PROBABILITY
AND
MATHEMATICAL STATISTICS
Vol. 32, Fasc. 1 (2012), pp. 1–10

ON INDISTINGUISHABILITY OF QUANTUM STATES

BY

MICHAŁ ADAMCZYK (ŁÓDŹ)

Abstract. In this paper we shall study quantum ancillary statistics. For a given quantum measurement M we will define the indistinguishability relation of states in the following way: Two states are *indistinguishable* by M if they generate with M the same probability measure. For such a relation the equivalence classes will be described. At the end we will give some elementary examples of informationally complete measurements that arise from the theorems characterizing the indistinguishability relation.

2000 AMS Mathematics Subject Classification: Primary: 46L53.

Key words and phrases: Quantum measurement, quantum ancillary statistic, informationally complete measurement.

1. INTRODUCTION

Let $\mathcal{H}$ be a separable Hilbert space. Denote by $\mathcal{S}(\mathcal{H})$ the set of quantum states on $\mathcal{H}$ (i.e. positive operators $\rho \in \mathcal{L}(\mathcal{H})$ such that $\mathrm{tr}\rho = 1$) and by $\mathcal{B}(\mathbb{R})$ the Borel σ-field of subsets of $\mathbb{R}$. Let $M\colon \mathcal{B}(\mathbb{R}) \to \mathcal{L}(\mathcal{H})$ be a positive operator valued measure (semi-spectral measure). We shall often call such a measure a *quantum random variable* or a *quantum measurement* in $\big(\mathcal{B}(\mathbb{R}), \mathcal{H}\big)$. For a fixed state $\rho \in \mathcal{S}(\mathcal{H})$, the mapping given by the formula

$$\mathcal{B}(\mathbb{R}) \ni E \mapsto \mathrm{tr}\,\big(M(E)\rho\big)$$

is a genuine probability distribution of a quantum random variable M.

Define a relation of indistinguishability *via* measurement M, denoted by $\simeq_M$, as follows:

$$(1.1)\quad \forall_{\rho_1,\rho_2\in\mathcal{S}(\mathcal{H})}\ \ \rho_1 \simeq_M \rho_2 \iff \forall_{B\in\mathcal{B}(\mathbb{R})}\ \ \mathrm{tr}\, M(B)\rho_1 = \mathrm{tr}\, M(B)\rho_2.$$

It is clear that $\simeq_M$ is an equivalence relation and that ρ_1 and ρ_2 are equivalent if and only if the probability distributions of the quantum random variable M are the same in both considered states. For a given family of states $\{\rho_\theta : \theta \in \Theta\}$, the measurement M for which ρ_θ lie in the same equivalence class of the relation $\simeq_M$ for any θ is called a *quantum ancillary statistic* [3]. The purpose of this paper is to describe the equivalence classes of this relation. More precisely, for a given measurement M we shall describe $[\rho]_{/\simeq_M}$ for any ρ in a certain subclass of $\mathcal{S}(\mathcal{H})$.

In the first part of this paper we shall present a characterization of $[\rho]_{/\simeq_M}$ for pure (vector) states (projections) ρ in the general case. Then we shall outline methods needed, and problems that occur, while trying to generalize the results from the first section to mixed states.

At the end we will recall some results in the dimension two and introduce some elementary constructions of informationally complete measurements which arise when characterization of the indistinguishability of quantum states in dimension two is taken into consideration. The example working in an arbitrary dimension will be given.

Similar issues as well as the background for our approach may be found, for instance, in [7], [4] or [9].

2. THE EQUIVALENCE CLASSES OF INDISTINGUISHABILITY RELATION IN THE GENERAL CASE

Denote by $\mathcal{S}'(\mathcal{H})$ the set of pure states on $\mathcal{H}$ (i.e. one-dimensional projections on $\mathcal{H}$). We shall start with considering the relation $\simeq|\mathcal{S}'(\mathcal{H})\times\mathcal{S}'(\mathcal{H})$. The following notation will be used: if $\star$ is a pure state then $[\star]_{\simeq_M}$ means the equivalence class of the relation of indistinguishability defined on $\mathcal{S}'(\mathcal{H})\times\mathcal{S}'(\mathcal{H})$, otherwise it means the equivalence class of $\simeq_M$ defined in the Introduction. Let $\Pi=\{\Pi_i\}_{i=1}^{\infty}$ be a projective (simple) measurement (i.e. a spectral measure $\Pi:\mathcal{B}(\mathbb{R})\to\mathcal{L}(\mathcal{H})$ such that $\Pi_i=\Pi(B_i)$ for some Borel decomposition $\{B_i\}$ of $\mathbb{R}$). Furthermore, we have $\mathcal{H}=\bigoplus_{n=1}^{\infty}\mathcal{H}_n$, where $\mathcal{H}_i=\operatorname{Ran}(\Pi_i)$. Let $\tilde{U}:\mathcal{H}_i\to\mathcal{H}_i$ be isometries for all i. Extend the operators $\tilde{U}_i$ to isometries on $\mathcal{H}$ trivially: If $\mathcal{H}\ni\phi=\phi_i+\phi_i^{\perp}$, where $\phi_i\in\mathcal{H}_i$, $\phi_i^{\perp}\in\mathcal{H}_i^{\perp}$, then

$$U_i\phi=\tilde{U}_i\phi_i+\phi_i^{\perp}.$$

Define an operator $U:\mathcal{H}\to\mathcal{H}$ by the formula

$$U=\prod_{i=1}^{\infty}U_i. \tag{2.1}$$

Note that the product in (2.1) is strongly convergent. It is also easy to check that U is an isometry on $\mathcal{H}$. Denote the set of such operators by $\mathcal{U}_\Pi$. Let us state an elementary fact that follows from the definition of the probability distribution of the measurement Π:

LEMMA 2.1. *Let $\phi\in\mathcal{H}$ be a pure state and $\Pi=\{\Pi_i\}_{i=1}^{\infty}$ be a simple measurement consisting of the projections Π_i onto subspaces $\mathcal{H}_i\subset\mathcal{H}$. Then*

$$[\phi]_{\simeq_\Pi}=\{U\phi : U\in\mathcal{U}_\Pi\}. \tag{2.2}$$

Note that in the formulation of the above lemma unitary operators instead of isometries may be taken.

Let now $\mathcal{H}$ be finite dimensional. We are now ready to consider a mixed state $\rho \in \mathcal{S}(\mathcal{H})$ with the following spectral decomposition:

$$\rho = \sum_{i=1}^{N} \lambda_i \Pi_{\phi_i}, \quad N \leqslant \dim\mathcal{H},$$

where Π_{ϕ_i} are projections into $\mathrm{lin}\{\phi_i\}$ for some state vectors ϕ_i. Let

$$\Phi = \sum_{i=1}^{N} \sqrt{\lambda_i}\phi_i \otimes \phi_i \in \mathcal{H} \otimes \mathcal{H}$$

be the purification of ρ (see [5] and [8]). Thus, for any $A \in \mathcal{L}(\mathbb{H})$ we have $\mathrm{tr}\,\rho A = \langle \Phi, (A \otimes I)\Phi \rangle$. That means that the measurement $\Pi \otimes I := \{\Pi_i \otimes I\}_{i\in\mathbb{N}}$ is equivalent to the measurement Π in the way that for all $i \in \mathbb{N}$ we have

$$\begin{aligned}\mu_\Phi(i) &= \langle \Phi, (\Pi_i \otimes I)\Phi \rangle \\ &= \mathrm{tr}\,\rho\Pi_i = \mu_\rho(i).\end{aligned}$$

In other words, the probability distribution of $\Pi \otimes I$ in state Φ is the same as that of Π in state ρ. The operators $\Pi_i \otimes I$ are projections onto $\widetilde{\mathcal{H}}_i = \mathcal{H}_i \otimes \mathcal{H}$. Obviously, $\mathcal{H} \otimes \mathcal{H} = \bigoplus_{i=1}^{N} \widetilde{\mathcal{H}}_i$. Applying Lemma 2.1 to the above measurement gives

$$[\Phi]_{/\simeq_{\Pi\otimes I}} = \{U\Phi : U \in \mathcal{U}_{\Pi\otimes I}\}.$$

According to the Schmidt decomposition (see [5]) any state vector $\psi \in \mathcal{H} \otimes \mathcal{H}$ is a purification of some state from $\mathcal{S}(\mathcal{H})$. This leads to the following

LEMMA 2.2. *Let $\mathcal{H}$ be finite dimensional and assume that $\rho \in \mathcal{S}(\mathcal{H})$ is a mixed state and $\Pi = \{\Pi_i\}$ is a simple measurement on $\mathcal{H}$ consisting of projections onto $\mathcal{H}_i$. Then*

$$[\rho]_{/\simeq_\Pi} = \{\mathrm{Tr}_2 U\Phi : U \in \mathcal{U}_{\Pi\otimes I}\},$$

where $\Phi \in \mathcal{H} \otimes \mathcal{H}$ is a purification of ρ and Tr_2 denotes a partial trace of an operator from $\mathcal{L}(\mathcal{H} \otimes \mathcal{H})$.

Note that the assumption $\dim\mathcal{H} < \infty$ is only necessary to prove the existence of the purification of a mixed state. In the following reasoning this assumption will be omitted.

We are now ready to apply Lemma 2.1 to prove the following

THEOREM 2.1. *Let $M = \{M_n\}_{n\in\mathbb{N}}$ be a semi-spectral measure having a countable number of outcomes and let $\mathcal{H}_n$ be a completion of $M_n(\mathcal{H})$ in the norm defined by*

$$\langle \cdot, \cdot \rangle_n = \langle \cdot, M_n \cdot \rangle.$$

Then pure states $\phi, \psi \in \mathcal{H}$ are indistinguishable via measurement M if and only if there exist isometries $\widetilde{U}_n$ on $\mathcal{H}_n$ such that

$$\psi = \sum_{n=1}^{\infty} M_n \widetilde{U}_n P_n \phi, \tag{2.3}$$

where $P_n \in \mathcal{L}(\mathcal{H})$ is the orthogonal projection onto $\overline{M_n(\mathcal{H})}$.

P r o o f. We shall use the construction from the Naimark dilation, so that we can apply Lemma 2.1 to the measurement M. For any $n \in \mathbb{N}$ we have

$$\mathcal{H} = \ker(M_n) \oplus \overline{M_n(\mathcal{H})}.$$

Furthermore, let $\widetilde{\mathcal{H}} = \bigoplus_{n=1}^{\infty} \mathcal{H}_n$ and $U : \mathcal{H} \to \widetilde{\mathcal{H}}$ be an isometry defined as follows: $U\eta = (P_n\eta)_{n\in\mathbb{N}}$ for any $\eta \in \mathcal{H}$, where $P_n \in \mathcal{L}(\mathcal{H})$ is the orthogonal projection onto $\overline{M_n(\mathcal{H})}$. Thus, if $\widetilde{E_n}$ are projections from $\widetilde{\mathcal{H}}$ to $\mathcal{H}$, i.e. $\widetilde{E_n}\big((\eta_k)_{k\in\mathbb{N}}\big) = (0, \dots, 0, \eta_n, 0, \dots)$, then

$$M_n = U^* \widetilde{E}_n U. \tag{2.4}$$

Since (2.4) holds, we infer that the states ϕ, ψ are indistinguishable *via* M if and only if $U\phi$ and $U\psi$ are indistinguishable *via* $\widetilde{E}$. Indeed,

$$\begin{aligned} \mu_\phi(n) &= \langle \phi, M_n \phi \rangle = \langle \phi, U^* \widetilde{E}_n U \phi \rangle \\ &= \langle U\phi, \widetilde{E}_n(U\phi) \rangle \end{aligned}$$

and, similarly,

$$\mu_\psi(n) = \langle U\psi, \widetilde{E}_n(U\psi) \rangle.$$

Hence, by Lemma 2.1, $\phi \in [\psi]_{/\simeq_M}$ if and only if there exists $\widetilde{U} \in \mathcal{U}_{\widetilde{E}}$ such that

$$U\psi = \widetilde{U} U \phi. \tag{2.5}$$

Since U is an isometry, $U^*U = I$. Therefore, we conclude that if ϕ, ψ are indistinguishable *via* M, then

$$\psi = U^* \widetilde{U} U \phi. \tag{2.6}$$

Note that

$$U\phi = (P_k \phi)_{k\in\mathbb{N}}$$

and recall that $\widetilde{U}$ is of the form

$$\widetilde{U} = \widetilde{U}_1 \widetilde{U}_2 \dots,$$

where $\widetilde{U}_k$ are isometries acting nontrivially only on $\mathcal{H}_n$. Hence

$$\widetilde{U}U\phi = (\widetilde{U}_k P_k \phi)_{k\in\mathbb{N}}.$$

What is left is to compute U^*. Let $\chi \in \mathcal{H}$ and $\eta = (\eta_n)_{n\in\mathbb{N}} \in \widetilde{H}$. We have

$$\begin{aligned}\langle(\eta_n), U\chi\rangle &= \langle(\eta_n), (P_n\chi)\rangle = \sum_{n\in\mathbb{N}} \langle \eta_n, P_n\chi_n\rangle_n \\ &= \sum_{n\in\mathbb{N}} \langle \eta_n, M_n P_n \chi\rangle = \sum_{n\in\mathbb{N}} \langle \eta_n, M_n\chi\rangle \\ &= \sum_{n\in\mathbb{N}} \langle M_n\eta_n, \chi\rangle = \Big\langle \sum_{n\in\mathbb{N}} M_n\eta_n, \chi\Big\rangle.\end{aligned}$$

Hence

$$U^*(\eta_n)_{n\in\mathbb{N}} = \sum_{N\in\mathbb{N}} M_n\eta_n.$$

Therefore

$$U^*\widetilde{U}U\phi = \sum_{n\in\mathbb{N}} M_n\widetilde{U}_n P_n\phi.$$

Thus we conclude that the condition (2.3) is necessary for indistinguishability *via* M. Note that the mentioned condition is also sufficient, as the mapping U^* is injective on $U(\mathcal{H})$. Indeed, if $U\xi \in \ker U^*$ for some $\xi \in \mathcal{H}$, then

$$0 = \sum_{n=1}^{\infty} M_n U\xi = \sum_{n=1}^{\infty} M_n P_n\xi = \sum_{n=1}^{\infty} M_n\xi = \xi.$$

Therefore, the equations (2.5) and (2.6) are equivalent, which yields the sufficiency of (2.3). ∎

Consider once again the equation (2.5). It yields that the states ϕ, ψ are indistinguishable *via* M if and only if the equation

$$\|P_n\phi\|_n = \|P_n\psi\|_n \tag{2.7}$$

holds for any $n \in \mathbb{N}$. Recall that the characterization of indistinguishability of pure states for a simple measurement is similar, but does not involve norms defined by different forms than inner product in $\mathbb{H}$.

REMARK 2.1. Note that Theorem 2.1 can be applied to describe the equivalence classes of any pure state in the case when the measurement does not have a countable number of outcomes. We have $\phi \simeq_M \psi$ if and only if for any countable Borel decomposition $\{B_n\}$ of the real line $\phi \simeq_{M_n} \psi$, where $M_n = M(B_n)$. The above theorem gives $\phi \simeq_M \psi$ if and only if for any Borel decomposition $\{B_n\}$ of $\mathbb{R}$ there exist isometries $\widetilde{U^B}_n$ on $\mathcal{H}_n^B$ such that

$$\psi = \sum_{n=1}^{\infty} M_n^B \widetilde{U^B}_n P_n^B \phi, \tag{2.8}$$

where $M_n^B = M(B_n)$, $P_n^B \in \mathcal{L}(\mathcal{H})$ is the orthogonal projection onto $\overline{M_n^B(\mathcal{H}^{\mathcal{B}})}$, and $\mathcal{H}_n^B$ denotes completion of $M_n^B(\mathcal{H})$ in the norm defined by

$$\langle\cdot,\cdot\rangle_n^B = \langle\cdot, M_n^B\cdot\rangle.$$

A simple proof is left to the reader.

We managed to describe equivalence classes of the relation of indistinguishability *via* quantum measurement for pure states in the general case and for mixed states in case of $\dim\mathcal{H} < \infty$ and simple measurement. A question arises whether the assumptions of Lemma 2.2 may be weakened. Note that the existence of purification played an essential role in this theorem. Therefore, the analogue of Lemma 2.2 for infinite dimension cannot be shown as long as the purification in infinite dimension is not introduced. However, it is possible to formulate a similar theorem in finite dimension for a general measurement M having a countable number of outcomes. We can state that performing measurement M on a mixed state ρ is equivalent to performing measurement $M' = M \otimes I$ on a purification Φ of ρ. Then the formula (2.1) can be applied. Writing down the Naimark dilation for M' and applying Theorem 2.1 implies that pure states Φ, Ψ are indistinguishable *via* M' if and only if there exist isometries $\widetilde{U}_n$ on $\mathcal{H}_n$-completions of $M_n(\mathcal{H}) \otimes \mathcal{H}$ such that

$$\Psi = \sum_{n=1}^{\infty} M_n' \widetilde{U}_n P_n \Phi,$$

where P_n are orthogonal projections from $\mathcal{H} \otimes \mathcal{H}$ into $\overline{M_n(\mathcal{H}) \otimes \mathcal{H}}$. Using partial trace to get back to state ρ and measurement M leads to the following theorem:

THEOREM 2.2. *Let* $\dim\mathcal{H} < \infty$ *and let* M *be a measurement on* $\mathcal{H}$ *having a countable number of outcomes. Under the above notation the following equation holds*:

$$[\rho]_{/\simeq_M} = \Big\{\mathrm{Tr}_2 \sum_{n=1}^{\infty} (M_n \otimes I)\widetilde{U}_n P_n \Phi : \widetilde{U}_n \textit{ are isometries on } \mathcal{H}_n\Big\}.$$

3. ELEMENTARY EXAMPLES OF INFORMATIONALLY COMPLETE QUANTUM MEASUREMENTS

In [1] we proved two characterizations of indistinguishability *via* measurement in $\mathbb{C}^2$. Recall that in this case any state $\rho \in \mathcal{S}(\mathbb{C}^2)$ is of the form $\rho = \frac{1}{2}(I + \vec{r}\vec{\sigma})$ for some $\vec{r} \in \mathbb{R}^3$, $\|\vec{r}\| \leqslant 1$, where $\sigma = (\sigma_x, \sigma_y, \sigma_z)$ consists of the Pauli matrices. Moreover, due to the Radon–Nikodým theorem it can be proved easily that any measurement M in $\big(\mathcal{B}(\mathbb{R}), \mathbb{C}^2\big)$ is a measurement with density, i.e. it is of the form

$$\forall_{B\in\mathcal{B}(\mathbb{R})}\ M(B) = \int_B m(\xi)\nu(d\xi), \tag{3.1}$$

where ν is a semi-finite measure and $m(\xi) \in \mathcal{S}(\mathbb{C}^2)$ ν-a.e. Thus it follows that $m(\xi) = \frac{1}{2}(I + \vec{r}_\xi \vec{\sigma})$ ν-a.e. Let $L_M = \mathrm{lin}\{\vec{r}_B : B \in \mathcal{B}(\mathbb{R}), \nu(B) > 0\}$. Thus we have $\mathbb{R}^3 = L_M \oplus U$, $U \perp L_M$. Recall the following

THEOREM 3.1. *Let* $\rho_1, \rho_2 \in \mathcal{S}(\mathbb{C}^2)$, $\rho_i = \frac{1}{2}(I + \vec{r}_i \vec{\sigma})$, $i = 1, 2$. *Then*

$$\rho_1 \simeq_M \rho_2 \iff \vec{r}_1 - \vec{r}_2 \in U.$$

Thus, if $\rho_1 \simeq_M \rho_2$, *then their corresponding vectors in* $\mathbb{R}^3$ *lie in the same affine subspace* U *of* $\mathbb{R}^3$ *orthogonal to* L_M, *and hence of dimension* $3 - \mathrm{dim} L_M$.

If $\mathrm{dim} L_M = 3$, *then* $\rho_1 \simeq_M \rho_2 \iff \rho_1 = \rho_2$.

It leads to some easy results describing classes of equivalence of $\simeq_M$ depending on the dimension of L_M, which are left to the reader. Moreover, it shows that in the case of $\mathrm{dim} H = 2$, a finite number of outcomes are enough to distinguish all states. In fact, such measurements are called *informationally complete* in the sense introduced by Prugovecki in [10]. Recently, a theory of symmetric informationally complete measurements (SIC-POVM) has been developed. The measurements of that kind consist of operators $\{d\Pi_i\}$, where Π_i are rank-one projections, $d = \mathrm{dim}\mathcal{H}$ and the condition $\mathrm{Tr}[\Pi_i \Pi_j] = 1/(d+1)$, $i \neq j$, is fulfilled. There are some analytic and numerical examples of such measurements for the dimensions up to 67 (see [2]). Some constructions of SIC-POVM in particular dimensions were introduced using group theory techniques [11]. However, the existence of SIC-POVM for any finite dimension is still an open question.

Let now $\mathrm{dim} H = n > 2$. In the following theorem we shall give an elementary example of quantum informationally complete measurement. Although it is not symmetric, all the operators it consists of except one are of the form $\{d\Pi_k\}$ for some rank-one projections.

THEOREM 3.2. *If* $\mathrm{dim}\mathcal{H} = n$, *then there exists a measurement* M *having* n^2 *outcomes and such that for all states* ρ *we have* $[\rho]_{/\simeq_M} = \rho$, *i.e.* M *is informationally complete.*

Proof. Let $\{\varphi_i\}_{i=1}^n$ be an orthonormal basis in $\mathcal{H}$ and $\{\psi_0, \psi_1\}$ an orthonormal basis of $\mathbb{C}^2$. Denote by Π_k orthogonal projections onto $\mathrm{lin}\{\varphi_k\}$. For $k, l \in \{1, \ldots, n\}$, $k \neq l$, define a partial isometry $U_{kl} : \mathbb{C}^2 \mapsto \mathcal{H}$ as follows:

$$U_{kl}\psi_0 = \varphi_k,$$
$$U_{kl}\psi_1 = \varphi_l.$$

For $k, l \in \{1, \ldots, n\}$, $k < l$, let us define:

$$\mathbb{I}_{kl} = U_{kl} U_{kl}^* = \Pi_k + \Pi_l,$$
$$\sigma_{kl}^x = U_{kl} \sigma^x U_{kl}^*,$$
$$\sigma_{kl}^y = U_{kl} \sigma^y U_{kl}^*,$$

and

$$A_{kl} := \frac{1}{2}(\mathbb{I}_{kl} + \sigma^x_{kl}) = U_{kl}\frac{1}{2}(\mathbb{I} + \sigma^x)U^*_{kl},$$
$$B_{kl} := \frac{1}{2}(\mathbb{I}_{kl} + \sigma^y_{kl}) = U_{kl}\frac{1}{2}(\mathbb{I} + \sigma^y)U^*_{kl}.$$

Easy calculations show that for any $k, l \in \{1, \ldots, n\}$, $k \leqslant l$, we obtain $(\sigma^x_{kl})^2 = I_{kl} = (\sigma^y_{kl})^2$. Clearly, A_{kl}, B_{kl} are selfadjoint. Furthermore, we have

$$\begin{aligned} A^2_{kl} &= \frac{1}{4}\big(I^2_{kl} + I_{kl}\sigma^x_{kl} + \sigma^x_{kl}I_{kl} + (\sigma^x_{kl})^2\big) \\ &= \frac{1}{4}(I_{kl} + 2\sigma^x_{kl} + I^2_{kl}) \\ &= \frac{1}{2}(I_{kl} + \sigma^x_{kl}) = A_{kl}. \end{aligned}$$

Thus A_{kl} is an idempotent, and hence a projection on $\mathcal{H}$. Similarly, we show that $B^2_{kl} = B_{kl}$ and conclude that B_{kl} are projections. Consequently, $0 \leqslant A_{kl}, B_{kl} \leqslant I$ for all $k, l \in \{1, \ldots, n\}$, $k < l$.

Note that the set $\{A_{kl} : k, l \in \{1, \ldots, n\}, k < l\}$ consists of $\frac{1}{2}(n^2 - n)$ operators. Similarly, the set $\{B_{kl} : k, l \in \{1, \ldots, n\}, k < l\}$ has $\frac{1}{2}(n^2 - n)$ elements. Clearly, $0 \leqslant n^{-2}A_{kl}, n^{-2}B_{kl} \leqslant I$ for all $k, l \in \{1, \ldots, n\}$, $k < l$. Define

$$P = \sum_{i<j} \frac{1}{n^2}(A_{ij} + B_{ij}) + \sum_{k=1}^{n-1} \frac{1}{n^2}\Pi_k.$$

Clearly, P is selfadjoint. We easily get

$$\begin{aligned} \|P\| &\leqslant \sum_{i<j} \frac{1}{n^2}(\|A_{ij}\| + \|B_{ij}\|) + \sum_{k=1}^{n-1} \frac{1}{n^2}\|P_k\| \\ &\leqslant \sum_{i<j} 2\frac{1}{n^2} + \sum_{n} \frac{1}{n^2} \\ &= 2\frac{\frac{1}{2}(n^2 - n)}{n^2} + \frac{n}{n^2} = 1. \end{aligned}$$

Therefore, $\sigma(P) \subset (-\infty, 1\rangle$, and so $\sigma(I - P) \subset [0, +\infty)$, which means that $I - P$ is positive.

Let us consider the measurement M consisting of the following operators:

$$\Big\{\frac{1}{n^2}A_{1,2}, \ldots, \frac{1}{n^2}A_{1,n}, \frac{1}{n^2}A_{2,3}, \ldots, \frac{1}{n^2}A_{2,n}, \ldots, \frac{1}{n^2}A_{n-1,n},$$
$$\frac{1}{n^2}B_{1,2}, \ldots, \frac{1}{n^2}B_{1,n}, \frac{1}{n^2}B_{2,3}, \ldots, \frac{1}{n^2}B_{3,n}, \ldots, \frac{1}{n^2}B_{n-1,n},$$
$$\frac{1}{n^2}P_1, \ldots, \frac{1}{n^2}P_{n-1}, I - P\Big\}.$$

Clearly, M has n^2 outcomes.

To show that M distinguishes all states, note that the operators which the measurement M consists of span the linear space $\mathcal{L}(\mathcal{H})$. Thus, if two states $\rho_1, \rho_2 \in \mathcal{S}(\mathcal{H})$, which can be identified with normalized positive functionals on $\mathcal{L}(\mathcal{H})$, are different, they have to take different values on at least one operator from M, which means that the probability distributions generated by (M, ρ_1) and (M, ρ_2) are different. ■

We will generalize the construction above to the case of infinite-dimensional separable Hilbert spaces. It is clear that in the infinite-dimensional case it is impossible that a measurement consists only of operators of the form $d\Pi_i$ for some rank-one projectors Π_i. Let $\{\varphi_n\}_{n\in\mathbb{N}}$ be an orthonormal basis in $\mathcal{H}$ and I_{jk}, σ^x_{ij}, σ^y_{ij}, A_{ij}, B_{ij}, P_n be defined as in the proof of the theorem above. Now, there are countable numbers of operators A_{ij}, B_{ij} and P_n, so we have to choose the normalization parameters more carefully. Let $f : \mathbb{N} \mapsto \{(i,j) \in \mathbb{N} \times \mathbb{N} : i < j\}$ be bijective. Define

$$M_n = \begin{cases} (3 \cdot 2^k)^{-1} A_{f(k)} & \text{if } n = 3k \text{ for some } k \in \mathbb{N}, \\ (3 \cdot 2^k)^{-1} B_{f(k)} & \text{if } n = 3k-1 \text{ for some } k \in \mathbb{N}, \\ (3 \cdot 2^k)^{-1} P_k & \text{if } n = 3k-2 \text{ for some } k \in \mathbb{N}. \end{cases}$$

Clearly, $M_n \geqslant 0$ and $\sum_n M_n$ is norm convergent. Furthermore, $\big\| \sum_n M_n \big\| \leqslant \sum_n \|M_n\| \leqslant 1$, so $\sigma\big(\sum_n M_n\big) \subset (-\infty, 1]$ and $\sigma\big(I - \sum_n M_n\big) \subset [0, \infty)$, which means that $I - \sum_n M_n \geqslant 0$. Let $M_0 = I - \sum_n M_n$. From the above it is easy to show that $\{M_n\}_{n=0}^{\infty}$ is a measurement with a countable number of outcomes.

Clearly, the system $\{M_n\}_{n\in\mathbb{N}\cup 0}$ is a basis of $\mathcal{L}(\mathcal{H})$. Thus, as in the finite-dimensional case, if states $\rho, \rho' \in \mathcal{S}(\mathcal{H})$ are different, the probability distributions that they generate together with M are different.

The reasoning above is summarized in the following

THEOREM 3.3. *For any separable Hilbert space $\mathcal{H}$ there exists a measurement M with a countable number of outcomes such that $[\rho]_{/\simeq_M} = \rho$ for any state $\rho \in \mathcal{S}(\mathcal{H})$.*

The analysis of dimensions shows that the measurements constructed above are optimal when the amount of outcomes is taken into consideration.

REFERENCES

[1] M. Adamczyk, *On indistinguishability of quantum states*, XII Międzynarodowe Warsztaty dla Młodych Matematyków „Rachunek Prawdopodobieństwa i Statystyka" [The 12th International Workshops for Young Mathematicians "Probability and Statistics"], Institute of Mathematics, Jagiellonian University, 2010, pp. 197–202.

[2] D. M. Appleby, S. T. Flammia and Ch. A. Fuchs, *The Lie algebraic significance of symmetric informationally complete measurements*, preprint available at arXiv:1001.0004v1 [quant-ph]

[3] O. E. Barndorf-Nielsen, R. D. Gill and P. E. Jupp, *On quantum statistical inference*, preprint available at http://www.arxiv.org/quant-ph/0307189
[4] O. Hirota, A. S. Holevo and C. M. Caves (Eds.), *Quantum Communication, Computing, and Measurement*, Plenum Press, 1997.
[5] M. Hirvensalo, *Quantum Computing*, Springer, Berlin–Heidelberg 2003.
[6] A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory*, North-Holland, Amsterdam–New York–Oxford 1982.
[7] A. S. Holevo, *Statistical Structure of Quantum Theory*, Springer, Berlin–Heidelberg 2001.
[8] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.
[9] D. Petz, *Quantum Information Theory and Quantum Statistics*, Springer, Berlin–Heidelberg 2008.
[10] E. Prugovecki, *Information-theoretical aspects of quantum theory*, Internat. J. Theoret. Phys. 16 (5) (1977), pp. 321–331.
[11] J. M. Renes, R. Blume-Kohout, A. J. Scott and C. M. Caves, *Symmetric informationally complete quantum measurements*, preprint available at arXiv:quant-ph/0310075v1

Faculty of Mathematics and Computer Science
Łódź University
ul. Banacha 22
90-238 Łódź, Poland
E-mail: adamczykm@math.uni.lodz.pl

Received on 9.12.2010;
revised version on 1.10.2011