Mathematical Journal of Okayama University

Volume 40, *Issue* 1 | 1998 | *Article* 3

JANUARY 1998

Self-Dual Codes Constructed from Hadamard Matrices

Masaaki Harada*

*Yamagata University

Self-Dual Codes Constructed from Hadamard Matrices

Masaaki Harada

Abstract

In this note, we study self-dual codes constructed from Hadamard matrices. We also give a classification of self-dual codes over Fp constructed from Hadamard matrices of order n for any prime p and n $\leq$12, and p $\leq$ 17 and n = 16 and 20.

Math. J. Okayama Univ. **40** (1998), 15-21 [2000]

SELF-DUAL CODES CONSTRUCTED FROM HADAMARD MATRICES

MASAAKI HARADA

ABSTRACT. In this note, we study self-dual codes constructed from Hadamard matrices. We also give a classification of self-dual codes over $\mathbb{F}_p$ constructed from Hadamard matrices of order n for any prime p and $n \leq 12$, and $p \leq 17$ and $n = 16$ and 20.

1. INTRODUCTION

A linear $[n, k]$ code C over $\mathbb{F}_p$ is a k-dimensional vector subspace of $\mathbb{F}_p^n$, where $\mathbb{F}_p$ is the field with p elements, p prime. The elements of C are called codewords and the Hamming weight $wt(x)$ of a codeword x is the number of its non-zero coordinates. The minimum weight $mw(C)$ of C is defined by $\min\{wt(x) \mid 0 \neq x \in C\}$. An $[n, k, d]$ code is an $[n, k]$ code with minimum weight d. A matrix whose rows generate the code C is called a generator matrix of C. Two codes C and C' over $\mathbb{F}_p$ are *equivalent* if there exists an n by n monomial matrix P with entries from $\{0, 1, -1\}$ such that $C' = CP = \{xP \mid x \in C\}$. The dual code $C^\perp$ of C is defined as $C^\perp = \{x \in \mathbb{F}_p^n \mid x \cdot y = 0 \text{ for all } y \in C\}$. C is *self-dual* if $C = C^\perp$ and C is *self-orthogonal* if $C \subseteq C^\perp$. The *Hamming weight enumerator* is $W_C(x, y) = \sum A_i x^{n-i} y^i$ where there are A_i codewords in C of weight i.

A Hadamard matrix H of order n is an n by n matrix of $\pm$ 1's with $HH^T = nI_n$ where H^T denotes the transpose of H and I_n is the identity matrix of order n. We say that two Hadamard matrices H_1 and H_2 are *equivalent* if there exist monomial matrices P and Q with entries from $\{0, 1, -1\}$ such that $H_2 = PH_1Q$. All Hadamard matrices of order up to 28 have been classified (cf. [5] and the references given therein).

In this note, we study self-dual codes over $\mathbb{F}_p$ constructed from Hadamard matrices. In Section 2, we present a method for constructing self-dual codes from Hadamard matrices and we give some properties for minimum weights of such codes. In Section 3, we give a classification of self-dual codes over $\mathbb{F}_p$ constructed from Hadamard matrices of order n, for any prime p, and $n \leq 12$, and $p \leq 17$ and $n = 16$ and 20.

2. Basic Properties

First we provide a method to construct self-dual codes from Hadamard matrices.

Proposition 2.1. *Let H_n be a Hadamard matrix of order n. Let α be an element of $\mathbb{F}_p$ such that $\alpha^2+n \equiv 0 \pmod{p}$. Then the following two matrices*

$$G_{\pm} = (\ \pm\alpha I \ , \ H_n \ ),$$

generate equivalent self-dual codes over $\mathbb{F}_p$.

Proof. Follows from $G_{\pm} \cdot G_{\pm}^T = 0$ where $G_{\pm}^T$ denotes the transpose of $G_{\pm}$. □

Remark. This construction was mentioned in [1] and [7] for $p = 3$, in [6] for $p = 5$ and in [8] for $p = 7$. These papers motivate us to study self-dual codes over $\mathbb{F}_p$ constructed from Hadamard matrices.

$C_p(H_n)$ denotes the self-dual code over $\mathbb{F}_p$ constructed from a Hadamard matrix H_n by Proposition 2.1. For small n and p, α satisfying the assumption in Proposition 2.1 is listed in Table 1, where a blank means the non-existence of α.

Table 1. Self-dual codes over $\mathbb{F}_p$ from Hadamard matrices

n	2	4	8	12	16	20
$p=5$		1			2	
$p=7$				3		1
$p=11$	3		5			
$p=13$		3		1	6	
$p=17$	7	8	3		1	

Now we investigate some basic properties of the codes $C_p(H_n)$ where $p \geq 5$. First we consider properties of the minimum weight of $C_p(H_n)$. As mentioned in [6], an upper bound on the minimum weight $mw(C_p(H_n))$ of $C_p(H_n)$ is obtained from the observation that a sum of any two rows of H_n has weight $n/2$. Thus we have

$$mw(C_p(H_n)) \leq 2 + n/2. \tag{1}$$

Similarly we have the following lemma for the weight of a sum of at most three rows.

Lemma 2.2. *Let $G = (\ \alpha I_n \ , \ H_n \ )$ be the generator matrix of a self-dual code $C_p(H_n)$ $(p \geq 5)$, r_i, r_j and r_k being any distinct rows of G. Let β, γ and δ be non-zero elements of $\mathbb{F}_p$. Then*

(1) $wt(\beta r_i) = 1 + n$,
(2) $wt(\beta r_i + \gamma r_j) \geq 2 + n/2$ *and*
(3) $wt(\beta r_i + \gamma r_j + \delta r_k) \geq 3 + 3n/4$.

Proof. It is sufficient to prove (3). Let $v(x)$ denote the right half of a vector x. Without loss of generality we can assume that $v(\beta r_i)$, $v(\gamma r_j)$ and $v(\delta r_k)$ take the following form:

$$\begin{aligned} v(\beta r_i) &= (\beta, \cdots, \beta \quad \beta, \cdots, \beta \quad \beta, \cdots, \beta \quad \beta, \cdots, \beta\ ), \\ v(\gamma r_j) &= (\gamma, \cdots, \gamma \quad \gamma, \cdots, \gamma \quad -\gamma, \cdots, -\gamma \quad -\gamma, \cdots, -\gamma), \\ v(\delta r_k) &= (\underbrace{\delta, \cdots, \delta}_{(a)} \quad \underbrace{-\delta, \cdots, -\delta}_{(b)} \quad \underbrace{\delta, \cdots, \delta}_{(c)} \quad \underbrace{-\delta, \cdots, -\delta}_{(d)}), \end{aligned}$$

where each partition (a), (b), (c) and (d) consists of $n/4$ coordinates. If the sum of a partition is the zero-vector then the sums of other three partitions are nonzero-vectors. Thus we can prove (3). □

This lemma gives the following bound on the minimum weight of $C_p(H_n)$.

Proposition 2.3. *Let H_n be a Hadamard matrix of order n. Let $C_p(H_n)$ be the self-dual code from H_n with $p \geq 5$. Then*

(1) $mw(C_p(H_n)) = n/2 + 2$, *for* $2 \leq n \leq 12$,
(2) $mw(C_p(H_n)) = 8$, *for* $n = 16$ *and*
(3) $8 \leq mw(C_p(H_n)) \leq n/2 + 2$, *for* $20 \leq n$.

Proof. It follows from (1) and Lemma 2.2 that $mw(C_p(H_2)) = 3$ and $mw(C_p(H_4)) = 4$.

For $n = 8$ suppose that the minimum weight $d \leq 5$. Let $x = (u(x), v(x))$ be a codeword of weight d where $u(x)$ and $v(x)$ are vectors of $\mathbb{F}_p^4$. Clearly $d = wt(u(x)) + wt(v(x))$. Since the code is self-dual, the parity check matrix $P = (\ -{H_8}^T\ ,\ \alpha I_8\ )$ also generates the same code. Hence if $wt(u(x)) = k$ then the codeword x is a sum of k rows of G, moreover x is also a sum of $(d-k)$ rows of P. Thus it is sufficient to consider the weight of a sum of at most two rows of G and P. Since Lemma 2.2 holds even for the parity check matrix P, the weight of a sum of at most two rows of G or P is greater than or equal to 6.

For $n \geq 12$ we show that $mw(C_p(H_n)) \geq 8$. Similarly as in the case of $n = 8$, a codeword of weight $d \leq 7$ can be expressed as a sum of at most three rows of the generator matrix G or the parity check matrix P. The weight of a sum of at most three rows of G or P is greater than or equal to 8. Moreover when $n = 16$, any Hadamard matrix has a submatrix of the following form:

$$\begin{pmatrix} ++++ & ++++ & ++++ & ++++ \\ ++++ & ++++ & ---- & ---- \\ ++++ & ---- & ++++ & ---- \\ ++++ & ---- & ---- & ++++ \end{pmatrix},$$

where $+$ and $-$ denote 1 and -1, respectively. Thus there exists a codeword of weight 8. □

3. Classification of Self-Dual Codes Constructed from Hadamard Matrices

In this section, we give a classification of self-dual codes over $\mathbb{F}_p$ constructed from Hadamard matrices of order n for small n and p.

3.1. Lengths up to 24. Even if the following two lemmas may be trivial, the lemmas are useful when we classify self-dual codes constructed by Proposition 2.1 from Hadamard matrices of fixed order.

Lemma 3.1. *Let C and C' be linear $[2n, n]$ codes over $\mathbb{F}_p$ whose generator matrices are $(\ \alpha I_n\ ,\ A\ )$ and $(\ \alpha I_n\ ,\ A^T\ )$ respectively. If C is a self-dual code then C and C' are equivalent.*

Proof. Since C is self-dual, the parity check matrix $P = (\ -A^T\ ,\ \alpha I_n\ )$ of C is also a generator matrix of C. The code with generator matrix P is equivalent to C'. □

Lemma 3.2. *Let H and H' be two equivalent Hadamard matrices of order n. Then the self-dual codes over $\mathbb{F}_p$ constructed from H and H' by Proposition 2.1 are equivalent.*

Proof. Since H is equivalent to H', $H' = P \cdot H \cdot Q$, where P and Q are n by n monomial matrices of 0's, 1's and -1's. Thus we have

$$(\ \alpha I_n\ ,\ H'\ ) = (\ \alpha I_n\ ,\ P \cdot H \cdot Q\ ) = P\ (\ \alpha I_n\ ,\ H\ )\ R,$$

where $R = \begin{pmatrix} P^{-1} & O \\ O & Q \end{pmatrix}$ is a $2n$ by $2n$ monomial matrix. Here O denotes the n by n zero matrix. Therefore the two codes are equivalent. □

Thus it is sufficient to consider only codes constructed from inequivalent Hadamard matrices.

It is known that there is a unique Hadamard matrix of order n for $n =$ 4, 8, 12, up to equivalence. Thus Proposition 2.3 and Lemma 3.2 give the following:

Proposition 3.3. *Let H_n be a Hadamard matrix of order n. If the matrix $(\alpha I_n \ , \ H_n)$ generates a self-dual code $C_p(H_n)$ over $\mathbb{F}_p$ where α is an element of $\mathbb{F}_p$. Then the code $C_p(H_n)$ is a self-dual $[2n, n, n/2+2]$ code when $n = 2, 4, 8$ and 12. Moreover all self-dual codes with generator matrices of the form $(\alpha I_n \ , \ H_n)$ are equivalent.*

3.2. **Self-Dual [32, 16] Codes over $\mathbb{F}_5$.** Here we consider self-dual $[32, 16]$ codes over $\mathbb{F}_5$ constructed from Hadamard matrices of order 16. By Proposition 2.1 the matrix $(2I_{16} \ , \ H_{16})$ generates a self-dual code of length 32. Hall [2] proved that there are exactly five equivalence classes I, II, III, IV and V of Hadamard matrices of order 16. We denote the Hadamard matrices in classes I, II, III, IV and V by $H_{16,I}, H_{16,II}, H_{16,III}, H_{16,IV}$ and $H_{16,V}$ respectively.

By Proposition 2.3 $mw(C_5(H_{16})) = 8$. The numbers of codewords of weight 8 are 2240, 1216, 704, 448 and 448 in the codes $C_5(H_{16,I})$, $C_5(H_{16,II})$, $C_5(H_{16,III})$, $C_5(H_{16,IV})$ and $C_5(H_{16,V})$ respectively. On the other hand $H_{16,IV}$ and ${H_{16,V}}^T$ are equivalent. Thus it follows from Lemma 3.1 that the two codes $C_5(H_{16,IV})$ and $C_5(H_{16,V})$ are equivalent. Thus we have the following proposition.

Proposition 3.4. *Let H_{16} be a Hadamard matrix of order* 16. *Then the matrix $(2I_{16} \ , \ H_{16})$ generates a self-dual* $[32, 16, 8]$ *code over $\mathbb{F}_5$. Moreover there exist exactly four inequivalent self-dual codes constructed from all Hadamard matrices of order* 16.

3.3. **Self-Dual [40, 20] Codes over $\mathbb{F}_7$.** Here we consider self-dual $[40, 20]$ codes over $\mathbb{F}_7$ derived from Hadamard matrices of order 20. There are exactly three inequivalent Hadamard matrices of order 20 (cf. [3]). The matrix $(I_{20} \ , \ H_{20})$ generates a self-dual code of length 40 by Proposition 2.1.

By Proposition 2.3 we have

$$8 \leq mw(C_7(H_{20})) \leq 12.$$

Our computer search shows that the minimum weight is 12. Thus, in a sense, any of the codes are optimal. The number of codewords of weight 12 is 18240 in each self-dual code.

In order to distinguish the three codes, we examine an equivalent invariant described in [4]. Let C be a $[2n, n, d]$ code. Let $M = (m_{ij})$ be an A_d by $2n$ matrix whose rows are codewords of weight d in C where A_i denotes the number of codewords of weight i in C. For an integer k $(1 \leq k \leq 2n)$, let $n(j_1, \cdots, j_k)$ be the number of r $(1 \leq r \leq A_d)$ such that $m_{rj_1} \cdots m_{rj_k} \neq 0$

for $1 \leq j_1 < \cdots < j_k \leq 2n$. We consider a set

$$S = \{n(j_1, \ldots, j_k) | \text{ for any distinct } k \text{ columns } j_1, \ldots, j_k \}.$$

Let $M(k)$ and $m(k)$ be maximal and minimal numbers in S respectively. Since two equivalent codes have the same S, these numbers are invariant under the equivalence of codes. We have checked that the numbers $M(3)$ and $m(3)$ are distinct for the three codes over $\mathbb{F}_7$ where the numbers are given in Table 2.

TABLE 2. Self-dual codes over $\mathbb{F}_7$

Codes	$M(3)$ (maximal number)	$m(3)$ (minimal number)
$C_7(H_{20,Q})$	600	240
$C_7(H_{20,P})$	780	300
$C_7(H_{20,N})$	600	300

Table 2 gives the following proposition.

Proposition 3.5. *Let H_{20} be a Hadamard matrix of order 20. Then the matrix (I_{20} , H_{20}) generates a self-dual $[40,20,12]$ code over $\mathbb{F}_7$. Moreover there exist exactly three inequivalent self-dual codes derived from Hadamard matrices of order 20.*

3.4. Self-Dual [32, 16] Codes over $\mathbb{F}_{13}$ and $\mathbb{F}_{17}$.

Let us consider self-dual $[32,16]$ codes over $\mathbb{F}_{13}$ and $\mathbb{F}_{17}$ constructed from Hadamard matrices of order 16.

The numbers of codewords of weight 8 are $6720, 3648, 2112$ and 1344 in the codes $C_{13}(H_{16,I})$, $C_{13}(H_{16,II})$, $C_{13}(H_{16,III})$ and $C_{13}(H_{16,IV})$ respectively. In addition, the numbers of codewords of weight 8 are $8960, 4864, 2816$ and 1792 in the codes $C_{17}(H_{16,I})$, $C_{17}(H_{16,II})$, $C_{17}(H_{16,III})$ and $C_{17}(H_{16,IV})$ respectively. Thus we have the following proposition.

Proposition 3.6. *Let H_{16} be a Hadamard matrix of order 16. There exist exactly four inequivalent self-dual $[32,16,8]$ codes over $\mathbb{F}_{13}$ and $\mathbb{F}_{17}$ constructed from all Hadamard matrices of order 16.*

It was shown in [4] that there are exactly three inequivalent ternary self-dual codes constructed from Hadamard matrices of order 20. Therefore we have classified all self-dual codes over $\mathbb{F}_p$ constructed from Hadamard matrices of order n for any p and $n \leq 12$, and $p \leq 17$ and $n = 16$ and 20.

References

[1] E. Dawson, Self-dual ternary codes and Hadamard matrices, *Ars Combin.* **19**, 303–308 (1985).

[2] M. Hall, Jr., Hadamard matrices of order 16, *J.P.L. Research Summary* 36-10 1 21–26 (1961).

[3] M. Hall, Jr., Hadamard matrices of order 20, *J.P.L. Technical Report* No. 32–761 (1965).

[4] M. Harada, New extremal ternary self-dual codes, *Australas. J. Combin.* **17**, 133–145 (1998).

[5] H. Kimura, Classification of Hadamard matrices of order 28, *Discrete Math.* **133**, 171–180 (1994).

[6] J.S. Leon, V. Pless and N.J.A. Sloane, Self-dual codes over GF(5), *J. Combin. Theory Ser. A* **32**, 178–194 (1982).

[7] V. Pless, N.J.A. Sloane and H.N. Ward, Ternary codes of minimum weight 6 and the classification of self-dual codes of length 20, *IEEE Trans. Inform. Theory* **26**, 305–316 (1980).

[8] V.S. Pless and V.D. Tonchev, Self-dual codes over $GF(7)$, *IEEE Trans. Inform. Theory* **33**, 723-727 (1987).

Masaaki Harada
Department of Mathematical Sciences
Yamagata University
Yamagata 990–8560, Japan

(Received November 24, 1998)