Codes and Lattices of Hadamard Matrices

Akihiro Munemasa
Graduate School of Information Sciences
Tohoku University
munemasa@math.is.tohoku.ac.jp

June 12, 2007

Let H be a Hadamard matrix of order 24 whose first row is the all-ones vector. Let $C_3(H)$ denote the ternary code generated by the rows of H:

$$C_3(H) = \mathbb{F}_3^{24} H.$$

Let $B = \frac{1}{2}(H + J)$ be the binary Hadamard matrix associated to H, and let $C_2(H)$ denote the binary code generated by the rows of B:

$$C_2(H) = \mathbb{F}_2^{24} B.$$

Then

- $C_3(H)$ is a self-dual code with minimum weight 6 or 9.
- $C_2(H)$ is a doubly even self-dual code with minimum weight 4 or 8.

As a consequence of complete classification of Hadamard matrices of order 24 (there are 60 of them, up to equivalence, see [4, 5]), Assmus and Key [1] observed the following:

Observation. *$C_2(H)$ has minimum weight 8 if and only if $C_3(H^T)$ has minimum weight 9.*

Note that $C_2(H)$ has minimum weight 8 if and only if it is equivalent to the extended binary Golay code, while $C_3(H^T)$ has minimum weight 9 if and only if it is an extremal ternary self-dual $[24, 12, 9]$ codes which were classified in [6]. I found in January 2007, a proof which does not use the classification. In March 2007, I found another proof using lattices. In this report, I give the latter proof.

Let

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

Then $\Lambda(H)$ is an even unimodular lattice, and its minimum norm is 2 or 4.

Theorem 1. *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.*

Note that there are exactly two Hadamard matrices satisfying the conditions of Theorem 1. For one of these Hadamard matrices, the code $C_3(H^T)$ is the quadratic residue code, and for the other Hadamard matrix, $C_3(H^T)$ is the Pless symmetry code. For both of these Hadamard matrices, $C_2(H)$ is the binary extended Golay code, and $\Lambda(H)$ is the Leech lattice.

An interesting point is how the transpose of H come into play in (ii). The equivalence of (i) and (ii) can be shown directly (indeed this was the proof I discovered in January 2007), and that explains why H^T appears in (ii). The other proof involving (iii) also explains why H^T appears, as you will see below.

To prove Theorem 1, set

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

and observe

$$\begin{aligned} \text{(iii)} &\iff \Lambda(H) \text{ has minimum norm } > 2 \\ &\iff \Lambda_0(H) \text{ has minimum norm } > 2. \end{aligned}$$

Indeed, since $\Lambda(H) \setminus \Lambda_0(H) \subset \frac{1}{2\sqrt{2}}(1+2\mathbb{Z})^{24}$, $\Lambda(H) \setminus \Lambda_0(H)$ has minimum norm at least 3.

There are two unimodular lattices containing $\Lambda_0(H)$, other than $\Lambda(H)$. These are given by the following lemma.

Lemma 2. *The lattice $\Lambda_0(H)$ is a sublattice of index 2 in $\Lambda(H)$. The two unimodular lattices containing $\Lambda_0(H)$, other than $\Lambda(H)$ are*

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

In particular,

$$\begin{aligned} \Lambda_0(H) &= \{x \in \Lambda'(H) \mid \|x\|^2 \equiv 0 \pmod 2\} &(1)\\ &= \{x \in \Lambda''(H) \mid \frac{1}{\sqrt{2}}x \cdot \mathbf{1} \equiv 0 \pmod 2\}. &(2)\end{aligned}$$

Proof. Since

$$\mathbb{Z}^{48}\begin{bmatrix} H+J \\ 8I \end{bmatrix} \subset (2\mathbb{Z})^{24}$$

and $4e_1 + \mathbf{1} \notin (2\mathbb{Z})^{24}$, we have $\Lambda(H) \supsetneq \Lambda_0(H)$. Since

$$2(4e_1 + \mathbf{1}) = 8e_1 + (H+J)_1 \in \mathbb{Z}^{48}\begin{bmatrix} H+J \\ 8I \end{bmatrix},$$

we have $|\Lambda(H) : \Lambda_0(H)| = 2$.

Clearly, $\Lambda_0(H) \subset \Lambda'(H) \cap \Lambda''(H)$. Since $\Lambda_0(H)$ is even and $\Lambda'(H)$ is odd, $\Lambda_0(H) \subsetneq \Lambda'(H)$. Since $\Lambda'(H) = \langle \Lambda_0(H), \frac{1}{2\sqrt{2}}\mathbf{1}\rangle$ and $2 \cdot \frac{1}{2\sqrt{2}}\mathbf{1} \in \Lambda_0(H)$, we obtain $|\Lambda'(H) : \Lambda_0(H)| = 2$. Since $\Lambda''(H)$ is even, we have $\Lambda'(H) \neq \Lambda''(H)$ and since

$$\Lambda''(H) \subset \frac{1}{2\sqrt{2}}(2\mathbb{Z})^{24} \not\supset \Lambda(H),$$

we have $\Lambda''(H) \neq \Lambda(H)$.

Since $\mathbb{F}_2^{24}(\frac{1}{2}(H+J))$ is a self-dual code, $\Lambda''(H)$ is unimodular. Thus $\det \Lambda''(H) = 1 = \det \Lambda(H)$, and hence by [2, p.2],

$$\begin{aligned} |\Lambda''(H) : \Lambda_0(H)|^2 &= \frac{\det \Lambda_0(H)}{\det \Lambda''(H)} \\ &= \frac{\det \Lambda_0(H)}{\det \Lambda(H)} \\ &= |\Lambda(H) : \Lambda_0(H)|^2 \\ &= 2^2. \end{aligned}$$

The two expressions (1) and (2) for $\Lambda_0(H)$ follows by observing that each forms a proper sublattice of $\Lambda(H)$ containing $\Lambda_0(H)$. $\square$

By (1), we find

$$\begin{aligned}
&\min \Lambda_0(H)\\
&= \frac{1}{8}\min\{\|x\|^2 \mid 0 \neq x \in \mathbb{Z}^{48}\begin{bmatrix} H \\ 8I \end{bmatrix}\frac{1}{\sqrt{24}}H^T,\ \|x\|^2 \equiv 0 \pmod{16}\}\\
&= \frac{1}{3}\min\{\|x\|^2 \mid 0 \neq x \in \mathbb{Z}^{48}\begin{bmatrix} H^T \\ 3I \end{bmatrix},\ \|y\|^2 \equiv 0 \pmod{16}\}\\
&= \begin{cases} 2 & \text{if } C_3(H^T) \text{ has a codeword of weight 6,}\\ 4 & \text{otherwise.}\end{cases}
\end{aligned}$$

Also, by (2), we find

$$\begin{aligned}
\min \Lambda_0(H) &= \frac{1}{8}\min\{\|x\|^2 \mid 0 \neq x \in \mathbb{Z}^{48}\begin{bmatrix} H+J \\ 4I \end{bmatrix},\ x\cdot\mathbf{1} \equiv 0 \pmod{8}\}\\
&= \frac{1}{2}\min\{\|y\|^2 \mid 0 \neq y \in \mathbb{Z}^{48}\begin{bmatrix} B \\ 2I \end{bmatrix},\ y\cdot\mathbf{1} \equiv 0 \pmod{4}\}\\
&= \begin{cases} 2 & \text{if } C_2(H) \text{ has a codeword of weight 4,}\\ 4 & \text{otherwise.}\end{cases}
\end{aligned}$$

This completes the proof of Theorem 1.

References

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

[2] W. Ebeling, "Lattices and Codes," 2nd ed., Vieweg, 2002.

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

[4] N. Ito, J.S. Leon and J.Q. Longyear, Classification of 3-$(24, 12, 5)$ designs and 24-dimensional Hadamard matrices, J. Combin. Theory, Ser. A 31 (1981), 66–93.

[5] H. Kimura, New Hadamard matrix of order 24, Graphs Combin. 5 (1989), 235–242.

[6] 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.