Maximum nonlocality and minimum uncertainty using magic states
Mark Howard
Phys. Rev. A 91, 042103 — Published 6 April 2015
DOI: 10.1103/PhysRevA.91.042103
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

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 non-stabilizer. The optimal strategy for a qudit version of the Clauser-Horne-Shimony-Holt (CHSH) 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.

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 Tsirelson’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 non-stabilizer states, measurements (see e.g [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 non-classical [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 only exist in odd prime-power dimensions of the form \(d = 3 \mod 4\). A MUB-balanced state is automatically also a collision-entropic minimum uncertainty [22, 23] (or maximally certain [24]) state, important in cryptography, but balanced-ness is a stricter condition than minimum uncertainty. From a foundational point of view, MUB-balanced states are analogous to harmonic oscillator eigenstates insofar as the “direction” of a measurement is unimportant. Our results include a concise proof that magic states are balanced (as the “direction” of a measurement is independent of the choice of measurement). 

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

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

\[
M_{a,b,c} |+\rangle \quad a, b, c \in \mathbb{Z}_p
\]

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.,

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

where \(\gamma = e^{2\pi i / 8}\) and \(\xi = e^{2\pi i / 3}\) and \(a, b, c \in \mathbb{Z}_p\). 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 \(|f_{a,b,c}\rangle|f_{a,b',c'}\rangle| = \delta_{b,b'}\delta_{c,c'} + (1 - \delta_{b,b'})/\sqrt{p}\) [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:

\[
|J_{a,b,c}\rangle = \mathbb{I}_p \otimes M_{a,b,c} |\Phi\rangle, \quad |\Phi\rangle = \sum_{j} |jj\rangle/\sqrt{p}.
\]

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

The group of operations generated by (tensor products of) the Weyl-Heisenberg operators in Eq. (1) is the Pauli group (we denote it \(C_1\) for reasons that will become clear). The set of unitaries that map the Pauli group into itself under conjugation is the Clifford group \(C_2\). The unitaries that map the Pauli group into the Clifford group, under conjugation, define [30] the third level of the Clifford hierarchy, \(C_3\), and so on. Overall we have

\[
C_k := \{U | U C_j U^\dagger \subseteq C_{k-1}\}
\]

where \(C_1 \subseteq C_2 \subseteq C_3 \ldots \) but the sets \(C_{k}>1\) 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 \(C_3\) for multiple qubits are discussed in [30] whereas the diagonal single-qudit subset of \(C_3\) as discussed in [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 \((B)_{\text{LHV}} \leq 2\) with a Bell operator

\[
B = XX + YY + YX - YX = \sum_{x,y=0}^1 \omega^{xy} A_x B_y
\]

where \(\{A_0, A_1\} = \{B_0, B_1\} = \{X, Y\}\).
and $\omega = -1$ is a $p$-th 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, $\lambda_{\text{max}}(B)$, 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.,

$$\langle B\rangle_{\text{max}}^{\text{QM}} = \langle J_{1,0,0} | B | J_{1,0,0} \rangle = 2\sqrt{2}. \quad (11)$$

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

$$B_* = \frac{1}{p} \sum_{n \in \mathbb{Z}_p} \sum_{x,y \in \mathbb{Z}_p} \omega^{nxy} A^n_x A^n_y, \quad (12)$$

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

where $\omega = e^{2\pi i/p}$ so that $B = B_* + p\mathbb{1}$ and consequently $\lambda_{\text{max}}(B) = \lambda_{\text{max}}(B_*) + p$. The traceless version $B_*$ is more convenient to work with but the maximal value of $B$ is a more useful quantity.

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

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

where $x, y \in \mathbb{Z}_p$, so that $A_y/2 = B_y$. The operators $\{D_{||x||}, D_{||y/2||} \}$ 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 $B$ from Eq. (13) can be related to the quantum value, $0 \leq \nu \leq 1$, of a nonlocal game [5, 6], which takes the general form

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

for measurement settings $(x,y)$, outcomes $(a,b)$ and a predicate or pay-off 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 $V(a,b,x,y) = \delta_{a+b+x,y,0}$ we arrive at

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

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 [10]).

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

$$\vec{a} = (a_0, \ldots, a_{p-1}) \in \mathbb{Z}_p^n$$

$$\vec{b} = (b_0, \ldots, b_{p-1}) \in \mathbb{Z}_p^n$$

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

$$A_x \mapsto \omega^{a_x}, \quad B_y \mapsto \omega^{b_y}. \quad \text{The best choices of } \vec{a} \text{ and } \vec{b} \text{ maximize the quantity}$$

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

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

$$\langle B \rangle_{\text{max}}^{\text{LHV}} \geq 3p - 2.$$

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

$$\nu \leq \text{IC}(p) := \frac{1}{p} \left( 1 + \frac{p-1}{\sqrt{p}} \right) \quad (17)$$

Clearly this implies $\langle B \rangle_{\text{max}}^{\text{QM}} \leq p^2 \text{IC}(p)$ but it also applies to more general scenarios wherein Alice and Bob use POVMs. It is also shown [11] that classical strategies can achieve $\Omega\left( \frac{1}{\sqrt{q}} \right)$ if $q = p^k$ or $O \left( \frac{1}{\sqrt{q^{k-1}}} \right)$ if $q = p^{2k-1}$ for a very small ($\leq \frac{1}{700}$) positive constant $\epsilon_0$. 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 $\nu$ from above and it appears that the values so obtained coincide with $\text{IC}(p)$ 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:

$$K \leftrightarrow \begin{pmatrix} c_{0,\infty} & c_{0,0} & c_{0,1} & c_{0,2} \\ c_{1,\infty} & c_{1,0} & c_{1,1} & c_{1,2} \\ c_{2,\infty} & c_{2,0} & c_{2,1} & c_{2,2} \end{pmatrix}$$

where

$$c_{\nu,B} = \langle \psi_B^\nu | K | \psi_B^\nu \rangle = \langle \psi_B^\nu \rangle \text{ from Eq. (3)}$$

and the infinity basis label corresponds to the computational basis i.e., $|\psi_{\infty}^\nu \rangle = |\psi \rangle$. 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]

\[
K = \sum_{B,V} c_{V,B}|\psi_B^V\rangle\langle\psi_B^V| - \text{Tr}(K)I_p.
\]

With the above decomposition in hand we can characterize a density matrix \( \rho \) 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 \( H_B^B(\rho) = -\log(\sum_V c_{V,B}^2) \) whereas the min-entropy is given by \( H_{\text{min}}(\rho) = -\log \max_V c_{V,B} \) [23, 24]. For an arbitrary pure state \( |\phi\rangle \in \mathbb{C}^p \) this can be rewritten as

\[
H_B^B(|\phi\rangle) = -\log \left( \sum_V |\langle\phi|\psi_B^V\rangle|^4 \right),
\]

\[
H_{\text{min}}^B(|\phi\rangle) = -\log \max_V |\langle\phi|\psi_B^V\rangle|^2,
\]

which obey

\[
\log(p) \geq H_B^B(|\phi\rangle) \geq H_{\text{min}}^B(|\phi\rangle) \geq 0.
\]

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]

\[
\sum_{B \in \{\infty,\mathbb{Z}_p\}} -\log \sum_V |\langle\phi|\psi_B^V\rangle|^4 \geq -p(p+1) \log \frac{2}{p+1}.
\]  

(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-entropy uncertainty relation was proven for dimensions of the form \( d = 2^n \) in [24] and generally in [35]

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

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

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

(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., [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 \( \sigma_x \) and \( \sigma_y \), 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 in cryptographic settings [38–40]. This basis, which can be thought of as splitting the difference between the \( \sigma_x \) and \( \sigma_y \) bases allows Eve to ascertain Alice’s information with probability \( \frac{1}{2}(1 + \sqrt{2}) \approx 85\% \), (which is the optimal value of the CHSH nonlocal game) and the state \( |H^{(2)}\rangle \) 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 qutrit 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 \( B^* \) of Eq. (12) in the Weyl-Heisenberg basis using Eq. (14)

\[
B^* = \frac{1}{p} \sum_{n \in \mathbb{Z}_p^3, x, s \in \mathbb{Z}_p} (\omega^{S(s+x)}D_{(1,1,1|x,s-x)})^n,
\]

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

\[
C^\dagger B^* C = \frac{1}{p} \sum_{n \in \mathbb{Z}_p^3, x, s \in \mathbb{Z}_p} (\omega^{S(s+x)}D_{(1,0,0|x,s-x)})^n,
\]

where

\[
C := CSU_{12} = \sum_k |k\rangle\langle k| \otimes X^k : |j, k) \mapsto |j, k + j\rangle
\]

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

\[
C^\dagger B^* C = \frac{1}{p} \sum_{n \in \mathbb{Z}_p^3, x, s \in \mathbb{Z}_p} (\omega^{S(s+x)}D_{(1,0,0|x,s-x)})^n = pS^* \otimes |0\rangle|0\rangle
\]

with

\[
S^* = \frac{1}{p} \sum_{n \in \mathbb{Z}_p^3, x, s \in \mathbb{Z}_p} (\omega^{S(s+x)}D_{(1|x)})^n
\]

and

\[
S = \frac{1}{p} \sum_{n, s \in \mathbb{Z}_p} (\omega^{S(s+x)}D_{(1|x)})^n
\]

so that \( S = S^* + p|\langle 0|0 \rangle| + p \) as before. By the definition of stabilizer projectors in Eq. (2) we have

\[
S = \sum_B \langle \psi_{B}^+ | B^+ \rangle (\psi_{B}^+ | B^+ \rangle^\dagger)
\]

i.e. \( S \) is a sum of projectors, one from each of the non-computational bases. The final step is to note that \( \lambda_{\text{max}}(B^*) = \lambda_{\text{max}}(pS^* \otimes |0\rangle|0\rangle) = \lambda_{\text{max}}(pS^*) \) so that

\[
\lambda_{\text{max}}(B) = p\lambda_{\text{max}}(S).
\]

Overall, we find that the maximizing eigenvector of the Bell operator \( B \) gives an expectation that is the same as maximizing a simple single-qudit operator \( S \). Moreover, \( S \) is a sum of \( p \) stabilizer projectors, one from each of the non-computational stabilizer bases. We will show that \( S \) 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

\[
\langle J_{a,b,c} | B^* | J_{a,b,c} \rangle = \langle f_{a,b,c} | \langle 0 | C^\dagger B^* C | f_{a,b,c} \rangle = p\langle f_{a,b,c} | (S^* \otimes |0\rangle) | f_{a,b,c} \rangle
\]

TABLE I. Comparison of the bounds imposed by Information Causality (first column) and Weil (second column) with the LHV lower bounds are reproduced in Sec. IV we prove that the magic state \( |f_{a,b,c}\rangle \) is a sum of \( p \) independent of basis \( B \). Because we have restricted ourselves to Pauli measurements, the quantity \( |B|^p \) is less than what is achievable in the unrestricted case.

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 \( S \) 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.,

\[
\{|\psi_{B}^+ | f_{a,b,c} \rangle, V \in \mathbb{Z}_p\} \quad \text{independent of basis} \ B \quad \text{(27)}
\]

Our proof provides an explicit expression showing exactly how probabilities \( |\langle \psi_{B}^+ | f_{a,b,c} \rangle|^2 \) 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

\[
V_B = -B \left( B + \frac{1}{2} \right).
\]

Combining this with Eq. (25) we find

\[
\lambda_{\text{max}}(S) = \sum_B |\langle \psi_{B}^+ | f_{-1/12,-1/8,c} \rangle|^2
\]

(29)

Overall, we find that the maximizing eigenvector of the Bell operator \( B \) gives an expectation that is the same as maximizing a simple single-qudit operator \( S \). Moreover, \( S \) is a sum of \( p \) stabilizer projectors, one from each of the non-computational stabilizer bases. We will show that \( S \) 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

\[
\langle J_{a,b,c} | B^* | J_{a,b,c} \rangle = \langle f_{a,b,c} | \langle 0 | C^\dagger B^* C | f_{a,b,c} \rangle = p\langle f_{a,b,c} | (S^* \otimes |0\rangle) | f_{a,b,c} \rangle
\]

(20)

(21)

(23)

(24)

(22)

(25)
All overlaps between (non-computational) MUB vectors and magic states take the same form viz.
\[
|⟨ψ_B^V|f_{a,b,c}\rangle|^2 = \frac{1}{p} \sum_k ω^{ak^2 + (b−2−1)k^2 + (c−V)k}|^2 \tag{31}
\]
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
\[
|\sum_x ω^{f(x)}| \leq (n − 1)\sqrt{p} \tag{32}
\]
provided \( p \) does not divide \( n \). Applied to Eq. (30) the above bound implies
\[
⟨B⟩_{\text{QM}} = \lambda_{\text{max}}(S) \leq 4p. \tag{33}
\]
For \( p > 7 \) this bound is more restrictive than the Information Causality bound. In Table I we compare this bound with \( \lambda_{\text{max}}(S) = ⟨B⟩_{\text{QM}} \) and with the bound \( p \left( 1 + \frac{p−1}{\sqrt{p}} \right) \) 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, \( ⟨B⟩_{\text{QM}} = ⟨\mathbf{J}_{1,1,0}|B|\mathbf{J}_{1,1,0}\rangle = 3\sqrt{3}\cos(π/18) = 6.4115. \tag{34} \)

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 \( \vec{ϕ} = (ϕ_0 := 0, ϕ_1, \ldots, ϕ_{p−1}) \),
\[
|ψ_{eq}(\vec{ϕ})⟩ = \frac{1}{\sqrt{p}} \sum_{k=0}^{p−1} e^{iϕ_k}|k⟩. \tag{35}
\]
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-entropy uncertainty across \( p \) non-computational Pauli bases is bounded from below by
\[
\sum_{B∈\mathbb{Z}_p} −\log \left( \sum_V |⟨ψ_{eq}(\vec{ϕ})|ψ_B^V⟩|^4 \right) \geq -p \log \left( \frac{2}{p} \right) \tag{36}
\]
since \( \sum_V |⟨ψ_{eq}(\vec{ϕ})|V⟩|^4 = 1/p \) 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} |⟨f_{a,b,c}|ψ_B^V⟩|^4 \text{ is independent of } B \text{ 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
\[
\tilde{ϕ}_{\text{min}} = \arg\min_{\vec{ϕ}} \sum_{B∈\mathbb{Z}_p} H^B_{\text{min}} \left( |ψ_{eq}(\vec{ϕ})⟩ \right). \tag{37}
\]
For qutrits, see Fig. 2, we find that
\[
\tilde{ϕ}_{\text{min}} = (0, ϕ_1, ϕ_2) \tag{38}
\]
\[
= \frac{2π}{9} (0, 2a + 6b + 3c, a + 6b + 6c)
\]
\[
FIG. 2. Total min-entropy across 3 different bases: This plot shows contours of the total uncertainty for equatorial qutrit states parameterized as \( |ψ_{eq}(\vec{ϕ})⟩ = (1, ξ^x, ξ^y)/\sqrt{3} \) with 0 \( \leq x, y \leq 9 \in \mathbb{R} \) and \( ξ = e^{2πi/9} \). The minimum uncertainty states occur at the small white dots, which are integer values of \( x, y := 2a + 6b + 3c \mod 9 \) and \( y = a + 6b + 6c \mod 9 \) 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 amongst the set of equatorial states. This optimality of magic states \( |f_{a,b,c}\rangle \) holds numerically for prime dimensions \( p = \{2, 3, 5, 7\} \) but not for \( p = 11 \) or \( p = 13 \).

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

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

(39)

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.,

$$
p = 3: \sum_{B \in \mathbb{Z}_p} H^B_{\min} |\psi_{eq}(\phi_{\min})\rangle = 1.468
$$

(40)

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

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

(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 $\sum_{B \in \mathbb{Z}_p} H^B_{\min} |f_{a,b,c}\rangle = 19.8465 > 15.994$ but there is another non-magic equatorial state that achieves $17.7606$. For $p = 13$ a magic state of the form $|f_{a,b,c}\rangle$ achieves $23.471 > 20.6267$ but this can also be beaten by a non magic 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 $H_{\infty}$, the general Renyi entropy $H_{\alpha}$ is well-defined for a one parameter family $\alpha \geq 0$, so it could be the case that magic states also minimize uncertainty for other values of $\alpha$. Minimum uncertainty states can also be defined relative to the Shannon entropy (see e.g. [46]) but the results so obtained are qualitatively very different.

IV. THEOREMS & 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 IV.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 $S_{\alpha}$ (25) for all prime dimensions $p > 3$.

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

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

where $\lambda_j(S)$ 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.,

$$
D = \sum_{j,k} d_{j,k} |j\rangle\langle k| = U^\dagger SU = \begin{pmatrix} \sum_{g,h} \omega^{-\frac{\psi_2}{2} + \frac{\psi_3}{2} + t|m|} |0\rangle \langle m| \end{pmatrix}
$$

Next, insert

$$
S = s_{a,v} |u\rangle\langle v| = \sum_B \omega^\frac{2}{3}(u^2-v^2)+B(u+v) |u\rangle\langle v|,
$$

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

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

Perform the linear substitution

$$
(A, B, C) \Rightarrow (A + \bar{C}, B - \bar{A} - 1/4, \bar{A} - \bar{C})
$$

$$
\Rightarrow d_{j,k} = \sum_{A, B, C \in \mathbb{Z}_p} \omega^{\bar{C}j + \bar{C}(\bar{A} + \bar{B}^2 - j) + \bar{A}(k-j)}
$$

which satisfies

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

because

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

Hence $D$ is diagonal, as claimed. ■

**Theorem IV.2** All magic states $|f_{a,b,c}\rangle$ are MUBs, 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 $V_B = V_0 + \frac{1}{125} (B^2 - 4Bb)$

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

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

\[
T_{a,b,c} = T_{a,b+3ar,c+2br+3ar^2}.
\] (42)

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

\[
c_{V_0,0} = |\langle \psi_0^V | f_{a,b,c} \rangle|^2 = \frac{1}{p} \sum_k \omega^{ak^3 + bk^2 + (c + V_0)k} = T_{a,b,c+V_0}
\] (43)

Now consider a vector \( V_B \) in any other basis \( B \)

\[
c_{V_B,0} = |\langle \psi_B^V | f_{a,b,c} \rangle|^2 = \frac{1}{p} \sum_k \omega^{ak^3 + (b - B/2)k^2 + (c + V_0)k} = T_{a,b-B/2,c+V_B}
\] (44)

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

\[
c_{V_0,0} = c_{V_B,0}, \quad \forall B \in \mathbb{Z}_p
\] (45)

\[
\Rightarrow V_B = V_0 + \frac{1}{12a} (B^2 - 4Bb)
\] (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 permutations of probabilities occur when moving between bases.

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

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

which makes intuitive sense given that

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

Using the MUB decomposition introduced in the Sec. II C, the single-qutrit operator \( S \) looks like

\[
S = |\psi_0^0\rangle\langle \psi_0^0 | + |\psi_0^1\rangle\langle \psi_0^1 | + |\psi_1^1\rangle\langle \psi_1^1 |,
\]

\[
\Rightarrow S \leftrightarrow \begin{pmatrix} 1 & 5/3 & 5/3 & 2/3 \\ 1 & 2/3 & 2/3 & 5/3 \\ 1 & 2/3 & 2/3 & 2/3 \end{pmatrix},
\]

while the maximizing eigenstate takes the form

\[
|f_{1,1,0}\rangle|f_{1,1,0}\rangle \leftrightarrow \begin{pmatrix} 1/3 & 0.7124 & 0.7124 & 0.0859 \\ 1/3 & 0.2017 & 0.2017 & 0.7124 \\ 1/3 & 0.0859 & 0.0859 & 0.2017 \end{pmatrix}.
\]

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 with, 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 all \( p^2(p^2 - 1) \) single-qubit \( |f\rangle \)-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,

\[
|f_{a,b,c}\rangle = D_{(a|z)}|f_{a,0,0}\rangle,
\]

\[
\begin{pmatrix} x \\ z \end{pmatrix} = \begin{pmatrix} x \\ -z \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{\sqrt{2}} \end{pmatrix}
\]

\[
|f_{a,b,c}\rangle = |f_{a',b',c}\rangle
\]

whereas changing the value of \( a \) in \( |f_{a,b,c}\rangle \) requires at least a Clifford operation. In fact, in [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 \( p = 1 \mod 3 \) there are \( 3 \) 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 [48]) – it cycles through all but one of the bases. Define a Clifford gate \( C_{a,b,c} \) as follows

\[
C_{a,b,c} = M_{a,b,c}X M_{a,b,c}^\dagger
\]

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

\[
C^r |\psi_0^V\rangle = |\psi_{Vc}^V\rangle, \quad Vc = \frac{r}{2} (\frac{5}{2} + \frac{1}{2})
\]

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
\[ C|ψ^{V_s}_{−\frac{1}{2}}⟩ = |ψ^{V_{s+1}}_{\frac{1}{2}}⟩ \quad ∀s \in \mathbb{Z}_p, \]  
using the following argument,
\[ MXM|ψ^{V_s}_{−\frac{1}{2}}⟩ = MXf|ψ^{(−1)^{k+1}}V_s}_{−\frac{1}{2}}⟩, \]  
\[ = M \sum_k \omega^{(k+1)\frac{s}{p} + (k-1)(1+2x)}(−(k-1)(c+V_s))|k⟩, \]
\[ = M|f_{\frac{s}{p} + (2s+1)(V_s)}⟩, \]
\[ = |ψ^{V_s}_{−\frac{1}{2}}⟩ = |ψ^{V_{s+1}}_{\frac{1}{2}}⟩. \]  

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
\[ \theta_{a,c} = \frac{\sum_k \omega^{ak^3+ck}}{\sqrt{p}} \quad a \in \mathbb{Z}_p, \; c \in \mathbb{Z}_p \]  
is real and lies in the range \([-1,1]\) [49, 50]. The behaviour of Eq. (57) for different values of \( a, c \) and \( p \) is covered by the Sato-Tate conjecture (see [49] Sec. 1.4). Hence, magic states \( |f_{a,b,c}⟩ \) obey the same semicircular distribution of values \(-\frac{2}{\sqrt{p}} \leq \langle |f_{a,b,c}⟩ \leq \frac{2}{\sqrt{p}}\) observed by Amburg et al. [21, 22, 51] for their states \( |β⟩ \) 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 non-stabilizer 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 non-stabilizer 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 non-negatively 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 non-stabilizer. 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 non-stabilizer character.

One could argue the case for a number of different ways of quantifying non-stabilizerness. 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 entries) [18]. The last column describes the total min-entropy of \( |f_{a,b,c}⟩ \) across all measurement bases \( \{X, ZX, \ldots, ZX^{p-1}\} \). 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.

<table>
<thead>
<tr>
<th>( a )</th>
<th>( W_{\text{min}} )</th>
<th>( \text{Mana} )</th>
<th>( \sum_B H^B_{\text{min}} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>-0.027692</td>
<td>0.814835</td>
<td>7.87055</td>
</tr>
<tr>
<td>2</td>
<td>-0.089915</td>
<td>0.814835</td>
<td>12.3287</td>
</tr>
<tr>
<td>3</td>
<td>-0.034531</td>
<td>0.896212</td>
<td>9.35125</td>
</tr>
<tr>
<td>4</td>
<td>-0.034531</td>
<td>0.896212</td>
<td>9.35125</td>
</tr>
<tr>
<td>5</td>
<td>-0.089915</td>
<td>0.814835</td>
<td>12.3287</td>
</tr>
<tr>
<td>6</td>
<td>-0.027692</td>
<td>0.814835</td>
<td>7.87055</td>
</tr>
</tbody>
</table>
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 $p \geq 11$ (we highlight as an interesting open question whether any alternate choice of Pauli measurements (14) for Alice and Bob could result in $\lambda_{\text{max}}(B) > (B')_{\text{max}} = 37$). For $p < 11$ it should be borne in mind that [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 non-stabilizer 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 [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 inter-relationship 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 $|J_{a,b,c}\rangle$ 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, analogous 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 $q = p^n$ by using the field $\mathbb{F}_q$ rather than $\mathbb{F}_p$.

VII. ACKNOWLEDGEMENTS

We thank Jyrki Lahtonen for assistance regarding exponential sums, Earl Campbell for helpful suggestions and Joel Wallman for comments on an early draft. MH 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 W911NF-14-1-0103.
