

Quasi-orthogonal subalgebras of 4×4 matrices

Hiromichi Ohno^{1,4}, Dénes Petz^{2,5,6} and András Szántó^{3,6}

⁴ Graduate School of Information Sciences, Tohoku University
Aobaku, Sendai 980-8579, Japan

⁵ Alfréd Rényi Institute of Mathematics,
H-1364 Budapest, POB 127, Hungary

⁶ Department for Mathematical Analysis, BUTE,
H-1521 Budapest, POB 91, Hungary

Abstract: Maximal Abelian quasi-orthogonal subalgebras form a popular research problem. In this paper quasi-orthogonal subalgebras of $M_4(\mathbb{C})$ isomorphic to $M_2(\mathbb{C})$ are studied. It is proved that if 4 such subalgebras are given, then their orthogonal complement is always a commutative subalgebra. In particular, 5 such subalgebras do not exist. A conjecture is made about the maximal number of pairwise quasi-orthogonal subalgebras of $M_{2^n}(\mathbb{C})$.

Key words: Quasi-orthogonality, Pauli matrices, Cartan decomposition.

MSC: 15A30, 81R05.

1 Introduction

The motivation of this paper comes from the algebraic or matrix formalism of finite quantum systems. An n -level quantum system is described by the algebra $M_n(\mathbb{C})$ of $n \times n$ complex matrices. The matrix algebra of a composite system consisting of an n level and an m -level system is $M_n(\mathbb{C}) \otimes M_m(\mathbb{C}) \simeq M_{nm}(\mathbb{C})$. A subalgebra of $M_k(\mathbb{C})$ corresponds to a subsystem of a k -level quantum system.

¹E-mail: ono@ims.is.tohoku.ac.jp.

²E-mail: petz@math.bme.hu. Partially supported by the Hungarian Research Grant OTKA T068258.

³E-mail: szbandi@math.bme.hu. Partially supported by the Hungarian Research Grant OTKA TS-49835.

In this paper subalgebras always contain the identity and closed under the adjoint operation of matrices, that is, they are unital $*$ -subalgebras. The algebra $M_k(\mathbb{C})$ can be endowed by the inner product $\langle A, B \rangle = \text{Tr}(A^*B)$ and it becomes a Hilbert space.

A kind of quantum mechanical background gives motivation for the following definition [7]. Two subalgebras $\mathcal{A}(1)$ and $\mathcal{A}(2)$ of $M_k(\mathbb{C})$ are called quasi-orthogonal if $\text{Tr} A_1 A_2 = 0$, whenever $A_i \in \mathcal{A}(i)$ and $\text{Tr} A_1 = \text{Tr} A_2 = 0$. Since the intersection of $\mathcal{A}(1)$ and $\mathcal{A}(2)$ contain the identity, they cannot be orthogonal, but $\mathcal{A}_1 \ominus \mathbb{C}I \perp \mathcal{A}_2 \ominus \mathbb{C}I$ can happen, and this is exactly the quasi-orthogonality. In the literature of quantum mechanics the terminology complementarity is used instead of quasi-orthogonality, see [1, 5].

The analysis of pairwise quasi-orthogonal maximal Abelian subalgebras is a popular subject [2, 3]. If $\mathcal{A} \subset M_k(\mathbb{C})$ is a maximal Abelian subalgebra and W is a unitary, then \mathcal{A} and $W\mathcal{A}W^*$ are quasi-orthogonal if and only if W is a Hadamard matrix. The maximal number of pairwise quasi-orthogonal maximal Abelian subalgebras is an open problem [9].

A different problem is the analysis of pairwise quasi-orthogonal non-commutative subalgebras [6]. If $\mathcal{A} \subset M_{k^2}(\mathbb{C})$ is isomorphic to $M_k(\mathbb{C})$, then the commutant \mathcal{A}' of \mathcal{A} is quasi-orthogonal to \mathcal{A} . Another example of two quasi-orthogonal subalgebras isomorphic to $M_k(\mathbb{C})$ was shown in [6]. The maximal number of such (pairwise) quasi-orthogonal subalgebras is not known except for the case $k = 2$. Then the maximum is 4 as this was proved in [8]. The aim of the present paper is to study the structure of the 4 pairwise quasi-orthogonal subalgebras. The analysis of the structure gives that the quasi-orthogonal complement of 4 (pairwise) quasi-orthogonal subalgebras is always a maximal Abelian subalgebra.

Although we are mostly concentrate on subalgebras of $M_4(\mathbb{C})$, we try to extend the results to subalgebras of $M_{2^n}(\mathbb{C})$. Let $m(n)$ be the maximal number of pairwise quasi-orthogonal subalgebras of $M_{2^n}(\mathbb{C})$ which are isomorphic to $M_2(\mathbb{C})$. We show that

$$m(n) \geq \frac{4^n - 1}{3} - 1$$

and we conjecture that the inequality is actually an equality.

2 Preliminaries

A natural orthogonal basis of $M_2(\mathbb{C})$ consists of the Pauli matrices:

$$\sigma_0 := \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \sigma_1 := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_2 := \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \sigma_3 := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Computation in the Pauli basis is convenient.

For $x, y \in \mathbb{R}^3$ and

$$x \cdot \sigma := \sum_{i=1}^3 x_i \sigma_i, \quad y \cdot \sigma := \sum_{i=1}^3 y_i \sigma_i$$

we have

$$(x \cdot \sigma)(y \cdot \sigma) = \langle x, y \rangle \sigma_0 + i(x \times y) \cdot \sigma, \quad (1)$$

where $x \times y$ is the vectorial product in \mathbb{R}^3 .

If we want to construct a subalgebra of $M_k(\mathbb{C})$ which is isomorphic to $M_2(\mathbb{C})$, then it is enough to find $S_1, S_2, S_3 \in M_k(\mathbb{C})$ such that S_j is a self-adjoint unitary ($1 \leq j \leq 3$) and $S_3 = -iS_1S_2$. When a triplet (S_1, S_2, S_3) satisfies these condition, it will be called a Pauli triplet. For such a triplet $\text{Tr } S_i = 0$ and $\text{Tr } S_i S_j = 0$ for $i \neq j$. The latter relation is interpreted as the orthogonality of S_i and S_j . Given a Pauli triplet (S_1, S_2, S_3) , the linear mapping defined as

$$\sigma_0 \mapsto I, \quad \sigma_1 \mapsto S_1, \quad \sigma_2 \mapsto S_2, \quad \sigma_3 \mapsto -iS_1S_2$$

is an algebraic isomorphism between $M_2(\mathbb{C})$ and the linear span of the operators I, S_1, S_2 and S_3 .

Although our aim is to study subalgebras of $M_4(\mathbb{C})$, the next result is in a more general setting. If e, f, g are vectors of a Hilbert space, then the linear operator $|e\rangle\langle f|$ acts as $|e\rangle\langle f|g := \langle f, g\rangle e$.

Theorem 1 *Let E_i be an orthonormal basis in $M_n(\mathbb{C})$ and let $W = \sum_i E_i \otimes W_i \in M_n(\mathbb{C}) \otimes M_m(\mathbb{C})$ be a unitary. The subalgebra $W(\mathbb{C}I \otimes M_m(\mathbb{C}))W^*$ is quasi-orthogonal to $\mathbb{C}I \otimes M_m(\mathbb{C})$ if and only if*

$$\frac{m}{n} \sum_k |W_k\rangle\langle W_k|$$

is the identity mapping on $M_m(\mathbb{C})$. This condition cannot hold if $m < n$ and in the case $n = m$ the condition means that $\{W_k : 1 \leq k \leq n^2\}$ is an orthonormal basis in $M_m(\mathbb{C})$.

Proof: Assume that $A, B \in M_m(\mathbb{C})$ and $\text{Tr } B = 0$. Then the condition

$$W(I \otimes A^*)W^* \perp (I \otimes B)$$

is equivalently written as

$$\text{Tr}(W(I \otimes A)W^*(I \otimes B)) = \sum_{k,l} \text{Tr}(E_k E_l^*) \text{Tr}(W_k A W_l^* B) = \sum_k \text{Tr}(W_k A W_k^* B) = 0.$$

Putting $B - \text{Tr}(B)I_m/m$ in place of B , we get

$$\sum_k \text{Tr}(W_k A W_k^* B) = \frac{\text{Tr } B}{m} \sum_k \text{Tr}(W_k A W_k^*)$$

for every $B \in M_m(\mathbb{C})$. Let $\mathcal{E}_2 : M_n(\mathbb{C}) \otimes M_m(\mathbb{C}) \rightarrow M_m(\mathbb{C})$ be the linear mapping defined as

$$\mathcal{E}_2(K \otimes L) = \frac{\text{Tr } K}{n} L.$$

Since \mathcal{E}_2 is unit-preserving and W is a unitary,

$$I_m = \mathcal{E}_2(W^*W) = \mathcal{E}_2\left(\sum_{k,l} E_k^* E_l \otimes W_k^* W_l\right) = \frac{1}{n} \sum_{k,l} \text{Tr}(E_k^* E_l) W_k^* W_l = \frac{1}{n} \sum_k W_k^* W_k,$$

and we arrive at the relation

$$\sum_k \text{Tr } W_k A W_k^* B = \frac{n}{m} \text{Tr } A \text{Tr } B. \quad (2)$$

We can transform this into another equivalent condition in terms of the left multiplication, right multiplication and $|W_k\rangle\langle W_k|$ operators.

For $A, B \in M_m(\mathbb{C})$, the operator R_A is the right multiplication by A and the operator L_B is the left multiplication by B : $R_A, L_B : M_m(\mathbb{C}) \rightarrow M_m(\mathbb{C})$, $R_A X = X A$, $L_B X = B X$. If λ_i 's are the eigenvalues of A and μ_j 's are the eigenvalues of B , then $\lambda_i \mu_j$'s are the eigenvalues of $R_A L_B$. Therefore

$$\text{Tr } R_A L_B = \left(\sum_i \lambda_i\right) \left(\sum_j \mu_j\right) = \text{Tr } A \text{Tr } B.$$

We have

$$\begin{aligned} \sum_k \text{Tr } |W_k\rangle\langle W_k| R_A L_B &= \sum_k \langle W_k, R_A L_B W_k \rangle = \sum_k \text{Tr } W_k A W_k^* B \\ &= \frac{n}{m} \text{Tr } A \text{Tr } B = \frac{n}{m} \text{Tr } R_A L_B \end{aligned}$$

for every $A, B \in M_m(\mathbb{C})$. Since the operators $R_A L_B$ linearly span the space of all linear operators on $M_m(\mathbb{C})$, we have

$$\frac{m}{n} \sum_k |W_k\rangle\langle W_k| = I_{m^2}.$$

This is our statement. □

3 Main results

Assume that $\{\mathcal{A}(i)\}_{i=0}^3$ is a family of pairwise quasi-orthogonal subalgebras of $M_4(\mathbb{C})$ which are isomorphic to $M_2(\mathbb{C})$. The commutant of $\mathcal{A}(i)$ will be denoted by $\mathcal{A}(i)'$. Our aim is to describe the relation of the subalgebras $\{\mathcal{A}(i)\}_{i=0}^3$ and $\{\mathcal{A}(i)'\}_{i=0}^3$.

Without restricting the generality, we may assume that $\mathcal{A}(0) = \mathbb{C}I \otimes M_2(\mathbb{C})$. Then the commutant of $\mathcal{A}(0)$ is $\mathcal{A}(0)' = M_2(\mathbb{C}) \otimes \mathbb{C}I$, moreover there are unitaries W_i such that

$$W_i \mathcal{A}(0) W_i^* = \mathcal{A}(i) \quad \text{and} \quad \mathcal{A}(j)' = W_j \mathcal{A}(0)' W_j^* \quad (1 \leq j \leq 3). \quad (3)$$

Theorem 2 *Let \mathcal{A} and \mathcal{B} be quasi-orthogonal subalgebras of $M_4(\mathbb{C})$ which are isomorphic to $M_2(\mathbb{C})$. Then the intersection $\mathcal{A}' \cap \mathcal{B}$ is an at least two dimensional subspace of $M_4(\mathbb{C})$.*

Proof: We may assume that $\mathcal{A} = \mathcal{A}(0) = \mathbb{C}I \otimes M_2$.

The 4×4 matrices

$$C = \begin{bmatrix} a & 0 & 0 & b \\ 0 & c & d & 0 \\ 0 & d & c & 0 \\ b & 0 & 0 & a \end{bmatrix}$$

form a commutative algebra \mathcal{C} . Since

$$\sum_{i=0}^3 c_i \sigma_i \otimes \sigma_i = \begin{bmatrix} c_0 + c_3 & 0 & 0 & c_1 - c_2 \\ 0 & c_0 - c_3 & c_1 + c_2 & 0 \\ 0 & c_1 + c_2 & c_0 - c_3 & 0 \\ c_1 - c_2 & 0 & 0 & c_0 + c_3 \end{bmatrix},$$

\mathcal{C} is the linear span of the matrices $\sigma_i \otimes \sigma_i$, $0 \leq i \leq 3$. (These are the matrices which are diagonal in the so-called Bell basis.)

The algebra \mathcal{C} plays a special role. Any unitary in $M_4(\mathbb{C})$ can be written in the form

$$(L_1 \otimes L_2) N (L_3 \otimes L_4), \quad (4)$$

where L_1, L_2, L_3, L_4 are 2×2 unitaries and the unitary N is in \mathcal{C} . This is called Cartan decomposition, see equation (11) in [11] or [4].

There is a unitary $W \in M_4(\mathbb{C})$ such that

$$W(\mathbb{C}I \otimes M_2(\mathbb{C}))W^* = \mathcal{B}.$$

W has a Cartan decomposition (4). Since the subalgebra $W(\mathbb{C}I \otimes M_2(\mathbb{C}))W^*$ does not depend on L_3 and L_4 , we may assume that $L_3 = L_4 = I$. Moreover, the quasi-orthogonality of $W(\mathbb{C}I \otimes M_2(\mathbb{C}))W^*$ and $\mathbb{C}I \otimes M_2(\mathbb{C})$ does not depend on L_1 and L_2 . The quasi-orthogonality is determined by the factor $N \in \mathcal{C}$. Since the matrices $E_i = \sigma_i/\sqrt{2}$ form a basis in $M_2(\mathbb{C})$, Theorem 1 is conveniently applied for the unitary $N = \sum_{i=0}^3 c_i \sigma_i \otimes \sigma_i$, choose W_i as $c_i \sqrt{2} \sigma_i$. The theorem gives that

$$2 \sum_{i=0}^3 |c_i|^2 |\sigma_i\rangle \langle \sigma_i|$$

is the identity mapping on $M_2(\mathbb{C})$ which implies $|c_i|^2 = 1/4$ ($0 \leq i \leq 3$). In a trigonometric approach, let

$$\begin{aligned} c_0 &= \cos \alpha \cos \beta \cos \gamma + i \sin \alpha \sin \beta \sin \gamma, \\ c_1 &= \cos \alpha \sin \beta \sin \gamma + i \sin \alpha \cos \beta \cos \gamma, \\ c_2 &= \sin \alpha \cos \beta \sin \gamma + i \cos \alpha \sin \beta \cos \gamma, \\ c_3 &= \sin \alpha \sin \beta \cos \gamma + i \cos \alpha \cos \beta \sin \gamma. \end{aligned}$$

In order to get a proper unitary, two of the values of $\cos^2 \alpha, \cos^2 \beta$ and $\cos^2 \gamma$ equal $1/2$ and the third one may be arbitrary. Let \mathcal{N} be the set of all matrices such that the parameters α, β and γ satisfy the above condition, in other words two of the three values are of the form $\pi/4 + k\pi/2$. (k is an integer.) Let

$$\mathcal{N}_1 := \{N \in \mathcal{N} : \alpha \text{ is arbitrary, } \beta = \pi/4 + k_1\pi/2, \text{ and } \gamma = \pi/4 + k_2\pi/2\} \quad (5)$$

and define \mathcal{N}_2 and \mathcal{N}_3 similarly. ($\mathcal{N} = \mathcal{N}_1 \cup \mathcal{N}_2 \cup \mathcal{N}_3$.) Since the subalgebra $N(\mathbb{C}I \otimes M_2(\mathbb{C}))N^*$ does not depend on the integers k_1 and k_2 , we simply take $k_1 = k_2 = 0$. This makes computations a bit more convenient. One computes that

$$N_i(I \otimes \sigma_i)N_i^* = \pm \sigma_i \otimes I$$

for $N_i \in \mathcal{N}_i$ [10]. It follows that

$$(L_1 \otimes L_2)N_i(I \otimes \sigma_i)N_i^*(L_1^* \otimes L_2^*) = \pm L_1\sigma_iL_1^* \otimes I$$

for every unitary $N_i \in \mathcal{N}_i$. Therefore $L_1\sigma_iL_1^* \otimes I \in \mathcal{A}(0)' \cap \mathcal{B}$. \square

The theorem immediately gives that the maximal number of pairwise quasi-orthogonal subalgebras isomorphic to $M_2(\mathbb{C})$ is at most 4. Moreover, if $\{\mathcal{A}(j)\}_{j=0}^3$ are such subalgebras, then each subalgebra $\mathcal{A}(i)' \cap \mathcal{A}(j)$ is two-dimensional for $i \neq j$. Here is an example of 4 such subalgebras together with the commutants, each of them is determined by Pauli triplets:

$$\begin{array}{ccccc} \sigma_0 \otimes \sigma_1 & \sigma_0 \otimes \sigma_2 & \sigma_0 \otimes \sigma_3 & \sigma_1 \otimes \sigma_0 & \sigma_2 \otimes \sigma_0 & \sigma_3 \otimes \sigma_0 \\ \sigma_1 \otimes \sigma_0 & \sigma_2 \otimes \sigma_1 & \sigma_3 \otimes \sigma_1 & \sigma_0 \otimes \sigma_1 & \sigma_1 \otimes \sigma_2 & \sigma_1 \otimes \sigma_3 \\ \sigma_2 \otimes \sigma_0 & \sigma_1 \otimes \sigma_2 & -\sigma_3 \otimes \sigma_2 & \sigma_2 \otimes \sigma_1 & \sigma_2 \otimes \sigma_3 & -\sigma_0 \otimes \sigma_2 \\ \sigma_3 \otimes \sigma_0 & \sigma_1 \otimes \sigma_3 & \sigma_2 \otimes \sigma_3 & \sigma_0 \otimes \sigma_3 & \sigma_3 \otimes \sigma_1 & \sigma_3 \otimes \sigma_2 \end{array} \quad (6)$$

Our next aim is to describe the structure of 4 such algebras in general.

Theorem 3 *Assume that $\{\mathcal{A}(i)\}_{i=0}^3$ is a family of pairwise quasi-orthogonal subalgebras of $M_4(\mathbb{C})$ which are isomorphic to $M_2(\mathbb{C})$. For every $0 \leq i \leq 3$, there exists a Pauli triplet $A(i, j)$ ($j \neq i$) such that $\mathcal{A}(i)' \cap \mathcal{A}(j)$ is the linear span of I and $A(i, j)$. Moreover, the subspace linearly spanned by*

$$I \quad \text{and} \quad \left(\bigcup_{i=0}^3 \mathcal{A}(i) \right)^\perp$$

is a maximal Abelian subalgebra.

Proof: Since the intersection $\mathcal{A}(0)' \cap \mathcal{A}(j)$ is a 2-dimensional commutative subalgebra, we can find a self-adjoint unitary $A(0, j)$ such that $\mathcal{A}(0)' \cap \mathcal{A}(j)$ is spanned by I and $A(0, j) = x(0, j) \cdot \sigma \otimes I$, where $x(0, j) \in \mathbb{R}^3$. Due to the quasi-orthogonality of $\mathcal{A}(1)$, $\mathcal{A}(2)$ and $\mathcal{A}(3)$, the unit vectors $x(0, j)$ are pairwise orthogonal (see (1)). The matrices $A(0, j)$ anti-commute:

$$A(0, i)A(0, j) = i(x(0, i) \times x(0, j)) \cdot \sigma \otimes I = -i(x(0, j) \times x(0, i)) \cdot \sigma \otimes I = -A(0, j)A(0, i)$$

for $i \neq j$. Moreover,

$$A(0, 1)A(0, 2) = i(x(0, 1) \times x(0, 2)) \cdot \sigma$$

$x(0, 1) \times x(0, 2) = \pm x(0, 3)$ because $x(0, 1) \times x(0, 2)$ is orthogonal to both $x(0, 1)$ and $x(0, 2)$. If necessary, we can change the sign of $x(0, 3)$ such that $A(0, 1)A(0, 2) = iA(0, 3)$ holds.

Starting with the subalgebras $\mathcal{A}(1)'$, $\mathcal{A}(2)'$, $\mathcal{A}(3)'$ we can construct similarly the other Pauli triplets. In this way, we arrive at the 4 Pauli triplets, the rows of the following table:

$$\begin{array}{cccc} \star & A(0, 1) & A(0, 2) & A(0, 3) \\ A(1, 0) & \star & A(1, 2) & A(1, 3) \\ A(2, 0) & A(2, 1) & \star & A(2, 3) \\ A(3, 0) & A(3, 1) & A(3, 2) & \star \end{array} \quad (7)$$

When $\{\mathcal{A}(i)\}_{i=0}^4$ is a family of pairwise quasi-orthogonal subalgebras, then the commutants $\{\mathcal{A}(i)'\}_{i=0}^4$ are pairwise quasi-orthogonal as well. $\mathcal{A}(j)'' = \mathcal{A}(j)$ and $\mathcal{A}(i)'$ have nontrivial intersection for $i \neq j$, actually the previously defined $A(i, j)$ is in the intersection. For a fixed j the three unitaries $A(i, j)$ ($i \neq j$) form a Pauli triplet up to a sign. (It follows that changing sign we can always reach the situation where the first three columns of table (7) form Pauli triplets. $A(0, 3)$ and $A(1, 3)$ anti-commute, but it may happen that $A(0, 3)A(1, 3) = -iA(2, 3)$.)

Let $C_0 := \{\pm A(i, j)A(j, i) : i \neq j\} \cup \{\pm I\}$ and $C := C_0 \cup iC_0$. We want to show that C is a commutative group (with respect to the multiplication of unitaries).

Note that the products in C_0 have factors in symmetric position in (7) with respect to the main diagonal indicated by stars. Moreover, $A(i, j) \in \mathcal{A}(j)$ and $A(j, k) \in \mathcal{A}(j)'$, and these operators commute.

We have two cases for a product from C . Taking the product of $A(i, j)A(j, i)$ and $A(u, v)A(v, u)$, we have

$$(A(i, j)A(j, i))(A(u, v)A(v, u)) = I$$

in the simplest case, since $A(i, j)$ and $A(j, i)$ are commuting self-adjoint unitaries. It is slightly more complicated if the cardinality of the set $\{i, j, u, v\}$ is 3 or 4. First,

$$\begin{aligned} (A(1, 0)A(0, 1))(A(3, 0)A(0, 3)) &= A(0, 1)(A(1, 0)A(3, 0))A(0, 3) \\ &= \pm i(A(0, 1)A(2, 0))A(0, 3) \end{aligned}$$

$$= \pm i A(2, 0)(A(0, 1)A(0, 3)) = \pm A(2, 0)A(0, 2),$$

and secondly,

$$\begin{aligned} (A(1, 0)A(0, 1))(A(3, 2)A(2, 3)) &= \pm i A(1, 0)A(0, 2)(A(0, 3)A(3, 2))A(2, 3) \\ &= \pm i A(1, 0)A(0, 2)A(3, 2)(A(0, 3)A(2, 3)) \\ &= \pm A(1, 0)(A(0, 2)A(3, 2))A(1, 3) \\ &= \pm i A(1, 0)(A(1, 2)A(1, 3)) \\ &= \pm A(1, 0)A(1, 0) = \pm I \end{aligned} \tag{8}$$

So the product of any two operators from C is in C .

Now we show that the subalgebra \mathcal{C} linearly spanned by the unitaries $\{A(i, j)A(j, i) : i \neq j\} \cup \{I\}$ is a maximal Abelian subalgebra.

Since we know the commutativity of this algebra, we estimate the dimension. It follows from (8) and the self-adjointness of $A(i, j)A(j, i)$ that

$$A(i, j)A(j, i) = \pm A(k, \ell)A(\ell, k)$$

when i, j, k and ℓ are different. Therefore \mathcal{C} is linearly spanned by $A(0, 1)A(1, 0)$, $A(0, 2)A(2, 0)$, $A(0, 3)A(3, 0)$ and I . These are 4 different self-adjoint unitaries.

Finally, we check that the subalgebra \mathcal{C} is quasi-orthogonal to $\mathcal{A}(i)$.

If the cardinality of the set $\{i, j, k, \ell\}$ is 4, then we have

$$\text{Tr } A(i, j)(A(i, j)A(j, i)) = \text{Tr } A(j, i) = 0$$

and

$$\text{Tr } A(k, \ell)A(i, j)A(j, i) = \pm \text{Tr } A(k, \ell)A(k, \ell)A(\ell, k) = \pm \text{Tr } A(\ell, k) = 0.$$

Moreover, because $\mathcal{A}(k)$ is quasi-orthogonal to $\mathcal{A}(i)$, we also have $A(i, k) \perp A(j, i)$, so

$$\text{Tr } A(i, \ell)(A(i, j)A(j, i)) = \pm i \text{Tr } A(i, k)A(j, i) = 0.$$

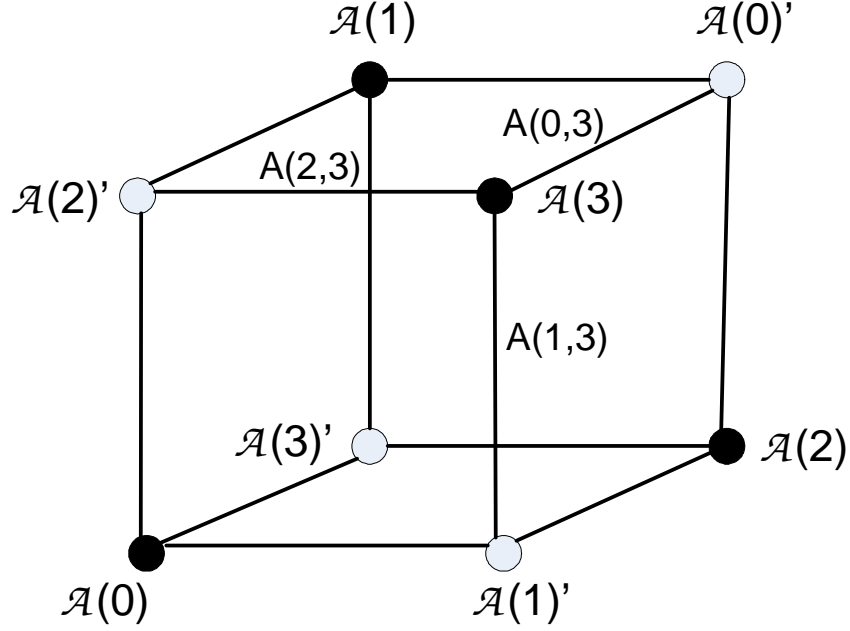
From this we can conclude, that

$$A(k, \ell) \perp A(i, j)A(j, i)$$

for all $k \neq \ell$ and $i \neq j$. □

Finally, we note that there is only one subalgebra of $M_4(\mathbb{C})$ isomorphic to $M_2(\mathbb{C})$ that is quasi-orthogonal to all $\mathcal{A}(i)$, ($i = 0, 1, 2$).

The subalgebras $\{\mathcal{A}(i)\}_{i=0}^2$ determine the matrices $\{A(i, j) : i \neq j, i, j \in \{0, 1, 2\}\}$. Since two anti-commuting matrices define the third element of a Pauli triplet, the matrices $\{A(j, 3)\}_{j \neq 3}$ are also determined. The matrices $\{A(j, 3)\}_{j \neq 3}$ must form a Pauli triplet and fix the fourth subalgebra.



The edges between two vertices represent the one-dimensional traceless intersection of the two subalgebras corresponding two vertices. The three edges starting from a vertex represent a Pauli triplet.

4 Possible extension

Next we consider the pairwise quasi-orthogonal subalgebras $\mathcal{A}_i \simeq M_2(\mathbb{C})$ in $M_{2^n}(\mathbb{C})$. The question is their maximal number $m(n)$.

The traceless subspaces of $M_2(\mathbb{C})$ and $M_{2^n}(\mathbb{C})$ are 3-dimensional and $(4^n - 1)$ -dimensional, respectively. Therefore,

$$m(n) \leq \frac{4^n - 1}{3} =: N_n.$$

Below, we construct $N_n - 1$ pairwise quasi-orthogonal subalgebras. We conjecture that this is the true value of $m(n)$. Theorem 3 contains the case $n = 2$

The Hilbert space $M_{2^n}(\mathbb{C})$ has a natural orthogonal basis

$$\sigma_{i_1} \otimes \sigma_{i_2} \otimes \dots \otimes \sigma_{i_n} =: (i_1, i_2, \dots, i_n),$$

where $i_j = 0, 1, 2, 3$ and $1 \leq j \leq n$. We put

$$P_n = \{(i_1, i_2, \dots, i_n) : 0 \leq i_j \leq 3, 1 \leq j \leq n\} \setminus \{I\}.$$

A triplet $(A_1, A_2, A_3) \in P_n^3$ is called a weak Pauli triplet if $A_1 A_2 = \pm i A_3$. and $(A_1, A_2, A_3) \in P_n^3$ is a commuting triplet if $A_1 A_2 = \pm A_3$. The linear span of elements of a weak Pauli triplet and I is a subalgebra isomorphic to $M_2(\mathbb{C})$.

Assume that $A = (A_1, A_2, A_3) \in P_n^3$ is a commuting triplet. Then we can construct three pairwise disjoint weak Pauli triplets: $\hat{A}^{(1)} := (\sigma_1 \otimes A_1, \sigma_2 \otimes A_2, \sigma_3 \otimes A_3)$ and $\hat{A}^{(2)} := (\sigma_2 \otimes A_1, \sigma_3 \otimes A_2, \sigma_1 \otimes A_3)$ and $\hat{A}^{(3)} := (\sigma_3 \otimes A_1, \sigma_1 \otimes A_2, \sigma_2 \otimes A_3)$ in P_{n+1}^3 . Therefore, to construct pairwise quasi-orthogonal subalgebras isomorphic to $M_2(\mathbb{C})$, it is useful to consider weak Pauli triplets and commuting triplets.

Example 1 There are 5 pairwise disjoint commuting triplets in P_2^3 . Indeed,

$$\begin{aligned} &((0, 1), (1, 0), (1, 1)), \quad ((0, 2), (2, 0), (2, 2)), \quad ((0, 3), (3, 0), (3, 3)), \\ &((1, 2), (2, 3), (3, 1)), \quad ((1, 3), (2, 1), (3, 2)). \end{aligned}$$

There are 21 pairwise disjoint commuting triplets in P_3^3 . Indeed,

$$\begin{aligned} &((1, 0, 1), (2, 0, 3), (3, 0, 2)), \quad ((1, 0, 2), (2, 0, 1), (3, 0, 3)), \quad ((0, 1, 1), (0, 2, 3), (0, 3, 2)), \\ &((0, 1, 3), (0, 1, 0), (0, 0, 3)), \quad ((0, 2, 2), (0, 2, 0), (0, 0, 2)), \quad ((0, 3, 1), (0, 3, 0), (0, 0, 1)), \\ &((3, 2, 1), (3, 0, 0), (0, 2, 1)), \quad ((2, 1, 2), (2, 0, 0), (0, 1, 2)), \quad ((1, 3, 3), (1, 0, 0), (0, 3, 3)), \\ &((3, 3, 1), (2, 3, 2), (1, 0, 3)), \quad ((3, 1, 1), (1, 1, 3), (2, 0, 2)), \quad ((2, 2, 2), (1, 2, 3), (3, 0, 1)), \\ &((1, 1, 1), (2, 2, 1), (3, 3, 0)), \quad ((1, 2, 1), (2, 3, 1), (3, 1, 0)), \quad ((1, 3, 1), (2, 1, 1), (3, 2, 0)), \\ &((1, 1, 2), (2, 2, 0), (3, 3, 2)), \quad ((1, 2, 2), (2, 3, 0), (3, 1, 2)), \quad ((1, 3, 2), (2, 1, 0), (3, 2, 2)), \\ &((1, 1, 0), (2, 2, 3), (3, 3, 3)), \quad ((1, 2, 0), (2, 3, 3), (3, 1, 3)), \quad ((1, 3, 0), (2, 1, 3), (3, 2, 3)). \end{aligned}$$

We show that P_n can be decomposed into commuting triplets.

Theorem 4 For each $n \geq 2$, there is a family of commuting triplets

$$\{A^{(i)} = (A_1^{(i)}, A_2^{(i)}, A_3^{(i)})\}_{i=1}^{N_n} \subset P_n^3$$

such that

$$\bigcup_{i=1}^{N_n} A^{(i)} = P_n.$$

Proof: In the case $n = 2$ and $n = 3$, it is already proven above. Assume it is proven in the case $n = k$, and we consider the case $n = k + 2$. Let $\{A^{(i)}\}_{i=1}^5$ and $\{B^{(j)}\}_{j=1}^{N_k}$ be the family of commuting triplets satisfying the theorem in the case of $n = 2$ and $n = k$, respectively. Then, for each $A^{(i)} = (A_1^{(i)}, A_2^{(i)}, A_3^{(i)})$ and $B^{(j)} = (B_1^{(j)}, B_2^{(j)}, B_3^{(j)})$, we can construct three commuting triplets in P_{k+2}^3 , that is, $(A_1^{(i)} \otimes B_1^{(j)}, A_2^{(i)} \otimes B_2^{(j)}, A_3^{(i)} \otimes B_3^{(j)})$ and $(A_1^{(i)} \otimes B_2^{(j)}, A_2^{(i)} \otimes B_3^{(j)}, A_3^{(i)} \otimes B_1^{(j)})$ and $(A_1^{(i)} \otimes B_3^{(j)}, A_2^{(i)} \otimes B_1^{(j)}, A_3^{(i)} \otimes B_2^{(j)})$. Moreover, we have other commuting triplets, i.e., $(A_1^{(i)} \otimes I_k, A_2^{(i)} \otimes I_k, A_3^{(i)} \otimes I_k)$ and $(I_2 \otimes B_1^{(j)}, I_2 \otimes B_2^{(j)}, I_2 \otimes B_3^{(j)})$. Consequently, we have $5 + N_k + 3 \cdot 5 \cdot N_k = N_{k+2}$ commuting triplets. Since $\bigcup_{i=1}^5 A^{(i)} = P_2$ and $\bigcup_{j=1}^{N_k} B^{(j)} = P_k$, $\{A_1^{(i)}, A_2^{(i)}, A_3^{(i)}\}_{i=1}^5$ and $\{B_1^{(j)}, B_2^{(j)}, B_3^{(j)}\}_{j=1}^{N_k}$ are distinct. Hence, we obtain the union of the above N_{k+2} commuting triplets is P_{k+2} . \square

The good point of this construction is that it is easy to use the induction.

Theorem 5 There exist $N_n - 1$ quasi-orthogonal subalgebras in $M_{2^n}(\mathbb{C})$.

Proof: The case $n = 2$ is already proven in Theorem 3. Assume it is proven for $n = k$, and we consider the case $n = k + 1$.

From Theorem 4, let $\{A^{(i)} = (A_1^{(i)}, A_2^{(i)}, A_3^{(i)})\}_{i=1}^{N_k}$ be commuting triplets in P_k^3 such that $\bigcup_{i=1}^{N_k} A^{(i)} = P_k$. Then we have $3N_k$ pairwise disjoint weak Pauli triplets, that is, $(\sigma_1 \otimes A_1^{(i)}, \sigma_2 \otimes A_2^{(i)}, \sigma_3 \otimes A_3^{(i)})$ and $(\sigma_2 \otimes A_1^{(i)}, \sigma_3 \otimes A_2^{(i)}, \sigma_1 \otimes A_3^{(i)})$ and $(\sigma_3 \otimes A_1^{(i)}, \sigma_1 \otimes A_2^{(i)}, \sigma_2 \otimes A_3^{(i)})$. Furthermore, we obtain another weak Pauli triplet $(\sigma_1 \otimes I_k, \sigma_2 \otimes I_k, \sigma_3 \otimes I_k)$. These $3N_k + 1$ weak Pauli triplets are pairwise disjoint. Moreover, the complement space of above $3N_k + 1$ Pauli triplets is $\mathcal{CI} \otimes M_{2^k}(\mathbb{C})$. Indeed, since $\bigcup_{i=1}^{N_k} A^{(i)} = P_k$, we have

$$\begin{aligned} & \{(\sigma_1 \otimes A_1^{(i)}, \sigma_2 \otimes A_2^{(i)}, \sigma_3 \otimes A_3^{(i)}), (\sigma_2 \otimes A_1^{(i)}, \sigma_3 \otimes A_2^{(i)}, \sigma_1 \otimes A_3^{(i)}), \\ & (\sigma_3 \otimes A_1^{(i)}, \sigma_1 \otimes A_2^{(i)}, \sigma_2 \otimes A_3^{(i)}), (\sigma_1 \otimes I_k, \sigma_2 \otimes I_k, \sigma_3 \otimes I_k) : 1 \leq i \leq N_k\} \\ = & \{\sigma_i \otimes \sigma_{j_1} \otimes \dots \otimes \sigma_{j_k} : i = 1, 2, 3, j_l = 0, 1, 2, 3, 1 \leq l \leq k\}. \end{aligned}$$

Therefore, the complement space is $\mathcal{CI} \otimes M_{2^k}(\mathbb{C})$ spanned by

$$\{\sigma_0 \otimes \sigma_{j_1} \otimes \dots \otimes \sigma_{j_k} : j_l = 0, 1, 2, 3, 1 \leq l \leq k\}.$$

Now we use the assumption that there are $N_k - 1$ pairwise disjoint weak Pauli triplets $B^{(i)} = (B_1^{(i)}, B_2^{(i)}, B_3^{(i)})$ in $M_{2^k}(\mathbb{C})$ ($1 \leq i \leq N_k - 1$). Then

$$(\sigma_0 \otimes B_1^{(i)}, \sigma_0 \otimes B_2^{(i)}, \sigma_0 \otimes B_3^{(i)})$$

give pairwise disjoint weak Pauli triplets in P_{k+1}^3 . Summing up, we have $3N_k + 1 + N_k - 1 = 4N_k = N_{k+1} - 1$ pairwise disjoint weak Pauli triplets. \square

Similarly, we can prove the following. If there exist N_n pairwise quasi-orthogonal subalgebras in $M_{2^n}(\mathbb{C})$ for some n , then there exist N_k pairwise quasi-orthogonal subalgebras in $M_{2^k}(\mathbb{C})$ for all $k \geq n$.

References

- [1] L. Accardi, Some trends and problems in quantum probability, in *Quantum probability and applications to the quantum theory of irreversible processes*, eds. L. Accardi, A. Frigerio and V. Gorini, Lecture Notes in Math. **1055**, pp. 1–19. Springer, 1984.
- [2] S. Bandyopadhyay, P.O. Boykin, V. Roychowdhury and F. Vatan, A new proof for the existence of mutually unbiased bases, *Algoritmica* **34**(2002), 512–528.
- [3] P.O. Boykin, M. Sitharam, P.H. Tiep and P. Wocjan, Mutually unbiased bases and orthogonal decompositions of Lie algebras, arXiv:quant-ph/0506089, 2005.
- [4] D. D'Alessandro and F. Albertini, Quantum symmetries and Cartan decompositions in arbitrary dimensions, quant-ph/0504044, 2005.

- [5] K. Kraus, Complementarity and uncertainty relations, *Phys. Rev. D.* **35**(1987), 3070-3075.
- [6] D. Petz, Complementarity in quantum systems, preprint, 2006, to be published in *Rep. Math. Phys.*
- [7] D. Petz, K.M. Hangos, A. Szántó and F. Szöllősi, State tomography for two qubits using reduced densities, *J. Phys. A: Math. Gen.* **39**(2006), 10901–10907.
- [8] D. Petz and J. Kahn, Complementary reductions for two qubits, *J. Math. Phys.* **48**(2007), 012107.
- [9] A.O. Pittenger and M.H. Rubin, Mutually unbiased bases, generalized spin matrices and separability, *Linear Algebra Appl.* **390**(2004), 255–278.
- [10] A. Szántó, Student report, BUTE, 2006.
- [11] J. Zhang, J. Vala, K.B. Whaley and S. Sastry, A geometric theory of non-local two-qubit operations, *Phys. Rev.* **A67**(2003), 042313.