States with the Same Probability Distribution for Each Basis in a Complete Set of MUBs

William K. Wootters

Department of Physics, Williams College, Williamstown, MA 01267, USA

Consider a simple harmonic oscillator in one dimension, and let $\hat{x}$ and $\hat{p}$ be dimensionless position and momentum operators, scaled so that the energy of the oscillator is proportional to $x^2 + p^2$. There is a sense in which the continuous set of operators $\hat{S}(\theta) = (\cos\theta)\hat{x} + (\sin\theta)\hat{p}$, with $0 \leq \theta < \pi$, corresponds to a complete set of mutually unbiased bases: any eigenstate of $\hat{S}(\theta)$ is uniformly distributed with respect to $\hat{S}(\theta')$ as long as θ' is different from θ. With respect to these operators, the eigenstates of the Hamiltonian $\hat{x}^2 + \hat{p}^2$ have a special property, namely, that the probability distribution over the eigenvalues of $\hat{S}(\theta)$ is independent of θ. (For example, for any of these harmonic oscillator eigenstates, the momentum distribution is the same as the position distribution.) To put it in other words, the Wigner function of each energy eigenstate of the harmonic oscillator is isotropic around the origin in phase space.[1]

This property—that is, having the same probability distribution for each member of a complete set of mutually unbiased bases—has an analogue in systems with finite-dimensional Hilbert spaces. In any prime-power dimension d, let us consider the complete set of mutually unbiased bases constructed in Ref. [1]. Let us call a state "isotropic" if it yields the *same* collection of probabilities with respect to *each* of the mutually unbiased bases.[2] (As in the continuous case, the term "isotropic" refers to directions in phase space, but now the phase space is discrete—see below.) That such states exist when d is a power of two was shown in Ref. [2], and more progress was made by Sussman [3] and Appleby [4]. Appleby has subsequently shown that such states exists for every prime-power dimension for which the dimension

[1] Here "isotropic" means "the same in every direction" (starting from a specific point). In the continuous phase space this is equivalent to "rotationally invariant." But in the discrete case to be considered shortly, the two concepts are not equivalent, because rotations will not be able to cover all the directions.

[2] In this talk I am not concerned with any *ordering* of the index over which the probability distribution is defined.

d is of the form $4n + 3$ where n is an integer [5]. It is also known that any isotropic state is automatically a *minimum-uncertainty state*, in the sense that the order-2 Renyi entropy of the probability distribution, averaged over all of the mutually unbiased bases, is minimized [6, 2, 4]. In the rest of this talk I consider only the case of *prime* d of the form $4n+3$. (So $d = 3, 7, 11, 19$, and so on.) For each of several such values of d, I examine numerically the one isotropic state identified in Ref. [3], partly to see if it resembles, in any other respect, one of the harmonic oscillator eigenstates of the continuous case. As we will see, up to now I have found very few similarities, but these states nevertheless have some intriguing properties.

We begin by recalling that the mutually unbiased bases in our d-dimensional Hilbert space can be associated with the "striations," that is, the sets of parallel lines, in a $d \times d$ phase space whose axis variables x and p take values in the field $\mathbb{F}_d$, which for our case of prime d is simply $\mathbb{Z}_d$ [7]. To find isotropic states, it is natural to look for states that are invariant under "rotations" of this phase space, just as a harmonic oscillator eigenstate is invariant under rotations of the continuous phase space. (But see footnote 1.)

What does "rotation" mean for our discrete phase space? First we define "circles": a circle around the origin in the discrete phase space is the set of points (x, p) satisfying $x^2 + p^2 = c$ for some nonzero value c in $\mathbb{Z}_d$.[3] There are $d - 1$ circles around the origin, each containing $d + 1$ points. Note that half of the circles possess a "radius" in $\mathbb{Z}_d$—that is, their values of c have square roots in $\mathbb{Z}_d$—while the other half do not. Let us call the former "good circles" and the latter "bad circles." One can also show that half of the lines through the origin (rays) pass only through good circles, and the other half pass only through bad circles [3]; so we have "good rays" and "bad rays." And each ray is associated with one of the mutually unbiased bases; hence there are "good bases" and "bad bases." That such a distinction exists will become significant in what follows.

Let us define a rotation to be a linear transformation on the phase space, with determinant equal to +1, that preserves all the circles. One can show that for prime $d = 4n + 3$, all but one of the rotations can be written as

$$R(m) = \frac{1}{1+m^2}\begin{pmatrix} 1-m^2 & -2m \\ 2m & 1-m^2 \end{pmatrix}, \tag{1}$$

[3] This definition makes sense only because for $d = 4n + 3$, the field element -1 has no square root in the field. So the equation $x^2 + p^2 = 0$ has no solution other than $x = p = 0$. In contrast, in $\mathbb{Z}_5$, for example, we have $1^2 + 2^2 = 0$.

where m ranges over all the elements of $\mathbb{F}_d$. The remaining rotation is

$$R(\infty) = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2}$$

(Note that $R(\infty)$ is, in form, what one would get by taking the limit of $R(m)$ if m were a real variable. But the components of $R(\infty)$ are elements of $\mathbb{Z}_d$.) A *primitive rotation* is a rotation whose powers generate all the other rotations. Note that any rotation always takes good rays to good rays and bad rays to bad rays. So a rotation does not cycle through all the striations of the phase space.

Now, for every unit-determinant linear transformation on our phase space, there is an associated unitary transformation on the Hilbert space, and the correspondence is given by a simple formula [4]. Up to an overall phase factor, the unitary transformation associated with $R(m)$ turns out to be given as follows in terms of its matrix elements (for m not equal to zero or infinity) [3].

$$U(m)_{jk} \propto \frac{1}{\sqrt{d}}\, \omega^{\frac{1}{4}\left(m-\frac{1}{m}\right)\left(j^2+k^2\right)+\frac{1}{2}\left(m+\frac{1}{m}\right)jk}, \tag{3}$$

where $\omega = \exp(2\pi i/d)$ and the arithmetic in the exponent is to be done in $\mathbb{Z}_d$. If $R(m)$ is a primitive rotation, one can show that the eigenvalues of $U(m)$ are (up to an overall phase factor) the $(d+1)$st roots of unity with one root left out. Let us choose the phase factor so that -1 is the omitted root. The eigenvectors of such a $U(m)$ are our candidates for isotropic states.

But one finds that these eigenvectors are typically *not* isotropic states. Because $R(m)$ does not cycle through all the striations, $U(m)$ does not cycle through all the bases. (In fact there exists no cycling unitary for these values of d, as has been shown by Appleby [4].) Each eigenvector of a primitive $U(m)$ yields the same collection of probabilities for all the *good* bases, and also for all the *bad* bases, but the good do not have to match the bad. However, it is possible to show that there is *one* eigenvector of a primitive $U(m)$ for which the good and bad probability distributions do match [3]. With the above convention for the overall phase, it is the eigenvector corresponding to the eigenvalue 1. This one eigenvector is therefore an isotropic state.[4] Let us call

[4] The argument outlined here does not prove that an isotropic state exists for all prime d of the form $4n+3$, because we have not shown that a primitive value of m exists for all such d, and I have no such proof to offer. However, as I have mentioned earlier, Appleby has proved (by a different method) that isotropic states exist for all such dimensions (also for *prime power* dimensions of this form) [5].

this state $|\beta_d\rangle$. The rest of the talk explores the properties of $|\beta_d\rangle$ for several values of d.

That the state $|\beta_d\rangle$ is isotropic is one property it shares with the energy eigenstates of a harmonic oscillator. Another is this: $|\beta_d\rangle$ is a real vector (if we choose its overall phase correctly), just as the harmonic oscillator eigenstates can be represented by real functions of position. But we should not expect $|\beta_d\rangle$ to look like a harmonic oscillator eigenstate when we plot its components, because the elements of $\mathbb{Z}_d$ are not ordered as the real numbers are. (For example, the elements of $\mathbb{Z}_d$ that are squares of other elements of $\mathbb{Z}_d$ are mixed in with those that are not, whereas for the reals, the positive and negative numbers are neatly separated.) To give a sense of what these states look like, I plot in Fig. 1, for $d = 3511$, the components $\langle x|\beta_d\rangle$ as a function of x, where $x \in \mathbb{Z}_d$ labels the elements of the standard basis.

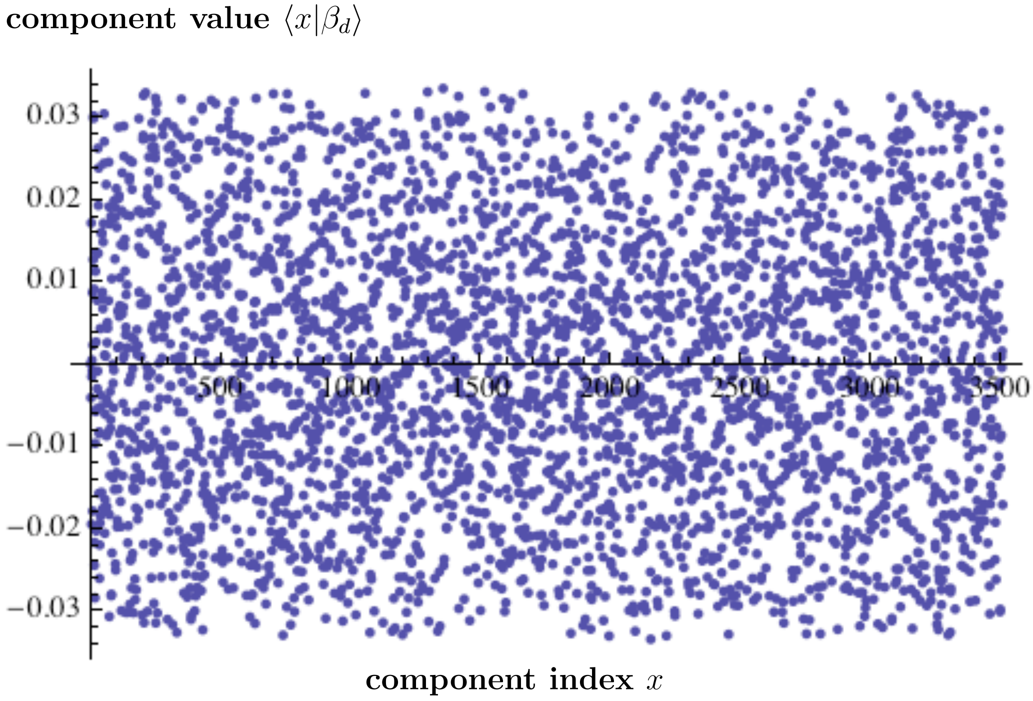

FIG. 1. The components of the real vector $|\beta_{3511}\rangle$.

As one might guess from the figure, $\langle x|\beta_d\rangle$ is always an odd function of x; that is, $\langle -x|\beta_d\rangle = -\langle x|\beta_d\rangle$. So if we are to think of $|\beta_d\rangle$ as analogous to a harmonic oscillator eigenstate, it would presumably have to be a state with an odd value of the harmonic-oscillator quantum number.

One feature of Fig. 1 that I find surprising is the sharp cut-off around ±0.034 in the values of the components. This value is approximately equal to $2/\sqrt{d} = 2/\sqrt{3511} = 0.0338$, and one finds a similar pattern for other values of d. This feature suggests that it might be interesting to look at a histogram of the values of the components. That is, imagine making several horizontal slices through Fig. 1 of uniform thickness, and count the number of dots in each slice. Such a histogram is plotted in Fig. 2. (A histogram for $d = 547$ appears in Ref. [3].)

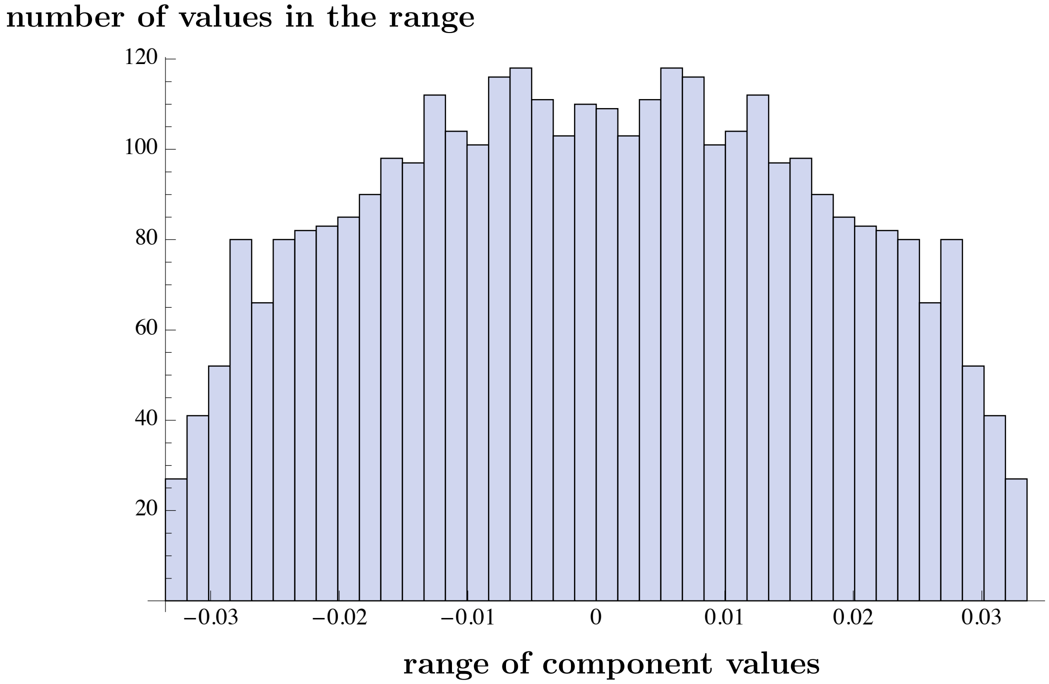

FIG. 2. A histogram of the components of the real vector $|\beta_{3511}\rangle$.

Notice that the histogram looks like a semicircle. The distributions for the other large values of d I have considered are likewise roughly semicircular, though there are occasional spikes and dips. Semicircular distributions are well known in the theory of random matrices; under broad conditions, the distribution of eigenvalues of a random symmetric matrix is semicircular. It is intriguing that such a distribution would appear in the present setting where there is no randomness at all. Each state $|\beta_d\rangle$ is a specific eigenvector of a specific unitary matrix.

As one test of the semicircularity, I have computed, for several values of d, the Shannon information of the probability distribution $P_d(x) = |\langle x|\beta_d\rangle|^2$—that is, $\log_2 d$ minus the Shannon entropy—and compared it to what one would expect if the distribution of values of $\langle x|\beta_d\rangle$ were exactly semicircular. (This expected value is $1/(2\ln 2) \approx 0.721$.) Fig. 3 shows the result. Also plotted is the Shannon information averaged over all pure states (that is, averaged with respect to the unitarily invariant measure over the unit sphere). One sees that at least by this test, $|\beta_d\rangle$ acts as if its components were distributed nearly semicircularly for large d. I do not know of any sense in which a harmonic oscillator eigenstate in the continuous case manifests such a semicircular distribution.

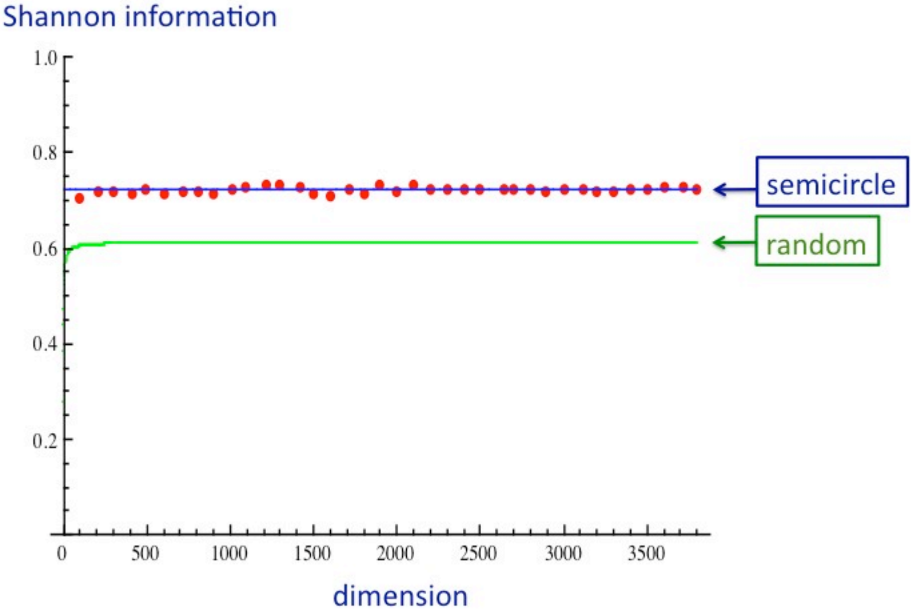

FIG. 3. Shannon information of $P_d(x) = |\langle x|\beta_d\rangle|^2$ for several values of d. The curve marked "random" shows the average Shannon information over all pure states, which is $(\log_2 d) - [(1/2 + 1/3 + \cdots + 1/d)/\ln 2]$. For large d, a pure state chosen at random (with respect to the unitarily invariant measure) is likely to have a value of the Shannon information close to this average value.

Thus the special state $|\beta_d\rangle$, which is isotropic in that it "looks the same" from the perspective of each of the mutually unbiased bases, does not obviously resemble an eigenstate of a harmonic oscillator in many other respects. Of course the analogy we have pursued here is quite formal. We have replaced the real numbers of the harmonic oscillator case with a finite field that has a modular arithmetic, and we have used algebraic analogies to go from continuous rotations to discrete rotations. In the end there are many respects in which the discrete case is different from the continuous case. For example, in the continuous case, each rotationally invariant state is automatically isotropic, whereas in the discrete case (with prime $d = 4n+3$), we have found only one isotropic state out of the d that are rotationally invariant.

We have seen, though, that there is something intriguing about this special isotropic state. For large values of d, the distribution of the *components* of the state vector appears to be roughly semicircular. Surely there is some good mathematical reason for this to be the case.

References

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

[2] W. K. Wootters and D. M. Sussman, arXiv:0704.1277 (2007).

[3] D. M. Sussman, "Minimum Uncertainty States and Rotational Invariance in Discrete Phase Space," Thesis, Williams College (2007).

[4] D. M. Appleby, arXiv:0909.5233 (2009).

[5] D. M. Appleby, unpublished notes. See also Ref. [4].

[6] D. M. Appleby, H. B. Dang, and C. A. Fuchs, arXiv:0707.2071 (2007).

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