JOURNAL OF MATHEMATICAL PHYSICS VOLUME 43, NUMBER 9 SEPTEMBER 2002

Qubits as parafermions

L.-A. Wu and D. A. Lidar[a)]
Chemical Physics Theory Group, University of Toronto,
80 St. George Street, Toronto, Ontario M5S 3H6, Canada

(Received 21 November 2001; accepted for publication 16 May 2002)

Qubits are neither fermions nor bosons. A Fock space description of qubits leads to a mapping from qubits to parafermions: particles with a hybrid boson-fermion quantum statistics. We study this mapping in detail, and use it to provide a classification of the algebras of operators acting on qubits. These algebras in turn classify the universality of different classes of physically relevant qubit-qubit interaction Hamiltonians. The mapping is further used to elucidate the connections between qubits, bosons, and fermions. These connections allow us to share universality results between the different particle types. Finally, we use the mapping to study the quantum computational power of certain anisotropic exchange Hamiltonians. In particular, we prove that the XY model with nearest-neighbor interactions only is *not* computationally universal. We also generalize previous results about universal quantum computation with encoded qubits to codes with higher rates. © *2002 American Institute of Physics.* [DOI: 10.1063/1.1499208]

I. INTRODUCTION

It is an experimental fact that there are only two types of *fundamental* particles in nature: bosons and fermions. Bosons are particles whose wavefunction is unchanged under permutation of two identical particles. The wavefunction of fermions is multiplied by -1 under the same operation. An equivalent statement is that bosons transform according to the one-dimensional, symmetric, irreducible representation (irrep) of the permutation group, while fermions belong to the one-dimensional antisymmetric irrep. The permutation group has only these two one-dimensional irreps. What about particles transforming according to higher-dimensional irreps of the symmetric group? Much research went into studying this possibility, in the early days of the quark model, before the concept of ''colored'' quarks gained widespread acceptance.[1,2] However, there are now good reasons to believe that particles obeying such ''parastatistics'' do not exist (Ref. 3, p. 137). Nevertheless, as we will show below, the traditional definition of a Hilbert space of qubits is inconsistent with the properties of either bosons or fermions.

The description of bosons and fermions in terms of their properties under particle permutations uses the language of first quantization. A useful alternative description is the second-quantized formalism of Fock space.[3,4] A basis state in the boson or fermion Hilbert–Fock space can be written as $|n_1^\alpha, n_2^\alpha, \ldots\rangle$, where n_i^α counts how many bosons ($\alpha = b$) or fermions ($\alpha = f$) occupy a given mode, or site i. Note that the total number of modes does not need to be specified in the Fock-basis. Ignoring normalization, raising, $\alpha_i^\dagger$ (lowering, α_i) operators increase (decrease) n_i^α by 1. A consequence of the permutation properties of bosons and fermions is that their corresponding raising and lowering operators satisfy commutation and anticommutation relations:

$$[b_i^\dagger, b_j^\dagger] = 0, \quad [b_i, b_j^\dagger] = \delta_{ij} \quad \text{bosons},$$

$$\{f_i^\dagger, f_j^\dagger\} = 0, \quad \{f_i, f_j^\dagger\} = \delta_{ij} \quad \text{fermions}.$$

[a)]Electronic mail: dlidar@chem.utoronto.ca

From this follow a number of well-known facts.[3,4] Let $\hat{n}_i^\alpha = \alpha_i^\dagger \alpha_i$; this is the number operator, which is diagonal in the Fock-basis $|n_1^\alpha, n_2^\alpha, \ldots\rangle$, and has eigenvalues n_i^α. Then we have the following.

(i) $[b_i^\dagger, b_j^\dagger] = 0 \Rightarrow$ an arbitrary number of bosons n_i^α can occupy a given mode i. On the other hand, $\{f_i^\dagger, f_j^\dagger\} = 0 \Rightarrow$ only $n_i^f = 0,1$ is possible for fermions.

(ii) $[b_i, b_j^\dagger] = \delta_{ij} \Rightarrow$ the Hilbert space of bosons has a natural tensor product structure, i.e., $|n_1^b, n_2^b, \ldots\rangle = |n_1^b\rangle \otimes |n_2^b\rangle \otimes \cdots$. More specifically, it is possible to *independently* operate on each factor of the Hilbert space. However,

$$\{f_i, f_j^\dagger\} = \delta_{ij} \Rightarrow f_j |n_1^f, \ldots, n_{j-1}^f, 1, n_{j+1}^f, \ldots\rangle = (-1)^{\sum_{k=1}^{j-1} n_k^f} |n_1^f, \ldots, n_{j-1}^f, 0, n_{j+1}^f, \ldots\rangle,$$

which means that the outcome of operating on a mode of a multi-fermion state depends on all previous modes (the order of modes is actually arbitrary). This nonlocal property means that the fermionic Fock space does not have a natural tensor product structure, although it can be mapped onto one that does using the Jordan–Wigner transformation[5] (see Ref. 6 for a more detailed discussion).

What about qubits? The standard notion of what a qubit is, is the following:[7]

Qubit:

(i) A qubit is a vector in a two-dimensional Hilbert space $\mathcal{H}_i = \mathrm{span}\{|0\rangle_i, |1\rangle_i\}$ (like a fermion).

(ii) An N-qubit Hilbert space has a tensor product structure: $\mathcal{H} = \otimes_{i=1}^N \mathcal{H}_i$ (like bosons).

It appears that a qubit is a hybrid fermion-boson particle! We conclude that *qubits do not exist as fundamental particles*. This motivates us to consider an intermediate statistics of ''parafermions'' in order to have a Fock space description of a qubit. We define the parafermionic commutation relations by[8,9]

$$\{a_i, a_i^\dagger\} = 1, \qquad [a_i, a_j^\dagger] = 0 \quad \text{if} \quad i \neq j. \tag{1}$$

Here i,j are different modes, or different qubits. The relation $[a_i, a_j^\dagger] = 0$ for $i \neq j$ immediately implies a tensor product structure, while $\{a_i, a_i^\dagger\} = 1$, which together with $a_i|0\rangle = 0$ ($|0\rangle$ is the vacuum state) implies

$$a_i a_i = a_i^\dagger a_i^\dagger = 0 \tag{2}$$

in the standard (irreducible) two-dimensional representation. Therefore a double-occupation state cannot be realized, i.e., the single-particle Hilbert space is two-dimensional. These are exactly the requirements for a qubit.

In fact, the notion of particles with ''intermediate'' statistics such as parafermions is well known and established in condensed matter physics, e.g., hard-core bosons, excitons, or the Cooper pairs of superconductivity[10] (see also Sec. VI). Such particles are always *composite*, i.e., they are not fundamental. Another way of obtaining a particle that is neither a boson nor a fermion is to simply ignore one or more degrees of freedom. This is by and large the approach taken in current proposals for the physical implementation of quantum computers. For example, a single spin-$\frac{1}{2}$, without the orbital component of its wavefunction, behaves exactly like a qubit. This is the case of the electron-spin qubit in quantum dots.[11] Related to this, a truncated multi-level atom can also approximate a qubit, as in the ion-trap proposal.[12] What are the implications of this for quantum computing (QC)? In a nutshell, ''ideal'' qubits are hard to come by. If a qubit is to exist as an approximate two-level system, or as a composite particle, or as a partial description of an object with additional degrees of freedom, this means that some robustness is lost and the door is opened to decoherence. For example, the additional levels in a multi-level Hilbert space can cause ''leakage,'' the orbital degrees of freedom act as a bath coupled to the spin-qubit, and a composite particle may decay (e.g., the exciton-qubit[13]).

The advantages of the parafermionic formalism for qubits, however, are not necessarily in understanding these sources of decoherence, because this formalism ''accepts'' qubits as particles. Instead, the parafermionic formalism allows us to naturally establish mappings between qubits, fermions, and bosons. This mapping serves to transport well-known results about one type of particle to another, which, as we show below, clarifies questions regarding the ability of sets of one type of particle to act as universal simulators[14] of sets of another type of particle. It also helps in connecting the Hamiltonians of condensed matter physics to standard tools of quantum computation.

The structure of the article is as follows. In the next section we formally introduce the second quantization of qubits. We then classify the algebraic structure of parafemionic operators in Sec. III. This classification, into subalgebras with different conservation properties, is very useful for establishing which subsets of qubit operators are universal, either on the full Hilbert space, or only on a subspace. This is taken up in the next two sections, where we establish the connection between parafermions and fermions (Sec. IV) and bosons (Sec. V). The connection to fermions and bosons also works in the opposite direction: we are able to classify which fermionic and bosonic operator sets are universal. This has implications, e.g., for the linear optics quantum computing proposals.[15,16] Section VI shows how to construct parafermions out of paired fermions and bosons, emphasizing the compound-particle aspect of qubits. With the connections between fermions, bosons, and parafermions clarified, we explain in Sec. VII a remarkable difference between parafermions and the other particle types: bilinear parafermionic Hamiltonians are sufficient for universal quantum computation, whereas fermionic and bosonic Hamiltonians are not. In Sec. VIII we briefly use the mapping to fermions to derive the thermal fluctuations of noninteracting parafermions at finite temperature. In Sec. IX we apply the classification of the various parafermionic operator subalgebras to the problem of establishing universality of typical Hamiltonians encountered in solid state physics. We generalize a number of our previous results.[17,18] In particular, we establish that the XY model is not universal with nearest-neighbor interactions only; and, we prove universality of the XXZ model for codes with arbitrarily high rates. We conclude in Sec. X.

II. SECOND QUANTIZATION OF QUBITS

As in the cases of bosons and fermions, a parafermion number operator in mode i can be defined as

$$\hat{n}_i = a_i^\dagger a_i ,$$

with eigenvalues $n_i = 0,1$. The total number operator is $\hat{n} = \Sigma_i \hat{n}_i$. A normalized basis state in the parafermionic Fock space is

$$|\cdots n_i \cdots\rangle = \prod_i (a_i^\dagger)^{n_i} |0\rangle,$$

which we think of as representing a state with the ith qubit in the ''up'' (''down'') state if the ith parafermion is present (absent), i.e., $n_i = 1$ (0). *Qubit computational basis states are thus mapped to parafermionic Fock states*. Equivalently, consider the following mapping from qubits to parafermions:

$$|0_1 \cdots 0_{i-1} 0_i 0_{i+1} \cdots\rangle \to |0\rangle,$$

$$|0_1 \cdots 0_{i-1} 1_i 0_{i+1} \cdots\rangle \to a_i^\dagger |0\rangle,$$

where on the left 0 and 1 represent the standard (first-quantized) logical states of a qubit. *Qubits can thus be identified with parafermionic operators*.

The mapping of qubits to parafermions is completed by mapping the Pauli matrices σ_i^α to parafermionic operators:

$$\sigma_i^+ \to a_i^\dagger, \quad \sigma_i^- \to a_i, \quad \sigma_i^z \to 2n_i - 1. \tag{3}$$

It is then straightforward to check that the standard sl(2) commutation relations of the Pauli matrices,

$$[\sigma_i^+, \sigma_j^-] = \delta_{ij}\sigma_i^z,$$

$$[\sigma_i^z, \sigma_j^\pm] = \pm\delta_{ij}\sigma_i^\pm,$$

are preserved, so that we have a faithful second-quantized representation of the qubit system Hilbert space and algebra. [Of course we could also have mapped $su(2) = \{\sigma^x, \sigma^y, \sigma^z\}$ to the parafermionic operators, by appropriate linear combinations.] To illustrate the multi-qubit Hilbert–Fock space representation, consider the case of two modes, i.e., $i,j = 1,2$. The space splits into a vacuum state $|00\rangle = |\mathtt{0}\rangle$, single-particle states $|01\rangle = a_1^\dagger|\mathtt{0}\rangle$ and $|10\rangle = a_2^\dagger|\mathtt{0}\rangle$, and a two-particle state $|11\rangle = a_1^\dagger a_2^\dagger|\mathtt{0}\rangle$. It is important to emphasize that the parafermionic formalism is mathematically equivalent to the standard Pauli matrix formalism. We will be using both in the sections that follow, starting with the parafermionic, as it makes particularly transparent the translation of known results about fermions to qubits.

III. GENERAL PROPERTIES OF PARAFERMIONIC OPERATORS

N-qubit operators in QC are elements of the group $U(2^N)$. We will begin our discussion by identifying a set of infinitesimal parafermionic generators for $U(2^N)$. Recall that with any r-parameter Lie group there are associated r infinitesimal generators,[19] e.g., in the case of su(2) these are, in the two-dimensional irreducible representation, the Pauli matrices $\{\sigma_x, \sigma_y, \sigma_z\}$. Now, let $\alpha = \{\alpha_i\}, \beta = \{\beta_j\}$, where α_i, β_j can be 0 or 1. In terms of parafermionic operations, any element of $U(2^N)$ can be written as $U(b) = \exp(-i\Sigma_{\alpha,\beta} b^{\alpha\beta} Q_{\alpha,\beta}(N))$, where $b^{\alpha\beta}$ are continuous parameters (generalized Euler angles) and the $2^N \times 2^N$ *infinitesimal group generators* $Q_{\alpha,\beta}(N)$ are defined as follows: Let $N_\alpha = \Sigma_{i=1}^N \alpha_i$, and

$$q_\alpha^\dagger(N_\alpha) = (a_N^\dagger)^{\alpha_N} \cdots (a_1^\dagger)^{\alpha_1}, \quad q_\beta(N - N_\alpha) = a_N^{\beta_N} \cdots a_1^{\beta_1}. \tag{4}$$

Then,

$$Q_{\alpha,\beta}(N) = q_\alpha^\dagger(N_\alpha) q_\beta(N - N_\alpha). \tag{5}$$

The $Q_{\alpha,\beta}(N)$ will be recognized as all possible transformations between N-qubit computational basis states, e.g., for $N = 2$ the set of 16 operators is

$$\{I, a_1^\dagger, a_2^\dagger, a_1, a_2, a_2^\dagger a_1^\dagger, a_1 a_2, a_1^\dagger a_1, a_1^\dagger a_2, a_2^\dagger a_1, a_2^\dagger a_2, a_2^\dagger a_1^\dagger a_1, a_2^\dagger a_1^\dagger a_2, a_1^\dagger a_1 a_2, a_2^\dagger a_2 a_1, a_2^\dagger a_1^\dagger a_2 a_1\},$$

where I is the identity operator. The set $Q_{\alpha,0}(N)$ generates all possible basis states from the vacuum state. Hermitian forms are $Q + Q^\dagger$ and $i(Q - Q^\dagger)$. We will turn to the Hermitian set of generators in the discussion of applications, in Sec. IX.

Note that infinitesimal generators are not the generators one usually considers in QC. Rather, in QC, a gate operation is obtained by the unitary evolution generated through the turning on/off of a set of physically available *Hamiltonians* $\{H_\mu\}$, which are generally a small subset of the $2^N \times 2^N$ infinitesimal generators $Q_{\alpha,\beta}(N)$. "Generated" here has the usual meaning of allowing linear combinations and commutation of Hamiltonians. We will say that *a set of Hamiltonians* $\{H_\mu\}$ *is universal with respect to a Lie group* $\mathcal{G}$ if it generates the Lie algebra of that group. The question of the dimension of the universal set of Hamiltonians with respect to $\mathrm{U}(2^N)$ is somewhat subtle, since it is context dependent. Lloyd showed that given two noncommuting operators A, B, represented by $n\times n$ matrices, one can almost always generate $\mathrm{U}(n)$.[20] However, it is not necessarily clear how this result is related to *physically available* Hamiltonians, since in practice one may have only limited control over terms in a Hamiltonian, e.g., the standard Hamiltonian generators for SU(4) (two qubits) is the five-element set $\{\sigma_1^z,\sigma_2^z,\sigma_1^x,\sigma_2^x,\sigma_1^z\sigma_2^z\}$. However, the four-element set $\{\sigma_1^z,\sigma_2^z,\sigma_1^z\sigma_2^x-\sigma_1^x\sigma_2^z,\vec{\sigma}_1\cdot\vec{\sigma}_2\}$ also generates SU(4), and may be physically available.[17] Another example are the following sets of, respectively, five, four, and three generators: $\{\sigma_1^x,\sigma_2^x,\sigma_1^z,\sigma_2^z,\sigma_1^z\sigma_2^z\}$, $\{\sigma_1^x,\sigma_2^x,c_1\sigma_1^z+c_2\sigma_2^z,\sigma_1^z\sigma_2^z\}$, and $\{\sigma_1^x,\sigma_2^x,c_1\sigma_1^z+c_2\sigma_2^z+c_3\sigma_1^z\sigma_2^z\}$ (where c_i are constants). Which set of generators is physically available (i.e., directly controllable) depends on the specific system used to implement the quantum computer. As we will show later in this work, it is sometimes the case that a given, physically available, set of Hamiltonians is universal with respect to a *subgroup* of $\mathrm{U}(2^N)$, which may be quite useful, provided the subgroup is sufficiently large (typically, still exponential in N). This notion of universality with respect to a subgroup is what gives rise to the idea of *encoded universality*:[17,18,21–24,52] one encodes a logical qubit into two or more physical qubits, and studies the universality of the subgroup-generating Hamiltonians with respect to these encoded/logical qubits.

The infinitesimal parafermionic generators $Q_{\alpha,\beta}(N)$ can be rearranged into certain subsets of operators with clear physical meaning, which we now detail.

(1) Local subalgebras: The tensor product structure of qubits is naturally enforced by $[a_i,a_j^\dagger]=0$ for $i\neq j$. This induces a tensor product structure $\otimes_{i=1}^N \mathrm{sl}_i(2)$ on the subalgebras formed by the grouping $\mathrm{sl}_i(2)=\{a_i,a_i^\dagger,1-2n_i\}$. Each $\mathrm{sl}_i(2)$ can only change states within the same mode.

(2) SAp—Subalgebra with *conserved parity*: Define a *parity* operator as

$$\hat{p}=(-1)^{\hat{n}}.$$

It has eigenvalues 1 (-1) for even (odd) total particle number. The operators that commute with the parity operator form a subalgebra, which we denote by SAp. Let k (l) be the number of $a_i^\dagger$ (a_i) factors in $Q_{\alpha,\beta}(N)$, i.e.,

$$k=\sum \alpha_i, \quad l=\sum \beta_i.$$

SAp consists of those operators having $k-l$ even, so its dimension (i.e., number of generators) is $2^{2N}/2$. To see this, let Q_I be in SAp, and consider its action on a state with an even number of particles $|n\rangle$. Since $k-l$ is even, $Q_I|n\rangle=|n'\rangle$ where n' is also even. Now, $\hat{p}Q_I|n\rangle=\hat{p}|n'\rangle=+|n'\rangle$, but also $Q_I\hat{p}|n\rangle=Q_I(+|n\rangle)=|n'\rangle$ so $[\hat{p},Q]=0$. For example, for $N=2$ SAp consists of $\{I,a_2^\dagger a_1^\dagger,a_1a_2,a_1^\dagger a_1,a_1^\dagger a_2,a_2^\dagger a_1,a_2^\dagger a_2,a_2^\dagger a_1^\dagger a_2 a_1\}$.

(3) SAn—subalgebra with *conserved particle number*. This subalgebra, which we denote SAn, is formed by all operators commuting with the number operator $\hat{n}$. These are the operators for which $k=l$, so its dimension is $\Sigma_{k=0}^N \binom{N}{k}^2=(2N)!/N!N!$. To see this, let Q_{II} be in SAn, and consider its action on a state $|n\rangle$ with n particles. Q_{II} cannot change this number since $k=l$, but it can transform $|n\rangle$: $\hat{n}Q_{II}|n\rangle=\hat{n}|n\rangle'=n|n\rangle'$. However, $Q_{II}\hat{n}|n\rangle=nQ_{II}|n\rangle=n|n\rangle'$, so $[Q_{II},\hat{n}]=0$. For example, for $N=2$ SAn consists of $\{I,a_1^\dagger a_1,a_1^\dagger a_2,a_2^\dagger a_1,a_2^\dagger a_2,a_2^\dagger a_1^\dagger a_2 a_1\}$. Clearly, SA$n\subset$SA$p$.

(4) Subsets of bilinear operators: There are two types of bilinear operators for $i\neq j$: $a_i^\dagger a_j$ (which conserve the particle number) and $a_ia_j,a_i^\dagger a_j^\dagger$ (which conserve parity). Let $\mu=(ij)$. Then first

$$T_\mu^x=a_j^\dagger a_i+a_i^\dagger a_j,$$
$$T_\mu^z=n_i-n_j, \tag{6}$$

and $T_\mu^y=i[T_\mu^x,T_\mu^z]$ form an su(2) subalgebra, that we denote $\mathrm{su}_\mu^t(2)$. Clearly, $\mathrm{su}_\mu^t(2)\in$SAn. Second,

$$R^x_\mu = a_i a_j + a_i^\dagger a_j^\dagger,$$
$$R^z_\mu = n_i + n_j - 1, \tag{7}$$

and R^y_μ form another su(2) subalgebra, that we denote $\mathrm{su}^r_\mu(2) \in \mathrm{SA}p$. Note that $[\mathrm{su}^t_\mu(2), \mathrm{su}^r_\mu(2)] = 0$ since any product of raising/lowering operators from these algebras contains a factor of $a_i a_i$ or $a_i^\dagger a_i^\dagger$. Consider as an example the case of $N=2$ modes. Whereas the direct product group $\mathrm{SU}_1(2) \otimes \mathrm{SU}_2(2)$ yields all product states, the group $\mathrm{SU}^t(2) \oplus \mathrm{SU}^r(2)$ can transform between states with equal particle number and states differing by two particle numbers.

(5) Generators of $\mathrm{SA}n(N)$: The set of Hamiltonians $\{a_i^\dagger a_j\}_{i,j=1}^{N+1}$ generates $\mathrm{SA}n(N)$, i.e., the subalgebra of conserved particle number on N modes (qubits). Proof: this set maps to the XY model (see Sec. IX B). The rest follows using the method of Ref. 18. Note that $\{a_i^\dagger a_j\}_{i,j=1}^{N+1}$ does *not* generate $\mathrm{SA}n(N+1)$, since this set cannot generate $\hat{n}_1 \hat{n}_2 \cdots \hat{n}_N$.

(6) Generators of $\mathrm{SA}p(N)$: The set of Hamiltonians $\{a_i^\dagger a_j, a_i a_j + a_i^\dagger a_j^\dagger, i(a_i a_j - a_i^\dagger a_j^\dagger)\}_{i,j=1}^{N}$ yields all states with even particle number on N modes from the vacuum state. (Proof is trivial.)

(7) Generators of $\mathrm{SU}(2^N)$: In order to transform between states differing by an odd number of particles it is necessary to include the operators $\{a_i, a_i^\dagger\}$ as well. The corresponding set $\{a_i^\dagger a_j, a_i a_j, a_i^\dagger a_j^\dagger, a_i, a_i^\dagger\}_{i,j=1}^{N}$ generates a set of universal gates (proof is trivial), and then by standard universality results[25,26] the entire $\mathrm{SU}(2^N)$.

Additional structure emerges from a mapping between fermions and parafermions. This structure helps both in simulating fermionic system using qubits, and in understanding the universality of qubit systems.

IV. FERMIONS AND PARAFERMIONS

A general fermionic Fock state is

$$|n_1, n_2, \cdots\rangle_F, \tag{8}$$

where $n_i = 0,1$ is the occupation number of mode i. As is well known,[27] the fermionic ("supergroup"[19]) $\mathrm{U}(2^N)$ has infinitesimal generators

$$\tilde{Q}^f_{\alpha,\beta}(N) = (f_N^\dagger)^{\alpha_N} \cdots (f_1^\dagger)^{\alpha_1} A f_N^{\beta_N} \cdots f_1^{\beta_1},$$

where

$$A = \bigotimes_{i=1}^{N} (1 - n_i).$$

This basis is equivalent by a linear transformation to the more familiar set

$$Q^f_{\alpha,\beta}(N) = (f_N^\dagger)^{\alpha_N} \cdots (f_1^\dagger)^{\alpha_1} f_N^{\beta_N} \cdots f_1^{\beta_1},$$

which transforms between all possible fermionic Fock states ("fermionic computational basis state"). There is a group chain of this group,

$$\mathrm{U}(2^N) \supset \mathrm{SO}(2N+1) \supset \mathrm{SO}(2N) \supset \mathrm{U}(N) \tag{9}$$

and the generators of the subgroups are known.[19]

The Jordan–Wigner (JW) transformation,[5] recently generalized in Ref. 28, allows one to establish an isomorphism between fermions and parafermions. Defining

$$S_i^f \equiv \bigotimes_{k=1}^{i-1} (1 - 2n_k^f), \quad S_i \equiv \bigotimes_{k=1}^{i-1} (1 - 2n_k), \tag{10}$$

TABLE I. Infinitesimal generators (h.c. = Hermitian conjugate).

Group	Fermions	Parafermions
$U(2^N)$	$Q^f_{\alpha,\beta}(N)$	$Q_{\alpha,\beta}(N)$
$SO(2N+1)$	$f_i^\dagger f_j, f_i f_j, f_i$, h.c.	$a_i^\dagger S_i S_j a_j, a_i S_i S_j a_j, a_i S_i$, h.c.
$SO(2N)$	$f_i^\dagger f_j, f_i f_j$, h.c.	$a_i^\dagger S_i S_j a_j, a_i S_i S_j a_j$, h.c.
$U(N)$	$f_i^\dagger f_j$	$a_i^\dagger S_i S_j a_j$

the mapping is

$$n_i^f \to n_i,$$
$$f_i \to a_i S_i, \tag{11}$$
$$f_i^\dagger \to a_i^\dagger S_i.$$

The action of the fermionic operators on the state (8) is equivalent to that of the corresponding parafermionic operators on the state $|n_1, n_2, \ldots\rangle$. To see this, note that $[a_i, S_i]=0$. Therefore the effect of the JW transformation is quite simple: by commuting all S_i to the left when mapping a fermionic infinitesimal generator to a parafermionic one, we see that (i) the parafermionic $a_i, a_i^\dagger$ operators will yield a state with the same parafermionic occupation numbers as the corresponding fermionic state and (ii) the action of the product of S_i's is to produce a phase ± 1. (This may become a relative phase when acting on a state that is a superposition of computational basis states.) This allows us to study algebraic properties of one set of particles in terms of the other.

Using the JW transformation we find that the same subgroup chain (9) holds for parafermions, and we can immediately write down also the infinitesimal generators for the corresponding parafermionic subgroups. The result is given in Table I.

The significance of these subgroups for QC is in the classification of the universality properties of fermionic and parafermionic Hamiltonians. For example, a Hamiltonian of noninteracting fermions, i.e., one including only bilinear terms $\{f_i^\dagger f_j, f_i f_j, f_j^\dagger f_i^\dagger\}$, is not by itself universal since it merely generates $SO(2N)$. Recent work has clarified what needs to be added to such a Hamiltonian in order to establish universality.[6,29,30] Regarding $SO(2N+1)$, note that one must carefully discuss the Hermitian terms $f_i + f_i^\dagger$ and $i(f_i - f_i^\dagger)$ if one wants to consider them as Hamiltonians, since it is unclear which physical process can be described by such Hamiltonians (a single fermion creation/annihilation operator can turn an isolated fermion into a boson, a process that does not seem to occur in nature).

A more powerful classification, from the QC viewpoint, is in terms of physically available Hamiltonian generators of the subgroups. An interesting restriction of the set of infinitesimal generators to a physically reasonable set of Hamiltonians is to consider only nearest-neighbor interactions, where possible. The results known to us in this case are presented in Table II.

A couple of comments are in order regarding Table II: First, note the group $SO(2N+1)$ may be unphysical not just for fermions since its generators must contain terms like $f_i + f_i^\dagger$ in its Hamiltonian, but also for parafermions: it requires a nonlocal Hamiltonian due to the S_i term. Second, the corresponding fermionic generators for $U(2^N)$ given here is unphysical because it

TABLE II. Hamiltonian generators.

Group	Fermions	Parafermions
$U(2^N)$	$f_i S_i^f, f_i^\dagger f_{i+1}$, h.c.	$a_i, a_i^\dagger a_{i+1}$, h.c.
$SO(2N+1)$	f_i, h.c.	$a_i S_i$, h.c.
$SO(2N)$	$f_i^\dagger f_{i+1}, f_i f_{i+1}$, h.c.	$a_i^\dagger a_{i+1}, a_i a_{i+1}$, h.c.
$SU(N)$	$f_i^\dagger f_{i+1}$, h.c.	$a_i^\dagger a_{i+1}$, h.c.

includes terms that are linear in f_i and furthermore nonlocal. A physically acceptable set is $\{f_i^\dagger f_{i+1}, f_i f_{i+1}, f_i^\dagger f_{i+1}^\dagger f_i f_{i+1}, \text{h.c.}\}$, but this set is not universal over the full 2^N-dimensional Hilbert space (since it conserves parity). This means that a qubit needs to be encoded into two fermions in this case, a situation we explore further in Sec. VI. Now let us verify the claims of Table II. Our strategy is to show that in each case, we can use the Hamiltonians for generating all infinitesimal generators of the corresponding subgroup in Table I.

Consider first the subgroup SU(N): In the fermionic case, we claim that this subgroup has nearest-neighbor Hamiltonian generators $f_i^\dagger f_{i+1}$ and their Hermitian conjugates. For example, for $N=3$, if we have the four operators $f_1^\dagger f_2$, $f_2^\dagger f_3$ and h.c., then we can generate $f_1^\dagger f_3 = [f_1^\dagger f_2, f_2^\dagger f_3]$ and h.c., as well as $\hat{n}_i^f - \hat{n}_j^f = [f_i^\dagger f_j, f_j^\dagger f_i]$. This yields a total of nine operators, eight of which are linearly independent, that generate SU(3). As for parafermions, we can use the JW transformation to get $f_{i+1}^\dagger f_i \rightarrow a_{i+1}^\dagger S_{i+1} a_i S_i = a_{i+1}^\dagger (1-2\hat{n}_i) a_i = a_{i+1}^\dagger a_i$ (where we have used $[a_i, S_i]=0$ and $\hat{n}_i a_i = a_i^\dagger a_i a_i = 0$). This establishes an isomorphism between the fermionic and parafermionic generators for SU(N). Hence the parafermionic subgroup SU(N) is generated by $a_i^\dagger a_{i+1}$ and h.c.

Now consider SO($2N$): In the fermionic case we have $f_1^\dagger f_2^\dagger$, and using the result for U(N) we also have $f_4^\dagger f_1$; therefore we have $[f_4^\dagger f_1, f_1^\dagger f_2^\dagger] = f_4^\dagger f_2^\dagger$. Clearly, the interaction range can be extended to cover all generators. For the parafermionic case, using the JW transformation we find $f_{i+1}^\dagger f_i^\dagger \rightarrow a_{i+1}^\dagger S_{i+1} a_i^\dagger S_i = a_{i+1}^\dagger (1-2\hat{n}_i) a_i^\dagger = a_{i+1}^\dagger a_i^\dagger$, so that we again have an isomorphism with the fermionic case.

Next consider the (unphysical) subgroup SO($2N+1$): In the fermionic case it suffices to note that $\frac{1}{2}[f_i, f_j] = f_i f_j$ and $\frac{1}{2}[f_i^\dagger, f_j] = f_i^\dagger f_j$, $i \leqslant j$ so that we can generate all infinitesimal generators by the linear terms f_i and $f_i^\dagger$. The parafermionic case follows by the JW transformation.

Finally, in the U(2^N) case the universality of the parafermionic set $\{a_i, a_i^\dagger a_{i+1}, \text{h.c.}\}$ follows from that of the set of all single qubit operations together with the Hamiltonian of the nearest-neighbor XY model [Eq. (17) below], proved in Ref. 31. The fermionic case follows by the JW transformation.

Let us recapitulate the meaning of the results presented in this section: we have shown how to classify subalgebras of fermionic/parafermionic operators in terms of the groups they generate. This therefore classifies their universality properties with respect to these groups. This is particularly important in the context of a given set of physically available Hamiltonians. Our method employed a mapping between fermions and parafermions, which allowed us to easily transport known results about one type of particle to the other.

V. BOSONS FROM PARAFERMIONS

A linear combination of different-mode parafermions can approximately form a boson. Define

$$B = \frac{1}{\sqrt{N}} \sum_{i=1}^{N} a_i .$$

Then using Eq. (1) we have

$$[B, B^\dagger] = \frac{1}{N} \sum_{i=1}^{N} 1 - 2\hat{n}_i = 1 - \frac{2\hat{n}}{N}.$$

If the parafermion number is much smaller than the available number of sites/modes, i.e., when $n \ll N$, then $[B, B^\dagger] \approx 1$, which is an approximate single-mode boson commutation relation.

To get K boson modes, we can divide N into K approximately equal parts. Each part has $N_\alpha = N/K$ qubits and approximately represents a boson. The kth boson is $B_\alpha = (1/\sqrt{N_\alpha}) \sum_{i=1}^{N_\alpha} a_i$. Then

$$[B_\alpha, B_\beta^\dagger] = \delta_{\alpha\beta} \left(1 - \frac{2\hat{n}_\alpha}{N_\alpha}\right) \overset{n_\alpha \ll N_\alpha}{\approx} \delta_{\alpha\beta}.$$

Physically, this means that a low-energy qubit system (with most qubits in their ground state) can macroscopically behave like a boson, or a collection of bosons. If the Hamiltonian is of the bilinear form $H=-B^{\dagger}B=-(1/N)\,(\hat{n}+\Sigma_{i\neq j}^{N}a_i^{\dagger}a_j)$, the ground state with $n\ll N$ parafermions is $(B^{\dagger})^n|0\rangle$, i.e., $\hat{n}[(B^{\dagger})^n|0\rangle]\approx n[(B^{\dagger})^n|0\rangle]$.

A separate conclusion that follows from this result is that a low-energy noninteracting qubit system can *naturally simulate the dynamics of bosons*.

VI. PARAFERMIONS FROM FERMIONS AND BOSONS

As stated in the Introduction, qubits do not exist as fundamental particles. This means that they are either approximate descriptions (e.g., a spin in the absence of its spatial degrees of freedom) or have to be prepared by appropriately combining bosons or fermions, i.e., a qubit can be *encoded* in terms of bosons or fermions under certain conditions (see also Ref. 32). We consider bosonic or fermionic systems with $2N$ single-particle states. Let $k=1,2,\ldots,N$ denote all relevant quantum numbers (including spin, if necessary). The following three cases yield parafermions.

Case 1: Fermionic particle-particle pairs—Under the condition $n_{2k-1}^{f}=n_{2k}^{f}$ it can be shown that $\{f_{2k}f_{2k-1},f_{2k-1}^{\dagger}f_{2k}^{\dagger}\}=1$ and $[f_{2k-1}f_{2k},f_{2l-1}^{\dagger}f_{2l}^{\dagger}]=0$ for $k\neq l$. Furthermore, the set $\{f_{2k-1},f_{2k-1}^{\dagger}f_{2k}^{\dagger},n_{2k-1}^{f}+n_{2k}^{f}-1\}$ satisfies the commutation relations of sl(2). Therefore the mapping $a_k\Leftrightarrow f_{2k}f_{2k-1}$, $a_k^{\dagger}\Leftrightarrow f_{2k-1}^{\dagger}f_{2k}^{\dagger}$ and $2n_k\Leftrightarrow n_{2k-1}^{f}+n_{2k}^{f}$ is a mapping to parafermions. The vacuum state of parafermions in this case corresponds to the vacuum state $|0\rangle_f$ of fermions. An example is Cooper pairs.

Case 2: Fermionic particle-hole pairs—Under the condition $n_{2k-1}^{f}+n_{2k}^{f}=1$ it can be shown as in case 1 that $a_k\Leftrightarrow f_{2k}^{\dagger}f_{2k-1}$, $a_k^{\dagger}\Leftrightarrow f_{2k-1}^{\dagger}f_{2k}$ and $2n_k-1\Leftrightarrow n_{2k-1}^{f}-n_{2k}^{f}$ is a mapping to parafermions. However, in this case the vacuum state of parafermions is $|0\rangle=f_{2N}^{\dagger}\cdots f_4^{\dagger}f_2^{\dagger}|0\rangle_f$, because then $a_k|0\rangle=0$ for all k. This vacuum state plays the role of a Fermi level. An example is excitons. In fact, all quantum computer proposals that use electrons, e.g., quantum dots,[11] and electrons on Helium,[33,34] are equivalent to this case. For example, $f_2^{\dagger}f_1$ and $f_1^{\dagger}f_2$ can represent the transition operators between two spin states in the quantum dot proposal.

Case 3: Bosonic "particle-hole" pairs—Under the condition $n_{2k-1}^{b}+n_{2k}^{b}=1$ it can be shown as in case 1 that $a_k\Leftrightarrow b_{2k}^{\dagger}b_{2k-1}$, $a_k^{\dagger}\Leftrightarrow b_{2k-1}^{\dagger}b_{2k}$ and $2n_k-1\Leftrightarrow n_{2k-1}^{b}-n_{2k}^{b}$ is a mapping to parafermions. However, in this case the vacuum state of parafermions is $|0\rangle=b_{2N}^{\dagger}\cdots b_{2k}^{\dagger}\cdots b_4^{\dagger}b_2^{\dagger}|0\rangle_b$, again because then $a_k|0\rangle=0$ for all k. An example is dual-rail photons in the optical quantum computer proposal.[15]

This classification illustrates the by-necessity compound nature of a qubit, and puts into a unified context the many different proposals for constructing qubits in physical systems. Note that it is possible to use more than two fermions or bosons to construct a parafermion. Further implications, especially as related to the simulation of models of superconductivity (Case 1) on a quantum computer, have been explored in Ref. 35.

VII. PARAFERMIONIC BILINEAR HAMILTONIANS ARE UNIVERSAL BUT FERMIONIC AND BOSONIC ARE NOT

In this section we discuss a rather striking difference between the universality of bilinear Hamiltonians acting on fermions and bosons, as compared to parafermions. Let us consider the set of particle-number-conserving bilinear operators of bosons, fermions and parafermions:

$$b_i^{\dagger}b_j,\quad f_i^{\dagger}f_j,\quad a_i^{\dagger}a_j.$$

As noted in Table I, in the fermionic case these operators generate the group U(N) where N is the number of particles. The same is true for bosons.[19] Clearly, therefore, fermionic and bosonic Hamiltonians containing only these operators are not universal with respect to an interesting (i.e., exponentially large) SU(2^N) subgroup. On the other hand, as discussed in the previous section, these fermionic and bosonic operators can be used to define parafermionic operators $a_i^{\dagger}a_j$ in two-to-one correspondence. As mentioned in Sec. III, the set $\{a_i^\dagger a_j\}_{i,j=1}^{N+1}$ generates the subalgebra SA$n(N)$, with dimension $(2N)!/N!N!$ $(>2^N)$ [recall that the total number of $Q_{\alpha,\beta}(N)$ operators is 2^{2N}]. The corresponding Lie group appears to be large enough to be interesting for universal quantum computation. This expectation is borne out, since one can construct an XY model, Eq. (17), using the set $\{a_i^\dagger a_j\}$. As shown in Ref. 23, the XY model is by itself universal provided one uses three physical qubits per *encoded qutrit*, together with nearest-neighbor and next-nearest-neighbor interactions (see also Sec. IX D 1). We discuss the XY model in detail in Sec. IX B. First, however, let us argue qualitatively where the difference between parafermions (qubits) and fermions and bosons originates from. An example will illuminate this. For the case of bosons and fermions, $[b_1^\dagger b_2, b_2^\dagger b_3] = b_1^\dagger b_3$ and $[f_1^\dagger f_2, f_2^\dagger f_3] = f_1^\dagger f_3$. But for parafermions, $[a_1^\dagger a_2, a_2^\dagger a_3] = a_1^\dagger a_3(1-2\hat{n}_2)$. (An easy way to check this, without explicitly calculating the commutator, is to use the mapping to fermions: $f_i^\dagger f_{i+1} \leftrightarrow a_i^\dagger a_{i+1}$ and the Jordan–Wigner transformation $f_i \rightarrow a_i S_i$.) Thus the difference is that *bosons and fermions preserve locality, but parafermions do not*.

Similarly, we can consider additional bilinear operators. For fermions, if we also have $f_i f_j$ and $f_j^\dagger f_i^\dagger$, the group is SO$(2N)$, which is too small to be interesting for QC. In fact this is a model of noninteracting fermions: there exists a canonical transformation to a sum of quadratic terms each of which acts only on a single mode (see also Refs. 6, 29, 30, 32, and 36). For bosons, if we include $b_i b_j$ and $b_j^\dagger b_i^\dagger$, the group generated is the $N(2N+1)$-parameter symplectic group Sp$(2N,R)$ which is noncompact, implying that it has no finite dimensional irreps.[19] If we further include the set of annihilation and creation operators $b_i, b_i^\dagger$ together with the identity operator I, the set $\{I, b_i, b_i^\dagger, b_i b_j, b_j^\dagger b_i^\dagger, b_j^\dagger b_i\}$ generates the semidirect-product group $N(N) \otimes \mathrm{Sp}(2N,R)$, where $N(N)$ is the Heisenberg group, with $(N+1)(2N+1)$ generators (Ref. 19, Chap. 20). This is therefore still too small to be interesting for universal QC. In fact, *this is exactly the reason why linear optics by itself is insufficient for universal QC*. The situation does not change even after introduction of the displacement operators $D_i(\alpha) = \exp(\alpha b_i^\dagger - \alpha^* b_i)$,[16] since $D_i(\alpha) \in N(N) \otimes \mathrm{Sp}(2N,R)$.

The way to universality [with respect to SU(2^N)] is to introduce nonlinear operations such as a Kerr nonlinearity,[37] self-interaction,[38] or conditional measurements.[15,16] A Kerr nonlinearity is a two-qubit interaction of the form $n_i^b n_j^b$ (where i and j are different modes), which directly provides a CPHASE gate. To see this, consider a dual-rail encoding:[37] Suppose that one qubit is encoded into $|0\rangle = b_1^\dagger |\mathtt{0}\rangle$, $|1\rangle = b_2^\dagger |\mathtt{0}\rangle$, while a second qubit is encoded into $|0\rangle = b_3^\dagger |\mathtt{0}\rangle$, $|1\rangle = b_4^\dagger |\mathtt{0}\rangle$ ($|\mathtt{0}\rangle$ is the vacuum state). The two-qubit states are

$$|00\rangle = b_3^\dagger b_1^\dagger |\mathtt{0}\rangle, \quad |01\rangle = b_3^\dagger b_2^\dagger |\mathtt{0}\rangle,$$

$$|10\rangle = b_4^\dagger b_1^\dagger |\mathtt{0}\rangle, \quad |11\rangle = b_4^\dagger b_2^\dagger |\mathtt{0}\rangle.$$

(This is related to case 3 of Sec. VI, where we showed how to make qubits from bosons.) It is then simple to verify that $\exp(-i\pi n_2^b n_4^b)$ acts exactly as a CPHASE gate, i.e., it is represented by the matrix diag$(1,1,1,-1)$ in this two-qubit basis. Here we wish to point out that a recently introduced alternative to a Kerr nonlinearity,[38] namely the self-interaction $(n_i^b)^2$, is in fact closely related to the Kerr nonlinearity. Thus methods developed to use one of these nonlinear interactions can be transported to the other. Let us demonstrate this point by giving a simple circuit to show how one interaction simulates the other. We start with the operator identity

$$\exp(\phi(a^\dagger b - b^\dagger a)) b^\dagger \exp(-\phi(a^\dagger b - b^\dagger a)) = \cos\phi\, b^\dagger + \sin\phi\, a^\dagger,$$

which can be proved directly from the Baker–Hausdorff formula

$$e^{-\alpha A} B e^{\alpha A} = B - \alpha[A,B] + \frac{\alpha^2}{2!}[A,[A,B]] - \frac{\alpha^3}{3!}[A,[A,[A,B]]] + \cdots . \tag{12}$$

Using the latter identity it is then simple to verify the following identity, *which holds on the two-qubit subspace above*,

$$\exp(-i\pi n_2^b n_4^b)=\exp\left(-\frac{\pi}{4}(b_2^\dagger b_4-b_4^\dagger b_2)\right)\exp\left(-i\pi\frac{(n_2^b)^2+(n_4^b)^2-n_2^b-n_4^b}{2}\right)$$
$$\times\exp\left(\frac{\pi}{4}(b_2^\dagger b_4-b_4^\dagger b_2)\right).$$

This is an exact three-gate simulation of the Kerr CPHASE gate in terms of the self-interaction. The simulation uses the linear bosonic operators $b_i^\dagger b_j$ and the local energies n_i^b in order to unitarily rotate the self-interaction terms $(n_2^b)^2+(n_4^b)^2$ to a Kerr interaction.

VIII. FLUCTUATIONS IN PARAFERMION NUMBER AT FINITE TEMPERATURE

So far we have not really made use of the full power of the Fock space representation, which allows to consider the case of fluctuating particle number. The quantum statistics of parafermions is determined by their commutation relations, like fermions (Fermi–Dirac statistics) and bosons (Bose–Einstein statistics). A simple case to consider is that of noninteracting parafermions. The Fermi–Dirac distribution for an ideal Fermi gas is derived using only the restriction that no more than a single fermion can occupy a given mode.[39] Hence the statistics of noninteracting parafermions is clearly the same as that of noninteracting fermions.

Fluctuations in particle number will be a result of interaction of the system with an external bath, which imposes a chemical potential μ (essentially the gradient of the particle flow). As a simple example, consider the following system-bath interaction Hamiltonian:

$$H_I=\sum_{i=1}^{N}\sigma_i^z\otimes B_i^z\rightarrow\sum_{i=1}^{N}(2\hat{n}_i-1)\otimes B_i^z, \tag{13}$$

where B_i^z are bath operators. To further simplify things assume the bath is treated classically, i.e., B_i^z are positive c-numbers. With this Hamiltonian, one can study the fluctuations of parafermions under finite temperature T. Mapping from the well-know result for a noninteracting Fermi gas,[39] it then follows that the average occupation for the ith qubit site is

$$\langle n_i\rangle=\frac{1}{e^{(2B_i^z-\mu)/kT}+1},$$

where k is Boltzman's constant. This is the average value of the qubit-''spin'' (whether it is $|0\rangle$ or $|1\rangle$). Keeping the chemical potential μ fixed, in the limit of $T\rightarrow 0$ we find that $\langle n_i\rangle\rightarrow 1$ if $B_i^z<\mu$, but $\langle n_i\rangle\rightarrow 0$ if $B_i^z>\mu$. Thus, as expected, it is essential to keep the interaction with the bath weak (compared to μ) to prevent fluctuations in qubit ''orientation'' at low temperatures. At finite T we find $\langle n_i\rangle<1$, meaning that some fluctuation is unpreventable. Of course, our model is very naive, and the picture is modified when qubit interactions are taken into account. However, it should be clear that a Fock space description of qubits, i.e., in terms of parafermions, could be valuable in studying qubit statistics at finite temperatures.

IX. UNIVERSALITY OF EXCHANGE-TYPE HAMILTONIANS

In this final section we conclude with an application of the formalism we developed earlier to the study of the universality power of Hamiltonians. We have considered this question in detail before for general exchange-type Hamiltonians (isotropic and anisotropic).[17,18] We first briefly review the universality classification of various physically relevant bilinear Hamiltonians. It will be seen that while in certain cases the Hamiltonian is not sufficiently powerful to be universal with respect to U(2^N), it is universal with respect to a subgroup. As mentioned in Sec. III, this result requires the use of *encoding of physical qubits into logical qubits*.[21–24,52] We then consider in detail the representative example of the XY model, where we give a new proof about universality (in fact, the lack thereof) in the case of nearest-neighbor-only interactions. We then present new results about codes with higher rates than considered in Refs. 17 and 18. For simplicity we revert when convenient to the Pauli matrix notation in this section, which is more familiar to practitioners of QC.

A. Classification of bilinear Hamiltonians

The most general bilinear Hamiltonian for a qubit system is

$$H(t)\equiv H_0+V+F=\sum_i \frac{1}{2}\varepsilon_i\sigma_i^z+\sum_{i<j} V_{ij}+F, \tag{14}$$

where H_0 is the qubit energy term, the interaction between qubits i and j is

$$V_{ij}=\sum_{\alpha,\beta=x,y,z} J_{ij}^{\alpha\beta}(t)\sigma_i^\alpha\sigma_j^\beta,$$

and the external single-qubit operations are

$$F=\sum_i f_i^x(t)\sigma_i^x+f_i^y(t)\sigma_i^y.$$

Recall the "standard" result about universal quantum computation: The group $U(2^N)$ on N qubits can be generated using arbitrary single qubit gates and a nontrivial two-qubit entangling gate such as CNOT.[25] The general Hamiltonian $H(t)$ can generate such a universal gate set, e.g., as follows: Suppose there are controllable σ_i^z and σ_i^x terms. Then σ_i^y can be generated using Euler angles:

$$\sigma_i^y=\exp(-i\pi\sigma_i^z/4)\sigma_i^x\exp(i\pi\sigma_i^z/4).$$

This is an instance of a simple but extremely useful result: let A and B be anticommuting Hermitian operators where $A^2=I$ (I is the identity matrix). Then, using $Ue^VU^\dagger=e^{UVU^\dagger}$ (U is unitary, V is arbitrary),

$$C_A^\varphi\circ\exp(i\theta B)\equiv\exp(-iA\varphi)\exp(i\theta B)\exp(iA\varphi)=\begin{cases}\exp(-i\theta B) & \text{if } \varphi=\pi/2,\\ \exp[i\theta(iAB)] & \text{if } \varphi=\pi/4.\end{cases} \tag{15}$$

One can also derive these relations for su(2) angular momentum operators, without assuming that $\{A,B\}=0$ and $A^2=I$. Let J_x and J_z be generators of su(2). Then, using the Baker–Hausdorff relation Eq. (12), and $[J_z,J_x]=iJ_y$,

$$\exp(-i\varphi J_z)J_x\exp(i\varphi J_z)=J_x\cos\varphi+J_y\sin\varphi.$$

From here follows, using $Ue^VU^\dagger=e^{UVU^\dagger}$ again,

$$C_{J_z}^\varphi\circ\exp(i\theta J_x)=\exp(i\theta(J_x\cos\varphi+J_y\sin\varphi)),$$

and Eq. (15) can be verified, with $\varphi\to 2\varphi$, and $AB\to[A,B]$.

Different QC proposals usually have different two-qubit interactions. Typical types include $\sigma_i^z\sigma_{i+1}^z,\sigma_i^y\sigma_{i+1}^y$ (or $\sigma_i^x\sigma_{i+1}^x$), $\sigma_i^x\sigma_{i+1}^x+\sigma_i^y\sigma_{i+1}^y$ (XY model), and $\vec{\sigma}_i\cdot\vec{\sigma}_j$ (Heisenberg model). It is simple to show that they can all be transformed into a common canonical form $\sigma_i^z\sigma_{i+1}^z$, using a few unitary transformation. The term $\sigma_i^z\sigma_{i+1}^z$ can be used to generate CPHASE and, from there, CNOT.[7] For example, the XY term can first be transformed into $\sigma_i^x\sigma_{i+1}^x$ using Euler angle rotations about σ_i^x, which flips the sign of the $\sigma_i^y\sigma_{i+1}^y$ term:

$$\exp\left[\frac{i\theta}{2}(\sigma_i^x\sigma_{i+1}^x+\sigma_i^y\sigma_{i+1}^y)\right]\left(C_{\sigma_i^x}^{\pi/2}\circ\exp\left[\frac{i\theta}{2}(\sigma_i^x\sigma_{i+1}^x+\sigma_i^y\sigma_{i+1}^y)\right]\right)=\exp(i\theta\sigma_i^x\sigma_{i+1}^x),$$

which can subsequently be transformed into the canonical form using another Euler angle rotation,

$$C_{\sigma_i^y+\sigma_{i+1}^y}^{\pi/4}\circ\sigma_i^x\sigma_{i+1}^x=\sigma_i^z\sigma_{i+1}^z,$$

where using $[\sigma_i^y,\sigma_{i+1}^y]=0$ we have abbreviated $C_{\sigma_{i+1}^y}^{\pi/4}\circ C_{\sigma_i^y}^{\pi/4}$ as $C_{\sigma_i^y+\sigma_{i+1}^y}^{\pi/4}$. The method of Euler angle rotations as applied here is also known as ''selective recoupling'' in the NMR literature.[40]

Not all QC proposals have an interaction Hamiltonian that appears to be of the form V_{ij}, e.g., the ion-trap proposal[12] looks quite different since it involves interactions between ions mediated by a phonon. The interaction between the ith ion and the phonon has the form $\sigma_i^- b^\dagger+\sigma_i^+ b$. This is nevertheless equivalent to an XY model, since

$$\sigma_i^x\sigma_{i+1}^x+\sigma_i^y\sigma_{i+1}^y=C_{\sigma_i^z-\sigma_{i+1}^z}^{\pi/4}\circ 2i[\sigma_i^- b^\dagger+\sigma_i^+ b,\sigma_{i+1}^- b^\dagger+\sigma_{i+1}^+ b].$$

Therefore, in many cases it suffices to study the interaction $\sigma_i^z\sigma_{i+1}^z$.

Let us now consider a number of more restricted models.

1. No external single-qubit operations

If $F=0$, then the *nearest-neighbor* set $\{\sigma_i^z,\sigma_i^z\sigma_{i+1}^z,\sigma_i^x\sigma_{i+1}^z,\sigma_{i+1}^x\sigma_i^z\}$ is still universal, since

$$\sigma_i^y=C_{\sigma_{i+1}^z\sigma_i^z}^{\pi/4}\circ\sigma_{i+1}^z\sigma_i^x.$$

This is the case when H_0 is controllable. More physically, the set $\{\sigma_i^z,\vec{\sigma}_i\cdot\vec{\sigma}_{i+1},(\vec{\sigma}_i\times\vec{\sigma}_{i+1})_y=\sigma_i^z\sigma_{i+1}^x-\sigma_{i+1}^z\sigma_i^x\}$ is also universal, where $\vec{\sigma}=(\sigma^x,\sigma^y,\sigma^z)$. The term $\vec{\sigma}_i\times\vec{\sigma}_{i+1}$ is an anisotropic (Dzyaloshinskii–Moriya) interaction which arises, e.g., in quantum dots in the presence of spin-orbit coupling.[17,41–44]

2. No external single-qubit operations and H_0 uncontrollable

If $F=0$ and H_0 is not controllable, then the nearest-neighbor set $\{\sigma_i^z\sigma_{i+1}^z,\sigma_i^x\sigma_{i+1}^z,\sigma_i^z\sigma_{i+1}^x,\sigma_i^y\sigma_{i+1}^z,\sigma_i^z\sigma_{i+1}^y\}$ is universal, meaning that the interaction term V by itself is universal. One way to see this is to map the set to parafermionic operators and note that it overlaps with the set that generates the parafermionic $U(2^N)$ (Table II).

3. Scalar anisotropic exchange-type interactions

Consider the case $J_{ij}^{\alpha\beta}=J_{ij}^{\alpha}\delta_{\alpha\beta}$ (denoting V by V'), which amounts to limiting the Hamiltonian to scalar anisotropic exchange-type interactions. Using Eq. (3) we then arrive at the second-quantized form

$$H_0=\sum_i \eta_i n_i,$$

$$F=\sum_i (f_i^* a_i+f_i a_i^\dagger), \qquad (16)$$

$$V'=\sum_{i<j}\Delta_{ij}(a_i a_j+a_i^\dagger a_j^\dagger)+J_{ij}(a_i^\dagger a_j+a_j^\dagger a_i)+4J_{ij}^z n_i n_j,$$

where

$$\eta_i=\varepsilon_i+\left(\sum_j J_{ij}^z+J_{ji}^z\right), \quad f_i=(f_i^x-if_i^y),$$

$$\Delta_{ij}=J_{ij}^x-J_{ij}^y, \quad J_{ij}=J_{ij}^x+J_{ij}^y,$$

and we dropped a constant energy term.

V' is the so-called XYZ model of solid state physics. Considering the structure of V' and the classification of operator algebras we carried out in Secs. III and IV, it should be clear that some immediate conclusions can be drawn about the universality power of this Hamiltonian. The full Hamiltonian $H_0+V'+F$ contains the generators of the parafermionic $U(2^N)$ (Table II), so it is universal. On the other hand, without external single qubit operations ($F=0$), we have $[H_0+V',\hat{p}]=0$, so $H_0+V'\in \mathrm{SA}p$, i.e., preserves parity. This immediately implies that the XYZ model (even with H_0) is by itself not universal. However, it can be made universal by *encoding* logical qubits into several (two are in fact sufficient) physical qubits.[17] The elimination of single-qubit operations ($F=0$) can be quite useful, since typically single- and two-qubit operations involve very different constraints. In some cases single-qubit operations can be very difficult to implement (see Refs. 17, 18, and 22 and references therein for extensive discussions of this point).

B. XY model

Consider now the XY model, which is defined by

$$V_{XY}=\sum_{i<j} J_{ij}(a_i^\dagger a_j+a_j^\dagger a_i). \tag{17}$$

It is relevant to a number of proposals for quantum computing, including quantum Hall systems,[45,46] quantum dots in microcavities,[32] quantum dots coupled by exciton exchange,[47] and atoms in microcavities.[48] Let us summarize what is currently known about quantum computational universality of this model.

(i) In Ref. 31 it was shown that the XY model with nearest-neighbor interactions only, together with single-qubit operations, is universal.

(ii) In Ref. 23 it was argued that the XY model is universal without single-qubit operations, provided these gates can be applied between nearest-neighbor and next-nearest-neighbor pairs of qubits. This involved encoding a logical qutrit into three physical qubits: $|0_L\rangle=|001\rangle$, $|1_L\rangle=|010\rangle$, $|2_L\rangle=|100\rangle$. We reconsider this in Sec. IX D in the context of the XXZ model (but using the methods of Ref. 18, the results are valid also for the XY model).

(iii) In Ref. 18 we showed that the XY model is universal using only nearest- and next-nearest-neighbor ($J_{i,i+2}$) interactions, together with single-qubit σ_z terms. This too involved an encoding of a logical qubit into two physical qubits: $|0_L\rangle=|01\rangle$, $|1_L\rangle=|10\rangle$. Two comments are in order about this result: first, next-nearest-neighbor interactions can be nearest neighbor in 2D (e.g., in an hexagonal array); second, unlike Ref. 31, we did not assume the σ_z terms to be controllable, i.e., there is no individual control over ε_i [Eq. (14)]. A similar model is treated in Sec. IX C.

The question now arises: *Is the XY model universal with nearest-neighbor interactions only?* We prove that it is not.

The nearest-neighbor XY model in its parafermionic form is

$$H=\sum_i^N \epsilon_i n_i+\sum_i^N J_{i,i+1}(a_i^\dagger a_{i+1}+a_{i+1}^\dagger a_i).$$

Consulting Table II, we see that H can only generate $\mathrm{SU}(N)$, which is clearly too small even for encoded quantum computation.

C. Antisymmetric XY model

To illustrate the idea of encoding for universality, let us briefly consider the ''antisymmetric XY model:''

$$V_{aXY}=\sum_{i<j} J_{ij}^{xy}\sigma_i^x\sigma_j^y+J_{ij}^{yx}\sigma_i^y\sigma_j^x. \tag{18}$$

Here J_{ij}^{xy} and J_{ij}^{yx} are real. We encode a logical qubit into pairs of nearest-neighbor physical qubits. Letting

$$\tilde{\Delta}_{ij}=J_{ij}^{xy}-J_{ij}^{yx}, \quad \tilde{J}_{ij}\equiv J_{ij}^{xy}+J_{ij}^{yx}, \quad \epsilon_m^{\pm}\equiv\varepsilon_{2m-1}-\varepsilon_{2m}, \tag{19}$$

using the compact notation $\cdot_m\equiv\cdot_{2m-1,2m}$, and assuming that interactions are on only inside pairs of qubits encoding one qubit, we find for the Hamiltonian $H=H_0+V_{aXY}$

$$H_{aXY}=\sum_{m=1}^{N/2}(\tilde{J}_mR_m^y+\epsilon_m^+R_m^z)+(\tilde{\Delta}_mT_m^y+\epsilon_m^-T_m^z), \tag{20}$$

where the T and R operators were defined in Eqs. (6) and (7). Since the T and R operators form commuting sl(2) algebras, the Hilbert space splits into two independent computational subspaces. The R operators conserve parity, so that an appropriate encoding in the axially symmetric case $(\tilde{\Delta}_m=0)$, using standard qubit notation, is $|0_L\rangle=|00\rangle$ and $|1_L\rangle=|11\rangle$. On the other hand, the T operators preserve particle number, so that if $\tilde{J}_m=0$ (axially antisymmetric case), the encoding is $|0_L\rangle=|01\rangle$, $|1_L\rangle=|10\rangle$. In both cases control over the pair of parameters $\{\tilde{J}_m,\epsilon_m^+\}$ (or $\{\tilde{\Delta}_m,\epsilon_m^-\}$) is sufficient for the implementation of the single-encoded-qubit $SU_m(2)$ group (the subscript m refers to the mth logical/encoded qubit).

Logic operations between encoded qubits require the ''encoded selective recoupling'' method introduced in Ref. 18. Consider the ''axially antisymmetric qubit'' $|0_L\rangle=|01\rangle$, $|1_L\rangle=|10\rangle$. First, note that, using Eq. (15),

$$C_{T_{12}^x}^{\pi/2}\circ T_{23}^x=i\sigma_1^z\sigma_2^zT_{13}^x. \tag{21}$$

Now assume we can control $\tilde{\Delta}_{13}$. Then,

$$C_{T_{13}^x}^{\pi/4}\circ(C_{T_{12}^x}\circ T_{23}^x)=\sigma_2^z(\sigma_3^z-\sigma_1^z)/2. \tag{22}$$

Since $\sigma_1^z\sigma_2^z$ is constant on the code subspace it can be ignored. On the other hand, $\sigma_2^z\sigma_3^z$ acts as $-T_1^zT_2^z$:

$$|0_L\rangle_1|0_L\rangle_2=|01\rangle_{12}|01\rangle_{34}\overset{\sigma_2^z\sigma_3^z}{\rightarrow}-|01\rangle_{12}|01\rangle_{34}=-|0_L\rangle_1|0_L\rangle_2, \tag{23}$$

and similarly for the other three combinations: $|0_L\rangle|1_L\rangle\rightarrow|0_L\rangle|1_L\rangle$, $|1_L\rangle|0_L\rangle\rightarrow|1_L\rangle|0_L\rangle$, $|1_L\rangle|1_L\rangle\rightarrow-|1_L\rangle|1_L\rangle$, i.e., $\sigma_2^z\sigma_3^z$ acts as an encoded $\sigma^z\otimes\sigma^z$. This establishes universal encoded computation in the antisymmetric XY model.

D. Codes with higher rates

The encoding of one logical qubit into two physical qubits is not very efficient. Can we do better? That is, can we perform encoded universal QC on codes with a rate (no. of logical qubit to no. of physical qubits) that is greater than $\frac{1}{2}$? We will show how in the case of the XXZ model, defined as $H=H_0+H_{XXZ}$, where

$$H_{XXZ}=\sum_{i<j} J_{ij}^{x}(\sigma_i^x\sigma_j^x+\sigma_i^y\sigma_j^y)+J_{ij}^{z}\sigma_i^z\sigma_j^z .$$

When surface and interface effects are taken into account, the XY examples of QC proposals,[31,45–48] as well as the Heisenberg examples,[11,49,50] are better described by the axially symmetric XXZ model. Additional sources of nonzero J_{ij}^z in the XY examples can be second-order effects (e.g., virtual cavity-photon generation without spin-flips[31]). A natural XXZ example is that of electrons on helium.[33,34]

First, note that the code used in the XY model, $|0_L\rangle=|01\rangle$, $|1_L\rangle=|10\rangle$, is applicable here as well: $T_{ij}^x=\frac{1}{2}(\sigma_i^x\sigma_j^x+\sigma_i^y\sigma_j^y)$ preserves particle number, and serves as an encoded σ^x; σ_i^z terms from H_0 serve as encoded σ^z, and $\sigma_i^z\sigma_{i+1}^z$ applied to physical qubits belonging to different encoded qubits acts as encoded $\sigma^z\otimes\sigma^z$.

In the general encoding case we consider a block of N qubits where codewords are computational basis states (bitstrings of 0's and 1's): $\{q_\alpha^\dagger(N_\alpha)|\mathtt{0}\rangle\}_\alpha$, where $\alpha=\{\alpha_i\}$ and α_i can be 0 or 1, while $N_\alpha=0,\ldots,N$. A code-subspace $\mathcal{C}(N,n)$ will be defined by having a fixed number n of 1's (i.e., of parafermions). Thus there are

$$d_{N,n}\equiv\dim[\mathcal{C}(N,n)]=\binom{N}{n}$$

codewords in a subspace. Examples are considered below. Note that these subspaces are decoherence-free under the process of collective dephasing,[51] and have been analyzed extensively in this context in Ref. 52. Figure 1 in Ref. 52 provides a nice graphical illustration of the $\mathcal{C}(N,n)$ subspaces. Since the decoherence-avoidance properties of the codes we consider here have been extensively discussed before,[51,52] and even implemented experimentally,[53,54] we do not address this issue here. We further note that Ref. 52 provided an in-principle proof that universal encoded QC is possible on all subspaces $\mathcal{C}(N,n)$ independently. However, this proof had several shortcomings: (i) it used a short-time approximation, (ii) it did not make explicit contact with physically realizable Hamiltonians, and (iii) it proceeded by induction, and thus did not explicitly provide an *efficient* algorithm for universal QC. We remedy all these shortcomings here, i.e., we (i) use only finite-time operations, (ii) use only the XXZ Hamiltonian, and (iii) provide an efficient algorithm that scales polynomially in N.

We need a measure that captures how efficient a $\mathcal{C}(N,n)$ code is. If there are d codewords, supported over N p-dimensional objects ($p=2$ is the case of bits), and information is measured in units of q, then we define the rate of the code as

$$r(d,p,q)=\frac{\log_q d}{\log_q p^N}.$$

The traditional definition for qubits is recovered by setting $p=q=2$, i.e., the rate of a code is the ratio of the number of logical qubits $\log_2 d$ to the number of physical qubits N, which in our case becomes

$$r=\frac{\log_2 d_{N,n}}{N}\overset{N\gg 1}{\longrightarrow} S(\epsilon), \tag{24}$$

where $\epsilon\equiv k/N$,

$$S(\epsilon)=-\epsilon\log_2\epsilon-(1-\epsilon)\log_2(1-\epsilon)$$

is the Shannon entropy, and we have used the Stirling formula $\log x!\approx x\log x-x$. Since $S(\frac{1}{2})=1$ the code has a rate that is asymptotically unity for the "symmetric subspace" $\mathcal{C}(N,N/2)$, where the number of 1's equals the number of 0's in each computational basis state. However, we will not in fact attempt to encode $\log_2 d_{N,n}$ logical qubits in the subspace $\mathcal{C}(N,n)$, since the subspace does not have a natural tensor product structure. Instead we will consider $\mathcal{C}(N,n)$ as a subspace encoding a qu*d*it, where $d=d_{N,n}$. Using the generalized definition of a rate above, and measuring information in units of d so that each subspace encodes one unit of information, the rate of such a code is $r=(\log_d d)/(\log_d 2^N)$. This, however, exactly coincides with r of Eq. (24). Therefore we see that the advantage of working with the symmetric subspace $\mathcal{C}(N,N/2)$ in the limit of large N is that its rate approaches unity.

Before embarking on the general analysis, let us note that for an encoding of one logical qubit into N physical qubits, there is a simple construction in terms of parafermionic operators: $Q_{\alpha,\beta}(N)$, $Q^{\dagger}_{\alpha,\beta}(N)$, and $[Q^{\dagger}_{\alpha,\beta}(N), Q_{\alpha,\beta}(N)]$ (which is a function of parafermion number) form an su(2) algebra in the basis $|0_L\rangle=q^{\dagger}_{\alpha}(N_\alpha)|\mathtt{0}\rangle$ and $|1_L\rangle=q^{\dagger}_{\beta}(N-N_\alpha)|\mathtt{0}\rangle$, e.g., for $N=2$ there are two cases: the sets $\{a_1a_2, a_2^{\dagger}a_1^{\dagger}, \hat{n}_1+\hat{n}_2-1\}$ and $\{a_1^{\dagger}a_2, a_2^{\dagger}a_1, \hat{n}_1-\hat{n}_2\}$, with corresponding bases $|0_L\rangle=|\mathtt{0}\rangle$, $|1_L\rangle=a_1^{\dagger}a_2^{\dagger}|\mathtt{0}\rangle$ and $|0_L\rangle=a_1^{\dagger}|\mathtt{0}\rangle$, $|1_L\rangle=a_2^{\dagger}|\mathtt{0}\rangle$. These two encodings are universal (in the sense of blocks of N physical qubits) when only H_0 and V' are controllable [Eq. (16)].

Let us now move on to the general subspace case, starting with an example.

1. Encoded operations: Example

Consider $\mathcal{C}(3,1)=\mathrm{Span}\{|0\rangle\equiv|001\rangle,|1\rangle\equiv|010\rangle,|2\rangle\equiv|100\rangle\}$, i.e., an encoding of a logical qutrit into three physical qubits, as in Ref. 23. Let us count qubits as $i=0,\ldots,N-1$. Our first task is to show how to generate su(3) on this subspace. It is simple to check that $T^x_{01}|001\rangle=0$, $T^x_{01}|010\rangle=|100\rangle$, $T^x_{01}|100\rangle=|010\rangle$, and in total

$$T^x_{01}=\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}=|1\rangle\langle 2|+|2\rangle\langle 1|\equiv X_{12},$$

where the notation X_{12} denotes a σ^x operation between states $|1\rangle\equiv|010\rangle$ and $|2\rangle\equiv|100\rangle$. Similarly, it is simple to check that $T^x_{12}=X_{01}$ and $T^x_{02}=X_{02}$. Further, using $T^z_{ij}\equiv\frac{1}{2}(\sigma^z_i-\sigma^z_j)$, we have $T^z_{01}=Z_{12}$, $T^z_{12}=Z_{01}$, and $T^z_{02}=Z_{02}$, where Z_{12} denotes a σ^z operation between states $|1\rangle$ and $|2\rangle$, etc. Therefore each pair $\{T^x_{ij},T^z_{ij}\}$ generates an encoded su(2). But in the sense of generating, su(N) is a sum of overlapping su(2)'s,[55] so using just the nearest-neighbor interactions $\{T^x_{01},T^z_{01},T^x_{12},T^x_{12}\}$ we can generate all of su(3) on $\mathcal{C}(3,1)$. Note that $[X_{01},X_{12}]=iY_{02}$, so that su(2) between states $|0\rangle,|2\rangle$ can in fact be generated using T^x_{ij}'s alone, without T^z_{ij}'s. This conclusion clearly holds for the generation of all of su(3) on $\mathcal{C}(3,1)$, as first pointed out in Ref. 23.

Next, we need to show how to implement encoded logical operations between two $\mathcal{C}(3,1)$ code subspaces. Let us number the qubits as $i=0,1,2$ for the first block and $i=3,4,5$ for the second block. Consider the effect of turning on J^z_{23}, i.e., consider the action of $\sigma^z_2\sigma^z_3$ on the tensor product space $\mathcal{C}(3,1)\otimes\mathcal{C}(3,1)$. The operator $\sigma^z_2\sigma^z_3$ is represented by a nine-dimensional diagonal matrix on this space, which is easily found to have the following form in the ordered basis $\{|0\rangle\otimes|0\rangle,|0\rangle\otimes|1\rangle,\ldots,|2\rangle\otimes|2\rangle\}$:

$$\sigma^z_2\sigma^z_3=\mathrm{diag}(-1,1,1,-1,1,1,1,-1,-1)=\mathrm{diag}(-1,1,1)\otimes\mathrm{diag}(1,1,-1),$$

e.g., $\sigma^z_2\sigma^z_3|2\rangle\otimes|2\rangle=\sigma^z_2\sigma^z_3|100\rangle\otimes|100\rangle=(+|100\rangle)\otimes(-|100\rangle)=-|2\rangle\otimes|2\rangle$, which explains the -1 in the ninth position in the diagonal matrix above. The important point is that $\sigma^z_2\sigma^z_3$ acts as a tensor product operator on $\mathcal{C}(3,1)\otimes\mathcal{C}(3,1)$, which *puts a relative phase* between the basis states of each $\mathcal{C}(3,1)$ factor. This means that $\sigma^z_2\sigma^z_3$ acts as an "su(3)-like" $\sigma^z\otimes\sigma^z$ on $\mathcal{C}(3,1)\otimes\mathcal{C}(3,1)$. [It is an "su(3)-like" $\sigma^z\otimes\sigma^z$ since for su(2) $\sigma^z=\mathrm{diag}(1,-1)$ and here we have instead $\mathrm{diag}(-1,1,1)$ and $\mathrm{diag}(1,1,-1)$.] It is well known[7] that the CPHASE gate can be generated from the Hamiltonian $\sigma^z\otimes\sigma^z$. The same holds here, so that we can generate a CPHASE gate between two $\mathcal{C}(3,1)$ subspaces by simply turning on a nearest-neighbor interaction between the last qubit in the first block and the first qubit in the second block.

With this example in mind we can move on to the general case.

2. Encoded operations: General subspace case

Let us now consider the case of a general subspace $\mathcal{C}(N,n)$. We can enumerate the codewords as $\{|0\rangle,\ldots,|d_{N,n}\rangle\}$ where $|0\rangle=|0,\ldots,01,\ldots,1\rangle$, etc., to $|d_{N,n}\rangle=|1,\ldots,10,\ldots,0\rangle$, where there are N qubits in total and n 1's in each codeword. Consider a fixed nearest-neighbor pair of qubits at positions $i,i+1$, and the action of $T^x_{i,i+1},T^z_{i,i+1}$. The four possibilities for qubit values at these positions are {00,01,10,11}. Now consider a pair of codewords $|t\rangle$, $|t'\rangle$ such that $|t\rangle$ has 01 in the $i,i+1$ positions while $|t'\rangle$ has 10 in the $i,i+1$ positions, and they are identical everywhere else. We can always find such a pair by definition of $\mathcal{C}(N,n)$. The action of $T^x_{i,i+1},T^z_{i,i+1}$ on $|t\rangle$, $|t'\rangle$ is to generate su(2) between them, just as shown in the case of $\mathcal{C}(3,1)$ above. On the other hand, the action of $T^x_{i,i+1},T^z_{i,i+1}$ in the case of 00 or 11 in the $i,i+1$ positions is to annihilate all corresponding codewords [which are anyhow outside of the given $\mathcal{C}(N,n)$ subspace]. This null action means that, when exponentiated, $T^x_{i,i+1},T^z_{i,i+1}$ act as identity on these codewords. Therefore the action of $T^x_{i,i+1},T^z_{i,i+1}$ is precisely to generate su(2) between $|t\rangle$, $|t'\rangle$, and nothing more. Denote this by $\mathrm{su}(2)^{(1)}_{i,i+1}$. Let us now keep the 01 and 10 at positions $i,i+1$ fixed, and vary all other $N-2$ positions in $|t\rangle$, $|t'\rangle$, subject to the constraint of n 1's, and in the same manner in both $|t\rangle$, $|t'\rangle$. We then run over $K=\binom{N-2}{n-1}$ codewords, and $T^x_{i,i+1},T^z_{i,i+1}$ generate su(2) between each pair of new $|t\rangle$, $|t'\rangle$. Denote these by $\mathrm{su}(2)^{(k)}_{i,i+1}$, $k=1,\ldots,K$. By further letting $i=0,\ldots,N-2$ we generate $N-1$ *overlapping* su(2)'s. These su(2)'s can be connected by swaps so that we can generate all $\mathrm{su}(2)^{(k)}_{i,j}$, $k=1,\ldots,K$, $i<j$. We thus have a total of $\binom{N-2}{n-1}\binom{N}{2}$ su(2)'s. To generate the entire su($d_{N,n}$) we need no more than $d_{N,n}=\binom{N}{n}$ overlapping su(2)'s. Since $\binom{N-2}{n-1}\binom{N}{2}/\binom{N}{n}=\frac{1}{2}n(N-n)>1$, we have more than enough overlapping su(2)'s, and su($d_{N,n}$) can be generated.

What is left is to show that we can perform a controlled operation between two $\mathcal{C}(N,n)$ subspaces. To do so we again use the nearest-neighbor interaction $\sigma^z_{N-1}\sigma^z_N$, where the first factor (σ^z_{N-1}) acts on the last qubit $(N-1)$ of the first $\mathcal{C}(N,n)$ subspace, and the second factor (σ^z_N) acts on the first qubit (N) of the second $\mathcal{C}(N,n)$ subspace. Now let us sort the codewords in the two subspaces in an identical manner, e.g., by increasing binary value. Then consider the action of $\sigma^z_{N-1}\sigma^z_N$ on the resulting ordered basis $\{|0\rangle\otimes|0\rangle,|0\rangle\otimes|1\rangle,\ldots,|d_{N,n}\rangle\otimes|d_{N,n}\rangle\}$. This action generates a representation of $\sigma^z_{N-1}\sigma^z_N$ by a $d_{N,n}\times d_{N,n}$ diagonal matrix. As in the $\mathcal{C}(3,1)$ case considered earlier, this matrix is actually a tensor product of an "su($d_{N,n}$)-like" $\sigma^z\otimes\sigma^z$ on $\mathcal{C}(N,n)\otimes\mathcal{C}(N,n)$. It is simple to determine the form of these two (different) σ^z's. For the codewords belonging to the left $\mathcal{C}(N,n)$ factor, write down a $+1$ (-1) for each 0 (1) in the Nth position. These numbers are the diagonal entries of the left "su($d_{N,n}$)-like" σ^z factor. Similarly, for the codewords belonging to the right $\mathcal{C}(N,n)$ factor, write down a $+1$ (-1) for each 0 (1) in the $(N+1)$th position. These numbers are the diagonal entries of the right "su($d_{N,n}$)-like" σ^z factor. Since each such "su($d_{N,n}$)-like" σ^z puts relative phases between the basis states of $\mathcal{C}(N,n)$, the action of $\sigma^z_{N-1}\sigma^z_N$ is that of a generalized CPHASE between the two code subspaces. This is sufficient together with su($d_{N,n}$) on each block to perform universal quantum computation.[56]

X. CONCLUSIONS

The standard quantum information-theoretic approach to qubits and operations on qubits emphasizes qubits as *vectors* in a Hilbert space and operations as *transformations* of these vectors.[7] This is the point of view of the first-quantized formulation of quantum mechanics. An alternative, mathematically equivalent, point of view is the Fock space, second-quantized formulation of quantum mechanics, which emphasizes the particlelike nature of quantum states. Qubit up/down states are replaced by qubit presence/absence, while rotations are replaced by operators that count or change particle occupation numbers. The mapping of qubits to parafermions discussed in this article is a mapping between these first- and second-quantized formulations. It proved to be a useful tool in studying the connection between qubits, bosons, and fermions, in analyzing the algebraic structure of qubit Hamiltonians, and in studying related quantum computational universality questions. In particular, it allowed us to classify subalgebras of fermion, boson, and qubit operators and decide their power for quantum computational universality. These results are relevant for physical implementation of quantum computers: a physical N-qubit system comes equipped with a given Hamiltonian, which generates a subalgebra of su(2^N). It is important to know whether this Hamiltonian is by itself universal or needs to be supplemented with additional operations, or whether one needs to encode physical qubits into logical qubits in order to attain universality. Our classification settles this question for many subalgebras of physical interest.

Another potential advantage of the parafermionic approach, as a second-quantized formalism for qubits, lies in its ability to naturally deal with a ''qubit-field,'' i.e., situations where the qubit number is not a conserved quantity. This is certainly a concern for optical and various solid-state quantum computer implementations. We leave the study of a qubit field theory as an open area for future explorations.

ACKNOWLEDGMENTS

This material is based on research sponsored by the Defense Advanced Research Projects Agency under the QuIST program and managed by the Air Force Research Laboratory (AFOSR), under agreement F49620-01-1-0468. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the Air Force Research Laboratory or the U.S. Government. D.A.L. further gratefully acknowledges financial support from PREA, NSERC, PRO, and the Connaught Fund. We thank Dr. M. S. Byrd for useful discussions.

[1] H. S. Green, Phys. Rev. **90**, 270 (1953).
[2] O. W. Greenberg, Phys. Rev. Lett. **13**, 598 (1964).
[3] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer, Dordrecht, 1998).
[4] N. March, W. H. Young, and S. Sampanthar, *The Many-Body Problem in Quantum Mechanics* (Dover, New York, 1995).
[5] P. Jordan and E. Wigner, Z. Phys. **47**, 631 (1928).
[6] S. Bravyi and A. Kitaev, quant-ph/0003137.
[7] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, UK, 2000).
[8] The mapping from qubits to parafermions was first pointed out in L.-A. Wu and D. A. Lidar, quant-ph/0103039v1. Our definition of a parafermion is inspired by Green[1] and Greenberg,[9] but differs somewhat. Like these authors we start from $\{a_i, a_i^\dagger\}=1$ and $[a_i, a_j^\dagger]=0$ for $i\neq j$. Green was the first to introduce these commutation relations, but did not name the corresponding particles. Greenberg did not name them either, but called ''parafermion'' a particle defined by $a^\dagger=\Sigma_{j=1}^N a_j^\dagger$. The commutation relation we use to define parafermions is therefore different from Greenberg's. Nevertheless we prefer to call a particle satisfying these relations a ''parafermion,'' since they emphasize the two-dimensional Hilbert–Fock space of an individual particle (like fermions). The opposite choice of commutation relations, $[a_i, a_i^\dagger]=1$ and $\{a_i, a_j^\dagger\}=0$ for $i\neq j$, can be used to define ''parabosons:'' particles with unlimited occupation number per mode, but without a natural tensor product structure. Finally, we note that the particle we are referring to as a parafermion is also known sometimes as a ''hardcore boson,'' e.g., K. Bernardet *et al.*, Phys. Rev. B **65**, 104519 (2002).
[9] O. W. Greenberg and K. I. Macrae, Nucl. Phys. B **219**, 358 (1983).
[10] G. D. Mahan, *Many-Particle Physics*, 3rd ed. (Kluwer Academic, New York, 2000).
[11] D. Loss and D. P. DiVincenzo, Phys. Rev. A **57**, 120 (1998).
[12] J. I. Cirac and P. Zoller, Phys. Rev. Lett. **74**, 4091 (1995).
[13] P. Chen, C. Piermarocchi, and L. J. Sham, Phys. Rev. Lett. **87**, 067401 (2001).
[14] S. Lloyd, Science **273**, 1073 (1996).
[15] E. Knill, R. Laflamme, and G. J. Milburn, Nature (London) **409**, 46 (2001).
[16] T. C. Ralph, W. J. Munro, and G. J. Milburn, quant-ph/0110115.
[17] L.-A. Wu and D. A. Lidar, Phys. Rev. A **65**, 042318 (2002).
[18] D. A. Lidar and L.-A. Wu, Phys. Rev. Lett. **88**, 017905 (2002).
[19] B. Wybourne, *Classical Groups for Physicists* (Wiley, New York, 1974).
[20] S. Lloyd, Phys. Rev. Lett. **75**, 346 (1995). See N. Weaver, J. Math. Phys. **41**, 240 (2000) for a formal proof.
[21] D. Bacon, J. Kempe, D. A. Lidar, and K. B. Whaley, Phys. Rev. Lett. **85**, 1758 (2000).
[22] D. P. DiVincenzo, D. Bacon, J. Kempe, G. Burkard, and K. B. Whaley, Nature (London) **408**, 339 (2000).
[23] D. Bacon, J. Kempe, D. P. DiVincenzo, D. A. Lidar, and K. B. Whaley, in *Proceedings of the 1st International Conference on Experimental Implementations of Quantum Computation, Sydney, Australia*, edited by R. Clark (Rinton, Princeton, NJ, 2001), p. 257.
[24] D. A. Lidar, D. Bacon, J. Kempe, and K. B. Whaley, Phys. Rev. A **63**, 022307 (2001).
[25] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, and H. Weinfurter, Phys. Rev. A **52**, 3457 (1995).

[26] D. P. DiVincenzo, Phys. Rev. A **51**, 1015 (1995).
[27] B. Judd and J. Elliott, *Topics in Atomic and Nuclear Theory* (University of Canterbury, Christchurch, N.Z., 1970).
[28] C. D. Batista and G. Ortiz, Phys. Rev. Lett. **86**, 1082 (2001).
[29] B. M. Terhal and D. P. DiVincenzo, Phys. Rev. A **65**, 032325 (2002).
[30] E. Knill, ''Fermionic Linear Optics and Matchgates,'' quant-ph/0108033.
[31] A. Imamoḡlu, D. D. Awschalom, G. Burkard, D. P. DiVincenzo, D. Loss, M. Sherwin, and A. Small, Phys. Rev. Lett. **83**, 4204 (1999).
[32] L. Viola, E. Knill, and R. Laflamme, J. Phys. A **34**, 7067 (2001).
[33] P. M. Platzman and M. I. Dykman, Science **284**, 1967 (1999).
[34] M. I. Dykman and P. M. Platzman, Fortschr. Phys. **48**, 1095 (2000).
[35] L.-A. Wu, M. S. Byrd, and D. A. Lidar, Phys. Rev. Lett. **89**, 057904 (2002).
[36] P. Zanardi, Phys. Rev. A **65**, 042101 (2002).
[37] I. L. Chuang and Y. Yamamoto, Phys. Rev. A **52**, 3489 (1995).
[38] R. Ionicioiu and P. Zanardi, quant-ph/0204118.
[39] L. D. Landau and E. M. Lifshitz, *Statistical Physics Part 1* (Pergamon, Oxford, 1989).
[40] C. Slichter, *Principles of Magnetic Resonance*, No. 1 in *Springer Series in Solid-State Sciences* (Springer, Berlin, 1996).
[41] K. V. Kavokin, Phys. Rev. B **64**, 075305 (2001).
[42] N. E. Bonesteel, D. Stepanenko, and D. P. DiVincenzo, Phys. Rev. Lett. **87**, 207901 (2001).
[43] G. Burkard and D. Loss, Phys. Rev. Lett. **88**, 047903 (2002).
[44] L.-A. Wu and D. A. Lidar, quant-ph/0202135.
[45] V. Privman, I. D. Vagner, and G. Kventsel, Phys. Lett. A **239**, 141 (1998).
[46] D. Mozyrsky, V. Privman, and M. L. Glasser, Phys. Rev. Lett. **86**, 5112 (2001).
[47] L. Quiroga and N. F. Johnson, Phys. Rev. Lett. **83**, 2270 (1999).
[48] S.-B. Zheng and G.-C. Guo, Phys. Rev. Lett. **85**, 2392 (2000).
[49] B. E. Kane, Nature (London) **393**, 133 (1998).
[50] R. Vrijen, E. Yablonovitch, K. Wang, H. W. Jiang, A. Balandin, V. Roychowdhury, T. Mor, and D. DiVincenzo, Phys. Rev. A **62**, 012306 (2000).
[51] L.-M Duan and G.-C. Guo, Phys. Rev. A **57**, 737 (1998).
[52] J. Kempe, D. Bacon, D. A. Lidar, and K. B. Whaley, Phys. Rev. A **63**, 042307 (2001).
[53] P. G. Kwiat, A. J. Berglund, J. B. Altepeter, and A. G. White, Science **290**, 498 (2000).
[54] D. Kielpinski, V. Meyer, M. A. Rowe, C. A. Sackett, W. M. Itano, C. Monroe, and D. J. Wineland, Science **291**, 1013 (2001).
[55] R. N. Cahn, *Semi-Simple Lie Algebras and Their Representations* (Benjamin/Cummings, Reading, MA, 1984), available online at http://www-physics.lbl.gov/~rncahn/book.html.
[56] That arbitrary single-qu*d*it operations, together with a controlled operation between two qu*d*its, are sufficient for universal quantum computation, follows from Theorem 1 in J.-L. Brylinski and R. Brylinski, quant-ph/0108062.