# Discrete Wigner functions and quantum computational speedup

Ernesto F. Galvão
*Perimeter Institute for Theoretical Physics, 31 Caroline Street North, Waterloo, Ontario, N2L 2Y5, Canada*
(Received 17 June 2004; published 1 April 2005)

Gibbons *et al.* [Phys. Rev. A **70**, 062101 (2004)] have recently defined a class of discrete Wigner functions $W$ to represent quantum states in a finite Hilbert space dimension $d$. I characterize the set $C_d$ of states having non-negative $W$ simultaneously in all definitions of $W$ in this class. For $d \leqslant 5$ I show $C_d$ is the convex hull of stabilizer states. This supports the conjecture that negativity of $W$ is necessary for exponential speedup in pure-state quantum computation.

DOI: 10.1103/PhysRevA.71.042302 PACS number(s): 03.67.Lx, 03.67.Hk, 03.65.Ca

## I. INTRODUCTION

Continuous-variable quantum systems can be represented in phase space using various quasiprobability distributions, notably the Wigner function $W(q,p)$ [1,2]. This real-valued function plays some of the roles of the classical Liouville density, for example, allowing us to calculate some system properties through phase-space integrals weighted by $W(q,p)$. Despite these similarities, $W(q_0,p_0)$ cannot be interpreted as the probability of simultaneously measuring observables $\hat{p}$ and $\hat{q}$ with eigenvalues $p_0$ and $q_0$: such dispersion-free values for noncommuting observables are not allowed in quantum mechanics. In fact, $W(q,p)$ can even be *negative* in some phase-space regions, something that obviously could not happen were $W(q,p)$ a true probability distribution (hence the term "quasiprobability").

The connection between negativity of $W(q,p)$ and nonclassicality has not been completely fleshed out, partly due to different subjective views on what qualifies as "nonclassical behavior" (see Refs. [3,4]). Negativity of $W(q,p)$ has been linked to nonlocality [5], but the relation is not straightforward. For example, the original Einstein-Podolsky-Rosen state can display nonlocality despite having positive $W(q,p)$ in all phase space [6–8].

Buot [9] and Hannay and Berry [10] seem to have been among the first to propose analogs of the Wigner function for finite-dimensional Hilbert spaces. Their finds were rediscovered later by Cohen and Scully [11] and Feynman [12], who defined a discrete Wigner function $W$ for the case of a single qubit. This work was developed by Wootters [13] and Galetti and de Toledo Piza [14], who introduced a Wigner function for prime-dimensional Hilbert spaces. There followed other definitions valid for dimension $d$ which is odd [15], even [16], power-of-prime [17,18], or arbitrary [19–21]. These have been recently used to visualize and get insights on teleportation [22,23], quantum algorithms [20,21], and decoherence [24]. A recent review of phase-space methods for finite-dimensional systems is given in Ref. [25].

In this paper I investigate the relation between negativity of discrete Wigner functions and quantum computational speedup. I will focus on the class of Wigner functions defined by Wootters [17] and Gibbons *et al.* [18] for power-of-prime dimensions. Wigner functions in this class are defined by associating lines in a discrete phase space to projectors belonging to a fixed set of mutually unbiased bases. We will see that the set of states displaying negativity of $W$ depends on a number of arbitrary choices required to pick a particular definition of $W$ from the class. I eliminate this arbitrariness by characterizing the set $C_d$ of states having non-negative $W$ simultaneously in *all* definitions in the class, for $d$-dimensional Hilbert space.

For a single qubit, I show that the set $C_2$ consists of states which fail to provide quantum computational advantage in a model recently proposed by Bravyi and Kitaev [26]. For dimensions $2 \leqslant d \leqslant 5$, I show that the set $C_d$ is the convex hull of a set of *stabilizer* states, i.e., simultaneous eigenstates of generalized Pauli operators [27,28]. This is interesting, as quantum computation which is restricted to stabilizer states and gates from the Clifford group can be simulated efficiently on a classical computer [29]. If the result holds for arbitrary power-of-prime dimensions (as I conjecture), then pure states in $C_d$ would be "classical" in the sense of having an efficient description using the stabilizer formalism. This suggests that states with negative $W$ may be *necessary* for exponential quantum computational speedup with pure states.

## II. DISCRETE WIGNER FUNCTIONS

In this section we review the discrete Wigner functions introduced by Wootters [13] and Galetti and de Toledo Piza [14] for prime dimensions, and elaborated on recently by Wootters [17] and Gibbons, Hoffman, and Wootters [18] for prime-power dimensions. We start by defining discrete analogs of phase space and its partitions into parallel "lines" (i.e., striations). Then we review how to define a class of discrete Wigner functions $W$ by associating lines with projectors onto basis vectors from a set of mutually unbiased bases (MUB's).

### A. Phase space and striations

The discrete analogue of phase space in a $d$-dimensional Hilbert space is a $d \times d$ real array. Unlike the continuous phase space, in this discrete setting we do not have geometrical lines of points. Instead, a "line" is defined as a set of $d$ points in discrete phase space.

 

It is clear that our discrete phase space can then be partitioned in multiple ways into collections of parallel lines (i.e., disjoint sets of $d$ phase-space points). Following Wootters [17], we call each such partition a striation.

In Ref. [18] a procedure for building $(d+1)$ striations of a $d\times d$ phase-space array was outlined, resulting in striations with the following three useful properties: (i) given any two points, exactly one line contains both points, (ii) given a point $\alpha$ and a line $\lambda$ not containing $\alpha$, there is exactly one line parallel to $\lambda$ that contains $\alpha$, and (iii) two nonparallel lines intersect at exactly one point. The construction of these $(d+1)$ special striations involves labeling the discrete phase space with elements of finite fields, and defining lines using natural properties of the field (for details, see Ref. [18]). These striations play a central role in the definition of the discrete Wigner function $W$, as we will see below.

### B. Mutually unbiased bases

Wootters' definition of discrete Wigner functions makes use of a special set of $d+1$ bases for a $d$-dimensional Hilbert space. Consider two different orthonormal bases $B_1$ and $B_2$:

$$B_1 = \{|\alpha_{1,1}\rangle, |\alpha_{1,2}\rangle, \ldots, |\alpha_{1,d}\rangle\}, |\langle\alpha_{1,i}|\alpha_{1,j}\rangle|^2 = \delta_{i,j}, \tag{1}$$

$$B_2 = \{|\alpha_{2,1}\rangle, |\alpha_{2,2}\rangle, \ldots, |\alpha_{2,d}\rangle\}, |\langle\alpha_{2,i}|\alpha_{2,j}\rangle|^2 = \delta_{i,j}. \tag{2}$$

These two bases $B_1$ and $B_2$ are said to be mutually unbiased or mutually conjugate if

$$|\langle\alpha_{i,j}|\alpha_{k,l}\rangle|^2 = \frac{1}{d} \text{ if } i \neq k. \tag{3}$$

Wootters and Fields showed that one can define $(d+1)$ such mutually unbiased bases (MUB's) for power-of-prime dimension $d$ [30]. Note that this is exactly the number of striations one can find with properties (i)–(iii) above; we will use this now to define a class of discrete Wigner functions $W$.

### C. Defining a class of discrete Wigner functions

We now have the ingredients to define a class of discrete Wigner functions: a set of $(d+1)$ mutually unbiased bases $\{B_1, B_2, \ldots, B_{d+1}\}$; and a set of $(d+1)$ striations $\{S_1, S_2, \ldots, S_{d+1}\}$ of our $d\times d$ phase space into $d$ parallel lines (i.e., disjoint sets) of $d$ points each. To define a discrete Wigner function we need to choose two one-to-one maps: each basis set $B_i$ is associated with one striation $S_i$ and each basis vector $|\alpha_{i,j}\rangle$ is associated with a line $\lambda_{i,j}$ (the $j$th line of the $i$th striation). With these associations, the Wigner function $W$ is uniquely defined if we demand that

$$\mathrm{Tr}(|\alpha_{i,j}\rangle\langle\alpha_{i,j}|\hat{\rho}) = \sum_{\alpha\in\lambda_{i,j}} W_\alpha, \tag{4}$$

i.e., we want the sum of the Wigner function elements corresponding to each line to equal 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 $W$ using the same fixed set of MUB's. The procedure outlined above then leads not to a single definition of $W$, but to a class of Wigner functions instead.

## III. WIGNER FUNCTION FOR A QUBIT

Let us illustrate Wootters' definition of a discrete Wigner function with the simplest case, a qubit. The discrete Wigner function $W$ is defined on a $2\times 2$ array:

$$W = \begin{array}{|c|c|}\hline W_{1,1} & W_{1,2} \\ \hline W_{2,1} & W_{2,2} \\ \hline \end{array} \tag{5}$$

There are three striations of this phase space with properties (i), (ii), (iii) as required. Below I list them, using numbers $j=1,2$ to arbitrarily label the two lines $\lambda_{i,j}$ in each striation $S_i$:

$$S_1: \begin{array}{|c|c|}\hline 1 & 1 \\ \hline 2 & 2 \\ \hline \end{array}, \quad S_2: \begin{array}{|c|c|}\hline 1 & 2 \\ \hline 1 & 2 \\ \hline \end{array}, \quad S_3: \begin{array}{|c|c|}\hline 1 & 2 \\ \hline 2 & 1 \\ \hline \end{array}. \tag{6}$$

Now we need to define a set of three mutually unbiased bases for a qubit. These can be conveniently chosen as the eigenstates of the three Pauli operators $\hat{\sigma}_x$, $\hat{\sigma}_y$, and $\hat{\sigma}_z$. Let us label these basis vectors $|\alpha_{i,j}\rangle$, where $i\in\{1,2,3\}$ indexes the MUB ($i=1,2,3$, respectively, for the operators $\hat{\sigma}_x$, $\hat{\sigma}_y$, $\hat{\sigma}_z$), and $j\in\{1,2\}$ indexes the basis vector in each MUB ($j=1,2$ indicates eigenstates with eigenvalues respectively equal to $+1$, $-1$).

We can now define $W$ by imposing condition (4), i.e., we want the sum of $W_{i,j}$ in each line $\lambda$ to be the probability $p_{i,j}$ of projecting the state onto the basis vector $|\alpha_{i,j}\rangle$:

$$p_{i,j} \equiv \mathrm{Tr}(|\alpha_{i,j}\rangle\langle\alpha_{i,j}|\hat{\rho}) = \sum_{\alpha\in\lambda_{i,j}} W_\alpha. \tag{7}$$

Using the three striations we defined, these conditions can be explicitly stated in terms of the probabilities $p_{i,j}$:

$$W_{1,1} + W_{1,2} = p_{1,1}, \tag{8}$$

$$W_{2,1} + W_{2,2} = p_{1,2}, \tag{9}$$

$$W_{1,1} + W_{2,1} = p_{2,1}, \tag{10}$$

$$W_{1,2} + W_{2,2} = p_{2,2}, \tag{11}$$

$$W_{1,1} + W_{2,2} = p_{3,1}, \tag{12}$$

$$W_{1,2} + W_{2,1} = p_{3,2}. \tag{13}$$

The equations above define uniquely the Wigner function $W$ in terms of the probabilities $p_{i,j}$:

$$W_{1,1} = \frac{1}{2}(p_{1,1} + p_{2,1} + p_{3,1} - 1), \tag{14}$$

$$W_{1,2} = \frac{1}{2}(p_{1,1} + p_{2,2} + p_{3,2} - 1), \tag{15}$$

$$W_{2,1} = \frac{1}{2}(p_{1,2} + p_{2,1} + p_{3,2} - 1), \tag{16}$$

$$W_{2,2} = \frac{1}{2}(p_{1,2} + p_{2,2} + p_{3,1} - 1). \quad (17)$$

Here we should keep in mind that not all probabilities $p_{i,j}$ are independent, as the sum over any MUB must add up to 1 (i.e., $\forall i,\ \Sigma_j p_{i,j} = 1$).

From the definitions (14)–(17) we can immediately read the conditions for non-negativity of the Wigner function

$$p_{1,1} + p_{2,1} + p_{3,1} \geqslant 1, \quad (18)$$

$$p_{1,1} + p_{2,2} + p_{3,2} \geqslant 1, \quad (19)$$

$$p_{1,2} + p_{2,1} + p_{3,2} \geqslant 1, \quad (20)$$

$$p_{1,2} + p_{2,2} + p_{3,1} \geqslant 1. \quad (21)$$

Because of the conditions $\Sigma_j p_{i,j} = 1$, there are only three free variables in the inequalities above. We can thus pick one $p_{i,j}$ for each MUB $i$ (say, $p_{i,1}$), and represent states by points in this three-dimensional probability space. This representation is equivalent to the more familiar Bloch sphere, with the advantage of generalizing easily to power-of-prime dimension $d$. In that case (to be discussed in Sec. V), there are a total of $(d^2 - 1)$ independent probabilities $p_{i,j}$ describing any mixed quantum state. Note that the probabilities $p_{i,j}$ combine linearly for convex combinations (probabilistic mixtures) of quantum states, a consequence of the linearity of the trace in Eq. (7).

The inequalities (18)–(21) for non-negativity of $W$ are satisfied by state $\vec{p} = (p_{1,1}, p_{2,1}, p_{3,1})$ if and only if $\vec{p}$ lies inside the tetrahedron

$$T_1 = \text{convex hull of } \{(0,0,1),(0,1,0),(1,0,0),(1,1,1)\} \quad (22)$$

(see Fig. 1). By contrast, there exist quantum states whose $W$ is negative in some phase-space points, i.e., lying outside of tetrahedron $T_1$. This is illustrated in Fig. 1, where the set of points corresponding to quantum states is the ball of radius $r = 1/2$ and with center $(\frac{1}{2}, \frac{1}{2}, \frac{1}{2})$.

Let me draw attention to two features of the set of states with non-negative $W$. First, there exist points $\vec{p} \in T_1$ which do not correspond to any one-qubit quantum state [e.g., $\vec{p} = (1,1,1)$]. We must also keep in mind that there were arbitrary choices involved in the particular definition of $W$ that we picked. We have chosen arbitrary one-to-one maps between MUB's and striations, and also between lines in a striation and basis vectors. In the next section we take these two points into account, defining a set which consists solely of quantum states, and for which the Wigner function is non-negative for *all* definitions of $W$.

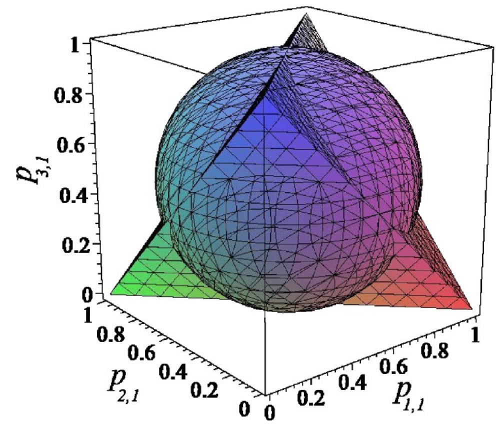


FIG. 1. Tetrahedron in $\vec{p} = (p_{11}, p_{21}, p_{31})$ space representing states with non-negative Wigner function $W$, for the definition of $W$ given by Eqs. (14)–(17). The ball represents one-qubit quantum states.

## IV. ONE-QUBIT STATES WITH NON-NEGATIVE WIGNER FUNCTIONS

In this section I use negativity of $W$ to define the set $C_d$ of states in $d$-dimensional Hilbert space having non-negative $W$ for all definitions of $W$ based on a fixed set of MUB's. I will then argue that single-qubit states in $C_2$ behave "classically" in a concrete computational sense.

Having fixed a set of three MUB's for a single qubit, Wigner functions $W$ can be defined in a number of ways, corresponding to the $3!(2!)^3 = 48$ different associations between lines and basis vectors, and between striations and MUB's. For each of these 48 Wigner function definitions we can do as above, and find the set of points in $\vec{p}$ space for which $W$ is non-negative. A simple calculation shows that depending on the definition, this set is either the original tetrahedron $T_1$ or the tetrahedron whose vertices are the other four $\vec{p}$-cube vertices: $T_2 = $convex hull of {(1, 1, 0), (1, 0, 1), (0, 1, 1), (0, 0, 0)}. Now I define the set $C_d$ of states in $d$-dimensional Hilbert space which I will argue behave "classically" in a computational sense.

*Definition*. The set $C_d$ is defined as the states in a $d$-dimensional Hilbert space whose Wigner function $W$ is non-negative in all phase space points *and* for all definitions of $W$ using a fixed set of mutually unbiased bases.

In the remainder of this article I will characterize the set $C_d$ for some small dimensions $d$, and discuss the limitations of doing quantum computation solely with states in $C_d$. For a qubit, the set $C_2$ is given in $\vec{p}$-space as the intersection of the two tetrahedra $T_1$ and $T_2$ presented above. This corresponds to an octahedron inscribed inside the ball of quantum states:

$$C_2 = \text{convex hull of } \left\{\left(1,\frac{1}{2},\frac{1}{2}\right),\left(0,\frac{1}{2},\frac{1}{2}\right),\left(\frac{1}{2},1,\frac{1}{2}\right),\left(\frac{1}{2},0,\frac{1}{2}\right),\left(\frac{1}{2},\frac{1}{2},1\right),\left(\frac{1}{2},\frac{1}{2},0\right)\right\} \quad (23)$$

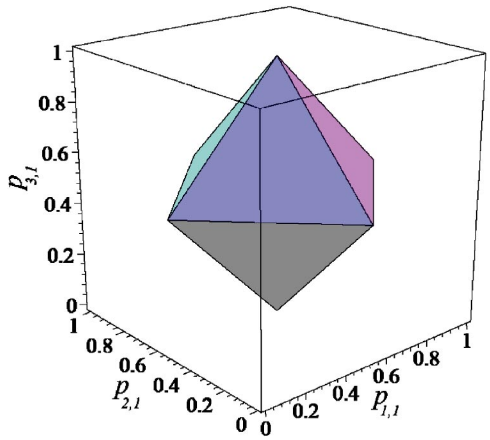


FIG. 2. Octahedron in $\vec{p}=(p_{11},p_{21},p_{31})$ space representing states with non-negative Wigner functions $W$ for all definitions of $W$ using a fixed set of mutually unbiased bases.

(see Fig. 2). We see that set $C_2$ can be characterized in a simpler way as the set of states which are convex combinations of the six basis vectors of the three chosen MUB's:

$$\hat{\rho} \in C_2 \Leftrightarrow \hat{\rho} = \sum_{i,j} q_{i,j} |\alpha_{i,j}\rangle\langle\alpha_{i,j}|, \quad \sum_{i,j} q_{i,j} = 1. \qquad (24)$$

There are at least two motivations for considering the set $C_2$, as opposed to states with non-negative $W$ in a single definition (the sets $T_1$ or $T_2$). The first one is the realization that *a priori* there is no preferred definition of $W$ from the full class of definitions, and any concept of "classical states" based on non-negativity of $W$ should be definition-independent. The second motivation only became apparent after we calculated $C_2$: unlike the sets $T_1$ and $T_2$, all states in $C_2$ are physical states, i.e. obtainable from measurements on a single qubit.

*States in $C_2$ and quantum computing*. We have just characterized the set $C_2$ of single-qubit quantum states which have non-negative $W$ in all definitions of $W$ using a fixed set of MUB's. Let us now review an argument for the "classicality" of the set $C_2$, from a computational point of view.

Recently Bravyi and Kitaev [26] proposed the following model of computation. Imagine that for some reason there are a few quantum computational operations which we can perform perfectly—let us denote these by $O_{\text{ideal}}$. In addition to those, some operations in set $O_{\text{faulty}}$ can only be performed imperfectly. Now let us consider a particular choice for $O_{\text{ideal}}$: preparing a qubit in state $|0\rangle$ (i.e., an eigenstate of the $\hat{\sigma}_z$ operator), applying unitary operators from the Clifford group (such as the Hadamard and CNOT gates), and measuring an eigenvalue of a Pauli operator ($\hat{\sigma}_x$, $\hat{\sigma}_y$ or $\hat{\sigma}_z$) on any qubit. The Gottesman-Knill theorem [27] states that the operations in $O_{\text{ideal}}$ above can only create a restricted set of states known as stabilizer states, i.e., simultaneous eigenstates of the Pauli group of operators. Moreover, such operations do not allow for universal quantum computation, and can be efficiently simulated on a classical computer.

In addition to these perfect operations, Bravyi and Kitaev proposed a set $O_{\text{faulty}}$ with a single extra imperfect operation: preparing an auxiliary qubit in a mixed state $\hat{\rho}$. In this model of computation, it is easy to see that auxiliary qubits in states $\hat{\rho} \in C_2$ cannot be used to perform universal quantum computation [26]. States in $C_2$ are linear convex combinations of the six eigenstates of single Pauli operators. As such, they can be prepared efficiently from operations in $O_{\text{ideal}}$, namely, Clifford gates to obtain any Pauli eigenstate deterministically from the initial $\hat{\sigma}_z$ eigenstate, together with classical coin tosses to prepare them with the appropriate weights given by the desired convex combination. These are operations that can be efficiently simulated on a classical probabilistic computer. This justifies my "classicality" claim for states in $C_2$.

Interestingly, in Ref. [26] it was shown that some "non-classical" states $\hat{\rho} \notin C_2$ can be used to attain universal quantum computation in this model. The basic idea is to use auxiliary pure states outside of $C_2$ to implement gates outside of the Clifford group, using operations in $O_{\text{ideal}}$ only. A single generic non-Clifford gate together with the set of Clifford gates allows for universal quantum computation. This procedure works also for a large class of mixed states $\hat{\rho} \notin C_2$, through a distillation of pure nonstabilizer pure states from $\hat{\rho}^{\otimes N}$ using Clifford operations only [26].

This enables us to identify nonstabilizer states as a resource which can be tapped to implement non-Clifford gates and achieve universal quantum computation. This idea was first suggested by Shor [31], and has since been elaborated on by other authors [32–36].

## V. HIGHER DIMENSIONS

We can follow Gibbons *et al.* and define a discrete Wigner function $W$ whenever the Hilbert space dimension $d$ is a power of prime. In this section I use the definition of $C_d$ to characterize this set for states in small Hilbert space dimensions $d$.

In $d$ dimensions, the probability-space point $\vec{p}$ describing each state has $(d^2-1)$ components. Requiring non-negativity of $W$ for all definitions will correspond to a set of inequalities for $\vec{p}$, each delimiting a half-space where $W$ is non-negative at a particular phase-space point, and for a particular definition of Wigner function. States in the set $C_d$ are those which satisfy all these inequalities, constituting a convex polytope.

Any convex polytope admits two descriptions, one in terms of the half-space inequalities ($H$ description) and one in terms of its vertices ($V$ description). The set $C_d$ is, by definition, an $H$ polytope. For one qubit we have found the equivalent $V$ description: there are six vertices corresponding to the six basis vectors of the three MUB's used to define $W$.

Let us now see how to find the equivalent $V$ description for the $H$-polytope $C_d$ defined above. The starting point is the general expression for the $d$-dimensional Wigner function at phase-space point $\alpha$ (see Ref. [18]):

$$W_\alpha = \frac{1}{d}\left[\sum_{\lambda_{i,j} \ni \alpha} p_{i,j} - 1\right], \qquad (25)$$

where the sum is over the probabilities associated with projectors corresponding to all lines $\lambda_{i,j}$ containing phase-space point $\alpha$. By construction of the striations, each point belongs to exactly one line from each striation. Thus for each point $\alpha$, the sum above has $(d+1)$ terms $p_{i,j}$, one from each MUB.

We want to find which conditions on $p_{i,j}$ correspond to the demand of non-negativity of $W_\alpha$ for all points $\alpha$ *and* for all definitions of $W$ using a fixed MUB set. For a fixed phase-space point $\alpha$, changing the definition of $W$ will correspond to picking a different set of $(d+1)$ probabilities $p_{i,j}$ in Eq. (25), one from each MUB $i$. There are only $d^{(d+1)}$ ways of doing so, and this is the total number of expressions for $W_\alpha$ which we would like to take only non-negative values. These $d^{(d+1)}$ inequalities of the form $W_\alpha \geqslant 0$ constitute our $H$ description of the polytope $C_d$.

From this $H$ description it is possible to find the equivalent $V$ description using a convex hull program based on the QUICKHULL algorithm [37]. While this is considered to be a computationally hard problem in general, it was possible to do the calculation for $d\leqslant 5$. The results are similar to the one-qubit case. For $d=3$, 4, and 5 I found that the $V$ description of $C_d$ has $d(d+1)$ vertices, each corresponding to one of the MUB basis vectors used to define $W$. For $d=5$, for example, the $H$-polytope $C_5$ in $5^2-1=24$-dimensional $\vec{p}$ space is delimited by $5^6=15\,625$ half-space inequalities corresponding to non-negativity of $W$ in all definitions. The $V$ description of this polytope consists of exactly $5\times 6=30$ vertices, each corresponding to one of the basis vectors of the six MUB's.

It is not hard to see that the MUB basis vectors have non-negative $W$ in every single definition of $W$ using those basis vectors. For $d\leqslant 5$, the computation described above shows that these are the only pure states for which this is true for all definitions, and moreover that the mixed states with the same property are exactly their convex combinations. In the next section we will discuss the implications for quantum computing.

*The set $C_d$ and quantum computing*. Given the results above for $d=2$, 3, 4, and 5, it is natural to make the following conjecture.

*Conjecture*. For any power-of-prime Hilbert space dimension $d$, the polytope $C_d$ is equivalent to the $V$ polytope whose vertices are the basis vectors of the MUB's used to define $W$.

It is easy to show that the latter $V$ polytope is contained in $C_d$; the converse seems to be harder to prove for general power-of-prime $d$.

To understand the relevance of this conjecture for quantum computation, we need to review some known facts about mutually unbiased bases. Various authors have come up with constructions of MUB's [30,38–42]. For $d=2^N$, i.e., for the case of $N$ qubits, the corresponding basis vectors can always be written as simultaneous eigenstates of tensor products of single-qubit Pauli operators [40]. More generally, for any power-of-prime dimension $d$ the MUB basis vectors can be chosen to be eigenstates of generalized Pauli operators [39,43]. In other words, the basis vectors of MUB's can always be chosen to be a set of stabilizer states.

The conjecture would then mean that for any $d$, the set $C_d$ would be the convex hull of the particular subset of stabilizer states used as basis vectors of the MUB's. Pure-state quantum computation which is restricted to states in $C_d$ would then only ever reach the MUB basis vectors, all of which admit an efficient classical description using the stabilizer formalism.

As I have already remarked, it is well known that quantum computation that is restricted to pure stabilizer states and gates from the Clifford group is not universal, and can be efficiently simulated on a classical computer [27]. If the conjecture holds, then a wide class of unitary dynamics restricted to pure states inside $C_d$ would be easy to simulate on a classical computer—for example, any gate from the Clifford group. This suggests that nontrivial pure-state quantum computation may require states outside of $C_d$, i.e., having negative Wigner function $W$ in at least some of the definitions of $W$ in the class proposed by Gibbons, Hoffman, and Wootters [18].

## VI. CONCLUSION

In this paper I related the negativity of the discrete Wigner function $W$ with quantum computational speedup. I characterized the set of states with non-negative $W$ using the class of Wigner functions $W$ proposed by Wootters and collaborators in Refs. [17,18]. Wigner functions in this class are defined using projectors on a fixed set of mutually unbiased bases (MUB's). The set of states with non-negative $W$ depends on which definition of $W$ from this class we choose.

I defined the set $C_d$ of $d$-dimensional states having non-negative $W$ simultaneously in *all* definitions of $W$ in the class. States in $C_2$ are classical in the sense of failing to provide quantum computational advantage in a recent model proposed by Bravyi and Kitaev [26]. For dimensions $2\leqslant d \leqslant 5$ I showed that $C_d$ is the convex hull of the stabilizer states used as basis vectors in the MUB set.

These results for small dimensions $d$ support the conjecture that for *any* power-of-prime dimension $d$, the set $C_d$ is the convex hull of a set of stabilizer states. This would mean that pure states in $C_d$ are "classical" in the sense of admitting an efficient classical description using the stabilizer formalism. This suggests that states with negative $W$ may be *necessary* for exponential pure-state quantum computational speedup.

## ACKNOWLEDGMENTS

I would like to thank Angelo Carollo, David Poulin, Rob Spekkens, Daniel Gottesman, and Lucien Hardy for helpful discussions. This work was supported in part by Canada's NSERC.

[1] E. P. Wigner, Phys. Rev. **40**, 749 (1932).
[2] M. Hillary, R. F. O'Connell, M. O. Scully, and E. P. Wigner, Phys. Rep. **106**, 121 (1984).
[3] R. L. Hudson, Rep. Math. Phys. **6**, 249 (1974).
[4] V. Buzek, A. Vidiella-Barranco, and P. L. Knight, Phys. Rev. A **45**, 6570 (1992).
[5] J. S. Bell, in *New Techniques and Ideas in Quantum Measurement Theory* (New York Academy of Sciences, New York, 1986).
[6] O. Cohen, Phys. Rev. A **56**, 3484 (1997).
[7] K. Banaszek and K. Wodkiewicz, Phys. Rev. A **58**, 4345 (1998).
[8] K. Banaszek and K. Wodkiewicz, Phys. Rev. Lett. **82**, 2009 (1999).
[9] F. A. Buot, Phys. Rev. B **10**, 3700 (1974).
[10] J. H. Hannay and M. V. Berry, Physica D **1**, 267 (1980).
[11] L. Cohen and M. Scully, Found. Phys. **16**, 295 (1986).
[12] R. P. Feynman, in *Quantum Implications: Essays in Honour of David Bohm*, edited by B. J. Hiley and F. David Peat, (Routledge, New York, 1987), Chap. 13, pp. 235–248.
[13] W. K. Wootters, Ann. Phys. (N.Y.) **176**, 1 (1987).
[14] D. Galetti and A. F. R. de Toledo Piza, Physica A **149**, 267 (1988).
[15] O. Cohendet, P. Combe, M. Sirugue, and M. Sirugue-Collin, J. Phys. A **21**, 2875 (1988).
[16] U. Leonhardt, Phys. Rev. Lett. **74**, 4101 (1995).
[17] W. K. Wootters, IBM J. Res. Dev. **48**, 99 (2004).
[18] K. S. Gibbons, M. J. Hoffman, and W. K. Wootters, Phys. Rev. A **70**, 062101 (2004).
[19] A. M. F. Rivas and A. M. Ozorio de Almeida, Ann. Phys. (N.Y.) **276**, 223 (1999).
[20] P. Bianucci, C. Miquel, J. P. Paz, and M. Saraceno, Phys. Lett. A **297**, 353 (2002).
[21] C. Miquel, J. P. Paz, and M. Saraceno, Phys. Rev. A **65**, 062309 (2002).
[22] M. Koniorczyk, V. Buzek, and J. Janszky, Phys. Rev. A **64**, 034301 (2001).
[23] J. P. Paz, Phys. Rev. A **65**, 062311 (2002).
[24] C. C. Lopez and J. P. Paz, Phys. Rev. A **68**, 052305 (2003).
[25] A. Vourdas, Rep. Prog. Phys. **67**, 267 (2004).
[26] S. Bravyi and A. Kitaev, Phys. Rev. A (to be published).
[27] D. Gottesman, Ph.D. thesis, California Institute of Technology, 1997.
[28] D. Gottesman, Chaos, Solitons Fractals **10**, 1749 (1999).
[29] D. Gottesman, in Group 22: Proceedings of the XXII International Colloquium on Group Theoretical Methods in Physics, edited by S. P. Corney, R. Delbourgo, and P. D. Jarvis (International Press, Cambridge, MA, 1999), pp. 32–43.
[30] W. K. Wootters and B. D. Fields, Ann. Phys. (N.Y.) **191**, 363 (1989).
[31] P. W. Shor, in *37th Symposium on Foundations of Computing* (IEEE Computer Society Press, Los Alamitos, CA, 1996), pp. 56–65.
[32] E. Dennis, Phys. Rev. A **63**, 052314 (2001).
[33] D. Gottesman and I. L. Chuang, Nature (London) **402**, 390 (1999).
[34] X. Zhou, D. W. Leung, and I. L. Chuang, Phys. Rev. A **62**, 052316 (2000).
[35] P. Jorrand and S. Perdrix, quant-ph/0404125.
[36] A. M. Childs, D. W. Leung, and M. A. Nielsen, Phys. Rev. A (to be published).
[37] C. B. Barber, D. P. Dobkin, and H. T. Huhdanpaa, ACM Trans. Math. Softw. **22**, 469 (1996); http://www. qhull.org.
[38] I. D. Ivanovic, J. Phys. A **14**, 3241 (1981).
[39] S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury, and F. Vatan, Algorithmica **34**, 512 (2002).
[40] J. Lawrence, Č. Brukner, and A. Zeilinger, Phys. Rev. A **65**, 032320 (2002).
[41] A. O. Pittenger and M. H. Rubin, Linear Algebr. Appl. **390**, 255 (2004).
[42] A. Klappenecker and M. Rötteler, Lect. Notes Comput. Sci. **2948**, 137 (2004).
[43] A. Pittenger and M. H. Rubin, Phys. Rev. A **62**, 032313 (2000).