European Journal of Combinatorics 33 (2012) 519–533

Contents lists available at SciVerse ScienceDirect

European Journal of Combinatorics

journal homepage: www.elsevier.com/locate/ejc

The codes and the lattices of Hadamard matrices

Akihiro Munemasa, Hiroki Tamura

Graduate School of Information Sciences, Tohoku University, Sendai, 980-8579, Japan

ARTICLE INFO

Article history:
Received 10 November 2010
Accepted 19 September 2011
Available online 7 January 2012

ABSTRACT

It has been observed by Assmus and Key as a result of the complete classification of Hadamard matrices of order 24, that the extremality of the binary code of a Hadamard matrix H of order 24 is equivalent to the extremality of the ternary code of H^T. In this note, we present two proofs of this fact, neither of which depends on the classification. One is a consequence of a more general result on the minimum weight of the dual of the code of a Hadamard matrix. The other relates the lattices obtained from the binary code and the ternary code. Both proofs are presented in greater generality to include higher orders. In particular, the latter method is also used to show the equivalence of (i) the extremality of the ternary code, (ii) the extremality of the $\mathbb{Z}_4$-code, and (iii) the extremality of a lattice obtained from a Hadamard matrix of order 48.

1. Introduction

A Hadamard matrix is a square matrix H of order n with entries ± 1 satisfying $HH^T = nI$, where I denotes the identity matrix. If m is an odd integer such that $n \equiv 0 \pmod{m}$ and $(m, \frac{n}{m}) = 1$, then the row vectors of a Hadamard matrix of order n generate a self-dual code of length n over $\mathbb{Z}/m\mathbb{Z}$, called the code of H over $\mathbb{Z}/m\mathbb{Z}$. In particular, the ternary code of a Hadamard matrix of order 24 is a self-dual code of length 24. A ternary self-dual code of length 24 is called extremal if its minimum weight is 9. Such codes have been classified in [13], 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 (see [9–11]), there are exactly two Hadamard matrices, up to equivalence, whose codes are extremal ternary self-dual codes. One is the Paley matrix, and the other is the matrix $H58$ (cf [1]).

For a Hadamard matrix H, the matrix $B = \frac{1}{2}(H + J)$, where J denotes the all-one matrix, is called the binary Hadamard matrix associated to H. A Hadamard matrix H is said to be normalized if all

E-mail addresses: munemasa@math.is.tohoku.ac.jp (A. Munemasa), tamura@ims.is.tohoku.ac.jp (H. Tamura).

0195-6698/$ – see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ejc.2011.11.007

the entries of its first row are 1. For a normalized Hadamard matrix H, the binary code generated by the row vectors of 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 Hadamard equivalent normalized Hadamard matrices, then the binary codes of H, H' are equivalent. The binary code of a Hadamard matrix of order n is doubly even self-dual if $n \equiv 8 \pmod{16}$ (see [7, Section 17.3]). More generally, the code over $\mathbb{Z}/2m\mathbb{Z}$ generated by the row vectors of B is type II self-dual if $n \equiv 0 \pmod{8m}$ and $(2m, \frac{n}{8m}) = 1$. In particular, the binary code of every normalized Hadamard matrix of order 24 is a binary doubly even self-dual code of length 24. A binary doubly even self-dual code of 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 $H8$ (cf [1]).

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, p. 286] 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 Hadamard equivalent to the matrix $H8$. Since the Paley matrix is Hadamard 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 paper is to give a theoretical explanation of this phenomenon, which does not depend on the classification of Hadamard matrices of order 24. Two different proofs will be given of this fact. In Section 3, we give an elementary and direct method to analyze the existence of a codeword of small Euclidean norm in the dual of the code of a Hadamard matrix. This method can be adapted to deal with the binary case, and the proof is a simple consequence (Corollary 10). In Section 4, we will consider the unimodular lattices obtained from the $\mathbb{Z}_m$-code and the $\mathbb{Z}_{n/4m}$-code of a (binary) Hadamard matrix of order n. It is shown in particular, that the lattice obtained from the ternary code of a Hadamard matrix H of order 24 is isometric to a neighbor L of the lattice L_2 obtained from the binary code of H. Then the extremality of the ternary code or that of the binary code is shown to be equivalent to the common neighbor Λ of L and L_2 being the Leech lattice. We also show that the extremality of the ternary code of a Hadamard matrix of order 48 is equivalent to the extremality (in the sense of Euclidean norm) of the $\mathbb{Z}_4$-code of its binary transpose, and to the extremality of the even unimodular lattice obtained as above Λ. We note that a weaker equivalence for order 48 will be proved in Section 3 without using lattices.

2. Elementary divisors of Hadamard matrices

We denote the all-one matrix by J, and the all-one vector by $\mathbf{1}$. We also denote by e_i the vector with a 1 in the i-th coordinate and 0 elsewhere. We refer the reader to [14] for unexplained terminology in codes.

Lemma 1. *If positive integers x, y, z, w satisfy $xy = wz$ and $(x, y) = 1$, then $x = (x, z)(x, w)$.*

The following lemma follows immediately from [18, Chap. II, Exercise 4]. See also [20, Part 4, Theorem 10.7].

Lemma 2. *Let H be a Hadamard matrix of order n, and let $d_1|d_2|\cdots|d_n$ be the elementary divisors of H. Then we have $d_i d_{n+1-i} = n$ for all i.*

Proof. Take $P, Q \in GL(n, \mathbb{Z})$ so that $PHQ = \mathrm{diag}(d_1, \ldots, d_n)$. Then we have $Q^{-1}H^TP^{-1} = \mathrm{diag}(\frac{n}{d_1}, \ldots, \frac{n}{d_n})$ and $\frac{n}{d_n}|\cdots|\frac{n}{d_2}|\frac{n}{d_1}$ are also the elementary divisors of H. $\square$

Lemma 3. *Let H be a Hadamard matrix of order n, m an integer such that $m|n$ and $(m, \frac{n}{m}) = 1$. Then the row vectors of H generate a self-dual code of length n over $\mathbb{Z}/m\mathbb{Z}$.*

Proof. Let C be the code over $\mathbb{Z}/m\mathbb{Z}$ generated by the row vectors of H. Clearly, C is self-orthogonal. Let $d_1|d_2|\cdots|d_n$ be the elementary divisors of H. Since

$$\begin{aligned}|C| &= \prod_{i=1}^{n} \frac{m}{(m, d_i)} \\ &= \prod_{i=1}^{n/2} \frac{m}{(m, d_i)} \cdot \frac{m}{(m, n/d_i)} \quad \text{(by Lemma 2)} \\ &= \prod_{i=1}^{n/2} \frac{m^2}{m} \quad \text{(by Lemma 1)} \\ &= m^{n/2}.\end{aligned}$$

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. If the elementary divisors of H are $1 = d_1|d_2|\cdots|d_n$, then those of B are $1|\frac{d_2}{2}|\cdots|\frac{d_n}{2}$.*

Proof. We can assume that H is normalized as $\begin{pmatrix} 1 & \dots & 1 \\ -1 & & \\ \vdots & H' & \\ -1 & & \end{pmatrix}$. Then

$$\begin{pmatrix} 1 & 0\dots0 \\ 1 & \\ \vdots & I_{n-1} \\ 1 & \end{pmatrix} H = \begin{pmatrix} 1 & \dots & 1 \\ 0 & & \\ \vdots & H'+J & \\ 0 & & \end{pmatrix}$$

and

$$B = \frac{1}{2}(H+J) = \begin{pmatrix} 1 & \dots & 1 \\ 0 & & \\ \vdots & \frac{1}{2}(H'+J) & \\ 0 & & \end{pmatrix}.$$

The result follows by comparing the above two equalities. □

Let m be a positive integer, and set $V = \mathbb{Z}/m\mathbb{Z}$. We regard an element $u \in V$ as an element of the set of integers $\{0, 1, \dots, m-1\}$, and define the Lee weight and the Euclidean norm of an element $u \in V$ by

$$\begin{aligned}&\mathrm{Lee}(u) = \min\{u, m-u\}, \\ &\mathrm{Norm}(u) = (\mathrm{Lee}(u))^2.\end{aligned}$$

For a vector $u = (u_1, \dots, u_n) \in V^n$, we set

$$\mathrm{Norm}(u) = \sum_{i=1}^{n} \mathrm{Norm}(u_i).$$

Alternatively, the Euclidean norm can be defined as

$$\mathrm{Norm}(u) = \min\{\|v\|^2 \mid v \in \mathbb{Z}^n, v \bmod m = u\}.$$

Recall that a self-dual code over $\mathbb{Z}/2m\mathbb{Z}$ is type II if the Euclidean norm of every codeword is divisible by $4m$.

Lemma 5. *Let H be a normalized Hadamard matrix of order n, B the binary Hadamard matrix associated to H. Let $\ell \geq 2$ be an integer such that $4\ell | n$ and $(\ell, \frac{n}{4\ell}) = 1$. Then the row vectors of B generate a self-dual code over $\mathbb{Z}/\ell\mathbb{Z}$ of length n, which is type II if ℓ is even.*

Proof. Let C be the code over $\mathbb{Z}/\ell\mathbb{Z}$ generated by the row vectors of B. Since H is normalized, we have

$$\begin{aligned} BB^T &= \frac{1}{4}(H+J)(H^T+J) \\ &= \frac{n}{4}(I + e_1^T\mathbf{1} + \mathbf{1}^T e_1 + J) \\ &\equiv 0 \pmod{\ell}. \end{aligned} \tag{1}$$

Thus C is self-orthogonal. Let $d_1|d_2|\cdots|d_n$ be the elementary divisors of H. Since

$$(\ell, d_i/2)(\ell, n/2d_i) = (\ell, d_i/2)(\ell, (n/4)/(d_i/2)) = \ell$$

by Lemma 1, we have

$$\begin{aligned} |C| &= \ell \prod_{i=2}^{n} \frac{\ell}{(\ell, d_i/2)} \quad \text{(by Lemma 4)} \\ &= \ell \prod_{i=2}^{n/2} \frac{\ell}{(\ell, d_i/2)} \cdot \frac{\ell}{(\ell, n/2d_i)} \quad \text{(by Lemma 2)} \\ &= \ell \prod_{i=2}^{n/2} \frac{\ell^2}{\ell} \\ &= \ell^{n/2}. \end{aligned}$$

Thus C is self-dual. Finally, since $\ell | \frac{n}{4}$, (1) implies that the diagonal entries of BB^T are divisible by 2ℓ. Thus C is type II if ℓ is even by Bannai et al. [2, Lemma 2.2]. □

3. Minimum weights of codes of Hadamard matrices

We introduce two types of pair of norms of a vector over $V = \mathbb{Z}/m\mathbb{Z}$. First, assume m is odd. We define the odd norm and the even norm by

$$\begin{aligned} \mathrm{Norm_o}(u) &= \min(\{\|v\|^2 \mid v \in \mathbb{Z}^n,\ v \bmod m = u\} \cap (1+2\mathbb{Z})), \\ \mathrm{Norm_e}(u) &= \min(\{\|v\|^2 \mid v \in \mathbb{Z}^n,\ v \bmod m = u\} \cap 2\mathbb{Z}). \end{aligned}$$

The assumption that m be odd is required to ensure that both parities occur among the norms of vectors v satisfying $v \bmod m = u$. If $u = v \bmod m$ and $\mathrm{Norm}(u) = \|v\|^2$, then

$$\begin{aligned} \{\mathrm{Norm_o}(u), \mathrm{Norm_e}(u)\} &= \{\|v\|^2, \min_i\{\|v \pm me_i\|^2\}\} \\ &= \left\{\mathrm{Norm}(u), \mathrm{Norm}(u) + m\left(m - 2\max_i\{\mathrm{Lee}(u_i)\}\right)\right\}. \end{aligned} \tag{2}$$

In particular, for $u \neq 0$, we have

$$|\mathrm{Norm_o}(u) - \mathrm{Norm_e}(u)| \leq m^2 - 2m.$$

Lemma 6. *Let H be a Hadamard matrix of order n, and let C be the code over $\mathbb{Z}/m\mathbb{Z}$ generated by the rows of H, where $m \geq 3$ is an odd integer. Then the following statements hold.*

(i) *$C^\perp$ has no codeword of odd norm less than m^2,*
(ii) *For any $u \in C^\perp \setminus \{0\}$, we have $\mathrm{Norm}(u) \geq 2m$. Equality holds only if nonzero entries of u are all equal to 1 or -1.*

Proof. (i) Let v be a vector in $\mathbb{Z}^n$ such that $v \bmod m$ is $u \in C^\perp$ and $\|v\|^2 = \mathrm{Norm}_o(u)$. Then we have $vH^T \equiv 0 \pmod m$ and $vH^T \equiv v\mathbf{1}^T\mathbf{1} \equiv \mathbf{1} \pmod 2$ and thus $vH^T \equiv m\mathbf{1} \pmod{2m}$. So we have $\|v\|^2 = \frac{1}{n}vH^THv^T = \frac{1}{n}\|vH^T\|^2 \ge m^2$.
(ii) By (i) and (2), we have

$$m^2 \le \mathrm{Norm}_o(u) \le \mathrm{Norm}(u) + m\left(m - 2\max_i\{\mathrm{Lee}(u_i)\}\right).$$

So we have $1 \le \max_i\{\mathrm{Lee}(u_i)\} \le \frac{\mathrm{Norm}(u)}{2m}$. $\square$

Next, we define type I norm and type II norm for an integer m and $u \in \mathbf{1}^\perp \subset V^n$ by

$$\mathrm{Norm}_{\mathrm{I}}(u) = \min\{\|v\|^2 \mid v \in \mathbb{Z}^n,\ v \bmod m = u,\ v \cdot \mathbf{1} \equiv m \pmod{2m}\},$$
$$\mathrm{Norm}_{\mathrm{II}}(u) = \min\{\|v\|^2 \mid v \in \mathbb{Z}^n,\ v \bmod m = u,\ v \cdot \mathbf{1} \equiv 0 \pmod{2m}\}.$$

If $u = v \bmod m$ and $\mathrm{Norm}(u) = \|v\|^2$, then

$$\begin{aligned}\{\mathrm{Norm}_{\mathrm{I}}(u), \mathrm{Norm}_{\mathrm{II}}(u)\} &= \left\{\|v\|^2, \min_i\{\|v \pm me_i\|^2\}\right\}\\ &= \left\{\mathrm{Norm}(u), \mathrm{Norm}(u) + m\left(m - 2\max_i\{\mathrm{Lee}(u_i)\}\right)\right\}. \qquad (2')\end{aligned}$$

In particular, for $u \ne 0$, we have

$$|\mathrm{Norm}_{\mathrm{I}}(u) - \mathrm{Norm}_{\mathrm{II}}(u)| \le m^2 - 2m.$$

Lemma 7. *Let H be a normalized Hadamard matrix of order n, and let B be the binary Hadamard matrix associated to H. Let C be the code over $\mathbb{Z}/\ell\mathbb{Z}$ generated by the rows of B, where $\ell \ge 2$ is an integer. Then the following statements hold.*

(i) *$C^\perp$ has no codeword of type* I *norm less than ℓ^2,*
(ii) *For any $u \in C^\perp \setminus \{0\}$, we have* $\mathrm{Norm}(u) \ge 2\ell$. *Equality holds only if nonzero entries of u are all equal to* 1 *or* -1.

Proof. (i) Let v be a vector in $\mathbb{Z}^n$ such that $v \bmod \ell$ is $u \in C^\perp$, $v \cdot \mathbf{1} \equiv \ell \pmod{2\ell}$ and $\|v\|^2 = \mathrm{Norm}_{\mathrm{I}}(u)$. Then we have $vB^T \equiv 0 \pmod \ell$ and thus $vH^T = v(2B^T - J) = 2vB^T - (v\cdot\mathbf{1})\mathbf{1} \equiv \ell\mathbf{1} \pmod{2\ell}$. So we have $\|v\|^2 = \frac{1}{n}\|vH^T\|^2 \ge \ell^2$.
(ii) The proof is similar to that of Lemma 6(ii). $\square$

When m is odd, and $u \in \mathbf{1}^\perp$, then

$$\mathrm{Norm}_{\mathrm{I}}(u) = \mathrm{Norm}_o(u),$$
$$\mathrm{Norm}_{\mathrm{II}}(u) = \mathrm{Norm}_e(u).$$

The Euclidean norm over $\mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/3\mathbb{Z}$ is equal to the weight. Moreover both type I norm and type II norm over $\mathbb{Z}/2\mathbb{Z}$ are equal to the weight.

The minimum odd, even, type I, and type II norms of a code C over $\mathbb{Z}/m\mathbb{Z}$ are defined by

$$\min(\{\mathrm{Norm}_*(u) \mid u \in C\} \setminus \{0\}), \quad * = \mathrm{o}, \mathrm{e}, \mathrm{I}, \mathrm{II},$$

respectively, provided m is odd for $* =$ o,e, $C \subset \mathbf{1}^\perp$ for $* =$ I,II. Note that the minimum odd norm and the minimum type I norm of a code over $\mathbb{Z}/m\mathbb{Z}$ is at most m^2 which is the odd norm and the type I norm of the zero vector.

Theorem 8. *Let H be a normalized Hadamard matrix of order n, and let B be the binary Hadamard matrix associated to H. Let $m \ge 3$ be an odd integer, and let $\ell \ge 2$ be an integer satisfying $(\ell, m) = 1$ and $n \equiv 0 \pmod{4\ell m}$. Let C_m be the code over $\mathbb{Z}/m\mathbb{Z}$ generated by the rows of H^T, and let C'_ℓ be the code over $\mathbb{Z}/\ell\mathbb{Z}$ generated by the rows of B. Then the following statements hold.*

(i) *Suppose* $C_m^\perp$ *has a codeword of even norm* d *and odd norm* m^2+k *where* $k < d - d/\ell$. *Then there exists a vector* $v \in \mathbb{Z}^n$ *such that* $u = (1/2m)vH \mod \ell$ *is a nonzero codeword of* C'_ℓ *with* $\mathrm{Norm}_{\mathrm{II}}(u) \le dn/4m^2$. *If, moreover* $d < 2m\lfloor(\ell+2)/2\rfloor$, *then* $\mathrm{Norm}_{\mathrm{II}}(u) = \mathrm{Norm}(u) = dn/4m^2$, *and if* $k = 0$, *then* $\mathrm{Norm}_{\mathrm{II}}(u) = \mathrm{Norm}(u) = \mathrm{wt}(u) = dn/4m^2$.

(ii) *Suppose* $C_\ell'^\perp$ *has a codeword of type* II *norm* d *and type* I *norm* ℓ^2+k *where* $k < d - d/m$. *Then there exists a vector* $v \in \mathbb{Z}^n$ *such that* $u = (1/2\ell)vH^T \mod m$ *is a nonzero codeword of* C_m *with* $\mathrm{Norm}_{\mathrm{e}}(u) \le dn/4\ell^2$. *If, moreover* $d < \ell(m+1)$, *then* $\mathrm{Norm}_{\mathrm{e}}(u) = \mathrm{Norm}(u) = dn/4\ell^2$, *and if* $k = 0$, *then* $\mathrm{Norm}_{\mathrm{e}}(u) = \mathrm{Norm}(u) = \mathrm{wt}(u) = dn/4\ell^2$.

Proof. (i) By the assumption, there exists a vector $v \in \mathbb{Z}^n$ satisfying $vH \equiv 0 \pmod{2m}$, $\|v\|^2 = d$ and $\|v - me_i\|^2 = m^2 + k$ for some i. Let $c = (c_1, \ldots, c_n) = \frac{1}{2m}vH$. We will show that $c \mod \ell$ is a nonzero codeword of C'_ℓ with the desired property. Since $(\ell, m) = 1$, there exists an integer t such that $mt \equiv 1 \pmod{\ell}$, and $c = \frac{1}{m}(vB - \frac{1}{2}vJ) \equiv t(vB - \frac{v\cdot\mathbf{1}}{2}\mathbf{1}) \pmod{\ell}$. Thus $c \mod \ell$ is a codeword of C'_ℓ, and since $c\mathbf{1}^T = \frac{n}{2m}v_1 \equiv 0 \pmod{2\ell}$, we have

$$\mathrm{Norm}_{\mathrm{II}}(c \mod \ell) \le \|c\|^2 = \frac{1}{(2m)^2}vHH^Tv^t = \frac{dn}{4m^2}.$$

We show $c \mod \ell \ne 0$. We have $(v - me_i)H = m(2c_1 - h_{i1}, \ldots, 2c_n - h_{in})$ where $H = (h_{ij})_{i,j}$, and

$$dn = \|vH\|^2 = 4m^2\sum_{j=1}^n c_j^2,$$

$$\begin{aligned}(m^2+k)n = \|(v-me_i)H\|^2 &= m^2\sum_{j=1}^n(2c_j - h_{ij})^2\\ &= m^2n + 4m^2\sum_{j=1}^n c_j(c_j - h_{ij}).\end{aligned}$$

Since $k\ell < d(\ell-1)$, we have

$$\begin{aligned}\sum_{j=1}^n |c_j|(|c_j| - \ell) &= \sum_{j=1}^n (c_j^2 - \ell|c_j|)\\ &\le \sum_{j=1}^n (c_j^2 - \ell h_{ij}c_j)\\ &= \sum_{j=1}^n (\ell c_j(c_j - h_{ij}) - (\ell-1)c_j^2)\\ &= \frac{k\ell n}{4m^2} - \frac{d(\ell-1)n}{4m^2}\\ &= \frac{(k\ell - d(\ell-1))n}{4m^2}\\ &< 0.\end{aligned}$$

Thus there exists $j \in \{1, \ldots, n\}$ such that $0 < |c_j| < \ell$. Therefore, $c \mod \ell \ne 0$.

It remains to show $\mathrm{Norm}(c \mod \ell) = \mathrm{Norm}_{\mathrm{II}}(c \mod \ell) = \|c\|^2$ when $d < 2m\lfloor\frac{\ell+2}{2}\rfloor$ or $k = 0$. This will follow if $|c_j| \le \lfloor\frac{\ell}{2}\rfloor$ for all j. If $d < 2m\lfloor\frac{\ell+2}{2}\rfloor$, we have $|c_j| = |(\frac{1}{2m}vH)_j| \le \lfloor\frac{\|v\|^2}{2m}\rfloor \le \frac{d}{2m} < \lfloor\frac{\ell+2}{2}\rfloor$ and thus $|c_j| \le \lfloor\frac{\ell}{2}\rfloor$. If $k = 0$, we have $c_j(c_j - h_{ij}) = 0$ and thus $c_j \in \{0, \pm1\}$, which implies $\mathrm{wt}(c \mod \ell) = \|c\|^2$.

(ii) If $C_\ell'^\perp$ has such a codeword, then there exists a vector $v \in \mathbb{Z}^n$ satisfying $vB^T \equiv 0 \pmod{\ell}$, $v \cdot \mathbf{1} \equiv 0 \pmod{2\ell}$, $\|v\|^2 = d$ and $\|v - \ell e_i\|^2 = \ell^2 + k$ for some i. Since $H^T = 2B^T - J$, we have $vH^T \equiv -(v \cdot \mathbf{1})\mathbf{1} \equiv 0 \pmod{2\ell}$. Let $c = (c_1, \dots, c_n) = \frac{1}{2\ell} vH^T$. Since $(2\ell, m) = 1$, there exists an integer t such that $2\ell t \equiv 1 \pmod m$, and $c \equiv tvH^T \pmod m$. Thus $c \bmod m$ is a codeword of C_m, and since $\|c\|^2 \equiv ch_1^T = \frac{n}{2\ell} v_1 \equiv 0 \pmod 2$ where h_1^T is the first column of H, we have

$$\mathrm{Norm}_{\mathrm{e}}(c \bmod m) \le \|c\|^2 = \frac{1}{(2m)^2} vH^T H v^t = \frac{dn}{4m^2}.$$

By the same argument as above, we have $c \not\equiv 0 \pmod m$ for $k < d - \frac{d}{m}$. In particular, for all j, we have $|c_j| < \frac{m}{2}$ if $d < \ell(m+1)$, and $c_j \in \{0, \pm 1\}$ if $k = 0$. $\square$

Corollary 9. *Under the same assumption and notation as in Theorem 8, the following hold for* $0 < d < 2\ell m$.

(i) *If* $C_m^\perp$ *has a codeword of even norm* d, *then* C'_ℓ *has a nonzero codeword of type* II *norm at most* $dn/4m^2$.
(ii) *If* $C'^\perp_\ell$ *has a codeword of type* II *norm* d, *then* C_m *has a nonzero codeword of even norm at most* $dn/4\ell^2$.

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 [13]).

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. *Let* C_3 *be the ternary code generated by the rows of* H^T, *and let* C'_2 *be the binary code of* H. *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. By Lemmas 3 and 5, C_3 is self-dual while C'_2 is doubly even self-dual. Since C_3 has no codeword of weight 3 by Lemma 6(ii), it suffices to show that C_3 has a codeword of weight 6 if and only if C'_2 has a codeword of weight 4. This follows immediately from Corollary 9. $\square$

Next, we consider the case $(\ell, m, n) = (4, 3, 48)$.

Corollary 11. *Let* H *be a normalized Hadamard matrix of order* 48, *and let* B *the binary Hadamard matrix associated to* H. *Let* C_3 *be the ternary code generated by the rows of* H^T, *and let* C'_4 *be the code over* $\mathbb{Z}/4\mathbb{Z}$ *generated by the rows of* B. *Then the following statements hold.*

(i) *Let* $d = 2, 3$ *or* 4. *If* C_3 *has a codeword of weight* $3d$, *then* C'_4 *has a codeword of type* II *norm* $8\lceil \frac{d}{2} \rceil$, *and moreover whose nonzero entries are all equal to* ± 1 *when* $d = 2$ *or* 3.
(ii) *Let* $d = 2$ *or* 4. *If* C'_4 *has a codeword* u *of type* II *norm* $4d$, *then* C_3 *has a nonzero codeword of weight at most* $3d$, *and exactly* $3d$ *when* $\mathrm{Norm}_{\mathrm{I}}(u) = 16$.
(iii) C_3 *is an extremal self-dual* $[48, 24, 15]$ *code if and only if* C'_4 *has minimum type* II *norm* 24.

Proof. By Lemmas 3 and 5, C_3 is self-dual while C'_4 is type II self-dual. Since the even norm and the odd norm of a nonzero vector over $\mathbb{Z}/3\mathbb{Z}$ of weight $3d$ are $6\lceil \frac{d}{2} \rceil$ and $6\lfloor \frac{d}{2} \rfloor + 3$ respectively, the even norm is less than $2\lfloor \frac{\ell+2}{2} \rfloor m = 18$ for $d \le 4$ and the odd norm is 9 for $d = 2, 3$. Thus (i) follows from Theorem 8(i). (ii) follows from Theorem 8(ii). As for (iii), first note that by Lemma 6, C_3 is an extremal self-dual $[48, 24, 15]$ code if and only if C_3 has no codeword of weight 6,9 or 12. By (i) and (ii), this is equivalent to the non-existence of codewords of type II norm 8 or 16 in C'_4. $\square$

We will show in the next section that the condition (iii) in Corollary 11 is also equivalent to C'_4 having minimum Euclidean norm 24.

Remark 12. It is known that there are at least two inequivalent extremal ternary self-dual codes of length 48, the quadratic residue code and the Pless symmetry code. The codewords of weight 48 in these codes constitute the rows and their negatives of a Hadamard matrix ([5, Sections 2.8, 2.10 of Chap. 3]). We will also show in the next section that this is the case for any extremal ternary self-dual [48, 24, 15] code.

4. Lattices

We refer the reader to [5] for unexplained terminology in lattices. We write $\Lambda \cong \Lambda'$ if the two lattices Λ and Λ' are isometric. Let C be a code of length n over $\mathbb{Z}/m\mathbb{Z}$ with generator matrix H. We regard the entries of H as integers, and let $\mathbb{Z}^k H$ denote the row $\mathbb{Z}$-module of H, that is, the set of $\mathbb{Z}$-linear combinations of the row vectors of H, where k is the number of rows of H. The lattice $A(C)$ of the code C is defined as $A(C) = \frac{1}{\sqrt{m}}\mathbb{Z}^{k+n}\begin{bmatrix} H \\ mI \end{bmatrix}$, and $A(C)$ is integral (resp. unimodular, even unimodular) if and only if C is self-orthogonal (resp. self-dual, type II). If m is odd and C is a self-orthogonal code over $\mathbb{Z}_m$, then

$$\min(\{\|x\|^2 \mid x \in A(C) \setminus \sqrt{m}\mathbb{Z}^n\} \cap 2\mathbb{Z}) = \frac{1}{m} \min_{u \in C \setminus \{0\}} \mathrm{Norm}_e(u),$$

and thus

$$\min(\{\|x\|^2 \mid 0 \neq x \in A(C)\} \cap 2\mathbb{Z}) = \min\left\{2m, \frac{1}{m} \min_{u \in C \setminus \{0\}} \mathrm{Norm}_e(u)\right\}. \tag{3}$$

If C is a self-orthogonal code over $\mathbb{Z}_m$ satisfying $C \subset \mathbf{1}^{\perp}$, then

$$\min\left\{\|x\|^2 \mid 0 \neq x \in A(C),\ \frac{1}{\sqrt{m}} x \cdot \mathbf{1} \equiv 0 \bmod 2\right\} = \min\left\{2m, \frac{1}{m} \min_{u \in C \setminus \{0\}} \mathrm{Norm}_{\mathrm{II}}(u)\right\}. \tag{4}$$

Lemma 13. *Let H be a normalized Hadamard matrix, and let $B = \frac{1}{2}(H + J)$ be the binary Hadamard matrix associated to H. Let $m \geq 3$ be an odd integer. Then H and B generate the same code over $\mathbb{Z}/m\mathbb{Z}$.*

Proof. The code generated by H can also be generated by $\mathbf{1}$ and $H + J = 2B$. Since m is odd, B and $2B$ generate the same code over $\mathbb{Z}/m\mathbb{Z}$, while the first row of B is $\mathbf{1}$ since H is normalized. The result follows. □

In the following, let $m \geq 3$ be an odd integer, ℓ an integer such that $(\ell, m) = 1$, H a normalized Hadamard matrix of order $n = 4\ell m$. Then by Lemma 3, the code C_m over $\mathbb{Z}/m\mathbb{Z}$ generated by the row vectors of H^T is self-dual, and thus the lattice

$$A(C_m) = \frac{1}{\sqrt{m}}\mathbb{Z}^{2n}\begin{bmatrix} H^T \\ mI \end{bmatrix}$$

is odd unimodular.

Let $h_1 = [h_{11} \dots h_{n1}]$ be the transpose of the first column of H, and let $D = \mathrm{diag}(h_1)$. Since $H^T D$ is normalized, we have

$$A(C_m)D = \frac{1}{\sqrt{m}}\mathbb{Z}^{2n}\begin{bmatrix} \frac{1}{2}(H^T D + J) \\ mI \end{bmatrix},$$

by Lemma 13, thus

$$A(C_m) = \frac{1}{\sqrt{m}}\mathbb{Z}^{2n}\begin{bmatrix} \frac{1}{2}(H^T + \mathbf{1}^T h_1) \\ mI \end{bmatrix} = \frac{1}{\sqrt{m}}\mathbb{Z}^{2n+1}\begin{bmatrix} \frac{1}{2}(H^T + \mathbf{1}^T h_1) \\ m(I + \mathbf{1}^T e_1) \\ me_1 \end{bmatrix}. \tag{5}$$

This implies

$$A(C_m)\frac{1}{\sqrt{n}}H = \frac{1}{\sqrt{\ell}}\mathbb{Z}^{2n+1}\begin{bmatrix} \ell(I+\mathbf{1}^T e_1) \\ \frac{1}{2}(H+J) \\ \frac{1}{2}\mathbf{1} \end{bmatrix}. \tag{6}$$

So when $\ell = 1$, the lattice $A(C_m)$ is equivalent to the unimodular lattice

$$D_n^+ = \mathbb{Z}^{n+1}\begin{bmatrix} I+\mathbf{1}^T e_1 \\ \frac{1}{2}\mathbf{1} \end{bmatrix}.$$

For the remainder of this section, we assume $\ell > 1$. By Lemma 5, the code C'_ℓ over $\mathbb{Z}/\ell\mathbb{Z}$ generated by the row vectors of $\frac{1}{2}(H+J)$ is self-dual, and thus the lattice

$$A(C'_\ell) = \frac{1}{\sqrt{\ell}}\mathbb{Z}^{2n}\begin{bmatrix} \frac{1}{2}(H+J) \\ \ell I \end{bmatrix} = \frac{1}{\sqrt{\ell}}\mathbb{Z}^{2n+1}\begin{bmatrix} \frac{1}{2}(H+J) \\ \ell(I+\mathbf{1}^T e_1) \\ \ell e_1 \end{bmatrix} \tag{7}$$

is unimodular, which is even if and only if ℓ is even.

By (5), the even sublattice of $A(C_m)$ is

$$B(C_m) = \frac{1}{\sqrt{m}}\mathbb{Z}^{2n}\begin{bmatrix} \frac{1}{2}(H^T+\mathbf{1}^T h_1) \\ m(I+\mathbf{1}^T e_1) \end{bmatrix}. \tag{8}$$

Analogously, we define a sublattice $B(C'_\ell)$ of $A(C'_\ell)$ as

$$B(C'_\ell) = \frac{1}{\sqrt{\ell}}\mathbb{Z}^{2n}\begin{bmatrix} \frac{1}{2}(H+J) \\ \ell(I+\mathbf{1}^T e_1) \end{bmatrix} \subset A(C'_\ell). \tag{9}$$

Then

$$B(C_m) = B(C_m)\frac{1}{\sqrt{n}}H = B(C'_\ell). \tag{10}$$

Since

$$A(C_m)\frac{1}{\sqrt{n}}H \ni \frac{1}{2\sqrt{\ell}}\mathbf{1} \notin A(C'_\ell)$$

by (6) and (7), we see $A(C_m)\frac{1}{\sqrt{n}}H \neq A(C'_\ell)$. Thus there is a unique unimodular lattice containing $B(C'_\ell)$ other than $A(C'_\ell)$ and $A(C_m)\frac{1}{\sqrt{n}}H$ (see [19]). Let $\Lambda(C'_\ell)$ denote this lattice and let

$$\Lambda(C_m) = \Lambda(C'_\ell)\frac{1}{\sqrt{n}}H^T \tag{11}$$

be the unique unimodular lattice containing $B(C_m)$ other than $A(C_m)$ and $A(C'_\ell)\frac{1}{\sqrt{n}}H^T$. The relationship between the lattices introduced so far can conveniently described by the following diagram, where a line denotes inclusion.

$$\begin{tikzcd}[column sep=small]
A(C_m) \arrow[dr, dash] & \Lambda(C_m) \arrow[d, dash] & A(C'_\ell)\frac{1}{\sqrt{n}}H^T \arrow[dl, dash] & & A(C_m)\frac{1}{\sqrt{n}}H \arrow[dr, dash] & \Lambda(C'_\ell) \arrow[d, dash] & A(C'_\ell) \arrow[dl, dash] \\
& B(C_m) \arrow[rrrr, phantom, ""] & \arrow[r, "\frac{1}{\sqrt{n}}H"'] & {} & & B(C'_\ell) &
\end{tikzcd}$$

Since $A(C'_\ell) = B(C'_\ell) \cup (B(C'_\ell) + \sqrt{\ell} e_1)$ by (7) and $A(C_m)\frac{1}{\sqrt{n}}H = B(C'_\ell) \cup (B(C'_\ell) + \frac{1}{2\sqrt{\ell}}\mathbf{1})$ by (6), we have

$$\Lambda(C'_\ell) = \frac{1}{\sqrt{\ell}}\mathbb{Z}^{2n+1}\begin{bmatrix} \frac{1}{2}(H+J) \\ \ell(I + \mathbf{1}^T e_1) \\ \ell e_1 + \frac{1}{2}\mathbf{1} \end{bmatrix}, \tag{12}$$

$$\Lambda(C_m) = \frac{1}{\sqrt{m}}\mathbb{Z}^{2n+1}\begin{bmatrix} \frac{1}{2}(H^T + \mathbf{1}^T h_1) \\ m(I + \mathbf{1}^T e_1) \\ m e_1 + \frac{1}{2}h_1 \end{bmatrix}. \tag{13}$$

Observe also, by (7),

$$A(C'_\ell)\frac{1}{\sqrt{n}}H^T = \frac{1}{\sqrt{m}}\mathbb{Z}^{2n+1}\begin{bmatrix} m(I + \mathbf{1}^T e_1) \\ \frac{1}{2}(H^T + \mathbf{1}^T h_1) \\ \frac{1}{2}h_1 \end{bmatrix}. \tag{14}$$

Then,

$$A(C'_\ell)\frac{1}{\sqrt{n}}H^T \setminus B(C_m) = B(C_m) - \frac{1}{2\sqrt{m}}h_1 \subset \frac{1}{2\sqrt{m}}(1+2\mathbb{Z})^n \tag{15}$$

by (8) and (14),

$$\Lambda(C_m) \setminus B(C_m) = B(C_m) - \frac{1}{\sqrt{m}}\left(m e_1 + \frac{1}{2}h_1\right) \subset \frac{1}{2\sqrt{m}}(1+2\mathbb{Z})^n \tag{16}$$

by (8) and (13),

$$A(C_m)\frac{1}{\sqrt{n}}H \setminus B(C'_\ell) = B(C'_\ell) - \frac{1}{2\sqrt{\ell}}\mathbf{1} \subset \frac{1}{2\sqrt{\ell}}(1+2\mathbb{Z})^n \tag{17}$$

by (6) and (9), and

$$\Lambda(C'_\ell) \setminus B(C'_\ell) = B(C'_\ell) - \frac{1}{\sqrt{\ell}}\left(\ell e_1 + \frac{1}{2}\mathbf{1}\right) \subset \frac{1}{2\sqrt{\ell}}(1+2\mathbb{Z})^n \tag{18}$$

by (9) and (12).

Theorem 14. *Let H be a normalized Hadamard matrix of order $n = 4\ell m$, where $m \geq 3$ is an odd integer, $\ell \geq 2$ an integer such that $(\ell, m) = 1$. For an even integer $d < \min\{2\ell, 2m\}$, the following statements* (i)–(iii) *are equivalent, and moreover if $d \leq \max\{\ell, m + \delta_{\ell \bmod 2, 0}\}$,* (iii) *and* (iv) *are equivalent:*

(i) *C_m has minimum even norm dm,*
(ii) *C'_ℓ has minimum type* II *norm $d\ell$,*
(iii) *$B(C_m)$ has minimum norm d,*
(iv) *$\Lambda(C_m)$ has minimum norm d.*

Proof. The relations between $A(C_m), A(C'_\ell)$ and $B(C_m), B(C'_\ell)$ are given as

$$B(C_m) = \{x \in A(C_m) \mid \|x\|^2 \equiv 0 \pmod 2\},$$
$$B(C'_\ell) = \left\{x \in A(C'_\ell) \mid \frac{1}{\sqrt{\ell}}x \cdot \mathbf{1} \equiv 0 \pmod 2\right\}.$$

Thus, by (3), (4) and (10), we have

$$\begin{aligned}\min B(C_m) &= \min\left\{2m, \frac{1}{m}\min_{u\in C_m\setminus\{0\}}\mathrm{Norm}_{\mathrm{e}}(u)\right\}\\ &= \min B(C'_\ell) = \min\left\{2\ell, \frac{1}{\ell}\min_{u\in C'_\ell\setminus\{0\}}\mathrm{Norm}_{\mathrm{II}}(u)\right\}.\end{aligned} \tag{19}$$

Since $d < \min\{2\ell, 2m\}$, the equivalence of (i)–(iii) is established.

We have $\min(\Lambda(C_m)\setminus B(C_m)) \geq \ell$ by (16) and $\min(\Lambda(C'_\ell)\setminus B(C'_\ell)) \geq m$ by (18), and thus $\min(\Lambda(C_m)\setminus B(C_m)) \geq \max\{\ell, m\}$. If $\ell \equiv 0 \pmod 2$, $\Lambda(C_m)$ is an even lattice, so $\min(\Lambda(C_m)\setminus B(C_m)) \geq \max\{\ell, m+1\}$. This shows the equivalence of (iii) and (iv). □

We have the following as the complement of the above theorem.

Corollary 15. *Let H be a normalized Hadamard matrix of order $n = 4\ell m$, where $m \geq 3$ is an odd integer, $\ell \geq 2$ an integer such that $(\ell, m) = 1$. Let $d = \min\{2\ell, 2m\}$. Then the following statements* (i)–(iii) *are equivalent, and moreover if $d \leq \max\{\ell, m + \delta_{\ell \bmod 2,0}\}$,* (iii) *and* (iv) *are equivalent:*

(i) *C_m has minimum even norm at least (exactly if $d = 2\ell$) dm,*
(ii) *C'_ℓ has minimum type* II *norm at least (exactly if $d = 2m$) $d\ell$,*
(iii) *$B(C_m)$ has minimum norm d,*
(iv) *$\Lambda(C_m)$ has minimum norm d.*

Proof. By Theorem 14, we see the equivalence of (i)′ C_m has minimum even norm less than dm, (ii)′ C'_ℓ has minimum type II norm less than $d\ell$, and (iii)′ $B(C_m)$ has minimum norm less than d. Since $\min B(C_m)$ is at most d by (19), (i)–(iii) are the negatives of (i)′–(iii)′ respectively. Exactness in (i) and (ii) follows from

$$\min B(C_m) = \begin{cases} \dfrac{1}{m}\displaystyle\min_{u\in C_m\setminus\{0\}}\mathrm{Norm}_{\mathrm{e}}(u) & \text{if } d = 2\ell,\\ \dfrac{1}{\ell}\displaystyle\min_{u\in C'_\ell\setminus\{0\}}\mathrm{Norm}_{\mathrm{II}}(u) & \text{if } d = 2m.\end{cases}$$

The equivalence of (iii) and (iv) follows also from Theorem 14 provided $d \leq \max\{\ell, m+\delta_{\ell \bmod 2,0}\}$. □

Note that the minimum norm of C_m and C'_ℓ are both at most $n/2 = 2\ell m$, given by the sum of two distinct rows of H^T for C_m, and by any row except the first one of B for C'_ℓ.

Setting $(\ell, m, n) = (2, 3, 24)$ in Corollary 15, we have another proof of Corollary 10.

Corollary 16. *Let H be a normalized Hadamard matrix of order* 24*. The following statements are equivalent:*

(i) *C_3 has minimum weight* 9*,*
(ii) *C'_2 has minimum weight* 8*,*
(iii) *$\Lambda(C_3)$ has minimum norm* 4 *(hence is isometric to the Leech lattice).*

Proof. Since C_3 has minimum even norm 12 if and only if it has minimum weight 9 by the extremality condition, the result follows from Corollary 15. We note that when (iii) occurs, $\Lambda(C_3)$ is isometric to the Leech lattice by Conway and Sloane [5, chap. 12]. □

Let k be even and let H be a skew Hadamard matrix of order $n = 4k - 4$ with all diagonal entries -1. In [16], McKay gives a even unimodular lattice

$$L = \frac{1}{\sqrt{k}}\mathbb{Z}^{2n}\begin{bmatrix} I_n & H - I_n\\ O & kI\end{bmatrix},$$

and asserts that its minimum norm is 4 for $k \geq 4$ (see also [4]). Without loss of generality, we may assume the first row of H to be $-\mathbf{1}$. Then

$$\tilde{H} = \begin{bmatrix} -H & H^T D \\ H & H^T D \end{bmatrix},$$

where $D = \mathrm{diag}(-1, 1, 1, \dots, 1)$, is a normalized Hadamard matrix. We describe an isometry from L to $\Lambda(C_2')$, where C_2' is the binary doubly even self-dual code obtained from the binary Hadamard matrix associated to $\tilde{H}$. Set

$$U = \frac{1}{2\sqrt{k}} \begin{bmatrix} I_n & -H + I_n \\ H^T - I & I_n \end{bmatrix}.$$

Since U is an orthogonal matrix and

$$LU = \frac{1}{2}\mathbb{Z}^{2n} \begin{bmatrix} 4I_n & O \\ H^T - I_n & I_n \end{bmatrix}.$$

L is isometric to the lattice obtained from the $\mathbb{Z}_4$-code with generator matrix $[H^T - I_n \; I_n]$. Furthermore, set

$$V = \frac{1}{\sqrt{2}} \begin{bmatrix} I_n & D \\ -I_n & D \end{bmatrix}, \quad \text{and}$$

$$M = \frac{1}{2\sqrt{2}} \begin{bmatrix} 4I_n & 4D \\ H^T - 2I_n & H^T D \end{bmatrix}.$$

Then

$$\begin{aligned}
\Lambda(C_2') &= \frac{1}{\sqrt{2}}\mathbb{Z}^{2n+1} \begin{bmatrix} \frac{1}{2}(\tilde{H} + J) \\ 2(I + \mathbf{1}^T e_1) \\ 2e_1 + \frac{1}{2}\mathbf{1} \end{bmatrix} \\
&= \mathbb{Z}^{2n+1} \begin{bmatrix} \frac{1}{2}(H^T + J_n) - \mathbf{1}^T e_1 & -I_n - \mathbf{1}^T e_1 \\ \frac{1}{2}(H^T + J_n) - \mathbf{1}^T e_1 + \frac{n}{4} I_n & -I_n - \mathbf{1}^T e_1 - H \\ \frac{1}{2}(H^T + J_n) - \mathbf{1}^T e_1 & -2(I_n + \mathbf{1}^T e_1) \\ \frac{1}{2}(J_n D - D H^T) + D & 2(I_n + \mathbf{1}^T e_1) D \\ \mathbf{1} - 2e_1 & -3e_1 \end{bmatrix} M \\
&\subset \mathbb{Z}^{2n} M = \frac{1}{2}\mathbb{Z}^{2n} \begin{bmatrix} 4I_n & O \\ H^T - I_n & I_n \end{bmatrix} V = LUV.
\end{aligned}$$

Since L and $\Lambda(C_2')$ are both unimodular and V is an orthogonal matrix, we conclude that L is isometric to $\Lambda(C_2')$.

Corollary 17. *Let H be a normalized Hadamard matrix of order 48. The following statements are equivalent:*

(i) *C_3 has minimum weight 15,*
(ii) *C_4' has minimum type II norm 24,*
(iii) *$B(C_3)$ has minimum norm 6.*

Proof. Since the minimum weight of C_3 is at most 15 by the extremality condition, the result follows by setting $(\ell, m) = (4, 3)$ in Corollary 15. □

As a matter of fact, we have a stronger result by the following argument.

Lemma 18. *Let H be a normalized Hadamard matrix of order $n = 4\ell m$, where $m \geq 3$ is an odd integer, $\ell \geq 2$ an integer such that $(\ell, m) = 1$, and assume H^T is also normalized. Then the number of norm ℓ vectors of $A(C'_\ell) \setminus B(C'_\ell)$ (resp. $\Lambda(C_m) \setminus B(C_m)$) is equal to the number of codewords of C_m of even (resp. odd) weight whose nonzero entries are all equal to* 1.

Proof. Set

$$L = A(C_m) - \frac{1}{2\sqrt{m}}\mathbf{1},$$
$$X = \{x \in L \mid \|x\|^2 = \ell\}.$$

Then every element of X is of the form $v = \frac{1}{2\sqrt{m}}(\pm 1, \ldots, \pm 1)$, and hence the map

$$\rho : X \to C_m$$
$$v \mapsto \left(\sqrt{m}v + \frac{1}{2}\mathbf{1}\right) \bmod m,$$

gives a one-to-one correspondence between X and the set of codewords of C_m whose nonzero entries are all equal to 1. For $v \in X$, we have $\mathrm{wt}(\rho(v)) = \mathrm{Norm}(\rho(v)) = m\|v + \frac{1}{2\sqrt{m}}\mathbf{1}\|^2$. Thus $\mathrm{wt}(\rho(v))$ is even if and only if $v + \frac{1}{2\sqrt{m}}\mathbf{1} \in B(C_m)$. Since H^T is normalized, (10) and (15) imply $(A(C'_\ell) \setminus B(C'_\ell))\frac{1}{\sqrt{n}}H^T = B(C_m) - \frac{1}{2\sqrt{m}}\mathbf{1}$, and hence the set of norm ℓ vectors of $A(C'_\ell) \setminus B(C'_\ell)$ is

$$\left\{\frac{1}{\sqrt{n}}vH \mid v \in X,\ \mathrm{wt}(\rho(v)) \text{ even}\right\}.$$

Similarly, since

$$L = \left(B(C_m) - \frac{1}{2\sqrt{m}}\mathbf{1}\right) \cup \left(B(C_m) - \frac{1}{\sqrt{m}}\left(me_1 + \frac{1}{2}\mathbf{1}\right)\right) \quad \text{(disjoint)},$$

and by (16), the set of norm ℓ vectors of $\Lambda(C_m) \setminus B(C_m)$ is $\{v \in X \mid \mathrm{wt}(\rho(v)) \text{ odd}\}$. □

A ternary self-dual code of length n has minimum weight at most $3\lfloor n/12 \rfloor + 3$ (see [15]), thus at most 15 for $n = 48$. A type II self-dual code over $\mathbb{Z}/4\mathbb{Z}$ of length n has minimum Euclidean norm at most $8\lfloor n/24 \rfloor + 8$ (see [3, Corollary 13]), thus at most 24 for $n = 48$. An n-dimensional even unimodular lattice has minimum norm at most $2\lfloor n/24 \rfloor + 2$, thus at most 6 for $n = 48$. A code or a lattice achieving the upper bound is called extremal.

By Gaborit et al. [6, Proposition 3.3], the complete weight enumerator of any extremal [48, 24, 15] ternary self-dual code with all-one vector is uniquely determined to

$$W(x, y, z) = \sum x^{48} + 94\sum x^{24}y^{24} + x^3y^3z^3(\ldots), \tag{20}$$

given in [12, Table 1], where the sums are to be taken over the cyclic permutations of x, y, z. Now we have the following sharpening of Corollary 11(iii) and Corollary 17.

Theorem 19. *Let H be a normalized Hadamard matrix of order 48, and let B be the binary Hadamard matrix associated to H. Let C_3 be the ternary code generated by the rows of H^T, and let C'_4 be the code over $\mathbb{Z}/4\mathbb{Z}$ generated by the rows of B. The following statements are equivalent:*

(i) *C_3 is extremal,*
(ii) *C'_4 is extremal,*
(iii) *$\Lambda(C_3)$ is extremal.*

Proof. Since any row of B except the first one gives a codeword of C_4' with type II norm 24, (ii) implies that C_4' has minimum type II norm 24. Thus (ii)⇒(i) follows from Corollary 17. If $\Lambda(C_3)$ has minimum norm 6, then by (19), $B(C_3)$ has minimum norm 6. Thus (iii)⇒(i) follows also from Corollary 17.

To prove (i)⇒(ii), suppose that C_3 has minimum weight 15. Let $D = \mathrm{diag}(h_1)$ where h_1 is the first row of H^T. Then $H' = DH$ is a normalized Hadamard matrix such that ${H'}^T$ is also normalized. The rows of $\frac{1}{2}(H' + J)$ generate the $\mathbb{Z}/4\mathbb{Z}$ code C_4' since $\frac{1}{2}D(H' + J) + \frac{1}{2}(\mathbf{1} - h_1)^T\mathbf{1} = B$, while the rows of ${H'}^T$ generate the ternary code C_3D which is equivalent to C_3, and (11) implies $\Lambda(C_3D) \cong \Lambda(C_3)$. Thus, we may assume from the beginning that both H and H^T are normalized. Then Lemma 18 implies

$$|\{v \in A(C_4') \setminus B(C_4') \mid \|v\|^2 = 4\}| = |\{x \in C_3 \cap \{0, 1\}^{48} \mid \mathrm{wt}(x) \text{ even}\}|. \tag{21}$$

Note that $B(C_4') \cong B(C_3)$ has no vector of norm 2 or 4 by (10) and Corollary 17, and $A(C_4') \setminus B(C_4')$ has no vector of norm 2 by (10) and (15). Thus, the left-hand side of (21) coincides with the number of norm 4 vectors in $A(C_4')$. On the other hand, as H^T is normalized, C_3 contains the all-one vector, hence the right-hand side of (21) equals $1 + 94 + 1 = 96$ by (20). It follows that the 96 norm 4 vectors of $A(C_4')$ are $\pm 2e_i$ $(i = 1, \ldots, 48)$, and thus C_4' has no codeword of Euclidean norm 16. Therefore, C_4' has minimum Euclidean norm at least 24, and hence equal to 24. This proves (i)⇒(ii).

Replacing $A(C_4')$ by $\Lambda(C_3)$, $B(C_4')$ by $B(C_3)$ and $\mathrm{wt}(x)$ even by $\mathrm{wt}(x)$ odd in the proof of (i)⇒(ii), and by (16), we have that $\Lambda(C_3)$ has no vector of norm 2 or 4. Since $\Lambda(C_3)$ is even, it has minimum norm 6. This proves (i)⇒(iii). □

As mentioned in Remark 12, there are at least two extremal ternary self-dual [48, 24, 15] codes, namely, the quadratic residue code $C_{48q}^{(3)}$ and the Pless symmetry code $C_{48p}^{(3)}$. The code $C_{48q}^{(3)}$ (resp. $C_{48p}^{(3)}$) corresponds to the extremal $\mathbb{Z}_4$-code $C_{48q}^{(4)}$ (resp. $C_{48p}^{(4)}$), and the extremal even unimodular lattice P_{48q} (resp. P_{48p}) [8]. There is another known extremal even unimodular lattice P_{48n} [17]. But it is not known whether P_{48n} has a corresponding extremal ternary code.

The following is an analogue of [13, Theorem 5].

Theorem 20. *Every extremal ternary self-dual code of length* 48 *is generated by a Hadamard matrix.*

Proof. Without loss of generality, we may assume $\mathbf{1} \in C$. Then (20) implies that C is admissible in the sense of [12]. As remarked at the end of the paper [12], it follows from [12, Proposition 2] that the 96 codewords of weight 48 in C constitute the rows and their negatives of a Hadamard matrix. The result then follows from Lemma 3. □

Acknowledgments

We would like to thank Masaaki Kitazume for bringing this problem to our attention. We would also like to thank Masaaki Harada for helpful discussions. Finally, we would like to thank John McKay for pointing out a connection to his construction of the Leech lattice from a Hadamard matrix of order 12 [16].

References

[1] E.F. Assmus Jr., J.D. Key, Designs and their Codes, Cambridge University Press, Cambridge, 1992.
[2] E. Bannai, S.T. Dougherty, M. Harada, M. Oura, Type II codes, even unimodular lattices, and invariant rings, IEEE Trans. Inform. Theory 45 (1999) 1194–1205.
[3] A. Bonnecaze, P. Solé, C. Bachoc, B. Mourrain, Type II codes over $\mathbb{Z}_4$, IEEE Trans. Inform. Theory 43 (1997) 969–976.
[4] R. Chapman, Double circulant constructions of the Leech lattice, J. Austral. Math. Soc. (Series A) 69 (2000) 287–297.
[5] J.H. Conway, N.J.A. Sloane, Sphere Packing, Lattices and Groups, third ed., Springer-Verlag, New York, 1999.
[6] P. Gaborit, Construction of new extremal unimodular lattices, European J. Combin. 25 (2004) 549–564.
[7] M. Hall Jr., Combinatorial Theory, second ed., Wiley, New York, 1986.
[8] M. Harada, M. Kitazume, A. Munemasa, B. Venkov, On some self-dual codes and unimodular lattices in dimension 48, European J. Combin. 26 (2005) 543–557.
[9] N. Ito, J.S. Leon, J.Q. Longyear, The 24-dimensional Hadamard matrices and their automorphism groups, unpublished.
[10] N. Ito, J.S. Leon, J.Q. Longyear, Classification of 3-(24, 12, 5) designs and 24-dimensional Hadamard matrices, J. Combin. Theory Ser. A 31 (1981) 66–93.
[11] H. Kimura, New Hadamard matrix of order 24, Graphs Combin. 5 (1989) 235–242.

[12] H. Koch, The 48-dimensional analogues of the Leech lattice, Proc. Steklov Inst. Math. 208 (1995) 172–178.
[13] J.S. Leon, V. Pless, N.J.A. Sloane, On ternary self-dual codes of length 24, IEEE Trans. Inform. Theory 27 (1981) 176–180.
[14] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1977.
[15] C.L. Mallows, N.J.A. Sloane, An upper bound for self-dual codes, Inform. Control 22 (1973) 188–200.
[16] J. McKay, A setting for the Leech lattice, in: Finite Groups '72, North-Holland, Amsterdam, 1973, pp. 117–118.
[17] G. Nebe, Some cyclo-quaternionic lattices, J. Algebra 199 (1998) 472–498.
[18] M. Newman, Integral Matrices, in: Pure and Applied Mathematics, vol. 45, Academic Press, New York, 1972.
[19] B.B. Venkov, Odd unimodular lattices, J. Math. Sci. 17 (1986) 1967–1974.
[20] W.D. Wallis, A.P. Street, J.S. Wallis, Combinatorics: Room Squares, Sum-Free Sets, Hadamard Matrices, in: Lecture Notes in Mathematics, vol. 292, Springer-Verlag, Berlin, 1972.