Optimal single-shot discrimination of optical modes

Ignatius William Primaatmaja,[1] Asaph Ho,[1] and Valerio Scarani[1,2]
[1] *Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543, Singapore*
[2] *Department of Physics, National University of Singapore, 2 Science Drive 3, Singapore 117542, Singapore*

(Received 5 January 2021; accepted 22 April 2021; published 10 May 2021)

Retrieving classical information encoded in optical modes is at the heart of many quantum information processing tasks, especially in the field of quantum communication and sensing. Yet, despite its importance, the fundamental limits of optical mode discrimination have been studied only in a few specific examples. Here we present a toolbox to find the optimal discrimination of any set of optical modes. The toolbox uses linear and semidefinite programming techniques, which provide rigorous (not heuristic) bounds, and which can be efficiently solved on standard computers. We study both probabilistic and unambiguous single-shot discrimination in two scenarios: the channel-discrimination scenario, typical of metrology, in which the verifier holds the light source and can set up a reference frame for the phase; and the source-discrimination scenario, more frequent in cryptography, in which the verifier only sees states that are diagonal in the photon-number basis. Our techniques are illustrated with several examples. Among the results, we find that, for many sets of modes, the optimal state for mode discrimination is a superposition or mixture of at most two number states; but this is not general, and we also exhibit counterexamples.

DOI: 10.1103/PhysRevA.103.052410

I. INTRODUCTION

In quantum optical systems, information can be encoded in the quantum state, in the optical mode, or in both [1]. In this paper, we consider situations in which *classical information is encoded in optical modes* and address the problem of the ultimate limits in discriminating such modes (i.e., in retrieving the classical information). Consider a set of N modes associated to the annihilation operators $\{a_1, a_2, ..., a_N\}$ and characterized by their commutation relations:

$$[a_i, a_j^\dagger] = k_{ij}\mathbb{1} \ , \quad |k_{ij}| \leqslant 1. \tag{1}$$

Two modes are called orthogonal if $k_{ij} = \delta_{ij}$. The simplest example of nonorthogonal modes is $a_1 = a$, $a_2 = ka + \sqrt{1-|k|^2}b$ with $[a, b^\dagger] = 0$. This paper is devoted to *single-shot discrimination of modes* under an energy constraint that fixes the average number of photons $\bar{n}$. The constraint is motivated by the fact that any set of modes becomes perfectly distinguishable in the high intensity limit. Even for fixed $\bar{n}$, the probability of discrimination varies with the quantum state encoded in the modes [2]. This is the optimization that we need to tackle.

Mode discrimination takes different forms, depending on the experimental scenario that is considered. We shall consider two scenarios in this paper. In the *channel-discrimination scenario* [Fig. 1(a)], the mode is created by the unitary channel that maps a default mode a_0 onto one of the a_j. The source of light is in the hands of the verifiers, who can therefore avail themselves of a reference beam (idler) in addition to the beam that will be sent through the channel (signal). Then, the phase of the mode signal relative to the idler is defined; for instance, it becomes possible to discriminate $a_1 = a$ from $a_2 = -a$. If the reference is classical (i.e., an intense coherent state), as we shall assume here, the phase can be perfectly defined and the state in the channel can be taken to be pure; this choice is optimal for discrimination. The channel-discrimination scenario has a clearly *metrological* flavor: Besides the obvious case of phase discrimination [3,4], it can be seen as a special case of quantum reading [5–8], in which the devices to be discriminated are the unitary channels mentioned above. We refer to Ref. [9] for a review of such metrological schemes.

The situation is different in the *source-discrimination scenario*, in which the source of light is inside the same black box that performs the encoding of the mode [Fig. 1(b)]. From the point of view of the verifier, the phase of the signal mode is global and thus inaccessible. The state as seen from the verifier is the mixture over all possible values of the mode's phase: such a state is diagonal in the Fock basis [10].[1] The flavor of the source-discrimination scenario is more *cryptographic*. Information is encoded in the modes in all

[1] This statement should not be misread as contradicting the known facts that successive pulses in a laser may have relative coherence [11], and that such coherence may affect the unconditional security of cryptographic protocols, even if the encoding of classical information ignores those phases [12]. For one, here the modes to be discriminated may include relative phases between physical pulses (see, e.g., Sec. IV D). Once these modes are decided, we are studying *single-shot* discrimination, a task for which possible phases between successive instances of the modes indeed will not matter. In other words, we do not need to request the source to perform active phase randomization for the state to be Fock diagonal.

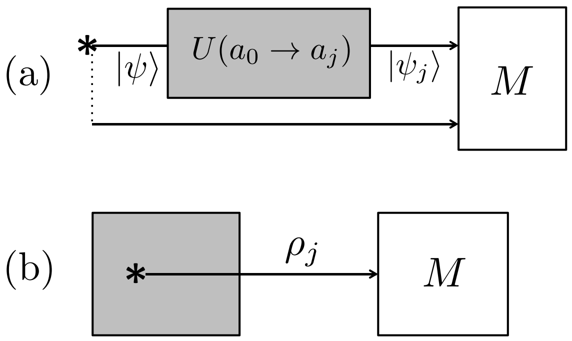

FIG. 1. The two scenarios considered in this paper for mode discrimination. (a) Channel-discrimination scenario, studied in Sec. II. The mode a_j to be discriminated is encoded by a unitary transformation from an input mode a_0. The verifier has control of the source (star) and can add a reference beam, with respect to which phase of the signal beam is well defined. If the reference is classical, the state in the signal beam can be taken as pure. (b) Source-discrimination scenario, studied in Sec. III. The source itself is in the black box, whence the signal exits encoded in the mode to be discriminated. For the verifier, the phase of the signal beam is global, and therefore the state appears as a photon-number mixture.

the discrete-variable (e.g., BB84 [13]) and distributed-phase-reference (e.g., differential phase shift (DPS) [14], coherent one-way (COW) [15]) protocols for quantum key distribution (QKD), and also in protocols other than QKD, for instance, quantum fingerprinting [16,17]. For all these protocols, Eve ultimately wants to learn the mode in which the signals were encoded. Furthermore, it is well-known that the security of these protocols also depends on the photon number distribution [18]. Of course, the analysis of a cryptographic protocol goes beyond single-shot mode discrimination [19–21]. This may be the reason why, to the best of our knowledge, the latter has not been previously studied in the source-discrimination scenario.

In this paper, we provide recipes to compute *upper bounds for single-shot discrimination (both probabilistic and unambiguous) of any set of modes,* i.e., for arbitrary commutation relations (1). Specifically, we show that those optimizations can be cast as a semidefinite programming (SDP) relaxation based on the work of Ref. [22]. Note that techniques based on SDP have also been used in the context of quantum state discrimination [23,24]. We present the recipes for the channel-discrimination scenario in Sec. II, and for the source-discrimination scenario in Sec. III. In Sec. IV, we illustrate our method with several case studies: two modes (Sec. IV A), phase discrimination (Sec. IV B), a family of d modes and its Fourier-dual family (Sec. IV C), and the modes that appear in the DPS QKD protocol (Sec. IV D). Finally, in Sec. V, we discuss the extension of our study when losses are present between the device that encodes the modes and the measurement.

II. CHANNEL-DISCRIMINATION SCENARIO

Let us first consider the channel-discrimination scenario. Suppose there are N different optical modes $\mathcal{M} = \{a_1, ..., a_N\}$, with commutation relations given by Eq. (1). As mentioned previously, in the presence of the reference beam, the phase of the signal mode could be defined relative to the the phase of the reference beam. Hence, the receiver's task is to discriminate between pure states $\mathcal{R} = \{|\psi_1\rangle, |\psi_2\rangle, ..., |\psi_N\rangle\}$, where

$$|\psi_j\rangle = \sum_{n=0}^{\infty} c_n \frac{(a_j^\dagger)^n}{\sqrt{n!}} |0\rangle \equiv \sum_{n=0}^{\infty} c_n |n_j\rangle\,, \tag{2}$$

where c_n is an arbitrary complex number such that $|c_n|^2 = p_n$ is the probability of the source emitting n photons. We also introduced the shorthand $|n_j\rangle$ denoting the n-photon state in the mode a_j. The inner product of the states associated to different modes can be computed easily:

$$\langle\psi_i|\psi_j\rangle = \sum_{n=0}^{\infty} p_n k_{ij}^n. \tag{3}$$

Note that the inner-product depends only on the photon number distribution $\{p_n\}$ and the commutation relations between different modes defined in Eq. (1).

A. Probabilistic mode discrimination

We first consider the setting for probabilistic discrimination. For uniform priors (our method can be easily generalized to any fixed priors), the optimal guessing probability is given by

$$P_{\text{corr}}^{\text{opt}} = \max_{\{M_j\},\{c_n\}} \frac{1}{N} \sum_{j=1}^{N} \langle\psi_j| M_j |\psi_j\rangle\,, \tag{4}$$

where M_j is the positive operator-valued measure (POVM) element associated with the outcome j and c_n is the coefficient of the state when written in the photon number basis. In other words, we have to optimize both the state and the measurements that maximize the guessing probability, subject to the energy constraint. Let us now cast this optimization into a SDP by adapting the techniques of Ref. [22]. Before getting to it, we notice that Refs. [22,25,26] consider a hierarchy of semidefinite relaxations, which, in general, only yield upper bounds on the guessing probability. However, since we only consider a single receiver with no classical inputs, going into the second level of the hierarchy will satisfy the rank loop condition [26] and hence the first level of the hierarchy is actually tight.

Here comes the construction. Consider the set $\mathcal{O} = \{\mathbb{1}, M_1, ..., M_N\}$. As discussed in [22,25,26], the $\{M_i\}$ can be taken as projective measurements without any loss of generality. Denoting O_i the elements of $\mathcal{O}$, one can define a set of vectors $\mathcal{S} = \{O_i|\psi_j\rangle : O_i \in \mathcal{O}, |\psi_j\rangle \in \mathcal{R}\}$. Since all Gram matrices are positive semidefinite, so is the $N(N+1) \times N(N+1)$ Gram matrix G associated to the set $\mathcal{S}$. Hence we have

$$\begin{aligned} P_{\text{corr}}^{\text{opt}} &= \max_{G,\{p_n\}} \frac{1}{N}\sum_{j=1}^{N} \langle\psi_j| M_j |\psi_j\rangle \\ \text{s.t. } & p_n \geqslant 0 \qquad \forall n, \\ & \sum_n p_n = 1, \\ & \sum_n p_n n = \bar{n}, \\ & G \succeq 0 \\ & \langle\psi_i|\psi_j\rangle = \sum_n p_n k_{ij}^n \qquad \forall i, j, \end{aligned} \tag{5}$$

where the last relation is Eq. (3) and determines the entries of G associated with $O_0 = \mathbb{1}$.

However, this is an optimization problem with infinitely many variables p_n and hence is computationally intractable. We the relax it by truncating the number of photons to $n_{\max}$ (i.e., we'll have $n_{\max}+1$ variables p_n). We do it in such a way as to obtain an *upper bound* $P_{\text{corr}}^{\text{SDP}} \geqslant P_{\text{corr}}^{\text{opt}}$ on the mode discrimination probabilities, that is, we derive some necessary (but not sufficient) conditions on the photon number distribution, and as a result the feasible region may be larger than the one allowed by quantum theory. Clearly, the relaxation can be made arbitrarily tight by increasing the photon number cutof, and we expect $P_{\text{corr}}^{\text{opt}} \approx P_{\text{corr}}^{\text{SDP}}$ when $\bar{n} \ll n_{\max}$.

We then define the truncated state

$$|\tilde{\psi}_j\rangle = \sum_{n=0}^{n_{\max}} c_n \frac{1}{\sqrt{n!}} a_j^{\dagger n} |0\rangle \tag{6}$$

that is subnormalized:

$$\sum_{n=0}^{n_{\max}} p_n \leqslant 1. \tag{7}$$

The inner product of the truncated states is

$$\langle\tilde{\psi}_i|\tilde{\psi}_j\rangle = \sum_{n=0}^{n_{\max}} p_n k_{ij}^n \tag{8}$$

and its difference with the inner product of the full states can be bounded as

$$\begin{aligned} |\langle\tilde{\psi}_i|\tilde{\psi}_j\rangle - \langle\psi_i|\psi_j\rangle| &= \left|\sum_{n>n_{\max}} p_n k_{ij}^n\right| \\ &\leqslant \sum_{n>n_{\max}} p_n |k_{ij}|^n \\ &\leqslant \left(1 - \sum_{n=0}^{n_{\max}} p_n\right) |k_{ij}|^{n_{\max}+1} \equiv \varepsilon_{ij}, \end{aligned} \tag{9}$$

where the first inequality is a consequence of triangle inequality and the second inequality is due to the fact that $|k_{ij}| \leqslant 1$. The constraint on the mean photon number can be relaxed to

$$\sum_{n=0}^{n_{\max}} p_n n + (n_{\max}+1)\left(1 - \sum_{n=0}^{n_{\max}} p_n\right) \leqslant \bar{n}. \tag{10}$$

All in all, we have $P_{\text{corr}}^{\text{opt}} \leqslant P_{\text{corr}}^{\text{SDP}}$ with

$$\begin{aligned} P_{\text{corr}}^{\text{SDP}} &= \max_{G,\{p_n\}} \frac{1}{N}\sum_{j=1}^{N} \langle\psi_j| M_j |\psi_j\rangle \\ \text{s.t. } & G \succeq 0 \\ & p_n \geqslant 0 \qquad \forall n \leqslant n_{\max} \\ & \sum_{n\leqslant n_{\max}} p_n \leqslant 1 \\ & \sum_{n\leqslant n_{\max}} p_n(n_{\max}+1-n) \geqslant n_{\max}+1-\bar{n} \\ & |\langle\psi_i|\psi_j\rangle - \langle\tilde{\psi}_i|\tilde{\psi}_j\rangle| \leqslant \varepsilon_{ij} \qquad \forall i, j, \end{aligned} \tag{11}$$

where the last constraint uses the expressions (8) and (9). That constraint is linear in the p_n when k_{ij} is real; when k_{ij} is complex, we can rewrite it as

$$\begin{pmatrix} \varepsilon_{ij} & \langle\psi_i|\psi_j\rangle - \langle\tilde{\psi}_i|\tilde{\psi}_j\rangle \\ (\langle\psi_i|\psi_j\rangle - \langle\tilde{\psi}_i|\tilde{\psi}_j\rangle)^* & \varepsilon_{ij} \end{pmatrix} \succeq 0, \tag{12}$$

which is a matrix inequality linear in the p_n, hence a valid SDP constraint.

B. Unambiguous mode discrimination

The same technique can be adapted to find the maximum success probability for unambiguous mode discrimination. For unambiguous discrimination, one must allow for the inconclusive outcome, which we associate to the POVM element $M_\varnothing$. The Gram matrix G will correspondingly increase in size to $N(N+2)\times N(N+2)$. Then we must add the constraint that the probability of error is zero:

$$\sum_{j=1}^{N}\sum_{i\neq j, i\neq\varnothing} \langle\psi_j| M_i |\psi_j\rangle = 0. \tag{13}$$

In the study of unambiguous discrimination, the aim is to minimize the probability of the inconclusive outcome or, equivalently, to maximize the success probability. Assuming uniform priors, the success probability is given by

$$P_{\text{UD}} = 1 - \frac{1}{N}\sum_{j=1}^{N} \langle\psi_j| M_\varnothing |\psi_j\rangle\,. \tag{14}$$

Note that both the success probability and the error probability are linear functions of the Gram matrix G. Hence, putting everything together, we have $P_{\text{UD}}^{\text{opt}} \leqslant P_{\text{UD}}^{\text{SDP}}$ with

$$\begin{aligned}
P_{\text{UD}}^{\text{SDP}} = \max_{G,\{p_n\}} \; & 1 - \frac{1}{N}\sum_{j=1}^{N} \langle\psi_j| M_\varnothing |\psi_j\rangle \\
\text{s.t. } & p_n \geqslant 0 \qquad \forall n \leqslant n_{\max} \\
& \sum_{n\leqslant n_{\max}} p_n \leqslant 1 \\
& \sum_{n\leqslant n_{\max}} p_n(n_{\max}+1-n) \geqslant n_{\max}+1-\bar{n} \qquad (15)\\
& G \succeq 0 \\
& |\langle\psi_i|\psi_j\rangle - \langle\tilde{\psi}_i|\tilde{\psi}_j\rangle| \leqslant \varepsilon_{ij} \qquad \forall i,j \\
& \sum_{j=1}^{N}\sum_{i\neq j, i\neq\varnothing} \langle\psi_j| M_i |\psi_j\rangle = 0.
\end{aligned}$$

Recall that unambiguous state discrimination is possible if and only if the states to be discriminated are linearly independent. But unambiguous mode discrimination is possible even for linearly dependent modes, as the linear independence of the states is provided by the multiphoton components. In fact, the families studied in Secs. IV B–IV D will be linearly dependent.

III. SOURCE-DISCRIMINATION SCENARIO

In the source-discrimination scenario, the task is to discriminate between states $\{\rho_1, \rho_2, ..., \rho_N\}$ that are *diagonal in the Fock basis*, subject to the energy constraint. Indeed, even assuming that the source produces a pure state

$$|\psi_j(\theta)\rangle = \sum_{n=0}^{\infty} c_n \frac{(e^{i\theta} a_j^\dagger)^n}{\sqrt{n!}} |0\rangle \qquad (16)$$

[this is Eq. (2) with explicit mention of the global phase θ of the signal mode], in the absence of a reference beam, the information available to the receiver is the phase-randomized state:

$$\rho_j = \int_0^{2\pi} \frac{d\theta}{2\pi} |\psi_j(\theta)\rangle\langle\psi_j(\theta)| = \sum_{n=0}^{\infty} p_n |n_j\rangle\langle n_j|. \qquad (17)$$

Since the states to be discriminated are diagonal in the Fock basis, nothing is lost if the receiver starts by measuring the number of photons, then uses the best discrimination strategy for the given value of n. This will manifest itself in the possibility of splitting the optimization in two steps.

A. Probabilistic mode discrimination

For probabilistic mode discrimination, the guessing probability is given by

$$\begin{aligned}
P_{\text{corr}}^{\text{opt}} &= \max_{\{p_n\},\{M_j\}} \frac{1}{N}\sum_{j=1}^{N} \text{Tr}(\rho_j M_j) \\
&\equiv \max_{\{p_n\}} \sum_{n=0}^{\infty} p_n P_{\text{corr}}^{(n)}, \qquad (18)
\end{aligned}$$

where

$$P_{\text{corr}}^{(n)} = \max_{\{M_j\}} \frac{1}{N}\sum_{j=1}^{N} \langle n_j| M_j |n_j\rangle \qquad (19)$$

is the optimal guessing probability for n photons. Therefore, as expected, we can split the optimization into two steps. In the first step, we solve (19) for each value of n. This can be done using the SDP technique of Ref. [22]. Similar to what we have done in the channel-discrimination scenario, consider the set $\mathcal{R}_n = \{|n_1\rangle, |n_2\rangle, ..., |n_N\rangle\}$ which are Fock state n from the set of modes $\mathcal{M}$. We define the set of vectors $\mathcal{S}_n = \{O_i|n_j\rangle : O_i \in \mathcal{O}, |n_j\rangle \in \mathcal{R}_n\}$. Now, denote the Gram matrix associated to $\mathcal{S}_n$ by $G^{(n)}$. The SDP to bound $P_{\text{corr}}^{(n)}$ is

$$\begin{aligned}
P_{\text{corr}}^{(n)} = \max_{G^{(n)}} \; & \frac{1}{N}\sum_{j=1}^{N} \langle n_j| M_j |n_j\rangle \\
\text{s.t. } & G^{(n)} \succeq 0 \qquad (20)\\
& \langle n_i| n_j\rangle = k_{ij}^n,
\end{aligned}$$

which we have to solve for each photon number n. In the second step, having $P_{\text{corr}}^{(n)}$ for each photon number n, we just need to enforce the energy constraint. This remaining step is a linear program (LP):

$$\begin{aligned}
P_{\text{corr}}^{\text{opt}} = \max_{\{p_n\}} \; & \sum_n p_n P_{\text{corr}}^{(n)} \\
\text{s.t. } & p_n \geqslant 0 \qquad \forall n, \\
& \sum_n p_n = 1, \qquad (21)\\
& \sum_n p_n n = \bar{n}.
\end{aligned}$$

Like in the channel-discrimination scenario, we have infinitely many variables p_n, so we need a cutoff that relaxes the original LP. With the same arguments as above, the resulting relaxation $P_{\text{corr}}^{\text{LP}} \geqslant P_{\text{corr}}^{\text{opt}}$ is given by

$$\begin{aligned}
P_{\text{corr}}^{\text{LP}} = \max_{\{p_n\}} \; & \sum_{n=0}^{n_{\max}} p_n P_{\text{corr}}^{(n)} + \left(1 - \sum_{n=0}^{n_{\max}} p_n\right) \\
\text{s.t. } & p_n \geqslant 0 \qquad \forall n \leqslant n_{\max}, \\
& \sum_{n=0}^{n_{\max}} p_n \leqslant 1, \qquad (22)\\
& \sum_{n=0}^{n_{\max}} p_n n + \left(1 - \sum_{n=0}^{n_{\max}} p_n\right)(n_{\max}+1) \leqslant \bar{n}.
\end{aligned}$$

Notice that this relaxation is equivalent to assuming that the modes are perfectly distinguishable for $n > n_{\max}$. This is a good approximation when we pick sufficiently high photon number cutoff $n_{\max}$.

B. Unambiguous mode discrimination

Also, for unambiguous state discrimination, the optimal success probability is of the form

$$P_{\mathrm{UD}}^{\mathrm{opt}} = \max_{\{p_n\}} \sum_n p_n P_{\mathrm{UD}}^{(n)} \tag{23}$$

and can be bounded in two steps. In the first step, $P_{\mathrm{UD}}^{(n)}$ is computed from the SDP,

$$\begin{aligned} P_{\mathrm{UD}}^{(n)} = \max_{G^{(n)}} 1 - \frac{1}{N}\sum_{j=1}^{N} \langle n_j|\, M_{\varnothing}\, |n_j\rangle \\ \text{s.t. } G^{(n)} \succeq 0, \\ \langle n_i|n_j\rangle = k_{ij}^{n}, \\ \langle n_j|\, M_i\, |n_j\rangle = 0, \quad \forall i \neq j, i \neq \varnothing, \end{aligned} \tag{24}$$

where the last constraint captures the unambiguous discrimination condition

$$\sum_{j=1}^{N} \sum_{i\neq j, i\neq\varnothing} \mathrm{Tr}(\rho_j M_i) = 0, \tag{25}$$

which is indeed satisfied if and only if $\langle n_j|\, M_i\, |n_j\rangle = 0$ for all n whenever $i \neq \varnothing$, $j \neq i$. In the second step, the energy constraint is enforced in a LP, which we write down directly for the relaxation $P_{\mathrm{UD}}^{\mathrm{LP}} \geqslant P_{\mathrm{UD}}^{\mathrm{opt}}$ with a photon-number cutoff:

$$\begin{aligned} P_{\mathrm{UD}}^{\mathrm{LP}} = \max_{\{p_n\}} \sum_{n=0}^{n_{\max}} p_n P_{\mathrm{UD}}^{(n)} + \left(1 - \sum_{n=0}^{n_{\max}} p_n\right) \\ \text{s.t. } p_n \geqslant 0 \qquad \forall n \leqslant n_{\max}, \\ \sum_{n=0}^{n_{\max}} p_n \leqslant 1, \\ \sum_{n=0}^{n_{\max}} p_n n + \left(1 - \sum_{n=0}^{n_{\max}} p_n\right)(n_{\max}+1) \leqslant \bar{n}. \end{aligned} \tag{26}$$

C. Toward an analytical solution of the LP

We have just seen that the final step of the optimization for the source-discrimination scenario is a LP of the form

$$\begin{aligned} P^{\mathrm{opt}} = \max_{\{p_n\}} \sum_n p_n \mathsf{a}_n \\ \text{s.t. } p_n \geqslant 0 \qquad \forall n, \\ \sum_n p_n = 1, \\ \sum_n p_n n = \bar{n}, \end{aligned} \tag{27}$$

where $\mathsf{a}_n = P_{\mathrm{corr}}^{(n)}$ for probabilistic discrimination and $\mathsf{a}_n = P_{\mathrm{UD}}^{(n)}$ for unambiguous discrimination. For a given set of coefficients $\{\mathsf{a}_n\}$, this LP can be solved analytically. We are going to show how this can be done and highlight a condition on the $\{\mathsf{a}_n\}$ under which the solution can be easily spelled out.

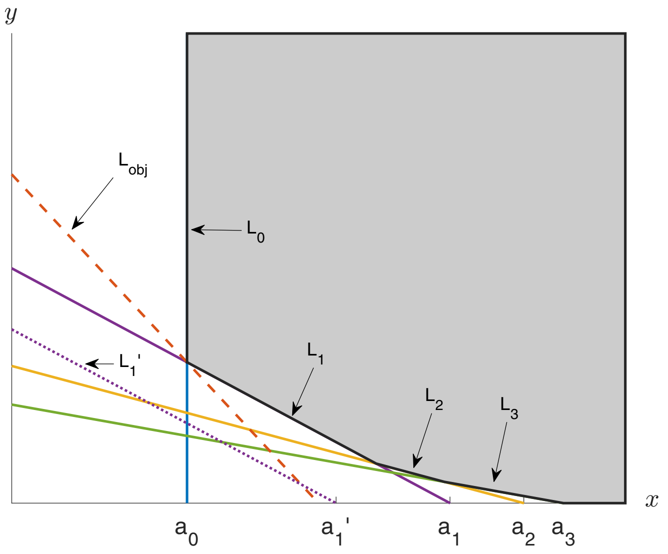

FIG. 2. Geometrical solution of the dual LP (28). The first constraint is associated to the line $L_0 : x = \mathsf{a}_0$, and is satisfied in the half-space $x \geqslant \mathsf{a}_0$. For $n > 0$, the constraint is associated to the line $L_n : y = -\frac{1}{n}(x - \mathsf{a}_n)$ and the region satisfying that constraint is the upper half-space above L_n. The *feasible region* is the region where all constraints are satisfied (shaded area, drawn for $n \leqslant 3$). The objective function is a line L_{obj} with gradient $-1/\bar{n}$ (dashed; for the plot, $\bar{n} = 0.5$). The dual problem can hence be understood as finding the minimum y-intercept by translating the line L_{obj} vertically while ensuring that it still touches the feasible region. The a_n satisfy (29) and thus all the L_n contribute nontrivially to the boundary of the feasible region. Had we chosen a_1' instead of a_1, the line L_1' (dotted) would not contribute to that boundary; that is, the constraint for $n = 1$ would always be satisfied within the feasible region.

The LP (27) is written in the so-called *primal* form. One could also consider its *dual* form given by [27]

$$\begin{aligned} d^* = \min_{x,y}\, x + \bar{n} y \\ \text{s.t. } y \geqslant -\frac{1}{n}(x - \mathsf{a}_n) \quad \forall n. \end{aligned} \tag{28}$$

Due to the strong duality of LP, we know that $d^* = P^{\mathrm{opt}}$ and hence it is sufficient to solve the dual problem.

Whereas the primal problem is an optimization over infinitely many variables with a few equality constraints, the dual problem is an optimization over two variables with infinitely many constraints, which define the *feasible region*. The way to solve the dual problem is easily understood geometrically (Fig. 2). One translates the lines $L_{\mathrm{obj}}(d) = \{(x, y)\,|\, x + \bar{n} y = d\}$ with fixed gradient $-1/\bar{n}$ till finding the lowest one that has at least one point in the feasible region. But the boundary of the feasible region is given by segments of straight lines L_n of gradient $-1/n$. So the limiting line $L_{\mathrm{obj}}(d^*)$ may touch the boundary of the feasible set either in a single point (the intersection of two L_n, as illustrated in the figure) or in a whole segment. The latter can only happen if $\bar{n} = n$, but this is not the only condition: It is further necessary that L_n contributes to the boundary of the feasible region. This may not always be the case, as illustrated in Fig. 2. By this recipe, one can always find the solution, given the a_n.

It is worth describing in detail the case where *all* the constraints in (28), i.e., all the L_n, contribute to the boundary of the feasible region in a nontrivial way. Given that the gradient of L_n is $-1/n$, a necessary and sufficient condition for the boundary to be as described is that $x_{n-1,n} < x_{n,n+1}$ where $(x_{n,m}, y_{n,m})$ are the coordinates of the intersection of L_n with L_m. From $y_{n-1,n} = -\frac{1}{n-1}(x_{n-1,n} - \mathsf{a}_{n-1}) = -\frac{1}{n}(x_{n-1,n} - \mathsf{a}_n)$, one immediately finds $x_{n-1,n} = n\mathsf{a}_{n-1} - (n-1)\mathsf{a}_n$. Thus, $x_{n-1,n} < x_{n,n+1}$ will be the case if and only if

$$\mathsf{a}_{n-1} - 2\mathsf{a}_n + \mathsf{a}_{n+1} < 0. \tag{29}$$

If this condition is satisfied, then the optimal discrimination takes up a very clear form. Indeed, for a boundary as described:

(i) If $\bar{n} \notin \mathbb{N}$, the intersection that defines d^* will be with a single point, namely, the intersection of $L_{\lfloor\bar{n}\rfloor}$ and $L_{\lceil\bar{n}\rceil}$. The optimal state is then a mixture of two Fock states with these numbers, and the suitable weights.

(ii) If $\bar{n} = n \in \mathbb{N}$, the intersection that defines d^* will be the whole segment of gradient $-1/n$, and the optimal state with be the Fock state $\rho = |n\rangle\langle n|$.

In other words, the solution of the LP will be $P^{\text{opt}} = p_{\lfloor\bar{n}\rfloor}\mathsf{a}_{\lfloor\bar{n}\rfloor} + p_{\lceil\bar{n}\rceil}\mathsf{a}_{\lceil\bar{n}\rceil}$, with

$$p_n = \begin{cases} 1 + \lfloor\bar{n}\rfloor - \bar{n} & \text{if } n = \lfloor\bar{n}\rfloor \\ \bar{n} - \lfloor\bar{n}\rfloor & \text{if } n = \lfloor\bar{n}\rfloor + 1 \\ 0 & \text{otherwise.} \end{cases} \tag{30}$$

Thus, in many cases, we can expect the optimal state for discrimination to consist of the Fock state $|\bar{n}\rangle$ if $\bar{n} \in \mathbb{N}$, and of the suitable mixture of the Fock states $|\lfloor\bar{n}\rfloor\rangle$ and $|\lceil\bar{n}\rceil\rangle$ if $\bar{n} \notin \mathbb{N}$. However, condition (29) does not always hold: In Sec. IV C, we shall see an example where it is not met for $n = 1$, and indeed the Fock state $|1\rangle$ will not be optimal for $\bar{n} = 1$.

IV. CASE STUDIES

We have derived efficient relaxations for estimating the parameters of mode discrimination, both probabilistic and unambiguous, in both the channel-discrimination and the source-discrimination scenario. In this section, we discuss some case studies.

A. Two modes

The discrimination between two modes is determined by a single parameter:

$$[a_1, a_2^\dagger] = k\mathbb{1}, \quad k \in \mathbb{C}, \ |k| \leqslant 1. \tag{31}$$

When $k = 1$, the two modes are identical and therefore indistinguishable. When $k = 0$, the two modes are orthogonal and can be perfectly distinguished when $\bar{n} \geqslant 1$.

Besides using our numerical tools, we are going to derive analytical solutions, exploiting the fact that the discrimination of two equally probable pure states has been solved long ago for both probabilistic [28] and unambiguous discrimination [29–31]:

$$\begin{aligned} P_{\text{corr}}^{\text{opt}} &= \tfrac{1}{2}\left(1 + \sqrt{1 - |\langle\psi_1|\psi_2\rangle|^2}\right), \\ P_{\text{UD}}^{\text{opt}} &= 1 - |\langle\psi_1|\psi_2\rangle|. \end{aligned} \tag{32}$$

With this, single-shot discrimination of two modes in the *source-discrimination scenario* can be fully solved analytically. Indeed, there is no need to solve the SDPs (20) and (24) since we know from (32) that $P_{\text{corr}}^{(n)} = \frac{1}{2}(1 + \sqrt{1 - |k|^{2n}})$ and $P_{\text{UD}}^{(n)} = 1 - |k|^n$ (notice that everything depends on $|k|$). Moving to the LP, it is immediate to verify that both expressions satisfy condition (29). So we can import from Sec. III C that the solution is

$$P_{\text{corr/UD}}^{\text{opt}} = p_{\lfloor\bar{n}\rfloor}P_{\text{corr/UD}}^{(\lfloor\bar{n}\rfloor)} + p_{\lceil\bar{n}\rceil}P_{\text{corr/UD}}^{(\lceil\bar{n}\rceil)}, \tag{33}$$

with the p_n given in (30).

In the *channel-discrimination scenario*, we know from (32) that $P_{\text{corr}}^{\text{opt}} = \frac{1}{2}(1 + \sqrt{1 - \chi^2})$ and $P_{\text{UD}}^{\text{opt}} = 1 - \chi$ with

$$\begin{aligned} \chi = \min_{\{p_n\}} & \left|\sum_{n=0}^{\infty} p_n k^n\right| \\ \text{s.t.} \ & p_n \geqslant 0 \qquad \forall n, \\ & \sum_n p_n = 1, \\ & \sum_n p_n n = \bar{n}, \end{aligned} \tag{34}$$

where we used the expression (3) of the scalar product. Instead of the SDPs, we could try and solve (34).

For $k \geqslant 0$, it is a LP of the form (28) with $\mathsf{a}_n \equiv -k^n$ (notice that here we are minimizing, whence the sign). Condition (29) reads $-k^{n-1}(1 + k^2) < 0$ and is therefore satisfied, so we know that the solution is

$$\chi = p_{\lfloor\bar{n}\rfloor}k^{\lfloor\bar{n}\rfloor} + p_{\lceil\bar{n}\rceil}k^{\lceil\bar{n}\rceil} \qquad [k \geqslant 0], \tag{35}$$

with the p_n given in (30). The corresponding optimal state is $\sqrt{p_{\lfloor\bar{n}\rfloor}}\,|\lfloor\bar{n}\rfloor\rangle + e^{i\varphi}\sqrt{p_{\lceil\bar{n}\rceil}}\,|\lceil\bar{n}\rceil\rangle$ for any φ. This value of χ shows that $P_{\text{corr}}^{\text{opt}}$ is larger than in the source-discrimination scenario (33), since $\sqrt{1 - \chi^2} \geqslant p_{\lfloor\bar{n}\rfloor}\sqrt{1 - k^{2\lfloor\bar{n}\rfloor}} + p_{\lceil\bar{n}\rceil}\sqrt{1 - k^{2\lceil\bar{n}\rceil}}$; while the value of $P_{\text{UD}}^{\text{opt}}$ is identical in the two scenarios.

For $k < 0$, the optimization (34) is also LP; but whether the absolute value adds a minus sign or not (i.e., whether $\mathsf{a}_n = +k^n$ or $-k^n$) is not known *a priori*. One would therefore have to solve the two LPs, then compare the solutions. In either case, condition (29) would be satisfied only for alternate n, and so the solution is not expected to involve only $\lfloor\bar{n}\rfloor$ and $\lceil\bar{n}\rceil$. As for $k \in \mathbb{C} \setminus \mathbb{R}$, the optimization (34) is quadratic, and there is no guarantee that an analytical solution can be found.

We thus turn to our SDPs (11) and (15). The results are shown in Fig. 3 for probabilistic discrimination, and in Fig. 4 for unambiguous discrimination. As expected, the modes are harder to distinguish when $k \approx 1$. More remarkable is the fact that distinguishability improves significantly in the region of negative phases. For instance, while it is known and rather obvious that perfect discrimination for $k = 0$ becomes possible for $\bar{n} \geqslant 1$, we see that when $k = -1$ the modes can already be perfectly distinguished for $\bar{n} = 0.5$ (more in Sec. IV B).

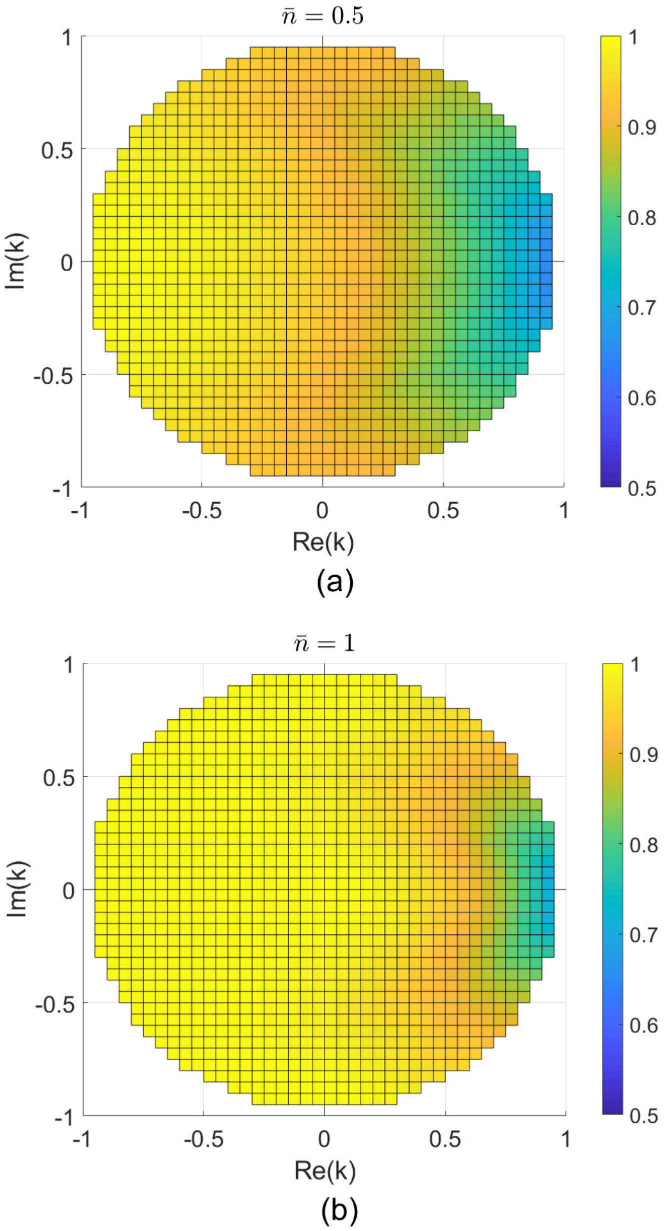

FIG. 3. Probabilistic channel discrimination between two modes: dependence on the mode overlap $k \in \mathbb{C}$. Upper bound $P^{\mathrm{SDP}}_{\mathrm{corr}}$ on the guessing probability, solution of the SDP (11) for $n_{\max} = 300$, in a polar plot of k, for (a) $\bar{n} = 0.5$ and (b) $\bar{n} = 1$.

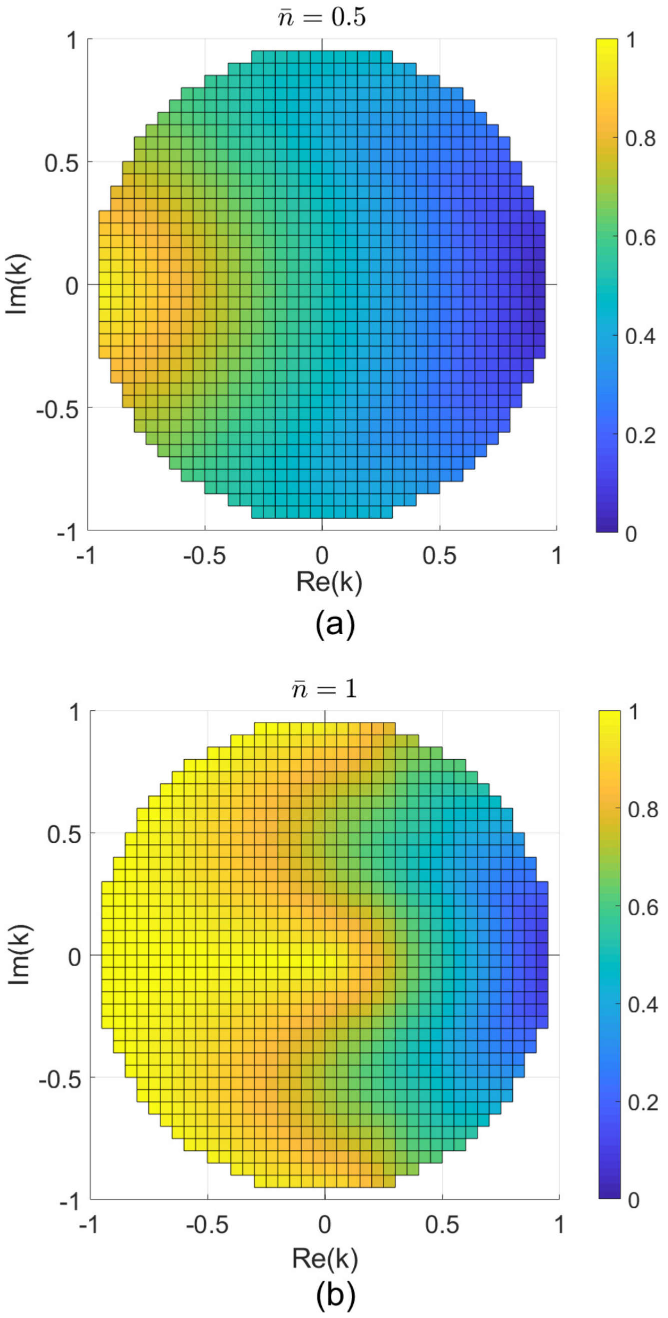

FIG. 4. Unambiguous channel discrimination between two modes: dependence on the mode overlap $k \in \mathbb{C}$. Upper bound $P^{\mathrm{SDP}}_{\mathrm{UD}}$ on the guessing probability, solution of the SDP (15) for $n_{\max} = 300$, in a polar plot of k, for (a) $\bar{n} = 0.5$ and (b) $\bar{n} = 1$.

B. Phase discrimination

Next we consider the problem of phase discrimination. Since the phase of an optical mode is not defined unless a reference beam is provided, this case study is restricted to the channel-discrimination scenario. The receiver's task is to guess one of a set of unitary channels $U_j = e^{i\varphi_j \hat{n}}$, where $\hat{n}$ is the number operator in the signal mode. In other words, the receiver can use pure states to distinguish modes of the form

$$a_j = e^{i\varphi_j} a, \tag{36}$$

where a is the initial signal mode prior to the phase-shift.

Our formalism can be applied to *any set of phases* to be discriminated. For the numerical case study, we choose the symmetric set $\{\varphi_j = 2\pi j/N | j = 0, \ldots, N-1\}$, whose probabilistic discrimination has been studied in the context of quantum sensing [4]. The commutation relations are then given by

$$[a_j, a_k^\dagger] = e^{i2\pi(j-k)/N} \mathbb{1}. \tag{37}$$

For probabilistic discrimination [see Fig. 5(a)], our SDP (11) recovers the same bound as Theorem 3 of Ref. [4]. The study of unambiguous discrimination is unique: the result is plotted in Fig. 5(b). Also notice that, for $N > 2$, the modes in this family are linearly dependent but, as discussed, unambiguous

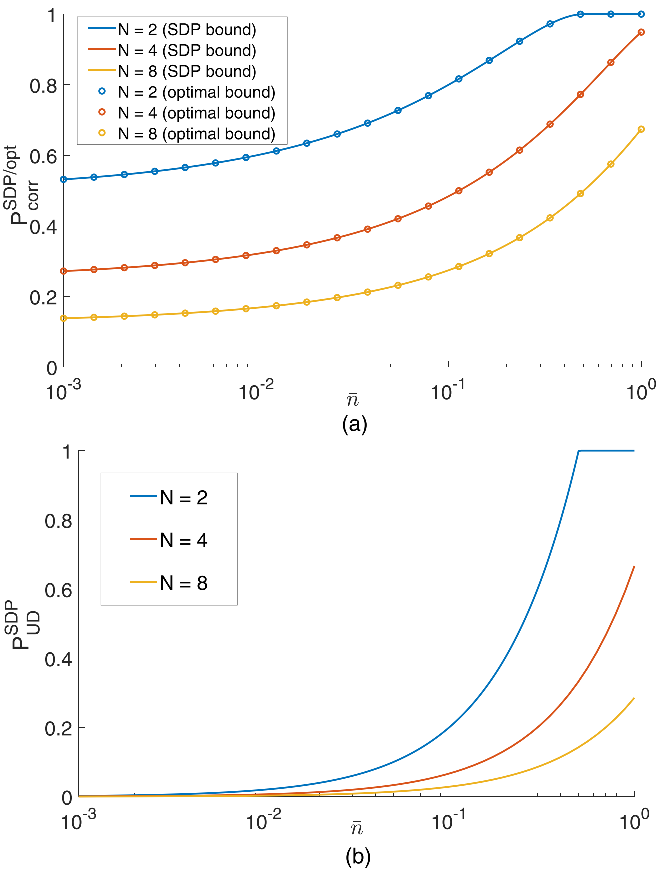

FIG. 5. Phase discrimination: Dependence on $\bar{n}$. (a) Upper bound $P_{\text{corr}}^{\text{SDP}}$ on the guessing probability, solution of the SDP (11). (b) Upper bound $P_{\text{UD}}^{\text{SDP}}$ on the success probability, solution of the SDP (15). Both SDPs solved for $n_{\max} = 50$. In (a), the circles denote the analytical bounds from Theorem 3 of Ref. [4].

discrimination is possible because one can create linearly independent states.

The $N = 2$ case corresponds to $k = -1$ in Sec. IV A. As we notice there and see again here, perfect discrimination becomes possible at $\bar{n} = 0.5$. This is because the pure states with $c_0 = c_1 = \frac{1}{\sqrt{2}}$ are orthogonal. Indeed, $|\psi_a\rangle = \frac{1}{\sqrt{2}}(|0\rangle + a^\dagger\,|0\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle_a)$, while $|\psi_{-a}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-a^\dagger)\,|0\rangle) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle_a)$. Since distinguishability cannot decrease when increasing $\bar{n}$, one expects to find two orthogonal states for any $\bar{n} \geqslant 0.5$. Indeed, these are $\sqrt{\frac{1-\delta}{4}}\,|m-1\rangle_a \pm \frac{1}{\sqrt{2}}\,|m\rangle_a + \sqrt{\frac{1+\delta}{4}}\,|m+1\rangle_a$ with $\bar{n} = m + \delta/2$ and $-1 \leqslant \delta < 1$. In general, these are superpositions of three Fock states, reducing to two only when $\bar{n} = m - \frac{1}{2}$ ($\delta = 0$). Thus, as anticipated, the optimal state does not obey (30).

C. Computational and Fourier transform basis modes

As our next example, we consider a family made of two sets of orthogonal modes. The first set $\mathcal{C}_d = \{a_0, a_1, ..., a_{d-1}\}$ is called *computational basis modes*. The second set $\mathcal{F}_d = \{b_0, b_1, ..., b_{d-1}\}$ is called *Fourier transform basis modes* and is defined as

$$b_k = \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}(\omega_d)^{jk}a_j, \tag{38}$$

where $\omega_d = e^{2\pi i/d}$ is the dth root of unity. This family of modes has appeared in quantum cryptography: The classical information is encoded into these modes in the famous BB84 protocol [13] for $d = 2$, and the case $d > 2$ defines one of its possible generalizations to higher alphabets [32]. However, in those QKD protocols, the classical information is encoded in the mode's *index*: one wants to determine j, whether from a_j or b_j. By contrast, here we stay with the task of mode discrimination and study both probabilistic and unambiguous discrimination from the set $\mathcal{M}_d = \mathcal{C}_d \cup \mathcal{F}_d$.

For given d, the commutation relations are

$$\begin{aligned} [a_j, a_k^\dagger] &= \delta_{jk}\mathbb{1}, \\ [b_j, b_k^\dagger] &= \delta_{jk}\mathbb{1}, \\ [a_j, b_k^\dagger] &= \frac{1}{\sqrt{d}}(\omega_d^*)^{jk}\mathbb{1}. \end{aligned} \tag{39}$$

We set $n_{\max} = 50$ and solve the SDP and/or LP for $\bar{n}$ varying from 10^{-3} to 10, and for $d = 2, 3, 4, 5$. The results for probabilistic discrimination are shown in Fig. 6(a); those for unambiguous discrimination in Fig. 6(b); both figures contain information about the channel-discrimination scenario (dashed) and the source-discrimination scenario (solid).

Channel discrimination is more powerful than source discrimination: while more marked for probabilistic discrimination, the difference is also present in unambiguous discrimination, contrary to what was the case for two modes (Sec. IV A). Another feature present in both figures, again more marked for probabilistic discrimination, is a crossover of behavior as a function of $\bar{n}$: for $\bar{n} \lesssim 1$, the discrimination is better for smaller d; whereas for $\bar{n} \gtrsim 1$, the discrimination is better for higher d. This can be understood qualitatively. In the limit $\bar{n} \to 0$, guessing the mode is hardly more than a random pick from a uniform distribution, the guessing probability is close to $\frac{1}{2d}$ and decreases with d. In the limit of large n, $|\langle n_{a_j}|n_{b_k}\rangle| = \sqrt{1/d^n}$ decreases with d and therefore the distinguishability increases.

In the source-discrimination scenario, we find that condition (29) is generally not satisfied for $\bar{n} = 1$, either for probabilistic or unambiguous discrimination.

For unambiguous discrimination, the reason is clear: the single-photon states are linearly dependent and hence unambiguous discrimination is not possible. For unambiguous discrimination to be possible, the state must contain some multiphoton component.

For probabilistic discrimination, we find that the condition (29) is violated for $d = 3, 4, 5$. To see that, we compare $P_{\text{corr}}^{\text{LP}}$ with that of Fock states in Fig. 7. For $d = 2, 3, 4, 5$, the single-photon bound is $P_{\text{corr}}^{(1)} = 0.5$. This corresponds to a simple strategy: Bet on one of the bases and measure in it.

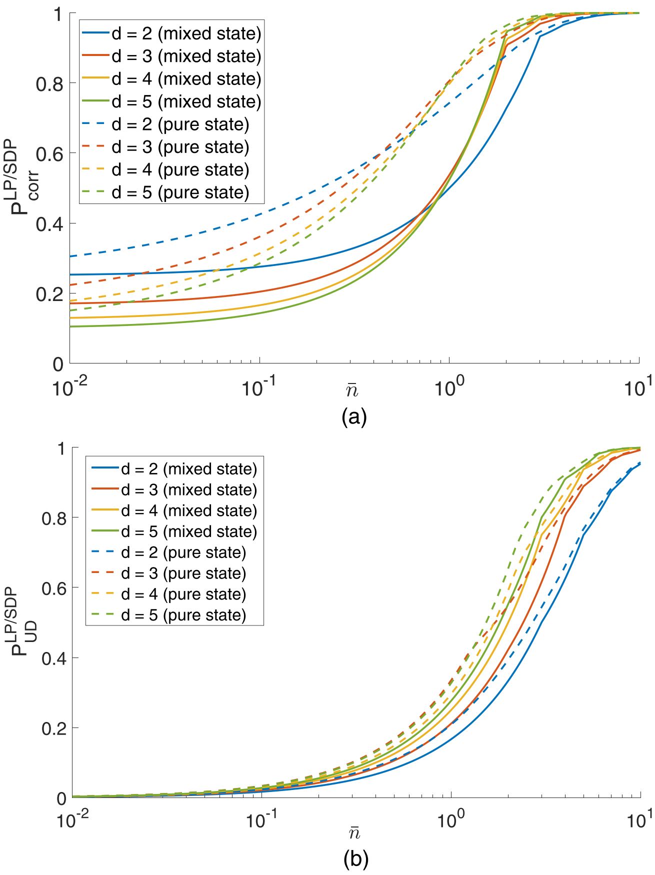

FIG. 6. Computational and Fourier transform basis modes: Dependence on $\bar{n}$. (a) Upper bound on the guessing probability for probabilistic discrimination. (b) Upper bound on the success probability for unambiguous discrimination. The solid lines are the bounds in the source-discrimination scenario, obtained by solving the LP (22) or (26), respectively, whereas the dashed curves are the bounds in the channel-discrimination scenario, obtained by solving the SDP (11) or (15). For this family of modes, it is sufficient to set $n_{\max} = 50$.

D. Differential-phase-shift modes

Lastly, we consider a family of modes inspired by the DPS QKD protocol [14]. In the protocol, the information is encoded in the relative phase between subsequent temporal modes. Abstractly, to any ℓ-bit strings $\mathbf{x}$, a mode is associated according to

$$b_{\mathbf{x}} = \frac{1}{\sqrt{\ell+1}}\left(a_0 + \sum_{i=1}^{\ell} e^{i\varphi_i^{(\mathbf{x})}} a_i\right), \tag{40}$$

where the $\{a_i\}_{i=0,\dots,\ell}$ are $(\ell+1)$ orthogonal modes (temporal ones in the original setting) and where

$$\varphi_i^{(\mathbf{x})} - \varphi_{i-1}^{(\mathbf{x})} = x_i \pi, \tag{41}$$

with $x_i \in \{0, 1\}$ the ith bit of the string $\mathbf{x}$ (by convention, we set the phase of the reference mode $\varphi_0^{(\mathbf{x})} = 0$ for all $\mathbf{x}$). For a given ℓ, there are 2^ℓ different modes, only linearly many of which are orthogonal among the 2^ℓ ones. The commutation relation for the modes associated to strings $\mathbf{x}$ and $\mathbf{y}$ can be computed recursively using the relation (41) and is given by

$$\left[b_{\mathbf{x}}, b_{\mathbf{y}}^\dagger\right] = \frac{1}{\ell+1}\left(1 + \sum_{i=1}^{\ell} e^{i(\varphi_i^{(\mathbf{x})} - \varphi_i^{(\mathbf{y})})}\right)\mathbb{1}. \tag{42}$$

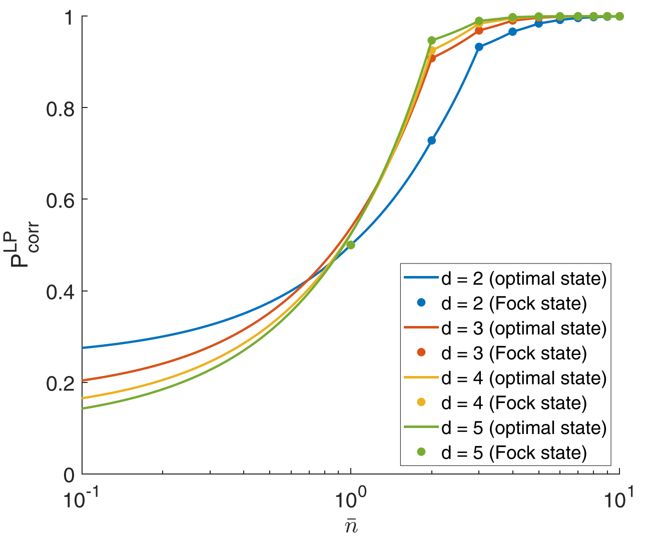

FIG. 7. Computational and Fourier transform basis modes: optimal state versus Fock states (for probabilistic discrimination in the source-discrimination scenario). The solid lines are the bound $P_{\text{corr}}^{\text{LP}}$, the solution to (22) with $n_{\max} = 50$. On the other hand, the dots represent the bound $P_{\text{corr}}^{(n)}$, the solution to the SDP (19).

Since the SDP scales badly with ℓ, in this paper we present the results only for $\ell = 1, 2, 3$. When $\ell = 1$, the two modes to be distinguished are orthogonal, and so this is a special case of what we studied in Sec. IV A. For $\ell = 2$, the four modes are all nonorthogonal. The eight modes for $\ell = 3$ form two sets of four orthogonal modes.

The results of our numerical method are shown in Fig. 8(a) for probabilistic discrimination, and in Fig. 8(b) for unambiguous discrimination. Since the family given by ℓ is constructed from $\ell + 1$ orthogonal modes (pulses), we found it more appropriate to compare the families for a given value of the *energy per pulse* $\mu = \bar{n}/(\ell + 1)$, rather than of the total energy $\bar{n}$. Even with this scaling, it proves more difficult to distinguish within a set with higher ℓ, since the receiver has to discriminate more modes.

Comparing the mixed state encoding to the pure state encoding, we find that the pure state encoding is more distinguishable only in the probabilistic discrimination setting. Remarkably, we find that the mixed state bounds coincide with that of the pure state encoding for the unambiguous discrimination setting.

V. CODA: ON LOSSES

In this last section, we review how the ultimate limits of mode discrimination are modified when there are *mode-independent losses* between the device to be tested and the measurement, as sketched in Fig. 9. This is modeled as a beam-splitter transformation $a_j \longrightarrow ta_j + rb_j$, where t and r can be taken as real and positive and $t^2 + r^2 = 1$. The state

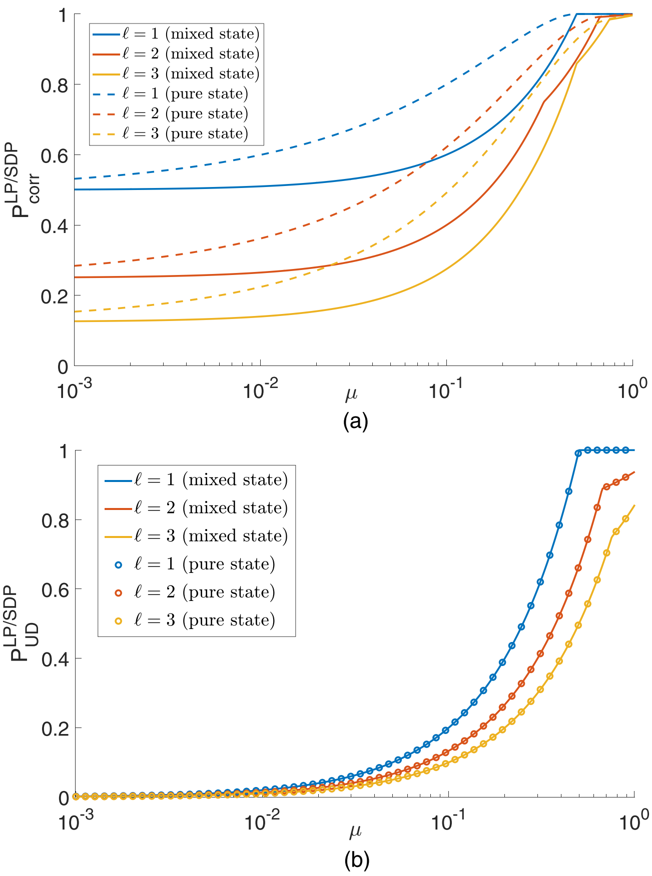

FIG. 8. Discriminating the differential-phase-shift modes: Dependence on the energy per pulse μ. (a) Upper bound on the guessing probability for probabilistic discrimination. (b) Upper bound on the success probability for unambiguous discrimination. In both cases, the solid lines are the bounds for source-discrimination scenario: Solutions to the LPs (22) and (26), respectively. The dashed curves in (a) and the circles in (b) are the bounds for channel-discrimination scenario obtained by solving the SDPs (11) and (15), respectively. Here, we set $n_{\max} = 50$.

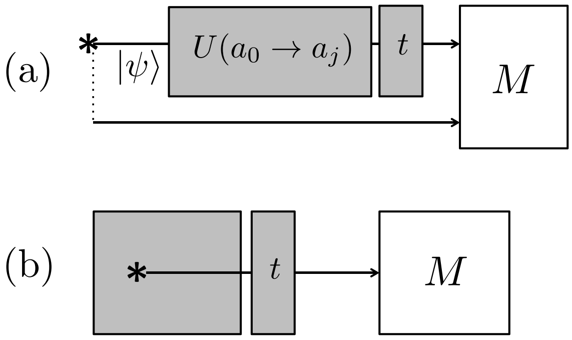

FIG. 9. The two scenarios studied in this paper, with additional mode-independent losses before the measurement device (t refers to the transmittivity).

TABLE I. Photon-number weights of the optimal input states, for $\bar{n} = 1$ and $k = 0.4$ (thick dots in Fig. 10). The result for $t^2 = 1$ is analytical [see (35) in Sec. IV A], the other values are the output of the heuristic optimization. The coherent state weights $e^{-1}/n!$ are given for reference in the last line.

t^2	p_0	p_1	p_2	p_3	p_4	p_5
1 (Fock)	0	1	0	0	0	0
0.9	0.1458	0.7088	0.1454	0.0000	0.0000	0.0000
0.5	0.3075	0.4363	0.2092	0.0430	0.0039	0.0001
0.2	0.3450	0.3914	0.1952	0.0567	0.0105	0.0012
coh	*0.3679*	*0.3679*	*0.1839*	*0.0613*	*0.0153*	*0.0031*

that arrives at the measurement station is now the partial state associated with the transmitted output.

The study of the source-discrimination scenario remains practically unchanged. Indeed, losses do not introduce any coherence between photon number states. So, if the state before the losses is given by Eq. (17), the state after the losses will still be a number mixture $\rho_j(t) = \sum_{n=0}^{\infty} q_n(t)|n_j\rangle\langle n_j|$, with

$$q_n(t) = \sum_{m\geqslant n} p_m \binom{m}{n} (1-t^2)^{m-n} t^{2n}. \tag{43}$$

If $\bar{n}$ still represents the energy constraint for the input state, one solves the LP under the energy constraints $\bar{n}t^2$ to get the $\{q_n(t)\}$. The $\{p_n\}$ to be prepared are then obtained by inverting the linear system of equations (43). The only practical worries may come from numerical cutoffs in this inversion when $\bar{n}$ is large.

On the contrary, the optimizations in the channel-discrimination scenario can no longer be cast as SDPs. Indeed, the initially pure state becomes mixed with losses. Thus, on the one hand, we cannot build Gram matrices as we did in Sec. II. On the other hand, the basis in which the mixed state is diagonal is not fixed, and is definitely not the Fock basis, so we cannot adapt the approach of Sec. III either.

In some simple cases, a *heuristic* optimization may still be trustful. For instance, let us look at the probabilistic discrimination of two modes with $k \geqslant 0$. We know [28] that the probability of discriminating correctly between two equally probable mixed states is given by $P_{\rm corr}(\rho_1, \rho_2) = \frac{1}{2}(1 + \frac{1}{2}{\rm Tr}|\rho_1 - \rho_2|)$. One can then write the algorithm that, given a $|\psi_j\rangle$ in the form (2), computes the $\rho_j(t)$ obtained after losses, then heuristically maximizes the trace distance $|\rho_1(t) - \rho_2(t)|$ over the complex parameters c_n under the energy constraint $\sum_n n|c_n|^2 = \bar{n}$ for the initial states. We implemented this procedure using the function fmincon of MATLAB. Inspection of the numerical solutions we obtained indicates that the relevant parameter in the input state are the $p_n = |c_n|^2$, while the arguments of the c_n (relative phases) do not seem to matter, just as in the lossless case (34).

An example is given in Fig. 10. The constraint is set at $\bar{n} = 1$: thus, in the absence of losses, the optimal state is the Fock state $|1\rangle$. When losses increase, this state becomes quickly suboptimal, while the probability $P_{\rm corr}^{\rm opt}(k, \bar{n}, t)$ of guessing correctly approaches the value corresponding to choosing a *coherent state* as the input state (see also Table I). Based on this observation, whenever $\bar{n} = m$ integer, for the sake of estimates one could use

$$P_{\rm corr}^{\rm opt} \gtrsim \max\left(P_{\rm corr}^{\rm coh}, P_{\rm corr}^{\rm Fock}\right) \tag{44}$$

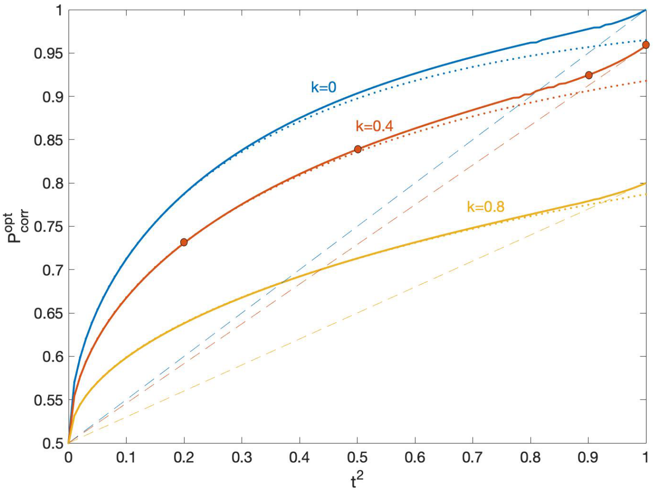

FIG. 10. Probabilistic discrimination of two modes as a function of losses (channel-discrimination scenario). Plot of $P^{\rm opt}_{\rm corr}(k,\bar{n},t)$ as a function of t^2 for $\bar{n}=1$ and $k=0,0.4,0.8$ (from top to bottom). The thick solid lines are the result of the heuristic optimization (for which the photon number was truncated at 5); on the line for $k=0.4$ are indicated the points reported in Table I. The dotted lines are the values $P^{\rm coh}_{\rm corr}$ for coherent state input; the dashed lines are the values $P^{\rm Fock}_{\rm corr}$ for Fock state input.

because the two probabilities on the right-hand side can be given analytically. Indeed, on a beam splitter, a coherent state splits as $|\alpha\rangle \rightarrow |t\alpha\rangle_T\,|r\alpha\rangle_R$; so the states in the transmitted mode are pure and a standard calculation gives $\langle t\alpha|_0\,|t\alpha\rangle_1 = e^{-|t\alpha|^2(1-k)}$ and, finally, $P^{\rm coh}_{\rm corr}(k,\bar{n},t)=\frac{1}{2}(1+\sqrt{1-e^{-2t^2\bar{n}(1-k)}})$. For a m-photon Fock state, the transmitted state reads $\rho_T=\sum_{n=0}^{m} q(n,m,t)\,|n\rangle\,\langle n|$ with $q(n,m,t)=\binom{m}{n}t^{2n}r^{2(m-n)}$. Because it's diagonal in the number basis, the optimal measurement to discriminate between the modes can be seen as follows: First, measure the photon number and thus project in a Fock state; then distinguish between the two Fock states. Thus $P^{\rm Fock}_{\rm corr}(k,m,t)=\frac{1}{2}(1+\sum_{n=0}^{m} q(n,m,t)\sqrt{1-k^{2n}})$.

VI. CONCLUSION

In this paper, we have presented efficient methods to compute the ultimate limits for single-shot discrimination of optical modes. The methods, based on linear and SDP, apply to any set of modes with any prior distribution (we wrote the paper for the uniform prior not to introduce further notation, but the modifications are obvious). The bounds that are obtained can be used as fundamental benchmark for the performance of realistic devices or measurement schemes.

We pointed out the importance of stating whether the verifier has the possibility of defining a reference frame for the modes' phase. Depending on the family of modes that is considered, the difference in discrimination is found to be significant and, of course, some tasks like phase discrimination only make sense if the reference is available. Note that we assumed that the reference beam is classical and hence its phase relative to the receiver's reference frame could be determined with arbitrary precision. We leave the study of the channel-discrimination scenario with a weak reference beam as an open problem.

Let us finish by pointing out two related topics that we have not dealt with in the current work. First, throughout the paper, the characterization of the optical modes has been taken as known and perfect. It is known that this could be relaxed in some situations. Indeed, randomness of quantum origin can be certified from the measurement of uncharacterized optical modes, based only on an energy constraint $\bar{n}<0.5$ [33]. Second, we have considered single-shot discrimination. For the discrimination of unitaries, it is known that perfect discrimination is always possible if one has enough copies [34], and a similar result for energy-constrained discrimination has been described recently [35].

ACKNOWLEDGMENTS

We thank Chee Wei Soh for help in the first part of this project, and Konrad Banaszek, Alessandro Bisio, Michele Dall'Arno, Claude Fabre, Charles Lim, Norbert Lütkenhaus, Matteo Paris, and Stefano Pirandola for comments and suggestions. This research is supported by the National Research Foundation and the Ministry of Education, Singapore, under the Research Centres of Excellence program.

[1] C. Fabre and N. Treps, Modes and states in quantum optics, Rev. Mod. Phys. **92**, 035005 (2020).

[2] B. E. Saleh and M. C. Teich, *Fundamentals of Photonics* (John Wiley & Sons, Hoboken, 1991).

[3] R. Demkowicz-Dobrzanski, U. Dorner, B. J. Smith, J. S. Lundeen, W. Wasilewski, K. Banaszek, and I. A. Walmsley, Quantum phase estimation with lossy interferometers, Phys. Rev. A **80**, 013825 (2009).

[4] R. Nair, B. J. Yen, S. Guha, J. H. Shapiro, and S. Pirandola, Symmetric m-ary phase discrimination using quantum-optical probe states, Phys. Rev. A **86**, 022306 (2012).

[5] S. Pirandola, Quantum Reading of a Classical Digital Memory, Phys. Rev. Lett. **106**, 090504 (2011).

[6] R. Nair, Discriminating quantum-optical beam-splitter channels with number-diagonal signal states: Applications to quantum reading and target detection, Phys. Rev. A **84**, 032312 (2011).

[7] A. Bisio, M. Dall'Arno, and G. M. D'Ariano, Tradeoff between energy and error in the discrimination of quantum-optical devices, Phys. Rev. A **84**, 012310 (2011).

[8] M. Dall'Arno, A. Bisio, G. M. D'Ariano, M. Miková, M. Ježek, and M. Dušek, Experimental implementation of unambiguous quantum reading, Phys. Rev. A **85**, 012308 (2012).

[9] S. Pirandola, B. R. Bardhan, T. Gehring, C. Weedbrook, and S. Lloyd, Advances in photonic quantum sensing, Nat. Photonics **12**, 724 (2018).

[10] K. Mølmer, Optical coherence: A convenient fiction, Phys. Rev. A **55**, 3195 (1997).

[11] S. J. Van Enk and C. A. Fuchs, Quantum state of a propagating laser field, Quantum Inf. Comput. **2**, 151 (2002).

[12] H.-K. Lo and J. Preskill, Security of quantum key distribution using weak coherent states with nonrandom phases, Quantum Inf. Comput. **7**, 431 (2007).

[13] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, 10-12 December* (IEEE, Piscataway, NJ, 1984), pp. 175–179.

[14] K. Inoue, E. Waks, and Y. Yamamoto, Differential Phase Shift Quantum Key Distribution, Phys. Rev. Lett. **89**, 037902 (2002).

[15] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, Fast and simple one-way quantum key distribution, Appl. Phys. Lett. **87**, 194108 (2005).

[16] J. M. Arrazola and N. Lütkenhaus, Quantum fingerprinting with coherent states and a constant mean number of photons, Phys. Rev. A **89**, 062305 (2014).

[17] M. Jachura, M. Lipka, M. Jarzyna, and K. Banaszek, Quantum fingerprinting using two-photon interference, Opt. Express **25**, 27475 (2017).

[18] N. Lütkenhaus and M. Jahma, Quantum key distribution with realistic states: Photon-number statistics in the photon-number splitting attack, New J. Phys. **4**, 44 (2002).

[19] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. **81**, 1301 (2009).

[20] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Secure quantum key distribution with realistic devices, Rev. Mod. Phys. **92**, 025002 (2020).

[21] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, Advances in quantum cryptography, Adv. Opt. Photon. **12**, 1012 (2020).

[22] Y. Wang, I. W. Primaatmaja, E. Lavie, A. Varvitsiotis, and C. C. W. Lim, Characterising the correlations of prepare-and-measure quantum networks, npj Quantum Inf. **5**, 17 (2019).

[23] M. Ježek, J. Řeháček, and J. Fiurášek, Finding optimal strategies for minimum-error quantum-state discrimination, Phys. Rev. A **65**, 060301(R) (2002).

[24] J. Fiurášek and M. Ježek, Optimal discrimination of mixed quantum states involving inconclusive results, Phys. Rev. A **67**, 012321 (2003).

[25] M. Navascués, S. Pironio, and A. Acín, Bounding the Set of Quantum Correlations, Phys. Rev. Lett. **98**, 010401 (2007).

[26] M. Navascués, S. Pironio, and A. Acín, A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations, New J. Phys. **10**, 073013 (2008).

[27] S. P. Boyd and L. Vandenberghe, *Convex Optimization* (Cambridge University Press, New York, 2004).

[28] C. W. Helstrom, Quantum detection and estimation theory, J. Stat. Phys. **1**, 231 (1969).

[29] I. Ivanovic, How to differentiate between non-orthogonal states, Phys. Lett. A **123**, 257 (1987).

[30] D. Dieks, Overlap and distinguishability of quantum states, Phys. Lett. A **126**, 303 (1988).

[31] A. Peres, How to differentiate between non-orthogonal states, Phys. Lett. A **128**, 19 (1988).

[32] L. Sheridan and V. Scarani, Security proof for quantum key distribution using qudit systems, Phys. Rev. A **82**, 030301(R) (2010).

[33] T. Van Himbeeck, E. Woodhead, N. J. Cerf, R. García-Patrón, and S. Pironio, Semi-device-independent framework based on natural physical assumptions, Quantum **1**, 33 (2017).

[34] A. Acín, Statistical Distinguishability Between Unitary Operations, Phys. Rev. Lett. **87**, 177901 (2001).

[35] S. Becker, N. Datta, L. Lami, and C. Rouzé, Energy-constrained discrimination of unitaries, quantum speed limits and a gaussian Solovay-Kitaev theorem arXiv:2006.06659.