Generalized parity measurements

Radu Ionicioiu,[1,*] Anca E. Popescu,[2,†] William J. Munro,[1] and Timothy P. Spiller[1]
[1]*Hewlett-Packard Laboratories, Filton Road, Stoke Gifford, Bristol BS34 8QZ, United Kingdom*
[2]*Bristol Robotics Laboratories, Coldharbour Lane, Bristol BS16 1QD, United Kingdom*
(Received 10 June 2008; published 14 November 2008)

Measurements play an important role in quantum computing (QC), either by providing the nonlinearity required for two-qubit gates (linear optics QC), or by implementing a quantum algorithm using single-qubit measurements on a highly entangled initial state (cluster state QC). Parity measurements can be used as building blocks for preparing arbitrary stabilizer states, and, together with one-qubit gates, are universal for quantum computing. Here we generalize parity gates by using a higher-dimensional (qudit) ancilla. This enables us to go beyond the stabilizer or graph state formalism and prepare other types of multiparticle entangled states. The generalized parity module introduced here can prepare in *one shot*, heralded by the outcome of the ancilla, a large class of entangled states, including Greenberger-Home-Zeilinger states GHZ_n, W_n, Dicke states $\mathcal{D}_{n,k}$, and, more generally, certain sums of Dicke states, like G_n states used in secret sharing. For W_n states it provides an exponential gain compared to linear-optics-based methods.

DOI: 10.1103/PhysRevA.78.052326 PACS number(s): 03.67.Lx, 03.67.Mn, 42.50.Dv

I. INTRODUCTION

Quantum-information processing (QIP) and quantum computation (QC) promise to be disruptive technologies: applications include quantum algorithms for fast factoring [1], database search [2], and secure key distribution [3]. However, storing and processing information on quantum systems is difficult due to decoherence, constraining state-of-the-art quantum hardware to a few qubits. This limitation implies that at present one of the best ways to use scarce quantum resources is distributed QIP over several nodes. Useful distributed tasks may be achieved even if the total number of qubits involved is less than that which can be simulated conventionally.

Measurement-based quantum computing has recently attracted considerable interest as a new paradigm for QIP. This interest has been spearheaded by two different models which complement the "standard model" of quantum computation, the quantum network model [4]. The first one initiated the field of linear optics QC [5,6], whereas the second started the cluster state QC [7].

In this context the cluster state emerged as a quintessential resource which can be constructed before, and consumed during, computation [7]. A core primitive used in building the cluster state is the parity gate [8,9]. As shown previously, the parity gate [10,11] and the related photonic module [12] can be used to prepare deterministically arbitrary stabilizer or graph states, hence any cluster state used as a resource in the one-way quantum computing model [7].

A standard quantum network for the parity gate uses a qubit ancilla [10]. Here we relax this constraint and instead use a qudit ancilla.[1] With this we show that we can prepare, heralded by the outcome of the ancilla, a large class of entangled states in one shot, i.e., with a *single* application of the generalized parity module. By tuning the dimension d of the ancilla with respect to the number of input qubits n we obtain several known families of entangled states: Greenberger-Home-Zeilinger states GHZ_n, W_n, Dicke $\mathcal{D}_{n,k}$, G_n, and their generalization $G_{n,k}$ states. These states are an important resource in several QIP protocols, including teleportation [14], dense coding [15], quantum key distribution [3], secret sharing $(G_n, G_{n,k})$ [16], $1 \rightarrow 3$ telecloning [17], and open destination teleportation $(\mathcal{D}_{4,2})$ [18].

A very appealing feature of the generalized parity module is that it can be implemented so as to prepare directly entangled states of photons. Thus the module can be used as the enabling building block in a distributed QIP network and for small scale QIP applications. The entangled states can be created with qubits that readily distribute, without any need for interconversion.

The structure of the paper is the following. In Sec. II we give a brief overview of the parity gate and its use in the photonic module. In Sec. III we find the solution for the generalized parity module, then construct examples of how to prepare several classes of entangled states. We conclude in Sec. IV.

II. PARITY MEASUREMENTS

A. The parity gate: An overview

Historically the parity gate has been used in linear optics to construct a controlled-NOT (CNOT) gate [8], but the outcome was probabilistic. The importance of the parity gate re-emerged in the context of fermionic quantum computation with linear elements. Beenakker *et al.* have shown that universality can be achieved in fermionic QC if we supplement linear gates with a single ingredient: charge parity measurements [9]. This result changed the prevailing wisdom that fermionic QC cannot be done with only linear elements and (single-qubit) measurements [19,20]. In contrast, bosons have no such limitations and universality can be achieved in

*radu.ionicioiu@hp.com
†anca.popescu@brl.ac.uk
[1]An example of using a high-dimensional (qudit) ancilla in teleportation is Ref. [13].

photonic QC with linear gates, single-photon sources and photon-number-discriminating detectors, as shown by Knill, Laflamme, and Milburn (KLM) [5]. The difference between bosons and fermions in terms of computational power comes from the contrasting behavior at a beam splitter: bunching (bosons) versus antibunching (fermions). This produced a flurry of activity in both theory and implementations, with several proposals for parity measurements in various systems [8,21–31].

A parity (P) gate can be viewed—in an implementation-independent manner—simply as a black box with two inputs x and y and an ancilla initialized to $|0\rangle$. The gate leaves invariant the basis states $|xy\rangle$, $x,y=0,1$, and outputs the parity $\mathsf{p}=x\oplus y:=x+y \bmod 2$ of the inputs, i.e.:

$$|xy\rangle|0\rangle \to |xy\rangle|x\oplus y\rangle. \tag{1}$$

Upon measurement, the ancilla gives a classical bit, the parity of the input state. If the input state is a superposition $\Sigma_{i,j}a_{ij}|ij\rangle$, the P gate projects it on a subspace of eigen-parity, i.e., on $a_{00}|00\rangle+a_{11}|11\rangle$ (for $\mathsf{p}=0$) or on $a_{01}|01\rangle+a_{10}|10\rangle$ (for $\mathsf{p}=1$). Building on previous work from quantum optics [8], Beenakker *et al.* [9] constructed a deterministic *quantum* CNOT gate out of two parity gates, an ancilla, and postprocessing, thus proving the universality of parity measurements (along with single-qubit gates).

In effect the P gate is an oracle, answering the simplest possible question when presented with two (classical) inputs x,y: Are the two inputs equal? In translation, $\mathsf{p}=0\Leftrightarrow$yes and $\mathsf{p}=1\Leftrightarrow$no. It is surprising that such a simple gate can provide universality, where single-qubit measurement failed to [19,20]. It confirms yet again how counterintuitive quantum mechanics is, exemplifying how *less is more* in the quantum world. This is to say, knowing less (the parity), we can do more (achieve universality). The key is knowing less in a quantum sense, i.e., maintaining superposition.

As can be inferred from the action (1), a quantum network for the P gate consists of two CNOT gates, coupling each input qubit once to the ancilla, followed by a measurement of the ancilla. We can extend the network to accommodate several input qubits, each coupled once (via a CNOT gate) to a common ancilla, which is then measured. In this case the gate gives the parity of all n inputs

$$|x_1x_2\cdots x_n\rangle|0\rangle \to |x_1x_2\cdots x_n\rangle|\mathsf{p}\rangle, \quad \mathsf{p}=\sum_i x_i \mod 2. \tag{2}$$

A very nice feature of this extension of the parity gate is that each qubit interacts only once with the ancilla. The qubits can therefore be naturally of travelling form; there is no need for them to wait around and interact again with the ancilla. For example, an extended parity gate therefore proves to be a very useful tool for preparing photonic stabilizer states and can function as a stand-alone *photonic module* [12]. Suppose we have an N-photon pulse and that each photon interacts (sequentially) with an ancilla qubit, e.g., an atom in a cavity or an NV center in diamond [32], via a simple controlled interaction: the interaction flips the atom state if the photon is σ^- polarized and does nothing if it is σ^+ polarized. For simplicity in the following we use $|\pm\rangle=(|0\rangle\pm|1\rangle)/\sqrt{2}$ states which differ from $\sigma^\pm$ by a simple phase shift, $\sigma^\pm=\mathrm{diag}(1,i)|\pm\rangle$. Thus we assume the interaction

$$|+\rangle|0\rangle_a \to |+\rangle|0\rangle_a,$$

$$|-\rangle|0\rangle_a \to |-\rangle X|0\rangle_a, \tag{3}$$

where $|i\rangle_a$ denotes the ancilla state; in the following we will denote the Pauli operators for a qubit by X,Y,Z. This photonic module can prepare an arbitrary N-photon stabilizer state using only parity measurements on the ancilla qubit (the atom) and single qubit gates. Given an N-photon state $|\Psi\rangle_N$ interacting sequentially with the ancilla qubit $|i\rangle_a$, the action of the photonic module is [12,33]

$$|\Psi\rangle_N|i\rangle_a \to (P_0\otimes\mathbb{1}+P_1\otimes X)|\Psi\rangle_N|i\rangle_a \tag{4}$$

where $P_k:=\frac{1}{2}[\mathbb{1}+(-1)^kX^{\otimes N}]$ are even (odd) parity projectors acting on the 2^N-dimensional photon space.

Let us now start to go beyond simple parity gates made from CNOT gates acting on the ancilla. The first question we address is the following: apart from the NOT gate, are there other unitary transformations $U\in\mathrm{U}(2)$ acting on the ancilla, such that the control-U gate (controlled by an input qubit) can be used to construct a parity gate? At first sight, there are two requirements for a good U. First, we need to have $|\phi\rangle\perp U|\phi\rangle$, for a suitable ancilla state $|\phi\rangle$. This is essential in order to unambiguously distinguish odd and even parity states. The second condition is $U^2=\mathbb{1}$, as we want the states $|00\rangle$ and $|11\rangle$ of the qubits to be indistinguishable. In the next section we will find the general solution of this problem and we will show that the second requirement is not independent: it is a simple consequence of the orthogonality condition, which is the crucial one.

B. Ancilla as a qubit

In this section we answer the previous question and find the general unitary $U\in\mathrm{U}(2)$ that can be used to construct a parity gate. The solution has practical consequences: it enables to find the right interactions required to implement a P gate.

We first consider the case where the ancilla is still a qubit, so $d=2$. We are looking for the unitaries $U\in\mathrm{U}(2)$ and the states $|\phi\rangle$ such that $|\phi\rangle$ and $|U\phi\rangle:=U|\phi\rangle$ are orthogonal, namely,

$$\langle\phi|U\phi\rangle=0. \tag{5}$$

By diagonalizing U, $U=VDV^\dagger$, with $V\in\mathrm{U}(2)$ and $D=e^{i\varphi_0}\mathrm{diag}(1,e^{i\varphi_1})$, the previous problem is equivalent to finding $|\psi\rangle:=V^\dagger|\phi\rangle$ satisfying $\langle\psi|D\psi\rangle=\langle\phi|U\phi\rangle=0$. Clearly V is just a change of basis, so the physics is in the eigenvalues. Neglecting the overall phase $e^{i\varphi_0}$, the solution follows immediately:

$$D=\begin{pmatrix}1 & \\ & -1\end{pmatrix}=Z,$$

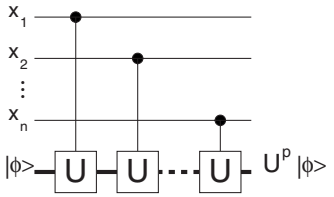

FIG. 1. A generalized parity module. The generalized parity is defined as $\mathsf{p}=\Sigma_i x_i \bmod d$, with $x_i=0,1$. The dimension of the ancilla (bold line) Hilbert space is $\dim \mathcal{H}=d$. If the ancilla is a qubit $d=2$ and $U=X$, the network is equivalent to the photonic module discussed in [12].

$$|\psi\rangle = (|0\rangle + e^{i\varphi}|1\rangle)/\sqrt{2}. \tag{6}$$

Now, although very simple, this solution has an intuitive geometric interpretation which will provide inspiration for the generalized solution that forms the main result of this paper. Furthermore, the key features of the result can be expressed mathematically in a form that lends naturally to generalization.

First, we observe that the states $|\psi\rangle$ are on the equator of the Bloch sphere and thus are perpendicular to the Oz axis associated with $D=Z$. Now any unitary U can be viewed as a rotation of the Bloch sphere through angle α around an axis $\vec{n}$, $U=\exp(i\alpha\vec{\sigma}\cdot\vec{n})$ [with $\vec{\sigma}=(X,Y,Z)$]. Therefore, in general, the states $|\phi\rangle$ satisfying $\langle\phi|U\phi\rangle=0$ are on the great circle of the Bloch sphere perpendicular to $\vec{n}$. Moreover, as the solution (6) satisfies $D^2=\mathbb{1}$, we obtain $U^2=\mathbb{1}$ rather than imposing it, and so $\alpha=\pi/2$. Hence U is of the form $U=i\vec{\sigma}\cdot\vec{n}$.

Second, we observe that the equator of the Bloch sphere is the orbit of $|+\rangle$ under the action of the group $G=\{\mathrm{diag}(1,e^{i\varphi})\}$. Thus all the states $|\psi\rangle$ satisfying $\langle\psi|Z|\psi\rangle=0$ can be written as $|\psi\rangle=g|+\rangle$, with $g\in G$. Note also that the group G is nothing but the commutant of Z (up to a global phase), namely $Z' := \{M\in \mathrm{U}(2),[M,Z]=0\}=\{\mathrm{diag}(e^{i\theta_0},e^{i\theta_1})\}$.

III. GENERALIZED PARITY

We are now ready to relax the constraint of the qubit ancilla and explore the general case where we have at our disposition a higher dimensional space, i.e., a qudit. Before proving the general result it will be illuminating to see an example.

A. A simple application: W states

In the simplest generalization of the P gate we have three qubits coupled to a common qutrit ancilla, as in Fig. 1 with $d=n=3$. In this case we are looking for a unitary $U\in \mathrm{U}(3)$ and a vector $|\psi\rangle$ such that the set $\{|\psi\rangle, U|\psi\rangle, U^2|\psi\rangle\}$ is orthonormal. A particular solution is given by

$$U=\mathrm{diag}(1,\omega,\omega^2),$$

$$|\psi\rangle = (|0\rangle + |1\rangle + |2\rangle)/\sqrt{3} \tag{7}$$

with $\omega=e^{2\pi i/3}$. Using the identities $1+\omega+\omega^2=0$ and $U^3=\mathbb{1}$, it can be easily shown that the above solution (7) satisfies the required orthogonality conditions.

A natural question arises: What is this useful for? We show that the simple network in Fig. 1 for the case $d=3$ can prepare (probabilistically) W states,

$$|\mathrm{W}\rangle = (|001\rangle + |010\rangle + |100\rangle)/\sqrt{3}. \tag{8}$$

Suppose that the initial product state of the qubits is the equal superposition of all basis states, i.e., $|+\rangle^{\otimes 3}=2^{-3/2}\Sigma_{i=0}^{7}|i\rangle$. The ancilla qutrit is prepared in the initial state $|\psi\rangle$ and, after interacting with the three qubits, is measured. Since the three possible states of the ancilla are orthogonal, they can be distinguish with certainty and upon the projective measurement, the qubit register is in one of the three possible states:

$$|\mathrm{GHZ}\rangle = (|000\rangle + |111\rangle)/\sqrt{2}, \quad p=1/4,$$

$$|\mathrm{W}\rangle = (|001\rangle + |010\rangle + |100\rangle)/\sqrt{3}, \quad p=3/8,$$

$$|\mathrm{W}'\rangle = (|110\rangle + |101\rangle + |011\rangle)/\sqrt{3}, \quad p=3/8 \tag{9}$$

where p is the probability. As $|\mathrm{W}'\rangle=X^{\otimes 3}|\mathrm{W}\rangle$, this simple quantum circuit prepares W states with probability $p(\mathrm{W})=3/4$. Postprocessing, i.e., locally bit flipping all qubits, can be applied to transform $|\mathrm{W}'\rangle$ to $|\mathrm{W}\rangle$ if required; alternatively this classical information can be supplied along with the W state, dependent upon what it is to be used for. The best method so far for producing W states using linear elements and postselection has a probability of success of 3/16 [34], hence four times lower.

It is worth emphasizing that W states are *not* stabilizer or graph states, hence they cannot be described in the stabilizer formalism. As such they cannot be prepared systematically, in one-shot, using the photonic module or P gates [10,12] as described above (they require extra resources or ancillas). It is known that W states belong to a different entanglement class than GHZ states, and the two families cannot be interconverted through local operations and classical communications [35]; thus they represent different entanglement resources. For example, W states are more robust under qubit losses than GHZ states.

B. Ancilla as a qudit

We are now ready to prove the general result, addressing the case where the ancilla is a qudit, so $\dim \mathcal{H}=d$. We let $\{|0\rangle,\ldots,|d-1\rangle\}$ be the computational (or Z) basis in $\mathcal{H}$. Let $\mathbb{Z}_d=\{0,1,\ldots,d-1\}$. The generalized Pauli operators X_d and Z_d for qudits are

$$X_d|i\rangle = |i\oplus 1\rangle,$$

$$Z_d|i\rangle = \omega^i|i\rangle, \tag{10}$$

with $\omega := e^{2\pi i/d}$ and $\oplus$ now addition mod d. Thus $Z_d := \mathrm{diag}(1,\omega,\omega^2,\ldots,\omega^{d-1})$ in this basis. We will also need the Fourier (or X) basis, defined as the Fourier transform of the Z basis:

$$|u_k\rangle = d^{-1/2}\sum_{j=0}^{d-1}\omega^{-kj}|j\rangle,$$

$$|j\rangle = d^{-1/2}\sum_{k=0}^{d-1} \omega^{jk}|u_k\rangle, \tag{11}$$

from which follows the useful identity $d^{-1}\Sigma_j \omega^{jk} = \delta_{0k}$. The action of the Pauli operators on this basis is

$$X_d|u_k\rangle = \omega^k|u_k\rangle,$$

$$Z_d|u_k\rangle = |u_{k-1}\rangle. \tag{12}$$

Generalizing the problem of Sec. II B to the full problem, we now want to find a unitary $U \in \mathrm{U}(d)$ and a state $|\phi\rangle \in \mathcal{H}$ such that the set $\{|\phi\rangle, U|\phi\rangle, \ldots, U^{d-1}|\phi\rangle\}$ is orthonormal; this is necessary as we want to discriminate unambiguously between states of different parity. The analogue of the previous condition (5) is now

$$\langle\phi|U^i\phi\rangle = 0, \quad \forall\ i = 1, \ldots, d-1. \tag{13}$$

Following similar reasoning to that of Sec. II B, we need only to consider diagonal unitaries. Let $U = VDV^\dagger$, with $D = \mathrm{diag}(\lambda_0, \ldots, \lambda_{d-1})$ containing the eigenvalues $\lambda_i := e^{i\varphi_i}$ of U; then $\langle\phi|U\phi\rangle = \langle\psi|D\psi\rangle = 0$ with $|\psi\rangle := V^\dagger|\phi\rangle$. Therefore, we can focus on diagonal unitaries $D \in U(d)$ satisfying

$$\langle\psi|D^i\psi\rangle = \delta_{0i}, \quad \forall\ i \in \mathbb{Z}_d \tag{14}$$

for some $|\psi\rangle \in \mathcal{H}$. The objective is to find solutions analogous to those given in (6).

First, we observe that it is clear that not all U will have solutions to the above equation. Indeed, suppose the unitary is an infinitesimal rotation, $U = \exp(i\epsilon Z)$, $\epsilon \approx 0$, i.e., very close to the identity. Then $\langle\phi|U\phi\rangle \simeq 1 + i\epsilon\langle\phi|Z|\phi\rangle \approx 1$ for all $|\phi\rangle \in \mathcal{H}$.

Second, generalizing the properties of the states given in (6), we observe that if for a given D there is a vector satisfying $\langle\psi_0|D^i\psi_0\rangle = 0$, then the orbit of $|\psi_0\rangle$ under the action of the commutant $D' := \{g \in U(d), [g, D] = 0\}$ will also be a solution. Hence, if $|\psi'\rangle = g|\psi_0\rangle$ with $g \in D'$, then $\langle\psi'|D^i\psi'\rangle = \langle\psi_0|g^\dagger D^i g\psi_0\rangle = \langle\psi_0|D^i\psi_0\rangle = 0$.

We decompose the state as $|\psi\rangle = \Sigma_{j\in\mathbb{Z}_d} a_j|j\rangle$, so Eq. (14) becomes

$$\sum_{j=0}^{d-1} |a_j|^2 \lambda_j^i = \delta_{0i}, \quad \forall\ i \in \mathbb{Z}_d. \tag{15}$$

There are two possible cases to address, dependent upon the nature of the eigenvalues of D.

Nondegenerate case. We assume all the eigenvalues of $D = \mathrm{diag}(\lambda_0, \ldots, \lambda_{d-1})$ are distinct, $\lambda_j \neq \lambda_k$, $\forall j \neq k$. Using the expansion of the Vandermonde determinant, we obtain

$$\frac{1}{|a_j|^2} = \prod_{i\in\mathbb{Z}_d, i\neq j} \left(1 - \frac{\lambda_j}{\lambda_i}\right)$$

$$= \prod_{i\in\mathbb{Z}_d, i\neq j} 2\left|\sin\frac{\varphi_j - \varphi_i}{2}\right| e^{(\varphi_j-\varphi_i)/2 - \pi/2 + n_{ij}\pi} \tag{16}$$

with $n_{ij} \in \mathbb{Z}$; the last equation follows from the polar decomposition of each term in the product. Requiring the right-hand side to be real and positive, it follows that $\varphi_j = \varphi_0 + (2\pi/d)m_j$, for some integers m_j. Since all the phases are different (as the eigenvalues are nondegenerate), we can take $\varphi_j = \varphi_0 + (2\pi/d)j$, modulo a reordering of the eigenvalues. The unitary transformation we are looking for is

$$D = e^{i\varphi_0}\,\mathrm{diag}(1, \omega, \omega^2, \ldots, \omega^{d-1}) = e^{i\varphi_0} Z_d. \tag{17}$$

Substituting these phases into Eq. (16) we get

$$\frac{1}{|a_j|^2} = \prod_{i\in\mathbb{Z}_d, i\neq j} (1 - \omega^{j-i}) = \prod_{1\leq i\leq d-1} (1 - \omega^i) = d. \tag{18}$$

This shows that $|\psi\rangle$ is an equal superposition of all basis states

$$|\psi\rangle = d^{-1/2}\sum_i e^{\theta_i}|i\rangle. \tag{19}$$

As before, there is an appealing geometric interpretation. The entire manifold of solutions $\mathcal{M} = \{|\psi\rangle\}$ can be generated by acting with the commutant of Z_d (in $U(d)$) on a single state, say $|u_0\rangle = d^{-1/2}\Sigma_i|i\rangle$; hence $\mathcal{M} = Z_d'|u_0\rangle$, i.e., is the orbit of $|u_0\rangle$ under Z_d'. The commutant is the set $Z_d' = \{\mathrm{diag}(e^{\theta_0}, \ldots, e^{\theta_{d-1}})\}$. Thus we have proved the following:

Proposition. Let $|\phi\rangle \in \mathcal{H}$, $\dim\mathcal{H} = d$, and $U \in U(d)$ a unitary acting on $\mathcal{H}$ such that the set $\{|\phi\rangle, U|\phi\rangle, \ldots, U^{d-1}|\phi\rangle\}$ is orthonormal. If U has nondegenerate eigenvalues, then

$$U = VZ_dV^\dagger$$

$$|\phi\rangle = Vg|u_0\rangle \tag{20}$$

where $V \in \mathrm{U}(d)$ is an arbitrary unitary and $g \in Z_d'$ belongs to the commutant of Z_d.

Degenerate case. We assume that D has degenerate eigenvalues, $D = \mathrm{diag}(\lambda_0\mathbb{1}_{k_0}, \ldots, \lambda_{s-1}\mathbb{1}_{k_{s-1}})$, where the k_i's are the degeneracies of the s distinct eigenvalues and $\Sigma_{i\in\mathbb{Z}_s} k_i = d$. In this case the system (15) is singular and we have only s independent equations with a Vandermonde discriminant. As before, the eigenvalues are $\lambda_j = e^{i\phi_0}\omega^j$, with $\omega = e^{2\pi i/s}$ a root of unity of degree s. Since $D^s = \mathbb{1}$, now we can have only s orthonormal vectors $\{|\psi\rangle, D|\psi\rangle, \ldots, D^{s-1}|\psi\rangle\}$. The absolute value of the amplitudes $|a_i|$ are no longer fixed as in the nondegenerate case from Eq. (18); in this case we have only s constraints for d variables $|a_j|^2$, namely,

$$|a_0|^2 + \cdots + |a_{k_0-1}|^2 = 1/s,$$

$$\vdots$$

$$|a_{d-k_s}|^2 + \cdots + |a_{d-1}|^2 = 1/s, \tag{21}$$

where now all the amplitudes $|a_i|$ belonging to a degenerate eigenspace are on a hypersphere of radius $s^{-1/2}$, generalizing Eq. (18).

C. A generalized parity module

Having determined the general solution for U, we can now calculate the action of the generalized parity module (Fig. 1) on an arbitrary state of the qubits. We discuss two cases, namely, $U = Z_d$ and $U = X_d$. In order to make the connection with the photonic module [12], we assume the qubits

are photons interacting with an atom in a cavity (the qudit ancilla). Of course, this is not the only possible implementation, but we use it here as an illustration of the application of the generalized parity module.

We assume the action of the module on a single photon qubit is

$$|0\rangle|\phi\rangle \to |0\rangle|\phi\rangle,$$

$$|1\rangle|\phi\rangle \to |1\rangle Z_d|\phi\rangle. \tag{22}$$

Now, if the atomic ancilla is in one of the Z-basis states $|j\rangle$, the transformation of an arbitrary photon state $|\psi\rangle = a|0\rangle + b|1\rangle$ is [33]

$$|\psi\rangle|j\rangle \to [a|0\rangle + \omega^j b|1\rangle]|j\rangle = [A_1^j|\psi\rangle]|j\rangle,$$

where now the photon gets a phase shift $A_1^j = \mathrm{diag}(1, \omega^j)$ dependent upon the basis state $|j\rangle$. The action of the module on a general N-photon state $|\Psi\rangle_N$ follows straightforwardly, as each photon interacts independently with the module: $|\Psi\rangle_N|j\rangle \to [A_N^j|\Psi\rangle_N]|j\rangle$; here $A_N := A_1^{\otimes N}$ is a tensor product of identical single-qubit phase shifts acting on each photon. If, alternatively, the ancilla is in one of the X-basis states $|u_k\rangle$, we have

$$|\Psi\rangle_N|u_k\rangle \to \sum_{i=0}^{d-1} P_i \otimes Z_d^i|\Psi\rangle_N|u_k\rangle. \tag{23}$$

The projectors are defined as

$$P_i := d^{-1}\sum_k \omega^{-ik} A_N^k \tag{24}$$

It is easy to see that the operators $\{P_j\}$ have the following properties: (i) $P_j^\dagger = P_j$; (ii) $P_j P_k = \delta_{jk} P_k$; (iii) $\Sigma_j P_j = \mathbb{1}$; hence they form a complete set of orthogonal projectors.

For a state $|\Psi\rangle$, the probability of projecting on the j parity subspace is

$$p(j) = \langle\Psi|P_j|\Psi\rangle. \tag{25}$$

The dimension of the jth parity subspace is $\dim P_j = 2^N \langle +|^N P_j |+\rangle^N$, where $|+\rangle^N := H^{\otimes N}|0\rangle^{\otimes N}$ is the equal superposition state of N qubits and H is the Hadamard gate. Since the P_j's are a complete set of projectors, we obviously have $\Sigma_j \dim P_j = 2^N$.

The interaction (22) is suitable if the photon encodes a dual-rail (or mode) qubit and the ancilla (e.g., an atom in a cavity) is situated in rail 1, in which case a Z_d gate is enacted on the ancilla. However, as discussed in Sec. II, for some systems a more natural interaction is with the $\sigma^\pm$ polarization states of the photon. Neglecting a trivial phase, we therefore also consider the following interaction:

$$|+\rangle|\phi\rangle \to |+\rangle|\phi\rangle,$$

$$|-\rangle|\phi\rangle \to |-\rangle X_d|\phi\rangle. \tag{26}$$

Then the action of the module is given by (with the ancilla in the Z-basis state $|j\rangle$)

$$|\Psi\rangle_N|j\rangle \to \sum_{i=0}^{d-1} \tilde{P}_i \otimes X_d^i|\Psi\rangle_N|j\rangle. \tag{27}$$

The new projectors are $\tilde{P}_i = d^{-1}\Sigma_k \omega^{-ik} B_N^k$, with $B_N := B_1^{\otimes N}$; $B_1 = H\mathrm{diag}(1, \omega)H = HA_1H$ is a single-qubit x rotation on the photon. Mathematically, this is nothing but a change of basis compared to (22)–(24), but this is relevant from a physical perspective: given a quantum system, certain gates are easier to implement experimentally than others. For example, atoms interact naturally with circularly polarized light and the same holds for excitons created in quantum dots.

It is worth mentioning an interesting duality property between the two actions discussed above: Z_d acts on (the ancilla prepared in) $|u_0\rangle$, which is the Fourier transform of the Z-basis state vector $|0\rangle$; similarly, X_d acts on the vector $|0\rangle$, which is the (inverse) Fourier transform of its own basis eigenvector $|u_0\rangle$. In other words, Z_d acts on the eigenvectors of its Fourier transform X_d (and vice versa).

D. Preparation of Dicke states

Having calculated the action of the generalized parity module on arbitrary input states of qubits, we use these results to show how the module can prepare certain classes of quantum states, interesting from the perspective of quantum information and/or many-body physics. Our first example is the class of Dicke states [36]. These are symmetric states of n particles with k excitations (i.e., 1's) and can be seen as multiparticle generalizations of W_n states [36,37]:

$$\mathcal{D}_{n,k} = \binom{n}{k}^{-1/2} \sum_j \mathcal{S}_j^{(n)}|0\rangle^{\otimes n-k}|1\rangle^{\otimes k}, \tag{28}$$

where the sum is over all *distinct* permutations $\mathcal{S}_j^{(n)}$ of n particles. Examples of Dicke states are n-particle W_n states, $\mathrm{W}_n = \mathcal{D}_{n,1} = n^{-1/2}(|10\ldots0\rangle + \cdots + |00\ldots1\rangle)$. They satisfy a simple duality property

$$\mathcal{D}_{n,n-k} = X^n \mathcal{D}_{n,k}, \tag{29}$$

where $X^n := X^{\otimes n}$ is a bit flip on all qubits.

The generalized parity module can prepare Dicke states in one shot, i.e., with a single application of the module. In any one run, the exact state prepared is heralded by the measurement outcome of the ancilla. Consider the case where the dimension of the ancilla space is $d=n$, i.e., equal to the number of qubits. Assume the initial product state of the n qubits is $|+\rangle^{\otimes n} = 2^{-n/2}\Sigma_{j\in\mathbb{Z}^n}|j\rangle$, an equal superposition of all basis states. Applying the parity module (Fig. 1) on this state will project it to one of the following n states:

$$\{\mathrm{GHZ}_n, \mathcal{D}_{n,1} = \mathrm{W}_n, \ldots, \mathcal{D}_{n,k}, \ldots, \mathcal{D}_{n,n-1} = X^n \mathrm{W}_n\}. \tag{30}$$

Taking into account the duality property (29), for $n>2$ there are only $\lfloor n/2 \rfloor + 1$ distinct states (up to local bit flips). If $n=2$ there is only one distinct state, since $|00\rangle + |11\rangle$ and $|01\rangle + |10\rangle$ are locally equivalent. The probability of obtaining one of these states is

$$p(\mathrm{GHZ}_n) = 2^{-n+1},$$

$$p(\mathcal{D}_{n,k}) = 2^{-n+1}\binom{n}{k}. \tag{31}$$

The probability peaks for Dicke states having half the number of excitations $\mathcal{D}_{n,n/2}$. For this specific example the probability scales extremely well, only damping with the root of the qubit number, so $(\mathcal{D}_{2k,k}) \sim 2/\sqrt{\pi k}$.

How efficient is this method compared to other means of preparing W_n states? From (31) we have $p(W_n)=n2^{1-n}$. In a recent article [34] the success probability for producing W_n states using linear elements and postselection was $p(W_n)=n2^{2-2n}$ (n odd) and $n2^{3-2n}$ (n even). This shows that our method gives an exponential gain of at least 2^{n-2} compared to the method in Ref. [34].

Before going further, we will review briefly the importance of these states. From a theoretical point of view various Dicke states have different entanglement properties and as such it is important to understand and characterize them. A recent study [38] showed that $\mathcal{D}_{4,2}$ states are more robust under decoherence that W_4, GHZ_4, and linear cluster states CL_4. Also, W_n states lead to stronger nonclassicality than GHZ_n states [39]. $\mathcal{D}_{4,2}$ can be used in $1\rightarrow 3$ telecloning and open destination teleportation [18]; it has another interesting property: measuring one qubit, one can obtain either a W_3 or a GHZ_3 state. As mentioned before, these two states belong to different entanglement families and cannot be transformed into each other by stochastic local operations and classical communication.

Several of these states have been observed experimentally in various systems. These include ion traps ($W_4,\ldots,W_8$ [40] and GHZ_6 [41]) and photons ($\mathcal{D}_{4,2}$ [18]).

E. The case $n>d$

In the previous section the number of qubits was equal to the dimension of the ancilla. Another interesting case is $n>d$. ($n<d$ is trivial.)

Suppose we again prepare the qubits in the equal superposition state $|+\rangle^{\otimes n}$. If after the measurement the ancilla is found to be k, $k=0,\ldots,d-1$, then the qubits are projected to (in the following we neglect normalizations)

$$\psi_k = \sum_{x:\mathrm{p}(x)=k \bmod d} |x\rangle = \binom{n}{k}^{1/2}\mathcal{D}_{n,k} + \binom{n}{k+d}^{1/2}\mathcal{D}_{n,k+d} + \cdots, \tag{32}$$

where $\mathcal{D}_{n,0}=|0\rangle^{\otimes n}$. The sum is over all basis states of n qubits $|x\rangle := |x_1x_2\cdots x_n\rangle$ such that the number of 1's is k mod d, $\mathrm{p}(x)=\Sigma_j x_j = k \bmod d$. Thus ψ_k is a weighted sum of Dicke states, and in general there is no simple way of characterizing such sums.

It is insightful to analyze a few examples and see how the projected states vary, first, with the dimension d of the ancilla (at a fixed number of qubits n) and second, with increasing number of qubits (when the ancilla has the same dimension).

Example 1. $n=4$, $d=3$. Upon measurement of the ancilla, we obtain one of the following states (the subscript indicates the eigenvalue of the measured ancilla, i.e., the generalized parity):

$$\psi_0 = 0000 + 1110 + 1101 + 1011 + 0111 = X^4\psi_1,$$

$$\psi_1 = 0001 + 0010 + 0100 + 1000 + 1111 = 2W_4 + 1111,$$

$$\psi_2 = \mathcal{D}_{4,2}. \tag{33}$$

Example 2. $n=5$, $d=3$. Increasing by 1 the number of qubits but keeping the ancilla the same we obtain (again, up to normalization)

$$\psi_0 = 00000 + \sqrt{10}\mathcal{D}_{5,3},$$

$$\psi_1 = \mathcal{D}_{5,1} + \mathcal{D}_{5,4} = (\mathbb{1} + X^5)W_5,$$

$$\psi_2 = \sqrt{10}\mathcal{D}_{5,2} + 11111 = X^5\psi_0. \tag{34}$$

Example 3. $n=5$, $d=4$. In this case the four projected states are

$$\psi_0 = 00000 + \sqrt{5}\mathcal{D}_{5,4} = X^5\psi_1,$$

$$\psi_1 = \sqrt{5}W_5 + 11111,$$

$$\psi_2 = \mathcal{D}_{5,2},$$

$$\psi_3 = \mathcal{D}_{5,3} = X^5\psi_2. \tag{35}$$

F. Generalized G_n states and secret sharing

An interesting family of states is the G_n introduced in [16]

$$G_n := \frac{1}{\sqrt{2}}(W_n + X^nW_n). \tag{36}$$

Example 4. $d=n-2$. In this case one of the outcomes of the parity module is the G_n states (we omit normalization)

$$\psi_0 = 0^{\otimes n} + \binom{n}{2}^{1/2}\mathcal{D}_{n,n-2} = X^n\psi_2,$$

$$\psi_1 = W_n + \mathcal{D}_{n,n-1} = (\mathbb{1} + X^n)W_n = G_n,$$

$$\psi_2 = \binom{n}{2}^{1/2}\mathcal{D}_{n,2} + 1^{\otimes n},$$

$$\vdots$$

$$\psi_{n-3} = \mathcal{D}_{n,n-3} = X^n\mathcal{D}_{n,3}. \tag{37}$$

As shown in Ref. [16], the G_n states can be used for secret sharing. In this protocol, Alice (the secret holder) wants to distribute her secret among $n-1$ parties $B_1,\ldots,B_{n-1}$ (the Bobs) such that all these Bobs have to cooperate to find out the secret; hence, if at least one Bob is left outside, the remaining ones cannot recover Alice's secret.

Define the following generalization of G_n states

$$G_{n,k} := \frac{1}{\sqrt{2}}(\mathcal{D}_{n,k} + X^n\mathcal{D}_{n,k}), \quad n \neq 2k,$$

$$G_{2k,k} := \mathcal{D}_{2k,k}, \tag{38}$$

since $X^n\mathcal{D}_{2k,k}=\mathcal{D}_{2k,k}$; we obviously have $G_n=G_{n,1}$.

From Eq. (32) we notice that if $k+d=n-k$ and $k<d$, the n-qubit state corresponding to the kth value of the ancilla is $\psi_k=(1/\sqrt{2})(\mathcal{D}_{n,k}+\mathcal{D}_{n,n-k})=G_{n,k}$, so we have the following.

Example 5. $d=n-2k$, $k<d$. The parity module can naturally prepare $G_{n,k}$ states heralded by the kth value of the ancilla.

A simple calculation shows that

$$\langle G_{n,k}|X^n|G_{n,k}\rangle = 1,$$

$$\langle G_{n,k}|Y^n|G_{n,k}\rangle = \begin{cases} 0, & n=2m+1, \\ (-1)^{m+k}, & n=2m, \end{cases} \tag{39}$$

and obviously $\langle G_{2k,k}|Y^n|G_{2k,k}\rangle=1$. The previous properties are analogous to those of the $G_n=G_{n,1}$ states, which are essential for secret sharing [16]. Using a similar argument as in Ref. [16], we conjecture that the $G_{2m,k}$ states can also be used for secret sharing.

All these examples demonstrate the flexibility of the generalized parity module in preparing various forms of interesting and potentially useful entangled states, by varying the dimension of the ancilla and the number of qubits. Other states can be obtained if we use an initial state different from $|+\rangle^{\otimes n}$.

Although the success probability for some, but not for all, of the states decreases exponentially with n, as in Eq. (31), the main advantage of the generalized parity module is that it can prepare—heralded and in a single shot—a large spectrum of different families of entangled states: GHZ_n, W_n, $D_{n,k}$, G_n, and generalized $G_{n,k}$, states. We are not aware of any unified protocol or quantum gate that can prepare such a diverse set of useful entangled states with relatively simple resources: a qudit ancilla which interacts, sequentially and homogeneously, with n qubits. Our method is certainly useful to prepare various entangled states, using modest qubit and ancilla resources. For relatively small numbers of qubits—the likely experimental situation in the near future—the exponential damping (with qubit number) of specific preparation probabilities is not really an issue. Our approach therefore offers a very flexible tool for the future laboratory preparation of a wide range of entangled states.

IV. CONCLUSIONS

One of the major breakthroughs in quantum information was the insight that measurements are not only useful as the final step of a computation, but can be used during the computation itself. The KLM model [5] initiated the field of linear optics QC by proving that photon-discriminating detectors and active feedforward can provide the nonlinearity required for a photonic two-qubit gate. On the other hand, in cluster state QC [7] any quantum algorithm can be performed using single-qubit measurements (plus feedforward) performed on a highly entangled initial state; thus the cluster state and single qubit measurements are universal resources for QC.

Standard resources for preparing stabilizer and cluster states are parity gates [10] and photonic modules [12,33]. In this paper we introduced a generalized parity module and studied its use in preparing several families of entangled states. We have shown that using a qudit ancilla we can produce in one-shot measurements a large class of multiparticle entangled states, heralded by the measurement outcome of the ancilla. It is some what surprising that such a simple circuit can prepare a large class of entangled states, like GHZ_n, W_n, Dicke $\mathcal{D}_{n,k}$, and $G_{n,k}$ states, with the number of qubits n and the dimension of the ancilla d as the only free parameters. For W_n states, our model provides an exponential gain compared to linear optics and postselection [34]. The previous states are essential in several quantum-information protocols; examples include teleportation, dense coding, quantum key distribution, secret sharing $(G_n, G_{n,k})$, $1\rightarrow 3$ telecloning, and open destination teleportation $(\mathcal{D}_{4,2})$.

An important feature of the parity module is that all qubits interact once only and in the same way with the ancilla. This is particularly relevant in the case of the photonic module [12,33], for example. The qubits (photons) are sent sequentially through a cavity containing an atom (or a quantum dot in a photonic crystal); the cavity is prepared in a known state and subsequently measured after interacting with all photons. This means that there is no need of extra pulses applied to the cavity between the photons, resulting in a simplified design. Furthermore, the resultant entanglement is between photons, which are naturally amenable to distribution. A straightforward application of these highly entangled states is therefore in a distributed QIP network. Such states could enable useful quantum tasks, even with very modest numbers of qubits.

ACKNOWLEDGMENT

We thank the European Union for support through the QAP project.

[1] P. W. Shor, SIAM (Soc. Ind. Appl. Math.) J. Sci. Stat. Comput. **26**, 1484 (1997).
[2] L. K. Grover, Phys. Rev. Lett. **79**, 325 (1997).
[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[4] D. Deutsch, Proc. R. Soc. London, Ser. A **425**, 73 (1989).
[5] E. Knill, R. Laflamme, and G. Milburn, Nature (London) **409**, 46 (2001).
[6] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn, Rev. Mod. Phys. **79**, 135 (2007).
[7] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).
[8] T. B. Pittman, B. C. Jacobs, and J. D. Franson, Phys. Rev. A **64**, 062311 (2001).

[9] C. W. J. Beenakker, D. P. DiVincenzo, C. Emary, and M. Kindermann, Phys. Rev. Lett. **93**, 020501 (2004).
[10] R. Ionicioiu, Phys. Rev. A **75**, 032339 (2007).
[11] R. Ionicioiu, Int. J. Quantum Inf. **5**, 3 (2007).
[12] S. J. Devitt, A. D. Greentree, R. Ionicioiu, J. L. O'Brien, W. J. Munro, and L. C. L. Hollenberg, Phys. Rev. A **76**, 052312 (2007).
[13] S. G. R. Louis, A. D. Greentree, W. J. Munro, and K. Nemoto, e-print arXiv:0803.1342.
[14] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[15] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
[16] A. Sen(De), U. Sen, and M. Zukowski, Phys. Rev. A **68**, 032309 (2003).
[17] M. Murao, D. Jonathan, M. B. Plenio, and V. Vedral, Phys. Rev. A **59**, 156 (1999).
[18] N. Kiesel, C. Schmid, G. Tóth, E. Solano, and H. Weinfurter, Phys. Rev. Lett. **98**, 063604 (2007).
[19] E. Knill, e-print arXiv:quant-ph/0108033.
[20] B. M. Terhal and D. P. DiVincenzo, Phys. Rev. A **65**, 032325 (2002).
[21] H.-A. Engel and D. Loss, Science **309**, 586 (2005).
[22] A. Kolli, B. W. Lovett, S. C. Benjamin, and T. M. Stace, Phys. Rev. Lett. **97**, 250504 (2006).
[23] W. A. Coish, V. N. Golovach, J. C. Egues, and D. Loss, Phys. Status Solidi B **243**, 3658 (2006).
[24] B. Trauzettel, A. N. Jordan, C. W. J. Beenakker, and M. Büttiker, Phys. Rev. B **73**, 235331 (2006).
[25] T. M. Stace, S. D. Barrett, H.-S. Goan, and G. J. Milburn, Phys. Rev. B **70**, 205342 (2004).
[26] T. Rudolph and S. S Virmani, New J. Phys. **7**, 228 (2005).
[27] W. Mao, D. V. Averin, R. Ruskov, and A. N. Korotkov, Phys. Rev. Lett. **93**, 056803 (2004).
[28] R. Ruskov and A. N. Korotkov, Phys. Rev. B **67**, 241305(R) (2003).
[29] K. Nemoto and W. J. Munro, Phys. Rev. Lett. **93**, 250502 (2004).
[30] W. J. Munro, K. Nemoto, and T. P. Spiller, New J. Phys. **7**, 137 (2005).
[31] T. P. Spiller, K. Nemoto, S. L. Braunstein, W. J. Munro, P. van Loock, and G. J. Milburn, New J. Phys. **8**, 30 (2006).
[32] A. D. Greentree, J. Salzman, S. Prawer, and L. C. L. Hollenberg, Phys. Rev. A **73**, 013818 (2006).
[33] A. M. Stephens, Z. W. E. Evans, S. J. Devitt, A. D. Greentree, A. G. Fowler, W. J. Munro, J. L. O'Brien, K. Nemoto, and L. C. L. Hollenberg, Phys. Rev. A **78**, 032318 (2008).
[34] T. Tashima, S. K. Ozdemir, T. Yamamoto, M. Koashi, and N. Imoto, Phys. Rev. A **77**, 030302 (2008).
[35] W. Dür, G. Vidal, and J. I. Cirac, Phys. Rev. A **62**, 062314 (2000).
[36] R. H. Dicke, Phys. Rev. **93**, 99 (1954).
[37] G. Tóth, J. Opt. Soc. Am. B **24**, 275 (2007).
[38] O. Gühne, F. Bodoky, and M. Blaauboer, e-print arXiv:0805.2873.
[39] A. Sen(De), U. Sen, M. Wiesniak, D. Kaszlikowski, and M. Zukowski, Phys. Rev. A **68**, 062306 (2003).
[40] H. Häffner *et al.*, Nature (London) **438**, 643 (2005).
[41] D. Leibfried *et al.*, Nature (London) **438**, 639 (2005).