Multipartite entanglement, quantum-error-correcting codes, and entangling power of quantum evolutions

A. J. Scott*
Department of Physics and Astronomy, University of New Mexico, Albuquerque, New Mexico 87131-1156, USA
(Received 28 October 2003; published 27 May 2004)

We investigate the average bipartite entanglement, over all possible divisions of a multipartite system, as a useful measure of multipartite entanglement. We expose a connection between such measures and quantum-error-correcting codes by deriving a formula relating the weight distribution of the code to the average entanglement of encoded states. The multipartite entangling power of quantum evolutions is also investigated.

DOI: 10.1103/PhysRevA.69.052330 PACS number(s): 03.67.Mn

I. INTRODUCTION

The phenomenon of entanglement [1–3] is a remarkable feature of quantum physics that has been identified as a key ingredient in many areas of quantum information theory including quantum key distribution [4], superdense coding [5], and teleportation [6]. However, the general problem of how to quantify [1] the level of entanglement in an arbitrary multipartite system remains unresolved. There has been some progress towards a solution [7–17], but the task at hand is generally considered a difficult one and may never be completed. We are thus led to consider simple computable measures of entanglement [18,19] that although cannot fully characterize the multipartite nature of the correlations, may nevertheless still provide a useful gauge of their levels.

In this article we investigate the average bipartite entanglement, over all possible divisions of a multipartite system, as a useful measure of multipartite entanglement. Such measures might be considered the least sophisticated of choices; however, their simplicity allows theoretical calculations to be exercised with ease. We will restrict our study to pure-state entanglement where the subsystem linear entropy is a clear choice for the bipartite measure. It was recently shown by Brennen [20] that an entanglement measure proposed by Meyer and Wallach [19] is of the above-described form, and hence, the multipartite entanglement measures considered in this paper may be viewed as generalizations of the Meyer-Wallach measure. Our measures may also be viewed as variations of those considered by Pope and Milburn [21] where instead the minimum bipartite entanglement was considered.

We show that the average bipartite entanglement elects self-dual quantum-error-correcting codes to the status of maximally entangled states. The connection between entanglement and quantum-error-correcting codes has been highlighted elsewhere (e.g., [22]); however, we make this relationship explicit by expressing the average entanglement of encoded states in terms of the weight distribution of the code. We also investigate the multipartite entangling power of quantum evolutions. A simple extension of the work of Zanardi *et al.* [23] allows the derivation of an explicit formula. Such formulas are relevant to current studies in the entangling capabilities of chaotic systems [24–39]. An example treated in this article is the quantum kicked rotor.

The paper is organized as follows. In the next section we introduce the Meyer-Wallach entanglement measure and its generalizations. The connection between these measures and quantum-error-correcting codes is discussed in Sec. III. This relationship is further strengthened in Sec. IV where we derive a formula for the average entanglement over a subspace. In Sec. V we derive a formula for the multipartite entangling power of an arbitrary unitary. Finally in Sec. VI we conclude by applying our results to the quantum kicked rotor.

II. CLASS OF MULTIPARTITE ENTANGLEMENT MEASURES

It is generally accepted that when a bipartite quantum system is in an overall pure state, there is an essentially unique resource-based measure of entanglement between the two subsystems. This measure is given by the von Neumann entropy of the marginal density operators [40,41]. To ease theoretical calculations, one often replaces the von Neumann entropy with its linearized version, the linear entropy. For a bipartite system in an overall pure state $|\psi\rangle \in \mathbb{C}^{D_A} \otimes \mathbb{C}^{D_B}$, the *subsystem linear entropy* is defined as

$$S_L(\psi) \equiv \eta(1 - \mathrm{tr}\rho_A{}^2), \quad \rho_A = \mathrm{tr}_B|\psi\rangle\langle\psi|, \tag{1}$$

where the normalization factor $\eta = D/(D-1)$, with $D = \min(D_A, D_B)$, is chosen such that $0 \leqslant S_L \leqslant 1$. The state is separable if and only if $S_L = 0$ and maximally entangled when $S_L = 1$.

In general, as the number of subsystems increases, an exponential number of independent measures is needed to quantify fully the amount entanglement in a multipartite system. Consequently, the following entanglement measures cannot be thought of as unique. Different measures will capture different aspects of multipartite entanglement.

The Meyer-Wallach measure [19] $Q(\psi)$, which can only be applied to multiqubit pure states $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$, is defined as follows. For each $j = 1, \ldots, n$ and $b \in \{0, 1\}$, we define the linear map $\iota_j(b): (\mathbb{C}^2)^{\otimes n} \to (\mathbb{C}^2)^{\otimes n-1}$ through its action on the product basis:

*Electronic address: ascott@phys.unm.edu

$$\iota_j(b)|x_1\rangle \otimes \cdots \otimes |x_n\rangle = \delta_{bx_j}|x_1\rangle \otimes \cdots \otimes |x_{j-1}\rangle \otimes |x_{j+1}\rangle \otimes \cdots \otimes |x_n\rangle, \quad (2)$$

where $x_i \in \{0,1\}$. The Meyer-Wallach entanglement measure is then

$$Q(\psi) \equiv \frac{4}{n}\sum_{j=1}^{n} D(\iota_j(0)|\psi\rangle, \iota_j(1)|\psi\rangle), \quad (3)$$

where

$$D(|\psi\rangle,|\phi\rangle) = \langle\psi|\psi\rangle\langle\phi|\phi\rangle - |\langle\psi|\phi\rangle|^2. \quad (4)$$

Meyer and Wallach showed that Q is invariant under local unitary transformations and that $0 \leqslant Q \leqslant 1$, with $Q(\psi)=0$ if and only if $|\psi\rangle$ is a product state.

Recently, it was shown by Brennen [20] that Q is simply the average subsystem linear entropy of the constituent qubits:

$$Q(\psi) = 2\left(1 - \frac{1}{n}\sum_{k=1}^{n} \mathrm{tr}\rho_k{}^2\right), \quad (5)$$

where ρ_k is the density operator for the kth qubit after tracing out the rest. This simplification is easily understood [42] by first showing that $D(\iota_j(0)|\psi\rangle, \iota_j(1)|\psi\rangle)$ is unchanged by a local unitary applied to the jth qubit (a fact already proven by Meyer and Wallach) and, hence, invariant under a change in the qubit's fiducial basis. Consequently, a judicious choice of the Schmidt basis gives $D(\iota_j(0)|\psi\rangle, \iota_j(1)|\psi\rangle) = \lambda_j^1\lambda_j^2 = (1 - \mathrm{tr}\rho_j{}^2)/2$, where λ_j^1 and λ_j^2 are the Schmidt coefficients in the decomposition between the jth qubit and the remainder of the system.

Brennen's simplification immediately allows the generalization of Q to multiqudit states $|\psi\rangle \in (\mathbb{C}^D)^{\otimes n}$, and by considering all other possible bipartite divisions, we can now define a class of related multipartite entanglement measures in the obvious manner:

$$Q_m(\psi) \equiv \frac{D^m}{D^m - 1}\left(1 - \frac{m!\,(n-m)!}{n!}\sum_{|S|=m} \mathrm{tr}\rho_S{}^2\right),$$

$$m = 1, \ldots, \lfloor n/2 \rfloor, \quad (6)$$

where $S \subset \{1, \ldots, n\}$ and $\rho_S = \mathrm{tr}_{S'}|\psi\rangle\langle\psi|$ is the density operator for the qudits S after tracing out the rest and $\lfloor k \rfloor$ denotes the integer part of k. Note that Q_m reduces to the original Meyer-Wallach measure when $m=1$ and $D=2$. The above "multipartite" entanglement measures are merely averages over the well-established bipartite measure. Consequently, Q_m is invariant under local unitary transformations, nonincreasing on average under local quantum operations and classical communication—i.e., Q_m is an entanglement monotone [43]—and $0 \leqslant Q_m \leqslant 1$. The lower bound is only reached for product states.

Proposition 1: $Q_m(\psi)=0$ iff $|\psi\rangle = \otimes_{j=1}^{n}|\psi_j\rangle$ for some $|\psi_j\rangle \in \mathbb{C}^D$; i.e., $|\psi\rangle$ is a product state.

When $m=1$ the upper bound is reached by the generalized Greenberger-Horne-Zeilinger (GHZ) states

$$|\gamma\rangle = \frac{1}{\sqrt{D}}\sum_{j=0}^{D-1} |j\rangle^{\otimes n}. \quad (7)$$

In general,

$$Q_m(\gamma) = 1 - \frac{D^{m-1}-1}{D^m - 1}, \quad (8)$$

and hence the entangled states $|\gamma\rangle$ do not saturate the upper bound for $m>1$. We have not, however, established whether or not there even *exist* states which saturate the upper bound.

Define an *m-uniform* multiqudit state to be a state with the property that after tracing out all but m qudits we are left with the maximally mixed state, for any m-tuple of qudits. Thus, all information about the system is lost upon the removal of $n-m$ or more parties.

Proposition 2: $Q_m(\psi)=1$ iff $\rho_S = \mathrm{tr}_{S'}|\psi\rangle\langle\psi| = D^{-m}\hat{1}$ whenever $|S|=m$; i.e., $|\psi\rangle$ is m-uniform.

Obviously, if $|\psi\rangle$ is m-uniform then it is also $(m-1)$ uniform, and hence $Q_m(\psi)=1 \Rightarrow Q_{m-1}(\psi)=1$. However, note that the measures Q_m do not obey any ordering. For example, in the case of qubits, consider the generalized W states

$$|\omega\rangle = \frac{1}{\sqrt{n}}\sum_{j=1}^{n} |0\rangle^{\otimes j-1} \otimes |1\rangle \otimes |0\rangle^{\otimes n-j}. \quad (9)$$

One can calculate

$$Q_m(\omega) = \frac{2^{m+1}}{2^m - 1}\frac{(n-m)m}{n^2} \quad (10)$$

and hence, for $n=6$ say, $Q_1 = 5/9 < Q_3 = 4/7 < Q_2 = 16/27$. The measures Q_m also do not preserve the partial ordering of entangled states; i.e., $Q_{m'}(\psi) \leqslant Q_{m'}(\phi)$ does not necessarily imply that $Q_m(\psi) \leqslant Q_m(\phi)$ for other m. These facts might be considered as unlucky properties of Q_m. However they do suggest that the extremal entanglement measure $Q_{\lfloor n/2 \rfloor}$ does not necessarily tell the entire story; different Q_m capture different aspects of multipartite entanglement. The original Meyer-Wallach measure Q_1 is the average entanglement between individual qudits and the rest, whereas, on increasing m, Q_m measures the average entanglement between blocks of qudits, of an increasing size, and the rest. Consequently, as m increases, we expect that Q_m will be sensitive to correlations of an increasingly global nature.

Proposition 2 implies that the task of finding states which saturate the the upper bound 1 of Q_m is equivalent to the construction of m-uniform multiqudit states. We now show in the next section how quantum-error-correcting codes (QECC's) produce m-uniform multiqudit states. An example is the six-qubit hexacode state $|H\rangle$, which arises as the code subspace of the self-dual qubit stabilizer code $[[6,0,4]]$. In this case $Q_1(H) = Q_2(H) = Q_3(H) = 1$.

III. MULTIPARTITE ENTANGLEMENT AND QECC's

The idea behind quantum error correction [22,44–49] is to encode quantum states into qudits in such a way that a small number of errors affecting the individual qudits can be

measured and corrected to perfectly restore the original encoded state. The encoding of a K-dimensional quantum state into n qudits is simply a linear map from $\mathbb{C}^K$ to a subspace $\mathcal{Q}$ of $(\mathbb{C}^D)^{\otimes n}$. The subspace itself is referred to as the *code* and is orientated in such a way that errors on the qudits move encoded states in a direction perpendicular to the code.

A. General QECC's

An *error operator* E is a linear operator acting on $(\mathbb{C}^D)^{\otimes n}$. The error is said to be *detectable* by the quantum code $\mathcal{Q}$ if

$$\langle\psi|E|\psi\rangle = \langle\phi|E|\phi\rangle \tag{11}$$

for all normalized $|\psi\rangle, |\phi\rangle \in \mathcal{Q}$. Equivalently, if $\mathcal{Q}$ is spanned by an orthonormal *logical basis* $\{|j_L\rangle | j=0,\ldots,K-1\}$, then an error E is detectable if and only if

$$\langle j_L|E|i_L\rangle = C(E)\delta_{ij} \tag{12}$$

for all $0 \leqslant i,j \leqslant K-1$ where the constant $C(E)$ depends only on E. It is a general theorem of QECC's that a set of errors $\mathcal{E}$ can be *corrected* by a code $\mathcal{Q}$, if and only if for each $E_1, E_2 \in \mathcal{E}$, the error $E_2^\dagger E_1$ is detectable by $\mathcal{Q}$.

A *local error operator* has the form

$$E = M_1 \otimes \cdots \otimes M_n, \tag{13}$$

where each M_i acts on $\mathbb{C}^D$. The *weight* of a local error operator E, denoted by $\mathrm{wt}(E)$, is the number of elements, M_i, which are not scalar multiples of the identity. A quantum code $\mathcal{Q}$ has a *minimum distance* of at least d if and only if all local error operators of weight less than d are detectable by $\mathcal{Q}$. A code with minimum distance $d=2t+1$ allows the correction of arbitrary errors affecting up to t qudits. In the case of qubits, such codes are denoted by the triple $((n,K,d))$. We will use the notation $((n,K,d))_D$ for the general case of qudits [50]. An $((n,K,d))_D$ code is called *pure* if $\langle\psi|E|\psi\rangle = D^{-n}\,\mathrm{tr}\,E$ for all $|\psi\rangle \in \mathcal{Q}$ whenever $\mathrm{wt}(E) < d$. When considering self-dual codes ($K=1$), we adopt the convention that the notation $((n,1,d))_D$ refers only to pure codes since the condition on the minimum distance is otherwise trivial.

There is a continuum of possible errors in a single qudit; however, due to the phenomenon of measurement collapse, the correction of an arbitrary single-qudit error only requires an ability to correct D^2 different types, each corresponding to an orthonormal basis element for single-qudit operations. One choice for a *nice error basis* [51–53] is the *displacement operator basis*

$$D(\mu,\nu) \equiv e^{i\pi\mu\nu/D} X^\mu Z^\nu, \quad 0 \leqslant \mu,\nu \leqslant D-1, \tag{14}$$

where the Weyl operators X and Z are defined on a basis $\{|j\rangle | j=0,\ldots,D-1\}$ for $\mathbb{C}^D$ through the equations

$$X|j\rangle = |j+1 \bmod D\rangle, \quad Z|j\rangle = e^{2\pi i j/D}|j\rangle. \tag{15}$$

The displacement operators reduce to the Pauli matrices for qubits, satisfy the relations

$$D(\mu,\nu) = e^{i\pi\nu} D(\mu+D,\nu) = e^{i\pi\mu} D(\mu,\nu+D), \tag{16}$$

$$D(\mu,\nu)^\dagger = D(-\mu,-\nu) = e^{i\pi(\mu+\nu+D)} D(D-\mu, D-\nu), \tag{17}$$

$$\begin{aligned} D(\mu,\nu)D(\alpha,\beta) &= e^{2\pi i(\nu\alpha-\mu\beta)/D} D(\alpha,\beta)D(\mu,\nu) \\ &= e^{\pi i(\nu\alpha-\mu\beta)/D} D(\mu+\alpha,\nu+\beta), \end{aligned} \tag{18}$$

$$\mathrm{tr}[D(\mu,\nu)^\dagger D(\alpha,\beta)] = D\delta_{\mu\alpha}\delta_{\nu\beta}, \tag{19}$$

and thus form an orthonormal basis for all single-qudit operators:

$$A = \frac{1}{D}\sum_{\mu,\nu=0}^{D-1} \mathrm{tr}[D(\mu,\nu)^\dagger A] D(\mu,\nu). \tag{20}$$

Similarly, the operators

$$\begin{aligned} \mathcal{D}(\boldsymbol{\mu},\boldsymbol{\nu}) &\equiv \mathcal{D}(\mu_1\cdots\mu_n,\nu_1\cdots\nu_n) \\ &\equiv D(\mu_1,\nu_1)\otimes\cdots\otimes D(\mu_n,\nu_n), \end{aligned}$$

$$0 \leqslant \mu_k,\nu_k \leqslant D-1, \tag{21}$$

form an orthonormal basis for the set of all n-qudit operators: $A = D^{-n}\Sigma_{\boldsymbol{\mu},\boldsymbol{\nu}} \mathrm{tr}[\mathcal{D}(\boldsymbol{\mu},\boldsymbol{\nu})^\dagger A]\mathcal{D}(\boldsymbol{\mu},\boldsymbol{\nu})$. The weight of $\mathcal{D}(\mu,\nu)$ is simply the number of pairs (μ_k,ν_k) different from $(0,0)$. We are now in a position to make a more explicit definition of what we mean by an $((n,K,d))_D$ QECC.

Definition: Let $\mathcal{Q}$ be a K-dimensional subspace of $(\mathbb{C}^D)^{\otimes n}$ spanned by the orthonormal logical basis $\{|j_L\rangle |\, j=0,\ldots,K-1\}$. Then $\mathcal{Q}$ is called an $((n,K,d))_D$ *quantum-error-correcting code* if

$$\langle j_L|\mathcal{D}(\boldsymbol{\mu},\boldsymbol{\nu})|i_L\rangle = C(\boldsymbol{\mu},\boldsymbol{\nu})\delta_{ij} \tag{22}$$

for all $\mathcal{D}(\boldsymbol{\mu},\boldsymbol{\nu})$ with $\mathrm{wt}[\mathcal{D}(\boldsymbol{\mu},\boldsymbol{\nu})] < d$ and $0 \leqslant i,j \leqslant K-1$. If $C(\boldsymbol{\mu},\boldsymbol{\nu}) = \delta_{\boldsymbol{\mu}\mathbf{0}}\delta_{\boldsymbol{\nu}\mathbf{0}}$, the code is called *pure*. An $((n,1,d))_D$ code must be pure by convention.

An $((n,K,d))_D$ QECC can detect and recover all errors acting on $<d/2$ qudits. It is now evident how quantum codes produce maximally entangled states.

Proposition 3: $Q_m(\psi)=1$ iff $|\psi\rangle$ is a (pure) $((n,1,m+1))_D$ quantum-error-correcting code.

Proof: If $Q_m(\psi)=1$ then $|\psi\rangle$ is m-uniform and, consequently,

$$\langle\psi|\mathcal{D}(\boldsymbol{\mu},\boldsymbol{\nu})|\psi\rangle = \mathrm{tr}\,[|\psi\rangle\langle\psi|\mathcal{D}(\boldsymbol{\mu},\boldsymbol{\nu})] \tag{23}$$

$$= D^{-n}\mathrm{tr}[\mathcal{D}(\boldsymbol{\mu},\boldsymbol{\nu})] \ (\text{whenever } \mathrm{wt}[\mathcal{D}(\boldsymbol{\mu},\boldsymbol{\nu})] \leqslant m) \tag{24}$$

$$= \delta_{\boldsymbol{\mu}\mathbf{0}}\delta_{\boldsymbol{\nu}\mathbf{0}} \tag{25}$$

given that the displacement operators are traceless for all $(\mu,\nu) \neq (0,0)$. Thus, $|\psi\rangle$ is an $((n,1,m+1))_D$ QECC.

Conversely, if $|\psi\rangle$ is an $((n,1,m+1))_D$ QECC, then rewriting $|\psi\rangle\langle\psi|$ in the displacement operator basis

$$D^n|\psi\rangle\langle\psi| = \hat{1} + \sum_{1\leqslant \mathrm{wt}[\mathcal{D}(\boldsymbol{\mu},\boldsymbol{\nu})]\leqslant m} c_{\boldsymbol{\mu\nu}}\mathcal{D}(\boldsymbol{\mu},\boldsymbol{\nu}) + \sum_{m+1\leqslant \mathrm{wt}[\mathcal{D}(\boldsymbol{\mu},\boldsymbol{\nu})]\leqslant n} c_{\boldsymbol{\mu\nu}}\mathcal{D}(\boldsymbol{\mu},\boldsymbol{\nu}), \quad (26)$$

we see that the coefficients $c_{\boldsymbol{\mu\nu}}=\langle\psi|\mathcal{D}(\boldsymbol{\mu},\boldsymbol{\nu})|\psi\rangle$ are nonzero only in the second sum, and hence, given the traceless property of the displacement operators,

$$\rho_S = \mathrm{tr}_{S'}|\psi\rangle\langle\psi| = D^{-m}\hat{1} \quad (27)$$

whenever $|S|=m$. Thus $|\psi\rangle$ is m-uniform and $Q_m(\psi)=1$. □

Note that any state $|\psi\rangle\in\mathcal{Q}$, where $\mathcal{Q}$ is a pure $((n,K,m+1))_D$ QECC, is itself an $((n,1,m+1))_D$ QECC. Consequently, pure $((n,K,m+1))_D$ codes define entire subspaces of maximally entangled states. The connection between quantum codes and entanglement is noted in [22] and alluded to elsewhere [17,46]; however, we cite the work of Rains [54] for a rigorous proof of the relationship even though no mention of entanglement can be found in the paper. Here quantum weight enumerators were studied extensively. It will later prove advantageous to now revisit Rains' work in the current article.

Defining $P_{\mathcal{Q}}$ as the projector onto the code subspace $\mathcal{Q}$ with dimension K, the Shor-Laflamme enumerators of a quantum code are [55]

$$A_i(P_{\mathcal{Q}}) = \frac{1}{K^2}\sum_{\mathrm{wt}[\mathcal{D}(\boldsymbol{\mu},\boldsymbol{\nu})]=i} |\mathrm{tr}[\mathcal{D}(\boldsymbol{\mu},\boldsymbol{\nu})P_{\mathcal{Q}}]|^2, \quad (28)$$

$$B_i(P_{\mathcal{Q}}) = \frac{1}{K}\sum_{\mathrm{wt}[\mathcal{D}(\boldsymbol{\mu},\boldsymbol{\nu})]=i} \mathrm{tr}[\mathcal{D}(\boldsymbol{\mu},\boldsymbol{\nu})P_{\mathcal{Q}}\mathcal{D}(\boldsymbol{\mu},\boldsymbol{\nu})^{\dagger}P_{\mathcal{Q}}], \quad (29)$$

where $i=0,\ldots,n$. Rains [54] defined two new enumerators

$$A_i'(P_{\mathcal{Q}}) = \frac{1}{K^2}\sum_{|S|=i} \mathrm{tr}_S[\mathrm{tr}_{S'}[P_{\mathcal{Q}}]^2], \quad (30)$$

$$B_i'(P_{\mathcal{Q}}) = \frac{1}{K}\sum_{|S|=i} \mathrm{tr}_{S'}[\mathrm{tr}_S[P_{\mathcal{Q}}]^2], \quad (31)$$

related to the Shor-Laflamme enumerators via the equations

$$A_m'(P_{\mathcal{Q}}) = D^{-m}\sum_{i=0}^{m}\frac{(n-i)!}{(m-i)!\,(n-m)!}A_i(P_{\mathcal{Q}}), \quad (32)$$

$$B_m'(P_{\mathcal{Q}}) = D^{-m}\sum_{i=0}^{m}\frac{(n-i)!}{(m-i)!\,(n-m)!}B_i(P_{\mathcal{Q}}). \quad (33)$$

This relationship was only given in the qubit case where the displacement operators reduce to Hermitian Pauli matrices. However, the proof extends easily to qudits with the the help of Eq. (17). It is easy to see that the weight enumerators satisfy the normalization condition $A_0'(P_{\mathcal{Q}})=B_0'(P_{\mathcal{Q}})=A_0(P_{\mathcal{Q}})=B_0(P_{\mathcal{Q}})=1$, and for self-dual codes ($K=1$)

$$B_i'(P_{\mathcal{Q}}) = A_i'(P_{\mathcal{Q}}) \quad [B_i(P_{\mathcal{Q}}) = A_i(P_{\mathcal{Q}})] \quad (34)$$

for all $0\leqslant i\leqslant n$. In general, the weight enumerators satisfy [54]

$$B_i'(P_{\mathcal{Q}}) \geqslant A_i'(P_{\mathcal{Q}}) \geqslant 0 \quad [B_i(P_{\mathcal{Q}}) \geqslant A_i(P_{\mathcal{Q}}) \geqslant 0] \quad (35)$$

for all $0\leqslant i\leqslant n$

Theorem [54]: Let $\mathcal{Q}$ be a quantum code with associated projector $P_{\mathcal{Q}}$. Then $\mathcal{Q}$ has minimum distance of at least d iff

$$B_{d-1}'(P_{\mathcal{Q}}) = A_{d-1}'(P_{\mathcal{Q}}) \quad [B_i(P_{\mathcal{Q}}) = A_i(P_{\mathcal{Q}}) \text{ for all } 0<i<d] \quad (36)$$

and is pure iff

$$B_{d-1}'(P_{\mathcal{Q}}) = A_{d-1}'(P_{\mathcal{Q}}) = \frac{D^{1-d}n!}{(d-1)!\,(n-d+1)!}$$

$$[B_i(P_{\mathcal{Q}}) = A_i(P_{\mathcal{Q}}) = 0 \text{ for all } 0<i<d]. \quad (37)$$

Proposition 3 is now immediately apparent since

$$Q_m(\psi) = \frac{D^m}{D^m-1}\left[1-\frac{m!\,(n-m)!}{n!}A_m'(|\psi\rangle\langle\psi|)\right] = 1-\frac{1}{D^m-1}\sum_{i=1}^{m}\frac{m!\,(n-i)!}{n!\,(m-i)!}A_i(|\psi\rangle\langle\psi|). \quad (38)$$

Noting that $KA_i'=B_{n-i}'$, one can use the above theorem to derive bounds on the minimum distance for general quantum codes. In the case of $((n,1,d))_D$ QECC's the following conditions must hold:

$$A_i' = A_{n-i}', \quad 0\leqslant i\leqslant n, \quad (39)$$

$$A_0 = 1, \quad (40)$$

$$A_i = 0, \quad 0<i<d, \quad (41)$$

$$A_i \geqslant 0, \quad d\leqslant i\leqslant n. \quad (42)$$

When $d=\lfloor n/2\rfloor+1$, these equations uniquely specify the weight distribution $\{A_i\}$. Solving Eqs. (39)–(41), we obtain

$$A_i = \frac{n!}{(n-i)!}\sum_{j=d}^{i}\frac{(-1)^{i-j}(D^{2j-n}-1)}{j!\,(i-j)!}, \quad d\leqslant i\leqslant n, \quad (43)$$

and under the condition $A_{d+1}\geqslant 0$, we find that we at least require

$$n \leqslant \begin{cases} 2(D^2-1) & \text{if } n \text{ is even,} \\ 2D(D+1)-1 & \text{if } n \text{ is odd,} \end{cases} \quad (44)$$

for an $((n,1,\lfloor n/2\rfloor+1))_D$ QECC to exist. Consequently, $Q_{\lfloor n/2\rfloor}(\psi)<1$ for all $|\psi\rangle$ whenever Eq. (44) is not satisfied. For $d\leqslant\lfloor n/2\rfloor$ we must resort to linear programming techniques on Eqs. (39)–(42) to prove the nonexistence of $((n,1,d))_D$ QECC's. However, tighter bounds could be obtained by using the generalized quantum shadow enumerators [56,57]. We make no attempt at this task in the current article, but

instead specialize to qubits where many examples of QECC's are already known.

B. Stabilizer qubit QECC's

An important class of quantum codes is composed of the so-called *additive* or *stabilizer* codes [44,45]. A *stabilizer code* is defined as a joint eigenspace of an Abelian subgroup S (called the *stabilizer*) of the *error group* $\mathcal{E}=\{\pm e^{i\pi\lambda/D}\mathcal{D}(\boldsymbol{\mu},\boldsymbol{\nu})\,|\,0\leq\mu_k,\nu_k,\lambda\leq D-1\}$. When D is prime, these codes can be described by an $(n-k)\times n$ stabilizer matrix over $\mathrm{GF}(D^2)$ and are examples of $((n,D^k,d))_D$ QECC's. The notation $[[n,k,d]]_D$ is then used or simply $[[n,k,d]]$ when $D=2$.

A classical *additive code over* GF(4) *of length n* is an additive subgroup $\mathcal{C}$ of $\mathrm{GF}(4)^n$. In the case of qubits, stabilizer codes correspond to classical additive codes over GF(4) [44]. This is shown as follows. Letting $\mathrm{GF}(4)=\{0,1,\omega,\overline{\omega}\}$ where $\overline{\omega}=\omega^2=1+\omega$, we define the *conjugate* of $x\in\mathrm{GF}(4)$, denoted $\bar{x}$, by the mapping $\overline{0}=0$, $\overline{1}=1$, and $\overline{\overline{\omega}}=\omega$. Next define the *trace* map $\mathrm{Tr}:\mathrm{GF}(4)\rightarrow\mathrm{GF}(2)$ by $\mathrm{Tr}(x)=x+x^2$—i.e., $\mathrm{Tr}(0)=\mathrm{Tr}(1)=0$ and $\mathrm{Tr}(\omega)=\mathrm{Tr}(\overline{\omega})=1$— and the *trace inner product* of two vectors $\mathbf{x}=x_1\ldots x_n$ and $\mathbf{y}=y_1\ldots y_n$ in $\mathrm{GF}(4)^n$ as

$$\mathbf{x}\star\mathbf{y}=\sum_{i=1}^{n}\mathrm{Tr}(x_i\overline{y_i})\ \in\mathrm{GF}(2). \tag{45}$$

The *weight* $\mathrm{wt}(\mathbf{x})$ of $\mathbf{x}\in\mathrm{GF}(4)^n$ is the number of nonzero components of $\mathbf{x}$, and the *minimum weight* of a code $\mathcal{C}$ is the smallest weight of any nonzero codeword in $\mathcal{C}$. Next, by defining the mapping $\Phi:\mathrm{GF}(4)^n\rightarrow\mathcal{E}$ by $\Phi(\mathbf{x})=\mathcal{D}(\phi^{-1}(\mathbf{x}))$ where $\phi(\mu,\nu)=\omega\mu+\overline{\omega}\nu$, we can associate elements of GF(4) with Pauli matrices $(\omega\rightarrow X,\overline{\omega}\rightarrow Z,1\rightarrow iXZ,0\rightarrow I)$, addition of vectors over $\mathrm{GF}(4)^n$ with multiplication of operators in $\mathcal{E}$ (neglecting phases), and the trace inner product on $\mathrm{GF}(4)^n$ with the commutator on $\mathcal{E}$.

If $\mathcal{C}$ is an additive code, its *dual* is the additive code $\mathcal{C}^{\perp}=\{\mathbf{x}\in\mathrm{GF}(4)^n\,|\,\mathbf{x}\star\mathbf{c}=0\ \forall\ \mathbf{c}\in\mathcal{C}\}$. The code $\mathcal{C}$ is called *self-orthogonal* if $\mathcal{C}\subseteq\mathcal{C}^{\perp}$ and *self-dual* if $\mathcal{C}=\mathcal{C}^{\perp}$. The following theorem now applies [44]: Suppose $\mathcal{C}$ is a self-orthogonal additive subgroup of $\mathrm{GF}(4)^n$, containing 2^{n-k} vectors, such that there are no vectors of weight $<d$ in $\mathcal{C}^{\perp}\backslash\mathcal{C}$. Then any joint eigenspace of $\Phi(\mathcal{C})$ is an $[[n,k,d]]$ QECC.

We say that $\mathcal{C}$ is *pure* if there are no nonzero vectors of weight $<d$ in $\mathcal{C}^{\perp}$. The associated QECC is then pure if and only if $\mathcal{C}$ is pure. By convention, an $[[n,0,d]]$ QECC corresponds to a self-dual additive code $\mathcal{C}$ with minimum weight d. Consequently, $[[n,0,d]]$ QECC's are always pure and are examples of $((n,1,d))$ QECC's which saturate the entanglement measures Q_m.

The advantage of making the above correspondence is that a wealth of classical coding theory immediately becomes available. Indeed the classical self-dual additive *hexacode* with generator matrix

$$\begin{bmatrix}1&0&0&1&\omega&\omega\\0&1&0&\omega&1&\omega\\0&0&1&\omega&\omega&1\\\omega&0&0&\omega&\overline{\omega}&\overline{\omega}\\0&\omega&0&\overline{\omega}&\omega&\overline{\omega}\\0&0&\omega&\overline{\omega}&\overline{\omega}&\omega\end{bmatrix} \tag{46}$$

gives the quantum hexacode $[[6,0,4]]$ mentioned previously. The rows of the generator matrix define a basis (under addition) for the classical code $\mathcal{C}$ and, with the above correspondence, define generators (up to a phase) for the stabilizer S in the quantum version. Another example is the $[[2,0,2]]$ qubit code generated by

$$\begin{bmatrix}1&1\\\omega&\omega\end{bmatrix} \tag{47}$$

In this case the quantum code is an Einstein-Podolsky-Rosen (EPR) state—e.g., $(|00\rangle+|11\rangle)/\sqrt{2}$. We can obtain a $[[5,0,3]]$ qubit code by deleting the first row and column of the hexacode generator matrix [Eq. (46)]. This process is called *shortening* [60]. A $[[3,0,2]]$ code

$$\begin{bmatrix}1&1&0\\\omega&\omega&\omega\\1&0&1\end{bmatrix} \tag{48}$$

is obtained by *lengthening* the $[[2,0,2]]$ code.

The four codes of lengths $n=2,3,5,$ and 6 mentioned thus far all produce quantum stabilizer codes with the property $Q_{\lfloor n/2\rfloor}(\psi)=1$. Unfortunately, known bounds on such codes prevent this from being the case for other lengths. An additive self-dual code is called *type II* if all codewords have even weight and *type I* otherwise. It can be shown that all type-II codes have even length. If d_I, d_{II} is the minimum weight of an additive self-dual type-I, type-II code, respectively, of length $n>1$, then [58–60]

$$d_I\leq\begin{cases}2\lfloor n/6\rfloor+1 & \text{if } n\equiv 0 \bmod 6,\\ 2\lfloor n/6\rfloor+3 & \text{if } n\equiv 5 \bmod 6,\\ 2\lfloor n/6\rfloor+2 & \text{otherwise,}\end{cases} \tag{49}$$

$$d_{II}\ \leq\ 2\lfloor n/6\rfloor+2. \tag{50}$$

If a code meets the appropriate bound, it is called *extremal*. A code is called *optimal* when it is not extremal and no code can exist with a larger minimum weight. The above bounds imply that $[[n,0,\lfloor n/2\rfloor+1]]$ stabilizer codes may exist only when $n=2$, 3, 5, 6, and 7. However, $[[7,0,3]]$ codes are known to be optimal and we are left with the remaining four cases.

The *weight distribution* of an additive code $\mathcal{C}$,

$$A_i\equiv|\{\mathbf{x}\in\mathcal{C}|\ \mathrm{wt}(\mathbf{x})=i\}|, \tag{51}$$

is also the weight distribution for the corresponding quantum stabilizer code, and thus, the entanglement of the stabilized state is easily calculated through formula (38). We can see

TABLE I. The weight distributions A_i and corresponding entanglement Q_m for extremal (or optimal for $n=7$ and 13) additive self-dual codes. In all but the cases $n=10$ and 13 these are the only possible weight distributions.

n	d	A_0	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8	A_9	A_{10}	A_{11}	A_{12}	A_{13}	Q_1	Q_2	Q_3	Q_4	Q_5	Q_6
2	2	1	0	3												1					
3	2	1	0	3	4											1					
4	2	1	0	6	0	9										1	2/3				
4	2	1	0	2	8	5										1	8/9				
5	3	1	0	0	10	15	6									1	1				
6	4	1	0	0	0	45	0	18								1	1	1			
7	3	1	0	0	7	21	42	42	15							1	1	34/35			
7	3	1	0	0	3	29	42	34	19							1	1	242/245			
8	4	1	0	0	0	42	0	168	0	45						1	1	1	24/25		
8	4	1	0	0	0	26	64	72	64	29						1	1	1	512/525		
9	4	1	0	0	0	26	48	136	160	93	48					1	1	1	932/945		
9	4	1	0	0	0	18	72	120	144	117	40					1	1	1	104/105		
10	4	1	0	0	0	30	0	300	0	585	0	108				1	1	1	104/105	212/217	
11	5	1	0	0	0	0	66	198	330	495	550	330	78			1	1	1	1	216/217	
12	6	1	0	0	0	0	0	396	0	1485	0	1980	0	234		1	1	1	1	1	146/147
13	5	1	0	0	0	0	15	236	356	1197	1530	2012	1956	650	239	1	1	1	1	13294/13299	26938/27027

this by noting that for stabilizer codes, the projection onto $\mathcal{Q}$ is given by [49]

$$P_Q = \frac{1}{|S|}\sum_{E\in S} \lambda(E)^{-1}E, \tag{52}$$

where S is the stabilizer and $\lambda(E)$ is the eigenvalue associated with E—i.e., $E|\psi\rangle=\lambda(E)|\psi\rangle$ for all $|\psi\rangle\in\mathcal{Q}$. We remark that the quantum weight distribution B_i corresponds to the classical weight distribution of the dual code $\mathcal{C}^{\perp}$.

In Table I the weight distributions for extremal (or optimal for $n=7$ and 13) additive self-dual codes are collected [61,62]. In all but the cases $n=10$ and 13 these are the only possible weight distributions. The weight distribution is unique for extremal type-II codes. Also tabulated is the corresponding entanglement Q_m for the quantum code.

Although the bounds mentioned above [Eqs. (49) and (50)] were given in the context of stabilizer codes, they also apply to general QECC's [56]. Consequently, for qubits, there exist states $|\psi\rangle$ with $Q_{\lfloor n/2\rfloor}(\psi)=1$ only in the cases $n=2,3,5,6$, and possibly when $n=7$ where a nonadditive $((7,1,4))$ code might still exist. It is not known what the supremum of $Q_m(\psi)$ is in general; however, given the examples in Table I, we expect it to be very close to 1 when n is large. It is interesting that the mean of $Q_m(\psi)$ (given in the next section) seems unaffected by the erratic behavior in the supremum.

For the most part, quantum coding theorists have primarily studied qubit codes. Some work on qudit codes exists [50,63–66], but there are very few known examples. One exception is the generalization of the hexacode. A $((6,1,4))_D$ code is known to exist for all D [50]. The $((6,1,4))_D$ code belongs to a class of optimal codes called maximum distance separable (MDS) codes which saturate the quantum Singleton bound [50]—i.e., $K=D^{n-2d+2}$. Quantum MDS codes must be pure and, thus, define subspaces of maximally entangled states. Self-dual quantum MDS codes have weight distributions specified by Eq. (43). Other examples of MDS codes include the $[[6,2,3]]_D$ and $[[7,3,3]]_D$ stabilizer codes which exist for all prime D [65]. More recently, the existence of some families of quantum MDS codes was proved [66]. For example, when D is a prime power and n is even, a self-dual $((n,1,n/2+1))_D$ code exists for all $3\leqslant n\leqslant D$.

IV. MULTIPARTITE ENTANGLEMENT OVER SUBSPACES

Using Lubkin's formula [67] for the average subsystem purity, one can easily calculate the mean entanglement for random pure states sampled according to the unitarily invariant Haar measure $d\mu$ [$\int d\mu(\psi)=1$]:

$$\langle Q_m(\psi)\rangle_\psi \equiv \int d\mu(\psi) Q_m(\psi) = 1 - \frac{D^m+1}{D^n+1}. \tag{53}$$

This shows that when the overall dimension D^n is large, a typical state has nearly maximal entanglement. One could also consider the average entanglement over a subspace $\mathcal{V}$ determined by the projector $P_{\mathcal{V}}$:

$$\langle Q_m(\psi)\rangle_{\psi\in\mathcal{V}} \equiv \int_{\mathcal{V}} d\mu_{\mathcal{V}}(\psi) Q_m(\psi). \tag{54}$$

Proposition 4:

$$\langle Q_m(\psi)\rangle_{\psi\in\mathcal{V}} = \frac{D^m}{D^m-1}\left\{1 - \frac{m!\,(n-m)!}{n!\,K(K+1)}\sum_{|S|=m}\left(\mathrm{tr}_S[\mathrm{tr}_{S'}[P_\mathcal{V}]^2] + \mathrm{tr}_{S'}[\mathrm{tr}_S[P_\mathcal{V}]^2]\right)\right\}, \tag{55}$$

where $K=\mathrm{tr}P_\mathcal{V}=\dim\mathcal{V}$.

Proof: Consider an arbitrary bipartite system $\mathcal{H}=\mathbb{C}^{D_A}\otimes\mathbb{C}^{D_B}$ and define the swap operators T_{ij} $(1\leqslant i<j\leqslant 4)$ which transpose the ith and jth factors of $\mathcal{H}^{\otimes 2}$. Using the identity $\mathrm{tr}[(A\otimes B)T]=\mathrm{tr}[AB]$, where T is the swap, we first rewrite the subsystem purity of a state $|\psi\rangle\in\mathcal{H}$ as

$$\mathrm{tr}\rho_A{}^2 = \mathrm{tr}[|\psi\rangle\langle\psi|^{\otimes 2}T_{13}], \tag{56}$$

where $\rho_A=\mathrm{tr}_B|\psi\rangle\langle\psi|$. Now consider the operator

$$\omega \equiv \int_\mathcal{V} d\mu_\mathcal{V}(\psi)|\psi\rangle\langle\psi|^{\otimes 2} \tag{57}$$

supported on the totally symmetric subspace $P\mathcal{V}^{\otimes 2}$, where the projector $P=(1+T_{13}T_{24})/2$. If we choose $d\mu_\mathcal{V}$ to be the unitarily invariant Haar measure on $\mathcal{V}$, then $[U^{\otimes 2},\omega]=0$ for all unitary operators $U\in\mathrm{U}(D_AD_B)$. And since the group elements $U^{\otimes 2}$ act irreducibly on $P\mathcal{V}^{\otimes 2}$, by Schur's lemma [68], ω is simply a scalar multiple of the identity (on $P\mathcal{V}^{\otimes 2}$). Hence,

$$\omega = \frac{2}{K(K+1)}P_\mathcal{V}{}^{\otimes 2}P \tag{58}$$

on $\mathcal{H}^{\otimes 2}$, where the constant factor is found through the normalization condition $\mathrm{tr}\,\omega=1$. Thus

$$\int_\mathcal{V} d\mu_\mathcal{V}(\psi)\mathrm{tr}\rho_A{}^2 = \frac{1}{K(K+1)}\mathrm{tr}[P_\mathcal{V}{}^{\otimes 2}(1+T_{13}T_{24})T_{13}] \tag{59}$$

$$= \frac{1}{K(K+1)}(\mathrm{tr}[P_\mathcal{V}{}^{\otimes 2}T_{13}] + \mathrm{tr}[P_\mathcal{V}{}^{\otimes 2}T_{24}]) \tag{60}$$

$$= \frac{1}{K(K+1)}(\mathrm{tr}\tilde{\rho}_A{}^2 + \mathrm{tr}\tilde{\rho}_B{}^2), \tag{61}$$

where $\tilde{\rho}_A=\mathrm{tr}_B P_\mathcal{V}$ and $\tilde{\rho}_B=\mathrm{tr}_A P_\mathcal{V}$. We have derived the average purity over a subspace for an arbitrary bipartite system. Given that the measures Q_m are simply averages over bipartite purities, one can now deduce the final result. □

In particular, for a QECC $\mathcal{Q}$, one can now explicitly determine the average entanglement of encoded states in terms of the weight distribution of the code. For example,

$$\langle Q_m(\psi)\rangle_{\psi\in\mathcal{Q}} = \frac{D^m}{D^m-1}\left\{1 - \frac{m!\,(n-m)!}{n!\,(K+1)}[KA'_m(P_\mathcal{Q}) + B'_m(P_\mathcal{Q})]\right\} \tag{62}$$

$$= 1 - \frac{1}{(D^m-1)(K+1)}\sum_{i=1}^{m}\frac{m!\,(n-i)!}{n!\,(m-i)!}[KA_i(P_\mathcal{Q}) + B_i(P_\mathcal{Q})]. \tag{63}$$

Such formulas make explicit the importance of entanglement as a resource for quantum error correction. Pure codes ($B_i=A_i=0, 0<i<d$) necessarily have high levels of entanglement, but impure codes ($B_i=A_i>0, 0<i<d$) need not. However, the most compact codes (least n) all seem to be pure [55]. The relationship between entanglement and QECC's remains relatively unexplored in the literature. We do not, however, pursue this line of research any further in the current article. Elements of the proof of proposition 4 were borrowed from the work of Zanardi *et al.* [23] where the concept of entangling power was defined. In the next section we investigate multipartite entangling power with respect to the measures Q_m.

V. MULTIPARTITE ENTANGLING POWER

Following the work of Zanardi *et al.* [23], we define the *multipartite entangling power* of the unitary operator $U\in\mathrm{U}(D^n)$ acting on $(\mathbb{C}^D)^{\otimes n}$ as simply the average entanglement generated over all product states:

$$e_p(U) \equiv \int d\mu_n(\psi_1,\ldots,\psi_n)E(U|\psi_1\rangle\otimes\cdots\otimes|\psi_n\rangle), \tag{64}$$

where $|\psi_i\rangle\in\mathbb{C}^D$. The measure $d\mu_n$ is chosen to be the product of n independent Haar measures over the constituent subsystems $\mathbb{C}^D$. Consequently, the entangling power is invariant under the action of local unitaries: $e_p(U_1\otimes\cdots\otimes U_nUV_1\otimes\cdots\otimes V_n)=e_p(U)$ for all $U_i,V_i\in\mathrm{U}(D)$. If we now restrict our attention to the entanglement measures $E=Q_m$, the calculation of e_p is facilitated by a simple formula.

Proposition 5:

$$e_p^{Q_m}(U) = \frac{D_m}{D^m-1}\left(1 - \frac{m!\,(n-m)!}{n!}\sum_{|S|=m}R_S(U)\right), \tag{65}$$

where the average subsystem purities

$$R_S(U) = \left(\frac{2}{D(D+1)}\right)^n\mathrm{tr}\left[U^{\otimes 2}\left(\prod_{i=1}^{n}P_{i,i+n}\right)U^{\dagger\otimes 2}\left(\prod_{i\in S}T_{i,i+n}\right)\right], \tag{66}$$

the swap operators $T_{ij}(1\leqslant i<j\leqslant 2n)$ transpose the ith and jth factors of $(\mathbb{C}^D)^{\otimes 2n}$, and $P_{ij}\equiv(1+T_{ij})/2$.

Proof: The derivation of this formula is similar to that for proposition 4 and follows Zanardi *et al.* [23]. We first rewrite the subsystem purity of a state $|\Psi\rangle\in(\mathbb{C}^D)^{\otimes n}$ as

$$\mathrm{tr}\rho_S{}^2 = \mathrm{tr}(|\Psi\rangle\langle\Psi|^{\otimes 2}\prod_{i\in S}T_{i,i+n}). \tag{67}$$

By choosing $|\Psi\rangle=U|\psi_1\rangle\otimes\cdots\otimes|\psi_n\rangle$ we have

$$R_S(U) \equiv \int d\mu_n(\psi_1,\ldots,\psi_n)\mathrm{tr}\rho_S{}^2 \tag{68}$$

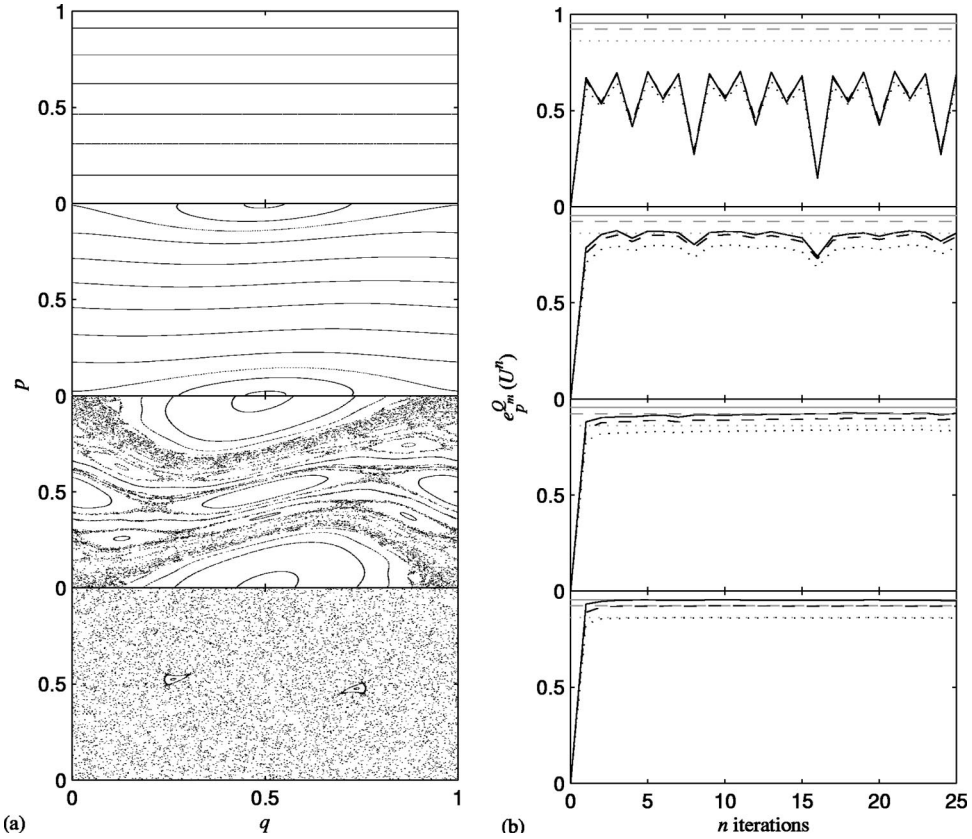

FIG. 1. (a) Phase-space portraits of the classical kicked rotor for $k=0,0.2,1$, and 6 (from top to bottom) and (b) the corresponding entangling power in the quantum case. A Hilbert space of six qubits was chosen, allowing investigation of the multipartite entanglement measures Q_m for $m=1$ (dotted line), 2 (dashed line), and 3 (solid line). The average entanglement for random states is shown in the lighter tones.

$$=\mathrm{tr}(U^{\otimes 2}\,\Omega\,U^{\dagger\otimes 2}\prod_{i\in S}T_{i,i+n}), \tag{69}$$

where

$$\Omega\equiv\int d\mu_n(\psi_1,\ldots,\psi_n)(|\psi_1\rangle\langle\psi_1|\otimes\cdots\otimes|\psi_n\rangle\langle\psi_n|)^{\otimes 2}. \tag{70}$$

Now, considering the operator $\omega\equiv\int d\mu_1(\psi)|\psi\rangle\langle\psi|^{\otimes 2}$ supported on the totally symmetric subspace $P_{12}(\mathbb{C}^D)^{\otimes 2}$, where $P_{12}=(1+T_{12})/2$, we know from previous results (see proof of proposition 4) that $\omega=2/D(D+1)P_{12}$ on $(\mathbb{C}^D)^{\otimes 2}$. Finally, given that Ω factorizes into the product of n independent averages of the form ω, we have

$$\Omega=\left(\frac{2}{D(D+1)}\right)^n\prod_{i=1}^{n}P_{i,i+n} \tag{71}$$

and our final result. □

Given our definition of the entangling power [Eq. (64)], the (Haar measure) average of $e_p(U)$ over $\mathrm{U}(D^n)$ is equivalent to the average entanglement found in random states:

$$\langle e_p^{Q_m}(U)\rangle_U=\langle Q_m(|\psi\rangle)\rangle_\psi=1-\frac{D^m+1}{D^n+1}. \tag{72}$$

Thus, typical unitaries generate nearly maximal entanglement when the overall dimension D^n is large.

VI. APPLICATION AND CONCLUSION

An immediate application of proposition 5 (and [23]) occurs in the study of the entangling capabilities of chaotic systems [24–39]. Consider a classical map of the toroidal phase space $[0,1)^2$. A quantized version may be constructed in a Hilbert space of dimension N spanned by the position states $|q_j\rangle$, where $q_j=(j+1/2)/N$ and $j=0,\ldots,N-1$. By choosing $N=D^n$, we can map our Hilbert space onto the tensor-product space $(\mathbb{C}^D)^{\otimes n}$ through the correspondence

$$|q_j\rangle=|x_1\rangle\otimes\cdots\otimes|x_n\rangle,\quad j=\sum_{i=1}^{n}x_iD^{n-i},\quad x_i\in\{0,\ldots,D-1\}, \tag{73}$$

and hence use the measures Q_m to investigate the quantum map's multipartite entangling power. The different constituent qudits x_i address the coarse (small i) and fine (large i) scales of position. Consequently, for chaotic maps where phenomena such as mixing and exponential sensitivity are

generic, we expect high levels of entanglement generation. This was noted in [36] where the entangling power of the quantum baker's map [69–73] was investigated.

For example, consider the kicked rotor (or standard map) [74]

$$q_{n+1} = q_n + p_{n+1} \bmod 1, \tag{74}$$

$$p_{n+1} = p_n + \frac{k}{2\pi}\sin 2\pi q_n \bmod 1. \tag{75}$$

The entangling power of the quantum version [75]

$$U|q_j\rangle = e^{i(kN/2\pi)\cos 2\pi q_j}\sum_{l=0}^{N-1} e^{i(\pi/N)(l-j)^2}|q_l\rangle \quad (N \text{ even}) \tag{76}$$

constructed in a Hilbert space of 6 qubits ($N=2^6$) is plotted in Fig. 1(b). Here we choose the parameter values $k=0, 0.2, 1,$ and 6 (from top to bottom), corresponding to the classical phase spaces drawn in Fig. 1(a). As expected, the entanglement saturates at a value predicted for random states [Eq. (53)] upon the appearance of chaos in the classical map. An alternative interpretation may be that quantized chaotic maps produce unitaries whose powers are typical in the space of all unitaries. This follows from Eq. (72).

In conclusion, we have shown that the average bipartite entanglement Q_m is a useful measure of multipartite entanglement, presenting a relationship between these measures and quantum-error-correcting codes. This was done by deriving an explicit formula relating the weight distribution of the code to the average entanglement of encoded states. We have also extended the work of Zanardi *et al.* (23) on entangling power to the multipartite case. Although the entanglement measures considered in this paper provide little intellectual gratification, their simplicity allows perhaps more important attributes such as computability and applicability. We must stress, however, that in defining such simple measures we offer no progress towards a deeper understanding of the nature of entanglement in the multipartite case.

ACKNOWLEDGMENTS

The author would like to thank Carlton Caves and Bryan Eastin for helpful discussions. This work was supported in part by ONR Grant No. N00014-00-1-0578 and by ARO Grant No. DAAD19-01-1-0648.

[1] M. Horodecki, Quantum Inf. Comput. **1**, 3 (2001).
[2] W. K. Wootters, Quantum Inf. Comput. **1**, 27 (2001).
[3] P. Horodecki and R. Horodecki, Quantum Inf. Comput. **1**, 45 (2001).
[4] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[5] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
[6] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[7] W. Dür, G. Vidal, and J. I. Cirac, Phys. Rev. A **62**, 062314 (2000).
[8] C. H. Bennett, S. Popescu, D. Rohrlich, J. A. Smolin, and A. V. Thapliyal, Phys. Rev. A **63**, 012307 (2001).
[9] J. Eisert and H. J. Briegel, Phys. Rev. A **64**, 022306 (2001).
[10] F. Verstraete, J. Dehaene, B. De Moor, and H. Verschelde, Phys. Rev. A **65**, 052112 (2002).
[11] F. Verstraete, J. Dehaene, and B. De Moor, Phys. Rev. A **68**, 012103 (2003).
[12] A. Miyake and M. Wadati, Quantum Inf. Comput. **2**, 540 (2002).
[13] A. Miyake, Phys. Rev. A **67**, 012108 (2003).
[14] G. Jaeger, M. Teodorescu-Frumosu, A. Sergienko, B. E. A. Saleh, and M. C. Teich, Phys. Rev. A **67**, 032307 (2003).
[15] M. Teodorescu-Frumosu and G. Jaeger, Phys. Rev. A **67**, 052305 (2003).
[16] G. Jaeger, A. V. Sergienko, B. E. A. Saleh, and M. C. Teich, Phys. Rev. A **68**, 022318 (2003).
[17] S. Bravyi, Phys. Rev. A **67**, 012313 (2003).
[18] A. Wong and N. Christensen, Phys. Rev. A **63**, 044301 (2001).
[19] D. A. Meyer and N. R. Wallach, J. Math. Phys. **43**, 4273 (2002).
[20] G. K. Brennen, Quantum Inf. Comput. **3**, 619 (2003).
[21] D. T. Pope and G. J. Milburn, Phys. Rev. A **67**, 052107 (2003).
[22] J. Preskill, *Lecture notes for Physics 219: Quantum Computation* (California Institute of Technology, Pasadena, CA, 1998); URL: http://www.theory.caltech.edu/people/preskill/ph219/
[23] P. Zanardi, C. Zalka, and L. Faoro, Phys. Rev. A **62**, 030301 (2000).
[24] M. Sakagami, H. Kubotani, and T. Okamura, Prog. Theor. Phys. **95**, 703 (1996).
[25] A. Tanaka, J. Phys. A **29**, 5475 (1996).
[26] K. Furuya, M. C. Nemes, and G. Q. Pellegrino, Phys. Rev. Lett. **80**, 5524 (1998).
[27] R. M. Angelo, K. Furuya, M. C. Nemes, and G. Q. Pellegrino, Phys. Rev. E **60**, 5407 (1999).
[28] P. A. Miller and S. Sarkar, Phys. Rev. E **60**, 1542 (1999).
[29] A. Lakshminarayan, Phys. Rev. E **64**, 036207 (2001).
[30] J. N. Bandyopadhyay and A. Lakshminarayan, Phys. Rev. Lett. **89**, 060402 (2002).
[31] A. Tanaka, H. Fujisaki, and T. Miyadera, Phys. Rev. E **66**, 045201 (2002).
[32] H. Fujisaki, T. Miyadera, and A. Tanaka, Phys. Rev. E **67**, 066201 (2003).
[33] A. Lahiri and S. Nag, Phys. Lett. A **318**, 6 (2003).
[34] A. Lakshminarayan and V. Subrahmanyam, Phys. Rev. A **67**, 052304 (2003).
[35] S. Bettelli and D. L. Shepelyansky, Phys. Rev. A **67**, 054303 (2003).
[36] A. J. Scott and C. M. Caves, J. Phys. A **36**, 9553 (2003).
[37] J. N. Bandyopadhyay and A. Lakshminarayan, Phys. Rev. E **69**, 016201 (2004).

[38] P. Jacquod, Phys. Rev. Lett. **92**, 150403 (2004).
[39] D. Rossini, G. Benenti, and G. Casati, e-print quant-ph/0309146.
[40] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[41] S. Popescu and D. Rohrlich, Phys. Rev. A **56**, R3319 (1997).
[42] C. M. Caves (private communication).
[43] G. Vidal, J. Mod. Opt. **47**, 355 (2000).
[44] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, IEEE Trans. Inf. Theory **44**, 1369 (1998).
[45] D. Gottesman, Ph.D. thesis, California Institute of Technology, Pasadena CA, 1997.
[46] E. Knill and R. Laflamme, Phys. Rev. A **55**, 900 (1997).
[47] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).
[48] M. Grassl, in *Mathematics of Quantum Computation*, edited by R. K. Brylinski and G. Chen (Chapman and Hall/CRC, London, 2002).
[49] A. Klappenecker and M. Rötteler, in *Mathematics of Quantum Computation*, edited by R. K. Brylinski and G. Chen (Chapman and Hall/CRC, London, 2002).
[50] E. M. Rains, IEEE Trans. Inf. Theory **45**, 1827 (1999).
[51] A. Klappenecker and M. Rötteler, IEEE Trans. Inf. Theory **48**, 2392 (2002).
[52] E. Knill, e-print quant-ph/9608048.
[53] E. Knill, e-print quant-ph/9608049.
[54] E. M. Rains, IEEE Trans. Inf. Theory **44**, 1388 (1998).
[55] P. Shor and R. Laflamme, Phys. Rev. Lett. **78**, 1600 (1997).
[56] E. M. Rains, IEEE Trans. Inf. Theory **45**, 2361 (1999).
[57] E. M. Rains, IEEE Trans. Inf. Theory **46**, 54 (2000).
[58] E. M. Rains, IEEE Trans. Inf. Theory **44**, 134 (1998).
[59] E. M. Rains and N. J. A. Sloane, in *Handbook of Coding Theory*, edited by V. S. Pless and W. C. Huffman (Elsevier, Amsterdam, 1998).
[60] P. Gaborit, W. C. Huffman, J.-L. Kim, and V. Pless, in *Proceedings of the 37th Allerton Conference on Communication, Control and Computing*, edited by B. Hajek and R. S. Sreenivas (Coordinated Science Laboratory UIUC, Urbana-Champaign, IL, 1999).
[61] P. Gaborit, W. C. Huffman, J.-L. Kim, and V. Pless, in *Codes and Association Schemes, DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, edited by A. Barg and S. Litsyn (American Mathematical Society, Providence, RI, 2001), Vol. 56.
[62] G. Höhn, Math. Ann. **327**, 227 (2003).
[63] A. Ashikhmin and E. Knill, IEEE Trans. Inf. Theory **47**, 3065 (2001).
[64] D. Schlingemann and R. F. Werner, Phys. Rev. A **65**, 012308 (2001).
[65] K. Feng, IEEE Trans. Inf. Theory **48**, 2384 (2002).
[66] M. Grassl, T. Beth, and M. Rötteler, e-print quant-ph/0312164.
[67] E. Lubkin, J. Math. Phys. **19**, 1028 (1978).
[68] W.-K. Tung, *Group Theory in Physics* (World Scientific, Singapore, 1985).
[69] N. L. Balazs and A. Voros, Ann. Phys. (N.Y.) **190**, 1 (1989).
[70] M. Saraceno, Ann. Phys. (N.Y.) **199**, 37 (1990).
[71] R. Schack and C. M. Caves, Appl. Algebra Eng. Commun. Comput. **10**, 305 (2000).
[72] A. N. Soklakov and R. Schack, Phys. Rev. E **61**, 5108 (2000).
[73] M. M. Tracy and A. J. Scott, J. Phys. A **35**, 8341 (2002).
[74] A. J. Lichtenberg and M. A. Lieberman, *Regular and Chaotic Dynamics* (Springer, New York, 1992).
[75] J. H. Hannay and M. V. Berry, Physica D **1**, 267 (1980).