Success probability for postselective transformations of pure quantum states

D. A. Kronberg *

Department of Mathematical Methods for Quantum Technologies, Steklov Mathematical Institute of Russian Academy of Sciences, Gubkina St. 8, Moscow 119991, Russia

(Received 20 July 2022; accepted 12 October 2022; published 31 October 2022)

The situation is studied when an ensemble of pure quantum states is mapped onto another ensemble of pure quantum states. In general, this operation may not be done with unit probability. In this work, the bounds for success probability of such operation are provided, with closed-form expressions involving the Gram matrices and quantum max-relative entropy. We also discuss a partial version of this operation which has arbitrary success probability.

DOI: 10.1103/PhysRevA.106.042447

I. INTRODUCTION

The class of quantum operations which can be implemented with nonunit success probability, is significantly broader, than the class of deterministic quantum operations [1–7]. A notable example is unambiguous state discrimination (USD) [8–10], which performs zero-error discrimination between the set of linearly independent nonorthogonal quantum states, while complete discrimination with unit probability is not allowed by the laws of quantum mechanics. USD may be viewed as a map from the ensemble of linearly independent states to the set of mutually orthogonal states.

In this paper, we consider a general transformation between the two arbitrary ensembles of pure quantum states, not necessarily linearly independent. The probability distributions of the states within the ensembles may be different, which corresponds to the situation when success probabilities are not the same for different input states. We provide lower and upper bounds for success probability of the transformation in terms of quantum max-relative entropy and Gram matrices for the input and output ensembles. As we show, these bounds do differ only in dealing with the environment.

The paper is organized as follows: In Sec. II we introduce our notations and recall the definitions for quantum instrument, the Gram matrix and max-relative entropy. In Sec. III we provide a lower bound for success probability and explicitly propose an instrument which does the work. In Sec. IV we generalize the statement to become an upper bound for arbitrary instrument which may perform the required map. Section V describes a generalization of our transformation which does partial work with arbitrary high success probability.

II. PRELIMINARIES

A general case of a quantum channel, i.e., a completely positive trace preserving (CPTP) map which includes discrete classical outcomes $\{m\}$, is described by a quantum instrument [11]

$$\mathcal{M} = \{V_{mk}\}_{m,k}, \quad \sum_{m,k} V_{mk}^\dagger V_{mk} = I. \tag{1}$$

The probability of the outcome m with input state ρ is given by

$$p(m|\rho) = \mathrm{Tr}\left(\sum_k V_{mk}\rho V_{mk}^\dagger\right),$$

and, in case of this outcome, the state is transformed into

$$\rho \xrightarrow{m} \frac{1}{p(m|\rho)}\sum_k V_{mk}\rho V_{mk}^\dagger = \Phi_m[\rho], \tag{2}$$

thus the total transformation can be written as

$$\Phi[\rho] = \sum_{m,k} V_{mk}\rho V_{mk}^\dagger = \sum_m p(m|\rho)\Phi_m[\rho], \tag{3}$$

where classical register value m becomes known after the transformation.

Let us consider an ensemble $\mathcal{E}_A = \{p_i, |\varphi_i\rangle\}_{i=1}^N$ of N pure quantum states, each with probability $p_i > 0$, in Hilbert space $\mathcal{H}_K$ of dimension $K \leqslant N$, and, similarly, another ensemble $\mathcal{E}_B = \{q_i, |\psi_i\rangle\}_{i=1}^N$ in the same Hilbert space, with $q_i \geqslant 0$, $\sum_i p_i = \sum_i q_i = 1$. For the input ensemble $\mathcal{E}_A$ we do not consider zero probabilities, as one can just remove the corresponding states.

We are interested in a particular case of instrument with two classical outcomes {succ, fail} corresponding to success and failure. This operation should in case of success perform the mapping $\mathcal{E}_A \xrightarrow{\text{succ}} \mathcal{E}_B$, i.e.,

$$p(\text{succ}|i)p_i\Phi_{\text{succ}}[|\varphi_i\rangle\langle\varphi_i|] = p_{\text{succ}}q_i|\psi_i\rangle\langle\psi_i|. \tag{4}$$

Here, q_i can be regarded as conditional probabilities, and, according to Bayes' theorem,

$$q_i = p(i|\text{succ}) = \frac{p(\text{succ}|i)p_i}{p_{\text{succ}}}, \tag{5}$$

where

$$p_{\text{succ}} = \mathrm{Tr}\left[\sum_k V_{\text{succ},k}\left(\sum_{i=1}^N p_i|\varphi_i\rangle\langle\varphi_i|\right)V_{\text{succ},k}^\dagger\right]$$
$$= \sum_{i=1}^N p(\text{succ}|i)p_i$$

*dmitry.kronberg@gmail.com

is average success probability for the input ensemble, and

$$p(\text{succ}|i) = \text{Tr}\left[\sum_k V_{\text{succ},k}|\varphi_i\rangle\langle\varphi_i|V^\dagger_{\text{succ},k}\right] = \frac{q_i}{p_i}p_{\text{succ}} \tag{6}$$

is conditional success probability for input state $|\varphi_i\rangle$.

The Gram matrices for the input and output ensembles read

$$G_A = \{\langle\varphi_i|\varphi_j\rangle\}^N_{i,j=1} = \{|e_i\rangle\langle\varphi_i|\varphi_j\rangle\langle e_j|\}^N_{i,j=1},$$
$$G_B = \{\langle\psi_i|\psi_j\rangle\}^N_{i,j=1} = \{|e_i\rangle\langle\psi_i|\psi_j\rangle\langle e_j|\}^N_{i,j=1}.$$

Here, $\{|e_i\rangle\}^N_{i=1}$ is some fixed orthonormal basis.

Let us also introduce matrices

$$P = \sum_{i=1}^N \sqrt{p_i}|e_i\rangle\langle e_i|, \quad Q = \sum_{i=1}^N \sqrt{q_i}|e_i\rangle\langle e_i|$$

for corresponding probabilities.

Recall that quantum max-relative entropy [12] is defined as

$$D_{\max}(\rho\|\sigma) = -\log_2 \max\{\lambda : \sigma - \lambda\rho \geqslant 0\},$$

or, if σ is invertible,

$$D_{\max}(\rho\|\sigma) = \log_2 \lambda_{\max}(\sigma^{-\frac{1}{2}}\rho\sigma^{-\frac{1}{2}}).$$

III. LOWER BOUND FOR SUCCESS PROBABILITY

We are now ready to formulate the main result:

Theorem 1. For the two given ensembles, $\mathcal{E}_A$ and $\mathcal{E}_B$, there exists a quantum channel (3), which maps $\mathcal{E}_A$ on $\mathcal{E}_B$ with average success probability

$$p_{\text{succ}} = 2^{-D_{\max}(QG_BQ\|PG_AP)}. \tag{7}$$

Proof. Let us first consider the case when all the states $\{|\varphi_i\rangle\}^N_{i=1}$ are linearly independent. Let us define

$$A = \sum_{i=1}^N |\varphi_i\rangle\langle e_i|, \quad G_A = A^\dagger A,$$
$$B = \sum_{i=1}^N |\psi_i\rangle\langle e_i|, \quad G_B = B^\dagger B.$$

Transformation A is invertible, and one can easily see the following:

$$A^{-1}|\varphi_i\rangle = |e_i\rangle, \quad P^{-1}A^{-1}\sqrt{p_i}|\varphi_i\rangle = |e_i\rangle,$$
$$QP^{-1}A^{-1}\sqrt{p_i}|\varphi_i\rangle = \sqrt{q_i}|e_i\rangle,$$
$$BQP^{-1}A^{-1}\sqrt{p_i}|\varphi_i\rangle = \sqrt{q_i}|\psi_i\rangle,$$

hence, the operator $M_s = cBQP^{-1}A^{-1}$ with some real c performs the required map (4). For the correct definition of the channel (3), the condition $I - M_s^\dagger M_s \geqslant 0$ is required, thus $\lambda_{\max}(M_s^\dagger M_s) \leqslant 1$, which results in

$$c^{-2} = \lambda_{\max}[(A^\dagger)^{-1}P^{-1}QB^\dagger BQP^{-1}A^{-1}] = \lambda_{\max}[(PA^\dagger AP)^{-1}(QB^\dagger BQ)] = 2^{D_{\max}(QG_BQ\|PG_AP)},$$

thus, $c^2 = 2^{-D_{\max}(QG_BQ\|PG_AP)}$, and we obtain from (5) that

$$q_i = 2^{-D_{\max}(QG_BQ\|PG_AP)}p_i, \quad i = 1,\ldots,N.$$

Hence, by using (6), we obtain

$$p(\text{succ}|i) = \text{Tr}[M_s|\varphi_i\rangle\langle\varphi_i|M_s^\dagger] = \frac{q_i}{p_i}2^{-D_{\max}(QG_BQ\|PG_AP)},$$

and, finally,

$$p_{\text{succ}} = \sum_{i=1}^N p(\text{succ}|i)p_i = 2^{-D_{\max}(QG_BQ\|PG_AP)}\sum_{i=1}^N q_i = 2^{-D_{\max}(QG_BQ\|PG_AP)}.$$

Let us now consider the case of linearly dependent states $\{|\varphi_i\rangle\}^N_{i=1}$. It follows directly from the definition of max-relative entropy, that if the rank of the Gram matrix G_B is larger than the rank of G_A, max-relative entropy equals $+\infty$, and $p_{\text{succ}} = 0$. Hence, let us consider only the case of $\text{rank}G_B \leqslant \text{rank}G_A$.

Without loss of generality, let us assume that the first K vectors are linearly independent, and consider the set of $K+1$ vectors for the following lemma, which states the linearity restriction for the output ensemble in terms of max-relative entropy:

Lemma 1. Consider the ensemble of K linearly independent states $\{p_i, |\varphi_i\rangle\}^K_{i=1}$, and the state $|\varphi_{K+1}\rangle$ with corresponding probability p_{K+1}, such that $\sqrt{p_{K+1}}|\varphi_{K+1}\rangle = \sum_{i=1}^K c_i\sqrt{p_i}|\varphi_i\rangle$. Let us also consider an output ensemble $\{q_i, |\psi_i\rangle\}^{K+1}_{i=1}$. If $\sqrt{q_{K+1}}|\psi_{K+1}\rangle \neq \sum_{i=1}^K c_i\sqrt{q_i}|\psi_i\rangle$, then for the corresponding Gram matrices $D_{\max}(QG_BQ\|PG_AP) = +\infty$.

Proof. Let us set $c_{K+1} = -1$, and consider a vector

$$|v\rangle = \sum_{i=1}^{K+1} c_i|e_i\rangle.$$

For this vector,

$$AP|v\rangle = \sum_{i=1}^{K+1} c_i\sqrt{p_i}|\varphi_i\rangle.$$

It is straightforward to see that $AP|v\rangle = 0$, hence, $\langle v|PG_AP|v\rangle = 0$. Now let us see that

$$BQ|v\rangle = \sum_{i=1}^{K+1} c_i\sqrt{q_i}|\psi_i\rangle,$$

and, according to the condition of Lemma, $BQ|v\rangle$ is not a zero vector. Hence, for any $\lambda > 0$,

$$\langle v|PG_AP - \lambda QG_BQ|v\rangle = -\lambda\langle v|QG_BQ|v\rangle < 0,$$

which implies $D_{\max}(QG_BQ\|PG_AP) = +\infty$. ∎

According to this lemma, if states configurations or their probabilities are not compatible with the linearity of quantum mechanics, this transformation is not possible, even in a probabilistic way. The generalization of this result for any number

$N > K$ of states is trivial, as it is sufficient to apply this lemma to any $K+1$ states, K of which are linearly independent.

Hence, if max-relative entropy is above zero, and the desired transformation is possible, one can consider only the linearly independent set of K input states $\{p_i, |\varphi_i\rangle\}_{i=1}^K$, and the set $\{q_i, |\psi_i\rangle\}_{i=1}^K$ of (not necessarily linearly independent) corresponding output states to define the transformation $\bar{M}_s$ similarly as above:

$$\bar{M}_s = 2^{-D_{\max}(QG_BQ\|PG_AP)}\bar{B}\bar{Q}\bar{P}^{-1}\bar{A}^{-1},$$

where

$$\bar{A} = \sum_{i=1}^{K} |\varphi_i\rangle\langle e_i|, \quad \bar{B} = \sum_{i=1}^{K} |\psi_i\rangle\langle e_i|,$$

$$\bar{P} = \sum_{i=1}^{K} \sqrt{p_i}|e_i\rangle\langle e_i|, \quad \bar{Q} = \sum_{i=1}^{K} \sqrt{q_i}|e_i\rangle\langle e_i|.$$

The equality

$$D_{\max}(QG_BQ\|PG_AP) = D_{\max}(\bar{Q}\bar{B}^\dagger\bar{B}\bar{Q}\|\bar{P}\bar{A}^\dagger\bar{A}\bar{P}),$$

which, as above, is needed for the condition $I - \bar{M}_s^\dagger\bar{M}_s \geqslant 0$, follows from the fact that these matrices are connected with the same linear operation L:

$$PG_AP - \lambda QG_BQ = L(\bar{P}\bar{A}^\dagger\bar{A}\bar{P} - \lambda\bar{Q}\bar{B}^\dagger\bar{B}\bar{Q})L^\dagger.$$

Hence, $\bar{M}_s$ performs the transformation (4) for the first K linearly independent states and, by linearity, it does the same for other $N-K$ states, thus total success probability is still $2^{-D_{\max}(QG_BQ\|PG_AP)}$, which completes the proof of the theorem. ■

Note that this theorem is far beyond the result that average state $\rho_A = \sum_{i=1}^N p_i|\varphi_i\rangle\langle\varphi_i|$ can be mapped onto $\rho_B = \sum_{i=1}^N q_i|\psi_i\rangle\langle\psi_i|$. Such result may be obtain deterministically just by considering the channel which transforms all the initial states into ρ_B [13].

This theorem may be formulated in an alternative way, by using conditional probabilities $\{p(\text{succ}|i)\}_{i=1}^N$. Consider the matrices $C = \sum_i \sqrt{p(\text{succ}|i)}|e_i\rangle\langle e_i|$, and $S = C^2 = \text{diag}\{p(\text{succ}|i)\}_{i=1}^N$.

Corollary 1. One can map the set $\{|\varphi_i\rangle\}_{i=1}^N$ to the set $\{|\psi_i\rangle\}_{i=1}^N$ with conditional success probabilities $\{p(\text{succ}|i)\}_{i=1}^N$ if

$$D_{\max}(CG_BC\|G_A) = 0. \tag{8}$$

This corollary is also closely connected with Theorem 3 in Ref. [2] and describes the particular case of this result in terms of max-relative entropy, see also Lemma 1 in Ref. [14].

An important particular case of such map is unambiguous state discrimination. For USD operation, the input ensemble is linearly independent, and the output ensemble is orthogonal, thus the output Gram matrix is identity.

Corollary 2. For the set $\{|\varphi_i\rangle\}_{i=1}^N$, unambiguous discrimination with conditional success probabilities $\{p(\text{succ}|i)\}_{i=1}^N$ is possible if

$$D_{\max}(S\|G_A) = 0. \tag{9}$$

This expression does not involve *a priori* state probabilities p_i, but if the optimization task is to maximize average success probability p_{succ} [15–18], they are also taken into account. Here, this optimization task is formulated in terms of finding the optimal set $\{p(\text{succ}|i)\}_{i=1}^N$ subject to the restriction (9) [19].

Note that, with additional requirement that success probabilities must coincide for all the input states, this corollary gets the known result that USD success probability equals minimal eigenvalue of the Gram matrix [19,20].

IV. UPPER BOUND

The lower bound for success probability (7) is not necessarily tight, i.e., sometimes a required transformation may be performed with higher success probability. Let us consider a simple example of two nonorthogonal equiprobable states $\{|\varphi_0\rangle, |\varphi_1\rangle\}$ on the input (let $\langle\varphi_0|\varphi_1\rangle = \varepsilon$ be real), and two coinciding equiprobable states $\{|\psi\rangle, |\psi\rangle\}$ on the output. The Gram matrices are

$$G_A = \begin{pmatrix} 1 & \varepsilon \\ \varepsilon & 1 \end{pmatrix}, \quad G_B = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \tag{10}$$

and one can easily find that

$$D_{\max}(QG_BQ\|PG_AP) = -\log_2(1-\varepsilon),$$

hence $p_{\text{succ}} = 1-\varepsilon$. But obviously such a transformation may be done in a deterministic way, as it is just a SWAP gate for the system and ancilla in initial state $|\psi\rangle$, with the Stinespring representation

$$\Phi[\rho] = \text{Tr}_E(\text{SWAP}_{AE}[\rho_A \otimes |\psi\rangle\langle\psi|_E]\text{SWAP}_{AE}).$$

Here, the environment comes into play. The total transformation with taking the environment into account reads

$$|\varphi_0\rangle|\psi\rangle \to |\psi\rangle|\varphi_0\rangle, \quad |\varphi_1\rangle|\psi\rangle \to |\psi\rangle|\varphi_1\rangle,$$

and for these states, the output Gram matrix is the same as the input one, thus success probability is 1. Then partial trace over the environment is performed, which in terms of the instrument elements can be described as

$$\text{Tr}_E(\rho) = \sum_{i,j,k} \langle e_i|_A\langle f_k|_E\rho|e_j\rangle_A|f_k\rangle_E|e_i\rangle\langle e_j|_A$$
$$= \sum_k V_k\rho V_k^\dagger,$$

where $V_k = \sum_i |e_i\rangle_A\langle e_i|_A\langle f_k|_E$, with $\{|e_i\rangle_A\}_i$ and $\{|f_i\rangle_E\}_i$ being orthonormal bases for $\mathcal{H}_A$ and $\mathcal{H}_E$, respectively. Note that here, unlike the situation of Theorem 1, we need more than one element of instrument for the succ outcome.

Hence, the generalization of (7) should take the environment into account (see also Refs. [2,14]). In this work, we consider only pure output states, thus the states in $\mathcal{H}_B \otimes \mathcal{H}_E$ have product form $|\varphi_i\rangle_B|\varepsilon_i\rangle_E$. For such states, inner product has product form, thus we have for the Gram matrix

$$G_{BE} = \{\langle\varphi_i|\varphi_j\rangle\langle\varepsilon_i|\varepsilon_j\rangle\}_{ij} = G_B \circ G_E, \tag{11}$$

where $G_B \circ G_E$ is the element-wise (Hadamard) product of G_B and G_E.

With the best possible non-negative Gram matrix G_E, the lower bound (7) now takes the form

$$p_{\text{succ}} = \max_{G_E \geqslant 0} 2^{-D_{\max}(QG_B \circ G_E Q \| PG_A P)}. \tag{12}$$

Let us now show that it is also an upper bound.

Theorem 2. For any instrument (1) performing the operation $\mathcal{E}_A \xrightarrow{\text{succ}} \mathcal{E}_B$, the success probability is upper-bounded by (12).

Proof. Let us first obtain the Gram matrix G_E for the environment by using methods similar to [21]. For the instrument elements $\{V_{\text{succ},k}\}_k$ corresponding to success, let us define

$$V'_{\text{succ},k} = V_{\text{succ},k} \otimes |f_k\rangle, \tag{13}$$

where $|f_k\rangle$ is orthonormal basis in auxiliary space $\mathcal{H}_E$. Next, let us consider a channel with success operator

$$M_s = \sum_k V'_{\text{succ},k} : \ \mathcal{H}_A \to \mathcal{H}_B \otimes \mathcal{H}_E. \tag{14}$$

Since

$$\text{Tr}_E[M_s \rho M_s^\dagger] = \sum_k V_{\text{succ},k} \rho V_{\text{succ},k}^\dagger \tag{15}$$

for any ρ, it implies that

$$M_s \sqrt{p_i} |\varphi_i\rangle = \sqrt{p_{\text{succ}}} \sqrt{q_i} |\psi_i\rangle_B \otimes |\varepsilon_i\rangle_E \tag{16}$$

for a set $\{|\varepsilon_i\rangle\}_{i=1}^N$. Here, the condition $\mathcal{E}_A \xrightarrow{\text{succ}} \mathcal{E}_B$ implies that output states for any input $|\varphi_i\rangle$ have product form, while the output for their linear combination $\sum_k c_k |\varphi_k\rangle$ may be entangled. Thus, M_s performs the required transformation with the output in $\mathcal{H}_B$, and it also yields additional states $\{|\varepsilon_i\rangle\}_{i=1}^N$ in $\mathcal{H}_E$, for which the Gram matrix G_E is now defined.

Let us now assume that p_{succ} for the transformation is above the bound (12). It follows that there exists $|v\rangle = \sum_i c_i |e_i\rangle$, such that

$$\langle v | (PG_A P - p_{\text{succ}} QG_B \circ G_E Q) | v \rangle < 0,$$

hence for $E = \sum_i |\psi_i\rangle_B |\varepsilon_i\rangle_E \langle e_i|$, and for the vectors

$$|w\rangle = AP|v\rangle = \sum_i c_i \sqrt{p_i} |\varphi_i\rangle_A,$$

$$|w'\rangle = EQ|v\rangle = \sum_i c_i \sqrt{q_i} |\psi_i\rangle_B |\varepsilon_i\rangle_E,$$

we have, according to (16),

$$M_s |w\rangle\langle w| M_s^\dagger = p_{\text{succ}} |w'\rangle\langle w'|,$$

while

$$\langle w | w \rangle < p_{\text{succ}} \langle w' | w' \rangle,$$

thus M_s increases trace, and it cannot be a part of a CPTP-map, as well as $\{V_{\text{succ},k}\}_k$. This contradiction shows that the assumption about p_{succ} above the bound (12) was incorrect, which completes the proof. ∎

V. PARTIAL TRANSFORMATION

In the two previous sections, we used a single success operator M_s to perform the required transformation $\mathcal{E}_A \xrightarrow{p_{\text{succ}}} \mathcal{E}_B$ with success probability p_{succ}. This framework allows for a partial transformation [22], which does not do the whole work, but may provide outcome with arbitrary high success probability p_{first}:

$$\mathcal{E}_A \xrightarrow{p_{\text{first}}} \mathcal{E}_C \xrightarrow{p_{\text{second}}} \mathcal{E}_B.$$

This operation result in other ensemble $\mathcal{E}_C$, and then one can "complete" this operation with the map $\mathcal{E}_C \xrightarrow{p_{\text{second}}} \mathcal{E}_B$, which has success probability p_{second}, and the total success probability remains the same as for the original operation:

$$p_{\text{succ}} = p_{\text{first}} p_{\text{second}}. \tag{17}$$

To show that, let us observe that success probability is given by the minimal eigenvalue of $M_s^\dagger M_s$:

$$p_{\text{succ}} = \lambda_{\min}(M_s^\dagger M_s), \tag{18}$$

hence, for any $t \in [0, 1]$ success probability for the transformation given by the operator M_s^t, equals $[\lambda_{\min}(M_s^\dagger M_s)]^t$, and one can easily find the appropriate t for a given success probability p_{first}. Thus, the generalization corresponds to the decomposition $M_s = M_s^{1-t} M_s^t$.

Let us note that the proposed method is not the only one to generalize this transformation for arbitrary success probability. As an example, let us consider the set of N equiprobable symmetric coherent states [23,24], and the transformation which amplifies their intensity, i.e., $p_k = q_k = \frac{1}{N}$, $k = 1, \ldots, N$, and

$$|\varphi_k\rangle = \left|\sqrt{\mu_A} e^{i\frac{2(k-1)}{N}\pi}\right\rangle, \quad |\psi_k\rangle = \left|\sqrt{\mu_B} e^{i\frac{2(k-1)}{N}\pi}\right\rangle. \tag{19}$$

Here, $\mu_B > \mu_A$, and the coherent states are given by $|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{+\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle$, where $\{|n\rangle\}_{n=0}^{+\infty}$ is the Fock basis.

The framework presented above leads to $M_s = BA^{-1}$, with A and B defined in a similar way, thus the generalization is given by M_s^t for parameter value $t \in [0, 1]$.

Nevertheless, other generalization is also possible, when the intermediate output states are also symmetric coherent states with the intensity $\mu_C \in [\mu_A, \mu_B]$. For this case, the success operator is given by

$$M'_s = CA^{-1}, \quad C = \sum_k \left|\sqrt{\mu_C} e^{i\frac{2(k-1)}{N}\pi}\right\rangle\langle e_k|. \tag{20}$$

Both generalizations of this example may be used for eavesdropping in quantum cryptography based on symmetric coherent states [25,26]. For this states configuration, the eavesdropper is restricted by the required success probability, which comes from the distance between the legitimate users.

Finding the best generalization which performs the part of the required transformation while maximizing the given function (e.g., the Holevo quantity [27] of the ensemble) for any partial success probability is a separate task.

VI. CONCLUSION

In this paper, we considered quantum operations with nonunit success probability, which may be also regarded as

postselective quantum operations. They play crucial role in quantum cryptography, as postselection with the use of classical authenticated channel is a source of advantage for the legitimate users, but it also provides new attacks to the eavesdropper based on USD [28] and PNS [29] scenarios, which utilize the channel attenuation.

We proposed a closed-form expression for success probability of the map between two arbitrary ensembles of pure quantum states, including linearly dependent ones. This expression involves Gram matrices, which have already been used to describe the distinguishability for the set of quantum states [19,20,30]. It also involves the input and output probabilities, and quantum max-relative entropy, which was shown to play important role in postselective quantum operations: e.g., USD criteria for an arbitrary ensemble can also be expressed in terms of max-relative entropy, as well as the advantage which can be gained by maximum confidence measurements [31], thus this works adds one more interpretation for this function.

We have also shown that the proposed framework provides a simple, but not unique, method for the generalization: one can perform a partial transformation with arbitrary high success probability. This generalization has similarities with the states separation method which makes the two states more distinguishable with a given success probability [32,33].

It is a challenging task to generalize the presented approach to the case of mixed quantum states, see, e.g., Ref. [14].

ACKNOWLEDGMENTS

This work was performed at the Steklov International Mathematical Center and supported by the Ministry of Science and Higher Education of the Russian Federation (Agreement No. 075-15-2022-265).

[1] A. Chefles, Quantum operations, state transformations and probabilities, Phys. Rev. A **65**, 052314 (2002).
[2] A. Chefles, R. Jozsa, and A. Winter, On the existence of physical transformations between sets of quantum states, Int. J. Quantum Inform. **02**, 11 (2004).
[3] T. Heinosaari, M. A. Jivulescu, D. Reeb, and M. M. Wolf, Extending quantum operations, J. Math. Phys. **53**, 102208 (2012).
[4] E. Chitambar and G. Gour, Quantum resource theories, Rev. Mod. Phys. **91**, 025001 (2019).
[5] G. Gour, Comparison of quantum channels by superchannels, IEEE Trans. Inf. Theory **65**, 5880 (2019).
[6] B. Regula, Tight constraints on probabilistic convertibility of quantum states, Quantum **6**, 817 (2022).
[7] B. Regula, Probabilistic Transformations of Quantum Resources, Phys. Rev. Lett. **128**, 110505 (2022).
[8] I. Ivanovic, How to differentiate between non-orthogonal states, Phys. Lett. A **123**, 257 (1987).
[9] D. Dieks, Overlap and distinguishability of quantum states, Phys. Lett. A **126**, 303 (1988).
[10] A. Peres, How to differentiate between non-orthogonal states, Phys. Lett. A **128**, 19 (1988).
[11] E. B. Davies and J. T. Lewis, An operational approach to quantum probability, Commun. Math. Phys. **17**, 239 (1970).
[12] N. Datta, Min-and max-relative entropies and a new entanglement monotone, IEEE Trans. Inf. Theory **55**, 2816 (2009).
[13] R. Wu, A. Pechen, C. Brif, and H. Rabitz, Controllability of open quantum systems with Kraus-map dynamics, J. Phys. A: Math. Theor. **40**, 5681 (2007).
[14] X.-F. Zhou, Q. Lin, Y.-S. Zhang, and G.-C. Guo, Physical accessible transformations on a finite number of quantum states, Phys. Rev. A **75**, 012321 (2007).
[15] G. Jaeger and A. Shimony, Optimal distinction between two non-orthogonal quantum states, Phys. Lett. A **197**, 83 (1995).
[16] J. A. Bergou, U. Futschik, and E. Feldman, Optimal Unambiguous Discrimination of Pure Quantum States, Phys. Rev. Lett. **108**, 250502 (2012).
[17] M. Jafarizadeh, M. Rezaei, N. Karimi, and A. Amiri, Optimal unambiguous discrimination of quantum states, Phys. Rev. A **77**, 042314 (2008).
[18] A. Peres and D. R. Terno, Optimal distinction between non-orthogonal quantum states, J. Phys. A: Math. Gen. **31**, 7105 (1998).
[19] G. Sentís, J. Calsamiglia, and R. Munoz-Tapia, Exact Identification of a Quantum Change Point, Phys. Rev. Lett. **119**, 140506 (2017).
[20] D. Horoshko, M. Eskandari, and S. Y. Kilin, Equiprobable unambiguous discrimination of quantum states by symmetric orthogonalisation, Phys. Lett. A **383**, 1728 (2019).
[21] D. Kronberg, Modification of quantum measurements by mapping onto quantum states and classical outcomes, Lobachevskii J. Math. **43**, 1663 (2022).
[22] D. Kronberg, Increasing the distinguishability of quantum states with an arbitrary success probability, Proc. Steklov Inst. Math. **313**, 113 (2021).
[23] A. Chefles and S. M. Barnett, Optimum unambiguous discrimination between linearly independent symmetric states, Phys. Lett. A **250**, 223 (1998).
[24] V. Dunjko and E. Andersson, Truly noiseless probabilistic amplification, Phys. Rev. A **86**, 042322 (2012).
[25] D. Kronberg, Generalized discrimination between symmetric coherent states for eavesdropping in quantum cryptography, Lobachevskii J. Math. **41**, 2332 (2020).
[26] D. A. Kronberg, Vulnerabilities of quantum cryptography on geometrically uniform coherent states, Quantum Electron. **51**, 928 (2021).
[27] A. S. Holevo, Bounds for the Quantity of Information Transmitted by a Quantum Communication Channel, Probl. Peredachi Inf. **93**, 3 (1973).
[28] M. Dušek, M. Jahma, and N. Lütkenhaus, Unambiguous state discrimination in quantum cryptography with weak coherent states, Phys. Rev. A **62**, 022306 (2000).

[29] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Limitations on Practical Quantum Cryptography, Phys. Rev. Lett. **85**, 1330 (2000).

[30] G. Sentís, E. Bagan, J. Calsamiglia, G. Chiribella, and R. Munoz-Tapia, Quantum Change Point, Phys. Rev. Lett. **117**, 150502 (2016).

[31] N. R. Kenbaev and D. A. Kronberg, Quantum postselective measurements: Sufficient condition for overcoming the Holevo bound and the role of max-relative entropy, Phys. Rev. A **105**, 012609 (2022).

[32] A. Chefles and S. M. Barnett, Quantum state separation, unambiguous discrimination and exact cloning, J. Phys. A: Math. Gen. **31**, 10097 (1998).

[33] E. Bagan, V. Yerokhin, A. Shehu, E. Feldman, and J. A. Bergou, A geometric approach to quantum state separation, New J. Phys. **17**, 123015 (2015).