Weighing matrices and spherical codes

Hiroshi Nozaki, Sho Suda
Department of Mathematics Education, Aichi University of Education
1 Hirosawa, Igaya-cho, Kariya, Aichi 448-8542, Japan
hnozaki@auecc.aichi-edu.ac.jp, suda@auecc.aichi-edu.ac.jp

January 13, 2015

Abstract

Mutually unbiased weighing matrices (MUWM) are closely related to an antipodal spherical code with 4 angles. In this paper, we clarify the relation between MUWM and the spherical codes, and determine the maximum size of a set of MUWM with weight 4 for any order. Moreover, we define mutually quasi-unbiased weighing matrices (MQUWM) as a natural generalization of MUWM from the viewpoint of spherical codes. We determine the maximum size of a set of MQUWM for the parameters $(d, 2, 4, 1)$ and $(d, d, d/2, 2d)$. This includes an affirmative answer to the problem of Best, Kharaghani, and Ramp.

1 Introduction

A weighing matrix W with weight k is a square $(\pm 1, 0)$-matrix W of order d such that $WW^T = kI$, where I is the identity matrix of order d and W^T denotes the transpose of W. If $k = d$ holds, the weighing matrix is a Hadamard matrix. Weighing matrices have been classified for small orders and weights [6, 16, 17, 11]. Note that the classification of self-orthogonal codes is used to classify weighing matrices in [11]. As a generalization of real mutually unbiased bases [4], Holzmann, Kharaghani and Orrick defined mutually unbiased weighing matrices (MUWM) in [13]. Recently, Best, Kharaghani, and Ramp studied MUWM further in [2]. In particular they obtained the maximum numbers of MUWM with order n and weight w for $(n, w) = (7, 4), (8, 4)$. Actually the two maximum examples correspond to the roots in the E_7, E_8 lattices, but the authors did not mention this.

The set of row vectors in a weighing matrix can be identified with a finite set on a sphere where two distinct vectors are orthogonal. From the viewpoint of this relationship, MUWM can be identified with an antipodal spherical code (or equivalently lines through the origin in $\mathbb{R}^d$) with only 4 angles, which is a union of disjoint cross-polytopes. Classification of root systems allows us to determine the maximum size of a set of mutually unbiased weighing matrices with weight 4.

We put forward a new concept, a set of mutually quasi-unbiased weighing matrices (MQUWM), which is a natural generalization of MUWM from the perspective of antipodal spherical codes with 4 angles. As well as being a natural generalization, a set of MQUWM leads to a set of MUWM. We prove that the existence of some spherical codes is equivalent to that of MQUWM, and we give constructions of such spherical codes from linear $\mathbb{Z}_2, \mathbb{Z}_4$-codes or root lattices. As a consequence, we obtain the maximum size of a set of MQUWM or MUWM for several parameters. The results include an affirmative answer to Conjecture 23 in [2], which says that for $d = 2^{2t+1}$, there are Hadamard matrices $H_1, \ldots, H_d$ of order d so that the entries of $H_i H_j^T$ $(i \neq j)$ have absolute values 0 or 2^{t+1}.

The rest of this paper is organized as follows. In Section 2, we define MQUWM, and show the relation between MQUWM and spherical codes. In Section 3, we give the maximum size of a set of MQUWM for the parameters $(d, 2, 4, 1)$. We give the maximum size of a set of MUWM with weight 4 by the cross-polytope decomposition of the set of roots in root lattices. In Section 4, we determine the maximum size of a set of MQUWM for the parameters $(d, d, d/2, 2d)$.

2 Mutually quasi-unbiased weighing matrices

In this section we introduce the concept of mutually quasi-unbiased weighing matrices (MQUWM) and their connection to mutually unbiased weighing matrices (MUWM). We also show that the existence of MQUWM is equivalent to that of some spherical code.

Two weighing matrices W_1, W_2 with order d and weight k are said to be *quasi-unbiased for the parameters* (d, k, l, a) if there exist a positive integer l and a positive real number a such that $(1/\sqrt{a})W_1 W_2^T$ is a weighing matrix with weight l. In this case, $l = k^2/a$ holds. Weighing matrices $W_1, \ldots, W_f$ are said to be *mutually quasi-unbiased weighing matrices (MQUWM) for the parameters* (d, k, l, a) if any distinct two are quasi-unbiased for the parameters (d, k, l, a).

The concept of quasi-unbiasedness is defined for unit weighing matrices as well [1]. In the real case, a is the square of an integer.

A set of MQUWM for the parameters (d, d, d, d) coincides with a set of mutually unbiased bases (MUB) in $\mathbb{R}^d$. A set of MQUWM is called a set of mutually unbiased weighing matrices (MUWM) for the parameters (d, k, k, k) coincides with a set of MUWM with order d and weight k [13]. Thus, the concept of MQUWM is a generalization of both MUB and MUWM.

If $\{W_1, \ldots, W_f\}$ is a set of mutually unbiased weighing matrices with order d and weight k, then the matrices $I, (1/\sqrt{k})W_1, \ldots, (1/\sqrt{k})W_f$ satisfy the property that any two row vectors belonging to different matrices have an inner product in $\{0, \pm 1/\sqrt{k}\}$. Multiplying the set $\{I, (1/\sqrt{k})W_1, \ldots, (1/\sqrt{k})W_f\}$ by the orthogonal matrix $(1/\sqrt{k})W_1^T$ from the right, the matrices $(1/\sqrt{k})W_1^T, I$, $(1/\sqrt{k})W_2 W_1^T, \ldots, (1/\sqrt{k})W_f W_1^T$ satisfy the same property. Thus $\{(1/\sqrt{k})W_1^T$, $(1/k)W_2 W_1^T, \ldots, (1/k)W_f W_1^T\}$ is a set of mutually unbiased weighing matrices with weight k.

Similarly, suppose $\{W_1, \dots, W_f\}$ is a set of mutually quasi-unbiased weighing matrices for the parameters (d, k, l, a). Then $\{(1/\sqrt{a})W_2W_1^T, \dots, (1/\sqrt{a})W_fW_1^T\}$ is a set of mutually unbiased weighing matrices with weight l. Not all MUWM can be obtained from MQUWM in this way. The following is an example.

Example 2.1. There exists a set of 8 MUWM with weight 4 and order 7 [2]. If we assume they come from MQUWM for the parameters $(7, k, 4, a)$, then $k \leq 7$ holds. Thus we have $4a = k^2 \leq 49$, and $a = 1, 4, 9$. For $(k, a) = (2, 1)$, there does not exist a set of 9 MQUWM with weight 2 by Proposition 3.3 below. The case $(k, a) = (4, 4)$ corresponds to the MUWM case. For $(k, a) = (6, 9)$, there does not exist a weighing matrix of weight 6 and order 7, because if the order is odd, then the weight must be a square [6]. Therefore we do not have the corresponding MQUWM.

Let rS^{d-1} denote the sphere in $\mathbb{R}^d$ whose radius is r. For a finite subset X of rS^{d-1}, let $A(X)$ be the set of usual inner products of two distinct vectors in X. We say $\{X_0, X_1, \dots, X_f\}$ is a *cross-polytope decomposition* of X if $\{X_0, X_1, \dots, X_f\}$ is a partition of X and elements of X_i consist of vectors of a scalar multiple of a cross-polytope for each $i \in \{0, 1, \dots, f\}$. Let $\Omega_d = \{0, \pm 1\}^d$ and $\Omega_{d,k} = \{x \in \Omega_d \mid \sum_i x_i^2 = k\}$. For a matrix A, denote the set of row vectors of A as $S(A)$.

The following proposition characterizes the existence of MQUWM in terms of certain spherical codes.

Proposition 2.2. *Let f, d, k and a be positive integers such that $f \geq 2$. The existence of the following are equivalent.*

(1) *A set $\{W_1, \dots, W_f\}$ of mutually quasi-unbiased weighing matrices for the parameters $(d, k, k^2/a, a)$.*

(2) *A subset $X \subset \Omega_{d,k}$ with the property that $A(X) = \{\pm\sqrt{a}, 0, -k\}$ and there exists a cross-polytope decomposition $\{X_1, \dots, X_f\}$ of X.*

Proof. (1)⇒(2): Let $X_i = S(W_i) \cup S(-W_i)$ for $i = 1, \dots, f$. Then $X = \bigcup_{i=1}^f X_i$ with $\{X_1, \dots, X_f\}$ satisfies (2).

(2)⇒(1): For each $i \in \{1, \dots, f\}$, any vector in X_i has k entries of ± 1, and the remaining entries are 0 because X is in $\Omega_{d,k}$.

For each $i \in \{1, \dots, f\}$, we define the matrix $W_i = [v_1, \dots, v_d]$ by the vectors $X_i = \{\pm v_1, \dots, \pm v_d\}$. Since $A(X) = \{\pm\sqrt{a}, 0, -k\}$, the entries of $W_iW_j^T$ are $0, \pm\sqrt{a}$ for distinct i, j. Thus $W_1, \dots, W_f$ form a set of MQUWM for the desired parameters. □

For MUWM, we obtain the following characterization.

Proposition 2.3. *Let f, d and k be positive integers such that $f \geq 2$. The existence of the following are equivalent.*

(1) *A set $\{W_1, \dots, W_f\}$ of mutually unbiased weighing matrices with weight k.*

(2) *A subset* $X \subset \sqrt{k}S^{d-1}$ *with the property that* $A(X) = \{\pm\sqrt{k}, 0, -k\}$ *and there exists a cross-polytope decomposition* $\{X_0, X_1, \ldots, X_f\}$ *of* X.

Proof. (1)⇒(2): Let $X_i = S(W_i) \cup S(-W_i)$ for $i = 1, \ldots, f$ and $X_0 = S(\sqrt{k}I) \cup S(-\sqrt{k}I)$. Then $X = \bigcup_{i=0}^{f} X_i$ with $\{X_0, \ldots, X_f\}$ satisfies (2).

(2)⇒(1): After transforming X_0 to $\{\pm\sqrt{k}e_1, \ldots, \pm\sqrt{k}e_d\}$, any vector in X_i ($i \in \{1, \ldots, f\}$) has k entries of ± 1. The rest of the argument is the same as that in Proposition 2.2. □

3 MQUWM for the parameters $(d, 2, 4, 1)$ and MUWM with weight 4

In this section, we show an upper bound for the size of a set of MQUWM for the parameters $(d, 2, 4, 1)$ with examples attaining the bound. We also introduce the relationship between MUWM with weight 4 and disjoint 2-frames in a root lattice, and determine the maximum size of a set of MUWM with weight 4 for any order.

We first introduce some basic definitions used in this section, as well as results about disjoint 2-frames in root lattices.

An integral lattice is called a *root lattice* if it is generated by roots, which are vectors whose norm is $\sqrt{2}$. It is well known that the irreducible root lattices are A_d ($d \geq 2$), D_d ($d \geq 4$), E_6, E_7, and E_8 (see for example [9]). The subset $F = \{\pm v_1, \ldots, \pm v_d\}$ in a lattice of rank d is called a *k-frame* if $(v_i, v_j) = k\delta_{ij}$, where δ_{ij} is the Kronecker delta.

We prepare several results about disjoint 2-frames in a root lattice. Let $\perp_i L_i$ denote the orthogonal direct sum of lattices L_i. Let $m(L)$ be the maximum number of disjoint 2-frames in a lattice L.

Lemma 3.1. *Let* $L = \perp_i L_i$*, where* L_i *is an irreducible root lattice. We then have* $m(L) = \min_i\{m(L_i)\}$.

Proof. Follows from the fact that if v is a root in L, then v is a root in L_i for some i. □

We use the notation

$$(a_1, \ldots, a_d)_d^P = \{(a_{\sigma(1)}, \ldots, a_{\sigma(d)}) \mid \sigma \in S_d\},$$

for $(a_1, \ldots, a_d) \in \mathbb{R}^d$, where S_d is the symmetric group of degree d.

Lemma 3.2. *We have the following.*

(1) *For any* $d \geq 2$, $m(A_d) = 0$.

(2) *For even* $d \geq 4$, $m(D_d) = d - 1$.

(3) *For odd* $d \geq 5$, $m(D_d) = 0$.

(4) $m(E_6) = 0$.

(5) $m(E_7) = 9$.

(6) $m(E_8) = 15$.

Proof. (1) The set of roots in the A_d lattice can be expressed by $(1, -1, 0, \ldots, 0)^P_{d+1}$ which has the size $d(d+1)$. Clearly the largest number of mutually orthogonal vectors is $\lfloor (d+1)/2 \rfloor$. Therefore (1) follows.

(2) The set of roots in the D_d lattice can be expressed by $(\pm 1, \pm 1, 0, \ldots, 0)^P_d$. Disjoint 2-frames in the D_d lattice are related to disjoint perfect matchings of the complete graph K_d. Recall that a matching is a set of pairwise non-adjacent edges, and is said to be perfect if every vertex is an endpoint of some edge in the matching. From a perfect matching M of K_d, we obtain a 2-frame as follows

$$F_M = \{(v_1, \ldots, v_d) \in D_d \mid \sum_k v_k^2 = 2, v_i = \pm 1, v_j = \pm 1, \{i, j\} \in M\}.$$

Since d is even, the complete graph K_d is 1-factorable, that is, the edge set $E(K_d)$ can be decomposed into $d-1$ disjoint perfect matchings [12, Theorem 9.1]. This implies that the set of roots in the D_d lattice is decomposed into $d-1$ disjoint 2-frames. Therefore (2) follows.

(3) For odd d, the largest number of mutually orthogonal roots in the D_d lattice is clearly $d-1$. Therefore (3) follows.

(4) Assume that there exists a 2-frame in E_6. Let L be a sublattice generated by the 2-frame. Then $|E_6/L| = \det(L)/\det(E_6) = 8/3$, a contradiction.

(5) There exists a set of 8 MUWM with weight 4 and order 7 [2]. Adding $(\pm 2, 0, \ldots, 0)^P_d$ to the set of row vectors in the 8 MUWM, we obtain 126 roots that must form the set of roots of E_7. This implies (5).

(6) There exists a set of 14 MUWM with weight 4 and order 8 [2]. Adding $(\pm 2, 0, \ldots, 0)^P_d$ to the set of row vectors in the 14 MUWM, we obtain 240 roots that must form the set of roots of E_8. This implies (6). □

Proposition 3.3. *Let $W = \{W_1, \ldots, W_f\}$ be a set of mutually quasi-unbiased weighing matrices for the parameters $(d, 2, 4, 1)$. Then we have*

$$f \leq d - 1.$$

Proof. Every row vector of W_i is in $(\pm 1, \pm 1, 0, \ldots, 0)^P_d$ whose size is $2d(d-1)$. This clearly shows the theorem. □

There does not exist a weighing matrix with weight 2 for odd order [1, 6]. For even order, we have a set of MQUWM meeting the upper bound in Proposition 3.3.

Theorem 3.4. *Suppose d is even. Then there exists a set of $d-1$ mutually quasi-unbiased weighing matrices for the parameters $(d, 2, 4, 1)$.*

Proof. By Lemma 3.2 (2), the roots $(\pm 1, \pm 1, 0, \ldots, 0)_d^P$ of the D_d lattice are decomposed into $d-1$ disjoint 2-frames. By Proposition 2.2, we obtain a set of MQUWM for the parameters $(d, 2, 4, 1)$. □

By Proposition 2.3, the existence of MUWM with order d and weight 4 is equivalent to that of a subset X of $2S^{d-1}$ having a cross-polytope decomposition such that $A(X) = \{2, 0, -2, -4\}$. The set $(1/\sqrt{2})X$ can be identified with a subset of roots in a root lattice, and the cross-polytopes correspond to disjoint 2-frames. If we determine the root lattice which has the maximum number of disjoint 2-frames among all root lattices of a fixed rank d, then we can obtain the maximum size of a set of MUWM with order d and weight 4.

Theorem 3.5. *Let $m(d)$ denote the maximum size of a set of MUWM with order d and weight 4. Then the value $m(d)$ is given in the following table, which also indicates the root lattices of rank d having the maximum number $m(d)$ of disjoint 2-frames.*

d	5	8	9	11	13	even $d \geq 4$ $(d \neq 8)$
$m(d)$	0	14	0	2	4	$d-2$
lattice	–	E_8	–	$D_4 \perp E_7$	$D_6 \perp E_7$	D_d $(d = 16, E_8 \perp E_8)$

d	odd $d \geq 15$, $d = 7$
$m(d)$	8
lattice	$(\perp_{a \text{ copies}} E_7) \perp (\perp_{b \text{ copies}} E_8) \perp (\perp_i (\perp_{t_i \text{ copies}} D_{d_i}))$ even $d_i \geq 10, d = 7a + 8b + \sum_i t_i d_i \quad (a \neq 0)$

For odd $d \geq 17$, we have the lattice $E_7 \perp D_{d-7}$ giving $m(d) = 8$ in the above table.

Proof. For each rank d, we consider possible irreducible components of a root lattice. By Lemmas 3.1 and 3.2, we obtain the maximum number of disjoint 2-frames. □

4 MQUWM for the parameters $(d, d, d/2, 2d)$

In this section, we give an upper bound and maximal examples of MQUWM for the parameters $(d, d, d/2, 2d)$.

To construct mutually quasi-unbiased weighing matrices, we prepare two codes, one over $\mathbb{Z}_2$ and the other over $\mathbb{Z}_4$. Let $\mathcal{B}(2, m)$ be a cyclic code of length $2^m - 1$ with defining set $C_1 \cup C_2 \cup C_3 \cup C_4$, where C_i is the 2-cyclotomic coset of i modulo $2^m - 1$ for $i = 1, 2, 3, 4$. The code $\mathcal{B}(2, m)$ is called the *narrow-sense BCH code* with designed distance 5. Then the dual code $\mathcal{B}(2, m)^\perp$ has the weights $\{0, 2^{m-1} - 2^{(m-1)/2}, 2^{m-1}, 2^{m-1} + 2^{(m-1)/2}\}$ [14, Table 11.2]. Let C be the code generated by the extended code of $\mathcal{B}(2, m)^\perp$ and the all-ones vector. Then C contains the first order Reed-Muller code $RM(1, m)$ of length 2^m as a subcode (see [14] for the Reed-Muller codes), and the set of its weights is $\{0, 2^{m-1} - 2^{(m-1)/2}, 2^{m-1}, 2^{m-1} + 2^{(m-1)/2}, 2^m\}$.

Define $\phi : \mathbb{Z}_4 \to \mathbb{Z}_2^2$ by $\phi(0) = (0,0), \phi(1) = (0,1), \phi(2) = (1,1), \phi(3) = (1,0)$. This map is extended component-wise to a map, also denoted by ϕ, from $\mathbb{Z}_4^d$ to $\mathbb{Z}_2^{2d}$. The map ϕ is called the Gray map. Let $ZRM(1,m)$ be the first order $\mathbb{Z}_4$-Reed-Muller code (see [14]). It is known that $\phi(ZRM(1,m)) = RM(1,m+1)$ [10, Theorem 7].

Let $h(x)$ be a primitive basic irreducible polynomial of degree m over $\mathbb{Z}_4$, and ξ a root of $h(x)$ so that $\xi^{2^m-1} = 1$. The Galois ring $R = GR(4^m)$ is defined to be $\mathbb{Z}_4[\xi]$. Set $\mathcal{T} = \{0, 1, \xi, \ldots, \xi^{2m-2}\}$. Then, any element $c \in GR(4^m)$ has a unique 2-adic representation $c = a + 2b$ for some $a, b \in \mathcal{T}$. The Frobenius map f from $GR(4^m)$ to itself is the ring automorphism that takes any element $c = a + 2b$ to $c^f = a^2 + 2b^2$. This automorphism f generates the Galois group of $GR(4^m)$ over $\mathbb{Z}_4$ of order m. The relative trace from $GR(4^m)$ to $\mathbb{Z}_4$ is defined by

$$T(c) = c + c^f + \cdots + c^{f^{m-1}} \quad (c \in GR(4^m)).$$

The $\mathbb{Z}_4$-linear Kerdock code $\mathcal{K}$ is

$$\mathcal{K} = \{(T(\lambda x) + \epsilon)_{x \in \mathcal{T}} \mid \lambda \in GR(4^m), \epsilon \in \mathbb{Z}_4\}.$$

The code $\mathcal{K}$ contains the first order $\mathbb{Z}_4$-Reed-Muller code $ZRM(1,m)$ as a subcode [10, Section IV].

The ring R has the unique maximal ideal $2R$, and $R/2R$ is a finite field with 2^m elements, identified with $GF(2^m)$, and tr denotes the usual trace map from $GF(2^m)$ to $\mathbb{Z}_2$. Let $h^\perp = \{x \in \mathcal{T} \mid \mathrm{tr}(\bar{x}h) = 0\}$ for an element $h \in \mathcal{T}$. Let $\mathcal{K}_h$ be the code obtained by projecting $\mathcal{K}$ onto the set of coordinates $h^\perp$.

The code $ZRM(1,m)$ is spanned by $2RM(1,m)$ and $\mathbf{1}$ over $\mathbb{Z}_4$, where $\mathbf{1}$ is the all-ones vector. The code $RM(1,m)$ is defined recursively, by $RM(1,1) = \mathbb{Z}_2^2$ and

$$RM(1,m) = \{(u, u + k\mathbf{1}) \mid u \in RM(1,m-1), k \in \mathbb{Z}_2\}.$$

The automorphism group of the Reed-Muller code is the general affine group, in particular contains the symmetric group of the coordinates [15, Chap. 13, Theorem 24]. Thus, the restriction of the first order $\mathbb{Z}_4$-Reed-Muller code $ZRM(1,m)$ onto any half part of the coordinates is the first order $\mathbb{Z}_4$-Reed-Muller code $ZRM(1,m-1)$. Therefore, the restriction of the first order $\mathbb{Z}_4$-Reed-Muller code $ZRM(1,m)$ as a subcode of $\mathcal{K}$ is the first order $\mathbb{Z}_4$-Reed-Muller code $ZRM(1,m-1)$. Moreover, by [5, Theorem 4.1], for m odd, the weight distribution of the Gray image $\phi(\mathcal{K}_h)$ coincides with that of the extended code of the dual code $\mathcal{B}(2,m)^\perp$.

Define $\psi : \mathbb{Z}_2^d \to \{1,-1\}^d$ as a map such that $\psi((x_i)_{i=1}^d) = ((-1)^{x_i})_{i=1}^d$. We use the Delsarte theory to prove an upper bound on the size of a set of MQUWM for the parameters $(d, d, d/2, 2d)$. See [7] for more information.

Theorem 4.1. *Let $W = \{W_1, \ldots, W_f\}$ be a set of mutually quasi-unbiased weighing matrices for the parameters $(d, d, d/2, 2d)$. Then we have*

$$f \leq d.$$

Proof. Let $\mathcal{C}$ be the set of the preimages of ψ for all the elements of $S(W_i) \cup S(-W_i)$ $(1 \leq i \leq f)$. Letting $\alpha(z) = 2fd(1-\frac{2z}{d})(1-\frac{z}{d})(1-\frac{2z}{d+\sqrt{2d}})(1-\frac{2z}{d-\sqrt{2d}})$ be the annihilator polynomial of $\mathcal{C}$, and $K_k(z)$ the Krawtchouk polynomial of degree k, we have the following expansion:

$$\alpha(z) = f(\frac{1}{d}K_0(z) + \frac{1}{d}K_1(z) + \frac{8}{d^2}K_2(z) + \frac{6}{d(d-2)}K_3(z) + \frac{6}{d^2(d-2)}K_4(z)).$$

Thus the linear programming bound [7, Theorem 5.23] shows that $f \leq d$. □

We use linear codes over $\mathbb{Z}_2$ or $\mathbb{Z}_4$ to obtain MQUWM. First we use linear codes over $\mathbb{Z}_2$ which contain the first order Reed-Muller code $RM(1,m)$ to obtain MQUWM.

Lemma 4.2. *Let C be a binary linear code of length $d = 2^m$ for a positive integer m. Assume that the set with weights of C is $\{0, d/2 \pm a, d/2, d\}$ where a is a positive integer with $a < d$, and C contains the first order Reed-Muller code $RM(1,m)$ as a subcode. Let $\{u_1, \ldots, u_f\}$ be a complete set of representatives for $C/RM(1,m)$. Then $\{\psi(u_i + RM(1,m)) \mid i = 1, \ldots, f\}$ provides a cross-polytope decomposition of $\psi(C)$ with the inner product set $\{\pm 2a, 0, -d\}$.*

Proof. Note that, for each pair of codewords $x, y \in \mathbb{Z}_2^d$, the Hamming distance of x and y is j if and only if $\langle \psi(x), \psi(y) \rangle$ is $d - 2j$. By the assumption on the weights of C, $A(\psi(C)) = \{\pm 2a, 0, -d\}$.

Put $D = RM(1,m)$. Since $\{u_1, \ldots, u_f\}$ is a complete set of representatives for C/D, $\{\psi(u_i + D) \mid i = 1, \ldots, f\}$ gives a partition of $\psi(C)$. Since the Reed-Muller code has the weights $\{0, d/2, d\}$, each $\frac{1}{\sqrt{d}}\psi(u_i + D)$ for $1 \leq i \leq f$ forms a cross-polytope, and the inner products between vectors in different $\psi(u_i + D)$'s are in $0, \pm 2a$. Therefore $\{\psi(u_i + D) \mid i = 1, \ldots, f\}$ provides a cross-polytope decomposition of $\psi(C)$ with the inner product set $\{\pm 2a, 0, -d\}$. □

Next we use linear codes over $\mathbb{Z}_4$ which contain the first order $\mathbb{Z}_4$-Reed-Muller code $ZRM(1,m)$ to obtain MQUWM.

Lemma 4.3. *Let C be a $\mathbb{Z}_4$-linear code of length $d = 2^m$ for a positive integer m. Assume that the set of weights of $\phi(C)$ is $\{0, d \pm a, d, 2d\}$ where a is a positive integer with $a < 2d$, and C contains the first order $\mathbb{Z}_4$-Reed-Muller code $ZRM(1,m)$ as a subcode. Let $\{u_1, \ldots, u_f\}$ be a complete set of representatives for $C/ZRM(1,m)$. Then $\{\psi(\phi(u_i + ZRM(1,m))) \mid i = 1, \ldots, f\}$ provides a cross-polytope decomposition of $\psi(\phi(C))$ with the inner product set $\{\pm 2a, 0, -2d\}$.*

Proof. Put $D = ZRM(1,m)$. Since $\{u_1, \ldots, u_f\}$ is a complete set of representatives for C/D, $\{\phi(u_i + D) \mid i = 1, \ldots, f\}$ gives a partition of $\phi(C)$. Thus $\{\psi(\phi(u_i + D)) \mid i = 1, \ldots, f\}$ gives a partition of $\psi(\phi(C))$.

It is easily shown that $\phi(u_i + D)$ has the same distance distribution as $RM(1, m+1)$. Therefore each $\frac{1}{\sqrt{2d}}\psi(\phi(u_i + D))$ for $1 \leq i \leq f$ forms a cross-polytope. The rest of the proof is same as Lemma 4.2. □

We construct examples attaining the bound in Theorem 4.1 for $d = 2^{2t+1}$ where t is a positive integer. This gives an affirmative answer to Conjecture 23 in [2].

Theorem 4.4. *For any positive integer t, there exists a set of mutually quasi-unbiased weighing matrices for the parameters $(d, d, d/2, 2d)$ attaining the bound in Theorem 4.1, where $d = 2^{2t+1}$.*

Proof. We provide two constructions of such MQUWM.

(1) Apply Lemma 4.2 and Proposition 2.2 to the code generated by the extended code of the $\mathcal{B}(2, 2t+1)^{\perp}$ and the all-ones vector.

(2) Apply Lemma 4.3 and Proposition 2.2 to the code $\phi(\mathcal{K}_h)$. □

Remark 4.5. In the proof of Theorem 4.4, two maximal MQUWM are given. The set of preimages of row vectors MQUWM by ψ is a binary code. The binary code corresponding to (1) in the proof of Theorem 4.4 is linear, but the other is non-linear.

Acknowledgments. We would like to thank the two anonymous refrees for their valuable comments for the first version of this paper. The first author was supported by JSPS KAKENHI Grant Number 25800011.

References

[1] D. Best, H. Kharaghani, and H. Ramp, On unit weighing matrices with small weight, *Discrete Math.* 313 (2013), no. 7, 855–864.

[2] D. Best, H. Kharaghani, and H. Ramp, Mutually unbiased weighing matrices, to appear in *Des. Codes Cryptogr.*

[3] A. Bonnecaze, and I. M. Duursma, Translates of linear codes over $\mathbb{Z}_4$, *IEEE Trans. Inform. Theory* 43 (1997), no. 4, 1218–1230.

[4] P. O. Boykin, M. Sitharam, M. Tarifi and P. Wocjan, Real mutually unbiased bases, preprint, arXiv:quant-ph/0502024v2.

[5] A. R. Calderbank and G. McGuire, $\mathbb{Z}_4$-linear codes obtained as projections of Kerdock and Delsarte-Goethals codes, *Linear Algebra and its Appl.*, 226/228 (1995) 647–665.

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

[7] P. Delsarte, An algebraic approach to the association schemes of coding theory, Philips Res. Rep. 10 (Suppl.) (1973).

[8] P. Delsarte, J. M. Goethals, and J. J. Seidel, Spherical codes and designs, *Geom. Dedicata* 6 (1977), 363–388.

[9] W. Ebeling, Lattices and Codes. A course partially based on lectures by Friedrich Hirzebruch. Third edition. Advanced Lectures in Mathematics. Springer Spektrum, Wiesbaden, 2013. xvi+167 pp.

[10] A. R. Hammons, P.V. Kumar, A. R. Calderbank, N. J. A. Sloane and P. Sole, The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes, *IEEE Trans. Inform. Theory* 40 (1994), no. 2, 301–319.

[11] M. Harada and A. Munemasa, On the classification of weighing matrices and self-orthogonal codes, *J. Combin. Des.* 20 (2012), no. 1, 45–57.

[12] F. Harary, Graph Theory, Addison-Wesley Publishing Co., Reading, Mass.-Menlo Park, Calif.-London 1969 ix+274 pp.

[13] W. H. Holzmann, H. Kharaghani and W. Orrick, On the real unbiased Hadamard matrices, Combinatorics and Graphs, 243–250, Contemp. Math. 531, Amer. Math. Soc., Providence, RI, 2010.

[14] W. C. Huffman and V. Pless, Fundamentals of Error-Correcting Codes, Cambridge University Press, Cambridge, 2003. xviii+646 pp.

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

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

[17] H. Ohmori and T. Miyamoto, Construction of weighing matrices $W(17, 9)$ having the intersection number 8, *Des. Codes Cryptogr.* 15 (1998), 259–269.