Weighing matrices and self-dual codes

Masaaki Harada
Department of Mathematics
Okayama University
Okayama 700
Japan

ABSTRACT. In this note, we give a method to construct binary self-dual codes using weighing matrices. By this method, we construct extremal self-dual codes obtained from weighing matrices. In particular, the extended Golay code and new extremal singly-even codes of length 40 are constructed from certain weighing matrices. We also get necessary conditions for the existence of some weighing matrices.

1 Introduction

A weighing matrix $W(n,k)$ of order n and weight k is an n by n (0,1,−1)-matrix such that $WW^t = kI$, $k \leq n$, where I is the identity matrix of order n and W^t denotes the transpose of W. A weighing matrix $W(n,n)$ is a Hadamard matrix. We say that two weighing matrices W_1 and W_2 of order n and weight k are equivalent if there exist monomial matrices of 0's, 1's and -1's P and Q with $W_1 = PW_2Q$.

Chan, Rodger and Seberry [1] classified the inequivalent weighing matrices of any order with weight less than 6. Ohmori [7] gave the complete enumeration of weighing matrices of order 12 and weight k ($6 \leq k \leq 10$). Recently, Ohmori [8] has determined inequivalent weighing matrices of order 13. Our terminology from weighing matrices follows [3].

Let $\mathbb{F} = GF(q)$ be the field with q elements where q is a prime power. An $[n,k]$ linear code C over $\mathbb{F}$ is a k-dimensional vector subspace of $\mathbb{F}^n$. In particular, codes over $GF(2)$ and $GF(3)$ is said binary and ternary codes, respectively. The elements of C are called codewords and the weight of the codeword is the number of its non-zero coordinates. A minimum weight is the smallest weight among non-zero codewords. An $[n,k]$ code with a minimum weight d is called an $[n,k,d]$ code. Two binary codes are

equivalent if one can be obtained from the other by a permutation of the coordinates.

The dual code $C^{\perp}$ of C is defined as $C^{\perp} = \{x \in \mathbb{F}^n | \ x \cdot y = 0$ for all $y \in C\}$. If $C \subset C^{\perp}$, C is called a self-orthogonal code. C is called self-dual if $C = C^{\perp}$. C is called doubly-even if the weights of all codewords of C are a multiple of four. A self-dual code is called singly-even if there exists at least one codeword whose weight is $\equiv 2 \pmod 4$.

A binary self-dual code C is called extremal if C has the largest possible minimum weight. For each length, the detail of the largest possible minimum weight is listed in TABLE I in [2]. Conway and Sloane [2] also gave a list of the possible weight enumerators of binary extremal self-dual codes. The existence of some extremal self-dual codes is an open question in [2].

For our consideration, we need some facts from coding theory. Our terminology and notation follow [6], [9].

There are some known methods for construction of self-dual codes. Some of these methods make use of properties of symmetric designs, Hadamard matrices and graphs. Tonchev [10] gave a method to construct self-dual codes based on Hadamard matrices. It is the aim of this note to discribe a method for construction of self-dual codes from weighing matrices. However the present method has no direct relevance to Tonchev's method in [10]. Some extremal self-dual codes derived from weighing matrices are constructed in Section 4. In particular, we reconstruct the extended Golay code and find new extremal singly-even codes of length 40 from some weighing matrices. Moreover we apply self-dual codes as a tool for investigating weighing matrices. In Section 3, we discuss the binary and ternary self-dual codes based on weighing matrices. Such codes imply necessary conditions for the existence of some weighing matrices.

2 Construction of Self-Dual Codes

First we discribe the method to construct self-dual codes in Tonchev [10]. The Hamming distance between each pair of rows of a Hadamard matrix of order n is $n/2$. The following construction of self-dual codes was proved using this fact.

Theorem 2.1 (Tonchev [10]) *Let H is a Hadamard matrix of order $n = 8t + 4$ such that the number of $+1$'s in all rows are congruent modulo 4. Then the matrix $[\ I\ ,\ (H+J)/2\ ]$ generates a binary self-dual code of length $2n$ where J is the all-one matrix of order n.*

Since a weighing matrix $W(n, n)$ is a Hadamard matrix, weighing matrices are a generalization of Hadamard matrices. Thus we investigate a method to construct self-dual codes using weighing matrices.

Let $\mathbb{F}_3$=$\{1,0,-1\}$ be the field with 3 elements and $\mathbb{F}_2$=$\{1,0\}$ the field with 2 elements. Let φ be a map from $M_n(\mathbb{F}_3)$ to $M_n(\mathbb{F}_2)$ where $\varphi(a_{ij}) = |a_{ij}|$ for a matrix $(a_{ij}) \in M_n(\mathbb{F}_3)$. Let $W(n,k)$ be a weighing matrix of order n and weight k. We can regard weighing matrices as matrices over $\mathbb{F}_3$. Hence $\varphi(W(n,k))$ is regarded as a matrix over $\mathbb{F}_2$. We state properties of the matrix $\varphi(W(n,k))$.

Lemma 2.2 *Let* $\mathbf{r}_i$ *and* $\mathbf{r}_j$ *be any distinct two rows of* $W(n,k)$ *and* $\mathbf{c}_i$ *and* $\mathbf{c}_j$ *be any distinct two columns for* $1 \leq i,j \leq n$. *Then it holds that* $|\varphi(\mathbf{r}_i) \cap \varphi(\mathbf{r}_j)| \equiv 0 \pmod 2$ *and* $|\varphi(\mathbf{c}_i) \cap \varphi(\mathbf{c}_j)| \equiv 0 \pmod 2$.

Proof: Suppose that $\mathbf{r}_k = (r_{k1}, \cdots, r_{kn})$ for $1 \leq k \leq n$. Since any two rows $\mathbf{r}_i$ and $\mathbf{r}_j$ are orthogonal to each other over $\mathbb{Z}$, it holds that

$$| \{ k : r_{ik} \cdot r_{jk} = 1 \} | = | \{ k : r_{ik} \cdot r_{jk} = -1 \} |.$$

By the definition of the map φ, we get that the number of k $(1 \leq k \leq n)$ such that $\varphi(r_{ik}) = \varphi(r_{jk}) = 1$ is even. The proof for columns is similar. □

Thus the matrix $\varphi(W(n,k))$ such that k is odd is the self-orthogonal design of type (iv) in term of Tonchev [10]. Hence we can construct binary self-dual codes based on weighing matrices as follows.

Proposition 2.3 *Let* $W(n,k)$ *be a weighing matrix of order* n *and weight* k *such that* k *is odd. Then* $[\ I\ ,\ \varphi(W(n,k))\ ]$ *generates a binary self-dual code of length* $2n$.

Proof: The orthogonality of the code follows from Lemma 2.2. □

Since there are many weighing matrices, we may obtain extremal self-dual codes from weighing matrices. We shall produce such extremal codes in Section 4.

Now we consider a construction of doubly-even self-dual codes using weighing matrices. We quote a well-known theorem in [9].

Lemma 2.4 (Pless [9]) *If the rows of a generator matrix for a binary* $[n,k]$ *code* C *have weights divisible by four and are orthogonal to each other, then* C *is a doubly-even self-orthogonal code.*

The following corollary is an easy consequence of Proposition 2.3 and Lemma 2.4.

Corollary 2.5 *If* $n \equiv 0 \pmod 4$ *and* $k \equiv 3 \pmod 4$, *then* $[\ I\ ,\ \varphi(W(n,k))\ ]$ *generates a binary doubly-even self-dual code of length* $2n$.

Now we discuss the relation between the equivalence of weighing matrices and one of the corresponding codes.

We recall that two weighing matrices W and W' are equivalent if there exist monomial matrices of 0's, 1's and -1's P and Q with $PW'Q = W$.

The following proposition indicates a relationship between an equivalence class of weighing matrices and one of the corresponding codes. Since a weighing matrix has many equivalent matrices, the proposition is useful if we get an equivalence class of self-dual codes from certain weighing matrices.

Proposition 2.6 *All self-dual codes derived from equivalent weighing matrices are equivalent to each other.*

Proof: Let W and W' be equivalent weighing matrices. Thus there exist monomial matrices P and Q with $PW'Q = W$. We can assume that $P = P_1P_2$ where P_1 is the permutation matrix and P_2 is the matrix of the operations which multiply rows by -1 ,and $Q = Q_2Q_1$ where Q_1 is the permutation matrix and Q_2 is the matrix of the operations which multiply rows by -1. By definition of the map φ, it holds that $\varphi(W) = P_1\varphi(W')Q_1$. This implies that the self-dual codes generated by $[\ I\ ,\ \varphi(W)\ ]$ and $[\ I\ ,\ \varphi(W')\ ]$ are equivalent to each other. Thus the assertion of the proposition now follows. □

In order to determine the inequivalent self-dual codes from all weighing matrices, it is sufficient to distinguish the codes from inequivalent weighing matrices in view of Proposition 2.6.

3 Necessary Conditions for the Existence of Weighing Matrices

In this section, we shall get necessary conditions for the existence of weighing matrices. In the previous section, we studied the method to construct self-dual codes based on weighing matrices.

We now note that a doubly-even $[2n, n]$ self-dual code exists if and only if $n \equiv 0 \pmod 4$ (cf. [6],[9]).

Theorem 3.1 *If there exists a weighing matrix of order n and weight k, then either $n \equiv 0 \pmod 4$ or $k \not\equiv 3 \pmod 4$.*

Proof: Let W be a weighing matrix of order n and weighing k such that $n \not\equiv 0 \pmod 4$ and $k \equiv 3 \pmod 4$. The number of 1's in every row of $[\ I\ ,\ \varphi(W)\ ]$ is $k + 1 \equiv 0 \pmod 4$. By Proposition 2.3 and Lemma 2.4, $[\ I\ ,\ \varphi(W)\ ]$ generates a binary doubly-even self-dual code of length $2n$. However if doubly-even $[2n, n]$ self-dual codes exist then n must be a mulutiple of four. Thus this completes a proof. □

Geramita and Seberry [3] gave some conditions for the existence of weighing matrices. The following result was shown in [3]. Here we give an alternative proof using ternary self-dual codes derived from weighing matrices.

Theorem 3.2 *If there exists a weighing matrix of order n and weight k, then either n is even or $k \not\equiv 2 \pmod 3$.*

Proof: Here we consider ternary self-dual codes generated by weighing matrices. It is easy to see that if W is a weighing matrix of order k with $k \equiv 2 \pmod 3$ then $[\, I \,,\, W \,]$ generates a ternary self-dual code. However it is well known that length of ternary self-dual codes is necessarily a multiple of four [6]. This completes a proof. □

4 Extremal Self-Dual Codes from Weighing Matrices

In this section, we shall produce some extremal self-dual codes using weighing matrices.

4.1 Intersection Pattern and Minimum Weight

Sometimes the intersection pattern (see [1] for definition) allows us to obtain considerable information about the structure of weighing matrices. Moreover the intersection pattern gives information about the minimum weight of self-dual codes from weighing matrices. We discuss a relationship between the intersection pattern of weighing matrices and the minimum weight of these codes.

Let W be any weighing matrix of order n and weight k. We say that p_{2i} rows of W intersect a row j in $2i$ places if there are p_{2i} rows, each of which has exactly $2i$ non-zero elements occurring in columns containing non-zero elements in row j. Then we have the following equalities [1] :

$$\sum_{i=0} p_{2i} = n - 1 \tag{1}$$

and

$$\sum_{i=0} i p_{2i} = k(k-1)/2. \tag{2}$$

By a similar argument as Theorem 2.2 in Tonchev [10], we get the following relation between the intersection pattern and the minimum weight of the self-dual code.

Theorem 4.1 *Let W be a weighing matrix of order n and weight k such that $k \equiv 3 \pmod 4$ (resp. $k \equiv 1 \pmod 4$) and $k \geq 7$ (resp. 5). Let C be a doubly-even (resp. singly-even) self-dual code whose the generator matrix*

G is $[\ I\ ,\ \varphi(W)\ ]$. The minimum weight of C is at least 8 (resp. 6) if and only if it holds that the intersection number $p_{k-1} = 0$ for any row of W.

Proof: It is sufficient to prove that the weight of any sum of at most three rows of G is at least 8 (resp. 6). It is obvious that the weight of a row of G is $k+1 \geq 8$ (resp. 6). If it holds that $p_{k-1} = 0$, in any two rows of $\varphi(W)$ the number of places where the two rows which do not intersect is at least 4. Thus the weight of a sum of any two rows of G ia at least 8 (resp. 6). Conversely if it holds that $p_{k-1} \geq 1$, then there exist two rows whose weight is 4. Since the code is self-dual, the parity check matrix

$$H = [\ (\varphi(W))^t\ ,\ I\ ]$$

is also a generator matrix of C. If there is a codeword of weight 4 which is a sum of three rows of G, then the codeword must be a row of H. Since the weight of a row of H is $k+1 \geq 8$ (resp. 6), this completes a proof. □

Theorem 4.1 gives a condition for extremality of self-dual codes obtained from weighing matrices of small orders. By Proposition 2.3 and Theorem 4.1, we shall construct some extremal self-dual codes using weighing matrices of small orders.

4.2 Reconstructing the Extended Golay Code

We shall consider self-dual codes from weighing matrices of order 12. The classifications of weighing matrices of order 12 and all weights were given in Chan, Rodger and Seberry [1] and Ohmori [7]. Ohmori [7] determined weighing matrices of order 12 and weight 7 and 9. There exist exactly three inequivalent weighing matrices of order 12 and weight 7 and exactly four inequivalent matrices of weight 9. First we discribe how to construct the extended Golay code using weighing matrices. According to [7], we denote the three inequivalent weighing matrices of order 12 and weight 7 by A_1, A_3 and A_8. Let C_1, C_3 and C_8 be doubly-even codes which are obtained from A_1, A_3 and A_8 by Corollary 2.5, respectively.

Since it holds that

$$p_6 = \begin{cases} 1, & \text{for } A_1, \\ 0, & \text{for } A_3 \text{ and } A_8, \end{cases} \tag{3}$$

the minimum weight of C_1 is 4 and C_3 and C_8 are extremal doubly-even [24,12,8] codes. Since there exists a unique doubly-even [24,12,8] code up to equivalence, C_3 and C_8 must be equivalent to the extended Golay code.

Thus we have the following proposition.

Proposition 4.2 *Two inequivalent doubly-even codes are derived from all weighing matrices of order* 12 *and weight* 7. *One of them is the extended Golay* $[24, 12, 8]$ *code and the other is the doubly-even* $[24, 12, 4]$ *code.*

It is impossible to construct an extremal doubly-even code from weighing matrices of order 12 except $W(12,7)$'s and $W(12,11)$'s. Next we shall consider doubly-even codes obtained from weighing matrices of order 12 and weight 11. There exists the intersection number p_{10} with $p_{10} > 0$ for any weighing matrix of order 12 and weight 11. By Theorem 4.1, the code which is obtained from any matrix of weight 11 is a doubly-even [24,12,4] code. Therefore weighing matrices of order 12 which generate the extended Golay [24,12,8] code are only two weighing matrices of weight 7 A_3 and A_8.

Now we shall consider extremal singly-even codes using weighing matrices of order 12. The largest possible minimum weight of singly-even codes of length 24 is 6 [2]. It is sufficient to consider singly-even self-dual codes from weighing matrices of weight 5 and 9.

Since it holds that $p_8 = 3$ for any weighing matrix of order 12 and weight 9 [7] and $p_4 \geq 1$ for any weighing matrices of weight 5 [1]. Thus all singly-even codes which is obtained from all weighing matrices of order 12 are singly-even [24,12,4] codes.

We now consider extremal codes from weighing matrices of order 13 and weight 9.

Recently Ohmori [8] has completed the classification of such weighing matrices. There are exactly eight inequivalent matrices. Let $W_i^*(1 \leq i \leq 8)$ be the inequivalent matrices as shown in Fig.5 [8].

Proposition 4.3 *Every self-dual code from weighing matrices of order* 13 *and weight* 9 *is an extremal singly-even* $[26, 13, 6]$ *code. Moreover all self-dual codes derived from all weighing matrices of order* 13 *and weight* 9 *are equivalent to each other.*

Proof: Let $C_{13,i}$ be the self-dual code generated by $[\, I \,,\, \varphi(W_i^*)\,]$. It holds that the intersection pattern $p_8 = 0$ for each W_i^* [8].

By Theorem 4.1, $C_{13,i}$ is an extremal singly-even [26,13,6] code for each i $(1 \leq i \leq 8)$. Moreover there is a unique extremal singly-even [26,13,6] code, up to equivalence [2]. Thus each $C_{13,i}$ must be equivalent to f_{13}^2 in [2]. This completes a proof. □

Remark It is obvious that $\varphi(W_i^*)$ is an incidence matrix of a symmetric 2-(13,9,6) design for any i $(1 \leq i \leq 8)$.

4.3 New Extremal Singly-Even Codes of Length 40

Here we investigate new extremal singly-even codes derived from weighing matrices of order 20. Examples of seven weighing matrices of weight 9

are given in [1]. We denote the circulant $W(20,9)$ by W_0 and No.i four-circulants $W(20,9)$'s by W_i $(i = 1, \cdots, 6)$ after [1]. Let C_i be the singly-even code whose the generator matrix is $[\ I\ ,\ \varphi(W_i)\ ]$ for $0 \leq n \leq 6$.

Extremal singly-even [40,20,8] codes have the following weight enumerator [2] :

$$W = 1 + (125 + 16\beta)y^8 + (1664 - 64\beta)y^{10} + (10720 + 32\beta)y^{12} + (44160 + 192\beta)y^{14} + \cdots, \tag{4}$$

where β is an undetermined parameter. In [2], extremal singly-even [40,20,8] codes were constructed corresponding to $\beta = 0$ and 10.

By a computer calculation, C_0, C_2 and C_3 are extremal singly-even [40,20,8] codes and these codes have the weight distributions with $\beta = 10$. Moreover we discuss the equivalence of these extremal codes. We definded K-matrices in [5] in order to check the equivalence of extremal self-dual codes. The author and Kimura [5] mentioned the following relation between the inequivalence of extremal codes and their K-matrices.

Proposition 4.4 (Harada and Kimura [5]) *Let C and C' be extremal singly-even codes of length n. Let K and K' be K-matrices for C and C', respectively. If C is equivalent to C', then it holds that $K = K'$.*

We compare K-matrices for our three codes with the known code in [2]. Such extremal codes have all distinct K-matrices of degree 10. By Proposition 4.4, we get the following proposition.

Proposition 4.5 *Extremal singly-even $[40, 20, 8]$ codes corresponding to $\beta = 10$ can be constructed from certain weighing matrices of order 20 and weight 9. Moreover these extremal codes and the known extremal singly-even $[40, 20, 8]$ code are inequivalent to each other.*

Remark Since the weight enumerator of any self-dual code must have non-negative integral coefficients, it holds that $0 \leq \beta \leq 26$ for any extremal singly-even code of length 40. Recently the author [4] has constructed extremal singly-even [40,20,8] codes corresponding to $\beta = 1$ and 2. But it is not known whether extremal singly-even [40,20,8] codes with $\beta \neq 0, 1, 2, 10$ exist or not.

Acknowledgment. The author would like to thank his adviser Professor Hitoshi Kaneta for helpful discussions.

References

[1] H.C. Chan, C.A. Rodger and J. Seberry, On inequivalent weighing matrices, *Ars Combin.* **21** (1986), 299–333.

[2] J.H. Conway and N.J.A. Sloane, A new upper bound on the minimal distance of self-dual codes, *IEEE. Trans. Inform. Theory* **36** (1990), 1319–1333.

[3] A.V. Geramita and J. Seberry, *Orthogonal Designs: Quadratic Forms and Hadamaed Matrices*, Marcel Dekker, New York, 1979.

[4] M. Harada, Existence of new extremal doubly-even codes and extremal singly-even codes, Designs, Codes and Cryptography, to appear.

[5] M. Harada and H. Kimura, New extremal doubly-even [64,32,12] codes, *Designs, Codes and Cryptography*, to appear.

[6] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.

[7] H. Ohmori, On the classifications of weighing matrices of order 12, *J. Combin. Math. Combin. Comput.* **5** (1989), 161–216.

[8] H. Ohmori, Classification of weighing matrices of order 13 and weight 9, *Discrete Math.* **116** (1993), 55–78.

[9] V. Pless, *An Introduction to the Theory of Error Correcting Codes*, Wiley-Interscience, New York, 1982.

[10] V.D.Tonchev, Self-orthogonal designs and extremal doubly-even codes, *J. Combin. Theory Ser. A* **52** (1989), 197–205.