

On orthogonal systems of matrix algebras

Mihály Weiner¹

*University of Rome “Tor Vergata”, Department of Mathematics
via della Ricerca Scientifica 1, 00133 Rome, Italy
(on leave from: Alfréd Rényi Institute of Mathematics
H-1364 Budapest, POB 127, Hungary)*

Abstract

In this work it is shown that certain interesting types of orthogonal system of subalgebras (whose existence cannot be ruled out by the trivial necessary conditions) cannot exist. In particular, it is proved that there is no orthogonal decomposition of $M_n(\mathbb{C}) \otimes M_n(\mathbb{C}) \cong M_{n^2}(\mathbb{C})$ into a number of maximal abelian subalgebras and factors isomorphic to $M_n(\mathbb{C})$ in which the number of factors would be 1 or 3.

In addition, some new tools are introduced, too: for example, a quantity $c(\mathcal{A}, \mathcal{B})$, which measures “how close” the subalgebras $\mathcal{A}, \mathcal{B} \subset M_n(\mathbb{C})$ are to being orthogonal. It is shown that in the main cases of interest, $c(\mathcal{A}', \mathcal{B}')$ — where \mathcal{A}' and \mathcal{B}' are the commutants of \mathcal{A} and \mathcal{B} , respectively — can be determined by $c(\mathcal{A}, \mathcal{B})$ and the dimensions of \mathcal{A} and \mathcal{B} . The corresponding formula is used to find some further obstructions regarding orthogonal systems.

Keywords: orthogonal (or: complementary) subalgebras
2000 MSC: 15A30, 47L05

1. Introduction

Matrix-algebraic questions have often their roots in quantum information theory. Mutually unbiased bases (MUB) are considered and investigated because of their relation for example to quantum state tomography [15] or quantum cryptography [3].

A collection of MUB can be viewed as a particular example of an orthogonal system of subalgebras of $M_n(\mathbb{C})$ (in this work by *subalgebra* we shall always mean a *-subalgebra containing $\mathbb{1} \in M_n(\mathbb{C})$; for definition and details on orthogonality between subalgebras see the next section). In algebraic terms, it is an orthogonal system of *maximal abelian* subalgebras (MASAs).

Recently research has began in the non-commutative direction [10, 11, 9, 7, 12], too. (Note that in some of these articles instead of “orthogonal” the term “quasi-orthogonal” or “complementary” is used.) Indeed, it should not be the commutativity of subalgebras

Email address: mweiner@renyi.hu (Mihály Weiner)

¹Supported in part by ... and by the ERC Advanced Grant 227458 OACFT “Operator Algebras and Conformal Field Theory”.

Preprint submitted to Elsevier

March 5, 2010

deciding whether something deserves to be studied or not. From the point of view of quantum physics, the interesting orthogonal systems and decompositions are those that contain factors and MASAs only. (Factors are related to subsystems and MASAs are related to maximal precision measurements.)

An example for a quantum physics motivated orthogonal system which is composed of both abelian and non-abelian algebras is the collection of following 3 subalgebras of $M_2(\mathbb{C}) \otimes M_2(\mathbb{C}) \equiv M_4(\mathbb{C})$ (i.e. the algebra of 2 quantum bits): $M_2(\mathbb{C}) \otimes \mathbb{1}$ (the algebra associated to the first qbit), $\mathbb{1} \otimes M_2(\mathbb{C})$ (the algebra associated to the second qbit), and the maximal abelian subalgebra associated to the so-called *Bell-basis* (which plays an important role e.g. in the protocol of *dense-coding*).

Existential and constructional questions are already difficult in the abelian case. We know many things when the dimension is a power of a prime [5, 4], but for example it is still a question, whether in 6 dimensions there exists a collection of 7 MUB or not [1, 6].

Little is known when not all subalgebras are assumed to be maximal abelian. What are the existing constructions and established obstructions (that is, reasons preventing the existence of certain such systems)? Of course there are some trivial necessary conditions (that will be discussed later). Considering systems containing not only factors and MASAs, it is easy to see, that in general these conditions, alone, cannot be also sufficient (see the example given in section 2.3). However, up to the knowledge of the author, previous to this work, nontrivial obstructions regarding “interesting” systems were only found in very small dimensions (namely in dimension 4, see [11, 9, 12]), using — in part — some rather explicit calculations. Moreover, existing constructions such as the ones in [9, 7] are usually carried out in prime-power dimensions, only. Thus there is a wide gap between constructions and obstructions where “anything could happen”.

The aim of this work is to shorten this gap. In particular, we shall exclude the existence of some interesting systems (and moreover, we shall do so not only in some low dimensions).

This paper is organized as follows. First, — partly for reasons of self-containment, partly for fixing notations — a quick overview (including a presentation of the known results) is given about orthogonal subalgebras and orthogonal decompositions. Though it is well-known to experts, certain parts — at least, up to the knowledge of the author — have never been collected together. In particular, 3 conditions will be singled out and listed as “trivial necessary conditions” of existence for a system.

Then in section 3 we consider decompositions of $M_n(\mathbb{C}) \otimes M_n(\mathbb{C}) = M_{n^2}(\mathbb{C})$. The tensorial product $M_n(\mathbb{C}) \otimes M_n(\mathbb{C}) \equiv M_{n^2}(\mathbb{C})$ appears in quantum physics when one deals with a bipartite system composed of two equivalent parts. Of course $M_{n^2}(\mathbb{C})$ has many subfactors isomorphic to $M_n(\mathbb{C})$ — in physics such a subfactor may stand for a subsystem; for example $M_n(\mathbb{C}) \otimes \mathbb{1}$ stands for the first part of the bipartite system. It seems therefore a natural question to investigate orthogonal decompositions of $M_{n^2}(\mathbb{C})$ into subfactors isomorphic to $M_n(\mathbb{C})$ and a number of MASAs. (As was mentioned, MASAs are related to maximal precision measurements.) We shall show that there is no such decomposition in which there would be only 1 factor (with the other algebras being maximal abelian) and neither there are decompositions with 3 factors. (Note that with 2 factors there are decompositions, see [12, Theorem 6], for example.) As far as the author knows, this is the first example² for excluding the existence of some “interesting” orthogonal systems

²In reality — though in a somewhat implicit manner — another work [14] of the present author

(whose existence cannot be ruled out by the trivial necessary conditions) in an infinite sequence of higher and higher dimensions.

We shall deal with these cases using a recent result [8], by which if we replace each subalgebra in such a decomposition with its commutant, we again get an orthogonal decomposition. However, this is something rather particular: in general, the commutants of two orthogonal subalgebras are not orthogonal anymore. To study the relation of the commutants, in section 4 for two subalgebras $\mathcal{A}, \mathcal{B} \subset M_n(\mathbb{C})$ we shall take the corresponding trace-preserving expectations $E_{\mathcal{A}}, E_{\mathcal{B}}$ and consider the quantity

$$c(\mathcal{A}, \mathcal{B}) := \text{Tr}(E_{\mathcal{A}}E_{\mathcal{B}}) \quad (1)$$

where $E_{\mathcal{A}}E_{\mathcal{B}}$ is viewed as an $M_n(\mathbb{C}) \rightarrow M_n(\mathbb{C})$ linear map (and hence its trace is well-defined). Then $c(\mathcal{A}, \mathcal{B}) \geq 1$ and equality holds if and only if \mathcal{A} and \mathcal{B} are orthogonal. Thus $c(\mathcal{A}, \mathcal{B})$ measures how much \mathcal{A} and \mathcal{B} are (or: how much they are *not*) orthogonal.

Note that a similar quantity has been introduced and studied [13] in the context of von Neumann algebras “measuring” the relative positions of subfactors of a type II_1 factor \mathcal{M} . In that case one considers the orthogonal projections $E_{\mathcal{A}}, E_{\mathcal{B}}$ onto the closed subspaces of $\mathcal{L}^2(\mathcal{M}, \tau)$ determined by the subfactors \mathcal{A} and \mathcal{B} in question. However, in contrast to our case, instead of a simple trace — with which we have no problems as we work in a finite dimensional space instead of the infinite dimensional space $\mathcal{L}^2(\mathcal{M}, \tau)$ — there one uses the spectral data of $E_{\mathcal{A}}E_{\mathcal{B}}E_{\mathcal{A}}$.

Concerning our quantity, we shall prove that if \mathcal{A} and \mathcal{B} satisfy a certain homogeneity condition (which is always satisfied, if they are factors or maximal abelian subalgebras) then

$$c(\mathcal{A}', \mathcal{B}') = \frac{n^2}{\dim(\mathcal{A})\dim(\mathcal{B})}c(\mathcal{A}, \mathcal{B}). \quad (2)$$

Finally, in the last section we shall show in some concrete examples how the derived formula can be used to generalize our earlier arguments and thus to exclude the existence of some further orthogonal systems. In some sense our examples will fall “close” to the cases dealt with in section 3. However, in contrast to those cases, here the commutants will not remain (exactly) orthogonal; so instead of “exact” statements we shall rely on our quantitative formula.

2. Preliminaries

2.1. Orthogonality between subalgebras

There is a natural scalar product on $M_n(\mathbb{C})$ (the so-called *Hilbert-Schmidt* scalar product) defined by the formula

$$\langle A, B \rangle = \text{Tr}(A^*B) \quad (A, B \in M_n(\mathbb{C})). \quad (3)$$

Thus if $\mathcal{A} \subset M_n(\mathbb{C})$ is a linear subspace, it is meaningful to consider the ortho-projection $E_{\mathcal{A}}$ onto \mathcal{A} . When \mathcal{A} is actually a $*$ -subalgebra containing $\mathbb{1} \in M_n(\mathbb{C})$ (or in short:

has already dealt with the case of a single factor; see the remark after corollary 3.2. However, the non-existence of this kind of decomposition was never stated there — that paper had a different aim.

a subalgebra), $E_{\mathcal{A}}$ coincides with the so-called *trace-preserving conditional expectation* onto \mathcal{A} .

Two subalgebras $\mathcal{A}, \mathcal{B} \subset M_n(\mathbb{C})$, as linear subspaces, cannot be orthogonal, since $\mathcal{A} \cap \mathcal{B} \neq \{0\}$ as $\mathbb{1} \in \mathcal{A} \cap \mathcal{B}$. At most, the subspaces $\mathcal{A} \cap \{\mathbb{1}\}^\perp$ and $\mathcal{B} \cap \{\mathbb{1}\}^\perp$ can be orthogonal, in which case we say that \mathcal{A} and \mathcal{B} are **orthogonal subalgebras**.

Note also that $A \in M_n(\mathbb{C})$ is orthogonal to $\mathbb{1}$ if and only if $\text{Tr}(A) = 0$ and so the subspace $\mathcal{A} \cap \{\mathbb{1}\}^\perp$ is simply the “traceless part” of \mathcal{A} . In other words, \mathcal{A} and \mathcal{B} are orthogonal subalgebras if and only if their traceless parts are orthogonal (as linear subspaces).

For an $X \in M_n(\mathbb{C})$ denote its traceless part by X_0 ; that is,

$$X_0 = X - \tau(X)\mathbb{1} \quad (4)$$

where $\tau = \frac{1}{n}\text{Tr}$ is the **normalized trace**. (Note that the normalization is done in such a way that $\tau(\mathbb{1}) = 1$.) Then the traceless parts A_0, B_0 of $A, B \in M_n(\mathbb{C})$ are orthogonal if and only if

$$0 = \tau(A_0^* B_0) = \tau((A^* - \overline{\tau(A)}\mathbb{1})(B - \tau(B)\mathbb{1})) = \tau(A^* B) - \overline{\tau(A)}\tau(B), \quad (5)$$

that is, if and only if $\tau(A^* B) = \tau(A^*)\tau(B)$. So, since if A is an element of the subalgebra, then so is A^* , we have that two subalgebras \mathcal{A}, \mathcal{B} of $M_n(\mathbb{C})$ are orthogonal if and only if for all $A \in \mathcal{A}$ and $B \in \mathcal{B}$,

$$\tau(AB) = \tau(A)\tau(B). \quad (6)$$

2.2. Factors, abelian subalgebras and MUB

For any subalgebra $\mathcal{A} \subset M_n(\mathbb{C})$ one can consider its **commutant**

$$\mathcal{A}' \equiv \{X \in M_n(\mathbb{C}) \mid \forall A \in \mathcal{A} : AX - XA = 0\} \quad (7)$$

which is again a subalgebra. One has that the **second commutant** $\mathcal{A}'' \equiv (\mathcal{A}')' = \mathcal{A}$. A subalgebra \mathcal{A} whose center

$$\mathcal{Z}(\mathcal{A}) = \mathcal{A} \cap \mathcal{A}' \quad (8)$$

is trivial (i.e. such that $\mathcal{Z}(\mathcal{A}) = \mathbb{C}\mathbb{1}$) is called a **factor**. If $\mathcal{A} \subset M_n(\mathbb{C})$ is a factor, then there exist j, k natural numbers such that $jk = n$, and that up to unitary equivalence, \mathcal{A} is of the form

$$\mathcal{A} = M_j(\mathbb{C}) \otimes \mathbb{1} \equiv \{A \otimes \mathbb{1} \mid A \in M_j(\mathbb{C})\} \subset M_j(\mathbb{C}) \otimes M_k(\mathbb{C}) \equiv M_{jk}(\mathbb{C}). \quad (9)$$

Then $\mathcal{A}' = \mathbb{1} \otimes M_k(\mathbb{C})$ and so if \mathcal{A} is factor, then \mathcal{A} and \mathcal{A}' are always orthogonal; this follows easily from the trace-criterion (6) and the fact that

$$\text{Tr}(A \otimes B) = \text{Tr}(A)\text{Tr}(B) \quad (10)$$

for all $A \in M_j(\mathbb{C})$ and $B \in M_k(\mathbb{C})$.

Another example of orthogonal subalgebras comes from mutually unbiased bases. Two orthonormal bases $\mathcal{E} = (\mathbf{e}_1, \dots, \mathbf{e}_n)$ and $\mathcal{F} = (\mathbf{f}_1, \dots, \mathbf{f}_n)$ in \mathbb{C}^n such that

$$|\langle \mathbf{e}_k, \mathbf{f}_j \rangle| = \text{constant} = \frac{1}{\sqrt{n}} \quad (11)$$

for all $k, j = 1, \dots, n$, are said to be **mutually unbiased**, or in short, \mathcal{E} and \mathcal{F} is a pair of MUB.

Clearly, unbiasedness does not depend on the order of vectors in \mathcal{E} and \mathcal{F} , nor on their “phase factors”. (That is, the MUB property is not disturbed by replacing a basis vector \mathbf{v} by $\lambda\mathbf{v}$, where $\lambda \in \mathbb{C}$, $|\lambda| = 1$.) For this reason, one often associates subalgebras to these bases (which do not depend on the order of vectors and their phases) and then works with them rather than with the actual bases.

Let us see how can we assign a subalgebra to an orthonormed basis \mathcal{E} . For a vector $\mathbf{v} \neq 0$, denote the ortho-projection onto the one-dimensional subspace $\mathbb{C}\mathbf{v}$ by $P_{\mathbf{v}}$. Then the linear subspace of $M_n(\mathbb{C})$

$$\mathcal{A}_{\mathcal{E}} \equiv \text{Span}\{P_{\mathbf{e}_j} \mid j = 1, \dots, n\} \quad (12)$$

is actually a subalgebra. Infact it is a **maximal abelian subalgebra** (in short: a MASA), and every MASA of $M_n(\mathbb{C})$ is of this form.

Elementary calculation shows that if \mathbf{v}, \mathbf{w} are vectors of unit length then

$$\text{Tr}(P_{\mathbf{v}}P_{\mathbf{w}}) = |\langle \mathbf{v}, \mathbf{w} \rangle|^2. \quad (13)$$

Hence by an application of the trace-criterion (6) one has that \mathcal{E} and \mathcal{F} is a pair of MUB if and only if the associated maximal abelian subalgebras $\mathcal{A}_{\mathcal{E}}$ and $\mathcal{A}_{\mathcal{F}}$ are orthogonal.

A famous question concerning MUB is: how many orthonormed bases can be given in n dimensions in such a way that any two of the given collection is a MUB? There is a simple bound concerning this maximum number — which we shall denote by $N(n)$ — namely, that if $n > 1$ then $N(n) \leq n + 1$. Let us recall now how this bound can be obtained by a use of the above introduced subalgebras.

The traceless part of $M_n(\mathbb{C})$ is $n^2 - 1$ dimensional, whereas the traceless part of a maximal abelian subalgebra of $M_n(\mathbb{C})$ is $n - 1$ dimensional. If $n > 1$, then at most

$$\frac{n^2 - 1}{n - 1} = n + 1 \quad (14)$$

$n - 1$ -dimensional orthogonal subspaces can be fitted in an $n^2 - 1$ dimensional space, implying that for $n > 1$ we have $N(n) \leq n + 1$.

It is known by construction [5, 4] that if n is a power of a prime, then $N(n) = n + 1$. However, apart from $n = p^k$ (where p is a prime), there is no other dimension $n > 1$ in which the value of $N(n)$ would be known. In particular, already the value of $N(6)$ is an open question with a long literature on its own; see e.g. [1, 6]. All we know is that $3 \leq N(6) \leq 7$ with numerical evidence [2] indicating that $N(6)$ is actually 3.

2.3. Orthogonal systems and decompositions

A collection of pairwise orthogonal subalgebras $\mathcal{A}_1, \mathcal{A}_2, \dots$ of $M_n(\mathbb{C})$ is said to form an **orthogonal system** in $M_n(\mathbb{C})$. If in addition the given subalgebras linearly span the full space $M_n(\mathbb{C})$, we say that the collection is an **orthogonal decomposition** of $M_n(\mathbb{C})$.

Suppose we are looking for an orthogonal system in $M_n(\mathbb{C})$ (or orthogonal *decomposition* of $M_n(\mathbb{C})$) $\mathcal{A}_1, \dots, \mathcal{A}_k$ such that \mathcal{A}_j is isomorphic to \mathcal{B}_j ($j = 1, \dots, k$), where $\mathcal{B}_1, \dots, \mathcal{B}_k$ are given matrix algebras. For example, we may look for an orthogonal system

in which each algebra is a MASA — as is the case when we want to find a collection of MUB — or, motivated by the study of “quantum bits” we may look for a system consisting of subalgebras all isomorphic to $M_2(\mathbb{C})$ — as is investigated in [11, 9].

What can we say about the existence of a specific system? Some necessary conditions are easy to establish. In particular, the following three will be referred as the “trivial necessary conditions” for the existence of a specific orthogonal system in $M_n(\mathbb{C})$ (or: orthogonal decomposition of $M_n(\mathbb{C})$).

- (1) $M_n(\mathbb{C})$ must contain *some* subalgebras $\mathcal{A}_1, \dots, \mathcal{A}_k$ isomorphic to the given algebras $\mathcal{B}_1, \dots, \mathcal{B}_k$, respectively,
- (2) the product $\dim(\mathcal{B}_i)\dim(\mathcal{B}_j) \leq n^2$ for all $1 \leq i < j \leq k$,
- (3) $\sum_{j=1}^k (\dim(\mathcal{B}_j) - 1) \leq n^2 - 1$ and a corresponding orthogonal system is an orthogonal *decomposition* if and only if in the above formula equality holds.

The first condition does not require too much explanation. Nevertheless, it rules out the existence of various orthogonal systems. For example, can we have an orthogonal system in $M_5(\mathbb{C})$ consisting of 3 subalgebras each of which is isomorphic to $M_2(\mathbb{C})$? Clearly no: simply, $M_5(\mathbb{C})$ does not contain any subalgebra that would be isomorphic to $M_2(\mathbb{C})$ since 2 does not divide 5.

The second condition, at first sight, is perhaps less evident; let us see now why is it necessary. Suppose \mathcal{A} and \mathcal{B} are orthogonal subalgebras of $M_n(\mathbb{C})$. Let $A_1, \dots, A_{d_{\mathcal{A}}}$ and $B_1, \dots, B_{d_{\mathcal{B}}}$ be orthonormed bases in \mathcal{A} and \mathcal{B} (with $d_{\mathcal{A}}, d_{\mathcal{B}}$ standing for the dimensions of \mathcal{A} and \mathcal{B}), respectively. Then, by definition of the (Hilbert-Schmidt) scalar product and by the trace property (6) we have that

$$\begin{aligned} n\langle A_i B_j, A_{i'} B_{j'} \rangle &= n^2 \tau((A_i B_j)^* A_{i'} B_{j'}) = n^2 \tau(A_i^* A_{i'} B_j B_j^*) = n^2 \tau(A_i^* A_{i'}) \tau(B_j B_j^*) \\ &= n^2 \tau(A_i^* A_{i'}) \tau(B_j^* B_{j'}) = \langle A_i, A_{i'} \rangle \langle B_j, B_{j'} \rangle, \end{aligned} \quad (15)$$

showing that $\sqrt{n}A_i B_j$ ($i = 1, \dots, d_{\mathcal{A}}; j = 1, \dots, d_{\mathcal{B}}$) is an orthonormed system in $M_n(\mathbb{C})$. Hence the number of members in this system must be less or equal than the dimension of the full space $M_n(\mathbb{C})$; that is, $d_{\mathcal{A}}d_{\mathcal{B}} \leq n^2$.

The third condition is necessary simply because if $\mathcal{A}_1, \dots, \mathcal{A}_k$ are orthogonal, then their traceless parts are orthogonal subspaces in the traceless part of $M_n(\mathbb{C})$. We argue exactly like we did at discussing the maximum number of MUB (which, for us, is just a particular case): we have k orthogonal subspaces of dimensions $\dim(\mathcal{A}_j) - 1$ ($j = 1, \dots, k$) in a $\dim(M_n(\mathbb{C})) - 1 = n^2 - 1$ dimensional space, implying the claimed inequality. Moreover, the subspaces span the full space (i.e. we have an orthogonal *decomposition*) if and only if the dimensions add up exactly to $n^2 - 1$.

So these conditions are necessary for existence. But are they also sufficient? The answer, in general, is not.

Example. Can we find an orthogonal system in $M_6(\mathbb{C})$ consisting of an abelian subalgebra \mathcal{A} of dimension 4 and a factor \mathcal{B} isomorphic to $M_3(\mathbb{C})$? The answer is: not. Indeed, assume by contradiction that \mathcal{A}, \mathcal{B} is such a pair. Let P_1, \dots, P_4 be the minimal projections of \mathcal{A} . Since we are in a 6-dimensional space, at least one of them is a projection onto a one-dimensional space. So suppose P_1 is the orthogonal projection onto the

subspace generated by the unit-length vector x . Then by the trace property (implied by orthogonality)

$$\langle x, Bx \rangle = \text{Tr}(P_1 B) = \frac{1}{6} \text{Tr}(P_1) \text{Tr}(B) = \frac{1}{6} \text{Tr}(B) \quad (16)$$

for all $B \in \mathcal{B}$. This shows that the linear map $B \mapsto Bx$ is injective on \mathcal{B} . Indeed, if $Bx = 0$ then $0 = \|Bx\|^2 = \langle Bx, Bx \rangle = \langle x, B^* Bx \rangle$, which by the above equation would mean that $\text{Tr}(B^* B) = 0$, implying that $B = 0$. However, this is a contradiction, as the dimension of \mathcal{B} is bigger than the dimension of the full space: $3^2 = 9 > 6$. Yet the listed necessary conditions would allow the existence of such a system. Indeed, the first condition is trivially satisfied, the second is satisfied as $\dim(\mathcal{A})\dim(\mathcal{B}) = 4 * 3^2 \leq 6^2$, whereas the third is satisfied since $(\dim(A) - 1) + (\dim(\mathcal{B}) - 1) = 3 + 8 \leq 6^2 - 1$.

Since our motivation is quantum information theory, we are mainly interested by orthogonal systems formed by maximal abelian subalgebras and factors. For such systems it is somewhat more difficult to show that the trivial necessary conditions are not also sufficient. Let us continue now by discussing the known examples of “interesting” systems.

The trivial necessary conditions allow the existence of an orthogonal system in $M_n(\mathbb{C})$ composed of k MASAs as long as $k \leq n+1$ (see the third condition). Moreover, an orthogonal system composed of exactly $n+1$ MASAs would give an orthogonal decomposition of $M_n(\mathbb{C})$. As was mentioned, the existence of such systems is a popular research theme (though the problem is usually considered rather in terms of MUB than MASA), and little is known when n is not a power of a prime.

Another, more recent problem is to find a system of orthogonal subalgebras in $M_{2^k}(\mathbb{C})$ in which all subalgebras are isomorphic to $M_2(\mathbb{C})$. Here there is a more direct motivation: a quantum bit, in some sense, is a subalgebra isomorphic to $M_2(\mathbb{C})$, whereas the full algebra $M_{2^k}(\mathbb{C}) \simeq M_2(\mathbb{C}) \otimes M_2(\mathbb{C}) \otimes \dots$ is used in the description of the register of a quantum computer containing k quantum bits.

In this case too, the first two trivial necessary conditions are automatically satisfied, whereas the third one says that such a system can consists of at most $(2^{2^k} - 1)/3 =: S(k)$ subalgebras. Again, exactly $S(k)$ such subalgebras would give an orthogonal decomposition. (It is easy to see that $S(k)$ is an integer.) In [9] $S(k) - 1$ such subalgebras are presented by a construction using induction on k . For $k > 2$ it is not known whether the construction is *optimal*; that is, whether the upper bound $S(k)$ could be realized or not. However, it is proved [11] that for $k = 2$ — i.e. in $M_4(\mathbb{C})$ — the construction is indeed optimal: there is no orthogonal system consisting of $S(2) = 5$ subalgebras isomorphic to $M_2(\mathbb{C})$. This shows that the listed trivial necessary conditions, even in the special case of our interest, are not always sufficient, too. (As far as the author of this work knows, this was the first example of an “interesting” orthogonal system satisfying the trivial conditions, whose existence was *disproved*.)

The case of $M_4(\mathbb{C})$ has received quite a bit of attention [11, 9, 12]. Indeed, this is the smallest dimension in which — at least from our point of view — something nontrivial is happening. As we are interested by factors and MASAs, let us consider an orthogonal decomposition of $M_4(\mathbb{C})$ consisting of a collection of MASAs (so subalgebras isomorphic to \mathbb{C}^4) and proper subfactors (so subalgebras isomorphic to $M_2(\mathbb{C})$). Again, the first two trivial necessary conditions are automatically satisfied, whereas dimension counting (third condition) says that for such a decomposition we need 5 subalgebras. The trivial necessary conditions do not give anything more. However, in [12] it was proved that such

a decomposition exists if and only if an even number of these 5 subalgebras are factors. So for example one can construct such a decomposition with 2 factors and 3 MASAs, but not with 3 factors and 2 MASAs. This again shows that the trivial necessary conditions are not always sufficient, too.

The problem with orthogonal copies of $M_2(\mathbb{C})$ in $M_{2^k}(\mathbb{C})$ can be also generalized in the sense that one may look for orthogonal copies of $M_n(\mathbb{C})$ in $M_{n^k}(\mathbb{C})$. As was mentioned, we shall show in this work the non-existence of an orthogonal decomposition of $M_{n^2}(\mathbb{C})$ into a number of maximal abelian subalgebras and factors isomorphic to $M_n(\mathbb{C})$ in which the number of factors would be 1 or 3. Note that it is a (partial) generalization of the above mentioned previous result. In the opinion of the author, this suggests that perhaps the number of factors in such a decomposition can never be odd.

If n is a power of a non-even prime, then $M_{n^k}(\mathbb{C})$ admits [7] an orthogonal decomposition consisting factors isomorphic to $M_n(\mathbb{C})$, only. (As was mentioned, when $k = 2$, there is *no* such a decomposition for $n = 2$. Note however that one needs $n^2 + 1$ factors for such a decomposition; i.e. an even number of factors when n is odd. Thus the mentioned result gives further support to our conjecture.) The proof of this fact is constructional and relies on the existence of finite fields and in some sense it is carried out in a similar manner to the construction of $n + 1$ MUB in dimension $n = p^\alpha$ (where $p > 2$ is a prime and α is a natural number).

3. Decompositions of $M_n(\mathbb{C}) \otimes M_n(\mathbb{C}) \equiv M_{n^2}(\mathbb{C})$

We shall now consider orthogonal decompositions of $M_{n^2}(\mathbb{C})$ into subfactors isomorphic to $M_n(\mathbb{C})$ and a number of MASAs. Such decompositions of $M_2(\mathbb{C}) \otimes M_2(\mathbb{C}) \equiv M_4(\mathbb{C})$ are well studied in [12]. However, there the achieved results rely on explicit calculations carried out in 4 dimensions. What can we do in higher dimensions? Note that the trivial necessary conditions do not rule out the existence of a decomposition of the mentioned type; all they say that such decompositions must consists of

$$\frac{n^4 - 1}{n^2 - 1} = n^2 + 1 \tag{17}$$

subalgebras (since both a maximal abelian subalgebra of $M_{n^2}(\mathbb{C})$ and the factor $M_n(\mathbb{C})$ is n^2 -dimensional).

Decomposition into MASAs is of course interesting, but it is known to be a hard question which is usually studied in terms of MUB and it is out of the scope of this article. Actually, there is a certain mathematical (or more precisely: operator algebraic) advantage of having not only MASAs: it is often helpful to consider the commutant of a subalgebra. (The commutant of a MASA is itself, so it does not give anything “new”.) Infact, the result in [11] concerning orthogonal copies of $M_2(\mathbb{C})$ in $M_4(\mathbb{C})$ is achieved exactly by considering commutants.

In [8] an important result is deduced about the orthogonality of commutants. We shall now recall this result (stating it in a slightly different form).

Lemma 3.1. *Let \mathcal{A}_1 and \mathcal{A}_2 be orthogonal subalgebras of $M_n(\mathbb{C})$. Then the commutants \mathcal{A}'_1 and \mathcal{A}'_2 are orthogonal if and only if $\dim(\mathcal{A}_1) \dim(\mathcal{A}_2) = n^2$.*

Proof. The observation established by calculation (15) shows that the required equality holds if and only if the set $\{A_1 A_2 \mid A_1 \in \mathcal{A}_1, A_2 \in \mathcal{A}_2\}$ spans $M_n(\mathbb{C})$. Hence our lemma is a simple reformulation of one of the claims of the original statement [8, Prop. 2] \square

Corollary 3.2. *There is no orthogonal decomposition of $M_{n^2}(\mathbb{C})$ into maximal abelian subalgebras and a (single) factor isomorphic to $M_n(\mathbb{C})$.*

Proof. Suppose the maximal abelian algebras $\mathcal{A}_1, \dots, \mathcal{A}_{n^2}$ together with the factor \mathcal{B} form such a decomposition. Then, since both $\dim(\mathcal{B}) = \dim(M_n(\mathbb{C})) = n^2$ and also the dimension of a maximal abelian subalgebra of $M_{n^2}(\mathbb{C})$ is n^2 , by the previous lemma we have that \mathcal{B}' is an orthogonal subalgebra to $\mathcal{A}'_k = \mathcal{A}_k$ ($k = 1, \dots, n^2$). But since \mathcal{B} is a factor, \mathcal{B}' is also orthogonal to \mathcal{B} . Hence \mathcal{B}' should be orthogonal to each member of an orthogonal decomposition, implying that \mathcal{B}' should be equal to the trivial subalgebra $\mathbb{C}\mathbb{1}$ and in turn, that $\mathcal{B} = \mathcal{B}'$ should be the full matrix algebra $M_{n^2}(\mathbb{C})$ (which is clearly a contradiction). \square

Remark. In [14] the author of the present work has shown that if $\mathcal{A}_1, \dots, \mathcal{A}_d$ is a system of d MASAs in $M_d(\mathbb{C})$, then any pair of elements in the orthogonal subspace $(\mathcal{A}_1 + \dots + \mathcal{A}_d)^\perp$ must commute. In particular, if $\mathcal{A}_1, \dots, \mathcal{A}_d, \mathcal{B}$ is an orthogonal system in $M_d(\mathbb{C})$ where $\mathcal{A}_1, \dots, \mathcal{A}_d$ are MASAs, then \mathcal{B} must be a commutative algebra. This is of course a much stronger affirmation than the above corollary. However, that article uses a much longer proof and the method presented here has the further advantage that — as we shall shortly see — it can be applied to cases when the number of MASAs is less than d . In any case, the aim of the cited work was to study mutually unbiased bases (and not orthogonal decompositions in general); the nonexistence of the above discussed system was not stated explicitly there.

Now how about decompositions of $M_{n^2}(\mathbb{C})$ into MASAs and *two* factors isomorphic to $M_n(\mathbb{C})$? Such decompositions, in general, cannot be ruled out. Indeed, as was mentioned, in [12] the case of $n = 2$ was treated and in particular an example was given for such a decomposition. Moreover, it was shown that there are no decompositions of $M_4(\mathbb{C})$ into MASAs and factors isomorphic to $M_2(\mathbb{C})$ in which the number of factors would be 1, 3 or 5. For general $n > 1$, we shall now prove that there is no decompositions of $M_{n^2}(\mathbb{C})$ into MASAs and factors isomorphic to $M_n(\mathbb{C})$ in which the number of factors is 3 (and we have already seen that nor it can be 1). We will need some preparatory steps.

Lemma 3.3. *Let \mathcal{A}_1 and \mathcal{A}_2 be orthogonal subalgebras of $M_n(\mathbb{C})$ and $A_1 \in \mathcal{A}_1$ and $A_2 \in \mathcal{A}_2$ two traceless operators. Then $A_j A_k \in \mathcal{A}_1 + \mathcal{A}_2$ if $j = k$ whereas if $j \neq k$ then $A_j A_k$ is orthogonal to the subspace $\mathcal{A}_1 + \mathcal{A}_2$.*

Proof. Apart from trivial affirmations, all we have to check that is that the “cross-terms” $A_j A_k$ (where $j \neq k$) are orthogonal to the subspace $\mathcal{A}_1 + \mathcal{A}_2$. If $X \in \mathcal{A}_1$, then

$$\langle X, A_1 A_2 \rangle = \text{Tr}(X^* A_1 A_2) = \text{Tr}((A_1^* X)^* A_2) = \langle (A_1^* X), A_2 \rangle = 0 \quad (18)$$

since $(A_1^* X) \in \mathcal{A}_1$ whereas A_2 is a traceless operator in \mathcal{A}_2 which is supposed to be orthogonal to \mathcal{A}_1 . If $X \in \mathcal{A}_2$ then using the invariance of trace under cyclic permutations we still get that

$$\langle X, A_1 A_2 \rangle = \text{Tr}(X^* A_1 A_2) = \text{Tr}(A_1 A_2 X^*) = \langle A_1^*, (A_2 X^*) \rangle = 0 \quad (19)$$

as the traceless element A_1^* of \mathcal{A}_1 is orthogonal to any element of \mathcal{A}_2 (and in particular, to A_2X^*). The rest (the orthogonality of the other cross-term: A_2A_1) follows by symmetry of the argument. \square

Lemma 3.4. *Let \mathcal{A}_1 and \mathcal{A}_2 be -orthogonal subalgebras of $M_n(\mathbb{C})$ and suppose that \mathcal{B} is a third subalgebra of $M_n(\mathbb{C})$ such that $\mathcal{B} \subset \mathcal{A}_1 + \mathcal{A}_2$. Then either $\mathcal{B} \subset \mathcal{A}_j$ for some $j = 1, 2$ or $\mathcal{B} \cap \mathcal{A}_1 = \mathcal{B} \cap \mathcal{A}_2 = \mathbb{C}\mathbb{1}$.*

Proof. Suppose there exists a $B \in \mathcal{B}$ which is neither in \mathcal{A}_1 nor in \mathcal{A}_2 . Then its traceless part

$$B_0 = B - \tau(B)\mathbb{1} = B - (\text{Tr}(B)/n)\mathbb{1} \quad (20)$$

is still an element of \mathcal{B} which is neither in \mathcal{A}_1 nor in \mathcal{A}_2 , so

$$B_0 = B_1 + B_2 \quad (21)$$

for some $B_j \in \mathcal{A}_j$ nonzero traceless operators ($j = 1, 2$). If $X \in \mathcal{B} \cap \mathcal{A}_1$ then again its traceless part X_0 is still in the intersection $\mathcal{B} \cap \mathcal{A}_1$. Thus $X_0B_1 \in \mathcal{A}_1$ whereas by lemma 3.3, X_0B_2 is orthogonal to $\mathcal{A}_1 + \mathcal{A}_2$ since $X_0 \in \mathcal{A}_1$. On the other hand, as $X_0 \in \mathcal{B}$, we have that $X_0B_1 + X_0B_2 = X_0B_0 \in \mathcal{B} \subset \mathcal{A}_1 + \mathcal{A}_2$. These two things imply that $X_0B_2 = 0$.

Of course the fact that $B_2 \neq 0$ is not enough for showing that $X_0 = 0$. However, the argument presented at equation (15) shows that — apart from a factor depending on the dimension n — the *trace-norm* of a product of two elements belonging to two orthogonal subalgebras is simply the product of norms. Hence in our case $X_0B_2 = 0$ actually *does* imply that one of the terms in the product must be zero, and so that $X_0 = 0$. Thus the arbitrary element X of the intersection $\mathcal{B} \cap \mathcal{A}_1$ is a multiple of the identity; that is $\mathcal{B} \cap \mathcal{A}_1 = \mathbb{C}\mathbb{1}$. The rest of the claim follows by repeating the argument with \mathcal{A}_1 and \mathcal{A}_2 exchanged. \square

Lemma 3.5. *Let \mathcal{A}_1 and \mathcal{A}_2 be orthogonal subalgebras of $M_n(\mathbb{C})$ and suppose that $A_j \in \mathcal{A}_j$ are traceless operators ($j = 1, 2$) such that $A^2 \in \mathcal{A}_1 + \mathcal{A}_2$ where $A = A_1 + A_2$. Then A_1 and A_2 must anti-commute.*

Proof. The claim is evident because by the previous lemma, in the expansion $A^2 = A_1^2 + A_2^2 + A_1A_2 + A_2A_1$, the first two terms are in $\mathcal{A}_1 + \mathcal{A}_2$ whereas the last two terms are orthogonal to this subspace. \square

Theorem 3.6. *Let \mathcal{A}_1 and \mathcal{A}_2 be orthogonal subalgebras of $M_n(\mathbb{C})$ and suppose that \mathcal{B} is a third subalgebra of $M_n(\mathbb{C})$ such that $\mathcal{B} \subset \mathcal{A}_1 + \mathcal{A}_2$. Then either $\mathcal{B} \subset \mathcal{A}_j$ for some $j = 1, 2$ or $\mathcal{B} \simeq \mathbb{C}^2$.*

Proof. Assume by contradiction that \mathcal{B} is not included in neither of the two given orthogonal subalgebras, but \mathcal{B} is not isomorphic to \mathbb{C}^2 . Then $\dim(\mathcal{B}) > 2$ (since up to isomorphism, there is only one two dimensional star-algebra: \mathbb{C}^2) and so the traceless part of \mathcal{B} ,

$$\mathcal{B}_0 := \mathcal{B} \cap \{\mathbb{1}\}^\perp \quad (22)$$

is at least 2-dimensional.

Let E_j be the trace-preserving expectation onto \mathcal{A}_j for $j = 1, 2$. For any traceless element $X \in \mathcal{A}_1 + \mathcal{A}_2$ we have that $X = E_1(X) + E_2(X)$, so $\mathcal{B}_0 \subset E_1(\mathcal{B}_0) + E_2(\mathcal{B}_0)$.

Moreover, this inclusion cannot be an equality, since in that case \mathcal{B}_0 would nontrivially intersect \mathcal{A}_1 or \mathcal{A}_2 , contradicting to our previous lemma. Thus at least one out of the subspaces: $E_1(\mathcal{B}_0), E_2(\mathcal{B}_0)$ must be more than 1-dimensional; we may assume that $\dim(E_2(\mathcal{B}_0)) > 1$.

Let $B \in \mathcal{B}$ be a traceless self-adjoint element. Then $B = B_1 + B_2$ where $B_j = E_j(B)$ ($j = 1, 2$), and since $\dim(E_2(\mathcal{B}_0)) > 1$, there exists a $\tilde{B} \in \mathcal{B}_0$ such that $\tilde{B}_2 = E_2(\tilde{B})$ is nonzero and orthogonal to B_1 . As \mathcal{B} is an algebra, we have that $B\tilde{B} \in \mathcal{B} \subset \mathcal{A}_1 + \mathcal{A}_2$. But $B\tilde{B} = B_1\tilde{B}_1 + B_2\tilde{B}_2 + B_1\tilde{B}_2 + B_2\tilde{B}_1$, and according to lemma 3.3, the first two terms in this sum are in $\mathcal{A}_1 + \mathcal{A}_2$ whereas the last two terms are orthogonal to this subspace, so actually $B_1\tilde{B}_2 + B_2\tilde{B}_1 = 0$. On the other hand, by using the product-property (6), the anti-commutativity of B_1 and B_2 (assured by lemma 3.5), and the fact that $B_2 = E_2(B)$ is self-adjoint (as so is B), we have that

$$\begin{aligned} \langle B_1\tilde{B}_2, B_2\tilde{B}_1 \rangle &= \text{Tr}((B_1\tilde{B}_2)^* B_2\tilde{B}_1) = \text{Tr}(\tilde{B}_2^* B_1 B_2 \tilde{B}_1) = -\text{Tr}(\tilde{B}_2^* B_2 B_1 \tilde{B}_1) \\ &= -n\tau(\tilde{B}_2^* B_2 B_1 \tilde{B}_1) = -n\tau(\tilde{B}_2^* B_2)\tau(B_1 \tilde{B}_1) = 0, \end{aligned} \quad (23)$$

since by assumption $0 = \langle \tilde{B}_2, B_2 \rangle = \text{Tr}(\tilde{B}_2^* B_2) = n\tau(\tilde{B}_2^* B_2)$. Thus $B_1\tilde{B}_2 = B_2\tilde{B}_1 = 0$ since they are orthogonal but their sum is zero. As $\tilde{B}_2 \neq 0$, this implies (by the argument already explained towards the end of the proof of lemma 3.4) that $B_1 = 0$. That is, $B = B_2$ is actually an element of \mathcal{A}_2 . But our assumption, together with lemma 3.4 imply that $\mathcal{B} \cap \mathcal{A}_2 = \mathbb{C}\mathbb{1}$. It should then further follow that $B = 0$; that is, we have shown that any self-adjoint traceless element in \mathcal{B} is zero and hence that $\mathcal{B} = \mathbb{C}\mathbb{1}$ which contradicts to the assumption that \mathcal{B} is *not* a subalgebra of \mathcal{A}_1 or \mathcal{A}_2 . \square

Theorem 3.7. *There are no orthogonal decompositions of $M_{n^2}(\mathbb{C})$ into maximal abelian subalgebras and factors isomorphic to $M_n(\mathbb{C})$ in which the number of factors would be 1 or 3.*

Proof. We have already proved the case in which the number of factors is 1, so now assume by contradiction that we have an orthogonal decomposition containing three factors: $\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3$ (all isomorphic to $M_n(\mathbb{C})$) and $n^2 - 2$ MASAs $\mathcal{A}_1, \dots, \mathcal{A}_{n^2-2}$. Then, as was already noted and applied, considering the commutants: $\mathcal{B}'_1, \mathcal{B}'_2, \mathcal{B}'_3, \mathcal{A}_1, \dots, \mathcal{A}_{n^2-2}$ (where we have used that the commutant of a MASA is itself), we still have an orthogonal decomposition. Thus, \mathcal{B}'_1 is orthogonal to both \mathcal{B}_1 (since it is a factor) and the algebras $\mathcal{A}_1, \dots, \mathcal{A}_{n^2-2}$ and hence $\mathcal{B}'_1 \subset \mathcal{B}_2 + \mathcal{B}_3$. By our previous theorem it then follows that \mathcal{B}'_1 is either equal to \mathcal{B}_2 or to \mathcal{B}_3 . Repeating our argument for \mathcal{B}_2 and \mathcal{B}_3 , we see that the $\mathcal{B}'_j = \mathcal{B}_{\sigma(j)}$ for some $\sigma : \{1, 2, 3\} \rightarrow \{1, 2, 3\}$ such that:

- $\sigma^2 = \text{id}$ (since the second commutant gives back the original algebra),
- σ has no fixed points ($\mathcal{B}'_j \neq \mathcal{B}_j$ as \mathcal{B}_j is not a MASA).

However, these two properties are evidently contradicting. \square

4. The trace formula

Suppose P and Q are the ortho-projections onto the subspaces N and K , respectively. By elementary arguments involving traces and positive operators, one has that $\text{Tr}(PQ)$

is a nonnegative real number,

$$\dim(N \cap K) \leq \text{Tr}(PQ) \leq \min\{\dim(N), \dim(K)\}, \quad (24)$$

and moreover that $\dim(N \cap K) = \text{Tr}(PQ)$ if and only if $N \cap (N \cap K)^\perp$ and $K \cap (N \cap K)^\perp$ are orthogonal. Thus we may say that the nonnegative number $\text{Tr}(PQ) - \dim(N \cap K)$ measures “how much” the subspaces $N \cap (N \cap K)^\perp$ and $K \cap (N \cap K)^\perp$ are *not* orthogonal. This number is zero if and only if they are orthogonal, and in some sense the bigger it is, the further away they are from orthogonality. Let us see now what this has to do with orthogonal subalgebras.

A subalgebra $\mathcal{A} \subset M_n(\mathbb{C})$ is in particular a linear subspace. As was discussed, $M_n(\mathbb{C})$ has a natural scalar product, so it is meaningful to talk about orthogonality. Thus we may consider the ortho-projection $E_{\mathcal{A}}$ onto \mathcal{A} . Note that this map is usually referred as the *unique trace-preserving expectation* onto \mathcal{A} . For two subalgebras $\mathcal{A}, \mathcal{B} \subset M_n(\mathbb{C})$ we shall now introduce the quantity

$$c(\mathcal{A}, \mathcal{B}) := \text{Tr}(E_{\mathcal{A}}E_{\mathcal{B}}). \quad (25)$$

Note that here Tr is the trace of the set of linear operators *acting* on $M_n(\mathbb{C})$, and not the trace of $M_n(\mathbb{C})$.

Recall that by “subalgebra” we always mean a *-subalgebra containing the identity, so $\mathcal{A} \cap \mathcal{B}$ is at least one-dimensional. Thus $c(\mathcal{A}, \mathcal{B})$ is a nonnegative real and infact

$$1 \leq c(\mathcal{A}, \mathcal{B}) \leq \min\{\dim(\mathcal{A}), \dim(\mathcal{B})\} \quad (26)$$

with $c(\mathcal{A}, \mathcal{B}) = 1$ if and only if \mathcal{A} and \mathcal{B} are orthogonal subalgebras.

We are interested by the relation between the quantities $c(\mathcal{A}, \mathcal{B})$ and $c(\mathcal{A}', \mathcal{B}')$ where \mathcal{A}' and \mathcal{B}' are the commutants of \mathcal{A} and \mathcal{B} , respectively. The next example shows that in general, $c(\mathcal{A}', \mathcal{B}')$ cannot be determined by knowing the value of $c(\mathcal{A}, \mathcal{B})$ and the (unitary) equivalence classes³ of the subalgebras \mathcal{A} and \mathcal{B} . (Of course, the knowledge of the unitary equivalence class of the pair \mathcal{A}, \mathcal{B} — so not just their *separate equivalence classes* — would suffice.)

Example. Let $\mathcal{A} := M_4(\mathbb{C}) \otimes \mathbb{1}_4 \subset M_4(\mathbb{C}) \otimes M_4(\mathbb{C}) \equiv M_{16}(\mathbb{C})$ and $\tilde{\mathcal{A}} := \mathcal{A}' = \mathbb{1}_4 \otimes M_4(\mathbb{C})$. Then clearly, \mathcal{A} and $\tilde{\mathcal{A}}$ are unitarily equivalent. Let further $P_1 \in M_4(\mathbb{C})$ be an ortho-projection onto a one-dimensional subspace and $P_2 \in M_4(\mathbb{C})$ an ortho-projection onto a two-dimensional subspace. Let $\mathcal{B} := \mathcal{D}_1 \otimes \mathcal{D}_2$ where $\mathcal{D}_1, \mathcal{D}_2 \subset M_4(\mathbb{C})$ are the abelian subalgebras generated by the single ortho-projections P_1 and P_2 , respectively. Then, as all of the algebras $\mathcal{A}, \mathcal{A}', \tilde{\mathcal{A}}, \mathcal{B}, \mathcal{B}'$ have a product-form, it is easy to see that

$$E_{\mathcal{A}}E_{\mathcal{B}} = (id_4 \otimes \text{Tr}_4)(E_{\mathcal{D}_1} \otimes E_{\mathcal{D}_2}) = E_{\mathcal{D}_1} \otimes \text{Tr}_4 = E_{\mathcal{D}_1 \otimes \mathbb{1}_4}, \quad (27)$$

so $c(\mathcal{A}, \mathcal{B}) = \text{Tr}(E_{\mathcal{A}}E_{\mathcal{B}}) = \text{Tr}(E_{\mathcal{D}_1 \otimes \mathbb{1}_4}) = \dim(\mathcal{D}_1) = 2$ and similarly, that $c(\tilde{\mathcal{A}}, \mathcal{B})$ is also equal to 2. However, as $\mathcal{B}' = \mathcal{D}'_1 \otimes \mathcal{D}'_2$ while the commutants of \mathcal{A} and $\tilde{\mathcal{A}}$ are $\tilde{\mathcal{A}}$ and \mathcal{A} , respectively, we have that

$$c(\mathcal{A}', \mathcal{B}') = \dim(\mathcal{D}'_2) = 2^2 + 2^2 \neq 1^2 + 3^2 = \dim(\mathcal{D}'_1) = c(\tilde{\mathcal{A}}, \mathcal{B}'). \quad (28)$$

³Two isomorphic subalgebras of $M_n(\mathbb{C})$ (that is: *-subalgebras containing $1 \in M_n(\mathbb{C})$) are not necessarily unitarily equivalent. For example, if P and Q are ortho-projections in $M_4(\mathbb{C})$ onto subspaces of dimensions 2 and 3, respectively, then $\mathcal{A} \simeq \mathcal{B} \simeq \mathbb{C}^2$ where $\mathcal{A} = \mathbb{C}P + \mathbb{C}1$ and $\mathcal{B} = \mathbb{C}Q + \mathbb{C}1$. However, clearly there is no unitary $U \in M_n(\mathbb{C})$ such that UAU^* would coincide with \mathcal{B} .

Thus the value of $c(\mathcal{A}, \mathcal{B})$, even together with the knowledge of the (separate) unitary equivalence classes of \mathcal{A} and \mathcal{B} , is insufficient for determining $c(\mathcal{A}', \mathcal{B}')$.

A subalgebra, up to unitary equivalence, is always of the form

$$\mathcal{A} = \oplus_k (M_{n_k}(\mathbb{C}) \otimes \mathbb{1}_{m_k}) \subset M_n(\mathbb{C}) \quad (29)$$

where $n = \sum_k n_k m_k$ (and $\mathbb{1}_x$ is the unit of $M_x(\mathbb{C})$) with commutant

$$\mathcal{A}' = \oplus_k (\mathbb{1}_{n_k}(\mathbb{C}) \otimes M_{m_k}(\mathbb{C})) \subset M_n(\mathbb{C}). \quad (30)$$

In case the ratios n_k/m_k are independent of the index k , we shall say that the subalgebra \mathcal{A} is **homogeneously balanced**. Note that if $n_k/m_k = \lambda$ for all indices k , then $n = \sum_k n_k m_k = \lambda \sum_k m_k^2 = \lambda \dim(\mathcal{A}')$ and $\dim(\mathcal{A}) = \sum_k n_k^2 = \lambda^2 \sum_k m_k^2 = \lambda^2 \dim(\mathcal{A}')$. Some evident, but important consequences of our definition and this last remark are:

- \mathcal{A} is homogeneously balanced if and only if so is \mathcal{A}' ,
- if $\mathcal{A} \subset M_n(\mathbb{C})$ and $\mathcal{B} \subset M_m(\mathbb{C})$ are homogeneously balanced then so is the tensorial product $\mathcal{A} \otimes \mathcal{B} \subset M_n(\mathbb{C}) \otimes M_m(\mathbb{C}) \equiv M_{nm}(\mathbb{C})$,
- factors and MASAs are automatically homogeneously balanced,
- if \mathcal{A} is homogeneously balanced then $\dim(\mathcal{A})\dim(\mathcal{A}') = n^2$
- this homogeneity, in general, is not a condition about the isomorphism class of \mathcal{A} , but about the way it “sits” in $M_n(\mathbb{C})$ (i.e. its unitary equivalence class): of two isomorphic subalgebras, one may be homogeneously balanced while the other is not.

Note that the algebra \mathcal{B} in the previous example was *not* homogeneously balanced. We shall now recall a simple, but important fact; for the more general statement and its proof see [8, Prop. 1].

Lemma 4.1. *If $\mathcal{A} \subset M_n(\mathbb{C})$ is homogeneously balanced and A_1, \dots, A_N is an orthonormal basis of \mathcal{A} , then $E_{\mathcal{A}'}(X) = \frac{n}{N} \sum_{j=1}^N A_j X A_j^*$ for all $X \in M_n(\mathbb{C})$.*

Theorem 4.2. *If $\mathcal{A}, \mathcal{B} \subset M_n(\mathbb{C})$ are homogeneously balanced then*

$$c(\mathcal{A}', \mathcal{B}') = \frac{n^2}{\dim(\mathcal{A})\dim(\mathcal{B})} c(\mathcal{A}, \mathcal{B}).$$

Proof. Let $A_1, \dots, A_N \in \mathcal{A}$ and $B'_1, \dots, B'_{\tilde{N}} \in \mathcal{B}'$ be two orthonormal bases, where $N := \dim(\mathcal{A})$ and $\tilde{N} := \dim(\mathcal{B}') = n^2/\dim(\mathcal{B})$. Using the previous lemma

$$\begin{aligned} \sum_{j,k} \text{Tr}(A_j B'_k A_j^* B_k'^*) &= \frac{N}{n} \sum_k \text{Tr}(E_{\mathcal{A}'}(B'_k) B_k'^*) = \frac{N}{n} \sum_k \text{Tr}(E_{\mathcal{A}'}(E_{\mathcal{A}'}(B'_k) B_k'^*)) \\ &= \frac{N}{n} \sum_k \text{Tr}(E_{\mathcal{A}'}(B'_k) E_{\mathcal{A}}(B_k'^*)) = \frac{N}{n} \sum_k \|E_{\mathcal{A}'}(B'_k)\|_{\text{Tr}}^2 \\ &= \frac{\dim(\mathcal{A})}{n} \text{Tr}(E_{\mathcal{A}'} E_{\mathcal{B}'}) \end{aligned} \quad (31)$$

where we have used the simple fact that if P, Q are ortho-projections then $\text{Tr}(PQ) = \sum_k \|Pq_k\|^2$ where q_1, \dots, q_s is an ortho-normed basis in the image of Q . However, we could have carried out the above calculation in a similar way but with the role of \mathcal{A} and \mathcal{B}' exchanged. Confronting the obtained form to the one appearing in the previous equation one can easily obtain the claimed formula. \square

5. Example applications of the formula

The so-far presented results relied on the result of Petz and Ohno which ensured that if $\mathcal{A}, \mathcal{B} \subset M_n(\mathbb{C})$ is an orthogonal pair of subalgebras and $\dim(\mathcal{A})\dim(\mathcal{B}) = n^2$ then also \mathcal{A}' and \mathcal{B}' form an orthogonal pair. Note that if \mathcal{A} and \mathcal{B} are homogeneously balanced, then this fact is a simple consequences of our formula obtained in the last section. In some sense, our formula gives a *quantitative generalization* of this fact. To make use of this quantitative information, all we need is the following observation.

Lemma 5.1. *Let $\mathcal{C} \subset M_n(\mathbb{C})$ be a subalgebra and $\mathcal{A}_1, \dots, \mathcal{A}_k \subset M_n(\mathbb{C})$ be a system of orthogonal subalgebras. Then*

$$(i) \dim(\mathcal{C}) \geq 1 - k + \sum_{j=1}^k c(\mathcal{A}_j, \mathcal{C}), \text{ and}$$

$$(ii) \dim(\mathcal{C}) \leq n^2 - 1 + \sum_{j=1}^k (c(\mathcal{A}_j, \mathcal{C}) - \dim(\mathcal{A}_j))$$

with equality holding in (i) if and only if $\mathcal{C} \subset \mathcal{A}_1 + \mathcal{A}_2 + \dots + \mathcal{A}_k$ (which is automatically satisfied if in particular $\mathcal{A}_1, \dots, \mathcal{A}_k$ is an orthogonal system of $M_n(\mathbb{C})$).

Proof. The subalgebra $\mathbb{C}\mathbb{1}$ is contained in every subalgebra, so $E_{\mathcal{A}_j} - E_{\mathbb{C}\mathbb{1}}$ is a projection; in fact it is the ortho-projection onto the “traceless part” of \mathcal{A}_j . Orthogonality of $\mathcal{A}_1, \dots, \mathcal{A}_k$ is then equivalent to the fact that the projections $(E_{\mathcal{A}_j} - E_{\mathbb{C}\mathbb{1}})$ are mutually orthogonal for $j = 1, \dots, k$. Moreover, in this case

$$F := E_{\mathbb{C}\mathbb{1}} + \sum_{j=1}^k (E_{\mathcal{A}_j} - E_{\mathbb{C}\mathbb{1}}) \tag{32}$$

is nothing else than the ortho-projection onto the subspace $\mathcal{A}_1 + \dots + \mathcal{A}_k$. Hence

$$\begin{aligned} \text{Tr}(FE_{\mathcal{C}}) &= \text{Tr}(E_{\mathbb{C}\mathbb{1}}E_{\mathcal{C}}) + \sum_{j=1}^k (\text{Tr}(E_{\mathcal{A}_j}E_{\mathcal{C}}) - \text{Tr}(E_{\mathbb{C}\mathbb{1}}E_{\mathcal{C}})) = \\ &= 1 + \sum_{j=1}^k (c(\mathcal{A}_j, \mathcal{C}) - 1) = 1 - k + \sum_{j=1}^k c(\mathcal{A}_j, \mathcal{C}) \end{aligned} \tag{33}$$

as $E_{\mathbb{C}\mathbb{1}}E_{\mathcal{C}} = E_{\mathbb{C}\mathbb{1}}$ is a projection onto a one-dimensional subspace. Thus (i) follows as

$$\text{Tr}(FE_{\mathcal{C}}) \leq \text{Tr}(E_{\mathcal{C}}) = \dim(\mathcal{C}) \tag{34}$$

with equality holding if and only if $E_{\mathcal{C}}$ is a smaller projection than F ; i.e. when $\mathcal{C} \subset (\mathcal{A}_1 + \dots + \mathcal{A}_k)$. The inequality (ii) follows by considering $\mathbb{1}$ as the sum of the two orthogonal

projections: $\mathbb{1} = F + (\mathbb{1} - F)$. Now F is an ortho-projection onto a $d := \dim(\sum_j \mathcal{A}_j)$ dimensional space, where by orthogonality

$$d = 1 + \sum_j (\dim(\mathcal{A}_j) - 1), \quad (35)$$

whereas $(\mathbb{1} - F)$ is the ortho-projection onto the orthogonal of $\mathcal{A}_1 + \dots + \mathcal{A}_k$, which is an $n^2 - d$ dimensional subspace. Thus

$$\dim(\mathcal{C}) = \text{Tr}(E_{\mathcal{C}}) = \text{Tr}(FE_{\mathcal{C}}) + \text{Tr}((\mathbb{1} - F)E_{\mathcal{C}}) \quad (36)$$

where $\text{Tr}((\mathbb{1} - F)E_{\mathcal{C}}) \leq n^2 - d = n^2 - 1 - \sum_j (\dim(\mathcal{A}_j) - 1)$. This, together with (33) expressing the term $\text{Tr}(FE_{\mathcal{C}})$, concludes our proof. \square

So let us see now how we can use our formula in practice. We begin with a fairly simple case; we shall consider an orthogonal system in $M_6(\mathbb{C})$ containing 6 maximal abelian subalgebras $\mathcal{A}_1, \dots, \mathcal{A}_6$ and a subalgebra \mathcal{B} isomorphic to $M_2(\mathbb{C})$. The trivial necessary conditions would allow the existence of such a system. Of course, as was explained in the remark made after Corollary 3.2, by using the strong result of [14], it is easy to show that such a system cannot exist. But how could we rule out its existence in a more direct manner? Now we cannot use Corollary 3.2: 6 is not a square number and more in particular $\dim(M_2(\mathbb{C})) = 2^2 \neq 6$, so \mathcal{B}' would not remain orthogonal to the subalgebras $\mathcal{A}_1, \dots, \mathcal{A}_6$.

So assume the existence of such a system. Then by the fact that \mathcal{A}_j is a MASA ($j = 1, \dots, 6$), and by an application of our formula

$$c(\mathcal{A}_j, \mathcal{B}') = c(\mathcal{A}'_j, \mathcal{B}') = \frac{6^2}{6 * 4} c(\mathcal{A}_j, \mathcal{B}) = \frac{3}{2}, \quad (37)$$

since $\dim(\mathcal{B}) = \dim(M_2(\mathbb{C})) = 4$ and $c(\mathcal{A}_j, \mathcal{B}) = 1$ by the assumed orthogonality of \mathcal{B} and \mathcal{A}_j . Moreover, $c(\mathcal{B}, \mathcal{B}') = 1$ because \mathcal{B} was assumed to be a factor. So considering the orthogonal system $\mathcal{A}_1, \dots, \mathcal{A}_6, \mathcal{B}$ and the algebra $\mathcal{C} := \mathcal{B}' \simeq M_3(\mathbb{C})$, we have $\dim(\mathcal{A}_j) = 6$, $\dim(\mathcal{B}) = 2^2 = 4$, and

$$\begin{aligned} n^2 - 1 + (c(\mathcal{B}, \mathcal{C}) - \dim(\mathcal{B})) + \sum_{j=1}^6 (c(\mathcal{A}_j, \mathcal{C}) - \dim(\mathcal{A}_j)) &= \\ 6^2 - 1 + (1 - 4) + 6 * \left(\frac{3}{2} - 6\right) &= 5, \end{aligned} \quad (38)$$

which is in conflict with (ii) of lemma 5.1, as $\dim(\mathcal{C}) = \dim(\mathcal{B}') = 3^2 = 9 \not\leq 5$.

This is nice, but — as was mentioned — it is a fairly simple case in which we have already known the nonexistence. So we shall finish by considering a somewhat more complicated example.

Proposition 5.2. *There is no orthogonal system in $M_6(\mathbb{C})$ consisting of 5 maximal abelian subalgebras and 3 factors isomorphic to $M_2(\mathbb{C})$.*

Proof. Again, note that the existence of such a system cannot be ruled out by the trivial necessary conditions. We assume $\mathcal{A}_1, \dots, \mathcal{A}_5, \mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3$ is such a system (with the “ \mathcal{A} ”

algebras being the maximal abelian ones, and the “ \mathcal{B} ” algebras the factors isomorphic to $M_2(\mathbb{C})$). To apply our formula, we will need to consider the commutants as well as the original algebras. If $\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3 \simeq M_2(\mathbb{C})$ and $\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3 \subset M_6(\mathbb{C})$, then their commutants $\mathcal{B}'_1, \mathcal{B}'_2, \mathcal{B}'_3 \simeq M_3(\mathbb{C})$. Since $M_2(\mathbb{C})$ cannot be embedded in $M_3(\mathbb{C})$ in an identity preserving way, we have that \mathcal{B}_j is not contained in \mathcal{B}'_k and consequently that

$$c(\mathcal{B}_j, \mathcal{B}'_k) < \dim(\mathcal{B}_j) = 4 \quad (39)$$

for every $j, k = 1, 2, 3$. However, we shall need a better estimate. Actually, more than just noting that $\mathcal{B}_j \not\subset \mathcal{B}'_k$, we can say something about their “minimal distance”. We shall shortly interrupt our proof with a lemma concerning this issue.

Lemma 5.3. $c(\mathcal{B}_j, \mathcal{B}'_k) \leq 3$.

Proof (of lemma). Let $X, Y, Z, W \in \mathcal{B}_j$ be an orthogonal basis such that $W = \mathbb{1}$ and X, Y, Z correspond to the Pauli-matrices in a suitable identification $\mathcal{B}_j \simeq M_2(\mathbb{C})$. Let us further denote the trace-preserving expectation onto \mathcal{B}'_k by E . Then $E(X)$ (and similarly $E(Y)$ and $E(Z)$, too) remains self-adjoint, so it is unitarily equivalent with a diagonal matrix. Moreover, as it belongs to $\mathcal{B}'_k \simeq M_3(\mathbb{C})$, we may actually assume it is unitarily equivalent with the diagonal matrix $\text{diag}(\lambda_1, \lambda_1, \lambda_2, \lambda_2, \lambda_3, \lambda_3) \in M_6(\mathbb{C})$. We have that

- $\lambda_1 + \lambda_2 + \lambda_3 = 0$,
- $\lambda_1, \lambda_2, \lambda_3 \in [-1, 1]$.

Indeed, the first equation follows as $\text{Tr}(E(X)) = \text{Tr}(X) = 0$, whereas the second follows from the fact $\mathbb{1} \pm E(X) = E(\mathbb{1} \pm X)$ — just as $\mathbb{1} \pm X$ — is a positive operator. Now elementary calculus shows that in the region determined by the two equation, we have

$$\text{Tr}(E(X)^2) = 2(\lambda_1^2 + \lambda_2^2 + \lambda_3^2) \leq 4. \quad (40)$$

On the other hand, $\text{Tr}(X^2) = \text{Tr}(\mathbb{1}) = 6$; actually, $X, Y, Z, \mathbb{1}$ is an orthogonal basis whose each member has (trace)norm-square equal to 6. Thus, using the arguments explained at and after equation (31), we have that

$$c(\mathcal{B}_j, \mathcal{B}'_k) = \frac{1}{6}(\text{Tr}(E(X)^2) + E(Y)^2 + E(Z)^2 + E(\mathbb{1})^2) \leq \frac{1}{6}(4 + 4 + 4 + 6) = 3 \quad (41)$$

which is just what we wanted to prove.

To finish the proof, we consider the algebra $\mathcal{C} := \mathcal{B}'_1 \simeq M_3(\mathbb{C})$ and the orthogonal system $\mathcal{A}_1, \dots, \mathcal{A}_5, \mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3$. As $\mathcal{A}'_k = \mathcal{A}_k$. By an application of our formula have that

$$c(\mathcal{A}_k, \mathcal{C}) = c(\mathcal{A}_k, \mathcal{B}'_1) = \frac{6^2}{6 * 2^2} c(\mathcal{A}_k, \mathcal{B}_1) = \frac{6^2}{2^2 * 6} = \frac{3}{2} \quad (42)$$

since $c(\mathcal{A}_k, \mathcal{B}_1) = 1$ by orthogonality. Now $c(\mathcal{B}_1, \mathcal{C}) = c(\mathcal{B}_1, \mathcal{B}'_1) = 1$ since \mathcal{B} is a factor, and finally, for $c(\mathcal{B}_2, \mathcal{C})$ and $c(\mathcal{B}_3, \mathcal{C})$ we can use the estimate provided by the lemma we have just made. To sum it up: we have $n^2 - 1 = 6^2 - 1 = 35$,

$$\begin{aligned} \sum_{j=1}^5 (c(\mathcal{A}_j, \mathcal{C}) - \dim(\mathcal{A}_j)) &= 5 * \left(\frac{3}{2} - 6\right) = -\frac{45}{2}, \quad \text{and} \\ \sum_{j=1}^3 (c(\mathcal{B}_j, \mathcal{C}) - \dim(\mathcal{B}_j)) &\leq (1 - 4) + (3 - 4) + (3 - 4) = -5 \end{aligned} \quad (43)$$

which gives $35 - (45/2) - 5 = 15/2 \not\geq 9 = \dim(\mathcal{C})$, in contradiction with point (ii) of lemma 5.1. \square

- [1] I. Bengtsson, W. Bruzda, Å. Ericsson, J.-A. Larsson, W. Tadej and K. Życzkowski: Mutually unbiased bases and Hadamard matrices of order six, *J. Math. Phys.* **48** (2007), 052106.
- [2] P. Butterley and W. Hall: Numerical evidence for the maximum number of mutually unbiased bases in dimension six, *Phys. Lett. A* **369** (2007), 5.
- [3] N. J. Cerf, M. Bourennane, A. Karlsson and N. Gisin: Security of quantum key distribution using d -level systems, *Phys. Rev. Lett.* **88** (2002), 127901.
- [4] B. D. Fields and W. K. Wootters: Optimal state-determination by mutually unbiased measurements, *Ann. Phys.* **191** (1989), 363.
- [5] I. D. Ivanović: Geometrical description of quantal state determination, *J. Phys. A* **14** (1981), 3241.
- [6] P. Jaming, M. Matolcsi, P. Móra, F. Szöllősi and M. Weiner: A generalized Pauli problem and an infinite family of MUB-triplets in dimension 6, *J. Phys. A* **42** (2009), no. 24, 245305.
- [7] H. Ohno: Quasi-orthogonal subalgebras of matrix algebras, *Linear Alg. Appl.* **429** (2008), 2146.
- [8] H. Ohno and D. Petz: Generalizations of Pauli channels. *Acta Math. Hungar.*, **124** (2009), 165.
- [9] H. Ohno, D. Petz and A. Szántó: Quasi-orthogonal subalgebras of 4×4 matrices, *Linear Alg. Appl.* **425** (2007), 109.
- [10] D. Petz, Complementarity in quantum systems, *Rep. Math. Phys.* **59** (2007), 209.
- [11] D. Petz and J. Kahn: Complementary reductions for two qubits, *J. Math. Phys.* **48** (2007) 012107.
- [12] D. Petz, A. Szántó and M. Weiner: Complementarity and the algebraic structure of 4-level quantum systems, *J. Infin. Dim. Anal. Quantum Probability and Related Topics* **12** (2009), 99.
- [13] T. Sano and Y. Watatani: Angles between two subfactors, *J. Oper. Theory* **32** (1944), 209.
- [14] M. Weiner: A gap for the maximum number of mutually unbiased bases. *Under peer-review*, [arXiv:0902.0635](https://arxiv.org/abs/0902.0635).
- [15] W. K. Wootters: A Wigner-function formulation of finite-state quantum mechanics, *Ann. Phys.* **176** (1987), 1.