

Complementary reductions for two qubits

Dénes Petz^{1,3} and Jonas Kahn²

¹ Alfréd Rényi Institute of Mathematics,
H-1053 Budapest, Reáltanoda u. 13-15, Hungary

² Université Paris-Sud 11, Département de Mathématique,
Bat 425, 91405 Orsay Cedex, France

Abstract: Reduction of a state of a quantum system to a subsystem gives partial quantum information about the true state of the total system. In connection with optimal state determination for two qubits, the question was raised about the maximum number of pairwise complementary reductions. The main result of the paper tells that the maximum number is 4, that is, if $\mathcal{A}^1, \mathcal{A}^2, \dots, \mathcal{A}^k$ are pairwise complementary (or quasi-orthogonal) subalgebras of the algebra $M_4(\mathbb{C})$ of all 4×4 matrices and they are isomorphic to $M_2(\mathbb{C})$, then $k \leq 4$. The proof is based on a Cartan decomposition of $SU(4)$. In the way to the main result, contributions are made to the understanding of the structure of complementary reductions.

Key words: Mutually unbiased bases, unbiased measurements, complementary subalgebras, unitaries, Cartan decomposition, Pauli matrices.

1 Introduction

There is an obvious correspondence between bases of an m -dimensional Hilbert space \mathcal{H} and maximal Abelian subalgebras of the algebra $\mathcal{A} \equiv B(\mathcal{H}) \simeq M_m(\mathbb{C})$. Given a basis, the linear operators diagonal in this basis form a maximal Abelian (or commutative) subalgebra. Conversely if $|e_i\rangle\langle e_i|$ are minimal projections in a maximal Abelian subalgebra, then $(|e_i\rangle)_i$ is a basis. From the points of view of quantum mechanics, a basis can be regarded as a measurement. Wootters and Fields argued that two measurements

³Supported by the Hungarian Research Grant OTKA T032662.

corresponding to the bases $\xi_1, \xi_2, \dots, \xi_m$ and $\eta_1, \eta_2, \dots, \eta_m$ yield the largest amount of information about the true state of the system in the average if

$$|\langle \xi_i, \eta_j \rangle|^2 = \frac{1}{m} \quad (1 \leq i, j \leq m),$$

[14]. Two bases satisfying this condition are called **mutually unbiased**. Mutually unbiased bases are interesting from many point of view, for example in quantum information theory, tomography and cryptography [6, 2, 5]. The maximal number of such bases is not known for arbitrary m . Nevertheless, $(m^2 - 1)/(m - 1) = m + 1$ is a bound being checked easily [9, 12].

The concept of mutually unbiased (or complementary) maximal Abelian subalgebras can be extended to more general subalgebras. In particular, a 4-level quantum system can be regarded as the composite system of two qubits, $M_4(\mathbb{C}) \simeq M_2(\mathbb{C}) \otimes M_2(\mathbb{C})$. A density matrix $\rho \in M_4(\mathbb{C})$ describes a state of the composite system and ρ determines the “marginal” or reduced states on both tensor factors. Since the decomposition $M_2(\mathbb{C}) \otimes M_2(\mathbb{C})$ is not unique, there are many reductions to different subalgebras, they provide partial quantum information about the composite system. It seems that the reductions provide the largest amount of information if the corresponding subalgebras are quasi-orthogonal or complementary in a different terminology. In [10] the state ρ was to be determined by its reductions. 4 pairwise complementary subalgebras were given explicitly, but the question remained open to know if 5 such subalgebras exist. The main result of this paper is to prove that at most 4 pairwise complementary subalgebras exist.

2 Preliminaries

In this paper an algebraic approach and language is used. A k -level quantum system is described by operators of the algebra $M_k(\mathbb{C})$ of $k \times k$ matrices. Although the essential part of the paper focuses on a 4-level quantum system, certain concepts can be presented slightly more generally. Let \mathcal{A} be an algebra corresponding to a quantum system. The normalized trace τ gives the Hilbert-Schmidt inner product $\langle A, B \rangle := \tau(B^* A)$ on \mathcal{A} and we can speak about orthogonality with respect to this inner product.

The projections in \mathcal{A} may be defined by the algebraic properties $P = P^2 = P^*$ and the partial ordering $P \leq Q$ means $PQ = QP = P$. We consider subalgebras of \mathcal{A} such that their minimal projections have the same trace. (A maximal Abelian subalgebra and a subalgebra isomorphic to a full matrix algebra have this property.) Let \mathcal{A}^1 and \mathcal{A}^2 be two such subalgebras of \mathcal{A} . Then the following conditions are equivalent:

- (i) If $P \in \mathcal{A}^1$ and $Q \in \mathcal{A}^2$ are minimal projections, then $\text{Tr } PQ = \text{Tr } P \text{Tr } Q$.
- (ii) The traceless subspaces of \mathcal{A}^1 and \mathcal{A}^2 are orthogonal with respect to the Hilbert-Schmidt inner product on \mathcal{A} .

The subalgebras \mathcal{A}^1 and \mathcal{A}^2 are called **complementary** (or quasi-orthogonal) if these conditions hold. This terminology was used in the maximal Abelian case [1, 6, 8, 9] and the case of noncommutative subalgebras appeared in [10]. More details about complementarity are presented in [11].

Given a density matrix $\rho \in \mathcal{A}$, its reduction $\rho_1 \in \mathcal{A}_1$ to the subalgebra $\mathcal{A}_1 \subset \mathcal{A}$ is determined by the formula

$$\mathrm{Tr} \rho A = \mathrm{Tr} \rho_1 A \quad (A \in \mathcal{A}_1).$$

In most cases ρ_1 is given by the partial trace but an equivalent way is based on the conditional expectation [3]. The orthogonal projection $E : \mathcal{A} \rightarrow \mathcal{A}_1$ is called conditional expectation. $\rho_1 = E(\rho)$ and

$$E(AB) = AE(B) \quad (A \in \mathcal{A}_1, B \in \mathcal{A})$$

is an important property.

The situation we are interested in is the algebra $M_4(\mathbb{C})$. In the paper $M_4(\mathbb{C})$ is regarded as a Hilbert space with respect to the inner product

$$\langle A, B \rangle = \frac{1}{4} \mathrm{Tr} A^* B = \tau(A^* B). \quad (1)$$

$M_4(\mathbb{C})$ has a natural orthonormal basis:

$$\sigma_i \otimes \sigma_j \quad (0 \leq i, j \leq 3),$$

where $\sigma_1, \sigma_2, \sigma_3$ are the Pauli matrices and σ_0 is the identity I :

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

3 Complementary subalgebras

Any subalgebra \mathcal{A}^1 of $M_4(\mathbb{C})$ isomorphic to $M_2(\mathbb{C})$ can be written $\mathbb{C}I \otimes M_2(\mathbb{C})$ in some basis, hence there is a unitary operator W such that $\mathcal{A}^1 = W(\mathbb{C}I \otimes M_2(\mathbb{C}))W^*$.

This section is organized as follows: we first give a characterization of the W such that \mathcal{A}^1 is complementary to $\mathcal{A}^0 = W(\mathbb{C}I \otimes M_2(\mathbb{C}))W^*$ (Theorem 1 for a general form and Theorem 2 for a form specific to our problem). The second stage consists in proving, using the form of W , that any such \mathcal{A}^1 has “a large component” along $\mathcal{B} = M_2(\mathbb{C}) \otimes \mathbb{C}I$. Theorem 3 gives the precise formulation. It entails that no more than four complementary subalgebras can be found (Theorem 4), which was our initial aim, and hence is our conclusion.

Although our main interest is $M_4(\mathbb{C})$, our first theorem is more general. E_{ij} stand for the matrix units.

Theorem 1 Let $W = \sum_{i,j=1}^n E_{ij} \otimes W_{ij} \in M_n(\mathbb{C}) \otimes M_n(\mathbb{C})$ be a unitary. The subalgebra $W(\mathbb{C}I \otimes M_n(\mathbb{C}))W^*$ is complementary to $\mathbb{C}I \otimes M_n(\mathbb{C})$ if and only if $\{W_{ij} : 1 \leq i, j \leq n\}$ is an orthonormal basis in $M_n(\mathbb{C})$ (with respect to the inner product $\langle A, B \rangle = \text{Tr} A^* B$).

Proof: Assume that $\text{Tr} B = 0$. Then the condition

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

is equivalently written as

$$\text{Tr} W(I \otimes A)W^*(I \otimes B) = \sum_{i,j=1}^n \text{Tr} W_{ij} A W_{ij}^* B = 0.$$

This implies

$$\sum_{i,j=1}^n \text{Tr} W_{ij} A W_{ij}^* B = (\text{Tr} A)(\text{Tr} B). \quad (2)$$

We can transform this into another equivalent condition in terms of the left multiplication and right multiplication operators. For $A, B \in M_n(\mathbb{C})$, the operator R_A is the right multiplication by A and L_B is the left multiplication by B : $R_A, L_B : M_n(\mathbb{C}) \rightarrow M_n(\mathbb{C})$, $R_B X = XB$, $L_A X = AX$. Equivalently, $L_A |e\rangle\langle f| = |Ae\rangle\langle f|$ and $R_B |e\rangle\langle f| = |e\rangle\langle B^* f|$. From the latter definition one can deduce that $\text{Tr} R_A L_B = \text{Tr} A \text{Tr} B$. Let $|e_i\rangle$ be a basis. Then $|e_i\rangle\langle e_j|$ form a basis in $M_n(\mathbb{C})$ and

$$\begin{aligned} \text{Tr} R_A L_B &= \sum_{ij} \langle |e_i\rangle\langle e_j|, R_A L_B |e_i\rangle\langle e_j| \rangle = \sum_{ij} \langle |e_i\rangle\langle e_j|, |B e_i\rangle\langle A^* e_j| \rangle \\ &= \sum_{ij} \langle e_i, B e_i \rangle \langle e_j, A e_j \rangle. \end{aligned}$$

The equivalent form of (2) is the equation

$$\sum_{i,j=1}^n \langle W_{ij}, R_A L_B W_{ij} \rangle = \text{Tr} A \text{Tr} B = \text{Tr} R_A L_B$$

for every $A, B \in M_n(\mathbb{C})$. Since the operators $R_A L_B$ linearly span the space of all linear operators on $M_n(\mathbb{C})$, we can conclude that W_{ij} form an orthonormal basis. \square

We shall call any unitary satisfying the condition in the previous theorem a useful unitary and we shall denote the set of all $n^2 \times n^2$ useful unitaries by $\mathcal{M}(n^2)$.

We try to find a useful 4×4 unitary W , that is we require that the subalgebra

$$W \begin{bmatrix} A & 0 \\ 0 & A \end{bmatrix} W^* \quad (A \in M_2(\mathbb{C}))$$

is complementary to $\mathcal{A}^0 \equiv \mathbb{C}I \otimes M_2(\mathbb{C})$. We shall use the **Cartan decomposition** of W given by

$$W = (L_1 \otimes L_2) N (L_3 \otimes L_4),$$

where L_1, L_2, L_3 and L_4 are 2×2 unitaries and

$$N = \exp(\alpha i \sigma_1 \otimes \sigma_1) \exp(\beta i \sigma_2 \otimes \sigma_2) \exp(\gamma i \sigma_3 \otimes \sigma_3) \quad (3)$$

is a 4×4 unitary in a special form, see equation (11) in [13] or [4]. The subalgebra

$$W(\mathbb{C}I \otimes M_2(\mathbb{C}))W^* = (L_1 \otimes L_2)N(\mathbb{C}I \otimes M_2(\mathbb{C}))N^*(L_1^* \otimes L_2^*)$$

does not depend on L_3 and L_4 , therefore we may assume that $L_3 = L_4 = I$.

The orthogonality of $\mathbb{C}I \otimes M_2(\mathbb{C})$ and $W(\mathbb{C}I \otimes M_2(\mathbb{C}))W^*$ does not depend on L_1 and L_2 . Therefore, the equations

$$\text{Tr } N(I \otimes \sigma_i)N^*(I \otimes \sigma_j) = 0$$

should be satisfied, $1 \leq i, j \leq 3$. We know from Theorem 1 that these conditions are equivalent to the property that the matrix elements of N form a basis.

A simple computation gives that

$$N = \sum_{i=0}^3 c_i \sigma_i \otimes \sigma_i,$$

where

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

Therefore, we have

$$\begin{aligned} N &= \begin{bmatrix} c_0 + c_3 & 0 & 0 & c_1 - c_2 \\ 0 & c_0 - c_3 & c_1 + c_2 & 0 \\ 0 & c_1 + c_2 & c_0 - c_3 & 0 \\ c_1 - c_2 & 0 & 0 & c_0 + c_3 \end{bmatrix} \\ &= \begin{bmatrix} e^{i\gamma} \cos(\alpha - \beta) & 0 & 0 & ie^{i\gamma} \sin(\alpha - \beta) \\ 0 & e^{-i\gamma} \cos(\alpha + \beta) & ie^{-i\gamma} \sin(\alpha + \beta) & 0 \\ 0 & ie^{-i\gamma} \sin(\alpha + \beta) & e^{-i\gamma} \cos(\alpha + \beta) & 0 \\ ie^{i\gamma} \sin(\alpha - \beta) & 0 & 0 & e^{i\gamma} \cos(\alpha - \beta) \end{bmatrix}. \quad (4) \end{aligned}$$

Since the 2×2 blocks form a basis (see Theorem 1), we have

$$\begin{aligned} \overline{(c_0 + c_3)}(c_0 - c_3) + \overline{(c_0 - c_3)}(c_0 + c_3) &= 0, \\ \overline{(c_1 - c_2)}(c_1 + c_2) + \overline{(c_1 + c_2)}(c_1 - c_2) &= 0, \\ |c_0 + c_3|^2 + |c_0 - c_3|^2 &= 1, \end{aligned}$$

$$|c_1 + c_2|^2 + |c_1 - c_2|^2 = 1.$$

These equations give

$$|c_0|^2 = |c_1|^2 = |c_2|^2 = |c_3|^2 = \frac{1}{4}$$

and we arrive at the following solution. 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.)

The conclusion of the above argument can be formulated as follows.

Theorem 2 $W \in \mathcal{M}(4)$ if and only if $W = (L_1 \otimes L_2)N(L_3 \otimes L_4)$, where L_i are 2×2 unitaries ($1 \leq i \leq 4$) and $N \in \mathcal{N}$.

We now turn to the “second stage”, that is proving that any such $W(CI \otimes M_2(\mathbb{C}))$ is far from being complementary to $M_2(\mathbb{C}) \otimes CI$. To get a quantitative result (Theorem 3), recall that we consider $M_4(\mathbb{C})$ as a Hilbert space with Hilbert-Schmidt inner product (see (1)). For the proof of Theorem 3, we shall need the following obvious lemma:

Lemma 1 Let \mathcal{K}_1 and \mathcal{K}_2 be subspaces of a Hilbert space \mathcal{K} and denote by $\mathbf{P}_i : \mathcal{K} \rightarrow \mathcal{K}_i$ the orthogonal projection onto \mathcal{K}_i ($i = 1, 2$). If $\xi_1, \xi_2, \dots, \xi_r$ is an orthonormal basis in \mathcal{K}_1 and $\eta_1, \eta_2, \dots, \eta_s$ is such a basis in \mathcal{K}_2 , then

$$\text{Tr } \mathbf{P}_1 \mathbf{P}_2 = \sum_{i,j} |\langle \xi_i, \eta_j \rangle|^2.$$

□

Theorem 3 Let $\mathcal{A}^0 \equiv CI \otimes M_2(\mathbb{C})$ and $\mathcal{B} \equiv M_2(\mathbb{C}) \otimes CI$. Assume that the subalgebra $\mathcal{A}^1 \subset M_2(\mathbb{C}) \otimes M_2(\mathbb{C})$ is isomorphic to $M_2(\mathbb{C})$ and complementary to \mathcal{A}^0 . If \mathbf{P} is the orthogonal projection onto the traceless subspace of \mathcal{A}^1 and \mathbf{Q} is the orthogonal projection onto the traceless subspace of \mathcal{B} , then

$$\text{Tr } \mathbf{P} \mathbf{Q} \geq 1.$$

Proof: There is a unitary $W = (L_1 \otimes L_2)N$ such that $\mathcal{A}^1 = W \mathcal{A}^0 W^*$, L_1, L_2 are 2×2 unitaries and $N \in \mathcal{M}(4)$. In the traceless subspace of \mathcal{B} ,

$$(L_1 \sigma_i L_1^*) \otimes I \quad (1 \leq i \leq 3)$$

form a basis, while

$$(L_1 \otimes L_2)N(I \otimes \sigma_i)N^*(L_1^* \otimes L_2^*) \quad (1 \leq i \leq 3)$$

is a basis in the traceless part of \mathcal{A}^1 . Therefore, we have to show

$$\sum_{i,j} \left| \langle (L_1 \otimes L_2)N(I \otimes \sigma_i)N^*(L_1^* \otimes L_2^*), L_1^* \sigma_j L_1 \otimes I \rangle \right|^2 = \left(\tau(N(I \otimes \sigma_i)N^*(\sigma_j \otimes I)) \right)^2 \geq 1.$$

In the computation we can use the conditional expectation $E : M_4(\mathbb{C}) \rightarrow \mathcal{B}$. Recall that it is defined as the linear operator which sends $\sigma_i \otimes \sigma_j$ to $\sigma_i \otimes I$, for all $0 \leq i, j \leq 3$.

Two of its main properties are that it preserves τ , and that $E(AB) = E(A)B$ when $B \in \mathcal{B}$. Hence

$$\tau\left(N(I \otimes \sigma_i)N^*(\sigma_j \otimes I)\right) = \tau\left(E\left(N(I \otimes \sigma_i)N^*\right)(\sigma_j \otimes I)\right).$$

Elementary computation in the basis $\sigma_i \otimes \sigma_j$ gives the following formulas:

$$\begin{aligned} E(N(I \otimes \sigma_1)N^*) &= \sin 2\beta \sin 2\gamma (\sigma_1 \otimes I), \\ E(N(I \otimes \sigma_2)N^*) &= \sin 2\alpha \sin 2\gamma (\sigma_2 \otimes I), \\ E(N(I \otimes \sigma_3)N^*) &= \sin 2\alpha \sin 2\beta (\sigma_2 \otimes I), \end{aligned}$$

where α, β and γ are from (3) and (4). Therefore,

$$\text{Tr } \mathbf{P}\mathbf{Q} = \sin^2 2\beta \sin^2 2\gamma + \sin^2 2\alpha \sin^2 2\gamma + \sin^2 2\alpha \sin^2 2\beta.$$

Recall that two of the parameters α, β and γ have rather concrete values, hence one of the three terms equals 1, and the proof is complete. \square

Our main results says that there are at most four pairwise complementary subalgebras of $M_4(\mathbb{C})$ if they are assumed to be isomorphic to $M_2(\mathbb{C})$. Given such a family of subalgebras, we may assume that the above defined \mathcal{A}^0 belongs to the family.

Theorem 4 *Assume that $\mathcal{A}^0 \equiv \mathbb{C}I \otimes M_2(\mathbb{C})$, $\mathcal{A}^1, \dots, \mathcal{A}^r$ are pairwise complementary subalgebras of $M_4(\mathbb{C})$ and they are isomorphic to $M_2(\mathbb{C})$. Then $r \leq 3$.*

Proof: Let \mathbf{P}_i be the orthogonal projection onto the traceless subspace of \mathcal{A}^i from $M_4(\mathbb{C})$, $1 \leq i \leq r$. Under these conditions $\sum_i \mathbf{P}_i \leq I$. As in Theorem 3, let \mathbf{Q} the orthogonal projection on the traceless subspace of $\mathcal{B} \equiv M_2(\mathbb{C}) \otimes \mathbb{C}I$. The estimate

$$3 = \text{Tr } \mathbf{Q} \geq \text{Tr} (\mathbf{P}_1 + \mathbf{P}_2 + \dots + \mathbf{P}_r)\mathbf{Q} = \sum_{i=1}^r \text{Tr } \mathbf{P}_i\mathbf{Q} \geq r$$

yields the proof. \square

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, *Algorithmica* **34**, 512–528, 2002.

- [3] P. Busch, P.J. Lahti and P. Mittelstaedt, *The Quantum Theory of Measurement*, Lecture Notes in Physics m2, Springer, 1991.
- [4] D. D'Alessandro and F. Albertini, Quantum symmetries and Cartan decompositions in arbitrary dimensions, quant-ph/0504044, 2005.
- [5] G. Kimura, H. Tanaka and M. Ozawa, Solution to the Mean King's problem with mutually unbiased bases for arbitrary levels, Phys. Rev. A **73**, 050301(R), 2006.
- [6] K. Kraus, Complementarity and uncertainty relations, Phys. Rev. D. **35**, 3070–3075, 1987.
- [7] H. Maasen and I. Uffink, Generalized entropic uncertainty relations, Phys. Rev. Lett. **60**(1988), 1103–1106.
- [8] M. Ohya and D. Petz, *Quantum Entropy and Its Use*, Springer-Verlag, Berlin, 1993, 2nd ed. 2004.
- [9] K.R. Parthasarathy, On estimating the state of a finite level quantum system, Infin. Dimens. Anal. Quantum Probab. Relat. Top. **7**, 607–617. 2004.
- [10] D. Petz, K.M. Hangos, A. Szántó and F. Szöllösi, State tomography for two qubits using reduced densities, J. Phys. A: Math. Gen. **39**, 10901–10907, 2006.
- [11] D. Petz, Complementarity in quantum systems, Rep. Math. Phys. **59**(2007), 209–224.
- [12] A. O. Pittenger and M. H. Rubin, Generalized spin matrices and separability, Linear Alg. Appl. **390**, 255–278, 2004.
- [13] J. Zhang, J. Vala, K.B. Whaley and S. Sastry, A geometric theory of non-local two-qubit operations, Phys. Rev. A **67**, 042313, 2003.
- [14] W.K. Wootters and B.D. Fields, Optimal state determination by mutually unbiased measurements, Annals of Physics, **191**, 363–381, 1989.