Minimum-error discrimination of qubit states: Methods, solutions, and properties

Joonwoo Bae[1,2,*] and Won-Young Hwang[3]

[1] *Center for Quantum Technologies, National University of Singapore, 3 Science Drive 2, 117542 Singapore*

[2] *ICFO–Institut de Ciéncies Fotóniques, Mediterranean Technology Park, 08860 Castelldefels (Barcelona), Spain*

[3] *Department of Physics Education, Chonnam National University, Gwangju 500-757, Korea*

(Received 14 June 2012; revised manuscript received 24 October 2012; published 30 January 2013)

We show a geometric formulation for minimum-error discrimination of qubit states that can be applied to arbitrary sets of qubit states given with arbitrary *a priori* probabilities. In particular, when qubit states are given with equal *a priori* probabilities, we provide a systematic way of finding optimal discrimination and the complete solution in a closed form. This generally gives a bound to cases when prior probabilities are unequal. Then it is shown that the guessing probability does not depend on detailed relations among the given states, such as the angles between them, but on a property that can be assigned by the set of given states itself. This also shows how a set of quantum states can be modified such that the guessing probability remains the same. Optimal measurements are also characterized accordingly, and a general method of finding them is provided.

DOI: 10.1103/PhysRevA.87.012334 PACS number(s): 03.67.Hk, 03.65.Ud, 03.65.Wj, 03.67.Mn

Discrimination of quantum states is a fundamental process to extract information encrypted in collected quantum states. In practical applications, its framework characterizes the communication capabilities of encoding and decoding messages via quantum states [1,2]. The process of distinguishing quantum states is generally a building block when quantum systems are applied to information processing, in particular for communication tasks [1]. Its usefulness as a theoretical tool to investigate quantum information theory has also been shown, with recent progress in secure communication, randomness extraction in classical-quantum correlations [3], and semi-device-independent quantum information tasks [4].

There has been much effort devoted to discrimination of various sets of quantum states so far (see reviews in Ref. [5] for theoretical and experimental developments); however, apart from the general method of two-state discrimination shown in 1976 [1] or restricted cases where some specific symmetry exists in given quantum states, e.g., Ref. [6], little is known in general about optimal discrimination of quantum states; see also the review in Ref. [7] of progress in this area. For instance, *the next simplest example that comes after the two-state discrimination is an arbitrary set of three-qubit states, for which no analytical solution is known yet*. When arbitrary quantum states are given, the general method for optimal discrimination has been a numerical procedure (e.g., Ref. [8]) which only numerically approximates the exact solution. Apart from its importance in its own right, the lack of a general method for state discrimination even in simple instances is, due to its fundamental importance, potentially a significant obstacle preventing further investigations in both quantum information theory and quantum foundations.

In the present work, we provide progress in the long-standing problem of minimum-error state discrimination, in particular, for arbitrarily given sets of qubit states. This could lead to significant improvement in understanding related problems in quantum information theory; see those in the review in Ref. [5] or the recent applications of state discrimination as in Ref. [4]. We show a geometric formulation of the optimal discrimination of qubit states by analysis of optimality conditions. This approach is called *the complementarity problem* in the context of semidefinite programming. We provide the guessing probability, i.e., the maximal probability of making correct guesses, in a closed form for cases where arbitrary qubit states, among which no symmetry may exist, are given with equal *a priori* probabilities. The geometric formulation also applies to other cases of unequal *a priori* probabilities, and we characterize optimal measurements accordingly. From these results, it is shown that the guessing probability does not depend on detailed relations among the given states in general but on a property assigned by the set of given states. This also shows how a set of states can be modified such that the modification cannot be recognized in the discrimination task in terms of the guessing probability.

For the purpose, let us briefly summarize the minimum-error discrimination in the context of a communication scenario of two parties Alice and Bob. They have agreed on N alphabets $\{x\}_{x=1}^N$ and states $\{\rho_x\}_{x=1}^N$, as well as *a priori* probabilities $\{q_x\}_{x=1}^N$. Alice's encoding works by mapping alphabet x to state ρ_x, and relating states with *a priori* probabilities $\{q_x\}_{x=1}^N$. This can be seen as Alice's pressing button x with probability q_x, and then Bob's guessing among states $\{\rho_x\}_{x=1}^N$ given with *a priori* probabilities $\{q_x\}_{x=1}^N$, which we write as $\{q_x,\rho_x\}_{x=1}^N$.

Bob's discrimination of quantum states is described by positive-operator-valued-measure (POVM) elements $\{M_x \geqslant 0\}_{x=1}^N$ satisfying $\sum_x M_x = I$ (completeness). Let $P_{B|A}(x|y)$ denote the probability that Bob has a detection event on M_x that leads to the conclusion that ρ_x is given, while a state ρ_y is provided by Alice's sending message y. This is computed as follows: $P_{B|A}(x|y) := P(x|y) = \mathrm{tr}[M_x\rho_y]$. The figure of merit is the maximal probability that Bob makes a correct guess on average, and is called *the guessing probability*,

$$P_{\mathrm{guess}} = \max_{\{M_x\}_{x=1}^N} \sum_x q_x \mathrm{tr}[M_x\rho_x], \quad \sum_x M_x = I, \qquad (1)$$

where the maximization runs over all POVM elements. This naturally introduces the discrimination as an optimization task.

*bae.joonwoo@gmail.com

In fact, the above can be put into the framework of semidefinite programming [8]. A useful property of this approach is that a given maximization (minimization) problem can be alternatively described by its dual, a minimization (maximization) problem. The dual problem to the maximization in Eq. (1) is obtained as follows:

$$P_{\text{guess}} = \min_{K} \text{tr}[K], \quad K \geqslant q_x \rho_x, \ \forall\, x = 1, \ldots, N. \quad (2)$$

In this case, the minimization works to find a single parameter K which then gives the guessing probability, as in the approach in Ref. [9].

For convenience, we call the problem in Eq. (1) the primal, with respect to the dual in Eq. (2). Note that solutions of the two problems do not generally coincide with each other. The fact that, in this case, the guessing probability can be obtained from both primal and dual optimizations follows from the property called strong duality. This holds when both primal and dual problems have a nonempty set of parameters satisfying given constraints; these are referred to as feasible problems. Once both problems are feasible, strong duality holds, and then it follows that the solutions of both problems coincide with each other.

Apart from solving those optimization problems, there is another approach called *a complementarity problem*. This collects optimality conditions that parameters of both primal and dual problems should satisfy, in order to give optimal solutions. Then, any set of parameters satisfying optimality conditions immediately provides optimal solutions of primal and dual problems. As more parameters are taken into account, the approach is not considered to be easier; however, the advantage lies in its usefulness for finding general structures in a given problem.

In the semidefinite programming formulation, the optimality conditions can be summarized by the so-called Karus-Khun-Tucker (KKT) conditions. For quantum-state discrimination, they are given, together with the two constraints in Eqs. (1) and (2), by

$$K = q_x \rho_x + r_x \sigma_x \quad (3)$$

and

$$r_x \text{tr}[\sigma_x M_x] = 0, \ \forall\ x = 1, \ldots, N \quad (4)$$

for a set of *complementary states* $\{\sigma_x\}_{x=1}^N$ with non-negative coefficients $\{r_x \geqslant 0\}_{x=1}^N$ and POVM elements $\{M_x\}_{x=1}^N$. Once states $\{r_x,\sigma_x\}_{x=1}^N$ and measurements $\{M_x\}_{x=1}^N$ satisfying these conditions are found, they are automatically optimal to give solutions in both primal and dual problems. From the fact that strong duality holds in this case, it is clear that the guessing probability is obtained from either of the problems. Note that the first condition in Eq. (3) is called the Lagrangian stability, and shows that there exists a single operator K that can be decomposed in N different ways. The second one in Eq. (4) is the complementary slackness which shows the orthogonality relation between primal and dual parameters.

The particular usefulness of the KKT conditions here is that, as shown above, they separate the guessing probability [i.e., $\text{tr}[K]$ in Eq. (2)] from the optimal measurements: a single operator K alone characterizes the guessing probability, and the optimal measurements themselves are independently expressed in Eq. (4). The operator K can be explained as having N decompositions with $q_x\rho_x$ and $r_x\sigma_x$ for $x = 1, \ldots, N$. Optimal measurements are described as POVM elements orthogonal to states $\{\sigma_x\}_{x=1}^N$ for each x. The discrimination problem is then equivalent to finding states $\{\sigma_x\}_{x=1}^N$ that fulfill these conditions.

We now show a geometric formulation to find the complementary states. Let us first define the polytope of the given states $\{q_x,\rho_x\}_{x=1}^N$, denoted as $\mathcal{P}(\{q_x,\rho_x\}_{x=1}^N)$, in the underlying state space, in which each vertex corresponds to $q_x\rho_x$. It is useful to rewrite the condition in Eq. (3) as

$$q_x\rho_x - q_y\rho_y = r_y\sigma_y - r_x\sigma_x, \quad \forall\ x,y. \quad (5)$$

This shows that the two polytopes $\mathcal{P}(\{q_x,\rho_x\}_{x=1}^N)$ of the given states and $\mathcal{P}(\{r_x,\sigma_x\}_{x=1}^N)$ of the complementary states, which we are searching for, are actually congruent. Thus, the structure of the complementary states is already determined from the given states $\{q_x,\rho_x\}_{x=1}^N$. Once the state geometry is clear (see, e.g., [10]), the formulation can be applied.

For qubit states, their geometry can generally be described on the Bloch sphere in which the distance measure is given by the Hilbert-Schmidt norm. In what follows, we restrict our consideration to qubit states and apply the geometric formulation to discrimination among them. For a qubit state ρ_x, we write the Bloch vector as $\vec{v}(\rho_x)$, with which $\rho_x = [I + \vec{v}(\rho_x)\cdot\vec{\sigma}]/2$, where $\vec{\sigma} = (X,Y,Z)$ are the Pauli matrices X, Y, and Z.

We first characterize the general form of optimal measurements for qubit-state discrimination, from the KKT condition in Eq. (4). Suppose that $r_x > 0$; otherwise, the measurement can be arbitrarily chosen. To fulfill the condition, it is not difficult to see that optimal POVM elements are either of rank 1 [11] or the null operator. If $\sigma_x = |\psi_x\rangle\langle\psi_x|$ then $M_x = m_x|\psi_x^{\perp}\rangle\langle\psi_x^{\perp}|$ with coefficients m_x, where it holds that $\vec{v}(\psi_x) = -\vec{v}(\psi_x^{\perp})$. If a state σ_x is not of rank 1, the only possibility to fulfill the KKT condition in Eq. (4) is that the measurement corresponds to the null operator, i.e., $M_x = 0$. In fact, optimal discrimination sometimes consists of a strategy that makes a guess without actual measurement [12]. Note, however, that, as measurements are done in most cases (otherwise, the completeness of POVM elements in the following is not fulfilled), one does not have to immediately assume that $\{\sigma_x\}_{x=1}^N$ are not of rank 1 from the beginning. Then, for cases where measurements are done, corresponding complementary states must be of rank 1—otherwise, the orthogonality in Eq. (4) cannot be fulfilled.

Once states $\{\sigma_x\}_{x=1}^N$ are found, optimal measurements are automatically obtained. What remains is that the POVM elements fulfill the completeness condition $\sum_x M_x = I$, or equivalently in terms of Bloch vectors $\sum_x m_x v(\psi_x^{\perp}) = 0$, while $\sum_x m_x = 2$ with $m_x \geqslant 0$, $\forall\ x$. This refers to finding a convex combination $\{m_x\}_{x=1}^N$ of Bloch vectors $\{\vec{v}(\psi_x^{\perp})\}_{x=1}^N$ such that their result is zero, i.e., the origin of the Bloch sphere. This is equivalent to the condition that the convex hull of Bloch vectors $\{\vec{v}(\psi_x)\}_{x=1}^N$ of complementary states contain the origin of the Bloch sphere. As we will show later, this is always fulfilled by complementary states. To summarize, once complementary states are found, the optimal POVMs follow automatically as their Bloch vectors are determined and completeness is also straightforward.

We can thus proceed to construction of complementary states in the Bloch sphere for qubit states $\{q_x,\rho_x\}_{x=1}^N$. Let us identify the polytope $\mathcal{P}(\{q_x,\rho_x\}_{x=1}^N)$ in the state space as the convex hull of their Bloch vectors $\{q_x,\vec{v}(\rho_x)\}_{x=1}^N$, so that each vertex $q_x\rho_x$ corresponds to the Bloch vector $q_x\vec{v}(\rho_x)$. Then, the task is to find the polytope $\mathcal{P}(\{r_x,\sigma_x\}_{x=1}^N)$ of complementary states that is congruent to $\mathcal{P}(\{q_x,\rho_x\}_{x=1}^N)$ in the Bloch sphere. Moreover, as we show, most of the complementary states $\{\sigma_x\}_{x=1}^N$ are of rank 1 and themselves lie at the border; thus, only their polytope $\mathcal{P}(\{\sigma_x\}_{x=1}^N)$ is maximal in the Bloch sphere. Using these properties of complementary states, a geometric approach can generally be employed.

All these results already give the guessing probability in a simple way for cases when the qubit states are given with equal *a priori* probabilities, that is, when $q_x = 1/N$ for all x. In this case, it is not difficult to see the general form of the guessing probability. Substituting $q_x = 1/N$ in the KKT condition in Eq. (3), the result is that the parameters $\{r_x\}_{x=1}^N$ are equal. We put $r := r_x$ for all x. This holds true for an arbitrary set of quantum states in general. Then the guessing probability is written as

$$P_{\text{guess}} = \text{tr}[K] = \frac{1}{N} + r \quad \text{with} \quad r = \frac{\left\| \frac{1}{N}\rho_x - \frac{1}{N}\rho_y \right\|}{\|\sigma_x - \sigma_y\|}, \tag{6}$$

where the equation for the parameter r is from the relation in Eq. (5), and the distance measure can be taken as the Hilbert-Schmidt norm D_{HS} (as is natural on the Bloch sphere) or the trace norm D_T. Both measures give the same value of r since they are related only by a constant: $D_{\text{HS}} = \sqrt{2}D_T$ for qubit states. This means that the parameter r can be obtained by either of the distance measures when referring to the geometry on the Bloch sphere, since the parameter is only a ratio; see Eq. (6).

The parameter r corresponds to the ratio between the two polytopes $\mathcal{P}(\{1/N,\rho_x\}_{x=1}^N)$ of the given states and $\mathcal{P}(\{\sigma_x\}_{x=1}^N)$ of the complementary states, as shown in Eq. (6). We recall that most of $\{\sigma\}_{x=1}^N$ are pure (i.e., of rank 1), lying at the border of the Bloch sphere. This implies that the polytope $\mathcal{P}(\{\sigma_x\}_{x=1}^N)$ of complementary states is clearly maximal in the Bloch sphere. In this way, the polytope $\mathcal{P}(\{\sigma_x\}_{x=1}^N)$ always contains the origin of the sphere, from which optimal measurements can be constructed. Note also that, from this, the completeness condition of the measurement is fulfilled; see Eq. (4). Finally, the two polytopes $\mathcal{P}(\{1/N,\rho_x\}_{x=1}^N)$ and $\mathcal{P}(\{\sigma_x\}_{x=1}^N)$ are, from the relation in Eq. (5), related by the ratio r, since the two polytopes $\mathcal{P}(\{1/N,\rho_x\}_{x=1}^N)$ and $\mathcal{P}(\{1/N,\sigma_x\}_{x=1}^N)$ are congruent.

We summarize the method of finding optimal discrimination in the following.

(1) Construct a polytope from given states as the convex hull of $\{1/N,\text{v}(\rho_x)\}_{x=1}^N$ in the Bloch sphere, where the vertices correspond to $\vec{v}(\rho_x)/N$.

(2) Expand the polytope such that it keeps being similar to the original one until it is maximal within the Bloch sphere (as most of $\{\sigma_x\}_{x=1}^N$ are pure), and then compute the ratio r of the resulting polytope with respect to the original one. The guessing probability is thus obtained, $P_{\text{guess}} = 1/N + r$.

(3) Rotate the maximal polytope within the Bloch sphere until it is found that corresponding lines are parallel to the original ones to fulfill Eq. (5). From this, the corresponding vertices are complementary states $\{\sigma_x\}_{x=1}^N$ and optimal POVM elements are explicitly constructed, according to Eq. (4).

This completely solves the problem of discrimination of qubit states given with equal *a priori* probabilities.

It has already been observed that the guessing probability does not depend on the detailed relations of the quantum states to be discriminated, but on a property from the whole set $\{\rho_x\}_{x=1}^N$, since the ratio r is the relevant parameter. If the given states are modified such that the polytope has the same ratio r, then the guessing probability remains the same. This means that, in the communication scenario we introduced earlier, Alice, who encodes messages can choose, or modify, sets of quantum states $\{\rho_x\}_{x=1}^N$ in such a way that Bob, who decodes from quantum states, cannot recognize her modification using optimal guessing. This actually defines equivalence classes of sets of quantum states in terms of optimal guessing [7].

In the following, we apply the method to various cases of qubit-state discrimination. The simplest example, and also the case when a general solution is known, is for $N = 2$, say ρ_1 and ρ_2. Following the instructions above, (i) the polytope constructed from the two given states corresponds to a line connecting two Bloch vectors of the states. The length can be computed using the trace distance as $\|\rho_1 - \rho_2\|/2$. Then, (ii) the maximal polytope similar to the original one is clearly the diameter of the Bloch sphere, which has length 2 in terms of the trace distance; hence, $r = \|\rho_1 - \rho_2\|/4$ (which equivalently can be obtained with the Hilbert-Schmidt distance). Substituting this in Eq. (6), the Helstrom bound in Ref. [1] is reproduced. Then, (iii) the diameter can be rotated until it is parallel to the original one. Thus, optimal measurements are also obtained.

Next, let us consider N states on the half plane. We can begin with N states $\{1/N,\rho_x\}_{x=1}^N$ that are equally distributed in the plane. They are characterized by Bloch vectors $\vec{v}(\rho_x) = f_x(\cos\theta_x, \sin\theta_x, 0)$ where $\theta_x = 2\pi x/N$. For these states, no general solution is known, except in cases of geometrically uniform states together with the condition that the $\{f_x\}_{x=1}^N$ are equal [6]. For convenience, we also suppose that N is an even number and assume that $f_{N/2} = f_N = \max_x f_x$. Then, applying the method introduced, one can easily find that the ratio depends on the maximal purity, that is, $r = f_N/N$, and the guessing probability is obtained as $P_{\text{guess}} = 1/N + f_N/N$, no matter what are purities of the other $N-2$ states; see also Fig. 1. This already reproduces the result in Ref. [6] for qubit states. The assumption of equal distribution over angles can be relaxed while keeping $\theta_N = \pi + \theta_{N/2}$ and $f_{N/2} = f_N = \max_x f_x$, for which the guessing probability then remains the same no matter how the other $N-2$ states are structured. This is because, as shown in Eq. (6), they are given with equal probabilities and the ratio r is unchanged.

Optimal measurements can be analyzed as follows, based on the geometric formulation; see also Fig. 1. For two states $\rho_{N/2}$ and ρ_N having the maximal purity, it is clear that a measurement is applied, and we let $\sigma_N = |\psi_N\rangle\langle\psi_N|$ and $\sigma_{N/2} = |\psi_{N/2}\rangle\langle\psi_{N/2}|$. From these expressions, obtaining optimal POVM elements is straightforward. For the other states, say $\{\rho_z\}$ having $f_z < f_N$, it holds from the KKT condition in Eq. (5) that $\vec{v}_N - \vec{v}_z$ is parallel to $r[\vec{v}(\sigma_N) - \vec{v}(\sigma_z)]$. This simply shows that their complementary states $\{\sigma_z\}$ cannot be

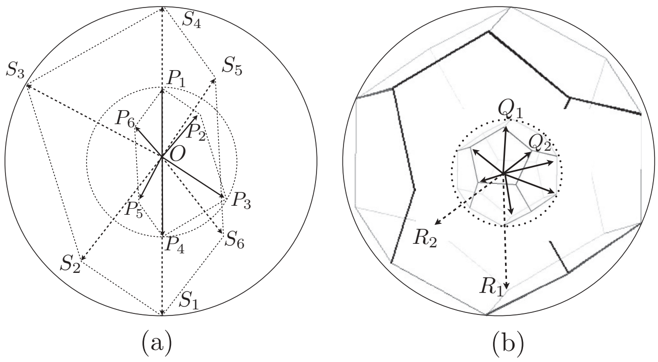

FIG. 1. (a) Six states $\{1/6,\rho_x\}_{x=1}^{6}$ in the half plane are given with purities $\{f_x\}_{x=1}^{6}$, i.e., $OP_x = f_x/6$, where three of them ($x = 1,3,4$) have the same purity and the others are less pure. See also that the relation in Eq. (5) is fulfilled. The ratio r in Eq. (6) can be obtained by expanding the given polytope until it is maximal in the plane. This is also the ratio between the radii of two circles covering the respective polygons. Thus, $P_{\text{guess}} = 1/6 + f_1/6$. The complementary state σ_x corresponds to OS_x. For $x = 2,5,6$, the states are not pure, and thus for these states, the optimal strategy is to make a guess without actual measurement [11]. (b) For $\{1/N,\rho_x\}_{x=1}^{N}$ pure states, each vertex of the polyhedron corresponds to the Bloch vector of state ρ_x/N. The ratio r is equal to Q_1Q_2/R_1R_2 [see also Eq. (5)], and thus $P_{\text{guess}} = 2/N$. Even if these states are modified, if the minimal sphere covering the polyhedron is unchanged, the guessing probability remains the same.

pure states, i.e., not of rank 1. Then, the corresponding POVM element is the null operator, that is, for these states the optimal strategy is to make a guess without actual measurement.

The method can be applied to a set of qubit states having a volume. For instance, let us look at the case when the given pure states are such that their Bloch vectors form a regular polyhedron of N vertices; see Fig. 1. Following the instructions above, the parameter r can be obtained as the ratio of two spheres, one the Bloch sphere and the other the minimal sphere covering the polyhedron of given states $\{1/N,\rho_x\}_{x=1}^{N}$. From this, we have $r = 1/N$, and the guessing probability is thus $P_{\text{guess}} = 2/N$. One can also modify the angles between those N states such that the minimal sphere covering the polyhedron remains the same, and then the guessing probability is unchanged.

The method of finding optimal state discrimination presented here can in principle be applied to high-dimensional states if their geometry is clear, or qubit states with unequal *a priori* probabilities. For the latter, although the geometry is clear, we do not have yet a general and systematic method to derive the guessing probability. Nevertheless, the geometric formulation can be applied and provides analytical solutions. The guessing probability under equal *a priori* probabilities, which is automatically computed via the geometric formulation, would then give an upper bound. Illuminating examples are presented in Ref. [7].

To conclude, we have shown a geometric formulation for qubit-state discrimination and provided the guessing probability in a closed form for equal *a priori* probabilities. This makes a significant contribution to the study of quantum-state discrimination. Optimal measurements are characterized accordingly. It is shown how qubit states can be modified while the guessing probability remains the same. As qubits are units of quantum information processing, we envisage that the method of discrimination and the results presented here will be useful to develop further investigations of qubit applications, e.g., Refs. [1,3,4], or approaches to related open questions, e.g., Ref. [13].

This work is supported by National Research Foundation and Ministry of Education, Singapore, and the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (Grant No. 2010-0007208).

[1] C. W. Helstrom, *Quantum Detection and Estimation Theory*, Mathematics in Science and Engineering Vol. 123 (Academic Press, New York, 1976).
[2] Y. C. Eldar and A. V. Oppenheim, Signal Process. Mag. **19**, 12 (2002).
[3] R. Koenig, R. Renner, and Ch. Schaffner, IEEE Trans. Inf. Theory **55**, 9 (2009).
[4] N. Brunner, M. Navascués, and T. Vértesi, arXiv:1209.5643.
[5] A. Chefles, Contemp. Phys. **41**, 401 (2000); J. A. Bergou, U. Herzog, and M. Hillery, in *Quantum State Estimation*, edited by M. Paris and J. Rehacek, Lecture Notes in Physics Vol. 649 (Springer, Berlin, 2004), pp. 417–465; J. A. Bergou, J. Phys: Conf. Ser. **84**, 012001 (2007); S. M. Barnett and S. Croke, Adv. Opt. Photon. **1**, 238 (2009); J. A. Bergou, J. Mod. Opt. **57**, 160 (2010).
[6] Y. C. Eldar and G. D. Forney, IEEE Trans. Inf. Theory **47**, 3 (2001).
[7] J. Bae, arXiv:1210.2845.
[8] S. Boyd and L. Vandenberghe, *Convex Optimization* (Cambridge University Press, Cambridge, 2004).
[9] M. E. Deconinck and B. M. Terhal, Phys. Rev. A **81**, 062304 (2010).
[10] I. Bengtsson and K. Zyczkowski, *Geometry of Quantum States* (Cambridge University Press, Cambridge, 2006).
[11] The only possibility of choosing a positive operator σ_x such that $\mathrm{tr}[\sigma_x M_x] = 0$ for a positive operator M_x of rank 2 is that $\sigma_x = 0$. This is taken into account in the case when $r_x = 0$ in the KKT conditions, and therefore excluded. Thus, POVM elements are either rank 1 or the null operator.
[12] K. Hunter, Phys. Rev. A **68**, 012306 (2003).
[13] http://qig.itp.uni-hannover.de/qiproblems, Problem 31.