

Complementarity and the algebraic structure of finite quantum systems

Dénes Petz

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

E-mail: petz@math.bme.hu

Abstract. Complementarity is a very old concept in quantum mechanics, however the rigorous definition is not so old. Complementarity of orthogonal bases can be formulated in terms of maximal Abelian algebras and this may lead to avoid commutativity of the subalgebras. In some sense this means that quantum information is treated instead of classical (measurement) information. The subject is to extend to the quantum case some features from the classical case. This includes construction of complementary subalgebras. The Bell basis has also some relation. Several open questions are discussed.

1. Introduction

The origin of complementarity is historically connected with the non-commutativity of operators describing observables in quantum theory. Although the concept was born together with quantum mechanics itself, the rigorous definition was given much later. Complementary bases or complementary measurements give maximal information about the quantum system. Complementarity is also used, for example, in state estimation [14, 24] and in quantum cryptography [2]. When non-classical, say quantum, information is considered, then non-commutative subalgebras or subsystems of the total system should be regarded. The study of complementary non-commutative subalgebras is rather recent [16].

Complementarity appeared in the history of quantum mechanics in the early days of the theory. According to *Wolfgang Pauli*, the new quantum theory could have been called the theory of complementarity [13]. This fact shows the central importance of the notion of complementarity in the foundations of quantum mechanics. Unfortunately, the importance did not make clear what the concept really means. The idea of complementarity was in connection with uncertainty relation and measurement limitations. Wolfgang Pauli wrote to *Werner Heisenberg* in 1926: “*One may view the world with the p -eye and one may view it with the q -eye but if one opens both eyes simultaneously then one gets crazy*”. The distinction between incompatible and complementary observables was not really discussed. This can be the reason that “complementarity” was avoided in the book [7] of *John von Neumann*, although the mathematical foundations of quantum theory were developed in a generally accepted way. The concept of complementarity was not clarified for many years, but it was accepted that the pair of observables of position and momentum must be a typical and important example (when complementarity means a relation of observables).

The canonically conjugate position and momentum, Q and P , are basic observables satisfying the commutation relation,

$$(QP - PQ)f = if \quad (f \in \mathcal{D})$$

which holds on a dense domain \mathcal{D} (for example, on the Schwartz functions in $L^2(\mathbb{R})$). The uncertainty relation,

$$\Delta(Q, f) \Delta(P, f) \geq \frac{1}{2} \quad (f \in \mathcal{D})$$

holds on the same domain. (Recall that the variance of the observable A in the vector state f is defined as $\Delta(A, f)^2 = \langle f, A^2 f \rangle - \langle f, A f \rangle^2$.)

The Fourier transform $\mathcal{F} : L^2(\mathbb{R}) \rightarrow L^2(\mathbb{R})$ is a unitary and makes a connection $P = \mathcal{F}^{-1}Q\mathcal{F}$ between P and Q . This extends also to the spectral measures $E^P(\cdot)$ and $E^Q(\cdot)$, so that one has

$$E^P(H) = \mathcal{F}^{-1}E^Q(H)\mathcal{F}$$

for all Borel sets $H \subset \mathbb{R}$. From the Fourier relation one can deduce that

$$\text{Tr } E^P(H_1)E^Q(H_2) = \frac{1}{2\pi} \lambda(H_1)\lambda(H_2) \quad (1)$$

for all bounded intervals $H_1, H_2 \subset \mathbb{R}$ with length $\lambda(H_1)$ and $\lambda(H_2)$. Note that the operators P and Q do not have eigenvectors and the connection (1) can be called complementarity. Since this paper concentrate on finite dimensional Hilbert spaces, P and Q are not discussed here, but we refer to the paper [4].

Herman Weyl used the finite Fourier transform to approximate the relation of P and Q in finite dimensional Hilbert spaces [25]. Let $|0\rangle, |1\rangle, \dots, |n-1\rangle$ be an orthonormal basis in an n -dimensional Hilbert space. The transformation

$$V_n : |i\rangle \mapsto \frac{1}{\sqrt{n}} \sum_{j=0}^{n-1} \omega^{ij} |j\rangle \quad (\omega = e^{2\pi i/n}) \quad (2)$$

is a unitary and it is nowadays called quantum Fourier transform. If the operator $A = \sum_i \lambda_i |e_i\rangle\langle e_i|$ is diagonal in the given basis and $B = V_n^* A V_n$, then the pair (A, B) approximates (Q, P) when the eigenvalues are chosen properly.

The complementarity of observables of a finite quantum system was emphasized by Accardi in 1983 during the Villa Mondragone conference [1]. His approach is based on conditional probabilities. If an observable is measured on a copy of a quantum system and another observables is measured on another copy (prepared in the same state), then one measurement does not help to guess the outcome of the other measurement, if all conditional probabilities are the same. If the eigenvectors of the first observable are ξ_i 's, the eigenvectors of the second one are η_j 's and the dimension of the Hilbert space is n , then complementarity means

$$|\langle \xi_i, \eta_j \rangle| = \frac{1}{\sqrt{n}}. \quad (3)$$

It is clear that the complementarity of two observables is actually the property of the two eigenbases, so it is better to speak about complementary bases. The Fourier transform (2) moves the standard basis $|0\rangle, |1\rangle, \dots, |n-1\rangle$ to a complementary basis $V_n|0\rangle, V_n|1\rangle, \dots, V_n|n-1\rangle$. The complementarity (3) is often called value complementarity and it was an important subject in the work of Schwinger [21, 22, 19].

2. From mutually unbiased bases to complementary subalgebras

Let \mathcal{H} be an n -dimensional Hilbert space with an orthonormal basis e_1, e_2, \dots, e_n . A unit vector $\xi \in \mathcal{H}$ is complementary with respect to the given basis e_1, e_2, \dots, e_n if

$$|\langle \xi, e_i \rangle| = \frac{1}{\sqrt{n}} \quad (1 \leq i \leq n). \quad (4)$$

(4) is equivalent to the formulation that the vector state $|\xi\rangle\langle\xi|$ gives the uniform distribution when the measurement $|e_1\rangle\langle e_1|, \dots, |e_n\rangle\langle e_n|$ is performed:

$$\text{Tr} |\xi\rangle\langle\xi| |e_i\rangle\langle e_i| = \frac{1}{n} \quad (1 \leq i \leq n).$$

When the Hilbert space \mathcal{H} is a tensor product $\mathcal{H}_1 \otimes \mathcal{H}_2$, then a unit vector complementary to a product basis is called maximally entangled state. (If a vector is complementary to a product basis, then it is complementary to any other product basis.) When $\dim \mathcal{H}_1 = \dim \mathcal{H}_2 = 2$, then the Bell basis

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \quad \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \quad \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \quad (5)$$

consists of maximally entangled states.

The goal of state determination is to recover the state of a quantum system by measurements. If the Hilbert space is n dimensional, then the density matrix of a state contains $n^2 - 1$ real parameters. If a measurement is repeated on many copies of the same system, then $n - 1$ parameters can be estimated. Therefore, at least $n + 1$ different measurement should be performed to estimate the $n^2 - 1$ parameters. A measurement (described by minimal orthogonal projections) can be identified with a basis. *Wootters* and *Fields* argued that in the optimal estimation scheme the $n + 1$ bases must be pairwise complementary [24]. Instead of pairwise complementary bases, Wootters and Fields used the expression ‘‘mutually unbiased bases’’ and this terminology has become popular. A different kind of optimality of the complementary bases was obtained in [15] in terms of the determinant of the average mean quadratic error matrix.

In case of a 2-level system, the three Pauli observables

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

can be used for several purposes. For example, the Bloch parametrization of the state space

$$\rho_\theta = \frac{1}{2}(I + \theta \cdot \sigma) = \frac{1}{2} \begin{bmatrix} 1 + \theta_3 & \theta_1 - i\theta_2 \\ \theta_1 + i\theta_2 & 1 - \theta_3 \end{bmatrix}, \quad (6)$$

is convenient. The Pauli observables are pairwise complementary: If ξ is an eigenvector of σ_i and η is an eigenvector of σ_j with $i \neq j$, then $|\langle \xi, \eta \rangle|^2 = 1/2$.

Let $\mathbf{u}(1)$, $\mathbf{u}(2)$ and $\mathbf{u}(3)$ be unit vectors in \mathbb{R}^3 and consider the observables

$$A(i) = \mathbf{u}(i) \cdot \sigma \quad (1 \leq i \leq 3)$$

for measurement. If each of them is measured r times and the relative frequency is $\nu(i)_r$ for the outcome 1 of $A(i)$, then

$$\hat{\theta} = 2T^{-1}(\nu(1)_r, \nu(2)_r, \nu(3)_r)^t - T^{-1}\mathbf{1} \quad (7)$$

is an estimate, where

$$T = \begin{bmatrix} \mathbf{u}(1)_1 & \mathbf{u}(1)_2 & \mathbf{u}(1)_3 \\ \mathbf{u}(2)_1 & \mathbf{u}(2)_2 & \mathbf{u}(2)_3 \\ \mathbf{u}(3)_1 & \mathbf{u}(3)_2 & \mathbf{u}(3)_3 \end{bmatrix}$$

is the transpose of the basis transformation. The eigenbases of the Pauli matrices are mutually unbiased and the eigenbases of $A(1)$, $A(2)$ and $A(3)$ are so if T is an orthogonal matrix. For the above estimate, the mean quadratic error matrix is

$$V^{(1)}(\theta) = 4T^{-1} \begin{bmatrix} 1 - (\mathbf{u}(1) \cdot \theta)^2 & 0 & 0 \\ 0 & 1 - (\mathbf{u}(2) \cdot \theta)^2 & 0 \\ 0 & 0 & 1 - (\mathbf{u}(3) \cdot \theta)^2 \end{bmatrix} (T^{-1})^*$$

which can be averaged with respect to the Lebesgue measure on the Bloch ball (or any other rotation invariant measure), see [15].

Theorem 1 *The determinant of the average mean quadratic error matrix is the smallest, if the vectors $\mathbf{u}(1)$, $\mathbf{u}(2)$ and $\mathbf{u}(3)$ are orthogonal, that is, the observables $A(1)$, $A(2)$ and $A(3)$ are complementary.*

The content of the theorem is similar to the result of [24], however in the approach of Wootters and Field not the mean quadratic error was minimized but the information gain was maximized. The complementary (or unbiased) measurements are optimal from both viewpoints. Similar result holds in higher dimensions, as well.

Relation (4) can be reformulated in terms of the generated subalgebras. The unital subalgebra generated by $|\xi\rangle\langle\xi|$ consists of operators $\lambda|\xi\rangle\langle\xi| + \mu|\xi\rangle\langle\xi|^\perp$ ($\lambda, \mu \in \mathbb{C}$), while the algebra generated by the orthogonal projections $|e_i\rangle\langle e_i|$ is $\{\sum_i \lambda_i |e_i\rangle\langle e_i| : \lambda_i \in \mathbb{C}\}$. Relation (4) can be reformulated in terms of these generated subalgebras.

Theorem 2 *Let \mathcal{A}_1 and \mathcal{A}_2 be subalgebras of $M_k(\mathbb{C})$ and let $\tau := \text{Tr}/k$ be the normalized trace. Then the following conditions are equivalent:*

- (i) *If $P \in \mathcal{A}_1$ and $Q \in \mathcal{A}_2$ are minimal projections, then $\tau(PQ) = \tau(P)\tau(Q)$.*
- (ii) *The subalgebras \mathcal{A}_1 and \mathcal{A}_2 are quasi-orthogonal in $M_n(\mathbb{C})$, that is the subspaces $\mathcal{A}_1 \ominus \mathbb{C}I$ and $\mathcal{A}_2 \ominus \mathbb{C}I$ are orthogonal.*
- (iii) *$\tau(\mathcal{A}_1\mathcal{A}_2) = \tau(\mathcal{A}_1)\tau(\mathcal{A}_2)$ if $A_1 \in \mathcal{A}_1$, $A_2 \in \mathcal{A}_2$.*
- (iv) *If $E_1 : \mathcal{A} \rightarrow \mathcal{A}_1$ is the trace preserving conditional expectation, then E_1 restricted to \mathcal{A}_2 is a linear functional (times I).*

This theorem was formulated in [16] and led to the concept of complementary subalgebras. Namely \mathcal{A}_1 and \mathcal{A}_2 are complementary if the conditions of the theorem hold. As we explained above complementary maximal Abelian subalgebras is a popular subject in the form of the corresponding bases. We note that complementary MASA's was studied also in von Neumann algebras [20]

Let \mathcal{A} and \mathcal{B} be maximal Abelian subalgebras of the algebra $M_n(\mathbb{C})$ of $n \times n$ matrices. Set

$$c^2 := \sup \{ \text{Tr} PQ : P \in \mathcal{A}, Q \in \mathcal{B} \text{ are minimal projections} \} \quad (8)$$

and for a density matrix ω let ω_A and ω_B be the reduced densities in \mathcal{A} and in iB . The uncertainty relation conjectured by Krauss and proven by Maasen and Uffink [6] is the inequality

$$S(\omega_A) + S(\omega_B) \geq -2 \log c. \quad (9)$$

for the von Neumann entropies $S(\omega_{\mathcal{A}})$ and $S(\omega_{\mathcal{B}})$. The lower bound is the largest if c^2 is the smallest. Since $n^2 c^2 \geq n$, the smallest value of c^2 is $1/n$. This happens if and only if \mathcal{A} and \mathcal{B} are complementary. Similar inequality for non-commutative subalgebras is not known.

Two orthonormal bases are connected by a unitary. It is quite obvious that two bases are mutually unbiased if and only if the absolute value of the elements of the transforming unitary is the same, $1/\sqrt{n}$ when n is the dimension. This implies that construction of mutually unbiased bases is strongly related (or equivalent) to the search for Hadamard matrices [23].

Let \mathcal{A}_1 and \mathcal{A}_2 be subalgebras of $M_k(\mathbb{C})$ and assume that both subalgebras are isomorphic to $M_m(\mathbb{C})$. Then $k = mn$ and we can assume that $\mathcal{A}_1 = \mathbb{C}I_n \otimes M_m(\mathbb{C})$. There exists a unitary W such that $W\mathcal{A}_1W^* = \mathcal{A}_2$. The next theorem characterizes W when \mathcal{A}_1 and \mathcal{A}_2 are complementary [10, 16]. (On the matrices the Hilbert-Schmidt inner product $\langle A, B \rangle = \text{Tr } A^*B$ is considered.)

Theorem 3 *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 $W(\mathbb{C}I_n \otimes M_m(\mathbb{C}))W^*$ is complementary 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 $M_m(\mathbb{C})$.

The condition in the Theorem 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 $M_m(\mathbb{C})$.

Example 1 Consider the unitary $W = V_{n^2}$ defined in (2) as an $n \times n$ block-matrix with entries from $M_n(\mathbb{C})$. Then the entries form an orthonormal basis in $M_n(\mathbb{C})$ and Theorem 3 tells us that the Fourier transform can be used to construct a complementary pair.

It is remarkable that the Fourier transform sends the standard basis into a complementary one but it can produce non-commutative complementary subalgebras as well. \square

A different method for the construction of complementary subalgebras is indicated in the next example.

Example 2 Assume that $p > 2$ is prime. Let e_0, e_1, \dots, e_{p-1} be a basis and let X be the unitary operator permuting the basis vectors cyclically:

$$Xe_i = \begin{cases} e_{i+1} & \text{if } 0 \leq i \leq p-2, \\ e_0 & \text{if } i = p-1. \end{cases}$$

Let $q := e^{i2\pi/p}$ and define another unitary by $Ze_i = q^i e_i$. Their matrices are as follows.

$$X = \begin{bmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & q & 0 & \cdots & 0 \\ 0 & 0 & q^2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & q^{p-1} \end{bmatrix}.$$

It is easy to check that $ZX = qXZ$ or more generally the relation

$$(X^{k_1} Z^{\ell_1})(X^{k_2} Z^{\ell_2}) = q^{k_2 \ell_1} X^{k_1+k_2} Z^{\ell_1+\ell_2}. \quad (10)$$

is satisfied. The unitaries

$$\{X^j Z^k : 0 \leq j, k \leq p-1\}$$

are pairwise orthogonal.

For $0 \leq k_1, \ell_1, k_2, \ell_2 \leq p-1$ set

$$\pi(k_1, \ell_1, k_2, \ell_2) = X^{k_1} Z^{\ell_1} \otimes X^{k_2} Z^{\ell_2}.$$

From (10) we can compute

$$\pi(u)\pi(u') = q^{-u \circ u'} \pi(u')\pi(u), \quad (11)$$

where

$$u \circ u' = k_1 \ell'_1 - k'_1 \ell_1 + k_2 \ell'_2 - k'_2 \ell_2 \pmod{p}$$

for $u = (k_1, \ell_1, k_2, \ell_2)$ and $u' = (k'_1, \ell'_1, k'_2, \ell'_2)$. Hence $\pi(u)$ and $\pi(u')$ commute if and only if $u \circ u'$ equals zero.

We want to define a homomorphism $\rho : M_p(\mathbb{C}) \rightarrow M_p(\mathbb{C}) \otimes M_p(\mathbb{C})$ such that

$$\rho(X) = \pi(k_1, \ell_1, k_2, \ell_2) \quad \text{and} \quad \rho(Z^{u \circ u'}) = \pi(u')$$

when $u \circ u' \neq 0$. Since the commutation relation (11) is the same as that for X and $Z^{u \circ u'}$, ρ can be extended to an embedding of $M_p(\mathbb{C})$ into $M_p(\mathbb{C}) \otimes M_p(\mathbb{C})$. Let $\mathcal{A}(u, u') \subset M_p(\mathbb{C}) \otimes M_p(\mathbb{C})$ be the range. This is a method to construct subalgebras. For example, if

$$\pi(u) = X \otimes X \quad \text{and} \quad \pi(u') = Z \otimes Z,$$

then the generated subalgebra $\mathcal{A}(u, u')$ is obviously complementary to $\mathbb{C}I \otimes M_p(\mathbb{C})$ and $M_p(\mathbb{C}) \otimes \mathbb{C}I$. (At this point we used the condition $p > 2$, since this implies that X and Z do not commute.) \square

The idea of the above example is used by Ohno to construct $p^2 + 1$ complementary subalgebras in $M_p(\mathbb{C}) \otimes M_p(\mathbb{C})$ if $p > 2$ is prime [9]. The case $p = 2$ is very different. It was proved by that $M_2(\mathbb{C}) \otimes M_2(\mathbb{C})$ does not contain 5 complementary subalgebras isomorphic to $M_2(\mathbb{C})$ [17].

Let \mathcal{A} and \mathcal{B} be subalgebras of $\mathcal{M} \equiv M_n(\mathbb{C})$. For a state ψ on \mathcal{M} the conditional entropy of the algebras \mathcal{A} and \mathcal{B} is defined as

$$H_\psi(\mathcal{A}|\mathcal{B}) := \sup \left\{ \sum_i \lambda_i \left(S(\psi_i|_{\mathcal{A}} \| \psi|_{\mathcal{A}}) - S(\psi_i|_{\mathcal{B}} \| \psi|_{\mathcal{B}}) \right) \right\} \quad (12)$$

where the supremum is taken over all possible decomposition of ψ into a convex combination $\psi = \sum_i \lambda_i \psi_i$ of states and $S(\cdot \| \cdot)$ stands for the relative entropy of states. This concept was introduced by Connes and Størmer in 1975 [5] and was called relative entropy of subalgebras. Since in the case of commutative algebras, the quantity becomes the usual conditional entropy, see Chap. 10 in [8], we are convinced that conditional entropy is the proper terminology.

Theorem 4 *Let \mathcal{A} and \mathcal{B} be subalgebras of $M_n(\mathbb{C})$. Assume that \mathcal{A} is Abelian subalgebra and its minimal projections have the same trace. Then the subalgebras \mathcal{A} and \mathcal{B} are complementary if and only if $H(\mathcal{A}|\mathcal{B})$ is maximal.*

This result was obtained in [18] and it turns out that in the general case the conditional entropy of subalgebras cannot characterize complementarity.

3. Two qubits

From the point of view of complementarity the algebra $\mathcal{M} := M_4(\mathbb{C}) \equiv M_2(\mathbb{C}) \otimes M_2(\mathbb{C})$ is an interesting and important particular case. An F-subalgebra is a subalgebra isomorphic to $M_2(\mathbb{C})$. "F" is the abbreviation of "factor", the center of such a subalgebra is minimal, $\mathbb{C}I$. If our 4-level quantum system is regarded as two qubits, then an F-subalgebra may correspond to one of the qubits. When the F-subalgebra \mathcal{A}_0 describes a "one-qubit-subsystem", then the relative commutant $\mathcal{A}' := \{B \in \mathcal{M} : BA = AB \text{ for every } A \in \mathcal{A}\}$ corresponds to the other qubit. If \mathcal{A} is an F-subalgebra of \mathcal{M} , then we may assume that $\mathcal{M} = \mathcal{A} \otimes \mathcal{A}'$.

An M-subalgebra is a maximal Abelian subalgebra, equivalently, it is isomorphic to \mathbb{C}^4 . (M is an abbreviation of "MASA", the center is maximal, it is the whole subalgebra.) An M-subalgebra is in relation to a von Neumann measurement, its minimal projections give a partition of unity.

Both the F-subalgebras and the M-subalgebras are 4 dimensional. We define a P-unitary as a self-adjoint traceless unitary operator. The eigenvalues of a P-unitary from \mathcal{M} are $-1, -1, 1, 1$. An F-triplet (S_1, S_2, S_3) consists of P-unitaries such that $S_3 = iS_1S_2$. An M-triplet (S_1, S_2, S_3) consists of P-unitaries such that $S_3 = S_1S_2$. One can see that if (S_1, S_2, S_3) is an X-triplet, then the linear span of I, S_1, S_2, S_3 is an X-subalgebra, $X=F, M$.

Example 3 Example 1 in the $n = 2$ case gives two F-subalgebras determined by the following two triplets:

$$\sigma_0 \otimes \sigma_1, \quad \sigma_0 \otimes \sigma_2, \quad \sigma_0 \otimes \sigma_3$$

and

$$\frac{1}{2}(-\sigma_2 \otimes \sigma_0 - \sigma_2 \otimes \sigma_3 + \sigma_3 \otimes \sigma_0), \frac{1}{2}(-\sigma_2 \otimes \sigma_0 - \sigma_2 \otimes \sigma_3 + \sigma_3 \otimes \sigma_0 + \sigma_3 \otimes \sigma_3), -\sigma_1 \otimes \sigma_0.$$

The linear combinations of the triplets and the identity are complementary subalgebras. \square

Example 4 In the Hilbert space $\mathbb{C}^4 = \mathbb{C}^2 \otimes \mathbb{C}^2$ the standard product basis is $|00\rangle, |01\rangle, |10\rangle, |11\rangle$. The Bell basis (5) consists of maximal entangled vectors and so it is complementary to the standard product basis. The Bell basis has important applications, for example, the teleportation of a state of a qubit.

The operators diagonal in the Bell basis form an M-subalgebra which is generated by the M-triplet

$$(\sigma_1 \otimes \sigma_1, \quad \sigma_2 \otimes \sigma_2, \quad \sigma_3 \otimes \sigma_3). \tag{13}$$

We call this standard Bell triplet.

It was proved in [18] that the Bell basis can be characterized abstractly in the language of complementarity. If \mathcal{A} is an F-subalgebra of $M_4(\mathbb{C})$, then an M-subalgebra complementary to both \mathcal{A} and to its commutant is given by the Bell basis (up to a unitary transformation). \square

It was a natural question if $M_4(\mathbb{C})$ contains 5 complementary F-subalgebras. The answer appeared in [17]. Assume that $\mathcal{A}_0, \mathcal{A}_1, \dots, \mathcal{A}_r$ are complementary F-subalgebras. It was proved that $\mathcal{A}_1, \dots, \mathcal{A}_r$ intersects the commutator of \mathcal{A}_0 , therefore $r \leq 3$.

The algebra $M_4(\mathbb{C})$ is not only two qubits but also two fermions:

Example 5 Let \mathcal{A} be the algebra generated by the operators a_1, a_1^*, a_2, a_2^* satisfying the canonical anticommutation relations:

$$\{a_1, a_1^*\} = \{a_2, a_2^*\} = I, \{a_1, a_1\} = \{a_1, a_2\} = \{a_1, a_2^*\} = \{a_2, a_2\} = 0,$$

where $\{A, B\} := AB + BA$. Let \mathcal{A}_1 be the subalgebra generated a_1 and \mathcal{A}_2 be the subalgebra generated a_2 . Then \mathcal{A}_1 and \mathcal{A}_2 are complementary. In the usual matrix representation

$$a_1 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad a_2 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \otimes \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix},$$

therefore

$$\mathcal{A}_1 = \left\{ \begin{bmatrix} a & 0 & b & 0 \\ 0 & a & 0 & b \\ c & 0 & d & 0 \\ 0 & c & 0 & d \end{bmatrix} \right\}, \quad \mathcal{A}_2 = \left\{ \begin{bmatrix} a & b & 0 & 0 \\ c & d & 0 & 0 \\ 0 & 0 & a & -b \\ 0 & 0 & -c & d \end{bmatrix} \right\}.$$

The subalgebra \mathcal{A}_1 is generated by the F-triplet

$$(\sigma_1 \otimes \sigma_0, \quad \sigma_2 \otimes \sigma_0, \quad \sigma_3 \otimes \sigma_0),$$

and \mathcal{A}_2 is spanned by the F-triplet

$$(\sigma_3 \otimes \sigma_1, \quad \sigma_3 \otimes \sigma_2, \quad \sigma_0 \otimes \sigma_3).$$

Observe that the standard Bell triplet (13) is complementary to both \mathcal{A}_1 and \mathcal{A}_2 .

The parity automorphism is defined by $\Theta(a_1) = -a_1$ and $\Theta(a_2) = -a_2$. It is induced by the unitary $\sigma_3 \otimes \sigma_3$:

$$\Theta(x) = (\sigma_3 \otimes \sigma_3)x(\sigma_3 \otimes \sigma_3)$$

The operators $\sigma_i \otimes \sigma_j$, $0 \leq i, j \leq 3$ are eigenvectors of the parity automorphism. The fixed point algebra is linearly spanned by

$$\sigma_0 \otimes \sigma_0, \quad \sigma_1 \otimes \sigma_1, \quad \sigma_2 \otimes \sigma_2, \quad \sigma_3 \otimes \sigma_3$$

and

$$\sigma_0 \otimes \sigma_3, \quad \sigma_1 \otimes \sigma_2, \quad \sigma_2 \otimes \sigma_1, \quad \sigma_3 \otimes \sigma_0.$$

The first group linearly spans the M-subalgebra corresponding to the Bell basis. It follows that all Bell states are even, that is the parity automorphism Θ leaves them invariant. \square

4. Complementary decompositions

In this section first we consider decompositions of $\mathcal{M} \equiv M_4(\mathbb{C})$ [18]. Decomposition of \mathcal{M} into pairwise complementary F- and M-subalgebras is known. It is really well-known that decomposition into 5 M-subalgebras is possible. (Recall that this fact is equivalent to the existence of 5 mutually unbiased bases in a 4 dimensional space.)

Theorem 5 *Let \mathcal{A}_k ($0 \leq k \leq 4$) be pairwise complementary subalgebras of \mathcal{M} such that all of them is an F-subalgebra or M-subalgebra. If ℓ is the number of F-subalgebras in the set $\{\mathcal{A}_k : 0 \leq k \leq 4\}$, then $\ell \in \{0, 2, 4\}$, and all those values are actually possible.*

There is an interesting result about for pairwise complementary F-subalgebras. If $\mathcal{A}_1, \dots, \mathcal{A}_4$ are such subalgebras, then the linear span of the orthogonal complement and identity is always an M-subalgebra which is actually generated by the Bell triplet [10]. If we consider n -fold tensor product $\mathcal{M} := M_2(\mathbb{C}) \otimes \dots \otimes M_2(\mathbb{C})$, then there are some open questions for $n > 2$.

What is the maximum number of pairwise complementary subalgebras of \mathcal{M} which are isomorphic to $M_2(\mathbb{C})$? If we calculate the dimensions, then $(4^n - 1)/3$ is an upper bound. In the paper [10] a conjecture is formulated: The maximum number is $(4^n - 1)/3 - 1$. So many subalgebras are actually constructed. If the conjecture is true, then one can ask the orthogonal complement of so many subalgebras: Is it a commutative subalgebra (if the identity is added)? The case of n qubit is rather special. Consider now the n -fold tensor product $\mathcal{M} := M_p(\mathbb{C}) \otimes \dots \otimes M_p(\mathbb{C})$ and ask the maximum number of pairwise complementary subalgebras of \mathcal{M} which are isomorphic to $M_p(\mathbb{C})$. The upper bound is

$$\frac{p^{2n} - 1}{p^2 - 1}.$$

If $p > 2$ is a prime number, then this upper bound is accessible [9].

5. Discussion

The motivation for complementary subalgebras was a certain kind of state tomography for two qubits [14] and a systematic study started in [16]. Maximal Abelian subalgebras correspond to orthogonal bases in the Hilbert space and the complementarity of two maximal Abelian subalgebras is the same as the mutually unbiased property of the corresponding two bases. Mutually unbiased bases have a huge literature and nice applications. Much less is known about complementary non-commutative subalgebras. An Abelian subalgebra (corresponding to a measurement) may give classical information about a quantum system and a non-commutative subalgebra provides quantum information about the total system. This is a very essential difference, to handle quantum information is more sophisticated. Parts of the information coming from several reduced state of a quantum system may be redundant. Intuitively, two subsystems are complementary if the knowledge of their reduced densities is the most informative; i.e. as little redundant as possible.

The construction of complementary subalgebras needs much research. For a 4-level quantum system (describing two qubits) a complete description is given in the paper. There is no non-commutative subalgebra complementary to both qubits and there is essentially one maximal Abelian subalgebra complementary to both qubits, this subalgebra is in strong relation with the Bell basis.

The difference between $M_2(\mathbb{C}) \otimes M_2(\mathbb{C})$ and $M_n(\mathbb{C}) \otimes M_n(\mathbb{C})$ is essential. The dimensional upper bound for the number of complementary subalgebras (isomorphic to $M_n(\mathbb{C})$) is $n^2 + 1$. This bound is not reached for $n = 2$ [17] but it is reached if $n > 2$ is a prime [9]. Several open questions can be formulated. It is interesting that the present methods for the construction of mutually unbiased bases and complementary subalgebras are similar, typically based on finite fields. However, the relation of the two subjects is not clear.

References

- [1] Accardi L 1984 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**, 1–19. Springer.
- [2] Bruss D 1998 Optimal eavesdropping in quantum cryptography with six states *Physical Review Letters* **81**, 3018–3021
- [3] Busch P and Lahti P J 1995 The complementarity of quantum observables: theory and experiment *Riv. Nuovo Cimento* **18** 27
- [4] Cassinelli G and Varadarajan V S 2002 On Accardi's notion of complementary observables *Infin. Dimens. Anal. Quantum Probab. Relat. Top.* **5** 135–144.
- [5] Connes A and Størmer E 1975 Entropy of II_1 von Neumann algebras, *Acta Math.* **134** 289–3006.
- [6] Maasen H and Uffink I 1988 Generalized entropic uncertainty relations *Phys. Rev. Lett.* **60** 1103–1106.
- [7] von Neumann J 1932 *Mathematische Grundlagen der Quantenmechanik* (Berlin: Springer)
- [8] Neshveyev S and Størmer E 2006 *Dynamical entropy in operator algebras* (Berlin: Springer)
- [9] Ohno H 2008 Quasi-orthogonal subalgebras of matrix algebras, preprint, arXiv:0801.1353.
- [10] Ohno H, Petz D and Szántó A 2007 Quasi-orthogonal subalgebras of 4×4 matrices *Linear Alg. Appl.* **425** 109–118.
- [11] Ohya M and Petz D 1993 *Quantum Entropy and Its Use* (Heidelberg: Springer)
- [12] Oppenheim J, Horodecki K, Horodecki M, Horodecki P and Horodecki R 2003 A new type of complementarity between quantum and classical information, *Phys. Rev. A* **68** 022307.
- [13] Pauli W 1980 *General Principles of Quantum Mechanics* (Berlin: Springer) (original German edition: 1933).
- [14] Petz D, Hangos K M, Szántó A and Szöllősi F 2006 State tomography for two qubits using reduced densities *J. Phys. A* **39** 10901–10907.
- [15] Petz D, Hangos K M and Magyar A 2007 Point estimation of states of finite quantum systems *J. Phys. A.* **40**, 7955–7969.
- [16] Petz D 2007 Complementarity in quantum systems *Rep. Math. Phys.* **59** 209–224.
- [17] Petz D and Kahn J 2007 Complementary reductions for two qubits *J. Math. Phys.* **48**, 012107.
- [18] Petz D, Szántó A and Weiner M 2008, Complementarity and the algebraic structure of 4-level quantum systems, *to be published*

- [19] Pittenger A O and Rubin M H 2004 Mutually unbiased bases, generalized spin matrices and separability *Linear Algebra Appl.* **390**, 255–278.
- [20] Popa S 1983 Orthogonal pairs of $*$ -subalgebras in finite von Neumann algebras *J. Operator Theory* **9**, 253–268.
- [21] Rédei M 1998 *Quantum Logic in Algebraic Approach* (Dordrecht: Kluwer)
- [22] Schwinger J 1960 Unitary operator bases *Proc. Nat. Acad. Sci. U.S.A.* **46**, 570–579.
- [23] Tadej W and Życzkowski K 2006 A concise guide to complex Hadamard matrices *Open Syst. Inf. Dyn.* **13** 133–177.
- [24] Wootters W K and Fields B D 1989 Optimal state determination by mutually unbiased measurements *Ann. Physics* **191**, 363–381.
- [25] Weyl H 1931 *Theory of groups and quantum mechanics* (Methuen)