2010

On the Equivalence Between Real Mutually Unbiased Bases and a Certain Class of Association Schemes

Nicholas LeCompte
Worcester Polytechnic Institute, nl@wpi.edu

William J. Martin
Worcester Polytechnic Institute, martin@wpi.edu

William Owens
Worcester Polytechnic Institute, wilco@wpi.edu

Suggested Citation

LeCompte, N., Martin, W. J., & Owens, W. (2010). On the Equivalence Between Real Mutually Unbiased Bases and a Certain Class of Association Schemes. *European Journal of Combinatorics, 31*(6), 1499-1512. http://dx.doi.org/http://dx.doi.org/10.1016/j.ejc.2009.11.014

On the equivalence between real mutually unbiased bases and a certain class of association schemes

Nicholas LeCompte, William J. Martin, William Owens
Department of Mathematical Sciences
Worcester Polytechnic Institute
Worcester, MA
{nl,martin,wilco}@wpi.edu

Submitted August 18, 2008. Final revision March 22, 2009.

Abstract

Mutually unbiased bases (MUBs) in complex vector spaces play several important roles in quantum information theory. At present, even the most elementary questions concerning the maximum number of such bases in a given dimension and their construction remain open. In an attempt to understand the complex case better, some authors have also considered real MUBs, mutually unbiased bases in real vector spaces. The main results of this paper establish an equivalence between sets of real mutually unbiased bases and 4-class cometric association schemes which are both Q-bipartite and Q-antipodal. We then explore the consequences of this equivalence, constructing new cometric association schemes and describing a potential method for the construction of sets of real MUBs.

1 Introduction

In quantum information theory, one important challenge is to construct mutually (i.e., pairwise) unbiased bases in complex vector spaces $\mathbb{C}^d$. A pair of unitary bases for $\mathbb{C}^d$ are "unbiased" with respect to one another if, in the change-of-basis matrix from one basis to the other, all entries have the same magnitude. While much progress has been made and various connections to combinatorics have emerged (see, e.g., [15, 2]), much remains to be done. In an effort to better understand the problem, several authors [5, 20] have recently proposed the study of real mutually unbiased bases. While the modified problem seems to be of a somewhat different nature, there are some similarities to the problem in complex space and the study of real MUBs seems interesting on its own. Our goal is to show that this latter problem is equivalent to the study of a certain class of association schemes whose characterization is implicit in the work of Delsarte [10] in 1973. Indeed, this connection is already evident in recent work on an important special case by Bannai and his co-authors [1, 4].

In the next section, we provide a very brief review of association schemes, giving all the definitions necessary for the statement of our results. Section 3, based on the paper [5] of Boykin, et al., summarizes what is currently known about sets of real MUBs. The main results of the paper are presented in Section 4 and the implications of these results are explored in Section 5. Finally, in the appendix, we include all parameters of the underlying association scheme that we study.

2 Cometric association schemes

We begin with a review of the basic definitions concerning cometric association schemes. The reader is referred to [3] or [6] for background material.

A *(symmetric) association scheme* $(X, \mathcal{R})$ consists of a finite set X of size v and a set $\mathcal{R}$ of binary relations on X satisfying

(i) $\mathcal{R} = \{R_0, \ldots, R_D\}$ is a partition of $X \times X$;

(ii) R_0 is the identity relation;

(iii) $R_i^\top = R_i$ for each i;

(iv) there exist integers p_{ij}^k such that $|\{c \in X : (a, c) \in R_i \text{ and } (c, b) \in R_j\}| = p_{ij}^k$ whenever $(a, b) \in R_k$, for each $i, j, k \in \{0, \ldots, D\}$.

As usual, we define A_i to be the matrix with rows and columns indexed by X with (a, b)-entry equal to one if $(a, b) \in R_i$ and zero otherwise. In this way, we obtain a collection of $v \times v$ symmetric 01-matrices $\mathbf{A} = \{A_0, A_1, \ldots, A_D\}$ such that:

(i') $\sum_{i=0}^{D} A_i = J$ where J is the all 1's matrix,

(ii') A_0 is the identity matrix;

(iii') $A_i^\top = A_i$ for each i;

(iv') the set $\mathbf{A}$ forms a basis for a commutative matrix algebra $\mathcal{A}$ called the *Bose-Mesner algebra*.

Since no two matrices in $\mathbf{A}$ have a nonzero entry in the same location, the Bose-Mesner algebra is also closed under entrywise (or Schur) multiplication, denoted $\circ$.

The matrices $\mathbf{A}$ may be simultaneously diagonalized; there are $D + 1$ maximal common eigenspaces for $\mathcal{A}$ known as the *eigenspaces* of the scheme, and it follows from elementary linear algebra that the primitive idempotents $E_0, E_1, \ldots, E_D$ representing orthogonal projection onto these eigenspaces form another basis for $\mathcal{A}$. If we let P_{ji} denote the eigenvalue of A_i on the j^{th} eigenspace of the scheme, i.e., P_{ji} satisfies

$$A_i E_j = P_{ji} E_j,$$

then the $(D+1) \times (D+1)$ matrix P containing P_{ji} as its entry in the j^{th} row, i^{th} column is called the *first eigenmatrix* of the association scheme.

The *second eigenmatrix* Q of the scheme is defined as $Q = vP^{-1}$ (so that $E_j = \frac{1}{v}\sum_i Q_{ij} A_i$) but also satisfies a second "orthogonality relation". If v_i denotes the valency of the relation R_i (i.e., the common row sum of the matrix A_i) and m_j denotes the dimension of the j^{th} eigenspace (i.e., the rank of E_j), then we have, for all i and j,

$$v_i Q_{ij} = m_j P_{ji} \tag{2.1}$$

(Equation (3), [6, p46]). Since we have $E_j = \frac{1}{v}\sum_i Q_{ij} A_i$, the entry in row a, column b of E_j is Q_{ij}/v whenever $(a,b) \in R_i$. This is also the value of the standard inner product of column a and column b of the same matrix E_j.

An association scheme is *metric* (or P-polynomial) if there is an ordering $R_0, R_1, \ldots, R_D$ on the relations so that, for each i, A_i may be expressed as a matrix polynomial of degree exactly i in A_1. Such an ordering is called a *P-polynomial ordering*. Delsarte [10] showed that metric association schemes, with specified P-polynomial ordering, are in one-to-one correspondence with distance-regular graphs (see [6, Prop. 2.7.1] or [3, Prop. III.1.1]). By analogy, an association scheme is said to be *cometric* (or Q-polynomial) if there is an ordering $E_0, E_1, \ldots, E_D$ on the primitive idempotents so that, for each j, E_j may be expressed as a polynomial of degree exactly j applied entrywise to the values in E_1. Such an ordering is called a *Q-polynomial ordering*.

It is becoming conventional to specify the parameters of a D-class cometric association scheme $(X, \mathcal{R})$ by its *Krein array*

$$\iota^*(X, \mathcal{R}) = \{b_0^*, b_1^*, \ldots, b_{D-1}^*;\, c_1^*, c_2^*, \ldots, c_D^*\}$$

where $b_j^* := q_{1,j+1}^j$ $(0 \le j < D)$ and $c_j^* := q_{1,j-1}^j$ $(1 \le j \le D)$. All parameters may be recovered from these few. For example, $m_1 = b_0^*$, $c_1^* = 1$ and the parameters $a_j^* := q_{1,j}^j$ $(0 \le j \le D)$ satisfy

$$c_j^* + a_j^* + b_j^* = m_1$$

for $0 \le j \le D$ where, by convention, we define $c_0^* = b_D^* = 0$.

A cometric association scheme $(X, \mathcal{R})$ is *Q-bipartite* if $q_{ij}^k = 0$ whenever $i+j+k$ is odd. Suzuki [18] points out that this is equivalent to $a_j^* = 0$ for $j = 1, 2, \ldots, D$. In [16], this is also shown to be equivalent to the condition

$$Q_{D-i,1} = -Q_{i,1}$$

for $0 \le i \le D$. For a bipartite distance-regular graph, the first column of the matrix P is symmetric about the origin; for a Q-bipartite cometric scheme, the first column of matrix Q has this property.

A cometric association scheme $(X,\mathcal{R})$ is *Q-antipodal* if $q_{i,D-j}^{D-k} = q_{i,j}^{k}$ whenever $j+k \neq D$. Suzuki [18] points out that this is equivalent to $b_j^* = c_{D-j}^*$ for for all $j = 0,1,2,\ldots,D-1$ except possibly $j = \lfloor \frac{D}{2} \rfloor$.

Throughout this paper, we use the *natural ordering* of the relations: we re-label relations $R_0,\ldots,R_D$ if necessary so that

$$Q_{0,1} > Q_{1,1} > \cdots > Q_{D,1}.$$

With this ordering, it is shown in [16] that the Q-antipodal condition is equivalent to the condition

$$Q_{i,D} = \begin{cases} m_D & i \text{ even;} \\ -1 & i \text{ odd.} \end{cases}$$

An antipodal distance-regular graph has the property that the graph (X,R_D) is a union of complete graphs of size v_D+1. A Q-antipodal cometric scheme has the property that the graph

$$(X, R_0 \cup R_2 \cup \cdots \cup R_e)$$

is a union of m_D+1 complete graphs where $e = 2\lfloor \frac{D}{2} \rfloor$.

An association scheme is said to be *imprimitive* if some graph (X,R_i) $(1 \leq i \leq D)$ is disconnected. Equivalently, the scheme is disconnected if some E_j $(1 \leq j \leq D)$ has repeated columns. It is well-known that an imprimitive distance-regular graph is either bipartite or antipodal or both.

Theorem 2.1 (Suzuki [18]). *If $(X,\mathcal{R})$ is a D-class imprimitive cometric association scheme with $D \neq 6$, then $(X,\mathcal{R})$ is either Q-bipartite or Q-antipodal or both.*

We remark that it is likely that this result holds for $D=6$ as well, but one exceptional series of parameter sets remains to be ruled out.

The vertex set of a Q-antipodal association scheme admits a natural partition

$$X = X_1 \cup X_2 \cup \cdots \cup X_w$$

into subsets of size v/w such that, for even i, each edge of the graph (X,R_i) lies within some X_j and, for each odd i, each edge of the graph (X,R_i) has endpoints in distinct cells X_j of this partition. In [16], a "Dismantlability Theorem" is proved which establishes that, for any $Y \subseteq X$ which is expressible as a union of some subcollection of the X_j the D relations restricted to Y induce a cometric subscheme of this association scheme.

3 Real mutually unbiased bases

Let $\mathcal{B}_1,\mathcal{B}_2,\ldots,\mathcal{B}_w$ be w orthonormal bases for $\mathbb{R}^d$. We say that these bases are *mutually unbiased* if, whenever $i \neq j$, the expansion of any element of $\mathcal{B}_i$ in terms of basis $\mathcal{B}_j$ has all coefficients of equal magnitude. That is, $\langle a,b\rangle = \pm\frac{1}{\sqrt{d}}$ whenever a and b are chosen from distinct bases among $\mathcal{B}_1,\ldots,\mathcal{B}_w$.

Example 3.1. *The 24-cell is a regular polytope in* $\mathbb{R}^4$ *with vertex set*

$$\{\pm \mathbf{e}_i : 1 \le i \le 4\} \cup \{(w,x,y,z) : \ w,x,y,z \in \{1/2, -1/2\} \ \} .$$

This corresponds naturally to a set of 3 real mutually unbiased bases in $\mathbb{R}^4$ *by taking one vector from each parallel pair among the twelve pairs of dependent vectors in the above set. With this coordinatization, the bases may be taken to be*

$$\mathcal{B}_1 = \{(1,0,0,0),\ (0,1,0,0),\ (0,0,1,0),\ (0,0,0,1)\} ,$$

$$\mathcal{B}_2 = \left\{ \left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right), \left(\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}, \frac{1}{2}\right), \left(\frac{1}{2}, -\frac{1}{2}, \frac{1}{2}, -\frac{1}{2}\right), \left(\frac{1}{2}, \frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}\right) \right\},$$

$$\mathcal{B}_3 = \left\{ \left(-\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right), \left(\frac{1}{2}, -\frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right), \left(\frac{1}{2}, \frac{1}{2}, -\frac{1}{2}, \frac{1}{2}\right), \left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, -\frac{1}{2}\right) \right\}.$$

It is no coincidence that these 24 vectors also determine a 4-class cometric association scheme.

For $d \ge 2$, let M_d denote the maximum number of real mutually unbiased bases in $\mathbb{R}^d$. Also, let N_n denote the maximum number of mutually orthogonal latin square (MOLS) of side n. The following theorem summarizes what is currently known about the numbers M_d.

Theorem 3.2 (Various authors). *Let* $d \ge 3$. *Then*

- *(i) [11]* $M_d \le \frac{d}{2} + 1$;
- *(ii) [7] if* $d = 4^k$ *for some integer* k, *then* $M_d = \frac{d}{2} + 1$;
- *(iii) [5] if* d *is not divisible by four, then* $M_d = 1$;
- *(iv) [5]* $M_d \ge 2$ *if and only if there is a Hadamard matrix of side* d;
- *(v) [5]* $M_d \ge 3$ *if and only if there exist Hadamard matrices* H_1, H_2, H_3 *of side* d *satisfying* $H_1 H_2 = \sqrt{d} H_3$
- *(vi) [5] if* d *is not a square, then* $M_d \le 2$;
- *(vii) [5] if* $d/4$ *is an odd square, then* $M_d \le 3$;
- *(viii) [20] if there exists a Hadamard matrix of side* $n = \sqrt{d}$, *then* $M_d \ge N_n + 2$.

Finally, $M_2 = 2$.

Some remarks are in order here. The paper [11] of Delsarte, Goethals and Seidel gives bounds on sets of lines through the origin with few angles. One of these bounds — the second example in Table I of [11] — applies directly to the situation at hand. When d is a power of four (d at least sixteen), there is a construction achieving the bound in part (i) of the theorem based on Kerdock codes. This configuration is implicit in [7] but the best source for the explicit set of vectors in Euclidean space is [8]. It is widely believed that Hadamard matrices exist of side n for all n divisible by four. The state of the art regarding the values N_n is summarized in [9, III.3.6].

4 The equivalence

In this section, we establish an equivalence between 4-class cometric association schemes which are both Q-bipartite and Q-antipodal, on the one hand, and collections of real mutually unbiased bases, on the other.

Let $\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_w$ be w mutually unbiased bases in $\mathbb{R}^d$ and set

$$X = \pm\mathcal{B}_1 \cup \pm\mathcal{B}_2 \cup \cdots \cup \pm\mathcal{B}_w.$$

Then $|X| = 2wd$ and any pair of vectors from X have inner product belonging to the set

$$A' = \left\{ \sigma_0 := 1,\ \sigma_1 := \frac{1}{\sqrt{d}},\ \sigma_2 := 0,\ \sigma_3 := -\frac{1}{\sqrt{d}},\ \sigma_4 := -1 \right\}.$$

For $a, b \in X$ and $0 \le i, j \le 4$, set

$$p_{i,j}(a,b) := \left| \{ c \in X : \langle a, c \rangle = \sigma_i,\ \langle c, b \rangle = \sigma_j \} \right|.$$

We aim to show that $p_{i,j}(a,b)$ is independent of the choice of a and b, but depends only on i, j and $\langle a, b \rangle$. This result generalizes a result of Bannai, et al. (see [4],[1]).

Theorem 4.1. *Let $\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_w$ be w mutually unbiased bases in $\mathbb{R}^d$ and let X be defined as above. Then relations $R_0, \ldots, R_4$ given by*

$$R_i = \{ (a,b) \in X \times X : \langle a, b \rangle = \sigma_i \}$$

form a Q-bipartite, Q-antipodal cometric association scheme on X with intersection numbers $L_i = [p^k_{ij}]_{k,j}$ given by $L_0 = I$,

$$L_1 = \begin{bmatrix} 0 & d(w-1) & 0 & 0 & 0 \\ 1 & \frac{d+\sqrt{d}}{2}(w-2) & d-1 & \frac{d-\sqrt{d}}{2}(w-2) & 0 \\ 0 & \frac{d}{2}(w-1) & 0 & \frac{d}{2}(w-1) & 0 \\ 0 & \frac{d-\sqrt{d}}{2}(w-2) & d-1 & \frac{d+\sqrt{d}}{2}(w-2) & 1 \\ 0 & 0 & 0 & d(w-1) & 0 \end{bmatrix}, L_2 = \begin{bmatrix} 0 & 0 & 2(d-1) & 0 & 0 \\ 0 & d-1 & 0 & d-1 & 0 \\ 1 & 0 & 2(d-2) & 0 & 1 \\ 0 & d-1 & 0 & d-1 & 0 \\ 0 & 0 & 2(d-1) & 0 & 0 \end{bmatrix},$$

$$L_3 = \begin{bmatrix} 0 & 0 & 0 & d(w-1) & 0 \\ 0 & \frac{d-\sqrt{d}}{2}(w-2) & d-1 & \frac{d+\sqrt{d}}{2}(w-2) & 1 \\ 0 & \frac{d}{2}(w-1) & 0 & \frac{d}{2}(w-1) & 0 \\ 1 & \frac{d+\sqrt{d}}{2}(w-2) & d-1 & \frac{d-\sqrt{d}}{2}(w-2) & 0 \\ 0 & d(w-1) & 0 & 0 & 0 \end{bmatrix}, L_4 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Proof. In most cases, it is straightforward to verify that a given intersection number is well-defined. For L_2, this follows from the observation that each set $\pm\mathcal{B}_i$ is the set of vertices of an orthoplex (or "cross polytope"). Moreover, the value of p^1_{21}, for instance, is obtained by noting that, for $\langle a, b \rangle = \sigma_1$, the map $c \mapsto -c$ on $\{c \in X : \langle a, c \rangle = 0\}$ is a bijection between

$$\{ c \in X : \langle a, c \rangle = 0, \langle c, b \rangle = \sigma_1 \}$$

and

$$\{c \in X : \langle a, c \rangle = 0, \langle c, b \rangle = \sigma_3\}.$$

Such considerations establish that all p_{ij}^k are well-defined except possibly the eight quantities

$$p_{11}^1,\ p_{13}^1,\ p_{11}^3,\ p_{13}^3,\ p_{31}^1,\ p_{33}^1,\ p_{31}^3,\ p_{33}^3.$$

Without assuming that we have an association scheme, we find that

$$\begin{aligned} p_{11}(a,b) + p_{13}(a,b) &= d(w-2) && (4.1)\\ p_{31}(a,b) + p_{33}(a,b) &= d(w-2) && (4.2)\\ p_{31}(a,b) &= p_{13}(a,b) && (4.3)\\ p_{11}(a,b) &= p_{13}(a,-b) && (4.4) \end{aligned}$$

whenever a and b are chosen from distinct extended bases among the $\pm\mathcal{B}_h$. So it suffices to prove that $p_{11}(a,b)$ does not depend on the choice of a and b provided $(a,b) \in R_1$.

To do so, we apply Lemma 7.3 in [12]. Since each orthoplex $\pm\mathcal{B}_h$ is a spherical 3-design in $\mathbb{R}^d$, the union of the w of them is also a spherical 3-design. So we can take $i = j = 1$ (since $1 + 1 \leq 3$) in Lemma 7.3 of [12] to obtain the linear equation

$$\sum_{h=0}^{4} \sum_{\ell=0}^{4} \sigma_h \sigma_\ell p_{h\ell}(a,b) = |X| \frac{\langle a, b \rangle}{d}.$$

which, for $(a,b) \in R_1$, reduces to

$$\frac{1}{d} p_{11}(a,b) - \frac{1}{d} p_{13}(a,b) - \frac{1}{d} p_{31}(a,b) + \frac{1}{d} p_{33}(a,b) + \frac{4}{\sqrt{d}} = \frac{2k}{\sqrt{d}}.$$

So, applying the above identifications, we obtain the linear system

$$\begin{aligned} p_{11}(a,b) + p_{13}(a,b) &= d(k-2) && (4.5)\\ p_{11}(a,b) - p_{13}(a,b) &= \sqrt{d}(k-2) && (4.6) \end{aligned}$$

which has a unique solution, independent of the choice of a and b, simply provided $(a,b) \in R_1$.

Now it is straightforward to verify that this association scheme is both Q-bipartite and Q-antipodal. Since R_4 consists of the pairs $(a, -a)$ for $a \in X$, we have an imprimitive scheme and this can only be a Q-bipartite system of imprimitivity, by Suzuki's Theorem. But we also have the partition of X into the orthoplexes $\pm\mathcal{B}_h$, which are of size at least four (provided $d > 1$); so the scheme is Q-antipodal as well. □

Our next result gives the reverse implication.

Theorem 4.2. *Let $(X, \mathcal{R})$ be a cometric 4-class association scheme which is both Q-antipodal and Q-bipartite and let E_1 denote the first primitive idempotent in a Q-polynomial ordering for $(X, \mathcal{R})$. Set $d = \operatorname{rank} E_1$. Write*

$$E_1 = \frac{d}{|X|} U U^\top$$

for some $|X| \times d$ matrix U with orthogonal columns all having the same norm $\sqrt{|X|/d}$. Then all rows of U are unit vectors in $\mathbb{R}^d$ and, for each row a of U, we have that $-a$ is also a row of U. Let $Y \subseteq S^{d-1}$ be constructed by choosing arbitrarily one vector from each such parallel pair of rows of U. Then Y is naturally partitioned into a collection of $w = |X|/2d$ real mutually unbiased bases in $\mathbb{R}^d$.

Proof. We apply basic facts about imprimitive cometric schemes first observed in [16]. Let Q be the matrix of dual eigenvalues Q_{ij} $(0 \le i,j \le 4)$ of $(X,\mathcal{R})$. Then, under the natural ordering of the relations, the second column of Q (with entries Q_{i1}) is symmetric about zero and we have

$$Q_{01} = m_1 \;>\; Q_{11} \;>\; Q_{21} = 0 \;>\; Q_{31} = -Q_{11} \;>\; Q_{41} = -m_1.$$

Since the entries in this column are all distinct, we can identify the elements of X with the columns of E_1 — or, equivalently, with the rows r_a of matrix U — in such a way that $(a,b) \in R_i$ precisely when $\langle r_a, r_b\rangle = Q_{i1}/m_1$. Since our association scheme is Q-antipodal, the relation

$$a \sim b \;\Leftrightarrow\; \langle r_a, r_b\rangle \in \{1, 0, -1\}$$

is an equivalence relation on X.

Identifying pairs a, b with $(a,b) \in R_4$ yields a 2-class quotient scheme, a strongly regular graph. Since our 4-class scheme is Q-antipodal, this graph must also be imprimitive. So it is a complete multipartite graph $\overline{wK_d}$ for some integers w and d satisfying $wd = \frac{1}{2}|X|$. The second eigenmatrix for this strongly regular graph is

$$\tilde{Q} = \begin{bmatrix} 1 & w(d-1) & w-1 \\ 1 & 0 & -1 \\ 1 & -w & w-1 \end{bmatrix}.$$

Standard properties of imprimitive schemes inform us that this matrix must appear as a submatrix of the second eigenmatrix Q of our 4-class scheme — in fact, the matrix $\tilde{Q}$ with each of its last two rows duplicated, gives us columns 0, 2 and 4 of Q. So our 4-class scheme has second eigenmatrix of the following form:

$$Q = \begin{bmatrix} 1 & m_1 & w(d-1) & wd - m_1 & w-1 \\ 1 & Q_{11} & 0 & -Q_{11} & -1 \\ 1 & 0 & -w & 0 & w-1 \\ 1 & -Q_{11} & 0 & Q_{11} & -1 \\ 1 & -m_1 & w(d-1) & -m_3 & w-1 \end{bmatrix}.$$

(Here, we have used standard identities such as [6, Lemma 2.2.1].) Since we have assumed a Q-polynomial ordering on the eigenspaces, we have the three-term recurrence

$$Q_{i1}^2 = m_1 + q_{11}^2 Q_{i2} \qquad (0 \le i \le 4).$$

(Since our scheme is Q-bipartite, we have $q_{11}^1 = 0$.) Taking $i = 2$ first gives $q_{11}^2 = m_1/w$; next, take $i = 0$ to find $m_1 = d$. Finally take $i = 1$ to establish $Q_{11} = \sqrt{d}$. Thus the $|X| = 2wd$

rows of the matrix U defined in the statement of the theorem have pairwise inner products $1, 0, -1$ for vectors in the same equivalence class, and $\pm\frac{1}{\sqrt{d}}$ for vectors chosen from distinct equivalence classes. Since each equivalence class has size $2d$, we may choose one vector from each parallel pair of rows of U and obtain w mutually unbiased bases in $\mathbb{R}^d$. □

The above two results are summarized in the following

Theorem 4.3. *Let w and d be integers with $w, d \geq 2$. Then there exist w real mutually unbiased bases in $\mathbb{R}^d$ if and only if there exists a cometric 4-class association scheme on $2wd$ vertices which is both Q-bipartite and Q-antipodal with Q-antipodal classes of size $2d$.* □

5 Applications of the main results

In view of the above results, every construction and every bound for real mutually unbiased bases gives rise to constructions and non-existence results for 4-class cometric association schemes which are both Q-bipartite and Q-antipodal.

As observed by [5] and other authors, any pair of MUBs in $\mathbb{R}^d$ is equivalent to a $d \times d$ Hadamard matrix. In this case, the underlying association scheme is not only Q-polynomial, but P-polynomial as well; these are the Hadamard graphs.

The construction of Wocjan and Beth [20] gives infinitely many new cometric association schemes with Krein arrays

$$\left\{d,\ d-1,\ d\frac{(w-1)}{w},\ 1;\ 1,\ \frac{d}{w},\ d-1,\ d\right\}$$

whenever there is a Hadamard matrix of side $n := \sqrt{d}$ and $2 \leq w \leq N_n + 2$.

The current state of affairs, regarding the optimal value of w for a given dimension d, is summarized in Theorem 3.2. For $d > 2$, only $w = 1$ is possible unless d is a multiple of four. (In this case, we have a trivial strongly regular graph.) For d a mutiple of four and $d \leq 120$, we have the following ranges for the maximum value of w:

d	4	8	12	16	20	24	28	32	36	40	44	48	52	56	60
w	3	2	2	9	2	2	2	2	2-3	2	2	2	2	2	2

d	64	68	72	76	80	84	88	92	96	100	104	108	112	116	120
w	33	2	2	2	2	2	2	2	2	2-3	2	2	2	2	2

So there are only a few open questions for these small parameter sets. Less is known about the optimal value of w for dimensions d of the form $d = 16s^2$, where s is not a power of two; for example it is not known if the absolute bound $w \leq \frac{d}{2} + 1$ can be achieved for any d other than d a power of four. Some key small values to consider are $d = 144$, 400, 576, 784, 1296 and 1600. For example, in $\mathbb{R}^{144}$, the construction of Wocjan and Beth gives $w = 7$ real MUBs but the best upper bound we have is $w \leq 73$.

In [16], an infinite family of cometric 4-class schemes is constructed by taking the "extended Q-bipartite doubles" of the Cameron-Seidel schemes; these 3-class cometric schemes were found in [7] as linked systems of symmetric designs. Using Theorem 4.2, this gives us

$\frac{d}{2}+1$ MUBs in $\mathbb{R}^d$ for $d=4^k$, $k\geq 2$. Of course, this is the same configuration as the one given in [8]. Bannai and co-authors [1, 4] were the first to realize that this configuration of MUBs gives rise to a cometric association scheme. But the Dismantlability Theorem in [16] tells us that any subcollection of the Q-antipodal classes in this association scheme also induce a cometric association scheme which is again both Q-bipartite and Q-antipodal. The configuration of MUBs which one obtains from these schemes are just those obtained from the extremal example by deleting some subcollection of bases.

In [17], Mathon conducted an exhaustive study of linked systems of $(16,6,2)$ symmetric designs. Via the extended Q-bipartite double construction and Theorem 4.2 above, these give rise to various configurations of maximal MUBs in $\mathbb{R}^{16}$ with less than the optimal number of bases. (The optimal value of nine bases is achievable only by the Cameron-Seidel construction.)

A *translation association scheme* [6, p65] is an association scheme which admits an abelian group acting regularly on its vertices. In [6, p425], Brouwer, et al. point out that a 4-class P-polynomial association scheme which is both antipodal and bipartite is equivalent to a symmetric (m,μ)-net [6, p18]: a set $\mathcal{P}$ of points and a set $\mathcal{L}$ of lines with the properties (i) any point lies on m lines; (ii) any line meets m points; (iii) any two points are joined by either μ or zero lines; (iv) any two lines meet in either μ or zero points; and (v) the configuration is non-degenerate. We simply observe that, since every translation scheme gives rise to a dual association scheme on its characters and the dual of a P-polynomial association scheme is Q-polynomial, with imprimitivity properties mapping over naturally, every symmetric (m,μ)-net which is a translation scheme gives rise in this way to a set of mutually unbiased bases in real space. It is an open question as to whether any non-trivial examples exist.

5.1 Arrangements of Hadamard matrices

As a precursor to our next theorem, we partition the adjacency matrices of our scheme according to the two imprimitivity systems discussed above. Suppose we have w mutually unbiased bases in $\mathbb{R}^d$. The rows and columns of the adjacency matrices shall be indexed so that elements in each Q-antipodal class are grouped together, and pairs in Q-bipartite classes correspond to consecutive row/column labels $2\ell-1$, 2ℓ. Put geometrically, we index by grouping the vectors in each of the w extended bases $\pm\mathcal{B}_i$ together, and index each parallel pair $\pm b$ consecutively. As usual, A_0 is the identity matrix of size $2dw$. Now A_1 encodes the relation

$$(a,b)\in R_1 \;\Leftrightarrow\; \langle a,b\rangle = \frac{1}{\sqrt{d}}$$

and therefore has the form

$$A_1 = \begin{bmatrix} 0 & N_{1,2} & \cdots & N_{1,w} \\ N_{2,1} & 0 & \cdots & N_{2,w} \\ \vdots & \vdots & \ddots & \vdots \\ N_{w,1} & N_{w,2} & \cdots & 0 \end{bmatrix},$$

where each $N_{i,j}$ is a $2d \times 2d$ 01-matrix composed of d^2 2×2 blocks each equal to $\left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$ or $\left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right]$. By the symmetry of A_1, $N_{i,j}^T = N_{j,i}$. Since A_3 describes the relation corresponding to pairs with inner product $-\frac{1}{\sqrt{d}}$, we have

$$A_3 = \begin{bmatrix} 0 & J_{2d} - N_{1,2} & \cdots & J_{2d} - N_{1,w} \\ J_{2d} - N_{2,1} & 0 & \cdots & J_{2d} - N_{2,w} \\ \vdots & \vdots & \ddots & \vdots \\ J_{2d} - N_{w,1} & J_{2d} - N_{w,2} & \cdots & 0 \end{bmatrix},$$

where J_{2d} is the all-ones matrix of size $2d$.

Next, A_2 encodes the orthogonality relation among these vectors, and is hence a block diagonal matrix with blocks of size $2d$, and blocks of the form $J_{2d} - I_d \otimes J_2$ on the diagonal; $A_2 = I_w \otimes (J_{2d} - I_d \otimes J_2)$. Finally, A_4 describes the relation of -1 cosine, and is a block diagonal matrix with dw blocks of the form $\left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right]$ on the diagonal.

Theorem 5.1. *There exist w mutually unbiased bases in $\mathbb{R}^d$ if and only if there exist $\binom{w}{2}$ Hadamard matrices of size d (say $H_{i,j}$, $1 \le i < j \le w$), satisfying $H_{i,j}H_{j,k} = \sqrt{d}H_{i,k}$ for each triple i, j, k of distinct values from $\{1, \ldots, w\}$ where write $H_{j,i} = H_{i,j}^T$ for $j > i$.*

Proof. For the proof in the forward direction, we will make use of a simple linear transformation ϕ mapping 2×2 matrices to real numbers. Define

$$\phi\left(\left[\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right]\right) = \frac{1}{2}(\alpha + \delta - \beta - \gamma)$$

and note that when at least one of M or N takes the form $\left[\begin{smallmatrix} a & b \\ b & a \end{smallmatrix}\right]$, we not only have $\phi(M+N) = \phi(M) + \phi(N)$ but also $\phi(MN) = \phi(M)\phi(N)$. We extend ϕ to map matrices $M = [m_{r,s}]$ of size $2wd \times 2wd$ to matrices of size $wd \times wd$ in the natural way: the (k, ℓ)-entry of the resulting matrix $\phi(M)$ is $\phi\left(\left[\begin{smallmatrix} m_{2k-1,2\ell-1} & m_{2k-1,2\ell} \\ m_{2k,2\ell-1} & m_{2k,2\ell} \end{smallmatrix}\right]\right)$.

Let our collection $\{\mathcal{B}_i : 1 \le i \le w\}$ of MUBs be given and consider the association scheme determined by any two of the bases, $\mathcal{B}_i$ and $\mathcal{B}_j$. From above, this association scheme has first adjacency matrix of the form

$$A_1 = \begin{bmatrix} 0 & N \\ N^\top & 0 \end{bmatrix},$$

where we have used the abbreviations $N = N_{i,j}$ and $N^\top = N_{j,i}$. Using the intersection numbers computed in Theorem 4.1, we have that

$$A_1^2 = dI + \frac{d}{2}A_2 = \begin{bmatrix} dI + \frac{d}{2}(J_d - I_d) \otimes J_2 & 0 \\ 0 & dI + \frac{d}{2}(J_d - I_d) \otimes J_2 \end{bmatrix}$$

giving $NN^\top = N^\top N = dI + \frac{d}{2}(J_d - I_d) \otimes J_2$. Applying ϕ to both sides of this equation gives $\phi(N)\phi(N)^\top = dI$. Clearly, since each 2×2 block of N is either I_2 or $J_2 - I_2$, each entry of $\phi(N)$ is ± 1. So for each $i \neq j$, the matrix $H_{i,j} := \phi(N_{i,j})$ is a $d \times d$ Hadamard matrix.

We use the same idea to establish $H_{i,j}H_{j,k} = \sqrt{d}H_{i,k}$ for any three distinct indices $i, j, k \in \{1, \ldots, w\}$. Again applying Theorem 4.1, we obtain a 4-class cometric association scheme with three Q-antipodal classes and, again using the above conventions for ordering the rows and columns, we have

$$A_1 = \begin{bmatrix} 0 & N_{i,j} & N_{i,k} \\ N_{j,i} & 0 & N_{j,k} \\ N_{k,i} & N_{k,j} & 0 \end{bmatrix}, A_3 = \begin{bmatrix} 0 & J - N_{i,j} & J - N_{i,k} \\ J - N_{j,i} & 0 & J - N_{j,k} \\ J - N_{k,i} & J - N_{k,j} & 0 \end{bmatrix},$$

with A_2 and A_4 as above being all zero off the diagonal blocks. From Theorem 4.1, we have now

$$A_1^2 = 2dA_0 + \frac{d + \sqrt{d}}{2}A_1 + dA_2 + \frac{d - \sqrt{d}}{2}A_3.$$

Consider some nondiagonal block of both sides of this equation, say block (i, k). We find

$$N_{i,j}N_{j,k} = \sqrt{d}N_{i,k} + \frac{d - \sqrt{d}}{2}J_{2d}.$$

Applying ϕ to both sides gives

$$H_{i,j}H_{j,k} = \sqrt{d}H_{i,k},$$

as desired. Since this holds for any choice of distinct indices i, j and k, the forward implication of the theorem is now established.

Now we reverse the construction. Suppose we are given $\binom{w}{2}$ Hadamard matrices of order d, $\{H_{i,j} \ : \ 1 \leq i < j \leq w\}$, enjoying the property

$$H_{i,j}H_{j,k} = \sqrt{d}H_{i,k} \tag{5.1}$$

whenever $i < j < k$. Defining $H_{j,i} := H_{i,j}^\top$ for $j > i$, one easily verifies that Equation (5.1) now holds whenever i, j and k are distinct elements of $\{1, \ldots, w\}$.

We blow up each $H_{i,j}$ in the obvious way to a 01-matrix $N_{i,j}$ by mapping $\psi : 1 \mapsto \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$ and $\psi : -1 \mapsto \left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right]$. Now we define

$$A_1 = \begin{bmatrix} 0 & N_{1,2} & \cdots & N_{1,w} \\ N_{2,1} & 0 & \cdots & N_{2,w} \\ \vdots & \vdots & \ddots & \vdots \\ N_{w,1} & N_{w,2} & \cdots & 0 \end{bmatrix}, A_3 = \begin{bmatrix} 0 & J - N_{1,2} & \cdots & J - N_{1,w} \\ J - N_{2,1} & 0 & \cdots & J - N_{2,w} \\ \vdots & \vdots & \ddots & \vdots \\ J - N_{w,1} & J - N_{w,2} & \cdots & 0 \end{bmatrix},$$

defining A_0, A_2 and A_4 in the obvious way as above.

Since $H_{j,i}H_{i,j} = dI$, we have

$$N_{j,i}N_{i,j} = dI_{2d} + \frac{d}{2}(J_{2d} - I_d \otimes J_2).$$

The second term on the right arises from considering the off-diagonal entries of $H_{j,i}H_{i,j}$, which is a sum of $\frac{d}{2}$ 1's and $\frac{d}{2}$ -1's, and hence under ψ map to $\frac{d}{2}J_2$. Similar considerations give $N_{i,j}N_{j,k} = \sqrt{d}N_{i,k} + \frac{d+\sqrt{d}}{2}J_{2d}$ for any three distinct i, j and k. Using these facts, we expand the various blocks

$$\sum_{i\neq j} N_{j,i}N_{i,j} = (w-1)\left(dI_{2d} + \frac{d}{2}(J_{2d} - I_d \otimes J_2)\right)$$

and

$$\sum_{j\neq i,k} N_{i,j}N_{j,k} = (w-2)\left(\sqrt{d}N_{i,k} + \frac{d+\sqrt{d}}{2}J_{2d}\right)$$

of A_1^2 to obtain

$$A_1^2 = d(w-1)A_0 + \frac{d+\sqrt{d}}{2}(w-2)A_1 + \frac{d}{2}(w-1)A_2 + \frac{d-\sqrt{d}}{2}(w-2)A_3.$$

In the same manner, one may routinely very the remaining equations $A_iA_j = \sum_k p_{ij}^k A_k$, thus concluding the proof that we have an association scheme with the same parameters as in the statement of Theorem 4.1. Then Theorem 4.2 gives the desired result. □

Before giving the next corollary, we introduce some convenient terminology. Fix a dimension d and consider a set system

$$\{C_j : j \in I\}$$

where I is some index set and each C_j consists of vectors in $\mathbb{R}^d$. (We will have only ± 1-vectors in our setting.) In this system, a *cohesive triple* refers to a set of three vectors $u, v, u \circ v$ all belonging to the same C_j. A *folded triple* refers to a set of three vectors $u, v, u \circ v$ with u and v belonging to the same C_k and $u \circ v$ an element of some C_j, $j \neq k$. Finally, a *split triple* refers to a set of three vectors $u, v, u \circ v$ all belonging to different sets C_j in this set system.

We will call a ± 1 vector z "balanced" if the number entries equal to -1 is congruent to zero modulo four and "semibalanced" if the number entries equal to -1 is congruent to two modulo four.

Corollary 5.2. *Suppose $d = 16s^2$ for some odd integer s and suppose $\{\mathcal{B}_1, \ldots, \mathcal{B}_w\}$ is a collection of mutually unbiased bases in $\mathbb{R}^d$. Fix any i, $1 \leq i \leq w$, and for each $j \neq i$ let C_j denote the set of columns of the matrix $H_{i,j}$ constructed in Theorem 5.1. With respect to the set system $\{C_j : j \neq i\}$, the following hold true:*

- *(i) each C_j contains d distinct vectors and the sets $\{C_j : j \neq i\}$ are pairwise disjoint;*
- *(ii) if $u, v, u \circ v$ is a cohesive triple in C_j, then every other vector in C_j is balanced and every vector in any C_k with $k \neq j$ is semibalanced;*
- *(iii) if $u, v, u \circ v$ is a folded triple with $u \circ v$ in C_j, then every other vector in C_j is balanced and every vector in any C_k with $k \neq j$ is semibalanced;*

(iv) *if $u, v, u \circ v$ is a split triple in $\{C_j : j \neq i\}$, then every other vector in the same C_j as either u, v or $u \circ v$ is semibalanced and every vector in any other C_k is balanced.*

Proof. By Theorem 5.1, the matrices $H_{i,j}$ are all Hadamard matrices and therefore can have no repeated columns. If $j \neq k$ and yet C_j and C_k have a vector in common, then some column of $H_{i,j}$ is equal to some column of $H_{i,k}$ — for simplicity, let us suppose this is the first column in each case. Then we have $H_{j,i} H_{i,k} = H_{i,j}^{\top} H_{i,k} = 4s H_{j,k}$ and yet the $(1,1)$-entry of this product is equal to $d = 16s^2$, a contradiction. This establishes (i).

For parts (ii)–(iv), we will use the Sylvester matrix

$$M = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

If $t = [t_1, t_2, t_3, t_4, t_5, t_6, t_7, t_8]$ is any vector and we write $x = [x_{000}, x_{001}, x_{010}, x_{011}, x_{100}, x_{101}, x_{110}, x_{111}]$, then the linear system $Mx = t$ has unique solution $x = \frac{1}{8} Mt$ with each entry of x having the form

$$x_{\dots} = \frac{t_1 \pm t_2 \pm \cdots \pm t_8}{8}.$$

Now suppose that z, u, v and $u \circ v$ are all members of $\cup_{j \neq i} C_j$. We consider the system of equations

$$\langle z, z \rangle = t_1 := 16s^2, \qquad \langle u, u \circ v \rangle = t_2, \qquad \langle v, u \circ v \rangle = t_3, \qquad \langle u, v \rangle = t_4,$$

$$\langle z, \mathbf{1} \rangle = t_5, \qquad \langle z, v \rangle = t_6, \qquad \langle z, u \rangle = t_7, \qquad \langle z, u \circ v \rangle = t_8$$

where $t_2, t_3, t_4, t_6, t_7, t_8 \in \{4s, 0, -4s\}$ and $t_5 = 16s^2 - 2\sigma$, σ being the number of -1's in the vector z. Now let x_{000} denote the number of coordinate positions h where $z_h = u_h = v_h = 1$, and similarly let $x_{001}, \ldots, x_{111}$ count coordinate positions h with the respectively properties

$$\begin{array}{lcl} x_{001} & : & z_h = 1,\ u_h = 1,\ v_h = -1 \\ x_{010} & : & z_h = 1,\ u_h = -1,\ v_h = 1 \\ x_{011} & : & z_h = 1,\ u_h = -1,\ v_h = -1 \\ x_{100} & : & z_h = -1,\ u_h = 1,\ v_h = 1 \\ x_{101} & : & z_h = -1,\ u_h = 1,\ v_h = -1 \\ x_{110} & : & z_h = -1,\ u_h = -1,\ v_h = 1 \\ x_{111} & : & z_h = -1,\ u_h = -1,\ v_h = -1 \end{array}$$

so that

$$x_{000} + x_{001} + x_{010} + x_{011} + x_{100} + x_{101} + x_{110} + x_{111} = 16s^2.$$

Then, with x as in the previous paragraph, the eight inner products above yield the linear system $Mx = t$. The fact that each $x_{\dots}$ must be an integer forces the integer

$$t_2 + t_3 + t_4 + t_5 + t_6 + t_7 + t_8$$

to be divisible by eight.

Now if $u, v, u \circ v$ is a cohesive triple, then $t_2 = t_3 = t_4 = 0$. If z belongs to the same cell C_j as these vectors, then $t_6 = t_7 = t_8 = 0$ as well and our linear system is solved to give

$$x_{001} = \frac{16s^2 + 16s^2 - 2\sigma}{8};$$

so z must be balanced. On the other hand, if z belongs to any other set C_k, we have $t_6 + t_7 + t_8 \in \{-12s, -4s, 4s, 12s\}$ and z must be semibalanced. The other cases are handled in a similar manner.

Without going into details, we remark that this result has strong implications for constructions of large sets of real MUBs in such dimensions, ruling out many configurations for two distinct triples of the form $u, v, u \circ v$.

Acknowledgments

The authors would like to thank Eiichi Bannai, Edwin van Dam and Chris Godsil for helpful discussions regarding related material.

During a portion of this work, all three authors were funded by NSA grant number H98230-07-1-0025, WJM as PI and NL and WO as summer research assistants. We are grateful to the US National Security Agency for this support.

References

[1] K. Abdukhalikov, E. Bannai, S. Suda. Association schemes related to universally optimal configurations, Kerdock codes and extremal Euclidean line-sets. *J. Combin. Theory, Ser. A* **116** (2009), 434-448.

[2] M. Aschbacher, A. M. Childs and P. Wocjan. Limitations of nice mutually unbiased bases. *J. Alg. Combin.* **25** (no. 2) (2007), 111–123.

[3] E. Bannai and T. Ito. Algebraic Combinatorics I: Association Schemes. Benjamin-Cummings, Menlo Park (1984).

[4] E. Bannai and E. Bannai. On antipodal spherical t-designs of degree s with $t \geq 2s - 3$. To appear, *J. Comb. Inf. Syst. Sci.*, special volume honoring the 75th birthday Prof. D. K. Ray-Chaudhuri.

[5] P. O. Boykin, M. Sitharam, M. Tarifi and P. Wocjan. Real mutually unbiased bases. Preprint. `arXiv:quant-ph/0502024v2 [math.CO]` (revised version dated Feb. 1, 2008)

[6] A. E. Brouwer, A. M. Cohen and A. Neumaier. Distance-Regular Graphs. Springer-Verlag, Berlin (1989).

[7] P. J. Cameron and J. J. Seidel. Quadratic forms over $GF(2)$. *Proc. Koninkl. Nederl. Akademie van Wetenschappen, Series A*, Vol. **76** (*Indag. Math.*, **35**) (1973), 1–8.

[8] A. R. Calderbank, W. M. Kantor, J. J. Seidel, N. J. A. Sloane. $\mathbb{Z}_4$-Kerdock codes, orthogonal spreads, and extremal Euclidean line-sets. *Proc. London Math. Soc.* **75**, no. 3 (1997), 436–480.

[9] C. J. Colbourn and J. H. Dinitz, eds. The CRC Handbook of Combinatorial Designs (2$^{\text{nd}}$ ed.) CRC Press, Boca Raton, 2006.

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

[11] P. Delsarte, J.-M. Goethals, J. J. Seidel. Bounds for systems of lines and Jacobi polynomials. *Philips Res. Rpts.* **30** (1975), 91-105.

[12] P. Delsarte, J.-M. Goethals, J. J. Seidel. Spherical codes and designs. *Geom. Ded.* **6** (1977), 363-388.

[13] C. D. Godsil. Algebraic Combinatorics. Chapman and Hall, New York (1993).

[14] A. Roy and C. Godsil. Equiangular lines, mutually unbiased bases, and spin models. In press, *Europ. J. Combin.*, 2008. (Appeared as `quant-ph/07000000`, 2007.)

[15] A Klappenecker and M. Rötteler. Constructions of mutually unbiased bases. pp. 137–144. in: *Finite Fields and Appl.*, Proceedings of 7th International Conference, Fq7, Toulouse, France, May 2003.

[16] W. J. Martin, M. Muzychuk and J. Williford. Imprimitive cometric association schemes: constructions and analysis. *J. Algebraic Combin.* **25** (2007), 399-415.

[17] R. Mathon. The systems of linked 2-$(16, 6, 2)$ designs. *Ars Combin.* **11** (1981), 131–148.

[18] H. Suzuki. Imprimitive Q-polynomial association schemes. *J. Alg. Combin.* **7** (1998), no. 2, 165–180.

[19] H. Suzuki. Association schemes with multiple Q-polynomial structures. *J. Alg. Combin.* **7** (1998), no. 2, 181–196.

[20] P. Wocjan and T. Beth. New constructions of mutually unbiased bases in square dimensions. *Quantum Information and Computation* **5** (2005), no. 2, 93–101.

Appendix: Remaining parameters of the association scheme

In this section, we give the eigenmatrices and Krein parameters for a 4-class Q-bipartite Q-antipodal association scheme. (The intersection numbers are given in the statement of Theorem 4.1.) The only free parameters are w and d where, as above, the vertices of the scheme correspond to w real MUBs in dimension d (so that $|X| = 2wd$).

$$P = \begin{bmatrix} 1 & d(w-1) & 2(d-1) & d(w-1) & 1 \\ 1 & \sqrt{d}(w-1) & 0 & -\sqrt{d}(w-1) & -1 \\ 1 & 0 & -2 & 0 & 1 \\ 1 & -\sqrt{d}(w-1) & 0 & \sqrt{d}(w-1) & -1 \\ 1 & -d & 2(d-1) & -d & 1 \end{bmatrix}, Q = \begin{bmatrix} 1 & d & w(d-1) & d(w-1) & w-1 \\ 1 & \sqrt{d} & 0 & -\sqrt{d} & -1 \\ 1 & 0 & -w & 0 & w-1 \\ 1 & -\sqrt{d} & 0 & \sqrt{d} & -1 \\ 1 & -d & w(d-1) & -d(w-1) & w-1 \end{bmatrix},$$

$$L_1^* = \begin{bmatrix} 0 & d & 0 & 0 & 0 \\ 1 & 0 & d-1 & 0 & 0 \\ 0 & d/w & 0 & d(w-1)/w & 0 \\ 0 & 0 & d-1 & 0 & 1 \\ 0 & 0 & 0 & d & 0 \end{bmatrix}, L_2^* = \begin{bmatrix} 0 & 0 & w(d-1) & 0 & 0 \\ 0 & d-1 & 0 & (d-1)(w-1) & 0 \\ 1 & 0 & w(d-2) & 0 & w-1 \\ 0 & d-1 & 0 & (d-1)(w-1) & 0 \\ 0 & 0 & w(d-1) & 0 & 0 \end{bmatrix},$$

$$L_3^* = \begin{bmatrix} 0 & 0 & 0 & d(w-1) & 0 \\ 0 & 0 & (d-1)(w-1) & 0 & w-1 \\ 0 & \frac{d}{w}(w-1) & 0 & \frac{d}{w}(w-1)^2 & 0 \\ 1 & 0 & (d-1)(w-1) & 0 & w-2 \\ 0 & d & 0 & d(w-2) & 0 \end{bmatrix}, L_4^* = \begin{bmatrix} 0 & 0 & 0 & 0 & w-1 \\ 0 & 0 & 0 & w-1 & 0 \\ 0 & 0 & w-1 & 0 & 0 \\ 0 & 1 & 0 & w-2 & 0 \\ 1 & 0 & 0 & 0 & w-2 \end{bmatrix}.$$

Clearly all Krein conditions are satisfied for $d, w \geq 2$.