ISSN 0081-5438, Proceedings of the Steklov Institute of Mathematics, 2021, Vol. 313, pp. 113–119. © Pleiades Publishing, Ltd., 2021.
Russian Text © The Author(s), 2021, published in Trudy Matematicheskogo Instituta imeni V.A. Steklova, 2021, Vol. 313, pp. 124–130.

Increasing the Distinguishability of Quantum States with an Arbitrary Success Probability

D. A. Kronberg [a]

Received September 7, 2020; revised November 5, 2020; accepted February 25, 2021

Abstract—It is well known that nonorthogonal quantum states cannot be reliably distinguished; however, for a number of sets of quantum states, the operation of unambiguous discrimination is possible, which either provides full information or yields an inconclusive result. In this paper, a generalization of such a transformation is constructed that has an increased success probability and makes the states more distinguishable. It is shown that after this transformation the states can be reliably distinguished without loss of the total success probability.

DOI: 10.1134/S0081543821020115

1. INTRODUCTION

Consider an ensemble $\{|\psi_i\rangle, p_i\}_{i=1}^N$ of pure linearly independent quantum states $\{|\psi_i\rangle\}_{i=1}^N$ with probabilities $\{p_i\}_{i=1}^N$ in a Hilbert space $\mathcal{H}$ of dimension N. It is well known that if these states are not mutually orthogonal, then their reliable discrimination is impossible. However, one can perform unambiguous state discrimination (USD), which in case of success provides full information on the signal, but sometimes it randomly gives an inconclusive result, which indicates failure [8, 6, 11].

Such a measurement is defined by a positive operator-valued measure (POVM) $\Pi = \{\Pi_i\}_{i=0}^N$, in which the elements corresponding to conclusive results are given by

$$\Pi_i = \eta_i |\psi_i^\perp\rangle\langle\psi_i^\perp|, \qquad i = 1, \dots, N, \tag{1.1}$$

where $|\psi_i^\perp\rangle$ is the projection onto the orthogonal complement of the space spanned by the states $\{|\psi_k\rangle\}$ with $k \neq i$. The element $\Pi_0 = I - \sum_{i=1}^N \Pi_i$ of the observable corresponds to an inconclusive result, and we should have $\Pi_0 \geq 0$. Each conclusive element Π_i corresponds to a state $|\psi_i\rangle$, since the probability of outcome i when another state is measured is zero:

$$p(i|j) = \mathrm{Tr}(\Pi_i |\psi_j\rangle\langle\psi_j|) = \eta_i |\langle\psi_i^\perp|\psi_j\rangle|^2 = p_i^{\mathrm{succ}} \delta_{ij}.$$

The quantity

$$p_i^{\mathrm{succ}} = \eta_i |\langle\psi_i^\perp|\psi_i\rangle|^2 \tag{1.2}$$

in this expression is the probability of a successful (conclusive) outcome for the state $|\psi_i\rangle$, and this quantity depends on the coefficient η_i.

One of the important longstanding problems was to construct an optimal unambiguous discrimination of states, i.e., to find the coefficients $\{\eta_i\}_{i=1}^N$ that maximize the average success probability

$$P^{\mathrm{succ}} = \sum_{i=1}^N p_i p_i^{\mathrm{succ}} \tag{1.3}$$

under the constraint $\Pi_0 \geq 0$. This problem was solved in [3] for an arbitrary set of pure states.

[a] Steklov Mathematical Institute of Russian Academy of Sciences, ul. Gubkina 8, Moscow, 119991 Russia.
E-mail address: dmitry.kronberg@gmail.com

In the present paper, we consider the problem of constructing a more general transformation which makes the input states more distinguishable but has a higher success probability compared with the unambiguous discrimination (1.1). However, in this case the output states cannot be made completely orthogonal, since this would mean obtaining reliable information with a success probability higher than that allowed by the unitarity relations.

The paper is organized as follows. Section 2 is devoted to constructing channels with two Kraus operators that make the states orthogonal in case of success. Then, in Section 3, we consider a generalization of this transformation to the case of an arbitrary success probability. In the Conclusions, we present considerations on the application of such transformations to eavesdropping in quantum cryptography.

2. ORTHOGONALIZING CHANNEL

In [5], the authors proposed the idea of a two-step postselective measurement: in the first step, one uses a channel related to an observable given by two operators

$$\Pi^{\mathrm{succ}} = \frac{p^{\mathrm{succ}}}{N}\rho^{-1} \qquad \text{and} \qquad \Pi^{\mathrm{fail}} = I - \Pi^{\mathrm{succ}},$$

where $\rho = \sum_{i=1}^{N} |\psi_i\rangle\langle\psi_i|$ and Π^{succ} corresponds to the successful application of the operation. The measurement in the second step has no postselection and is applied if the first step is successful.

Let us show that such a process can also be applied in a more general case.

Proposition 1. *Suppose that the vectors $\{|\psi_i\rangle\}_{i=1}^{N}$ are normalized and linearly independent. Then, for any operator*

$$Q = \sum_{i=1}^{N} q_i |\psi_i\rangle\langle\psi_i|, \tag{2.1}$$

where $q_i > 0$, the vectors $|\nu_i\rangle = Q^{-1/2}|\psi_i\rangle$ have the property

$$\langle\nu_i|\nu_j\rangle = \frac{1}{q_i}\delta_{ij}. \tag{2.2}$$

Proof. We use a simple generalization of the result from [12]. Consider an orthonormal basis $\{|\omega_i\rangle\}_{i=1}^{N}$ and an operator X of transition from this basis to the vectors $\{|\psi_i\rangle\}_{i=1}^{N}$: $|\psi_i\rangle = X|\omega_i\rangle$. Since the vectors $\{|\psi_i\rangle\}_{i=1}^{N}$ are linearly independent, X is nondegenerate; therefore, the inverse operator X^{-1} exists. The operator Q can be expressed as

$$Q = \sum_i q_i X|\omega_i\rangle\langle\omega_i|X^{\dagger} = X\left(\sum_i q_i|\omega_i\rangle\langle\omega_i|\right)X^{\dagger}; \tag{2.3}$$

hence,

$$Q^{-1} = (X^{\dagger})^{-1}\left(\sum_i \frac{1}{q_i}|\omega_i\rangle\langle\omega_i|\right)X^{-1}. \tag{2.4}$$

Now, for the inner product we obtain

$$\langle\nu_i|\nu_j\rangle = \langle\psi_i|Q^{-1}|\psi_j\rangle = \langle\omega_i|X^{\dagger}Q^{-1}X|\omega_j\rangle = \langle\omega_i|\left(\sum_k \frac{1}{q_k}|\omega_k\rangle\langle\omega_k|\right)|\omega_j\rangle = \frac{1}{q_i}\delta_{ij}. \qquad \square \tag{2.5}$$

This proposition implies that in case of success the channel defined by the Kraus operators

$$A^{\mathrm{succ}} = Q^{-1/2} \qquad \text{and} \qquad A^{\mathrm{fail}} = (I - Q^{-1})^{1/2} \tag{2.6}$$

(with $I - Q^{-1} \geq 0$) maps the states to a set of orthogonal states proportional to $|\nu_i\rangle$, with the success probability for each state being

$$p_i^{\text{succ}} = \langle\psi_i|Q^{-1}|\psi_i\rangle. \tag{2.7}$$

Let us show how any unambiguous discrimination (1.1) can be reduced to such an operation.

Proposition 2. *For an arbitrary set of positive coefficients $\{\eta_i\}_{i=1}^N$, consider the operator*

$$P = \sum_{i=1}^N \eta_i |\psi_i^\perp\rangle\langle\psi_i^\perp|.$$

Then the vectors $\{P^{1/2}|\psi_i\rangle\}_{i=1}^N$ are mutually orthogonal.

Proof. Let us show that the operators P and

$$Q = \sum_{i=1}^N \frac{1}{\eta_i |\langle\psi_i^\perp|\psi_i\rangle|^2} |\psi_i\rangle\langle\psi_i|$$

are mutually inverse. It is easy to see that for the product of these operators

$$PQ = \sum_{i=1}^N \frac{\langle\psi_i^\perp|\psi_i\rangle}{|\langle\psi_i^\perp|\psi_i\rangle|^2} |\psi_i^\perp\rangle\langle\psi_i|$$

and any states $|\psi_i\rangle$ and $|\psi_j\rangle$ the following equality holds:

$$\langle\psi_i|PQ|\psi_j\rangle = \langle\psi_i|\psi_i^\perp\rangle\langle\psi_i|\psi_j\rangle \frac{\langle\psi_i^\perp|\psi_i\rangle}{|\langle\psi_i^\perp|\psi_i\rangle|^2} = \langle\psi_i|\psi_j\rangle;$$

therefore, $PQ = I$. Using Proposition 1, we see that the vectors $\{P^{1/2}|\psi_i\rangle\}_{i=1}^N$ are mutually orthogonal. □

It is easy to see that the success probability coincides with the success probability (1.2) under the application of (1.1):

$$p_i^{\text{succ}} = \langle\psi_i|P|\psi_i\rangle = \eta_i |\langle\psi_i^\perp|\psi_i\rangle|^2.$$

Thus, for any set of positive coefficients $\{\eta_i\}_{i=1}^N$, the measurement (1.1) can be reduced to a transformation of the form (2.6) that maps the states to an orthogonal set with given success probabilities.

When some of the coefficients $\{\eta_i\}_{i=1}^N$ vanish, the success probability on the corresponding state is obviously zero, and so the measurement (1.1) does not identify the corresponding states in this case. Setting coefficients to zero may make sense both in the case of maximizing the success probability on states for which this is more important (different problems may imply different importance of success for different states) and, for example, in the case of applying unambiguous discrimination to a set of states that contains a linearly dependent subset. Since unambiguous discrimination is impossible for linearly dependent states, it often makes sense to choose zero coefficients for the signals corresponding to linearly dependent states; then the remaining signals would yield unambiguous discrimination for the states for which this is possible.

Proposition 2 also remains valid in the presence of zero coefficients $\{\eta_i\}_{i=1}^N$, with the only difference that in this case only the states corresponding to nonzero coefficients become orthogonal, and the summation in the operator Q is performed only over such positions.

Note that this correspondence loses its meaning when the measurement (1.1) contains only one nonzero coefficient. Such a measurement corresponds to unambiguous identification of one of the states of the ensemble, and the probability of a conclusive outcome on this state can be made maximal in this case. However, the problem of mapping a single state to an orthogonal set is, of course, meaningless.

3. INCREASING THE DISTINGUISHABILITY OF STATES WITH ARBITRARY SUCCESS PROBABILITY

An important property of the transformation (2.6) is the fact that it can be applied in a weak form, as will be shown in this section.

First, notice that if $I - Q^{-1} = 0$, then $\lambda_{\max}(Q^{-1}) = \lambda_{\min}(Q) = 1$, where $\lambda_{\max}$ and $\lambda_{\min}$ are the maximum and minimum eigenvalues, respectively. If the inequality in the applicability condition for (2.6) is strict ($I - Q^{-1} > 0$), then, instead of the operator $Q^{-1/2}$ in (2.6), we can consider the proportionally increased operator $(\lambda_{\max}(Q^{-1}))^{-1/2}Q^{-1/2}$, which improves all the success probabilities (2.7) due to the inequality $\lambda_{\max}(Q^{-1}) < 1$. Therefore, below we assume that $\lambda_{\max}(Q^{-1}) = \lambda_{\min}(Q) = 1$.

Now, consider a generalization of the channel (2.6) with a parameter p:

$$A^{\mathrm{succ}} = Q^{-p/2} \qquad \text{and} \qquad A^{\mathrm{fail}} = (I - Q^{-p})^{1/2}. \tag{3.1}$$

For $p = 1$, this channel corresponds to the original transformation (2.6); however, for smaller values of p, this is a partial application of a similar transformation, which does not make the states of the ensemble completely orthogonal any longer but has (as we will show below) a higher success probability. For $p = 0$, this is a trivial transformation, which is always successful but does nothing with the ensemble of states.

Under the transformation (3.1), in case of success the original ensemble turns into the ensemble

$$\{|\psi_i\rangle, p_i\} \to \left\{ \frac{Q^{-p/2}|\psi_i\rangle}{\sqrt{\langle\psi_i|Q^{-p}|\psi_i\rangle}}, p_i\langle\psi_i|Q^{-p}|\psi_i\rangle \right\},$$

and one can easily verify that applying the transformation described by the channel

$$A^{\mathrm{succ}} = Q^{-(1-p)/2} \qquad \text{and} \qquad A^{\mathrm{fail}} = (I - Q^{p-1})^{1/2} \tag{3.2}$$

to the new ensemble yields, in case of success, the orthogonal (by Proposition 1) set

$$\left\{ \frac{Q^{-1/2}|\psi_i\rangle}{\sqrt{\langle\psi_i|Q^{-1}|\psi_i\rangle}}, p_i\langle\psi_i|Q^{-1}|\psi_i\rangle \right\}. \tag{3.3}$$

This is the essence of "partial" application of unambiguous discrimination of states: under the transformation (3.1), the ensemble of states turns, in case of success, into a new ensemble which can be further brought to an orthogonal ensemble with higher success probability compared to that for the original ensemble. The total success probability is not changed, which means that the constructed transformation is efficient:

$$p_i^{\mathrm{succ}} = \langle\psi_i|Q^{-p}|\psi_i\rangle\langle\psi_i|Q^{p-1}|\psi_i\rangle = \langle\psi_i|Q^{-1}|\psi_i\rangle.$$

Since $p_i^{\mathrm{succ}} < 1$ for any ensemble of nonorthogonal states, it is obvious from the last relation that the success probability for each of the two partial transformations above is higher than the success probability for the final transformation. By appropriately setting the parameter p, one can get any average success probability for the first transformation,

$$P_p^{\mathrm{succ}} = \sum_{i=1}^{N} p_i\langle\psi_i|Q^{-p}|\psi_i\rangle,$$

in the range $[P^{\mathrm{succ}}, 1]$, where P^{succ} is the quantity defined in (1.3). In a similar way one can decompose the transformation into a sequence of partial transformations whose parameters $\{p_k\}_k$ sum to unity. There is no decrease in the total success probability in this case.

The results presented above can be formulated as the following theorem.

Theorem. *Let $\mathcal{E}$ be an ensemble of pure linearly independent states. Suppose that the unambiguous discrimination observable* (1.1) *yields the average success probability* (1.3) *equal to p^{succ}. Then, for any probability $p' \in [p^{\mathrm{succ}}, 1)$, there exists a parameter $p \in (0, 1]$ such that the map*

$$A^{\mathrm{succ}} = Q^{-(1-p)/2} \qquad \text{and} \qquad A^{\mathrm{fail}} = (I - Q^{p-1})^{1/2}$$

has the following properties:

(1) *it maps the ensemble $\mathcal{E}$ to a new ensemble $\mathcal{E}'$ with success probability p'*;

(2) *for the new ensemble $\mathcal{E}'$, the success probability of unambiguous discrimination is higher than p_{succ}.*

Note that the channel defined by the Kraus operators $\{\Pi_i^{-1/2}\}_{i=0}^N$ related to the observable (1.1) does not transform states to orthogonal ones. The orthogonality of output states can be achieved by using classical measurement outcomes to prepare new states, which corresponds to the channel [4]

$$A_i = \frac{\sqrt{p_i^{\mathrm{succ}}}}{|\langle\psi_i^\perp|\psi_i\rangle|}|a_i\rangle\langle\psi_i^\perp|$$

with an orthogonal set $|a_i\rangle$ (augmented with an inconclusive outcome operator A_0), which cannot be directly generalized to the case of an arbitrary success probability.

Note also that for any $p \in [0, 1]$ the condition $I - Q^{-1} = 0$ implies the equality $I - Q^{-p} = 0$; therefore, the channels (3.1) and (3.2) are well defined.

As an example of such a transformation, we can consider the case of unambiguous discrimination (1.1) in which the success probability (1.2) is the same for all states of the ensemble, which is achieved by setting

$$\eta_i \propto \frac{1}{|\langle\psi_i^\perp|\psi_i\rangle|^2}.$$

Such an observable corresponds to the operator $Q = \alpha\sum_{i=1}^N |\psi_i\rangle\langle\psi_i|$, where α is chosen from the requirement $\lambda_{\min}(Q) = 1$. For such a choice of the parameters, the transformation (3.1) makes the ensemble of states more distinguishable by approaching it to the ensemble of orthogonal states, while preserving their probabilities. In other particular cases, such a transformation can be used for eavesdropping in quantum cryptography.

As another example, consider the operator Q in which the signal probabilities are taken into account:

$$Q = \alpha\sum_{i=1}^N p_i|\psi_i\rangle\langle\psi_i|,$$

where α is again chosen from the requirement $\lambda_{\min}(Q) = 1$. A remarkable property of the channel (3.1) associated with such an operator is that for $p = 1$ the mean state of the new ensemble (3.3) is proportional to the identity operator:

$$\begin{aligned}\sum_{i=1}^N p_i\langle\psi_i|Q^{-1}|\psi_i\rangle\frac{Q^{-1/2}|\psi_i\rangle\langle\psi_i|Q^{-1/2}}{\langle\psi_i|Q^{-1}|\psi_i\rangle} &= \sum_{i=1}^N p_i Q^{-1/2}|\psi_i\rangle\langle\psi_i|Q^{-1/2}\\ &= Q^{-1/2}\left(\sum_{i=1}^N p_i|\psi_i\rangle\langle\psi_i|\right)Q^{-1/2} = \frac{1}{\alpha}I.\end{aligned}$$

This implies that all states become equiprobable.

Consider the Holevo quantity of an ensemble of states [7], which characterizes the maximum of classical information extracted from the ensemble and which is equal for pure states to

$$\chi(\{|\psi_i\rangle\},\{p_i\}) = S\left(\sum_{i=1}^{N} p_i|\psi_i\rangle\langle\psi_i|\right),$$

where $S(\rho) = -\operatorname{Tr}\rho\log\rho$ is the von Neumann entropy.

For the transformation in the last example, the Holevo quantity of the ensemble increases with increasing p, until it becomes equal to $\log N$ for $p = 1$, i.e., to the Holevo quantity for the ideal data transmission, which is achieved, among other things, by changing the probabilities of states: the most probable states give a successful result with lower probability, while the low-probability states have higher success probability, which affects the final probabilities of the states. Note also that the last transformation can be applied to the case of classical (diagonalizable in a single basis) signals as well, which results in equalization of the signal probabilities, namely, in the exclusion of a part of states of highest probability.

However, in the general case of arbitrary Q, we cannot argue that the Holevo quantity for the channel (2.6) will certainly increase in case of success, because changes in signal probabilities that lead to a decrease in this quantity are also possible.

CONCLUSIONS

An important property of ensembles of quantum states is that they cannot be reliably distinguished. However, in a number of cases, this restriction can be overcome in a probabilistic way with the use of postselective measurements. In this paper, we have proposed a generalization of the transformation of unambiguous discrimination of quantum states, which can be constructed for any success probability. In case of success, this transformation makes the states more distinguishable in the sense that the probability of unambiguous discrimination of new states becomes higher.

The proposed transformation also applies to sets of states for which reliable discrimination is impossible due to their linear dependence. The situation is similar to that with the filtering transformation [1], which, in the case of four states in the two-dimensional space, makes the states in each pair mutually orthogonal.

A particular case of the transformation is the soft filtering operation, which has already been used in constructing new eavesdropping strategies in quantum cryptography (see [2, 9, 10]).

The main reasons why such a transformation may be useful to the eavesdropper are as follows:

- the eavesdropper does not need to spend resources on distinguishing between all states, because in a number of protocols one can use the subsequently obtained additional information; for example, this may be the information that the states belong to a subset of the original ensemble, which is important in the presence of control states or in the case when the transmitted states are divided into different bases;
- in a configuration of states for which the probability of unambiguous discrimination of all states is too low, such a transformation allows one to obtain partial information with higher success probability; in particular, this makes partial eavesdropping more efficient for large distances between legitimate users;
- the additional parameter allows one to better adjust the attack parameters to different situations, thus making eavesdropping more flexible.

A drawback of the proposed transformation is that it cannot be directly generalized to the case of unambiguous identification of one of the states of the ensemble, because the transformation is aimed at mapping a set of vectors to an orthogonal set, which loses its meaning for a set consisting of only one state.

Another drawback of the constructed transformation is that it does not produce the desired effect on a set of mixed states. It is known that in many cases mixed states can also be unambiguously distinguished; however, Proposition 1 does not hold for them, because the operator Q involved in it maps mixed states to a set of mixed states for which it is inappropriate to speak of mutual orthogonality. Thus, the proposed construction needs to be modified for one to be able to apply it to mixed states.

ACKNOWLEDGMENTS

I am grateful to N. Kenbaev, A. Kozubov, and A. Gaidash for useful discussions.

FUNDING

This work is supported by the Russian Science Foundation under grant 20-71-10072.

REFERENCES

1. A. Acín, N. Gisin, and V. Scarani, "Coherent-pulse implementations of quantum cryptography protocols resistant to photon-number-splitting attacks," Phys. Rev. A **69** (1), 012309 (2004).
2. A. S. Avanesov, D. A. Kronberg, and A. N. Pechen, "Active beam splitting attack applied to differential phase shift quantum key distribution protocol," p-Adic Numbers, Ultrametric Anal. Appl. **10** (3), 222–232 (2018).
3. J. A. Bergou, U. Futschik, and E. Feldman, "Optimal unambiguous discrimination of pure quantum states," Phys. Rev. Lett. **108** (25), 250502 (2012).
4. A. Chefles, "Unambiguous discrimination between linearly independent quantum states," Phys. Lett. A **239** (6), 339–347 (1998).
5. S. Croke, E. Andersson, S. M. Barnett, C. R. Gilson, and J. Jeffers, "Maximum confidence quantum measurements," Phys. Rev. Lett. **96** (7), 070401 (2006).
6. D. Dieks, "Overlap and distinguishability of quantum states," Phys. Lett. A **126** (5–6), 303–306 (1988).
7. A. S. Holevo, *Quantum Systems, Channels, Information* (MTsNMO, Moscow, 2010). Engl. transl.: *Quantum Systems, Channels, Information: A Mathematical Introduction* (de Gruyter, Berlin, 2012), de Gruyter Stud. Math. Phys. **16**.
8. I. D. Ivanovic, "How to differentiate between non-orthogonal states," Phys. Lett. A **123** (6), 257–259 (1987).
9. D. A. Kronberg and Yu. V. Kurochkin, "Role of intensity fluctuations in quantum cryptography with coherent states," Quantum Electron. **48** (9), 843–848 (2018) [transl. from Kvant. Electron. **48** (9), 843–848 (2018)].
10. D. A. Kronberg, A. S. Nikolaeva, Yu. V. Kurochkin, and A. K. Fedorov, "Quantum soft filtering for the improved security analysis of the coherent one-way quantum-key-distribution protocol," Phys. Rev. A **101** (3), 032334 (2020).
11. A. Peres, "How to differentiate between non-orthogonal states," Phys. Lett. A **128** (1–2), 19 (1988).
12. M. Sasaki, K. Kato, M. Izutsu, and O. Hirota, "Quantum channels showing superadditivity in classical capacity," Phys. Rev. A **58** (1), 146–158 (1998).

Translated by I. Nikitin