Let m be a positive integer, and let K be a $2m \times n$ matrix with entries in $\{\pm 1\}$ satisfying $KK^T = nI_{2m}$. If $\mathbf{1}_{2m} K \equiv 0 \pmod{2m}$, then $\mathbf{1}_{2m} K$ has $\frac{n}{2m}$ entries equal to $\pm 2m$, and all other entries are 0.*

Proof. For a subset S of $M = \{1, \ldots, 2m\}$, set

$$
\begin{aligned}
A_S &= \{j \mid 1 \leq j \leq n,\ S = \{i \mid K_{ij} = 1\}\}, \\
a_S &= |A_S|.
\end{aligned}
$$

Then clearly

$$
\begin{aligned}
\{1, \ldots, n\} &= \bigcup_S A_S \quad \text{(disjoint)}, \\
n &= \sum_S a_S,
\end{aligned}
$$

where S runs through all subsets of M. Since $\mathbf{1}_{2m}K \equiv 0 \pmod{2m}$, and $-2m \le (\mathbf{1}_{2m}K)_j \le 2m$, we have $(\mathbf{1}_{2m}K)_j \in \{0, \pm 2m\}$ for all j. Thus $a_S = 0$ unless $|S| = 0, m$ or $2m$. Since

$$\begin{aligned}
0 &= \sum_{i_1 \neq i_2} (KK^T)_{i_1,i_2} \\
&= \sum_{i_1 \neq i_2} \sum_{j=1}^{n} K_{i_1 j} K_{i_2 j} \\
&= \sum_{i_1 \neq i_2} \sum_{S} \sum_{j \in A_S} (-1)^{|S \cap \{i_1\}|+1} (-1)^{|S \cap \{i_2\}|+1} \\
&= \sum_{i_1 \neq i_2} \sum_{S} (-1)^{|S \cap \{i_1, i_2\}|} a_S. \\
&= \sum_{S} a_S \sum_{i_1 \neq i_2} (-1)^{|S \cap \{i_1, i_2\}|} \\
&= a_\emptyset \sum_{i_1 \neq i_2} (-1)^0 + a_M \sum_{i_1 \neq i_2} (-1)^2 + \sum_{|S|=m} a_S \sum_{i_1 \neq i_2} (-1)^{|S \cap \{i_1, i_2\}|} \\
&= 2m(2m-1)(a_\emptyset + a_M) + \sum_{|S|=m} a_S (2m(m-1) - 2m^2) \\
&= 4m^2(a_\emptyset + a_M) - 2m \sum_{S} a_S \\
&= 4m^2(a_\emptyset + a_M) - 2mn,
\end{aligned}$$

we have

$$\begin{aligned}
\frac{n}{2m} &= a_\emptyset + a_M \\
&= |A_\emptyset \cup A_M| \\
&= |\{j \mid 1 \le j \le n,\ |\{i \mid K_{ij} = 1\}| = 0 \text{ or } 2m\}| \\
&= |\{j \mid 1 \le j \le n,\ (\mathbf{1}_{2m}K)_j = \pm 2m\}|.
\end{aligned}$$

□

Theorem 9. *Let H be a Hadamard matrix of order n, and let B be the binary Hadamard matrix associated to H. Let C_p be the code over $\mathbb{F}_p$ generated by the rows of H^T, where p is an odd prime, and let C_2 be the binary code generated by the rows of B together with the all-ones vector. Then the following statements hold.*

(i) *If $C_2^{\perp}$ has a codeword of weight 4, then C_p has a codeword of weight $n/4$.*

(ii) *If $C_3^{\perp}$ has a codeword of weight 6, then C_2 has a codeword of weight $n/6$.*

Proof. (i) If $C_2^{\perp}$ has a codeword of weight 4, then there is a set of 4 columns of B whose sum is 0 modulo 2. By Lemma 7, this implies that there is a set of 4 rows of H^T whose sum is 0 modulo 4. Let K be the $4 \times n$ matrix formed by these 4 rows. Then by Lemma 8, $\mathbf{1}_4 K$ has $n/4$ entries equal to ± 4, and all other entries are 0. Thus, $\mathbf{1}_4 K \bmod p$ is a codeword of C_p of weight $n/4$.

(ii) If $C_3^{\perp}$ has a codeword of weight 6, then there is a set of 6 columns of H^T whose sum with coefficients ± 1 is 0 modulo 3, or equivalently, there is a set of 6 rows of H whose sum with coefficients ± 1 is 0 modulo 6. Multiplying some of these 6 rows of H by -1, we obtain a Hadamard matrix H' of which there is a set of 6 rows whose sum with is 0 modulo 6. Let K be the $6 \times n$ matrix formed by these 6 rows of H'. Then by Lemma 8, $\mathbf{1}_6 K$ has $n/6$ entries equal to ± 6, and all other entries are 0. Let $K^{(2)}$ denote the submatrix of $B' = \frac{1}{2}(J + H')$ corresponding to the 6 rows of K. Then $\mathbf{1}_6 K^{(2)}$ has $n/6$ entries equal to 0 or 6, and $5n/6$ entries equal to 3. Thus, $\mathbf{1}_6 K^{(2)} \bmod 2$ has weight $5n/6$. Since the matrices H and H' differ in signs of some rows, the matrices B and B' are the same up to the exchange of 0 and 1 in some rows. This implies that the row vectors modulo 2 belong to C_2, and hence C_2 has a codeword of weight $5n/6$. Since C_2 contains the all-ones vector, there is a codeword of weight $n/6$. □

A ternary self-dual $[n, n/2]$ code C has minimum weight at most $3\lfloor n/12 \rfloor + 3$, and C is called extremal if C has minimum weight exactly $3\lfloor n/12 \rfloor + 3$. For $n = 24$, extremal ternary self-dual codes are those self-dual codes having no codewords of weight 3 or 6. It is known that there are two extremal ternary self-dual codes of length 24 up to equivalence (see [3]).

A binary doubly even self-dual $[n, n/2]$ code C has minimum weight at most $4\lfloor n/24 \rfloor + 4$, and C is called extremal if C has minimum weight exactly $4\lfloor n/24 \rfloor + 4$. For $n = 24$, extremal binary doubly even self-dual codes are those binary doubly even self-dual codes having no codewords of weight 4. It is known that there is a unique extremal binary doubly even self-dual code of length 24 up to equivalence, namely, the extended binary Golay code.

Corollary 10. *Let H be a normalized Hadamard matrix of order 24, C_2 the binary code of H. Let C_3 be the ternary code generated by the rows of*

H^T. *Then* C_3 *is an extremal self-dual* $[24, 12, 9]$ *code if and only if* C_2 *is an extremal doubly even self-dual binary* $[24, 12, 8]$ *code.*

Proof. Note that C_3 is self-dual by Lemma 3, while C_2 is doubly even self-dual by Lemma 5. Since C_2 contains the all-ones vector, Theorem 9 implies that C_3 has a codeword of weight 6 if and only if C_2 has a codeword of weight 4, or equivalently, C_2 is non-extremal. Since C_3 has no codeword of weight 3 by Lemma 6, the former condition is equivalent to C_3 being non-extremal. □

Acknowledgements
I would like to thank Masaaki Kitazume for bringing this problem to the author's attention. I would also like to thank Masaaki Harada for helpful discussions.

References

[1] E. F. Assmus, Jr. and J. D. Key, "Designs and Their Codes," Cambridge University Press, Cambridge, 1992.

[2] M. Hall, Jr., "Combinatorial Theory," 2nd edition, Wiley, New York, 1986.

[3] J.S. Leon, V. Pless and N.J.A. Sloane, On ternary self-dual codes of length 24, IEEE Trans. Inform. Theory 27 (1981), 176–180.