Maximum nonlocality and minimum uncertainty using magic states

Mark Howard

Institute for Quantum Computing and Department of Applied Mathematics, University of Waterloo, Waterloo, Ontario, Canada, N2L 3G1

(Received 11 February 2015; published 6 April 2015)

We prove that magic states from the Clifford hierarchy give optimal solutions for tasks involving nonlocality and entropic uncertainty with respect to Pauli measurements. For both the nonlocality and uncertainty tasks, stabilizer states are the worst possible pure states, so our solutions have an operational interpretation as being highly nonstabilizer. The optimal strategy for a qudit version of the Clauser-Horne-Shimony-Holt game in prime dimensions is achieved by measuring maximally entangled states that are isomorphic to single-qudit magic states. These magic states have an appealingly simple form, and our proof shows that they are "balanced" with respect to all but one of the mutually unbiased stabilizer bases. Of all equatorial qudit states, magic states minimize the average entropic uncertainties for collision entropy and also, for small prime dimensions, min-entropy, a fact that may have implications for cryptography.

DOI: 10.1103/PhysRevA.91.042103 PACS number(s): 03.65.Ud, 03.67.Dd

I. INTRODUCTION AND MOTIVATION

In the context of fault-tolerant quantum computing using error-correcting codes, there exist single-particle pure states, "magic states," with desirable properties. Having access to a supply of these states expands the sets of robustly implementable operations to encompass a universal gate set. Moreover, impure versions of these states can be purified using only the fault-tolerant operations provided by the error-correcting code. There is a privileged family of magic states, well defined for both qubits and qudits of odd prime dimension p, whose structure reflects a group-theoretical object called the Clifford hierarchy. Here we will show that the utility of these magic states extends beyond the arena of quantum computation; they essentially provide optimal strategies for both (i) a nonlocal game wherein both Alice and Bob each use p Pauli measurements and (ii) a cryptographically motivated scenario wherein we try to minimize the average entropic uncertainty with respect to a set of p mutually unbiased measurements. Qudits can have operational advantages for nonlocal or cryptographic tasks in terms of tolerating inefficiencies or the addition of white noise [1–3], but the geometry of state space becomes notoriously complex when we venture past the qubit Bloch sphere. In this work we prove that the optimal states have a simple structure and furthermore that these states have connections to group-theoretical and number-theoretical structures. These ideas may prove useful elsewhere.

Given the fundamental importance of the Clauser-Horne-Shimony-Holt [4] (CHSH) game in quantum information theory [5–7], it is well motivated to study generalizations to different numbers of measurement settings, parties, and so on. By preserving the structure of the CHSH game while enlarging the size of the input-output alphabet to d symbols (using qudits), we can examine how the quantum advantage scales with dimension or investigate new features that arise due to additional degrees of freedom. Buhrman and Massar [8] studied such a generalization and found bounds on the allowable quantum value. Ji *et al.* [9] constructed a Bell operator from qudit Pauli measurements, whose maximization describes a quantum strategy for the qudit CHSH game. For small prime dimensions they analyzed classical (i.e., local hidden variable) and quantum values. A follow-up work by Liang *et al.* [10] expanded on this analysis and broadened the numerical search to allow non-Pauli measurements. Most recently Bavarian and Shor [11] looked at a generalized CHSH game wherein the alphabet consists of all field elements $\mathbb{F}_q$ where q is a prime power, and proved a generalization of Tsirelon's bound using Information Causality [12]. As was done by Ji *et al.* [9], we will restrict our analysis to projective Pauli measurements. Quantifying nonlocality is a tricky task, particularly if one is motivated by operational considerations. For example, an experimental test may achieve higher statistical significance via lower statistical error [13] or higher statistical strength via larger statistical divergence with any classical model [14]. One conceptually simple metric for nonlocality is to measure the amount by which a Bell inequality is violated. If Bell inequality violation is the only figure of merit, then restricting to Pauli measurements is suboptimal; larger violations are possible with non-Pauli measurements whenever $p > 3$. Nevertheless, we remain particularly interested in nonstabilizer states, measurements (see, e.g., Ref. [15]), or transformations that emerge as privileged with respect to their stabilizer counterparts, due to some geometrical or operational relationship. This is motivated in part by the clean mathematical and conceptual framework provided by the so-called "stabilizer subtheory" [16–18] of quantum mechanics for odd-dimensional qudits, loosely speaking, states and operations far outside this subtheory are highly nonclassical [19].

Mutually unbiased bases (MUBs) are a crucial component in a variety of quantum-informational settings. They are necessary for the creation of maximally strong entropic uncertainty relations [20], which describe limits on the allowed probability distributions associated with multiple measurements on quantum states. In cryptographic scenarios, uncertainty relations can be used to bound an eavesdropper's knowledge of quantum states transmitted between two parties. In [21] Amburg *et al.* motivate the study of "MUB-balanced states," i.e., pure states for which, relative to a complete set of $d + 1$ MUBs, the list of probabilities of the d outcomes of one of these measurements is independent of the choice of measurement, up to permutations. Recent work by Appleby *et al.* [22] suggests that MUB-balanced states exist only in odd prime-power dimensions of the form $d = 3 \bmod 4$. A MUB-balanced state is automatically also a collision-entropic minimum uncertainty [22,23] (or

maximally certain [24]) state, important in cryptography, but balancedness is a stricter condition than minimum uncertainty. From a foundational point of view, MUB-balanced states are analagous to harmonic oscillator eigenstates insofar as the "direction" of a measurement is unimportant. Our results include a concise proof that magic states are balanced with respect to p out of a total of $p+1$ total bases in a complete set of MUBs. This suggests that magic states may be relevant in quantum cryptography, in analogy with the Breidbart basis for qubits. We also comment on the connection between magic states and the Sato-Tate distribution that arises in number theory.

II. BACKGROUND MATERIAL

A. Prerequisites and notation

The Weyl-Heisenberg operators $D_{(x|z)}$ are a generalized p-dimensional version of qubit Pauli operators,

$$D_{(x|z)} = \omega^{2^{-1}xz} \sum_k \omega^{kz} |k+x\rangle\langle k| = \omega^{\frac{xz}{2}} X^x Z^z$$

with

$$X|j\rangle = |j+1\rangle \quad Z|j\rangle = \omega^j |j\rangle \quad (\omega = e^{2\pi i/p}), \tag{1}$$

where we always treat expressions like $\frac{1}{a}$ to mean the mutiplicative inverse $a^{-1} \in \mathbb{Z}_p = \{0,1,\ldots,p-1\}$. The choice of phase has the convenient feature that $D^n_{(x|z)} = D_{(nx|nz)}$, and we use symplectic notation to keep track of X and Z powers separately, so that multiqudit operators look like

$$D_{(x_1|z_1)} \otimes D_{(x_2|z_2)} = D_{(x_1,x_2|z_1,z_2)}.$$

The rank-1 projector onto the ω^V eigenspace of $D_{(1|B)}$ (in other words, the projector onto the Vth vector of the B-th Weyl-Heisenberg basis) is given by

$$|\psi^V_B\rangle\langle\psi^V_B| = \frac{1}{p} \sum_j \omega^{-jV} D^j_{(1|B)}, \tag{2}$$

so that

$$|\psi^V_B\rangle = \frac{1}{\sqrt{p}} \sum_{k\in\mathbb{F}_q} \omega^{(\frac{1}{2}Bk^2 - Vk)} |k\rangle. \tag{3}$$

The p^2 states $\{|\psi^V_B\rangle, B,V \in \mathbb{Z}_p\}$, along with those of the computational basis, comprise both (i) a complete set of mutually unbiased bases and (ii) the complete set of stabilizer states (Pauli eigenstates), for a single qudit.

Consider the family of magic states f and magic gates M (diagonal in the computational basis) [25–27]

$$|f_{a,b,c}\rangle = \frac{1}{\sqrt{p}} \sum_k \omega^{ak^3+bk^2+ck} |k\rangle \quad p>3 \tag{4}$$

$$= M_{a,b,c}|+\rangle \quad a \in \mathbb{Z}^*_p, \quad b,c \in \mathbb{Z}_p, \tag{5}$$

where $|+\rangle$ is the equal-weighted superposition of all computational basis states and $\mathbb{Z}^*_p = \{1,2,\ldots,p-1\}$. Note that the above expressions require a minor modification for the smallest prime dimensions [27], i.e.,

$$|f_{a,b,c}\rangle = \begin{cases} \frac{1}{\sqrt{2}}(|0\rangle + \gamma^{a+2b+4c}|1\rangle) & p=2, \\ \frac{1}{\sqrt{3}}(|0\rangle + \xi^{2a+6b+3c}|1\rangle + \xi^{a+6b+6c}|2\rangle) & p=3, \end{cases} \tag{6}$$

where $\gamma = e^{2\pi i/8}$ and $\xi = e^{2\pi i/9}$ and $a \in \mathbb{Z}^*_p$, $b,c \in \mathbb{Z}_p$. For a fixed value $a \in \mathbb{Z}^*_p$ the magic states, in addition to the computational basis, form a complete set of MUBs since $|\langle f_{a,b,c}|f_{a,b',c'}\rangle| = \delta_{b,b'}\delta_{c,c'} + (1-\delta_{b,b'})/\sqrt{p}$ [28,29]. Finally, define the Jamiołkowski state $|J_{a,b,c}\rangle$ as that which is created by applying a magic gate to one half of a Bell pair:

$$|J_{a,b,c}\rangle = \mathbb{I}_p \otimes M_{a,b,c}|\Phi\rangle, \quad |\Phi\rangle = \sum_j \frac{|jj\rangle}{\sqrt{p}}. \tag{7}$$

Clearly $|J_{a,b,c}\rangle$ is isomorphic to a single-qudit magic state $|f_{a,b,c}\rangle$ under the identification $|jj\rangle \in \mathbb{C}^{p^2} \leftrightarrow |j\rangle \in \mathbb{C}^p$.

The group of operations generated by (tensor products of) the Weyl-Heisenberg operators in Eq. (1) is the Pauli group (we denote it $\mathcal{C}_1$ for reasons that will become clear). The set of unitaries that map the Pauli group into itself under conjugation is the Clifford group ($\mathcal{C}_2$). The unitaries that map the Pauli group into the Clifford group, under conjugation, define [30] the third level of the Clifford hierarchy, $\mathcal{C}_3$, and so on. Overall we have

$$\mathcal{C}_k := \{U | U\mathcal{C}_1 U^\dagger \subseteq C_{k-1}\}, \tag{8}$$

where $\mathcal{C}_1 \subset \mathcal{C}_2 \subset \mathcal{C}_3 \cdots$ but the sets $\mathcal{C}_{k>3}$ no longer form a group. The operations in the first two levels arise naturally in the context of fault-tolerant quantum computation, whereas an operation from third level is typically also required to enable universal quantum computation. Properties of $\mathcal{C}_3$ for multiple qubits are discussed in Ref. [30] whereas the diagonal single-qudit subset of $\mathcal{C}_3$, as discussed in Ref. [27], is given by $M_{a,b,c}$ above. It is in this sense that we say states $|f_{a,b,c}\rangle$ and $|J_{a,b,c}\rangle$ reflect the structure of (the third level of) the Clifford hierarchy.

B. Generalizing the CHSH game

The familiar two-qubit CHSH inequality takes the form $\langle\mathcal{B}\rangle^{\text{LHV}}_{\max} \leqslant 2$ with a Bell operator

$$\mathcal{B} = XX + XY + YX - YY = \sum_{x,y=0}^{1} \omega^{xy} A_x B_y \tag{9}$$

where

$$\{A_0, A_1\} = \{B_0, B_1\} = \{X, Y\} \tag{10}$$

and $\omega = -1$ is a pth root of unity. The maximum expectation value using local hidden variables (LHV) is 2, whereas quantum mechanics can achieve $2\sqrt{2}$, which is the maximum eigenvalue, $\lambda_{\max}(\mathcal{B})$, of the Bell operator. The optimal shared state that Alice and Bob can measure in this case is given by $|J_{1,0,0}\rangle$ from Eq. (7), i.e.,

$$\langle\mathcal{B}\rangle^{\text{QM}}_{\max} = \langle J_{1,0,0}|\mathcal{B}|J_{1,0,0}\rangle = 2\sqrt{2}. \tag{11}$$

Generalizing the above CHSH Bell operator to qudits [9], we find it convenient to define two closely related operators:

$$\mathcal{B}^* = \frac{1}{p} \sum_{n\in\mathbb{Z}^*_p} \sum_{x,y\in\mathbb{Z}_p} \omega^{nxy} A^n_x B^n_y, \tag{12}$$

$$\mathcal{B} = \frac{1}{p} \sum_{n,x,y\in\mathbb{Z}_p} \omega^{nxy} A^n_x B^n_y, \tag{13}$$

where $\omega = e^{2\pi i/p}$ so that $\mathcal{B} = \mathcal{B}^* + p\mathbb{I}_{p^2}$ and consequently $\lambda_{\max}(\mathcal{B}) = \lambda_{\max}(\mathcal{B}^*) + p$. The traceless version $\mathcal{B}^*$ is more

convenient to work with, but the maximal value of $\mathcal{B}$ is a more useful quantity.

To aid our analysis we use the Pauli measurement operators adopted in Ref. [9]:

$$A_x = \omega^{x(2x+1)/2} D_{(1|x)}, \quad B_y = \omega^{y(y+1)/4} D_{(1|y/2)}, \tag{14}$$

where $x,y \in \mathbb{Z}_p$, so that $A_{y/2} = B_y$. The operators $\{D_{(1|j)}, j \in \mathbb{Z}_p\}$ are a generalization of the qubit measurements $\{X,Y\}$ used above insofar as they are the Pauli observables (excluding Z) whose eigenbases form mutually unbiased bases. In the qudit case, different orderings and phases of the measurement operators can have an effect on the quantumly achievable expectation value.

The expectation value of $\mathcal{B}$ from Eq. (13) can be related to the quantum value, $0 \leqslant \nu \leqslant 1$, of a nonlocal game [5,6], which takes the general form

$$\nu = \sum_{a,b,x,y \in \mathbb{Z}_p} P(x,y) V(a,b,x,y) P(a,b|x,y) \tag{15}$$

for measurement settings (x,y), outcomes (a,b) and a predicate or payoff function $V \in \{0,1\}$. By choosing a flat probability distribution over all measurement settings, $P(x,y) = 1/p^2$, and a winning condition $V(a,b,x,y) = \delta_{a+b+xy,0}$ we arrive at

$$\nu = \frac{1}{p^2} \langle \Psi | \mathcal{B} | \Psi \rangle = \frac{1}{p^2} \sum_{a+b+xy=0} P(a,b|x,y), \tag{16}$$

where the right-hand side of the above expression is a more general form for CHSH-type games, amenable to POVMs as well as projective measurements (see also a discussion in Ref. [10]).

The maximum classical value $\langle \mathcal{B} \rangle_{\max}^{\mathrm{LHV}}$ is given by finding local hidden variable assignments

$$\vec{a} = (a_0, \ldots, a_x, \ldots, a_{p-1}) \in \mathbb{Z}_p^p,$$
$$\vec{b} = (b_0, \ldots, b_y, \ldots, b_{p-1}) \in \mathbb{Z}_p^p$$

that tell Alice and Bob which element of the spectrum of their observable they should output for a given measurement setting, i.e.,

$$A_x \mapsto \omega^{a_x}, \quad B_y \mapsto \omega^{b_y}.$$

The best choices of $\vec{a}$ and $\vec{b}$ maximize the quantity

$$\langle \mathcal{B} \rangle_{\max}^{\mathrm{LHV}} = \frac{1}{p} \sum_{n,x,y=0}^{p-1} \omega^{nxy} (\omega^{a_x})^n (\omega^{b_y})^n$$
$$= \sum_{a,b,x,y \in \mathbb{Z}_p} \delta_{a_x + b_y + xy, 0};$$

i.e., they give the best classical strategy for participants trying to maximize the number of instances where $a + b + xy = 0 \bmod p$. Liang *et al.* [10] provide an explicit classical strategy achieving

$$\langle \mathcal{B} \rangle_{\max}^{\mathrm{LHV}} \geqslant 3p - 2.$$

Turning to quantum strategies, Bavarian and Shor's result [11] (restricted to $q = p$) says that the quantum value (16) of a generalized CHSH game is bounded above (via Information Causality [12]) by

$$\nu \leqslant IC(p) := \frac{1}{p} \left(1 + \frac{p-1}{\sqrt{p}} \right). \tag{17}$$

Clearly this implies $\langle \mathcal{B} \rangle_{\max}^{\mathrm{QM}} \leqslant p^2 IC(p)$, but it also applies to more general scenarios wherein Alice and Bob use POVMs. It is also shown [11] that classical strategies can achieve $\Omega(\frac{1}{\sqrt{q}})$ if $q = p^{2k}$ or $O(\frac{1}{\sqrt{q} q^{\epsilon_0}})$ if $q = p^{2k-1}$ for a very small ($\leqslant \frac{1}{700}$) positive constant ϵ_0. This classical bound was subsequently improved upon by Lunghi *et al.* [31]. The moral is that we might not expect a classical-quantum separation in the asymptotic limit. Liang *et al.* [10] used the Navascues-Pironio-Acin [32] hierarchy to numerically bound the quantum value ν from above and it appears that the values so obtained coincide with $IC(p)$ for $p = 5,7$.

C. Entropic uncertainty relations and eavesdropping

Fix the notation for the mutually unbiased basis (MUB) expansion of a generic operator K acting on a qutrit state space as follows:

$$K \leftrightarrow \left(\begin{array}{c|c|c|c} c_{0,\infty} & c_{0,0} & c_{0,1} & c_{0,2} \\ c_{1,\infty} & c_{1,0} & c_{1,1} & c_{1,2} \\ c_{2,\infty} & c_{2,0} & c_{2,1} & c_{2,2} \end{array} \right),$$

where

$$c_{V,B} = \langle \psi_B^V | K | \psi_B^V \rangle \quad \left[| \psi_B^V \rangle \text{ from Eq. (3)} \right]$$

and the infinity basis label corresponds to the computational basis, i.e., $|\psi_\infty^V\rangle = |V\rangle$. The generalization to higher dimensions is obvious. The coefficients $c_{V,B}$ correspond to probabilities when K is a normalized density operator, and the probability distribution associated with a basis B is given by $\{c_{0,B}, c_{1,B}, \ldots, c_{p-1,B}\}$. Inverting this decomposition, we find [33]

$$K = \sum_{B,V} c_{V,B} | \psi_B^V \rangle \langle \psi_B^V | - \mathrm{Tr}(K) \mathbb{I}_p.$$

With the above decomposition in hand we can characterize a density matrix ρ in terms of its associated probability distributions. The Renyi entropy of order 2 (i.e., the collision entropy) with respect to a particular basis B is given by $H_2^B(\rho) = -\log(\sum_V c_{V,B}^2)$, whereas the min-entropy is given by $H_{\min}^B(\rho) = -\log \max_V c_{V,B}$ [23,24]. (The choice of base is irrelevant for now but we adopt the base 2 for numerical calculations in Sec III and Table II.) For an arbitrary pure state $|\phi\rangle \in \mathbb{C}^p$ this can be rewritten as

$$H_2^B(|\phi\rangle) = -\log \left(\sum_V \left| \langle \phi | \psi_B^V \rangle \right|^4 \right),$$
$$H_{\min}^B(|\phi\rangle) = -\log \max_V \left| \langle \phi | \psi_B^V \rangle \right|^2,$$

which obey

$$\log(p) \geqslant H_2^B(|\phi\rangle) \geqslant H_{\min}^B(|\phi\rangle) \geqslant 0.$$

Typically we are interested in total or average entropies across a number of different measurement bases. The trade-offs that arise when we try to minimize entropy across multiple

measurement bases gives insights into the structure of quantum state space.

For a complete set of $p+1$ unbiased measurement bases, the total collision entropy associated with any pure state is bounded from below by [23,34]

$$\sum_{B\in\{\infty,\mathbb{Z}_p\}} -\log \sum_V \left|\langle\phi|\psi_B^V\rangle\right|^4 \geqslant -(p+1)\log\frac{2}{p+1}. \quad (18)$$

The factor of 2 in the numerator arises from the surprising fact that $\sum_{B,V}|\langle\phi|\psi_B^V\rangle|^4 = 2$ for *any* pure state $|\phi\rangle$. The above inequality is saturated whenever $\sum_V |\langle\phi|\psi_B^V\rangle|^4$ is independent of the basis B, as occurs for SIC-POVM fiducial states [34]. For this reason fiducial states qualify as "minimum-uncertainty states" (not all minimum uncertainty states are fiducial vectors, however). MUB-balanced states [21] have the same probability distribution for all $p+1$ bases and consequently also saturate this lower bound.

Now, instead of collision entropy, consider the total min-entropy across a number of unbiased measurement bases. The following min-entropic uncertainty relation was proven for dimensions of the form $d=2^n$ in Ref. [24] and generally in Ref. [35]:

$$\sum_{B\in\{\infty,\mathbb{Z}_d\}} H_{\min}^B(|\phi\rangle) \geqslant -(d+1)\log\left[\frac{1}{d}\left(1+\frac{d-1}{\sqrt{d+1}}\right)\right].$$

Later we will interested in the case there we omit the computational basis and restrict to prime-dimensional systems so the relevant lower bound becomes

$$\sum_{B\in\mathbb{Z}_p} H_{\min}^B(|\phi\rangle) \geqslant -p\log\left[\frac{1}{p}\left(1+\frac{p-1}{\sqrt{p}}\right)\right]. \quad (19)$$

As well as constraining quantum state space, the above entropic quantities have an operational meaning in the context of cryptography [20,23,36,37]. As explained in, e.g., Ref. [38], if the four possible signal states transmitted from Alice to Bob in the BB'84 quantum key distribution protocol [39] are the eigenstates of σ_x and σ_y, then the optimal measurement basis (see Fig. 1) for Eve's intercept-resend attack is the basis of magic states $\{|f_{1,0,0}\rangle,|f_{1,0,1}\rangle\}$ better known as $\{|H\rangle,|H^\perp\rangle\}$ in the context of quantum computation or the Breidbart basis

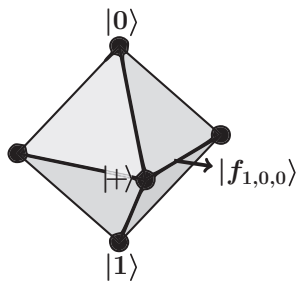

FIG. 1. The Breidbart basis $\{|f_{1,0,0}\rangle,|f_{1,0,1}\rangle\}$ (which is equal to $\{|H\rangle,|H^\perp\rangle\}$ in the magic state notation of Bravyi and Kitaev [54]) constitutes the optimal measurement basis for Eve if her goal is to infer as much information about Alice's state as possible. The cryptographic protocol [38–40] assumes Alice is sending one of the four equatorial Pauli eigenstates.

in cryptographic settings [38–40]. This basis, which can be thought of as splitting the difference between the σ_x and σ_y bases, allows Eve to ascertain Alice's information with probability $\frac{1}{2}(1+\frac{1}{\sqrt{2}})\approx 85\%$ (which is the optimal value of the CHSH nonlocal game), and the state $|H^{(\perp)}\rangle$ minimizes the average min-entropy for the X and Z basis measurements [20,41]. Finding higher-dimensional analogues of the Breidbart basis motivated Amburg *et al.* [21] to investigate MUB-balanced states. We shall see how qudit magic states obey many of the same desirable properties of the Breidbart basis.

III. RESULTS

Our results are broken up into two subsections, the first of which concerns nonlocality, while the second concerns entropic uncertainty. In the first subsection, we find a simple expression for the eigenbasis of the CHSH-Bell operator (13), which, after the application of a result from number theory, allows us to place good bounds on the quantum value of the restricted (to Pauli measurements) CHSH game. In the second subsection, we examine magic states in terms of their ability to minimize the total (or average) entropy across a number of different measurement bases. For this purpose we use collision entropy and min-entropy, both of which have operational significance in cryptographic settings. Among the subset of qudit states that we call equatorial states, magic states always minimize the collision entropy, and for small prime dimension they also simultaneously minimize the min-entropy.

A. Optimal strategy for CHSH game and bounds on the achievable value

Rewrite the Bell operator $\mathcal{B}^*$ of Eq. (12) in the Weyl-Heisenberg basis using Eq. (14),

$$\mathcal{B}^* = \frac{1}{p}\sum_{n\in\mathbb{Z}_p^*,x,s\in\mathbb{Z}_p}\left(\omega^{s(s+\frac{1}{2})}D_{(1,1|x,s-x)}\right)^n, \quad (20)$$

and note that conjugation by a Clifford gate $C^\dagger$ has the effect

$$C^\dagger D^n_{(1,1|x,s-x)}C = D^n_{(1,0|s,s-x)},$$

where

$$C := CSUM_{12} = \sum_k |k\rangle\langle k|\otimes X^k : |j,k\rangle \mapsto |j,k+j\rangle$$

is the generalized CNOT (Controlled-NOT) operator. Under this unitary operation the Bell operator becomes

$$C^\dagger\mathcal{B}^*C = \frac{1}{p}\sum_{n\in\mathbb{Z}_p^*,x,s\in\mathbb{Z}_p}\left(\omega^{s(s+\frac{1}{2})}D_{(1,0|s,s-x)}\right)^n \quad (21)$$

$$= p\mathcal{S}^*\otimes|0\rangle\langle 0| \quad (22)$$

with

$$\mathcal{S}^* = \frac{1}{p}\sum_{n\in\mathbb{Z}_p^*,s\in\mathbb{Z}_p}\left(\omega^{s(s+\frac{1}{2})}D_{(1|s)}\right)^n \quad (23)$$

and

$$\mathcal{S} = \frac{1}{p} \sum_{n,s\in\mathbb{Z}_p} \left(\omega^{s(s+\frac{1}{2})} D_{(1|s)}\right)^n \tag{24}$$

so that $\mathcal{S} = \mathcal{S}^* + p\mathbb{I}_p$ and $\lambda_{\max}(\mathcal{S}) = \lambda_{\max}(\mathcal{S}^*) + p$ as before. By the definition of stabilizer projectors in Eq. (2) we have

$$\mathcal{S} = \sum_B \left|\psi_B^{-B(B+\frac{1}{2})}\right\rangle\!\left\langle\psi_B^{-B(B+\frac{1}{2})}\right|; \tag{25}$$

i.e., $\mathcal{S}$ is a sum of projectors, one from each of the noncomputational bases. The final step is to note that $\lambda_{\max}(\mathcal{B}^*) = \lambda_{\max}(p\mathcal{S}^* \otimes |0\rangle\langle 0|) = \lambda_{\max}(p\mathcal{S}^*)$ so that

$$\lambda_{\max}(\mathcal{B}) = p\lambda_{\max}(\mathcal{S}). \tag{26}$$

Overall, we find that the maximizing eigenvector of the Bell operator $\mathcal{B}$ gives an expectation that is the same as maximizing a simple single-qudit operator $\mathcal{S}$. Moreover, $\mathcal{S}$ is a sum of p stabilizer projectors, one from each of the noncomputational stabilizer bases. We will show that $\mathcal{S}$ is maximized by a magic state $|f_{a,b,c}\rangle$ as in Eq. (4). It follows that the optimum quantum strategy for our restricted CHSH game is for Alice and Bob to measure a shared state $|J_{a,b,c}\rangle$ of Eq. (7) since

$$\begin{aligned}\langle J_{a,b,c}|\mathcal{B}^*|J_{a,b,c}\rangle &= \langle f_{a,b,c},0|C^\dagger\mathcal{B}^*C|f_{a,b,c},0\rangle \\ &= p\langle f_{a,b,c},0|\left(\mathcal{S}^*\otimes|0\rangle\langle 0|\right)|f_{a,b,c},0\rangle \\ &= p\langle f_{a,b,c}|\mathcal{S}^*|f_{a,b,c}\rangle \\ &= p\lambda_{\max}(\mathcal{S}^*).\end{aligned}$$

In Sec. IV we prove that the magic state $|f_{a,b,c}\rangle$, with $a = -1/12$ and $b = -1/8$ is a maximizing eigenvector for the single-qudit operator $\mathcal{S}$ for $p > 3$. Moreover, we show that all magic states are balanced with respect to Alice and Bob's measurements projectors given in Eq. (2), i.e.,

$$\left\{\left|\left\langle\psi_B^V|f_{a,b,c}\right\rangle\right|, V\in\mathbb{Z}_p\right\} \quad \text{independent of basis } B. \tag{27}$$

Our proof provides an explicit expression showing exactly how probabilities $|\langle\psi_B^V|f_{a,b,c}\rangle|^2$ are permuted between different bases. For the magic state $|f_{-1/12,-1/8,c}\rangle$ under consideration, the overlap with vector V_B in basis B is constant whenever

$$V_B = -B\left(B+\tfrac{1}{2}\right). \tag{28}$$

Combining this with Eq. (25) we find

$$\lambda_{\max}(\mathcal{S}) = \sum_B \left|\langle\psi_B^{-B(B+\frac{1}{2})}|f_{-1/12,-1/8,c}\rangle\right|^2 \tag{29}$$

$$= p|\langle +|f_{-1/12,-1/8,c}\rangle|^2. \tag{30}$$

All overlaps between (noncomputational) MUB vectors and magic states take the same form, viz.,

$$\left|\left\langle\psi_B^V|f_{a,b,c}\right\rangle\right|^2 = \frac{1}{p}\left|\sum_k \omega^{ak^3+(b-2^{-1}B)k^2+(c-V)k}\right|^2. \tag{31}$$

The values of these overlaps are constrained by the Weil bound [42,43], which says that a polynomial f of degree n over a prime field $\mathbb{Z}_p$ satisfies

$$\left|\sum_x \omega^{f(x)}\right| \leqslant (n-1)\sqrt{p} \tag{32}$$

TABLE I. Comparison of the bounds imposed by Information Causality (first column) and Weil (second column) with the optimal quantum and local hidden variable strategies (third and fourth columns). The LHV lower bounds are reproduced from Ref. [10] whereas the operator norm $\langle\mathcal{B}\rangle_{\max}^{\mathrm{QM}}$ is attained by measuring the maximally entangled states $|J_{a,b,c}\rangle$. Because we have restricted ourselves to Pauli measurements, the quantity $\langle\mathcal{B}\rangle_{\max}^{\mathrm{QM}}$ is less than what is achievable in the unrestricted case.

p	$p(1+\frac{p-1}{\sqrt{p}})$	4p	$\langle\mathcal{B}\rangle_{\max}^{\mathrm{QM}}$	$\langle\mathcal{B}\rangle_{\max}^{\mathrm{LHV}}$
3	6.4641	–	6.4115	6
5	13.9443	20	13.0902	12
7	22.8745	28	19.4112	19
11	44.1662	44	34.6464	37
13	56.2666	52	48.3481	47
17	82.9697	68	55.1022	$\geqslant$66
19	97.4602	76	72.6084	$\geqslant$79
23	128.508	92	74.8954	$\geqslant$99
29	179.785	116	104.819	$\geqslant$135

provided p does not divide n. Applied to Eq. (30) the above bound implies

$$\langle\mathcal{B}\rangle_{\max}^{\mathrm{QM}} = \lambda_{\max}(\mathcal{S}) \leqslant 4p. \tag{33}$$

For $p > 7$ this bound is more restrictive than the Information Causality bound. In Table I we compare this bound with $\lambda_{\max}(\mathcal{S}) = \langle\mathcal{B}\rangle_{\max}^{\mathrm{QM}}$ and with the bound $p(1+\frac{p-1}{\sqrt{p}})$ imposed by Information Causality.

The qutrit case must be handled individually; terms like $-1/12$ are ill-defined and the Weil bound is not applicable. One can explicitly check that the optimal quantum state for Alice and Bob to measure is what we have come to expect, i.e., a maximally entangled state that is isomorphic to a magic state,

$$\langle\mathcal{B}\rangle_{\max}^{\mathrm{QM}} = \langle J_{1,1,0}|\mathcal{B}|J_{1,1,0}\rangle = 3\sqrt{3}\cos(\pi/18) = 6.4115. \tag{34}$$

Liang *et al.* [10] have shown that this is truly the quantum maximum; even allowing for POVMs this value cannot be surpassed.

B. Minimum uncertainty equatorial states

Define a generalized equatorial state in terms of a vector of phases $\vec{\phi} = (\phi_0 := 0, \phi_1, \ldots, \phi_{p-1})$,

$$|\psi_{eq}(\vec{\phi})\rangle = \frac{1}{\sqrt{p}}\sum_{k=0}^{p-1} e^{i\phi_k}|k\rangle. \tag{35}$$

This state has $p-1$ free real parameters, which is exactly half the number of parameters that specify an arbitrary pure state. This is already a very important class of states for cryptographic protocols, e.g., optimal cloning procedures are known for states of this form [44,45].

The total collision-entropic uncertainty across p noncomputational Pauli bases is bounded from below by

$$\sum_{B\in\mathbb{Z}_p} -\log\sum_V \left|\langle\psi_{eq}(\vec{\phi})|\psi_B^V\rangle\right|^4 \geqslant -p\log\left(\frac{2-\frac{1}{p}}{p}\right) \tag{36}$$

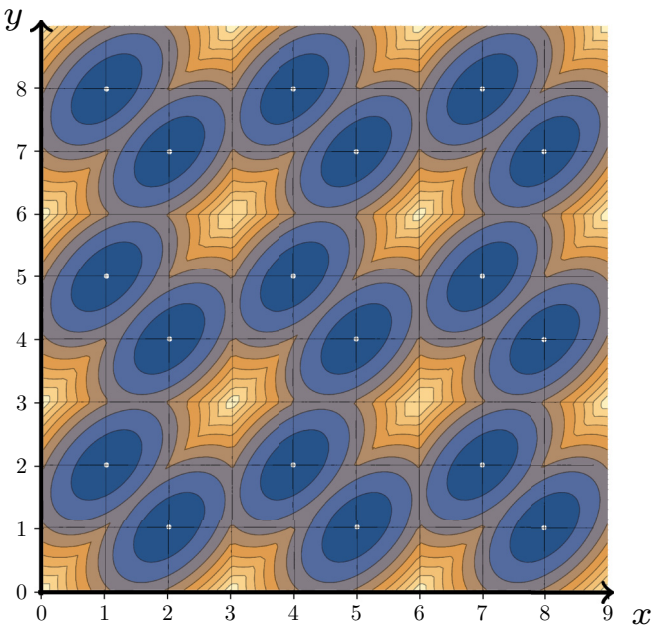

FIG. 2. (Color online) Total min-entropy across three different bases: This plot shows contours of the total uncertainty for equatorial qutrit states parameterized as $|\psi_{eq}(\vec{\phi})\rangle = (1,\xi^x,\xi^y)/\sqrt{3}$ with $0 \leqslant x,y \leqslant 9 \in \mathbb{R}$ and $\xi = e^{2\pi i/9}$. The minimum uncertainty states occur at the small white dots, which are integer values of x,y such that $x = 2a + 6b + 3c \bmod 9$ and $y = a + 6b + 6c \bmod 9$ with $a \in \mathbb{Z}_3^*$ and $b,c \in \mathbb{Z}_3$. In other words, magic states $|f_{a,b,c}\rangle$ as defined in Eq. (6) are minimum uncertainty states among the set of equatorial states. This optimality of magic states $|f_{a,b,c}\rangle$ holds numerically for prime dimensions $p \in \{2,3,5,7\}$ but not for $p = 11$ or $p = 13$.

since $\sum_V |\langle\psi_{eq}(\vec{\phi})|V\rangle|^4 = 1/p$ and we already know from Eq. (18) that the sum over all $p+1$ bases is identically 2 for any pure state. Because of the balancedness property of $|f_{a,b,c}\rangle$ proven in Sec. IV we have that $\sum_V |\langle f_{a,b,c}|\psi_B^V\rangle|^4$ is independent of B and therefore the above inequality is saturated. In summary, of all equatorial states (35) it turns out that magic states minimize the total collision entropy and saturate the above entropic uncertainty relation.

Using magic states, we will not generally be able to saturate the lower bound of Eq. (19) on the total min-entropy across p mutually unbiased measurements. However, for small prime dimensions, it is feasible to check numerically whether magic states minimize the total min-entropy when we restrict to the manifold of equatorial states defined in Eq. (35). To that end define

$$\vec{\phi}_{\min} = \operatorname*{argmin}_{\vec{\phi}} \sum_{B\in\mathbb{Z}_p} H_{\min}^B[|\psi_{eq}(\vec{\phi})\rangle]. \tag{37}$$

For qutrits, see Fig. 2, we find that

$$\begin{aligned}\vec{\phi}_{\min} &= (0,\phi_1,\phi_2)\\ &= \frac{2\pi}{9}(0,2a+6b+3c,a+6b+6c),\end{aligned} \tag{38}$$

whereas for primes $p = 5$ or $p = 7$ we find

$$\vec{\phi}_{\min} = (\ldots,\phi_k,\ldots) = \frac{2\pi}{p}(ak^3 + bk^2 + ck). \tag{39}$$

TABLE II. Different characterizations of seven-dimensional magic states: Magic states have surprising additional structure in prime dimensions of the form $p = 1 \bmod 3$ [29], which opens the door for operational inequivalence of magic states $|f_{a,b,c}\rangle$ depending on the value of the parameter $a \in \{1,2,\ldots,p-1\}$. The nonzero elements of $\mathbb{Z}_7$ can be partitioned into equivalence classes of cubic residues and their cosets, i.e., $\mathbb{Z}_7^* = \{1,6\} \cup \{2,5\} \cup \{3,4\}$. Depending on which of the operationally relevant quantities ($W_{\min}$, Mana, or $\sum_B H_{\min}^B$) we focus on, we find a different choice of optimal equivalence class. The quantity $W_{\min}$ denotes the minimal value of the Wigner function of $|f_{a,b,c}\rangle$ in phase space [17], while Mana effectively describes the magnitude of the sum of all the negative entries [18]. The last column describes the total min-entropy of $|f_{a,b,c}\rangle$ across all measurement bases $\{X,XZ,\ldots,XZ^{p-1}\}$. Note that lower bound for arbitrary (not necessarily equatorial) states is $7.693 = -7\log[(1+(7-1)/\sqrt{7})/7]$ so the magic state performs well.

a	$W_{\min}$	Mana	$\sum_B H_{\min}^B$
1	−0.027 692	0.814 835	7.870 55
2	−0.089 915	0.814 835	12.3287
3	−0.034 531	0.896 212	9.351 25
4	−0.034 531	0.896 212	9.351 25
5	−0.089 915	0.814 835	12.3287
6	−0.027 692	0.814 835	7.870 55

This set of phases is exactly what defines the magic states $|f_{a,b,c}\rangle$ in (4) and (6) In some cases the total min-entropy they achieve is quite close to the bound that applies to generic states, e.g,

$$p = 3: \quad \sum_{B\in\mathbb{Z}_p} H_{\min}^B|\psi_{eq}(\vec{\phi}_{\min})\rangle = 1.468 \tag{40}$$

(where we used $\log_2$), which is not much greater than the lower bound

$$-3\log_2\left[\frac{1}{3}\left(1+\frac{2}{\sqrt{3}}\right)\right] = 1.4324. \tag{41}$$

Similarly for $p = 5$ we get $4.667 > 4.2113$ and for $p = 7$ (see Table II) we get $7.871 > 7.693$. For $p = 11$ we find a counterexample to the optimality of $|f_{a,b,c}\rangle$, i.e., we find $\sum_{B\in\mathbb{Z}_p} H_{\min}^B|f_{a,b,c}\rangle = 19.8465 > 15.994$ but there is another nonmagic equatorial state that achieves 17.7606. For $p = 13$ a magic state of the form $|f_{4,b,c}\rangle$ achieves $23.471 > 20.6267$, but this can also be beaten by a nonmagic equatorial state that achieves a total min-entropy of 23.1336.

Minimum uncertainty states are defined relative to a particular notion of entropy and we have chosen two instances that appear to have both operational and geometrical interpretations. Besides the collision entropy H_2 and the min-entropy $H_{\alpha=\infty}$, the general Renyi entropy H_α is well defined for a one parameter family $\alpha \geqslant 0$, so it could be the case that magic states also minimize uncertainty for other values of α. Minimum uncertainty states can also be defined relative to the Shannon entropy (see, e.g., Ref. [46]), but the results so obtained are qualitatively very different.

IV. THEOREMS AND PROOFS

This section contains the two key mathematical results and their proofs. Many of their implications have already been used in preceding sections. The definitions and notation were established in Sec. II A:

Theorem 1. The magic state $|f_{a,b,c}\rangle$, with $a=-1/12$ and $b=-1/8$ is a maximizing eigenvector for the single-qudit operator $\mathcal{S}$ (25) for all prime dimensions $p>3$.

We claim that the eigenbasis that diagonalizes $\mathcal{S}$ is given by the set of orthogonal magic states $\{|f_{-1/12,-1/8,c}\rangle, c\in\mathbb{Z}_p\}$. The proof is obtained by constructing a unitary U with these states as columns and showing that conjugating $\mathcal{S}$ with $U^\dagger$ produces a diagonal matrix D:

$$\text{Claim}: \; D=U^\dagger \mathcal{S} U=\begin{pmatrix}\lambda_1(\mathcal{S}) & 0 & 0\\ 0 & \ddots & 0\\ 0 & 0 & \lambda_p(\mathcal{S})\end{pmatrix},$$

where $\lambda_i(\mathcal{S})$ are the eigenvalues in no particular order. Perform matrix multiplication to find the explicit matrix elements $d_{j,k}$ of our putative diagonal matrix, D, i.e.,

$$\begin{aligned} D&=\sum_{j,k} d_{j,k}|j\rangle\langle k| = U^\dagger \mathcal{S} U\\ &=\left(\sum_{g,h}\omega^{\frac{g^3}{12}+\frac{g^2}{8}+gh}|g\rangle\langle h|\right)\mathcal{S}\\ &\quad\times\left(\sum_{l,m}\omega^{-(\frac{m^3}{12}+\frac{m^2}{8}+lm)}|l\rangle\langle m|\right).\end{aligned}$$

Next, insert

$$\mathcal{S}=s_{u,v}|u\rangle\langle v|=\sum_B \omega^{\frac{B}{2}(u^2-v^2)+B(B+\frac{1}{2})(u-v)}|u\rangle\langle v|,$$

which is a consequence of Eqs. (25) and (3). After some tidying and relabeling we find

$$d_{j,k}=\sum_{A,B,C\in\mathbb{Z}_p}\omega^{\frac{1}{12}(A^3-C^3)+(\frac{B}{2}+\frac{1}{8})(A^2-C^2)+(\frac{B}{2}+B^2)(A-C)+kC-jA}.$$

Perform the linear substitution

$$\begin{aligned}&(A,B,C)\mapsto(\tilde{A}+\tilde{C},\tilde{B}-\tilde{A}/2-1/4,\tilde{A}-\tilde{C})\\ &\Rightarrow\; d_{j,k}=\sum_{\tilde{A},\tilde{B},\tilde{C}\in\mathbb{Z}_p}\omega^{\frac{\tilde{C}^3}{6}+\tilde{C}(-\frac{1}{8}+2\tilde{B}^2-j-k)+\tilde{A}(k-j)},\end{aligned}$$

which satisfies

$$d_{j,k\neq j}=0$$

because

$$\sum_{\tilde{A}\in\mathbb{Z}_p}\omega^{\tilde{A}(k-j)}=p\delta_{k,j}.$$

Hence D is diagonal, as claimed. ■

Theorem 2. All magic states $|f_{a,b,c}\rangle$ are MUB-balanced with respect to the mutually unbiased measurements $\{X, XZ, \ldots, XZ^{p-1}\}$. Moreover, the V_B-th coefficient in the B-th basis is given by the V_0-th coefficient in the X measurement basis when $V_B=V_0+\frac{1}{12a}(B^2-4Bb)$.

First, define the quantity $T_{a,b,c}$ as

$$T_{a,b,c}=\frac{1}{p}\left|\sum_k \omega^{ak^3+bk^2+ck}\right|$$

and note that, after a linear substitution $k\mapsto k+r$ (where r is some fixed element $r\in\mathbb{Z}_p$) that does not change the value of the sum, we find

$$T_{a,b,c}=T_{a,b+3ar,c+2br+3ar^2}. \tag{42}$$

Take the probability $c_{V_0,0}$ associated with an arbitrary vector V_0 in the first measurement basis, $B=0$:

$$\begin{aligned}c_{V_0,0}&=\left|\langle\psi_0^{V_0}|f_{a,b,c}\rangle\right|^2=\frac{1}{p}\left|\sum_k\omega^{ak^3+bk^2+(c+V_0)k}\right|^2\\ &=T_{a,b,c+V_0}.\end{aligned} \tag{43}$$

Now consider a vector V_B in any other basis B:

$$\begin{aligned}c_{V_B,B}&=\left|\langle\psi_B^{V_B}|f_{a,b,c}\rangle\right|^2=\frac{1}{p}\left|\sum_k\omega^{ak^3+(b-B/2)k^2+(c+V_B)k}\right|^2\\ &=T_{a,b-B/2,c+V_B}.\end{aligned} \tag{44}$$

Then, with the aid of Eq. (42), we find the condition that makes Eqs. (43) and (44) equal:

$$c_{V_0,0}=c_{V_B,B},\quad \forall B\in\mathbb{Z}_p, \tag{45}$$

$$\Rightarrow V_B=V_0+\frac{1}{12a}(B^2-4Bb). \tag{46}$$

■

A geometrical argument for the balancedness of magic states was implicit in recent work of Blanchfield [47] (see the proof of Theorem 1 therein) although that study concerned relationships between different MUB constructions. Not only have we proven that magic states $|f_{a,b,c}\rangle$ are MUB-balanced, we have shown exactly which permutation of probabilities occurs when moving between bases.

This theorem applied to the magic state $|f_{-1/12,-1/8,c}\rangle$ that maximizes $\mathcal{S}$ gives

$$V_B=\frac{1}{12(-1/12)}[B^2-4B(-1/8)]=-B\left(B+\frac{1}{2}\right), \tag{47}$$

which makes intuitive sense given that

$$\mathcal{S}=\sum_B|\psi_B^{-B(B+\frac{1}{2})}\rangle\langle\psi_B^{-B(B+\frac{1}{2})}|. \tag{48}$$

Using the MUB decomposition introduced in the Sec. II C, the single-qutrit operator $\mathcal{S}$ looks like

$$\begin{aligned}\mathcal{S}&=|\psi_0^0\rangle\langle\psi_0^0|+|\psi_1^0\rangle\langle\psi_1^0|+|\psi_2^1\rangle\langle\psi_2^1|\\ \Rightarrow\;\mathcal{S}&\leftrightarrow\left(\begin{array}{c|c|c|c}1&5/3&5/3&2/3\\1&2/3&2/3&5/3\\1&2/3&2/3&2/3\end{array}\right),\end{aligned}$$

while the maximizing eigenstate takes the form

$$|f_{1,1,0}\rangle\langle f_{1,1,0}|\leftrightarrow\left(\begin{array}{c|c|c|c}1/3&0.7124&0.7124&0.0859\\1/3&0.2017&0.2017&0.7124\\1/3&0.0859&0.0859&0.2017\end{array}\right).$$

V. SYMMETRIES, CYCLERS, AND SATO-TATE

In this section we outline some symmetries of the states and operators that we have previously used. We then mention a connection between our work and that of Amburg *et al.* [21].

To begin, there is an obvious *asymmetry* associated with magic states $|f_{a,b,c}\rangle$; they treat the computational basis differently to the remaining Weyl-Heisenberg (Pauli) bases. There is nothing special about the computational Z basis; in fact we can exhaustively create all $p^2(p^2-1)$ single-qudit $|f\rangle$-type magic states by applying the Clifford unitary that maps $Z \mapsto X$ followed by (multiple applications) of the Clifford that maps $X \mapsto XZ$. Any of these magic states will be balanced with respect to all but one Pauli measurement bases. Conversely we lose nothing by restricting our analysis to the equatorial class of magic states that we have so far considered.

The b and c components of magic states are modified by the action of Pauli operators,

$$|f_{a,b,c}\rangle = D_{(x|z)}|f_{a,0,0}\rangle, \quad \begin{pmatrix} x \\ z \end{pmatrix} = \begin{pmatrix} -\frac{b}{3a} \\ c - \frac{b^2}{3a} \end{pmatrix}, \tag{49}$$

whereas changing the value of a in $|f_{a,b,c}\rangle$ requires at least a Clifford operation. In fact, in Ref. [29] it was shown that magic states $|f_{a,b,c}\rangle$ and $|f_{a',b',c'}\rangle$ with different values $a \neq a'$ are connected via a Clifford if and only if these values lie in the same equivalence class of cubic residues modulo p. The noticeable effect of this is that in prime dimensions $p = 1 \bmod 3$ there are three equivalence classes of magic state that have different operational and geometrical features. In Table II we examine seven-dimensional magic states in terms of different operationally relevant quantities and see interesting differences arising from the inequivalent classes.

One of the main approaches to finding minimum uncertainty states has been to find so-called MUB cyclers: a single unitary that, when repeatedly applied to a basis state, maps basis vectors from one basis to the next, eventually wrapping around cyclically to return to the original basis. Eigenstates of these unitaries are often minimum-uncertainty states. These unitaries are known to not exist in prime dimensions, so the unitary we define below is the best possible alternative (see also Ref. [48]); it cycles through all but one of the bases. Define a Clifford gate $C_{a,b,c}$ as follows:

$$C_{a,b,c} = M_{a,b,c} X M_{a,b,c}^{\dagger}, \tag{50}$$

then it follows from the definitions that $C_{a,b,c}|f_{a,b,c}\rangle = |f_{a,b,c}\rangle$. Consider $C := C_{-1/12,-1/8,c}$, then

$$C^r \left|\psi_0^0\right\rangle = \left|\psi_{-\frac{r}{2}}^{V_r}\right\rangle, \quad V_r = \frac{r}{2}\left(-\frac{r}{2} + \frac{1}{2}\right), \tag{51}$$

so that for $p = 5$ we find that repeated application of C takes us through the basis indices $(0,2,4,1,3,0,2,4,\ldots)$. It is fairly straightforward to prove the equivalent claim,

$$C\left|\psi_{-\frac{s}{2}}^{V_s}\right\rangle = \left|\psi_{-\frac{s+1}{2}}^{V_{s+1}}\right\rangle \quad \forall s \in \mathbb{Z}_p, \tag{52}$$

using the following argument:

$$MXM^{\dagger}\left|\psi_{-\frac{s}{2}}^{V_s}\right\rangle = MX\left|f_{\frac{1}{12},\frac{1-2s}{8},-(c+V_S)}\right\rangle, \tag{53}$$

$$= M\sum_k \omega^{\frac{(k-1)^3}{12} + \frac{(k-1)^2(1-2s)}{8} - (k-1)(c+V_s)}|k\rangle,$$

$$= M\left|f_{\frac{1}{12},-\frac{(2s+1)}{8},\frac{s}{2}-(c+V_S)}\right\rangle, \tag{54}$$

$$= \left|f_{0,-\frac{s+1}{4},\frac{s}{2}-V_S}\right\rangle, \tag{55}$$

$$= \left|\psi_{-\frac{s+1}{2}}^{V_s-\frac{s}{2}}\right\rangle = \left|\psi_{-\frac{s+1}{2}}^{V_{s+1}}\right\rangle. \tag{56}$$

Hence, magic states are eigenstates of MUB-cycling Clifford unitaries that cycle through p out of $p+1$ bases.

For prime dimensions $p > 3$ magic states [as defined in Eq. (4)] are equal weighted superpositions of roots of unity with a cubic polynomial in the exponent. Exponential sums are commonplace in number theory and many results are known. The distribution

$$\theta_{a,c} = \frac{\sum_k \omega^{ak^3+ck}}{2\sqrt{p}} \quad a \in \mathbb{Z}_p^*, \quad c \in \mathbb{Z}_p \tag{57}$$

is real and lies in the range $[-1,1]$ [49,50]. The behavior of Eq. (57) for different values of a,c, and p is covered by the Sato-Tate conjecture (see Ref. [49], Sec. 1.4). Hence, magic states $|f_{a,0,c}\rangle$ obey the same semicircular distribution of values $-\frac{2}{\sqrt{p}} \leqslant \langle +|f_{a,0,c}\rangle \leqslant \frac{2}{\sqrt{p}}$ observed by Amburg *et al.* [21,22,51] for their states $|\beta\rangle$ that are balanced with respect to all $p+1$ mutually unbiased bases. Also, $\theta_{a,c}$ becomes increasingly equidistributed as p grows to infinity [50] meaning that the Weil bound [Eq. (33)] is saturated in this limit.

VI. DISCUSSION AND CONCLUSIONS

Characterizing highly nonstabilizer states and their operational capabilities is important. Stabilizer states appear naturally within the context of fault-tolerant quantum computation and also as basis vectors for complete sets of mutually unbiased bases. Here we have picked out a natural family of highly nonstabilizer states and showed their optimality in terms of both nonlocality and minimizing entropic uncertainty, where we have restricted to Pauli measurements in both scenarios. Finding concise optimal solutions to problems like these is of independent interest.

Whenever Alice and Bob are restricted to using qudit Pauli measurements we cannot ever observe nonlocality by measuring a stabilizer state. This is due to the existence of a local, noncontextual hidden variable model for nonnegatively represented states in a particular discrete Wigner function [16,17,53]. By showing that magic states give the maximal violation relative to a stabilizer CHSH scenario, this gives an operational interpretation to the concept of being highly nonstabilizer. Similarly, a stabilizer state is a maximally uncertain state with respect to a set of mutually unbiased Pauli bases. By showing that magic states minimize the entropic uncertainty, this gives another operational characterization of their highly nonstabilizer character.

One could argue the case for a number of different ways of quantifying nonstabilizerness. The correct metric will most likely depend on the exact nature of the task for which this state or operation is a resource. In [18] two measures were put forward that were tailored toward fault-tolerant quantum computation via magic state distillation. The relative entropy between the test state and the closest positively represented state, as well as the sum negativity (the sum of all the negative quasiprobabilities in the discrete Wigner function) of the state were both highlighted. It is worth noting the disagreement

in Table II between the state $|f_{3,b,c}\rangle$ that Mana picks out as opposed to the state $|f_{1,b,c}\rangle$ that min-entropy picks out. Other studies have characterized nonstabilizer states and operations in terms of convex geometry [57] and in terms of frame potentials [58].

For qubits, the Tsirelson bound for the CHSH scenario can be saturated using Pauli measurements applied to a particular maximally entangled state. The maximally nonlocal state $|J_{1,0,0}\rangle$ (11) can be understood as the image of a "pi-over-eight" gate applied to one half of a Bell pair $|\Phi\rangle$. It is intuitively pleasing that this connection between optimality and the Clifford hierarchy continues for all higher prime values of p, as we have shown here. Less pleasing is that the quantum advantage diminishes with increasing dimension, and seems to disappear entirely for $p \geqslant 11$ [we highlight as an interesting open question whether *any* alternate choice of Pauli measurements (14) for Alice and Bob could result in $\lambda_{\max}(\mathcal{B}) > \langle\mathcal{B}\rangle_{\max}^{\mathrm{LHV}} = 37$]. For $p < 11$ it should be borne in mind that Ref. [13] showed a clear operational advantage for restricting to stabilizer measurements when statistical significance, rather than the amount of Bell inequality violation, is adopted as the figure of merit. One possible practical application of our results is the benchmarking of nonstabilizer resources for fault-tolerant computation. Any imperfect $|J_{a,b,c}\rangle$ (or equivalently $M_{a,b,c}$) that still allows for violation of the qudit Bell-CHSH inequality is also suitable for promoting fault-tolerant Clifford gates to universal quantum computation via magic state distillation [52]. This is a sufficient condition but not necessary, as the distillation routines of Ref. [26] can also enable universality with imperfect $|J_{a,b,c}\rangle$ that have lost the ability to violate the Bell inequalities [9] that we used here.

The interrelationship between entanglement, nonlocality, steering, complementarity, and uncertainty is a fascinating and ongoing research program. Oppenheim and Wehner [55] have shown that the presence of uncertainty limits the amount of nonlocality, whereas Tomamichel and Hänggi [56] have shown that uncertainty is necessary in order to observe nonlocality. In the qubit case, the similarity between the Information Causality bound of Eq. (17) and the entropic uncertainty bound of Eq. (19) arises because of these links between nonlocality and uncertainty. The fact that the qudit expressions also have the same form suggests that this connection may hold generally, although this is complicated by the fact that the qudit CHSH game is no longer an XOR game [11].

There are some obvious avenues for further investigation. Magic states $|f_{a,b,c}\rangle$ reflect the structure of the third level of the Clifford hierarchy and take a simple exponential sum form for higher dimensions. Both of these facets are amenable to further analysis using group-theoretical and number-theoretical ideas. Moreover, they both suggest natural generalizations for classes of states that may prove useful, analagous to what we have proven here. The Clifford hierarchy is well-defined for multiple particles (e.g., controlled-Clifford gates are elements of the third level) but for single-particle diagonal gates the relationship between hierarchy level and the order of polynomials in the exponential sum is more transparent. The Weil bound (33) suggests that states defined as exponential sums of higher order polynomials may sometimes perform better. Finally, as with all calculations over prime fields, it is worth investigating how many of our results carry over to the case where we consider systems of prime-power dimensions $q = p^r$ by using the field $\mathbb{F}_q$ rather than $\mathbb{F}_p$.

ACKNOWLEDGMENTS

We thank Jyrki Lahtonen for assistance regarding exponential sums, Earl Campbell for helpful suggestions, and Joel Wallman for comments on an early draft. The author acknowledges financial support from FQXi, CIFAR, and the Government of Canada through NSERC. This research was supported by the US Army Research Office through Grant No. W911NF-14-1-0103.

[1] A. Acín, T. Durt, N. Gisin, and J. I. Latorre, Quantum nonlocality in two three-level systems, Phys. Rev. A **65**, 052325 (2002).

[2] A. Acín, J. L. Chen, N. Gisin, D. Kaszlikowski, L. C. Kwek, C. H. Oh, and M. Zukowski, Coincidence Bell inequality for three three-dimensional systems, Phys. Rev. Lett. **92**, 250404 (2004).

[3] T. Durt, N. J. Cerf, N. Gisin, and M. Zukowski, Security of quantum key distribution with entangled qutrits, Phys. Rev. A **67**, 012311 (2003).

[4] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Proposed experiment to test local hidden-variable theories, Phys. Rev. Lett. **23**, 880 (1969).

[5] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Bell nonlocality, Rev. Mod. Phys. **86**, 419 (2014).

[6] H. Buhrman, R. Cleve, S. Massar, and R. de Wolf, Nonlocality and communication complexity, Rev. Mod. Phys. **82**, 665 (2010).

[7] B. W. Reichardt, F. Unger, and U. Vazirani, Classical command of quantum systems, Nature (London) **496**, 456 (2013).

[8] H. Buhrman and S. Massar, Causality and Tsirelson's bounds, Phys. Rev. A **72**, 052103 (2005).

[9] S.-W. Ji, J. Lee, J. Lim, K. Nagata, and H.-W. Lee, Multisetting Bell inequality for qudits, Phys. Rev. A **78**, 052103 (2008).

[10] Y.-C. Liang, C.-W. Lim, and D.-L. Deng, Reexamination of a multisetting Bell inequality for qudits, Phys. Rev. A **80**, 052116 (2009).

[11] M. Bavarian and P. W. Shor, Information Causality, Szemerdi-Trotter and Algebraic Variants of CHSH, arXiv:1311.5186 (2013).

[12] M. Pawłowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, and M. Żukowski, Information causality as a physical principle, Nature (London) **461**, 1101 (2009).

[13] B. Jungnitsch, S. Niekamp, M. Kleinmann, O. Gühne, H. Lu, W. Gao, Y. Chen, Z. Chen, and J. Pan, Increasing the statistical significance of entanglement detection in experiments, Phys. Rev. Lett. **104**, 210401 (2010).

[14] A. Acín, R. Gill, and N. Gisin, Optimal Bell tests do not require maximally entangled states, Phys. Rev. Lett. **95**, 210402 (2005).

[15] J. M. Renes, R. Blume-Kohout, A. J. Scott, and C. M. Caves, Symmetric informationally complete quantum measurements, J. Math. Phys. **45**, 2171 (2004).
[16] D. Gross, Hudson's theorem for finite-dimensional quantum systems, J. Math. Phys. **12**, 122107 (2006).
[17] V. Veitch, C. Ferrie, D. Gross, and J. Emerson, Negative quasi-probability as a resource for quantum computation, New J. Phys. **14**, 113011 (2012).
[18] V. Veitch, S. A. H. Mousavian, D. Gottesman, and J. Emerson, The resource theory of stabilizer quantum computation, New J. Phys. **16**, 013009 (2014).
[19] M. Howard, J. Wallman, V. Veitch, and J. Emerson, Contextuality supplies the magic for quantum computation, Nature (London) **510**, 351 (2014).
[20] S. Wehner and A. Winter, Entropic uncertainty relations – a survey, New J. Phys. **12**, 025009 (2010).
[21] I. Amburg, R. Sharma, D. M. Sussman, and W. K. Wootters, States that "look the same" with respect to every basis in a mutually unbiased set, J. Math. Phys. **55**, 122206 (2014).
[22] D. M. Appleby, I. Bengtsson, and H. B. Dang, Galois Unitaries, Mutually Unbiased Bases, and MUB-balanced states, arXiv:1409.7987 (2014).
[23] W. K. Wootters and D. M. Sussman, Discrete phase space and minimum-uncertainty states, arXiv:0704.1277 (2007).
[24] P. Mandayam, S. Wehner, and N. Balachandran, A. transform of complementary aspects with applications to entropic uncertainty relations, J. Math. Phys. **51**, 082201 (2010).
[25] E. T. Campbell, H. Anwar, and D. E. Browne, Magic state distillation in all prime dimensions using quantum Reed-Muller codes, Phys. Rev. X **2**, 041021 (2012).
[26] E. T. Campbell, Enhanced fault-tolerant quantum computing in d-level systems, Phys. Rev. Lett. **113**, 230501 (2014).
[27] M. Howard and J. Vala, Qudit versions of the qubit $\pi/8$ gate, Phys. Rev. A **86**, 022316 (2012).
[28] W. O. Alltop, Complex sequences with low periodic correlations, IEEE Trans. Inform. Theory **26**, 350 (1980).
[29] I. Bengtsson, K. Blanchfield, E. Campbell, and M. Howard, Order 3 symmetry in the Clifford hierarchy, J. Phys. A **47**, 455302 (2014).
[30] D. Gottesman and I. L. Chuang, Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations, Nature (London) **402**, 390 (1999).
[31] T. Lunghi, J. Kaniewski, F. Bussieres, R. Houlmann, M. Tomamichel, S. Wehner, and H. Zbinden, Practical relativistic bit commitment, arXiv:1411.4917 (2014).
[32] M. Navascues, S. Pironio, and A. Acín, Bounding the set of quantum correlations, Phys. Rev. Lett. **98**, 010401 (2007).
[33] I. D. Ivonovic, Geometrical description of quantal state determination, J. Phys. A **14**, 3241 (1981).
[34] D. M. Appleby, H. B. Dang, and C. A. Fuchs, Symmetric informationally-complete quantum states as analogues to orthonormal bases and minimum-uncertainty states, Entropy **16**, 1484 (2014).
[35] A. E. Rastegin, Uncertainty relations for MUBs and SIC-POVMs in terms of generalized entropies, Eur. Phys. J. D **67**, 269 (2013).
[36] J. M. Renes, Duality of privacy amplification against quantum adversaries and data compression with quantum side information, Proc. Royal Soc. A **467**, 1604 (2011).
[37] S. Wu, S. Yu, and K. Mø lmer, Entropic uncertainty relation for mutually unbiased bases, Phys. Rev. A **79**, 022104 (2009).
[38] M. Williamson and V. Vedral, Eavesdropping on practical quantum cryptography, J. Mod. Opt. **50**, 1989 (2003).
[39] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in *Proc. IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, New York, 1984), pp. 175–179.
[40] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, Experimental quantum cryptography, J. Cryptol. **5**, 3 (1992).
[41] H. Maassen and J. B. M. Uffink, Generalized entropic uncertainty relations, Phys. Rev. Lett. **60**, 1103 (1988).
[42] A. Weil, On some exponential sums, Proc. Natl. Acad. Sci. USA **34**, 204 (1948).
[43] E. Bombieri, On exponential sums in finite fields, Am. J. Math. **88**, 71 (1966).
[44] H. Fan, H. Imai, K. Matsumoto, and X. Wang, Phase-covariant quantum cloning of qudits, Phys. Rev. A **67**, 022317 (2003).
[45] V. Scarani, S. Iblisdir, N. Gisin, and A. Acín, Quantum cloning, Rev. Mod. Phys. **77**, 1225 (2005).
[46] P. J. Coles, L. Yu, and M. Zwolak, Relative entropy derivation of the uncertainty principle with quantum side information, arXiv:1105.4865 (2011).
[47] K. Blanchfield, Orbits of mutually unbiased bases, J. Phys. A **47**, 135303 (2014).
[48] D. M. Appleby, Properties of the extended Clifford group with applications to SIC-POVMs and MUBs, arXiv:0909.5233.
[49] T. D. Browning, Exponential sums over finite fields, Lecture Notes (2010), http://www.maths.bris.ac.uk/matdb/tcc/EXP/EXP.pdf
[50] R. Livné, The average distribution of cubic exponential sums, J. Reine Angew. Math. **375/376**, 362 (1987).
[51] N. M. Katz, Rigid local systems and a question of Wootters, Comm. Number Theor. Phys. **6**, 223 (2012).
[52] M. Howard and J. Vala, Nonlocality as a benchmark for universal quantum computation in Ising anyon topological quantum computers, Phys. Rev. A **85**, 022304 (2012).
[53] M. Howard, E. Brennan, and J. Vala, Quantum contextuality with stabilizer states, Entropy **15**, 2340 (2013).
[54] S. Bravyi and A. Kitaev, Universal quantum computation with ideal Clifford gates and noisy ancillas, Phys. Rev. A **71**, 022316 (2005).
[55] J. Oppenheim and S. Wehner, The uncertainty principle determines the nonlocality of quantum mechanics, Science **330**, 1072 (2010).
[56] M. Tomamichel and E. Hänggi, The link between entropic uncertainty and nonlocality, J. Phys. A **46**, 055301 (2013).
[57] W. van Dam and M. Howard, Noise thresholds for higher-dimensional systems using the discrete Wigner function, Phys. Rev. A **83**, 032310 (2011).
[58] D. Andersson, I. Bengtsson, K. Blanchfield, and H. B. Dang, States that are far from being stabilizer states, arXiv:1412.8181 (2014).