Open Systems & Information Dynamics
Vol. 22, No. 1 (2015) 1550001 (10 pages)
DOI:10.1142/S1230161215500018

World Scientific
www.worldscientific.com

An Improvement on the Delsarte-Type LP-Bound with Application to MUBs

M. Matolcsi

Alfréd Rényi Institute of Mathematics
Hungarian Academy of Sciences POB 127 H-1364 Budapest, Hungary
e-mail: matolcsi.mate@renyi.mta.hu

M. Weiner

Budapest University of Technology & Economics (BME)
Department of Mathematical Analysis
Müegyetem rkp. 3–9, H–1111 Budapest, Hungary
e-mail: mweiner@math.bme.hu

(Received: September 25, 2014; Accepted: November 25, 2014; Published: March 18, 2015)

Abstract. The linear programming (LP) bound of Delsarte can be applied to several problems in various branches of mathematics. We describe a general Fourier analytic method to get a slight improvement on this bound. We then apply our method to the problem of mutually unbiased bases (MUBs) to prove that the Fourier family $F(a, b)$ in dimension 6 cannot be extended to a full system of MUBs.

1. Introduction

The linear programming bound of Delsarte was first applied in [6] in coding theory to the following problem: determine the maximal cardinality $A(n, d)$ of binary codewords of length n such that each two of them differ in at least d coordinates. In the past decades the method of Delsarte has been applied to several other problems, most notably to sphere packings [5], and the unit-distance graph of $\mathbb{R}^n$ [7]. In this note we will recall a Fourier analytic formulation of Delsarte's bound [13]. This is not the most general form of the method but it captures most of the applications and is simple enough to require only elementary Fourier analysis.

After the description of the LP-bound we give a general method to get a slight improvement on it. Unfortunately, this improvement is usually very small numerically. However, in ceratin problems the Delsarte bound is already sharp in itself, and *any* improvement on it can lead to non-existence results. This is exactly the situation in the problem of mutually unbiased

bases (MUBs), as described in [13]. We will apply our improved bound to show that the Fourier family $F(a,b)$ of complex Hadamard matrices cannot be extended to a full system of MUBs in dimension 6. This result was previously proven by a massive computer search after a discretization scheme [11]. Our proof here is completely elementary and could also lead to similar results for other families of complex Hadamard matrices.

2. The Delsarte Bound

We recall the Fourier analytic formulation of Delsarte's bound, as described in [13] and [14].

Let G be a compact Abelian group, and let a symmetric subset $A = -A \subset G$, $0 \in A$ be given. We will call A the 'forbidden' set. We would like to determine the maximal cardinality of a set $B = \{b_1, \dots b_m\} \subset G$ such that all differences $b_j - b_k \in A^c \cup \{0\}$ (in other words, all differences avoid the forbidden set A).

We will also need the dual group $\hat{G}$, i.e. the group of multiplicative characters from G to $\mathbb{C}$. In this section we will use the multiplicative notation for the operation of the dual group, i.e. for $\gamma_1, \gamma_2 \in \hat{G}$ and $x \in G$ we define $(\gamma_1\gamma_2)(x) = \gamma_1(x)\gamma_2(x)$. In particular, the unit element of the dual group (i.e. the constant 1 function) will be denoted by $\mathbf{1} \in \hat{G}$.

We will use the normalized Haar measure on G (i.e. the measure of G is 1), and the following definition for the Fourier transform for any function $f : G \to \mathbb{C}$: $\hat{f}(\gamma) = \int_{x \in G} f(x)\gamma(x)dx$.

Let us now recall Delsarte's bound in this formulation [13, 14]. We also recall the proof here because we will need it later.

THEOREM 1 (Delsarte's bound) *Assume we have a witness function $h : G \to \mathbb{R}$ with the following properties: $h(x) \le 0$ for all $x \in A^c$, $\hat{h}(\gamma) \ge 0$ for all $\gamma \in \hat{G}$, the Fourier inversion formula is valid for h (in particular, h can be any finite linear combination of characters). Then for any $B = \{b_1, \dots b_m\} \subset G$ such that $b_j - b_k \in A^c \cup \{0\}$ we have $|B| \le \frac{h(0)}{\hat{h}(1)}$.*

Proof. For any $\gamma \in \hat{G}$ define $\hat{B}(\gamma) = \sum_{j=1}^{m} \gamma(b_j)$, and let us evaluate

$$S \;=\; \sum_{\gamma \in \hat{G}} |\hat{B}(\gamma)|^2 \hat{h}(\gamma)\,. \tag{1}$$

All terms are nonnegative, and the term corresponding to $\gamma = \mathbf{1}$ gives $|\hat{B}(\mathbf{1})|^2\hat{h}(\mathbf{1}) = |B|^2\hat{h}(\mathbf{1})$. Therefore

$$S \;\ge\; |B|^2 \hat{h}(\mathbf{1})\,. \tag{2}$$

On the other hand, $|\hat{B}(\gamma)|^2 = \sum_{j,k} \gamma(b_j - b_k)$, and therefore

$$S \;=\; \sum_{\gamma,j,k} \gamma(b_j - b_k)\hat{h}(\gamma)\,.$$

Summing up for fixed j, k we get (the Fourier inversion formula for h),

$$\sum_{\gamma} \gamma(b_j - b_k)\hat{h}(\gamma) \;=\; h(b_j - b_k)\,,$$

and therefore $S = \sum_{j,k} h(b_j - b_k)$. Notice that $j = k$ happens $|B|$-many times, and all the other terms (when $j \neq k$) are non-positive because $b_j - b_k \in A^c$, and h is required to be non-positive there. Therefore

$$S \;\leq\; h(0)|B|\,. \tag{3}$$

Comparing the two estimates (2), (3) we obtain

$$|B| \;\leq\; \frac{h(0)}{\hat{h}(\mathbf{1})}\,. \tag{4}$$

□

In principle, the best witness function h can be found by linear programming if G is finite. In practice, the cardinality of G needs to be small enough for the LP-code to be executed.

3. Improving the Delsarte Bound

When obtaining the lower bound (2) we have thrown away all non-trivial terms ($\gamma \neq \mathbf{1}$) on the right-hand side of (1). This seems rather wasteful. We will try to make use of the remaining terms in this section.

Assume we have some further restriction on the set B: not only must each $b_j - b_k$ falls into $A^c \cup \{0\}$ but also B must be contained in some prescribed set $C \subset G$.

THEOREM 2 *Let $C \subset G$ be a measurable subset. Assume h is a witness function as in the Delsarte bound: $h : G \to \mathbb{R}$, $h(x) \leq 0$ for all $x \in A^c$, $\hat{h}(\gamma) \geq 0$ for all $\gamma \in \hat{G}$, and the Fourier inversion formula holds for h. Let* Null *denote the set of γ's where $\hat{h}(\gamma) = 0$. Assume furthermore that we have another witness function $K : G \to \mathbb{C}$ with the following properties: $K(x) \geq 1$ for $x \in C$, $\hat{K}(\mathbf{1}) = 0$, and $\hat{K}(\gamma) = 0$ for all $\gamma \in Null$. Then any $B \subset C$ such that $B - B \subset A^c \cup \{0\}$ satisfies*

$$|B| \;\leq\; \frac{h(0)}{\hat{h}(\mathbf{1}) + \left(\sum_{\gamma \notin \mathrm{Null}} \frac{|\hat{K}(\gamma)|^2}{\hat{h}(\gamma)}\right)^{-1}}\,. \tag{5}$$

Proof. We will make use of the non-trivial terms in (1). Namely,

$$\Big(\sum_{\gamma\neq\mathbf{1},\gamma\notin\mathrm{Null}}|\hat{B}(\gamma)|^2\hat{h}(\gamma)\Big)\Big(\sum_{\gamma\neq\mathbf{1},\gamma\notin\mathrm{Null}}\frac{|\hat{K}(\gamma)|^2}{\hat{h}(\gamma)}\Big)$$
$$\geq\ \Big|\sum_{\gamma\neq\mathbf{1},\gamma\notin\mathrm{Null}}\hat{B}(\gamma)\overline{\hat{K}(\gamma)}\Big|^2\ =\ \Big|\sum_{\gamma\in\hat{G}}\hat{B}(\gamma)\overline{\hat{K}(\gamma)}\Big|^2$$
$$=\ \Big|\sum_{x\in G}B(x)\overline{K(x)}\Big|^2\ =\ \Big|\sum_{x\in C}B(x)\overline{K(x)}\Big|^2\ \geq\ |B|^2\,, \tag{6}$$

where we used Cauchy-Schwarz, the assumptions on $\hat{K}(\gamma)$, Parseval, and the assumptions on $B(x)$ and $K(x)$, respectively. Therefore, we get an improved version of (2), namely:

$$S\ \geq\ |B|^2\hat{h}(\mathbf{1})+\frac{|B|^2}{\displaystyle\sum_{\gamma\neq 0,\gamma\notin\mathrm{Null}}\frac{|\hat{K}(\gamma)|^2}{\hat{h}(\gamma)}}\,. \tag{7}$$

Comparing this with (3) yields the desired bound (5). □

We see that Theorem 2 requires a combination of two witness functions $h(x)$ and $K(x)$ (as well as a prescribed set C in which B is assumed to be located). Unfortunately, it is not at all clear how to optimize h and K in actual applications. The best chance to apply (5) successfully arises in situations when the Delsarte bound (4) is already sharp. In such cases the sheer *existence of any* K can lead to non-existence results, as we explain in the next paragraphs. Let us first state a corollary, which describes the usual situation in which Theorem 2 can be used.

COROLLARY 1 *Assume that for a given forbidden set* $0\in A=-A\subset G$ *we already have a witness function* $h(x)$ *as in Theorem 1, testifying that* $|B|\leq\frac{h(0)}{\hat{h}(1)}=m\in\mathbb{Z}$ *for any set* $B\subset G$ *such that* $B-B\subset A^c\cup\{0\}$. *Assume also that a few elements* $b_1,\dots,b_k\in G$ *are given with the property that* $b_i-b_j\in A^c$ *for all* $i\neq j$. *Let* D *denote the set of elements in* G *(different from* $b_1,\dots,b_k$*) such that* $d-b_j\in A^c$ *for all* $j=1,\dots,k$. *Assume furthermore that we have a second witness function* $K(x)$ *such that* $\hat{K}(\mathbf{1})=0$, $\hat{K}(\gamma)=0$ *for all* $\gamma\in Null$, *and* $\sum_{j=1}^k K(b_j)=1$ *while* $K(x)>\frac{-1}{m-k}$ *for all* $x\in D$ *or* $K(x)<\frac{-1}{m-k}$ *for all* $x\in D$. *Then, for any* $B\subset G$ *such that* $b_1,\dots,b_k\in B$ *and* $B-B\subset A^c\cup\{0\}$ *we have that* $|B|\leq m-1$.

Proof. This is a direct consequence of the proof of Theorem 2. Assume by contradiction that $|B|=m$. By the penultimate term of inequality (6)

this can only happen if $\sum_{x\in C} B(x)\overline{K(x)} = 0$ (otherwise, using (6), we could get *some* improvement on the bound $|B| \leq \frac{h(0)}{\hat{h}(\mathbf{1})} = m$). However, by the conditions above we have

$$\sum_{x\in C} B(x)\overline{K(x)} \;=\; 1 + \sum_{b\in B, b\in D} K(b) \neq 0\,,$$

because the sum is larger than zero if $K(x) > \frac{-1}{m-k}$ for all $x \in D$, while it is smaller than zero if $K(x) < \frac{-1}{m-k}$ for all $x \in D$. Therefore, B can contain at most $m-1$ elements. □

4. Application to Mutually Unbiased Bases (MUBs)

We now turn to an elegant application of Corollary 1 to the problem of mutually unbiased bases (MUBs). What makes this application possible is the fact that the Delsarte bound is already sharp in the MUB problem, as explained below (see also [13] for more details, where this idea was introduced).

We will use the formulation of the MUB problem in terms of complex Hadamard matrices. A complex Hadamard matrix H is a complex orthogonal matrix whose entries are of modulus 1. Two such matrices H_1, H_2 are called unbiased if any two columns $\boldsymbol{u} \in H_1, \boldsymbol{w} \in H_2$ satisfy $|\langle \boldsymbol{u}, \boldsymbol{w}\rangle| = \sqrt{n}$. A convenient formulation of the MUB problem is whether there exists a system $H_1, \ldots, H_n$ of pairwise mutually unbiased complex Hadamard matrices (MUHs) in dimension n. The answer is known to be positive if n is a prime-power (se e.g. [1, 9, 12, 17]), while the problem is open for any non-prime-power dimensions.

Assume that $H_1, \ldots, H_r$ is a system of mutually unbiased complex Hadamard matrices. The columns of each H_j are unimodular vectors which can be considered as elements of the group $G = \mathbb{T}^n$, where $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$. The group operation on G is coordinate-wise multiplication, the unit element is the constant 1 vector denoted by $\mathbf{1}$, and the dual group $\hat{G}$ is $\mathbb{Z}^n$ the unit of which is denoted by $\mathbf{0}$.[a] Also, any two distinct column vectors in this system must be either orthogonal or unbiased to each other (depending on whether they belong to the same matrix or not). Therefore, any two distinct columns $\boldsymbol{v}, \boldsymbol{w}$ satisfy

$$\Big|\sum_{j=1}^{n} v_j\overline{w_j}\Big|^2 \;=\; \Big|\sum_{j=1}^{n} \frac{v_j}{w_j}\Big|^2 \;=\; 0 \quad \text{or} \quad n\,.$$

[a] In this particular application it is more convenient to use the multiplication operation on $\mathcal{G}$ and the addition operation on $\hat{\mathcal{G}}$.

In the language of Theorem 1 this means that $\boldsymbol{v}/\boldsymbol{w}$ must fall into the set

$$A^c \;=\; \Big\{\boldsymbol{z}\in\mathbb{T}\,:\,\sum_{j=1}^{n} z_j = 0\Big\}\cup\Big\{\boldsymbol{z}\in\mathbb{T}\,:\,\Big|\sum_{j=1}^{n} z_j\Big|^2 = n\Big\}.$$

Consider now the witness function $h : G \to \mathbb{R}$, $h(\boldsymbol{z}) = |z_1 + \ldots + z_n|^2(|z_1 + \ldots z_n|^2 - n)$. It is fairly easy to check that this function satisfies all the conditions listed in Theorem 1, and $\frac{h(1)}{\hat{h}(\mathbf{0})} = n^2$. This testifies that the total number of column vectors in the matrices H_j cannot be larger than n^2, and hence the number of MUHs cannot be larger than n.

Of course, this bound cannot be improved if n is a prime-power, because a full system of MUBs (or, equivalently, MUHs) actually exists for such n. However, for any given Hadamard matrix H one can try to use Corollary 1 to rule out the possibility that H could be part of a full system of MUHs. In view of the witness function h above, all we need is a suitable function $\boldsymbol{z} \mapsto K(\boldsymbol{z})$ which is a linear combination of terms of the form $z_i z_j \overline{z}_k \overline{z}_l$ with $\{i, j\} \neq \{k, l\}$ (since these are exactly the non-constant terms appearing in h, this will ensure $\hat{K}(\gamma) = 0$ for all $\gamma \in \text{Null}$) and satisfies the bounds given in Corollary 1.

We shall now demonstrate the power of this method by an actual example. In dimension 6, the fact that no Hadamard matrix $F(a, b)$ of the Fourier family can be part of a full system of MUHs was proven by a massive computer search using a discretization scheme in [11]. In particular, there is no way to check that proof by hand. Here we shall give a simple proof of this statement requiring no computer assistance. However, in full generality the question of existence of a complete set of MUBs (or, equivalently, MUHs) in dimension 6 still remains open, despite considerable efforts in recent years [2–4, 11, 15].

THEOREM 3 *In dimension $n = 6$, no complex Hadamard matrix $F(a, b)$ of the Fourier family, or $F^T(a, b)$ of the transposed Fourier family can be extended to a full system of MUHs.*

Proof. It is trivial that any complex Hadamard matrix H can be extended to a full system of MUHs if and only if its conjugate $\overline{H}$, adjoint H^* or transpose H^T can. Therefore we may restrict our attention to the transposed Fourier family $F^T(a, b)$. The usual parametrization of $F^T(a, b)$ is given in [16]. However, it will be more convenient for us to permute rows and columns and work with an equivalent parametrization given by the following column vectors:

$$\begin{bmatrix} \boldsymbol{f}_0 \\ \boldsymbol{f}_0 \end{bmatrix}, \begin{bmatrix} \boldsymbol{f}_0 \\ -\boldsymbol{f}_0 \end{bmatrix}, \begin{bmatrix} \boldsymbol{f}_1 \\ a\boldsymbol{f}_1 \end{bmatrix}, \begin{bmatrix} \boldsymbol{f}_1 \\ -a\boldsymbol{f}_1 \end{bmatrix}, \begin{bmatrix} \boldsymbol{f}_2 \\ b\boldsymbol{f}_2 \end{bmatrix}, \begin{bmatrix} \boldsymbol{f}_2 \\ -b\boldsymbol{f}_2 \end{bmatrix}, \qquad (8)$$

where

$$\left[\begin{array}{ccc} \boldsymbol{f}_0 & \boldsymbol{f}_1 & \boldsymbol{f}_2 \end{array}\right] = \left[\begin{array}{ccc} 1 & 1 & 1 \\ 1 & e^{i\frac{2\pi}{3}} & e^{-i\frac{2\pi}{3}} \\ 1 & e^{-i\frac{2\pi}{3}} & e^{i\frac{2\pi}{3}} \end{array}\right] \tag{9}$$

and $a, b \in \mathbb{T}$ are two complex unit parameters. With a slight abuse of notation we will still denote the matrix formed by the six columns above by $F^T(a,b)$. Also, we will denote the columns in (8) by $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_6$, in accordance with the notation of Corollary 1. Note that the set D appearing in Corollary 1 consists of the vectors $\boldsymbol{z} \in \mathbb{T}^6$ which are unbiased to $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_6$.

Now we define the second witness function $K(\boldsymbol{z})$. For any $\boldsymbol{z} \in \mathbb{T}^6$ written in the form

$$\boldsymbol{z} = \left[\begin{array}{c} \boldsymbol{z}_\uparrow \\ \boldsymbol{z}_\downarrow \end{array}\right], \quad \boldsymbol{z}_\uparrow, \boldsymbol{z}_\downarrow \in \mathbb{T}^3 . \tag{10}$$

Let

$$\begin{aligned} K(\boldsymbol{z}) &= \frac{1}{N}\Big[\left(\langle \boldsymbol{z}_\uparrow, \boldsymbol{f}_0, \rangle \langle \boldsymbol{f}_0, \boldsymbol{z}_\downarrow \rangle\right)^2 + \left(\langle \boldsymbol{z}_\uparrow, \boldsymbol{f}_1, \rangle \langle a\boldsymbol{f}_1, \boldsymbol{z}_\downarrow \rangle\right)^2 \\ &\qquad + \left(\langle \boldsymbol{z}_\uparrow, \boldsymbol{f}_2, \rangle \langle b\boldsymbol{f}_2, \boldsymbol{z}_\downarrow \rangle\right)^2 \Big], \end{aligned} \tag{11}$$

where the normalizing term $N = 6 \cdot (3 \cdot 3)^2 = 486$ is chosen so that the sum taken over the columns $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_6$ of $F^T(a,b)$ is $\sum_{j=1}^{6} K(\boldsymbol{b}_j) = 1$. (This is trivial to check.)

The function K is a linear combination of terms of the form $z_i z_j \overline{z}_k \overline{z}_l$ with $\{i,j\} \neq \{k,l\}$, just as the witness function h. In order to apply Corollary 1 we need to estimate the value of $K(\boldsymbol{z})$ whenever $\boldsymbol{z} \in \mathbb{T}^6$ is an unbiased vector to our Hadamard matrix $F^T(a,b)$. We will show that $K(\boldsymbol{z}) < -\frac{1}{30}$, as required in Corollary 1. It is interesting to note here that we will be able to do this *without* the explicit knowledge of the unbiased vectors $\boldsymbol{z}$.

In what follows, suppose $\boldsymbol{z} = \left(\begin{array}{c} \boldsymbol{z}_\uparrow \\ \boldsymbol{z}_\downarrow \end{array}\right) \in \mathbb{T}^6$ is an unbiased vector to the matrix $F^T(a,b)$. In particular, it is unbiased to the first two columns $\boldsymbol{b}_1, \boldsymbol{b}_2$ listed at (8), which means

$$|\langle \boldsymbol{z}_\uparrow, \boldsymbol{f}_0 \rangle + \langle \boldsymbol{z}_\downarrow, \boldsymbol{f}_0 \rangle|^2 = |\langle \boldsymbol{z}_\uparrow, \boldsymbol{f}_0 \rangle - \langle \boldsymbol{z}_\downarrow, \boldsymbol{f}_0 \rangle|^2 = 6 . \tag{12}$$

This implies that the product $\langle \boldsymbol{z}_\uparrow, \boldsymbol{f}_0 \rangle \overline{\langle \boldsymbol{z}_\downarrow, \boldsymbol{f}_0 \rangle}$ (whose square appears in the definition of $K(\boldsymbol{z})$) is purely imaginary. Thus $|\langle \boldsymbol{z}_\uparrow, \boldsymbol{f}_0 \rangle|^2 + |\langle \boldsymbol{z}_\downarrow, \boldsymbol{f}_0 \rangle|^2 = 6$ and the term

$$\begin{aligned} \left(\langle \boldsymbol{z}_\uparrow, \boldsymbol{f}_0, \rangle \langle \boldsymbol{f}_0, \boldsymbol{z}_\downarrow \rangle\right)^2 &= -|\langle \boldsymbol{z}_\uparrow, \boldsymbol{f}_0 \rangle|^2 \, |\langle \boldsymbol{z}_\downarrow, \boldsymbol{f}_0 \rangle|^2 \\ &= -|\langle \boldsymbol{z}_\uparrow, \boldsymbol{f}_0 \rangle|^2 \left(6 - |\langle \boldsymbol{z}_\uparrow, \boldsymbol{f}_0 \rangle|^2\right). \end{aligned} \tag{13}$$

Similarly, introducing the notation $s_j = |\langle \boldsymbol{z}_\uparrow, \boldsymbol{f}_j\rangle|^2$, $j = 0, 1, 2$, we have that

$$6 - s_j \;=\; |\langle \boldsymbol{z}_\downarrow, \boldsymbol{f}_j\rangle|^2 \tag{14}$$

and obtain

$$K(\boldsymbol{z}) \;=\; -\frac{1}{N}(s_0(6-s_0) + s_1(6-s_1) + s_2(6-s_2))\,. \tag{15}$$

This can be further simplified using that

$$s_0 + s_1 + s_2 \;=\; \sum_{j=0}^{2} |\langle \boldsymbol{z}_\uparrow, f_j\rangle|^2 \;=\; 3\|\boldsymbol{z}_\uparrow\|^2 \;=\; 3\cdot 3 \;=\; 9\,, \tag{16}$$

as $\left\{\frac{1}{\sqrt{3}}\boldsymbol{f}_0, \frac{1}{\sqrt{3}}\boldsymbol{f}_1, \frac{1}{\sqrt{3}}\boldsymbol{f}_2\right\}$ is an orthonormal basis of $\mathbb{C}^3$. Therefore, after simplification,

$$K(\boldsymbol{z}) \;=\; \frac{s_0^2 + s_1^2 + s_2^2 - 54}{486}\,, \tag{17}$$

where $s_0, s_1, s_2 \geq 0$, and $s_0 + s_1 + s_2 = 9$. Note that in general the value of $K(\boldsymbol{z})$ is not necessarily real, but the formula above shows that it is so when evaluated at a vector $\boldsymbol{z}$ which is unbiased to $F^T(a, b)$.

Note that $0 \leq s_0, s_1, s_2 \leq 6$ by (14). Furthermore, we will see that the values of s_j cannot be close to 0 or 6. Indeed, consider the following optimization problem: minimize $|\langle \boldsymbol{f}_0, \boldsymbol{u}\rangle|^2$ over all $\boldsymbol{u} \in \mathbb{T}^3$ subject to the constraints $|\langle \boldsymbol{f}_1, \boldsymbol{u}\rangle|^2 \leq 6$, $|\langle \boldsymbol{f}_2, \boldsymbol{u}\rangle|^2 \leq 6$. We can assume without loss of generality that the first coordinate of $\boldsymbol{u}$ is 1, so that

$$\boldsymbol{u} \;=\; \begin{bmatrix} 1 \\ e^{i\alpha} \\ e^{i\beta} \end{bmatrix}. \tag{18}$$

For the discussion below we introduce the notations $g_j(\alpha, \beta) = |\langle \boldsymbol{f}_j, \boldsymbol{u}\rangle|^2$, $j = 0, 1, 2$. The two-parameter optimization problem above can be solved by standard methods. First, by a trivial compactness argument the minimum is actually attained at some point (α^*, β^*). Second, the point (α^*, β^*) must satisfy one of the following:

(i) the derivative of $g_0(\alpha, \beta)$ is zero at (α^*, β^*);

(ii) both constraints hold with equality, i.e. $g_j(\alpha^*, \beta^*) = 6$ for $j = 1, 2$;

(iii) one constraint holds with equality (say, $g_1(\alpha^*, \beta^*) = 6$), and by the method of Lagrangian multipliers we have $(\partial_\alpha g_0)(\partial_\beta g_1) = (\partial_\beta g_0)(\partial_\alpha g_1)$ at (α^*, β^*).

It is easy to see that (ii) cannot happen (because $g_1(\alpha,\beta)+g_2(\alpha,\beta)\leq 9$), while the cases of (i) are easy to determine and they either do not satisfy the side constraints $g_j(\alpha,\beta)\leq 6$, or do not lead to the actual minimum of the optimization problem. The actual minimum occurs in case (iii), which leads to the following system of equations (after introducing the variables $x_1=\cos\alpha, x_2=\cos\beta, y_1=\sin\alpha, y_2=\sin\beta$):

$$\begin{aligned}
&-x_1-x_2-x_1x_2+\sqrt{3}y_1-\sqrt{3}x_2y_1-\sqrt{3}y_2+\sqrt{3}x_1y_2-y_1y_2-3 \;=\; 0\,,\\
&2\sqrt{3}x_2y_1-4\sqrt{3}x_1x_2y_1+2\sqrt{3}x_2^2y_1+2\sqrt{3}x_1y_2+2\sqrt{3}x_1^2y_2\\
&\quad -4\sqrt{3}x_1x_2y_2-2\sqrt{3}y_1^2y_2-2\sqrt{3}y_1y_2^2 \;=\; 0\,,\\
&x_1^2+y_1^2-1 \;=\; 0\,,\\
&x_2^2+y_2^2-1 \;=\; 0\,.
\end{aligned}$$

This system can be solved exactly (by hand if necessary, but more conveniently with computer algebra), and leads to the lower bound

$$g_0(\alpha,\beta)\geq c \;=\; \frac{3}{2}-\frac{3}{2}\sqrt{16\sqrt{6}-39}\,,$$

showing that $s_0\geq c>0.843$. Consequently, we also obtain $s_0\leq 6-c$, because $6-s_0=|\langle \boldsymbol{z}_\downarrow,\boldsymbol{f}_0\rangle|^2$ must satisfy the same optimization problem. The same argument applies to s_1 and s_2, giving the bounds $c\leq s_0,s_1,s_2\leq 6-c$. Together with the fact that $s_0+s_1+s_2=9$ this implies $s_0^2+s_1^2+s_2^2\leq c^2+(6-c)^2+3^2<37$. Hence

$$K(\boldsymbol{z}) \;=\; \frac{s_0^2+s_1^2+s_2^2-54}{486} \;<\; -\frac{17}{486} \;<\; -\frac{1}{30}\,,$$

and Corollary 1 applies. □

We remark that Corollary 1 could have further similar applications in the future. For example, it is natural to try to prove in a similar manner that in dimension 6 the matrices $D(c)$ of the Dita-family cannot be extended to a full system of MUHs. The method could also be applied to the Fourier matrix F_n for any composite n, in which case we conjecture that F_n cannot be extended to a full set of MUHs (such a statement is currently only known in dimension 6, first settled by Grassl [8]). More generally, in any problem where Delsarte's method gives an upper bound, Theorem 2 might lead to an improvement if a suitable second witness function K can be found.

Finally, we remark that Corollary 1 could be applied together with the discretization scheme described in [10]. A witness function K may exist even if the entries of the first Hadamard matrix H_1 are only known to some precision. In principle, this can lead to a major improvement of the running time of the discretization method.

Acknowledgements

M. M. was supported bt OTKA grant No. 109789 and by ERC-AdG 321104. M. W. was supported by OTKA grant No. 104206 and by the "Bolyai János" Research Scholarship of the Hungarian Academy of Sciences".

The authors thank I. Z. Ruzsa for helpful discussions on the subject and for an alternative solution of the optimization problem presented at the end of the proof of Theorem 3.

Bibliography

[1] S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury, and F. Vatan, Algorithmica **34**, 512 (2002).

[2] I. Bengtsson, W. Bruzda, Å. Ericsson, J.-A. Larsson, W. Tadej, and K. Życzkowski, J. Math. Phys. **48**, 052106 (2007).

[3] S. Brierley and S. Weigert, Phys. Rev. A **78**, 042312 (2008).

[4] S. Brierley and S. Weigert, Phys. Rev. A **79**, 052316 (2009).

[5] H. Cohn and N. Elkies, Ann. Math. **157**, 689 (2003).

[6] P. Delsarte, Philips Res. Rep. **27**, 272 (1972).

[7] F. M. de Oliveira Filho and F. Vallentin, J. Eur. Math. Soc. **12**, 1417 (2010).

[8] M. Grassl, *On SIC-POVMs and MUBs in Dimension 6*, in: Proceedings of ERATO Conference on Quantum Information Science (2004), pp. 60–61.

[9] I. D. Ivanovic, J. Phys. A **14**, 3241 (1981).

[10] P. Jaming, M. Matolcsi, and P. Móra, Cryptography and Communications **2**, 211 (2010).

[11] P. Jaming, M. Matolcsi, P. Móra, F. Szöllősi, and M. Weiner, J. Phys. A: Math. Theor. **42**, 245305 (2009).

[12] A. Klappenecker and M. Rötteler, *Constructions of Mutually Unbiased Bases. Finite fields and applications*, Lecture Notes in Comput. Sci. **2948**, Springer, Berlin, 2004, pp. 137–144.

[13] M. Matolcsi, Studia Sci. Math. Hung. **49**, 482 (2012).

[14] M. Matolcsi and I. Z. Ruzsa, J. Fourier Anal. Appl. **20**, 17 (2014).

[15] P. Raynal, X. Lü, and B.-G. Englert, Phys. Rev. A **83**, 062303 (2011).

[16] W. Tadej and K. Życzkowski. Open Sys. Information Dyn. **13**, 133 (2006).

[17] W. K. Wootters and B. D. Fields, Ann. Phys. **191**, 363 (1989).