Extrema of discrete Wigner functions and applications

Andrea Casaccino,[1] Ernesto F. Galvão,[2] and Simone Severini[3]
[1]*Information Engineering Department, University of Siena, Via Roma 56, 53100 Siena, Italy*
[2]*Instituto de Física, Universidade Federal Fluminense, Av. Gal. Milton Tavares de Souza s/n Gragoatá, Niterói, RJ, 24210-340, Brazil*
[3]*Institute for Quantum Computing and Department of Combinatorics and Optimization, University of Waterloo, 200 University Avenue West, Waterloo, Canada N2L 3G1*
(Received 16 June 2008; published 7 August 2008)

We study the class of discrete Wigner functions proposed by Gibbons *et al.* [Phys. Rev. A **70**, 062101 (2004)] to describe quantum states using a discrete phase space based on finite fields. We find the extrema of such functions for small Hilbert-space dimensions and present a quantum-information application: a construction of quantum random-access codes. These are constructed using the complete set of phase-space point operators to find encoding states and to obtain the codes' average success rates for Hilbert-space dimensions 2, 3, 4, 5, 7, and 8.

DOI: 10.1103/PhysRevA.78.022310 PACS number(s): 03.67.Ac

I. INTRODUCTION

The Wigner function $W(q,p)$ was introduced by Wigner in 1932 [1] as a way to represent quantum states of one or more particles in phase space. It is a quasiprobability distribution, which means it retains some of the properties of a true probability distribution, while having some surprising properties due to quantum effects. For example, it can be negative in some regions in phase space.

There were many proposals of analogs of $W(q,p)$ to represent quantum systems with discrete degrees of freedom such as spins (see [2] and references therein for a review). These discrete Wigner functions have been applied to visualize quantum states and operations in the context of quantum information and computation [3–5].

In this paper we study properties and applications of the class of discrete Wigner functions defined by Gibbons *et al.* [2], which take values on a discrete phase space built with finite fields. We start in Secs. II and III by reviewing the definition of this class of functions. In Sec. IV we calculate the spectra of the phase-space point operators used to define the discrete Wigner functions. In Sec. V we describe how to use the calculated spectra to find the extremal values for the discrete Wigner function for some small Hilbert-space dimensions. We also describe how the phase-space point operators can be used in a quantum information application known as quantum random-access codes. In Sec. VI we introduce these codes with a simple example and present a quantum random-access code construction based on states that maximize the discrete Wigner function.

II. DEFINING A CLASS OF DISCRETE WIGNER FUNCTIONS

The discrete phase space is a $d\times d$ grid in which we identify some particular sets of d points called *lines*. *Parallel lines* are lines sharing no points in common. Following Gibbons *et al.* [2], a partition of the d^2 phase-space points into d parallel lines of d points each will be called a *striation*. The definition of lines and striations is done in such a way as to ensure, in this discrete geometry, some geometrical properties akin to the properties of lines in the usual geometry as follows.

(i) Given any two points, exactly one line contains both points.

(ii) Given a point α and a line λ not containing α, there is exactly one line parallel to λ that contains α.

(iii) Two nonparallel lines intersect at exactly one point.

Gibbons *et al.* described how to define $d(d+1)$ lines, partitioned into $d+1$ striations of d lines each, satisfying the requirements above. The construction is based on considering the discrete phase space as a two-dimensional vector space labeled by finite fields (for details, see [2]). In [6] Wootters discusses different geometrical problems associated with this construction.

To define a discrete Wigner function, we need to associate a projector onto a quantum state to each line in discrete phase space. These will be projectors onto a set of $d+1$ *mutually unbiased bases* (MUB). Consider two different orthonormal bases B_1 and B_2:

$$B_1=\{|v_{1,1}\rangle,|v_{1,2}\rangle,\ldots,|v_{1,d}\rangle\},|\langle v_{1,i}|v_{1,j}\rangle|^2=\delta_{i,j}, \quad (1)$$

$$B_2=\{|v_{2,1}\rangle,|v_{2,2}\rangle,\ldots,|v_{2,d}\rangle\},|\langle v_{2,i}|v_{2,j}\rangle|^2=\delta_{i,j}. \quad (2)$$

These two bases B_1 and B_2 are *mutually unbiased* if

$$|\langle v_{i,j}|v_{k,l}\rangle|^2=\frac{1}{d} \quad \text{if } i\neq k. \quad (3)$$

Wootters and Fields showed that one can define $d+1$ such mutually unbiased bases for power-of-prime dimension d [7]. Mutually unbiased bases have been studied because of their use in a number of quantum-information applications—for example, quantum cryptography [8] and quantum-state and -process tomography [9]—and in the construction of quantum t designs [10], used to estimate averages of functions over quantum states.

To define a discrete Wigner function (DWF) we pick a one-to-one map between the lines in discrete phase space and the projectors onto a complete set of MUB in the following way: (a) each basis set B_i is associated with one striation S_i

and (b) each basis vector projector $Q_{i,j} \equiv |v_{i,j}\rangle\langle v_{i,j}|$ is associated with a line $\lambda_{i,j}$ (the jth line of the ith striation).

These maps define uniquely the values of the DWF W_β for all points β if we impose the following constraints:

$$\mathrm{Tr}(Q_{i,j}\rho) = \sum_{\alpha \in \lambda_{i,j}} W_\alpha, \tag{4}$$

where ρ is the system's density matrix and the sum is over phase-space points α in the line λ associated with projector $Q_{i,j}$. These requirements amount to demanding that the sum of the Wigner function over each line must be equal to the probability of projecting onto the basis vector associated with that line.

Note that there are multiple ways of making these associations. In general, this will lead to different definitions of the DWF using the same fixed set of MUB. The procedure outlined above then leads not to a single definition of W, but to a class of Wigner functions instead.

We now define the *phase-space point operator* A_β associated with phase-space point β:

$$A_\beta \equiv \sum_{\lambda \supset \beta} Q_\lambda - I, \tag{5}$$

where the sum is over projectors Q_λ associated with lines λ containing point β and I represents identity. The operators A_β appear naturally when we invert Eq. (4) to write an expression for W_β in terms of the MUB projectors:

$$W_\beta = \frac{1}{d}\mathrm{Tr}(\rho A_\beta), \tag{6}$$

We see that the expectation value of A_β (multiplied by $1/d$) gives the value of the DWF at the phase-space point β.

The A operators form a complete basis in the space of $d \times d$ matrices. It can be shown that the DWF value at point α is simply the expansion coefficient of ρ corresponding to the A_α operator:

$$\rho = \sum_\alpha W_\alpha A_\alpha. \tag{7}$$

The multiple ways of associating projectors with lines in phase space result in multiple definitions for A_α. While a single definition of W requires d^2 operators A_α (one for each phase-space point), the full set of A_α one can define with the same fixed complete set of MUB has d^{d+1} elements. In Sec. VI we will make use of the full set of phase-space point operators to obtain a construction for a quantum-information application known as quantum random-access codes.

Negativity and nonclassicality

Cormick *et al.* [11] have characterized the set of states which have non-negative Wigner functions. These states turn out to have some interesting properties, which we will review here, as they motivate the work reported in the remainder of this paper.

For a d-dimensional quantum system, one can find complete sets of $d+1$ mutually unbiased bases using the finite-field construction introduced in Ref. [2]. This construction is only valid for power-of-prime d, since this is the necessary condition for a finite field to exist. One can then define the set C_d of d-dimensional states which have non-negative DWF in all definitions—that is, whose expectation values for *all* phase-space point operators are non-negative.

In [11] it was shown that the only pure states in C_d are the MUB projectors, which can always be chosen to be *stabilizer states*. The stabilizer formalism [12] provides a way to represent pure states in C_d using a number of bits which is polynomial in the number of qubits. Since general pure states require a description which is of exponential size, the set C_d is classical in the sense of having a short description.

For systems of prime dimensions, the two notions of classicality exactly coincide: the only pure states with non-negative DWF are exactly the stabilizer states. In this context, negativity of any DWF (as witnessed by negativity of one of the A_α operators) indicates nonclassicality in the sense of the absence of an efficient description using the stabilizer formalism. These results motivated us to investigate the extrema of the discrete Wigner functions.

Before proceeding, we need to review some constructions of complete sets of MUB for d-dimensional systems, as these are necessary to define DWF using Eqs. (5) and (6).

III. COMPLETE SETS OF MUTUALLY UNBIASED BASES

For prime dimension d there is a canonical construction of a complete set of $d+1$ MUB first proposed by Ivanovic [13]. To review this construction, let $|v_{r,k}\rangle_j$ denote the jth component of the kth vector in the rth basis, $r=0,1,\ldots,d$. The vectors in the complete set of $d+1$ MUB are then

$$|v_{0,k}\rangle_j = \delta_{jk}, \tag{8}$$

$$|v_{1,k}\rangle_j = \frac{1}{\sqrt{d}} e^{(2\pi i/d)(j^2+jk)}, \tag{9}$$

$$\vdots \tag{10}$$

$$|v_{r,k}\rangle_j = \frac{1}{\sqrt{d}} e^{(2\pi i/d)(rj^2+jk)}, \tag{11}$$

$$\vdots \tag{12}$$

$$|v_{(d-1),k}\rangle_j = \frac{1}{\sqrt{d}} e^{(2\pi i/d)[(d-1)j^2+jk]}, \tag{13}$$

$$|v_{d,k}\rangle_j = \frac{1}{\sqrt{d}} e^{(2\pi i/d)jk}. \tag{14}$$

When the Hilbert-space dimension is a prime power, there are different constructions of complete sets of MUB. Let us now review a simple construction of a complete set of MUB for n qubits (Hilbert-space dimension $d=2^n$) consisting solely of stabilizer states [14]. We start by considering the 4^n Pauli operators for n qubits, which are the tensor products of single-qubit Pauli operators X, Y, Z and identity. From this

TABLE I. Set of five MUB for two qubits.

1	XX	$X1$	$1X$
2	ZZ	$Z1$	$1Z$
3	YY	$Y1$	$1Y$
4	XY	YZ	ZX
5	XZ	YX	ZY

set, remove the identity operator. The remaining 4^n-1 Pauli operators can be partitioned into 2^n+1 sets, each containing 2^n-1 mutually commuting Pauli operators. It was proven in [14] that the common eigenstates of the operators in each such set form a basis and, moreover, that the 2^n+1 bases thus defined are mutually unbiased.

We will now provide two examples of this construction, which will be useful to us later on. The first example is a set of five MUB for two qubits, each basis being formed by the common eigenstates of each row of operators in Table I. In the table, operator XY, for example, stands for the tensor product of X on the first qubit by Y on the second.

The second example is a set of nine MUB for three qubits, comprising the common eigenstates of the operators in each row of Table II.

IV. SPECTRA OF PHASE-SPACE POINT OPERATORS

As we have seen in the previous sections, the DWF is defined by Eq. (6) using the phase-space point operators A. In this section we calculate the spectra of A for the constructions of complete sets of MUB we reviewed in Sec. III. The spectra we tabulate in Table III agree with the spectra calculated independently by Appleby *et al.* [15] for Hilbert-space dimensions $d=3$, 4, 5, and 7. In Table III we also report the number of phase-space point operators with each spectrum, information which will be necessary for the quantum-information application described in Sec. VI.

We have calculated the full spectra of all d^{d+1} phase-space point operators for $d=2$, 3, 4, 5, 7, and 8, but the latter two cases have too many different spectra for us to reproduce here. We would like to point out only one piece of information about these cases: the extremal eigenvalues found over all the A_α. For $d=7$ the largest eigenvalue is $\lambda_{max}=2.4178$ and the smallest is $\lambda_{min}=-1$, whereas for $d=8$ the largest is $\lambda_{max}=2.5490$ and the smallest is $\lambda_{min}=-0.9979$.

TABLE III. Spectra of phase-space point operators.

d	Number	Spectrum
2	8	$\{[(1/2+\sqrt{3}/2),(1/2-\sqrt{3}/2)]\}$
3	9	$\{-1,1,1\}$
	72	$\{[0,(1/2+\sqrt{5}/2),(1/2-\sqrt{5}/2)]\}$
4	320	$\{-0.50000,-0.50000,0.13397,1.86603\}$
	320	$\{-0.86603,-0.50000,0.86603,1.50000\}$
	384	$\{-0.89680,-0.14204,0.27877,1.76007\}$
5	1000	$\{-0.70281,-0.61803,-0.13294,0.48666,1.96712\}$
	2000	$\{-0.79859,-0.36221,0.00000,0.10661,2.05419\}$
	2000	$\{-0.83607,-0.81000,0.00000,1.05469,1.59139\}$
	3000	$\{-0.83726,-0.58152,-0.09576,0.62870,1.88584\}$
	1000	$\{-0.90039,-0.64018,-0.14531,1.06785,1.61803\}$
	3000	$\{-0.90932,-0.48701,0.00000,0.46853,1.92780\}$
	3000	$\{-0.94658,-0.51690,-0.18438,0.93842,1.70944\}$
	600	$\{-1.00000,-0.61803,0.00000,1.00000,1.61803\}$
	25	$\{-1.00000,-1.00000,1.00000,1.00000,1.00000\}$

For the case of two qubits ($d=4$) we calculated the spectra for all six different stabilizer MUB constructions of the kind described in [14], and the spectra found are identical to those of the MUB set in Table I. We have also established that for three qubits ($d=8$), one can find 960 different stabilizer constructions of this kind. Testing a few of those we found exactly the same spectra as for the example in Table II. Based on this, we conjecture that the phase-space point operator spectra is independent of which MUB set construction one uses.

V. EXTREMA OF DISCRETE WIGNER FUNCTIONS

Unlike probability distributions, we have seen that the discrete Wigner function can assume negative values. What are the extremal values that it can attain? Wootters conjectured that the minimal value min(W) that the discrete Wigner function could assume would be $-1/d$ for odd-prime Hilbert-space dimension d [16]. He also showed that min (W)$=-0.183$ for $d=2$ [17] and, together with Sussman [18], found a maximum value of max(W)$=0.319$ for some particular definitions of discrete Wigner functions for $d=8$. In this section we describe a general method for finding the extrema

TABLE II. Set of nine MUB for three qubits.

1	XXX	$XX1$	$X1X$	$X11$	$1XX$	$1X1$	$11X$
2	XXY	XYX	YXX	YYY	$ZZ1$	$Z1Z$	$1ZZ$
3	XXZ	XYY	$YZ1$	$Y1X$	ZXY	ZYZ	$1ZX$
4	XYZ	XZX	$YX1$	$Y1Y$	ZYX	ZZZ	$1XY$
5	$XY1$	$X1Z$	YXY	YZX	ZXX	ZZY	$1YZ$
6	XZY	$X1Y$	YZZ	$Y1Z$	ZZX	$Z1X$	$1Z1$
7	XZZ	$XZ1$	YYZ	$XY1$	ZXZ	$ZX1$	$11Z$
8	YXZ	YYX	YZY	$Y11$	$1XZ$	$1YX$	$1ZY$
9	ZYY	$ZY1$	$Z1Y$	$Z11$	$1YY$	$1Y1$	$11Y$

among all discrete Wigner functions definable with a fixed complete set of MUB and use it to explicitly calculate the extrema for $d=2$, 3, 4, 5, 7, and 8.

Recall that the phase-space point operator A_α associated with the phase-space point α is given as the sum over MUB projectors associated with all phase-space lines that contain α:

$$A_\alpha = \sum_{\lambda \supset \alpha} Q_\lambda - I, \quad (15)$$

where the sum is over projectors associated with lines λ containing point α and I represents identity.

Given a phase-space point operator A_α, we want to find the minimum of its expectation value:

$$\min\langle A_\alpha \rangle = \min\left[\mathrm{Tr}\left(\sum_{\lambda \supset \alpha} Q_\lambda |\psi\rangle\langle\psi| \right) \right] - 1. \quad (16)$$

The minimum results when $|\psi\rangle$ is the eigenvector associated with the smallest eigenvalue λ_{min} of A_α (see the Appendix for a proof). We can evaluate the spectrum of A_α to find its smallest eigenvalue λ^α_{min}. Then, using Eq. (6), the most negative value for the discrete WF at point α will be given by

$$\min(W_\alpha) = \frac{1}{d}\min\langle A_\alpha \rangle = \frac{1}{d}\lambda^\alpha_{min}. \quad (17)$$

To find the most negative value for the function, one needs to find all eigenvalues of all possible phase-space point operators. For a d-dimensional system there are d^{d+1} different phase-space point operators, only d^2 of which appear in any single definition of a DWF. Minimizing over α, we can use Eq. (17) to obtain the smallest value that the function can attain.

The same reasoning can be used to obtain the maxima of the DWF, using the largest eigenvalue of any of the A_α. Using the spectra tabulated in Sec. IV we obtained the extremal values of the DWF for small dimensions d, listed in Table IV. The results support Wootters' conjecture for odd-prime d.

TABLE IV. Extremal values for the DWF.

d	W_{max}	W_{min}
2	$(1/4)(1+\sqrt{3}) \simeq 0.683$	$(1/4)(1-\sqrt{3}) \simeq -0.183$
3	$(1/6)(1+\sqrt{5}) \simeq 0.539$	$-(1/3)$
4	0.4665	−0.2242
5	0.411	$-(1/5)$
7	0.3454	$-(1/7)$
8	0.3186	−0.1247

VI. APPLICATION: QUANTUM RANDOM-ACCESS CODES

In this section we review the quantum-information protocol known as quantum random-access codes and present a code construction that relies on states maximizing the discrete Wigner function. Let us start by recalling what these codes are using a simple example.

Imagine a situation in which Alice encodes m classical bits into n bits ($m > n$), which she sends to Bob, who will need to know that value of a *single* bit (out of the m possible ones) with a probability of at least p. We may represent such an encoding-decoding scheme by the notation $m \to n$.

Prior to sending the n-bit message, however, Alice does not know which of the m bits Bob will need to read out. To maximize the least probability of success, p, Alice and Bob need to agree on the use of a particular, efficient $m \to n$ encoding.

We can consider the quantum generalization of this situation, in which Alice can send Bob n qubits of communication, instead of n bits. The idea behind these so-called *quantum random-access codes* (QRACs) is very old by quantum-information standards; it appeared in a paper written circa 1970 and published in 1983 by Wiesner [19].

These codes were rediscovered in [20], where the explicit comparison with classical codes was made.

A. Example: 3→1 QRAC with a qubit

Let us illustrate the idea with a $3 \to 1$ QRAC that encodes three bits into a single qubit. This QRAC was attributed to Chuang in Ref. [20].

Instead of concerning ourselves with the least decoding probability of success p, we will use as a figure of merit the average probability of success, p_q. With three bits, Alice has $2^3=8$ possible bit strings $b_0 b_1 b_2$. For each possibility she will prepare one particular state from the set depicted in Fig. 1. These states lie on the vertices of a cube inscribed within the Bloch sphere, which is the representation of one-qubit pure states using spherical-coordinate angles θ and ϕ:

$$|\psi(\theta,\phi)\rangle = \cos(\theta/2)|0\rangle + \exp(i\phi)\sin(\theta/2)|1\rangle. \quad (18)$$

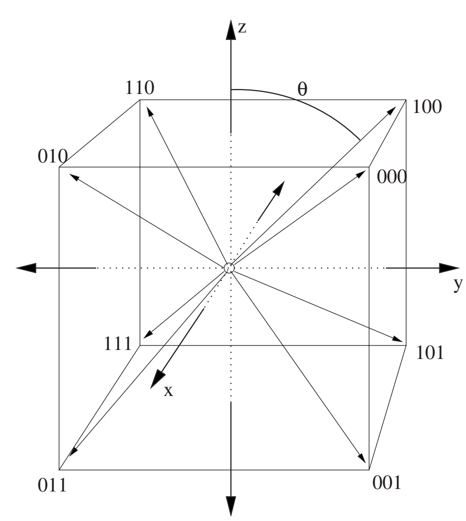

FIG. 1. Encoding states for the $3 \to 1$ QRAC using a single qubit. Alice prepares one out of eight states on the vertices of a cube inscribed within the Bloch sphere, depending on her three-bit string. The angle θ is such that $\cos^2(\theta/2) = 1/2 + \sqrt{(3)}/6 \simeq 0.79$, which is the probability of Bob correctly decoding a single bit out of the three.

If Bob wants to read out bit b_0, he measures along the x axis and associates a positive result with $b_0=0$. To read bits b_1 (b_2) he measures along the y axis (z axis) and again associates a positive result with $b_1=0$ ($b_2=0$). It is easy to see that Bob's average probability of success is given by $p_q=\cos^2(\theta/2)=1/2+\sqrt{(3)}/6\simeq 0.79$, where the angle θ is given in the caption to Fig. 1. The optimal classical $3\rightarrow 1$ random-access code succeeds only with average probability $p_c=0.75$, as can be checked easily through a search over all deterministic protocols.

Note that the QRAC just presented uses decoding measurements which are projections onto the canonical set of MUB for a qubit—that is, the X, Y, and Z bases. The encoding states are found by optimizing the probability of correctly decoding each coding state.

B. QRAC construction from A_α

The full set of d^{d+1} phase-space point operators A_α can be used to build a particularly symmetric set of quantum random-access codes. The encoding states will be those maximizing each $\langle A_\alpha\rangle$. Our results from Sec. V showed that those are the largest-eigenvalue eigenstates of each A_α.

Our goal is to construct a QRAC that encodes $d+1$ messages with d possible values each using a single quantum d-level system that will be sent by Alice and measured by Bob. As in the case with qubits, our strategy will be for Bob to decode by performing projective measurements onto one out of the $d+1$ MUB that exist for this d-dimensional system (for power-of-prime d). Alice has to find d^{d+1} different encoding states, each of which will decode correctly with the highest possible probability.

As we have shown in Sec. V, the pure quantum state $|\psi_\alpha\rangle$ that maximizes $\langle A_\alpha\rangle$ is the eigenvector with largest eigenvalue λ^α_{max} of $\langle A_\alpha\rangle$. Bob's decoding procedure involves measuring the encoding state $|\psi_\alpha\rangle$ onto one of the $d+1$ MUB. His average probability of successfully decoding will be the average $\frac{1}{d+1}\Sigma_{\lambda\supset\alpha}\langle Q_\lambda\rangle$. To maximize this decoding probability for encoding state $|\psi_\alpha\rangle$, we need to maximize

$$\max\left(\frac{1}{d+1}\sum_{\lambda\supset\alpha}\langle Q_\lambda\rangle\right)=\frac{1}{d+1}\max(\langle A_\alpha\rangle+1) \tag{19}$$

$$=\frac{1}{d+1}(\lambda^\alpha_{max}+1). \tag{20}$$

The average performance of this QRAC protocol can be found by averaging the probability of success of the d^{d+1} encoding states, each corresponding to one phase-space point operator A_α:

$$p_q=\frac{1}{d^{d+1}}\frac{1}{d+1}\sum_\alpha(\lambda^\alpha_{max}+1). \tag{21}$$

We see that the protocol's average success rate p_q depends on the value of the sum of the largest eigenvalues of each of the d^{d+1} possible phase-space point operators A_α.

Using the MUB constructions described in Sec. III and the point operator spectra calculated in Sec. IV, we were able to compute p_q for a $(d+1)\rightarrow d$ QRAC using systems of dimension $d=2$, 3, 4, 5, 7, and 8. The results are summarized in Table V. The construction recovers the known success rate of the $3\rightarrow 1$ QRAC with a qubit.

TABLE V. QRAC success rate p_q.

Dimension	p_q
$d=2$	$(1/6)(3+\sqrt{3})\simeq 0.789$
$d=3$	$(7/18)+(\sqrt{5}/2)\simeq 0.637$
$d=4$	0.5424
$d=5$	0.4700
$d=7$	0.3720
$d=8$	0.3372

It is clear that this construction can be extended to higher-dimensional systems, provided a DWF can be defined for them. This will be the case for power-of-prime dimensions d using, for example, the finite-field construction given in Ref. [2].

It would be interesting to investigate how these protocols fare against the optimal classical protocols. This would require evaluating the optimal probability of success for a $(d+1)\rightarrow d$ d-level classical random-access code, something that to our knowledge has not been done for $d>2$. In [20] some asymptotic results were obtained for large d, indicating that while there may be an advantage of quantum over classical for small dimensions d, this advantage practically disappears in the asymptotic regime.

VII. CONCLUSION

We have reviewed the definition of discrete Wigner functions given in [2] used to describe quantum systems in a discrete phase space. We calculated the spectra of phase-space point operators for small dimensions and used them to obtain the extrema of the discrete Wigner function for systems in Hilbert-space dimensions $d=2$, 3, 4, 5, 7, and 8. We then described the protocol known as quantum random-access codes and used the phase-space point operators to find encoding states and to obtain the efficiency of a QRAC construction whose encoding states maximize the discrete Wigner function at each phase-space point.

ACKNOWLEDGMENTS

The authors are grateful to Ilaria Cardinali and Enrico Martinelli for helpful discussions. E.F.G. acknowledges support from Brazilian funding agencies FAPERJ and CNPq. S.S. acknowledges financial support from DTO-ARO, ORDCF, Ontario-MRI, CFI, CIFAR, and MITACS.

APPENDIX

Let ρ be a density matrix, hence positive semidefinite, Hermitian, and with unit trace. Let $|\psi\rangle$ be a pure state. In this appendix we prove that the extrema of

$$\langle\phi|\rho|\phi\rangle \tag{A1}$$

are obtained when $|\phi\rangle$ is an eigenstate corresponding to extremal eigenvalues of ρ.

We start by showing that the state that maximizes this expression is the eigenstate $|\lambda_{max}\rangle$ corresponding to the largest eigenvalue λ_{max} of ρ. It is easy to evaluate Eq. (A1) for $|\phi\rangle=|\lambda_{max}\rangle$:

$$\langle\lambda_{max}|\rho|\lambda_{max}\rangle = \lambda_{max}\langle\lambda_{max}|\lambda_{max}\rangle = \lambda_{max}. \tag{A2}$$

Let us now consider the expansion of a general state $|\phi\rangle = \Sigma_i d_i|i\rangle$ in the basis that diagonalizes ρ. For $|\phi\rangle$, the expression we are trying to maximize takes the value

$$\langle\phi|\rho|\phi\rangle = \sum_i \lambda_i|d_i|^2 = \lambda_{max}(1-\Delta) + \sum_{j\neq\lambda_{max}} \lambda_i|d_i|^2, \tag{A3}$$

where λ_i are the eigenvalues of ρ. We have rewritten the sum to single out the term corresponding to λ_{max} and defined $\Delta > 0$ such that $(1-\Delta)=|d_{max}|^2$. Now, because all $\lambda_i \leqslant \lambda_{max}$ (by definition of λ_{max}), we have

$$\langle\phi|\rho|\phi\rangle = \lambda_{max}(1-\Delta) + \sum_{j\neq\lambda_{max}} \lambda_i|d_i|^2 \leqslant \lambda_{max}. \tag{A4}$$

So we have proven that any set of coefficients different from those of $|\lambda_{max}\rangle$ leads to a smaller expectation value for ρ, and so $|\lambda_{max}\rangle$ maximizes this expectation value. A similar argument can be made to prove that the state that minimizes $\langle\phi|\rho|\phi\rangle$ is the eigenstate corresponding to the smallest eigenvalue of ρ.

The claim following Eq. (16) is justified by applying the result above to $\rho=\frac{1}{d+1}\Sigma_{\lambda\supset\alpha}Q_\lambda$.

[1] E. P. Wigner, Phys. Rev. **40**, 749 (1932).

[2] K. S. Gibbons, M. J. Hoffman, and W. K. Wootters, Phys. Rev. A **70**, 062101 (2004).

[3] P. Bianucci, C. Miquel, J. P. Paz, and M. Saraceno, Phys. Lett. A **297**, 353 (2002).

[4] C. Miquel, J. P. Paz, and M. Saraceno, Phys. Rev. A **65**, 062309 (2002).

[5] J. P. Paz, A. J. Roncaglia, and M. Saraceno, Phys. Rev. A **72**, 012309 (2005).

[6] W. K. Wootters, e-print arXiv:quant-ph/0406032.

[7] W. K. Wootters and B. D. Fields, Ann. Phys. (N.Y.) **191**, 363 (1989).

[8] H. Bechmann-Pasquinucci and W. Tittel, Phys. Rev. A **61**, 062308 (2000).

[9] A. Bendersky, F. Pastawski, and J. P. Paz, Phys. Rev. Lett. **100**, 190403 (2008).

[10] A. Klappenecker and M. Rötteler, in *Proceedings of the 2005 IEEE International Symposium on Information Theory, Adelaide, Australia, 2005*, edited by A. Grant and R. A. Kennedy (IEEE, New York, 2005), pp. 1740–1744.

[11] C. Cormick, E. F. Galvão, D. Gottesman, J. P. Paz, and A. O. Pittenger, Phys. Rev. A **73**, 012301 (2006).

[12] Daniel Gottesman, Ph.D. thesis, California Institute of Technology, 1997.

[13] I. D. Ivanovic, J. Phys. A **14**, 3241 (1981).

[14] J. Lawrence, C. Brukner, and A. Zeilinger, Phys. Rev. A **65**, 032320 (2002).

[15] D. M. Appleby, I. Bengtsson, and S. Chaturvedi, e-print arXiv:0710.3013.

[16] W. K. Wootters, (private communication).

[17] W. K. Wootters, IBM J. Res. Dev. **48**, 99 (2004).

[18] W. K. Wootters and D. M. Sussman, e-print arXiv:0704.1277.

[19] S. Wiesner, SIGACT News **15**, 78 (1983).

[20] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani, J. ACM **49**, 1 (2002).