

Algebraic complementarity in quantum theory

Not for circulation

Dénes Petz¹

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

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

Abstract

This paper is an overview of the concept of complementarity, the relation to state estimation, to Connes-Størmer conditional (or relative) entropy and to uncertainty relation. Complementary Abelian and non-commutative subalgebras are analyzed. All the known results about complementary decompositions are described and several open questions are included. The paper contains only few proofs, typically references are given.

Key words and phrases. Complementarity, conditional entropy, mutually unbiased bases, Bell basis, subsystem, quantum information, qubits, Pauli channel, uncertainty relation.

The origin of complementarity is related to the non-commutativity of operators describing observables in quantum mechanics. Although the concept was born together with quantum mechanics itself, the rigorous definitions appeared much later. According to *Wolfgang Pauli*, the new quantum theory could have been called the theory of complementarity [19]. This fact already indicates the central importance of the notion of complementarity in the foundations of quantum mechanics.

Position and momentum are basic observables satisfying the commutation relation,

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

¹E-mail: petz@math.bme.hu. Partially supported by the Hungarian Research Grant OTKA T068258.

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 $\Delta(A, f) = \sqrt{\langle f, A^2 f \rangle - \langle f, A f \rangle^2}$ is the variance of the observable A in the vector state f .)

The Fourier connection $P = \mathcal{F}^{-1}Q\mathcal{F}$ 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 $H \subset \mathbb{R}$. *Herman Weyl* used the finite Fourier transform to approximate the relation of P and Q in finite dimensional Hilbert spaces [36]. Let $|0\rangle, |1\rangle, \dots, |n-1\rangle$ be an orthonormal basis in an n -dimensional Hilbert space. The transformation

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

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 observable 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

$$|\langle \xi_i, \eta_j \rangle| = \frac{1}{\sqrt{n}}. \quad (2)$$

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 (1) moves the standard basis $|0\rangle, |1\rangle, \dots, |n-1\rangle$ to a complementary basis $V_n|0\rangle, V_n|1\rangle, \dots, V_n|n-1\rangle$. This kind of complementarity (2) is often called value complementarity [5] and it was an important subject in the work of Schwinger [29, 30]. Note that the operators P and Q do not have eigenvectors and the complementarity may be defined in terms of the spectral projection-valued measures [5].

In connection with complementarity, Kraus made a conjecture about the entropy of two observables [8] which was proved by Maasen and Uffink [10] and there are generalizations [9, 28]. Although the old concept was in connection with the joint measurement of

observables. the present formulation (2) is about maximal information about the quantum system: The knowledge of the probability distribution of a single physical observable is not sufficient for determining the state of a system. On the other hand, a part of the information coming from the distributions of several observables may be redundant. Intuitively, two observables are complementary if the knowledge of their distributions is the most informative; i.e. as little redundant as possible. Complementarity is used, for example, in state estimation [21, 35] and in quantum cryptography [3]. Instead of pairwise complementary bases, Wootters and Fields used the expression “mutually unbiased bases” and this terminology has become popular.

Maximal precision measurements are related to maximal Abelian subalgebras. However, one is also motivated to study complementarity for non-Abelian subalgebras. For example, units that can be considered in a quantum computer to be qubits are described by subalgebras that are isomorphic to the algebra of 2×2 matrices. One might be interested to choose a collection of qubits that are as little redundant as possible. Conditional (or relative) entropy of subalgebras give also some justification of the intuitive meaning of complementarity. It can be shown that if the subalgebra \mathcal{A} is homogeneous and Abelian, then the conditional entropy $H(\mathcal{A}|\mathcal{B})$ is maximal if and only if \mathcal{A} and \mathcal{B} are complementary. When non-classical, say quantum, information is considered, then non-commutative subalgebras or subsystems of the total system should be chosen. The study of complementary non-commutative subalgebras is rather recent [20].

The content of the paper is arranged in the following way. Section 1 is devoted to the concept of complementarity subalgebras and the relation to mutually unbiased basis. Section 2 is about \mathbf{M}_2 and $\mathbf{M}_2 \times \mathbf{M}_2 = \mathbf{M}_4$. A simple example shows that complementary measurements are the most efficient. Complementary decompositions of \mathbf{M}_4 are described and abstract characterization of the Bell basis is given. Section 3 is about the relation to the conditional entropy of subalgebras introduced long time ago by Connes and Størmer. The main result says that complementarity is the maximality of the conditional entropy. Section 4 is a short summary of the entropic uncertainty relation discovered by Kraus.

1 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

$$|\langle \xi, e_i \rangle|^2 = \frac{1}{n} \quad (1 \leq i \leq n). \quad (3)$$

The basis $\xi_1, \xi_2, \dots, \xi_n$ is complementary to the basis e_1, e_2, \dots, e_n if every ξ_i is complementary to that basis. In other words, the bases $\xi_1, \xi_2, \dots, \xi_n$ and e_1, e_2, \dots, e_n are mutually unbiased.

When the Hilbert space \mathcal{H} is a tensor product $\mathcal{H}_1 \otimes \mathcal{H}_2$, then a unit vector comple-

mentary 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

$$\begin{aligned} |\beta_0\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), & |\beta_1\rangle &= \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) = (\sigma_1 \otimes I)|\beta_0\rangle, \\ |\beta_2\rangle &= \frac{i}{\sqrt{2}}(|10\rangle - |01\rangle) = (\sigma_2 \otimes I)|\beta_0\rangle, & |\beta_3\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = (\sigma_3 \otimes I)|\beta_0\rangle. \end{aligned}$$

consists of maximally entangled states.

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

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

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 (3) can be reformulated in terms of these generated subalgebras.

On the matrices the Hilbert-Schmidt inner product $\langle A, B \rangle = \mathrm{Tr} A^* B$ is considered.

Theorem 1 *Let \mathcal{A}_1 and \mathcal{A}_2 be subalgebras of $\mathbf{M}_k(\mathbb{C})$ and let $\tau := \mathrm{Tr}/k$ 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 $\mathbf{M}_n(\mathbb{C})$, that is the subspaces $\mathcal{A}_1 \ominus \mathbb{C}I$ and $\mathcal{A}_2 \ominus \mathbb{C}I$ are orthogonal.*
- (iii) *$\tau(A_1 A_2) = \tau(A_1)\tau(A_2)$ 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 led to the concept of complementary subalgebras [20]. 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 [27, 32].

The quasi-orthogonal relation gives an easy approach to have an upper bound for the number of complementary subalgebras. The traceless part of $\mathbf{M}_n(\mathbb{C})$ has dimension $n^2 - 1$ and the traceless part of a MASA is $n - 1$ dimensional. Therefore the maximum number of mutually unbiased bases is $(n^2 - 1)/(n - 1) = n + 1$. This upper bound is reached if n is a power of a prime number [2, 26]. It is also proven that if there are n mutually unbiased

bases, then there are $n + 1$ [34]. When we want subalgebras isomorphic to $\mathbf{M}_n(\mathbb{C})$ in $\mathbf{M}_n(\mathbb{C}) \otimes \mathbf{M}_n(\mathbb{C})$, then the dimensions give the bound $(4n^2 - 1)/(n^2 - 1) = n^2 + 1$. If $n = p^k$ with a prime number $p > 2$, then there are so many complementary subalgebras [14]. In the case $n = 2$ the maximum number is 4 (contrary to the bound 5) [23], but the case of $n = 2^k$ 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 [31].

Let \mathcal{A}_1 and \mathcal{A}_2 be subalgebras of $\mathbf{M}_k(\mathbb{C})$ and assume that both subalgebras are isomorphic to $\mathbf{M}_m(\mathbb{C})$. Then $k = mn$ and we can assume that $\mathcal{A}_1 = \mathbf{C}I_n \otimes \mathbf{M}_m(\mathbb{C})$. 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 [15, 20].

Theorem 2 *Let E_i be an orthonormal basis in $\mathbf{M}_n(\mathbb{C})$ and let $W = \sum_i E_i \otimes W_i \in \mathbf{M}_n(\mathbb{C}) \otimes \mathbf{M}_m(\mathbb{C})$ be a unitary. The subalgebra $W(\mathbf{C}I_n \otimes \mathbf{M}_m(\mathbb{C}))W^*$ is complementary to $\mathbf{C}I \otimes \mathbf{M}_m(\mathbb{C})$ if and only if*

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

is the identity mapping on $\mathbf{M}_m(\mathbb{C})$.

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 $\mathbf{M}_m(\mathbb{C})$. With $n = 2$ the CAR-algebra becomes a physically important example [20].

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

Example 1 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:

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

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

$$(X^{k_1} Z^{\ell_1})(X^{k_2} Z^{\ell_2}) = q^{k_2 \ell_1} X^{k_1+k_2} Z^{\ell_1+\ell_2}. \quad (4)$$

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 (4) we can compute

$$\pi(u)\pi(u') = q^{-u \circ u'} \pi(u')\pi(u), \quad (5)$$

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 (5) 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 $M_p(\mathbb{C}) \otimes M_p(\mathbb{C})$ [14].

2 Qubits

In computation 2×2 matrices are very well handable. In this section the relation of efficient state estimation to complementarity will be described (with proof) in the 2×2 case. Decomposition to complementary subalgebras is trivial, therefore the case of two qubits (or \mathbf{M}_4) will be the setting for detailed description of decomposition.

In the matrix algebra \mathbf{M}_2 of a qubit the convenient formalism is based on the Pauli matrices:

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

The normalized eigenvectors σ_i form an orthonormal basis for $i = 1, 2, 3$ and they are mutually unbiased.

The state estimation procedures are easily computed for a qubit. A state has the density matrix

$$\rho = \frac{1}{2} \left(I + \sum_{i=1}^3 \theta_i \sigma_i \right) = \frac{1}{2} (I + \theta \cdot \sigma) = \frac{1}{2} \begin{bmatrix} 1 + \theta_3 & \theta_1 - i\theta_2 \\ \theta_1 + i\theta_2 & 1 - \theta_3 \end{bmatrix}, \quad (6)$$

where $\theta_1^2 + \theta_2^2 + \theta_3^2 \leq 1$. Suppose that θ_3 is known and the unknown θ_1, θ_2 should be estimated by von Neumann measurements. Assume that the observables

$$E(x) = \frac{1}{2} (I + x \cdot \sigma) \quad (x = a, b)$$

are measured in the true state ρ , where a, b are unit vectors in \mathbb{R}^3 . The probabilities are

$$p_x := \frac{1 + \langle x, \theta \rangle}{2}, \quad p := (p_a, p_b).$$

If the measurements are performed r times, then p_x is estimated by the relative frequency ν_x of the outcome 1. The equations

$$\nu_x = \frac{1 + \langle x, \hat{\theta} \rangle}{2} \quad (x = a, b)$$

should be solved to find an estimate. In another form,

$$\begin{bmatrix} \nu_a \\ \nu_b \end{bmatrix} = \frac{1}{2} \left(\begin{bmatrix} 1 \\ 1 \end{bmatrix} + U \begin{bmatrix} \hat{\theta}_1 \\ \hat{\theta}_2 \end{bmatrix} + \begin{bmatrix} a_3 \theta_3 \\ b_3 \theta_3 \end{bmatrix} \right),$$

where

$$U = \begin{bmatrix} a_1 & a_2 \\ b_1 & b_2 \end{bmatrix}.$$

We have the estimator

$$\begin{bmatrix} \hat{\theta}_1 \\ \hat{\theta}_2 \end{bmatrix} = U^{-1} \left(2 \begin{bmatrix} \nu_a \\ \nu_b \end{bmatrix} - \begin{bmatrix} 1 \\ 1 \end{bmatrix} - \theta_3 \begin{bmatrix} a_3 \\ b_3 \end{bmatrix} \right)$$

The efficiency can be taken by the mean quadratic error matrix which is the expectation of

$$\begin{bmatrix} \hat{\theta}_1 \\ \hat{\theta}_2 \end{bmatrix} [\hat{\theta}_1 \quad \hat{\theta}_2].$$

It becomes

$$U^{-1} \begin{bmatrix} 1 - \langle a, \theta \rangle^2 & 0 \\ 0 & 1 - \langle b, \theta \rangle^2 \end{bmatrix} (U^{-1})^t. \quad (7)$$

In order to take the average, we integrate this with respect to the unknown θ_1 and θ_2 . Let $R := \sqrt{1 - \theta_3^2}$ and we integrate the variance on the disk $H := \{(\theta_1, \theta_2) : \theta_1^2 + \theta_2^2 \leq R^2\}$ with respect to the normalized Lebesgue measure:

$$\frac{1}{R^2\pi} \int_H \langle \lambda, \theta \rangle^2 d\theta_1 d\theta_2 = (\lambda_1^2 + \lambda_2^2)R^2/4 + \lambda_3^2\theta_3^2$$

So according to (7) we have the average mean quadratic error matrix

$$U^{-1} \begin{bmatrix} 1 - (a_1^2 + a_2^2)R^2/4 - a_3^2\theta_3^2 & 0 \\ 0 & 1 - (b_1^2 + b_2^2)R^2/4 - b_3^2\theta_3^2 \end{bmatrix} (U^{-1})^t.$$

Minimization of a matrix cannot be performed, so our idea is to minimize the determinant

$$\frac{(1 - (a_1^2 + a_2^2)(1 - \theta_3^2)/4 - a_3^2\theta_3^2)(1 - (b_1^2 + b_2^2)(1 - \theta_3^2)/4 - b_3^2\theta_3^2)}{\det U^2} \quad (8)$$

under the conditions $a_1^2 + a_2^2 + a_3^2 = 1$ and $b_1^2 + b_2^2 + b_3^2 = 1$.

Theorem 3 *Assume that $|\theta_3| \neq 1$. Then the determinant of the average of the quadratic mean error matrix is minimal if a and b are orthogonal and $a_3 = b_3 = 0$.*

Proof: Let $c = a_1^2 + a_2^2$ and $d = b_1^2 + b_2^2$. Then we have to minimize

$$\left(1 - \theta_3^2 - c \frac{1 + 3\theta_3^2}{4}\right) \left(1 - \theta_3^2 - d \frac{1 + 3\theta_3^2}{4}\right) \frac{1}{\det U^2}.$$

So c , d and $\det U^2 \leq cd$ should be big. In the optimal case $c = d = 1$ and $(a_1, a_2) \perp (b_1, b_2)$. (If $\theta_3^2 = 1$, then $\theta_1 = \theta_2 = 0$ and only the sign of θ_3 should be fixed.) \square

This example shows the relevance of complementarity to state estimation. The optimal measurements are complementary to each other and complementary to MASA determined by the known parameter. If the number of known parameters is 0 or two, then the result is similar [22, 25].

A 4-level quantum system is mathematically the Hilbert space \mathbb{C}^4 or the algebra $\mathcal{M} := \mathbf{M}_4(\mathbb{C})$. We are interested in two kinds of subalgebras. 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 2 Consider the unitary $W = V_{n^2}$ defined in (1) as an $n \times n$ block-matrix with entries from $\mathbf{M}_n(\mathbb{C})$. Then the entries form an orthonormal basis in $\mathbf{M}_n(\mathbb{C})$ and Theorem 2 tells us that the Fourier transform can be used to construct a complementary pair.

The Fourier transform sends the standard basis into a complementary one but it can produce non-commutative complementary subalgebras as well. If $n = 2$, then we get the following two F-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 Bell basis has important applications, for example, the teleportation of a state of a qubit. Theorem 4 shows that a complementarity property characterizes the Bell basis. Up to local unitary transformations, the Bell basis is unique [24].

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

$$(\sigma_1 \otimes \sigma_1, \quad \sigma_2 \otimes \sigma_2, \quad \sigma_3 \otimes \sigma_3). \tag{9}$$

We call this standard Bell triplet.

Theorem 4 *Let \mathcal{A} be an F-subalgebra of \mathbf{M}_4 . Assume that (X, Y, Z) is an M-triplet which is orthogonal to \mathcal{A} and \mathcal{A}' . Then there are F-triplets $(A_1, A_2, A_3) \in \mathcal{A}$ and $(B_1, B_2, B_3) \in \mathcal{A}'$ such that*

$$X = A_1B_1, \quad Y = A_2B_2, \quad Z = A_3B_3.$$

If the operators A_i and B_i are identified with σ_i ($i = 1, 2, 3$) in the theorem, then the triplet (X, Y, Z) can be identified with the standard Bell triplet (9).

Although \mathcal{M} has 5 pairwise complementary M-subalgebras, it does not have 5 pairwise complementary F-subalgebras [23]. The next theorem describes the possible complementary decompositions [24].

Theorem 5 *Let \mathcal{A}_k ($1 \leq k \leq 5$) be pairwise complementary subalgebras of \mathbf{M}_4 such that all of them is an F-subalgebra or M-subalgebra. If ℓ is the number of F-subalgebras in the set $\{\mathcal{A}_k : 1 \leq k \leq 5\}$, then $\ell \in \{0, 2, 4\}$, and all those values are actually possible.*

The Pauli channel $\alpha : \mathbf{M}_2 \rightarrow \mathbf{M}_2$ is formulated in the parametrization (6) of the density matrices:

$$\alpha \left(\begin{bmatrix} 1 + \theta_3 & \theta_1 - i\theta_2 \\ \theta_1 + i\theta_2 & 1 - \theta_3 \end{bmatrix} \right) = \begin{bmatrix} 1 + \lambda_3\theta_3 & \lambda_1\theta_1 - i\lambda_2\theta_2 \\ \lambda_1\theta_1 + i\lambda_2\theta_2 & 1 - \lambda_3\theta_3 \end{bmatrix}.$$

$-1 \leq \lambda_i \leq 1$ is an obvious condition to have a positive mapping, but complete positivity requires a different condition which is well-known. The setting of the Pauli channel is based on a complementary F-decomposition of \mathbf{M}_2 . A channel can be defined for decompositions of \mathbf{M}_n and the condition for complete positivity can be obtained [11, 16].

3 Conditional entropy

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

$$H_\psi(\mathcal{A}|\mathcal{B}) := \sup \left\{ \sum_i \lambda_i \left(S(\psi_i|_{\mathcal{A}} \| \psi|_{\mathcal{A}}) - S(\psi_i|_{\mathcal{B}} \| \psi|_{\mathcal{B}}) \right) \right\} \quad (10)$$

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 [7] 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 [13], we are convinced that conditional entropy is the proper terminology.

In what follows the reference state ψ will be always the unique normalized tracial state $\tau := \text{Tr}/n$ on $\mathcal{M} \equiv \mathbf{M}_n(\mathbb{C})$. So we shall omit the indication of the reference state and simply write $H(\mathcal{A}|\mathcal{B})$ instead of $H_\tau(\mathcal{A}|\mathcal{B})$. Also, instead of the states ψ_i , it will be often convenient to work with their density matrices ρ_i with respect to τ . It is an easy exercise to check that the conditional entropy is expressed with density matrices as

$$H(\mathcal{A}|\mathcal{B}) = \sup \left\{ \sum_i \lambda_i \left(\tau(\eta(E_{\mathcal{B}}\rho_i)) - \tau(\eta(E_{\mathcal{A}}\rho_i)) \right) \right\}, \quad (11)$$

where $E_{\mathcal{A}} : \mathcal{M} \rightarrow \mathcal{A}$ and $E_{\mathcal{B}} : \mathcal{M} \rightarrow \mathcal{B}$ are the τ -preserving conditional expectations, $\eta(t) = -t \log t$, and the supremum is taken over all possible convex decompositions of the identity $I = \sum_i \lambda_i \rho_i$.

Our primary interest concerns the case when the subalgebras in question are either maximal Abelian or isomorphic to some full matrix algebras. The two cases will be discussed together; for our argument it will be enough to assume that all minimal projections of \mathcal{A} have the same trace. Such subalgebra \mathcal{A} will be called homogeneous. Suppose that for every minimal projection $p \in \mathcal{A}$ we have $\tau(p) = d$. Then for every density operator ρ and minimal projection $p \in \mathcal{A}$, we have that

$$\tau(\eta(E_{\mathcal{A}}(\rho))) \geq \tau(\eta(p/d)) = \log d,$$

and equality holds if and only if $dE_{\mathcal{A}}(\rho)$ is a minimal projection of \mathcal{A} , which is trivially further equivalent with the fact that the range of ρ is contained in the range of a minimal projection of \mathcal{A} . On the other hand,

$$\tau(\eta(E_{\mathcal{B}}(\rho))) \leq \tau(\eta(I)) = 0.$$

This implies that

$$H(\mathcal{A}|\mathcal{B}) \leq -\log d. \quad (12)$$

In general it is easy to give some sufficient conditions ensuring that in the above inequality one has equality. When \mathcal{A} is Abelian, we can also give a simple necessary condition.

Lemma 1 *Let \mathcal{A} be a homogeneous subalgebra such that $\tau(p) = d$ for the minimal projections $p \in \mathcal{A}$. If there exists a decomposition $I = \sum_i \lambda_i p_i$ of the identity such that $\lambda_i > 0$ and p_i are minimal projections of \mathcal{A} satisfying $E_{\mathcal{B}}(p_i) = dI$, then equality holds in (12).*

Theorem 6 *Let \mathcal{A} and \mathcal{B} be subalgebras of $\mathbf{M}_n(\mathbb{C})$. Assume that \mathcal{A} is Abelian and homogeneous. Then the subalgebras \mathcal{A} and \mathcal{B} are complementary if and only if $H(\mathcal{A}|\mathcal{B})$ is maximal.*

Proof: If \mathcal{A} and \mathcal{B} are complementary, then for the minimal projections p_i of \mathcal{A} , $\sum_i p_i = I$ and $E_{\mathcal{B}}(p_i) = dI$ hold. So Lemma 1 tells us that the conditional entropy is $-\log d$.

Assume now that $H(\mathcal{A}|\mathcal{B}) = -\log d$. Then there exists a decomposition $I = \sum_i \lambda_i \rho_i$ of the identity into a convex combination of density operators such that $E_{\mathcal{B}}(\rho_i) = I$ and $q_i := E_{\mathcal{A}}(\rho_i)/n$ are minimal projections of \mathcal{A} .

Suppose that the image under the trace-preserving expectation E onto a subalgebra of a positive operator a is a multiple of a minimal projection p of the subalgebra. Then $x := (I - p)a(I - p)$ is a positive operator for which

$$E(x) = (I - p)E(a)(I - p) = 0,$$

and hence $x = 0$. It follows that $(I - p)\sqrt{a} = 0$ and we conclude $pa = ap = a$.

Applying the above, we have that for every minimal projection q of \mathcal{A}

$$q = qI = q \sum_i \lambda_i \rho_i = q \sum_i \lambda_i q_i \rho_i = \sum_i \lambda_i q q_i \rho_i = \sum_{\{i: q_i=q\}} \lambda_i q_i \rho_i = \sum_{\{i: q_i=q\}} \lambda_i \rho_i,$$

since the product $q q_i$ is zero, when $q_i \neq q$ and q_i when $q_i = q$. (Note that this is the point where we have used the fact the \mathcal{A} is Abelian). As $E_{\mathcal{B}}(\rho_i) = I$, the above decomposition of q shows that $E_{\mathcal{B}}(q)$ is a multiple of the identity, and hence (as q was arbitrary, and the minimal projections of \mathcal{A} span the whole algebra \mathcal{A}) that \mathcal{A} is quasi-orthogonal to \mathcal{B} . \square

Let \mathcal{A} and \mathcal{B} be subalgebras of $\mathbf{M}_n(\mathbb{C})$. Assume that \mathcal{A} is Abelian and homogeneous and choose a homogeneous algebra \mathcal{C} such that \mathcal{A} is maximal Abelian subalgebra of \mathcal{C} . If \mathcal{A} and \mathcal{B} are complementary, then $H(\mathcal{C}|\mathcal{B})$ is maximal (that is, equals $H(\mathcal{C})$). However, \mathcal{C} and \mathcal{B} is not necessarily complementary, in fact it is fairly easy to come up with an example in which their intersection is not trivial. Hence the conditional entropy cannot characterize the complementarity of subalgebras in the general case.

4 Entropic uncertainty relation

A positive operator-valued-measure (POVM) $\mathcal{E} = (E_1, E_2, \dots, E_m)$ is a finite sequence of positive operators satisfying the relation $\sum_{i=1}^m E_i = I$. (This is an extension of a commutative subalgebra when all E_i 's should be projections.) For a state φ the m -tuple $(\varphi(E_1), \varphi(E_2), \dots, \varphi(E_m))$ is a probability distribution and its Shannon entropy will be denoted by $H(\mathcal{E}, \varphi)$. Formally,

$$H(\mathcal{E}, \varphi) = \sum_{i=1}^m \eta(\varphi(E_i)) \quad (\eta(t) = -t \log t).$$

Given two different POVMs, $\mathcal{E} = (E_1, E_2, \dots, E_m)$ and $\mathcal{F} = (F_1, F_2, \dots, F_m)$ and a state ψ , the entropic uncertainty principle is lower bound for the sum $H(\mathcal{E}, \psi) + H(\mathcal{F}, \psi)$ of the two entropies. With the notation above the uncertainty relation

$$H(\mathcal{E}, \varphi) + H(\mathcal{F}, \varphi) \geq -2 \log c \tag{13}$$

holds when φ is pure state determined by the unit vector Φ and

$$c^2 = \sup \left\{ \frac{|\langle \Phi, E_i F_j \Phi \rangle|}{\|E_i^{1/2} \Phi\| \|F_j^{1/2} \Phi\|} : 1 \leq i, j \leq m, \quad \text{and} \quad E_i^{1/2} \Phi \neq 0, F_j^{1/2} \Phi \neq 0 \right\}.$$

Since

$$|\langle \Phi, E_i F_j \Phi \rangle| = |\langle E_i^{1/2} \Phi, E_i^{1/2} F_j^{1/2} F_j^{1/2} \Phi \rangle| \leq \|E_i^{1/2} F_j^{1/2}\| \|E_i^{1/2} \Phi\| \|F_j^{1/2} \Phi\|,$$

in the formula of c we have

$$\frac{|\langle \Phi, E_i F_j \Phi \rangle|}{\|E_i^{1/2} \Phi\| \|F_j^{1/2} \Phi\|} \leq \|E_i^{1/2} F_j^{1/2}\|.$$

The following uncertainty relation was conjectured for von Neumann measurements by Kraus (and it was proved for $n \leq 4$) [8].

Theorem 7 *The uncertainty relation (13) holds for any state φ if*

$$c^2 = \sup \left\{ \|E_i^{1/2} F_j^{1/2}\| : 1 \leq i, j \leq m \right\}.$$

Proof: From the above argument the theorem follows for pure states. Since the left-hand-side is concave in φ , this implies the inequality for an arbitrary state. \square

If $E_1, E_2, \dots, E_n, F_1, F_2, \dots, F_n$ are projections of rank one, then

$$\|E_i^{1/2} F_j^{1/2}\|^2 = \|F_j E_i F_j\| = \text{Tr } F_j E_i F_j = \text{Tr } E_i F_j$$

and the lower bound $-2 \log c$ in (13) is the largest when E_1, E_2, \dots, E_n and F_1, F_2, \dots, F_n correspond to complementary MASAs. The MASA case is the result of Maasen and Uffink [10] proved by the use of the Riesz-Thorin interpolation theorem. The use of POVM is a kind of extension of the case of MASA. Krishna and Parthasarathy modified first the argument to allow arbitrary projections. Then they used twice the Naimark theorem to allow arbitrary POVMs [9].

The Shannon entropy can be generalized by the Rényi entropy:

$$H_\alpha(\mathcal{E}, \varphi) = \frac{1}{1-\alpha} \log \sum_{i=1}^m \varphi(E_i)^\alpha,$$

$\alpha > 0$. The limit $\alpha \rightarrow 1$ recovers $H(\mathcal{E}, \varphi)$. The previous theorem of Krishna and Parthasarathy is extended to the Rényi entropy:

$$H_\alpha(\mathcal{E}, \varphi) + H_\beta(\mathcal{F}, \varphi) \geq -2 \log c \quad (14)$$

if $\alpha + \beta = 2$, see [28].

There are uncertainty relations also for more than 2 measurements, see the review [33].

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**, 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] D. Bruss, Optimal eavesdropping in quantum cryptography with six states. *Physical Review Letters*, **81**, 3018–3021, 1998.
- [4] P. Busch and P.J. Lahti, The complementarity of quantum observables: theory and experiment, *Riv. Nuovo Cimento* **18**(1995), 1–27.
- [5] G. Cassinelli and V.S. Varadarajan, On Accardi’s notion of complementary observables, *Infin. Dimens. Anal. Quantum Probab. Relat. Top.* **5**(2002), 135–144.

- [6] M. Choda, Relative entropy for maximal Abelian subalgebras of matrices and the entropy of antistochastic matrices, *Internat. J. Math.* **19**(2008), 767–776.
- [7] A. Connes and E. Størmer, Entropy of II_1 von Neumann algebras, *Acta Math.* **134**(1975), 289–3006.
- [8] K. Kraus, Complementary observables and uncertainty relations. *Phys. Rev. D* (3) **35**(1987), 3070–3075.
- [9] M. Krishna and K R Parthasarathy, An entropic uncertainty principle for quantum measurements, *Sankhya Indian J. Statistics* **64**, 842–851, 2002.
- [10] H. Maasen and I. Uffink, Generalized entropic uncertainty relations, *Phys. Rev. Lett.* **60**(1988), 1103–1106.
- [11] M. Nathanson and M.B. Ruskai, Pauli diagonal channels constant on axes, *J. Phys. A: Math. Theor.* **40**(2007), 8171–8204.
- [12] J. von Neumann, *Mathematische Grundlagen der Quantenmechanik*, Springer, Berlin, 1981. (Original edition: 1932).
- [13] S. Neshveyev and E. Størmer, *Dynamical entropy in operator algebras*, Springer-Verlag, Berlin, 2006.
- [14] H. Ohno, Quasi-orthogonal subalgebras of matrix algebras, *Linear Alg. Appl.* **429**(2008), 2146–2158.
- [15] H. Ohno, D. Petz and A. Szántó, Quasi-orthogonal subalgebras of 4×4 matrices, *Linear Alg. Appl.* **425**(2007), 109–118.
- [16] H. Ohno and D. Petz, Generalizations of Pauli channels, *Acta Math. Hungar.* **124**(2009), 165–177.
- [17] M. Ohya and D. Petz, *Quantum Entropy and Its Use*, Springer-Verlag, Heidelberg, 1993. Second edition 2004.
- [18] J. Oppenheim, K. Horodecki, M. Horodecki, P. Horodecki and R. Horodecki, A new type of complementarity between quantum and classical information, *Phys. Rev. A* **68**, 022307, 2003.
- [19] W. Pauli, *General Principles of Quantum Mechanics*, Springer, Berlin, 1980 (original German edition: 1933).
- [20] D. Petz, Complementarity in quantum systems, *Rep. Math. Phys.* **59**(2007), 209–224.
- [21] D. Petz, K.M. Hangos, A. Szántó and F. Szöllősi, State tomography for two qubits using reduced densities, *J. Phys. A*, **39**, 10901–10907, 2006.

- [22] D. Petz, K.M. Hangos and A. Magyar, Point estimation of states of finite quantum systems, *J. Phys. A*, **40**(2007), 7955–7969.
- [23] D. Petz and J. Kahn, Complementary reductions for two qubits, *J. Math. Phys.*, **48**(2007), 012107.
- [24] D. Petz, A. Szántó and M. Weiner, Complementarity and the algebraic structure of 4-level quantum systems, *J. Infin. Dim. Analysis Quantum Prob.* **12**(2009), 99–116.
- [25] D. Petz and L. Ruppert, Efficient quantum tomography and complementarity, in preparation
- [26] A.O. Pittenger and M.H. Rubin, Mutually unbiased bases, generalized spin matrices and separability, *Linear Algebra Appl.* **390**(2004), 255–278.
- [27] S. Popa, Orthogonal pairs of $*$ -subalgebras in finite von Neumann algebras, *J. Operator Theory* **9**(1983), 253–268.
- [28] A.E. Rastegin, Statement of uncertainty principle for quantum measurements in terms of the Rényi entropies, arXiv:0807.2691
- [29] M. Rédei, *Quantum Logic in Algebraic Approach*, Fundamental Theories of Physics Vol. **91**, Kluwer Academic Publishers, Dordrecht, Boston and London, 1998.
- [30] J. Schwinger, Unitary operator bases, *Proc. Nat. Acad. Sci. U.S.A.* **46**, 570–579, 1960.
- [31] W. Tadej and K. Życzkowski, A concise guide to complex Hadamard matrices, *Open Syst. Inf. Dyn.* **13**(2006), 133–177.
- [32] Y. Watatani and J. Wierzbicki, Commuting squares and relative entropy for two subfactors, *J. Functional Analysis*, **133**(1995), 329–341.
- [33] S. Wehner and A. Winter, Entropic uncertainty relations - A survey, arXiv: 0907.3704, 2009.
- [34] M. Weiner, A gap for the maximum number of mutually unbiased bases, arXiv: 0902.0635, 2009.
- [35] W.K. Wootters and B.D. Fields, Optimal state determination by mutually unbiased measurements, *Ann. Physics*, **191**, 363–381, 1989.
- [36] H. Weyl, *Theory of groups and quantum mechanics*, Methuen, 1931. (Reprint: Dover, 1950)