Lower bounds for the fidelity of entangled-state preparation

Rolando D. Somma,* John Chiaverini, and Dana J. Berkeland
Physics Division, Los Alamos National Laboratory, MS D454, Los Alamos, New Mexico 87545, USA
(Received 8 June 2006; published 1 November 2006)

Estimating the fidelity of state preparation in multiqubit systems is generally a time-consuming task. Nevertheless, this complexity can be reduced if the desired state can be characterized by certain symmetries measurable with the corresponding experimental setup. In this paper we give simple expressions to estimate the fidelity of multiqubit state preparation for rotational-invariant, stabilizer, and generalized coherent states. We specifically discuss the GHZ-type and W-type states, and obtain efficiently measurable lower bounds for the fidelity. We use these techniques to estimate the fidelity of a quantum simulation of an Ising-like interaction model using two trapped ions. These results are directly applicable to experiments using fidelity-based entanglement witnesses, such as quantum simulations and quantum computation.

DOI: 10.1103/PhysRevA.74.052302 PACS number(s): 03.67.Mn, 03.65.Wj, 03.65.Ta, 42.50.Xa

I. INTRODUCTION

Highly entangled states provide required resources for quantum information processing (QIP), a developing field advancing both the fundamental understanding of quantum systems and novel technologies. Entangled states are used to encode qubits for fault-tolerant quantum computation [1] and for more efficient quantum state readout [2]. Such states are also used for quantum communication over long distances and teleportation protocols [3]. Finally, highly entangled states are central to many-body quantum simulations, whose power lies in their ability to coherently manipulate such states for later analysis [4–7]. Entangled-state preparation in any QIP system and its verification is thus of paramount importance.

One successful architecture for QIP is the trapped-ion system, in which qubits are encoded in the internal electronic states of ions, and laser fields can control the collective internal and external states of the ions. Recently [8,9], multiqubit entanglement has been experimentally demonstrated in these devices. In Ref. [9], quantum state tomography (QST) [10,11] was employed to verify that W-type states for up to $N=8$ ions (qubits) were produced. Since the dimension of the Hilbert space $\mathcal{H}$ associated with a quantum system increases exponentially with the system size (as does the dimension of the density matrix), performing full QST is, in general, extremely inefficient for large systems. For example, realizing QST in an ion trap device requires on the order of $\mathcal{O}(3^N)$ measurements, where N is the number of qubits, each measured in the x, y, and z bases. In Ref. [9] the full QST process for $N=8$ ions required 656,100 measurements over ten hours. This extremely large data set reduced errors due to quantum projection noise [12], until other sources of error (such as imperfect optical pumping, ion addressing errors, nonresonant excitations, and optical decoherence) were dominant. Such examples illustrate a potential roadblock to practical implementation of large-scale QIP: it is impossible to exploit the speedups associated with QIP if an exponentially large amount of processing must be performed to verify the creation of the desired states.

It is important then to investigate efficient methods to estimate the reliability of experimental quantum state preparation. Here we point out that many useful entangled states have certain symmetries which allow fidelity determination without full QST. For these states, an efficient number (polynomial in N) of measurements is sufficient to obtain lower bounds for the fidelity. A similar technique has been used to determine a lower bound on the fidelity of several-particle quantum superposition (Schrödinger cat) states [8]; we describe and generalize such methods.

We then use the quantum fidelity as a measure related to the *distance* between quantum states [1]. Specifically, the quantum fidelity $\mathcal{F}$ between the actual state ρ_l prepared in the laboratory, which is in general mixed [i.e., $\mathrm{Tr}(\rho_l^2)<1$], and the desired pure state $|\psi\rangle$ to be prepared is defined by

$$\mathcal{F}(\rho_l,\rho_\psi)=\sqrt{\langle\psi|\rho_l|\psi\rangle}=[\mathrm{Tr}(\rho_l\rho_\psi)]^{1/2}. \tag{1}$$

Equation (1) can be evaluated by measuring the expectation value of the density operator $\rho_\psi=|\psi\rangle\langle\psi|$ over the state ρ_l. For example, if $|\psi\rangle$ is a product state, then ρ_ψ has only one nonzero matrix element (in the right basis) that is along its diagonal. The fidelity $\mathcal{F}(\rho_l,\rho_\psi)$ can be simply obtained by repeatedly preparing ρ_l and then measuring the population of the state $|\psi\rangle$.

More generally, the density matrix of an N-qubit system is a linear combination of operators belonging to the $\mathfrak{u}(2^N)$ algebra:

$$\rho=\sum_{\alpha_1,\ldots,\alpha_N}c^{\rho}_{\alpha_1,\ldots,\alpha_N}(\sigma^1_{\alpha_1}\otimes\cdots\otimes\sigma^N_{\alpha_N}), \tag{2}$$

where the subscripts $\alpha_j=0,1,2,3$ correspond to the Pauli operators $\mathbb{1}$, σ_x, σ_y, and σ_z, respectively. (The symbol $\otimes$ represents the matrix tensor product.) These operators are given by

$$\mathbb{1}=\begin{pmatrix}1&0\\0&1\end{pmatrix},\quad \sigma_x=\begin{pmatrix}0&1\\1&0\end{pmatrix},$$

*Electronic address: somma@lanl.gov

$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{3}$$

In particular, $\sigma^j_{\alpha_j} = \mathbb{1}^1 \otimes \cdots \otimes \mathbb{1}^{j-1} \otimes \sigma^j_{\alpha_j} \otimes \mathbb{1}^{j+1} \cdots \otimes \mathbb{1}^N$, with the Pauli matrix σ_{α_j} being located at the jth position in the decomposition. From now on, we remove the symbol $\otimes$ from the products of Pauli operators. We also adopt the convention $\langle \hat{A} \rangle_{\rho_l} \equiv \mathrm{Tr}[\rho_l \hat{A}]$.

The real coefficients $c^{\rho}_{\alpha_1,\alpha_2,\ldots,\alpha_N}$ are given by

$$c^{\rho}_{0,\ldots,0} = 2^{-N},$$

$$c^{\rho}_{\alpha_1,\ldots,\alpha_N} = 2^{-N}\mathrm{Tr}[\rho(\sigma^1_{\alpha_1} \cdots \sigma^N_{\alpha_N})] \quad \text{(otherwise)}. \tag{4}$$

Then,

$$\mathcal{F}^2(\rho_l,\rho_\psi) = \sum_{\alpha_1,\ldots,\alpha_N} c^{\rho_l}_{\alpha_1,\ldots,\alpha_N} c^{\rho_\psi}_{\alpha_1,\ldots,\alpha_N}, \tag{5}$$

and full QST is generally needed to estimate the coefficients $c^{\rho_l}_{\alpha_1,\ldots,\alpha_N}$ required to evaluate Eq. (5). However, if the state $|\psi\rangle$ can be uniquely characterized by certain symmetries, some of the coefficients $c^{\rho_\psi}_{\alpha_1,\ldots,\alpha_N}$ will vanish and the corresponding $c^{\rho_l}_{\alpha_1,\ldots,\alpha_N}$ need not be measured. Full QST over ρ_l is then no longer required, and the complexity of evaluating Eq. (5) or of setting a lower bound on $\mathcal{F}^2(\rho_l,\rho_\psi)$ can be greatly reduced.

A straightforward example of using symmetry to simplify fidelity estimation can be seen in previous work with N-qubit cat states $|\mathrm{GHZ}\rangle_N = \frac{1}{\sqrt{2}}(|0_1 0_2 \cdots 0_N\rangle + |1_1 1_2 \cdots 1_N\rangle)$ in trapped ion systems [13,14]. The $|\mathrm{GHZ}\rangle_N$ state is uniquely defined by the symmetry operators $\{\sigma^1_x \sigma^2_x \cdots \sigma^N_x, \sigma^1_z \sigma^2_z, \sigma^2_z \sigma^3_z, \ldots, \sigma^{N-1}_z \sigma^N_z\}$, that leave the state unchanged after their action. As we will show, the fidelity of having prepared $|\mathrm{GHZ}\rangle_N$ can be estimated by measuring the expectation values of the symmetry operators. In an ion trap setup, for example, repeated simultaneous measurements of the projections of all of the ion spins along the x axis, and of all of the ion spins along the z axis, gives the fidelity of having prepared the $|\mathrm{GHZ}\rangle_N$ state [15].

In Sec. II we expand this idea to study certain cases in which the desired state can be characterized by different types of symmetries. First, we focus on the class of rotational-invariant states (i.e., eigenstates of the total angular momentum operator) since some interesting entangled states for QIP tasks are in this class [16]. Second, we study the family of stabilizer states (SSs), which provide the foundation of the stabilizer formalism used in different quantum error-correcting procedures [17]. Third, we study the case of generalized coherent states (GCSs), which provide a natural framework to study certain quantum simulations of many-body problems [18,19]. In Sec. III we apply the obtained results to (numerically) estimate the fidelity of the evolution of the internal states of two trapped ions with an Ising-like Hamiltonian, using the methods described in Ref. [7]. Finally, in Sec. IV we discuss the estimation of the fidelity of state preparation due to the statistics of a finite number of experiments, and in Sec. V we present our conclusions.

II. QUANTUM FIDELITY AND HIGHLY SYMMETRIC STATES

The density operator of a pure state $|\psi\rangle$ that can be uniquely characterized by its symmetry operators $\{\hat{O}_1, \ldots, \hat{O}_L\}$ can be written in terms of these operators only. Thus, the fidelity of having prepared $|\psi\rangle$ [Eq. (1)] can be estimated by measuring observables, over the actual prepared state ρ_l, that solely involve correlations between the $\hat{O}_k$'s. In other words, measurements in bases not related to the symmetry operators are not required because they do not provide any information when evaluating the fidelity of state preparation. The purpose of this section is then to give lower bounds for estimating the fidelity of state preparation for three classes of highly-symmetric N-qubit quantum states, and to show that these can be efficiently obtained.

A. Rotational-invariant states

For a system of N qubits, the rotational-invariant pure states are completely specified by the equations

$$J^2|\psi\rangle = j(j+2)|j,j_z\rangle, \tag{6}$$

$$J_z|\psi\rangle = j_z|j,j_z\rangle, \tag{7}$$

where $J^2 = J_x^2 + J_y^2 + J_z^2$ is the (squared) total angular momentum operator, $J_\gamma = \sigma^1_\gamma + \sigma^2_\gamma + \cdots + \sigma^N_\gamma$ ($\gamma = x,y,z$), and σ^j_γ is the corresponding Pauli operator acting on the jth qubit. The factor 2 in Eq. (6) is due to our use of Pauli operators instead of the actual spin-1/2 operators. Then, the quantum numbers j and j_z satisfy the following properties: $j^{\max} = j_z^{\max} = N$, $|\Delta j| \geq 2$, $|\Delta j_z| \geq 2$, and $-N \leq j_z \leq N$ (the symbol Δ indicates the difference between different eigenvalues). In particular, if $-N+2 \leq j_z \leq N-2$, the state $|j,j_z\rangle$ is entangled. For $j=N$, $j_z = N-2$, then $|N,N-2\rangle = |W_N\rangle$, with

$$|W_N\rangle = \frac{1}{\sqrt{N}}[|1_1 0_2 \cdots 0_N\rangle + |0_1 1_2 \cdots 0_N\rangle + \cdots + |0_1 0_2 \cdots 1_N\rangle]. \tag{8}$$

Although the $|W_N\rangle$ states are not maximally entangled for $N>2$, they are particularly useful for processes such as teleportation [20] and quantum secure communication [21]. Their usefulness is due to the robustness of entanglement in W type states under the loss of one of the qubits, and to the existence of qubit-qubit quantum correlations for any pair of qubits. The former property can be seen by constructing the density operator of $N-1$ qubits by tracing out the other one. For example, when $N=3$, we obtain

$$\rho_{W_3(\hat{1})} = \mathrm{Tr}_{\hat{1}}[|W_3\rangle\langle W_3|] = \frac{2}{3}|\mathrm{Bell}\rangle\langle\mathrm{Bell}| + \frac{1}{3}|0_2 0_3\rangle\langle 0_2 0_3|, \tag{9}$$

where $\hat{1}$ refers to the loss of qubit 1 and $|\mathrm{Bell}\rangle = \frac{1}{\sqrt{2}}[|0_2 1_3\rangle + |1_2 0_3\rangle]$ is a Bell state (i.e., maximally entangled state) of qubits 2 and 3. This Bell state can then be used, for example, to perform quantum teleportation. Similar results are obtained when losing qubit 2 or 3.

The density operator ρ_{j,j_z} of an N-qubit rotational-invariant state with quantum numbers $j=N$ and $-N \leqslant j_z \leqslant N$, in terms of the symmetry operators J and J_z, is

$$\rho_{j,j_z} = \kappa^{-1}\Big[\hat{\prod}_{-j\leqslant j_z'\leqslant j} \hat{\pi}_{j_z'}\Big]\Big[\hat{\prod}_{0\leqslant j'\leqslant N} \hat{\pi}_{j'}\Big], \tag{10}$$

where $\hat{\pi}_{j_z'}=(J_z-j_z')$ and $\hat{\pi}_{j'}=[J^2-j'(j'+2)]$. The symbols $\hat{\Pi}$ denotes that the terms $\hat{\pi}_j$ and $\hat{\pi}_{jz}$ have been excluded from the product. The normalization constant κ is given by

$$\kappa = \hat{\prod}_{-j\leqslant j_z'\leqslant j} (j_z - j_z')\hat{\prod}_{0\leqslant j'\leqslant N} [j(j+2) - j'(j'+2)]. \tag{11}$$

To evaluate the fidelity of Eq. (1), that is $\mathcal{F}(\rho_l,\rho_{j,j_z}) = [\mathrm{Tr}(\rho_l\rho_{j,j_z})]^{1/2}$, it suffices to obtain the expectation values of the correlations between the operators J^2 and J_z appearing in Eq. (10) only. Although this procedure is still inefficient and an exponentially large amount (with respect to N) of observables (i.e., products of Pauli operators) must be measured, it is more resource efficient than performing full QST to obtain $\mathcal{F}(\rho_l,\rho_{j,j_z})$.

For example, if one is interested in preparing the Bell state $|\mathrm{Bell}\rangle = |j=2,j_z=0\rangle = \frac{1}{\sqrt{2}}[|1_1 0_2\rangle + |0_1 1_2\rangle]$ using an ion trap device, the fidelity of state preparation could be determined by measuring over three different bases only, corresponding to the expectation values $\langle\sigma_x^1\sigma_x^2\rangle_{\rho_l}$, $\langle\sigma_y^1\sigma_y^2\rangle_{\rho_l}$, $\langle\sigma_z^1\rangle_{\rho_l}$, $\langle\sigma_z^2\rangle_{\rho_l}$, and $\langle\sigma_z^1\sigma_z^2\rangle_{\rho_l}$, respectively.

To obtain a lower bound on the fidelity of rotational-invariant state preparation for $j=N$, we first define the operators $\mathcal{S}_{J_z} = -\frac{1}{4}(J_z - j_z)^2$ and $\mathcal{S}_{J^2} = -\frac{1}{64}[J^2 - N(N+2)]$. These satisfy

$$[\mathcal{S}_{J_z} + \mathcal{S}_{J^2}]|j',j_z'\rangle = e_{j',j_z'}|j',j_z'\rangle, \tag{12}$$

where $e_{j',j_z'} \leqslant -1$ for $(j',j_z') \neq (j,j_z)$ and $e_{j,j_z}=0$. Therefore, for a general pure state $|\phi\rangle = \Sigma_{j',j_z'} c_{j',j_z'}|j',j_z'\rangle$, we obtain

$$\langle\phi|\mathcal{S}_{J_z} + \mathcal{S}_{J^2} + 1|\phi\rangle = \sum_{j',j_z'} (e_{j',j_z'}+1)|c^2_{j',j_z'}| \leqslant |c_{j,j_z}|^2, \tag{13}$$

where $|c_{j,j_z}|^2$ is the probability of projecting $|\phi\rangle$ onto the state $|j=N,j_z\rangle$ (i.e., the squared fidelity between the states). Since the actual prepared state ρ_l is in general a convex combination of pure states, Eq. (13) yields

$$\mathcal{F}^2(\rho_l,\rho_{j,j_z}) \geqslant \langle\mathcal{S}_{J_z} + \mathcal{S}_{J^2}\rangle_{\rho_l} + 1. \tag{14}$$

This lower bound can be efficiently estimated by measuring only the observables J_z, J_z^2, and J^2 a large amount of times over the state ρ_l. Therefore, only a polynomial (in N) amount of expectation values of different products of Pauli operators must be measured ($3N^2 - 2N$ in this case).

When $j<N$, the subspace with quantum numbers j, j_z is degenerate and Eqs. (6) and (7) do not specify the state uniquely. Then, Eq. (10) becomes the projector onto the corresponding subspace. Nevertheless, the squared fidelity $\mathcal{F}^2(\rho_l,\rho_{j,j_z})$ will still equal the probability of having created a pure or mixed quantum rotational-invariant state with quantum numbers j, j_z. This equality is due to the fact that the operator ρ_{j,j_z} takes into account a sum over the probabilities of being in any eigenstate of J and J_z with eigenvalues j and j_z, respectively. When $j<N$, the operator $\mathcal{S}_{J^2}$ must be redefined as $\mathcal{S}_{J^2} = -\frac{1}{64}[J^2 - j(j+2)]^2$, so the properties for the coefficients $e_{j',j_z'}$ in Eq. (12) still hold. In this case, a lower bound on $\mathcal{F}^2(\rho_l,\rho_{j,j_z})$ can be obtained by measuring $N^4/4 - N^3 + 11N^2/4 - N$ (for N even) expectation values of different products of Pauli operators.

B. Stabilizer states

Another interesting family of states are the stabilizer states [17], which are defined by

$$\hat{O}_s|\psi\rangle = +1|\psi\rangle; \quad s \in [1,S]. \tag{15}$$

The stabilizer operators $\hat{O}_s \in \mathfrak{u}(2^N)$ are products of Pauli operators [22] and have ± 1 as possible eigenvalues. (Note that $\hat{O}_1 = \mathbb{1}$ is the trivial stabilzer.) An immediate consequence of Eq. (15) is that the operators $\hat{O}_s$ commute with each other: $[\hat{O}_s,\hat{O}_{s'}]=0$. Here, we focus on the case in which the state $|\psi\rangle$ is uniquely defined by Eq. (15); that is, the dimension of the stabilized space is one. The set $G_S = \{\hat{O}_1,\ldots,\hat{O}_S\}$ forms the so called stabilizer group for $|\psi\rangle$. For practical purposes, we define G_S in a compact way by its L linear independent generators [17]: $G_S \equiv (\hat{g}_1,\ldots,\hat{g}_L)$, satisfying

$$\hat{g}_i|\psi\rangle = +1|\psi\rangle; \quad i \in [1,L]. \tag{16}$$

Without loss of generality we can write $|\psi\rangle \equiv |g_1=1,\ldots,g_L=1\rangle$.

The eigenstates of the stabilizer operators (associated with the stabilizer state) form a complete set of the 2^N dimensional Hilbert space $\mathcal{H}$. Therefore, the density operator ρ_ψ can be written within this formalism as

$$\rho_\psi = |g_1=1,\ldots,g_L=1\rangle\langle g_1=1,\ldots,g_L=1| = \frac{1}{2^L}\prod_{i=1}^{L}(\hat{g}_i + \mathbb{1}), \tag{17}$$

where $\mathbb{1} \equiv \mathbb{1}^1 \otimes \cdots \otimes \mathbb{1}^N$. The fidelity [Eq. (1)] can then be estimated by measuring, over the actual state ρ_l, the expectation values of operators appearing in Eq. (17).

A lower bound on the fidelity can be obtained in this case by defining the operator $\mathcal{S}_{G_S} = \frac{1}{2}[(\Sigma_{i=1}^{L}\hat{g}_i) - (L-2)\mathbb{1}]$. Then,

$$\mathcal{S}_{G_S}|g_1,\ldots,g_L\rangle = e_{g_1,\ldots,g_L}|g_1,\ldots,g_L\rangle,\ g_i = \pm 1, \tag{18}$$

with $e_{1,\ldots,1}=1$ and $e_{g_1,\ldots,g_L} \leqslant 0$ otherwise. Following the same procedure used for rotational-invariant states, we arrive at the inequality

$$\mathcal{F}^2(\rho_l,\rho_\psi) \geqslant \langle\mathcal{S}_{G_S}\rangle_{\rho_l}, \tag{19}$$

which can be efficiently estimated by measuring the expectation values $\langle\hat{g}i\rangle_{\rho_l}\forall i \in [1,L]$.

As an example we consider the the Bell state $|\mathrm{Bell}\rangle = \frac{1}{\sqrt{2}}[|0_1 1_2\rangle - |1_1 0_2\rangle]$. For this state, the stabilizer group is defined by the generators $G_S \equiv (-\sigma_z^1\sigma_z^2, -\sigma_x^1\sigma_x^2)$. Then, $L=2$ and $\mathcal{S}_{G_S}=\frac{1}{2}[-\sigma_z^1\sigma_z^2-\sigma_x^1\sigma_x^2]$. Another example is the set of maximally entangled N-qubit states $|\mathrm{GHZ}\rangle_N=\frac{1}{\sqrt{2}}[|0_1 0_2\cdots 0_N\rangle + |1_1 1_2\cdots 1_N\rangle]$. For these states, the generators of the corresponding stabilizer group are given by $G_S\equiv(\sigma_x^1\sigma_x^2\cdots\sigma_x^N, \sigma_z^1\sigma_z^2, \sigma_z^2\sigma_z^3, \ldots, \sigma_z^{N-1}\sigma_z^N)$, as pointed out in Sec. I. For $N=3$, we have $L=3$, and $\mathcal{S}_{G_S}=\frac{1}{2}[\sigma_x^1\sigma_x^2\sigma_x^3+\sigma_z^1\sigma_z^2+\sigma_z^2\sigma_z^3-\mathbb{1}]$. Such Schrödinger cat states can be used for precision spectroscopy [8,14] and angle or displacement measurements [23] beyond the standard quantum limit. These Heisenberg-limited techniques can be used to obtain increased experimental sensitivity by utilizing the N-fold enhancement in phase sensitivity of cat states relative to product states.

For an arbitrary N-qubit pure state $|\psi\rangle = V|0_1,\ldots,0_N\rangle$, with V unitary, the corresponding stabilizer group is given by the operators $\tilde{\sigma}_z^j = V\sigma_z^j V^\dagger$; that is, $\tilde{\sigma}_z^j|\psi\rangle=+1|\psi\rangle$. To obtain a lower bound on the fidelity of preparation of $|\psi\rangle$ it suffices then to measure the expectation values $\langle\tilde{\sigma}_z^j\rangle_{\rho_l}$. However, these arbitrary symmetries will be, in the most general case, an exponentially large linear combination of products of Pauli operators. Therefore, if the stabilizer group does not take a simple form as in Eq. (15), the efficiency of estimating a lower bound on the fidelity can be lost.

C. Generalized coherent states

The last class of states we consider is the class of generalized coherent states (GCSs) [24]. This class is a generalization of the well-known class of bosonic coherent states to the case of finite dimensional Hilbert spaces, and, in particular, to N-qubit systems. As coherent states, GCSs possess many interesting properties. First, they are minimum uncertainty states with respect to a preferred set of observables. Second, the expectation values of the observables in this preferred set uniquely define the GCS, and they can be considered as the *generalized unentangled* states with respect to this set [25]. They are constructed by the action of a displacement operator (i.e., a certain group unitary operation) to a reference state such as $|0_1\cdots 0_N\rangle$. If the displacement operator can be related to a time-evolution operator, GCSs are then the states prepared during a quantum simulation. Below, we explain this in more detail and show that, when the set of generators of the time evolution operator is low in dimension, many interesting properties of the corresponding GCSs can be efficiently obtained.

For a semisimple, compact, M-dimensional Lie algebra $\mathfrak{h}=\{\hat{Q}_1,\hat{Q}_2,\ldots,\hat{Q}_M\}$, with $\hat{Q}_j=(\hat{Q}_j)^\dagger$ the N-qubit operators acting on the 2^N dimensional Hilbert space $\mathcal{H}$, the GCSs are defined via

$$|\mathrm{GCS}\rangle \equiv e^{i\mathfrak{h}}|\mathrm{hw}\rangle. \tag{20}$$

Here, $e^{i\mathfrak{h}}$ denotes a unitary group operation (specifically, a displacement) induced by $\mathfrak{h}$: $e^{i\mathfrak{h}}\equiv\exp[i(\Sigma_j\lambda_j\hat{Q}_j)]$, $\lambda_j\in\mathbb{R}$. The state $|\mathrm{hw}\rangle$ is the highest-weight state of $\mathfrak{h}$. To define it, one needs to assume a Cartan-Weyl decomposition $\mathfrak{h}=\mathfrak{h}_D\oplus\mathfrak{h}^+\oplus\mathfrak{h}^-$ [26,27]. The set $\mathfrak{h}_D=\{\hat{h}_1,\ldots,\hat{h}_r\}$ is the Cartan subalgebra of $\mathfrak{h}$ constructed from the largest set of commuting operators (observables) in $\mathfrak{h}$. The weight states $|\phi_i\rangle$, which form a basis of states for $\mathcal{H}$, are the eigenstates of $\mathfrak{h}_D$:

$$\hat{h}_k|\phi_i\rangle = u_k^i|\phi_i\rangle, \quad k\in[1,r], \quad i\in[0,2^N-1]. \tag{21}$$

The sets $\mathfrak{h}^+=\{\hat{e}_{\alpha_1}^+,\ldots,\hat{e}_{\alpha_l}^+\}$ and $\mathfrak{h}^-=\{\hat{e}_{\alpha_1}^-,\ldots,\hat{e}_{\alpha_l}^-\}$ are built from raising and lowering operators ($\hat{e}_{\alpha_j}^+=\hat{e}_{\alpha_j}^{-\dagger}$), and either map weight states into orthogonal weight states or annihilate them. (The subscripts $\alpha_j\in\mathbb{R}^r$ are the roots of $\mathfrak{h}$ and are considered to be positive.) Then, $|\mathrm{hw}\rangle$ is defined by

$$\hat{h}_k|\mathrm{hw}\rangle = v_k|\mathrm{hw}\rangle, \quad k\in[1,r], \tag{22}$$

$$\hat{\mathbf{e}}_{\alpha_j}^+|\mathrm{hw}\rangle = 0, \quad j\in[1,l], \tag{23}$$

with $v_k=u_k^0$ (i.e., we have assumed $|\mathrm{hw}\rangle\equiv|\phi_0\rangle$). Note that $M=r+2l$. In many cases, $|\mathrm{hw}\rangle=|0_1 0_2\ldots 0_N\rangle$, where $|0_i\rangle$ represents an eigenstate of σ_z^i.

As shown in Refs. [18,19,25], when the dimension of $\mathfrak{h}$ satisfies $M\leqslant\mathrm{poly}(N)$, the corresponding GCSs play a decisive role in the theory of entanglement and quantum and classical simulations of many-body systems. An example is given by the GCSs defined via

$$|\psi_I(t)\rangle = e^{-iH_I t}|0_1 0_2\cdots 0_N\rangle, \tag{24}$$

where H_I is the Hamiltonian corresponding to the exactly solvable one-dimensional anisotropic Ising model in a transverse magnetic field and periodic boundary conditions

$$H_I = \sum_{j=1}^N [\gamma_x\sigma_x^j\sigma_x^{j+1} + \gamma_y\sigma_y^j\sigma_y^{j+1} + B\sigma_z^j]. \tag{25}$$

In Sec. III we will discuss this system in more detail.

Any GCS is uniquely determined (up to a global phase) by the expectation values of the operators in $\mathfrak{h}$. The state $|\mathrm{hw}(t)\rangle=e^{-iHt}|\mathrm{hw}\rangle$, with $H\in\mathfrak{h}$, is the highest-weight state of $\mathfrak{h}$ in a rotated Cartan-Weyl basis, and satisfies

$$\hat{h}_k(t)|\mathrm{hw}(t)\rangle = v_k|\mathrm{hw}(t)\rangle, \quad k\in[1,r], \tag{26}$$

where $\hat{h}_k(t)=e^{-iHt}\hat{h}_k e^{iHt}=\hat{h}_k+i[\hat{h}_k,H]+\cdots\in\mathfrak{h}$. Thus,

$$\rho_{\mathrm{hw}}(t) = |\mathrm{hw}(t)\rangle\langle\mathrm{hw}(t)| = \kappa^{-1}\prod_{k,i\neq 0}[\hat{h}_k(t)-u_k^i\mathbb{1}], \tag{27}$$

where $\kappa=\Pi_{k,i\neq 0}(v_k-u_k^i)$ is a constant for normalization purposes. For a particular value of t, the operators $\hat{h}_k(t)=\Sigma_{j=1}^M\lambda_j(t)\hat{Q}_j$ can be obtained on a classical computer [i.e., the coefficients $\lambda_j(t)$] in time polynomial in M (see theorem 1 in Ref. [19]). To see this, note first that $\lambda_j(t)\propto\mathrm{Tr}[\hat{h}_k(t)\hat{Q}_j]$. Such a trace can be efficiently evaluated by working in the $(M\times M)$-dimensional matrix representation (or any other faithful representation) of $\mathfrak{h}$ rather than working in the $(2^N\times 2^N)$-dimensional original representation. Therefore, the fidelity of having prepared $|\mathrm{hw}(t)\rangle$ can be obtained by measuring, over the actual prepared state ρ_l, the expectation values of the observables appearing in Eq. (27).

In analogy to the previously discussed cases, a lower bound for the fidelity can be obtained by defining the operator $\mathcal{S}_{\mathfrak{h}_D}(t)=\{-\varepsilon[\Sigma_k\hat{h}_k(t)-v_k\mathbb{1}]^2\}+\mathbb{1}$, with $\varepsilon>0$ a constant determined by the spacing between the eigenvalues u_k^i (see below). If $u_k^i<v_k\,\forall\, i\in[1,2^N-1]$, it is more simple to consider $\mathcal{S}_{\mathfrak{h}_D}(t)=[-\varepsilon(\Sigma_k\hat{h}_k(t)-v_k\mathbb{1})]+\mathbb{1}$. Then,

$$\mathcal{S}_{\mathfrak{h}_D}(t)|\phi_i(t)\rangle = w_i|\phi_i(t)\rangle, \tag{28}$$

where $|\phi_i(t)\rangle=e^{-iHt}|\phi_i\rangle$ are the weight states in the rotated Cartan-Weyl basis [e.g., $|\text{hw}(t)\rangle\equiv|\phi_0(t)\rangle$], $w_i\in\mathbb{R}$, and $w_0=1$. Thus, ε is chosen such that $w_i=[-\varepsilon(\Sigma_k u_k^i-v_k)^2+1]$, when $\mathcal{S}_{\mathfrak{h}_D}(t)=\{-\varepsilon[\Sigma_k\hat{h}_k(t)-v_k\mathbb{1}]^2\}+\mathbb{1}$, or $w_i=[-\varepsilon(\Sigma_k u_k^i-v_k)+1]$, when $\mathcal{S}_{\mathfrak{h}_D}(t)=\{-\varepsilon[\Sigma_k\hat{h}_k(t)-v_k\mathbb{1}]\}+\mathbb{1}$, satisfies

$$w_i\leqslant 0\ \forall\, i\neq 0. \tag{29}$$

Then, for any t, we obtain

$$\mathcal{F}^2_{\rho_l,\rho_{\text{hw}(t)}}\geqslant\langle\mathcal{S}_{h_D}(t)\rangle_{\rho_l}. \tag{30}$$

This lower bound can be obtained experimentally by measuring the expectation values of the operators $\hat{h}_k(t)\hat{h}_{k'}(t)$ and (or) $\hat{h}_k(t)$, which are directly induced from the expectation values $\langle\hat{Q}_j\rangle_{\rho_l}$ and $\langle\hat{Q}_j\hat{Q}_{j'}\rangle_{\rho_l}\forall\, j,j'\in[1,M]$ (assumed to be measurable with our quantum device). If $M=\text{poly}(N)$ (e.g., an evolution due to the Ising Hamiltonian H_I), Eq. (30) can be efficiently estimated with $\mathcal{O}[\text{poly}(N)]$ measurements.

III. QUANTUM SIMULATIONS WITH TWO TRAPPED IONS

In this section we use some of the results obtained in Sec. II C to estimate the fidelity of evolving two trapped-ion qubits with the Ising-like interaction

$$H_I=J\sigma_x^1\sigma_x^2+B(\sigma_z^1+\sigma_z^2), \tag{31}$$

where J is the spin-spin coupling and B is a transverse magnetic field. Here, each qubit is described by two of the electronic levels of each trapped ion. We model the system of two identical ions confined in a linear Paul trap and interacting with resonant and nonresonant laser fields as described in Ref. [7]. Below, we estimate the reliability of having prepared the state $|\psi(t)\rangle=|\text{hw}(t)\rangle=e^{-iH_It}|0_10_2\rangle$ (for a particular t).

In this case, the interaction Hamiltonian for the ions in the trap is given by

$$H_{\text{trap}}=H_{\text{phonon}}+H_{l\text{-ion 1}}+H_{l\text{-ion 2}}+H_m, \tag{32}$$

$$H_{\text{phonon}}=\omega_{\text{c.m.}}a^\dagger_{\text{c.m.}}a_{\text{c.m.}}+\omega_{\text{br}}a^\dagger_{\text{br}}a_{\text{br}},$$

$$H_{l\text{-ion 1}}=-[\eta_{\text{c.m.}}\omega_{\text{c.m.}}(a^\dagger_{\text{c.m.}}+a_{\text{c.m.}})+\eta_{\text{br}}\omega_{\text{br}}(a^\dagger_{\text{br}}+a_{\text{br}})]\sigma_x^1,$$

$$H_{l\text{-ion 2}}=-[\eta_{\text{c.m.}}\omega_{\text{c.m.}}(a^\dagger_{\text{c.m.}}+a_{\text{c.m.}})-\eta_{\text{br}}\omega_{\text{br}}(a^\dagger_{\text{br}}+a_{\text{br}})]\sigma_x^2,$$

$$H_m=B(\sigma_z^1+\sigma_z^2).$$

Here, the operators $a^\dagger_{\text{c.m.}}$ ($a_{\text{c.m.}}$) and $a^\dagger_{\text{br}}$ (a_{br}) create (annihilate) an excitation in the center of mass and breathing modes, respectively. The coupling interactions $H_{l\text{-ion1}}$ and $H_{l\text{-ion2}}$ are due to the action of state-dependent dipole forces, which are generated by the interaction of nonresonant laser beams with the electronic levels of the ions (see Ref. [7]). H_m is due to the action of an effective magnetic field that can be external or generated by resonant laser beams. H_{phonon} is the energy of the normal modes with frequency $\omega_{\text{c.m.}}$ for the center-of-mass mode, and ω_{br} for the breathing mode. In the case of a single-well potential in one dimension, $\omega_{\text{br}}=\sqrt{3}\omega_{\text{c.m.}}$. The couplings (displacements) $\eta_{\text{c.m.}}$ and η_{br} are assumed to be small: $\eta_i\ll 1$. They depend on the intensity gradients of the laser beams and are given by

$$\eta_i=\frac{F}{\sqrt{2}\hbar\omega_i}\sqrt{\frac{\hbar}{2m\omega_i}}, \tag{33}$$

with $i=[\text{c.m.},\text{br}]$, F the dipole force acting on each ion, and m the mass of the ion.

For a fixed value of t, the actual two-qubit state prepared in the ion trap device is

$$\rho_l(t)=\text{Tr}_{\text{phonon}}[e^{-iH_{\text{trap}}t}\rho_{(\text{ion-phonon})}e^{iH_{\text{trap}}t}], \tag{34}$$

where we have traced out the vibrational modes. Here, the initial state is $\rho_{(\text{ion-phonon})}=|0_10_2\rangle\langle 0_10_2|\otimes\rho_{\text{phonon}}$, and $\rho_{\text{phonon}}\propto e^{-H_{\text{phonon}}/k_BT}$ is the density operator for the initial state of the phonons, with the ion motion in a thermal distribution corresponding to temperature T (k_B is the Boltzmann constant). The fidelity of having prepared the state $|\text{hw}(t)\rangle$ is then given by

$$\mathcal{F}^2[\rho_l(t),\rho_{\text{hw}}(t)]=\text{Tr}[\rho_l(t)\rho_{\text{hw}}(t)], \tag{35}$$

where the trace is over the internal degrees of freedom.

Following the results of Sec. II C, we first identify the set $\mathfrak{h}_D=\{\sigma_z^1,\sigma_z^2\}$ as the largest set of commuting observables in $\mathfrak{h}$ (i.e., the Cartan subalgebra). This subalgebra determines $|\text{hw}\rangle=|0_10_2\rangle$ according to Eq. (22). A bound on the fidelity of Eq. (35) can be obtained by using the time dependent symmetry operators

$$\tilde{\sigma}_z^j(t)=e^{-iH_It}\sigma_z^je^{iH_It}\quad(j=1,2), \tag{36}$$

to uniquely define the state $|\text{hw}(t)\rangle$ through the equations

$$\tilde{\sigma}_z^j(t)|\text{hw}(t)\rangle=+1|\text{hw}(t)\rangle. \tag{37}$$

Choosing $\varepsilon=1/2$ (see Sec. II) and considering that $v_1=v_2=1$, we obtain $\mathcal{S}_{\mathfrak{h}_D}(t)=\frac{1}{2}[\tilde{\sigma}_z^1(t)+\tilde{\sigma}_z^2(t)]$, which satisfies [Eq. (30)]

$$\mathcal{F}^2[\rho_l(t),\rho_{\text{hw}}(t)]\geqslant\langle\mathcal{S}_{h_D}(t)\rangle_{\rho_l(t)}. \tag{38}$$

The $\tilde{\sigma}_z^j(t)=(\sigma_z^j-it[H_I,\sigma_z^j]+\cdots)$ are linear combinations of operators belonging to the Lie algebra $\mathfrak{so}(4)=\{\sigma_z^1,\sigma_z^2,\sigma_x^1\sigma_x^2,\sigma_x^1\sigma_y^2,\sigma_y^1\sigma_x^2,\sigma_y^1\sigma_y^2\}$. To obtain the coefficients involved in these combinations one needs to find the trace between the corresponding operators. For example, to obtain the coefficient $\lambda_1(t)$ that accompanies the operator σ_z^1 in the decomposition of $\tilde{\sigma}_z^1(t)$, one needs to compute $1/4\,\text{Tr}[\sigma_z^1\tilde{\sigma}_z^1(t)]$. Remarkably, such a trace can be efficiently computed by working in the $(2N\times 2N)$-dimensional fundamental matrix representation of $\mathfrak{so}(2N)$ rather than in the

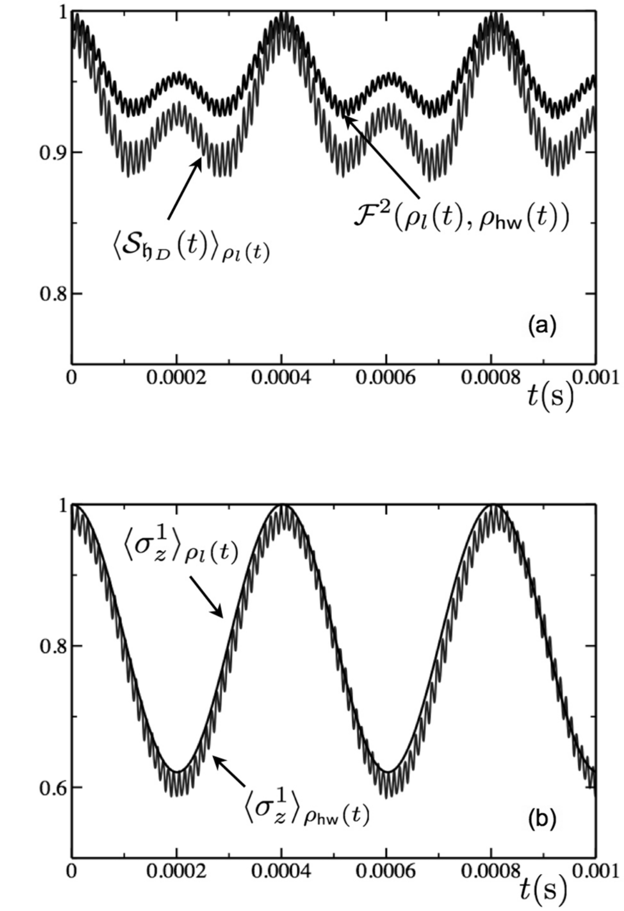

FIG. 1. Numerical simulation of the quantum evolution of two trapped ions interacting with laser fields. The parameters used are $\omega_{\text{c.m.}}=2\pi$ 100 kHz, $\eta_{\text{c.m.}}\approx 0.063$, $B=2\pi$ 560 Hz, $-J=2\pi 540$ Hz, $F=25\times 10^{-23}$ N, and $T=0$, and these are expected to be attained experimentally. (a) Squared fidelity (probability) of having prepared the state $|\text{hw}(t)\rangle = e^{-iH_I t}|0_1 0_2\rangle$, if the dynamics of the trapped ions are dominated by the trap Hamiltonian H_{trap} [Eq. (32)], and the corresponding lower bound $\langle \mathcal{S}_{\mathfrak{h}_D}(t)\rangle \rho_{l(t)}$, as given by Eq. (38), as a function of time. (b) Expectation values of the Pauli operator σ_z^1 as a function of time, if the evolution is governed by H_I and H_{trap}, respectively.

$(2^N \times 2^N)$-dimensional original representation (see Ref. [19] for details).

In brief, only six correlations [i.e., the elements of $\mathfrak{so}(4)$] need to be measured to evaluate the inequality of Eq. (38). The complexity of estimating the fidelity is then reduced since a naive approach to fidelity estimation would involve the measurement of fifteen correlations [i.e., the elements of the algebra $\mathfrak{su}(4)$]. Of course, the complexity of the problem is slightly reduced in this case but the difference is much greater for larger systems.

In Fig. 1 we plot $\mathcal{F}^2[\rho_l(t),\rho_{\mathfrak{h}w}(t)]$ [Eq. (35)] as a function of time and for certain values of F, ω_i, and B that could be attained experimentally. For these parameters the fidelity remains close to one, implying that the ion trap device can be used to perform a quantum simulation governed by the Ising-like Hamiltonian of Eq. (31). We also plot $\langle \mathcal{S}_{\mathfrak{h}_D}(t)\rangle \rho_{l(t)}$ and we observe that this lower bound on the (squared) fidelity is an excellent indicator of the accuracy of the simulation. For the sake of comparison, we also plot the expectation values $\langle \sigma_z^1\rangle \rho_{\text{hw}(t)}$ and $\langle \sigma_z^1\rangle \rho_{l(t)}$. Finally, in Fig. 2 we plot the coefficients $\lambda_j(t)$, $j\in[1,6]$, that determine the weighting of the six correlation measurements that contribute to the estimate of $\langle \mathcal{S}_{\mathfrak{h}_D}(t)\rangle \rho_{l(t)}$.

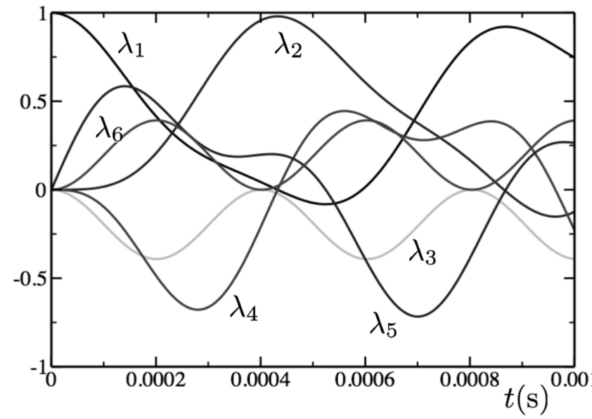

FIG. 2. Coefficients $\lambda_j(t)$, where $\tilde{\sigma}_z^1(t)=\lambda_1^1(t)\sigma_z^1+\lambda_1^2(t)\sigma_z^2+\lambda_1^3(t)\sigma_x^1\sigma_x^2+\lambda_1^4(t)\sigma_x^1\sigma_y^1+\lambda_1^5(t)\sigma_y^1\sigma_x^2+\lambda_1^6(t)\sigma_y^1\sigma_y^2\in\mathfrak{so}(4)$, used to obtain $\langle \mathcal{S}_{\mathfrak{h}_D}\rangle \rho_l(t)$ in Fig. 1. Note that, because of the symmetry under ion permutation, the same coefficients are obtained in the decomposition of $\tilde{\sigma}_z^2(t)$.

IV. STATISTICAL CONTRIBUTIONS TO MEASURED LOWER BOUND ON THE FIDELITY

In an actual experiment, expectation values can never be obtained exactly due to quantum projection noise. Thus, they must be estimated after a (typically large) sequence of projective measurements performed on identically prepared copies of the system. Commonly, maximum-likelihood methods (MLMs) [28,29] are used to estimate the most probable density matrix $\bar{\rho}_l$ from these measurements. As with full QST, these methods are usually inefficient, and they require input data concerning every correlation in the system. For example, if a MLM is used to estimate the density operator ρ_l of an N-qubit system, the estimation $\bar{\Sigma}_{\rho_l}$ of the expectation value of a particular operator $\Sigma=\sigma_{\alpha_1}^1\cdots\sigma_{\alpha_N}^N$ will require $\mathcal{O}((4^N-1)X)$ identically prepared copies of ρ_l, where X is the number of copies used to measure a particular correlation (product of Pauli operators) [30]. Such a complexity would then be translated to the estimation of the lower bounds of Eqs. (13), (19), and (30). In this section we argue that the exponential complexity can still be avoided when estimating these lower bounds with a certain (fixed) level of confidence.

For this purpose, we use results regarding the binomial distribution [31]. Observe that the operator Σ, as defined above, has ± 1 as possible eigenvalues. Then if we perform projective measurements of Σ over X identical copies of ρ_l, we obtain

$$\langle \Sigma\rangle_{\rho_l}=\bar{\Sigma}_{\rho_l}\pm\delta, \tag{39}$$

where $\bar{\Sigma}_{\rho_l}=\frac{X_+-X_-}{X}$ is the estimated expectation value (i.e., $X_\pm$ is the number of times we measured $\Sigma=\pm 1$, respectively), and δ is the corresponding standard deviation. The latter is given by

$$\delta = 2\sqrt{\frac{p_+ p_-}{X}}, \tag{40}$$

where $p_\pm$ are the (unknown) probabilities of measuring $\Sigma = \pm 1$, respectively. Then $\delta \leqslant \sqrt{1/X}$.

For sufficiently large X, the binomial distribution can be well-approximated by the normal distribution. In this context, Eq. (39) guarantees that $\bar{\Sigma}_{\rho_l}$ differs by at most $\sqrt{1/X}$ from the actual expectation value with (at least) 68% confidence [32]. For example, if Σ is estimated from ten thousand identical copies of ρ_l, then $\langle \Sigma \rangle_{\rho_l} = \bar{\Sigma}_{\rho_l} \pm 0.01$ with (at least) 68% confidence.

With no loss of generality, the bounds of Eqs. (13), (19), and (30) can be rewritten as

$$\mathcal{F}^2 \geqslant a_0 + \sum_{m=1}^{R} a_m \langle \Sigma^m \rangle_{\rho_l}, \quad a_0, a_m \in \mathbb{R}, \tag{41}$$

where each Σ^m involves a particular product of Pauli operators [$R = \text{poly}(N)$]. If each $\langle \Sigma^m \rangle_{\rho_l}$ is estimated from X identical copies of ρ_l, then $\langle \Sigma^m \rangle_{\rho_l} = \bar{\Sigma}^m_{\rho_l} \pm \sqrt{1/X}$ with 68% confidence, and

$$\mathcal{F}^2 \geqslant a_0 + \sum_{m=1}^{R} a_m \langle \Sigma^m \rangle_{\rho_l} \geqslant a_0 + \sum_{m=1}^{R} a_m \bar{\Sigma}^m_{\rho_l} - R/\sqrt{X}, \tag{42}$$

with the same confidence. Of course, Eq. (42) provides relevant information if $\bar{\Sigma}^m_{\rho_l} \geqslant 1/\sqrt{X}$. For example, if one is interested in preparing the state $|\text{GHZ}_N\rangle$, then $R = N$ and $\bar{\Sigma}^m_{\rho_l} \approx +1$. Choosing $X = 10^4 N^2$, a good estimation (with error 0.01) for the lower bound of the fidelity may be obtained. The method is then efficient: lower bounds on fidelity of state preparation can be obtained, with certain confidence, in poly(N) identical preparations of ρ_l.

We have not considered any source of error other than the one given by the statistics of projective measurements in the quantum world. Otherwise, the results obtained in the previous sections must be modified according to the specific sources of error or decoherence that can affect the state preparation.

V. CONCLUSIONS

We have studied the fidelity of state preparation for three different classes of states: the rotational-invariant states, stabilizer states, and generalized coherent states. Many interesting multipartite entangled states, such as Schrödinger cat or W-type states, belong to these classes. In particular, generalized coherent states are natural in the framework of quantum simulations. We have discussed the quantum simulation of the two-qubit Ising model using an ion trap device. In this case we observe that a lower bound of the fidelity of the simulation can be simply obtained and accurately estimates the reliability of the experiment. Such a bound can also be efficiently estimated for other multiple-qubit systems having Ising-like interactions. Similar approaches can be considered to study the fidelity of state preparation in general qudit or fermionic systems.

Our results provide an efficient method to estimate, with certain confidence, lower bounds on the fidelity of state preparation based on symmetries. Many of the states described contain N-particle entanglement, so the lower bounds can also be used to verify entanglement using entanglement witnesses [33,34]. These bounds are most accurate when the actual prepared state is not too far from the desired one, as in Fig. 1. Therefore, a consequence of our results is that instead of measuring every possible quantum correlation of a system a large number of times (as for QST), one should focus on having good estimations of certain relevant expectation values.

Note added. Recently, after this manuscript was submitted, we were alerted to the presence of some previous work that is relevant for a subset of the entangled states considered here. Efficient methods for lower bounds on the fidelity of GHZ-type state and Bell states have been pointed out before [35,36] in the entanglement witness formalism. However, the present work is more general in terms of a large class of states particularly useful for large-scale quantum information processing and quantum simulations, and the present approach is a complimentary one in terms of the general symmetries of certain types of quantum states.

ACKNOWLEDGMENTS

R.S. is grateful to the QiSci at the University of Queensland, G. Vidal, J. Harrington, F.M. Cucchietti, S. Boixo, and M. Boshier for discussions. This work has been supported by LANL Laboratory Directed Research and Development (LDRD).

[1] M. A. Nielsen, and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
[2] T. Schaetz, *et al.*, Phys. Rev. Lett. **94**, 010501 (2005).
[3] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[4] S. Lloyd, Science **273**, 1073 (1996).
[5] G. Ortiz, J. E. Gubernatis, E. Knill, and R. Laflamme, Phys. Rev. A **64**, 022319 (2001).
[6] R. Somma, G. Ortiz, J. E. Gubernatis, E. Knill, and R. Laflamme, Phys. Rev. A **65**, 042323 (2002).
[7] D. Porras and J. I. Cirac, Phys. Rev. Lett. **92**, 207901 (2004).
[8] D. Leibfried *et al.*, Nature (London) **438**, 639 (2005).
[9] H. Häffner *et al.*, Nature (London) **438**, 643 (2005).
[10] R. T. Thew, K. Nemoto, A. G. White, and W. J. Munro, Phys. Rev. A **66**, 012303 (2002).

[11] D. F. V. James, P. G. Kwiat, W. J. Munro, and A. G. White, Phys. Rev. A **64**, 052312 (2001).
[12] W. M. Itano *et al.*, Phys. Rev. A **47**, 3554 (1993).
[13] C. A. Sackett *et al.*, Nature (London) **404**, 256 (2000).
[14] D. Leibfried *et al.*, Science **304**, 1476 (2004).
[15] Ion trap devices allow us to obtain many-qubit correlations from single qubit (von Neumann) projective measurements in the corresponding basis.
[16] H. Breuer, J. Phys. A **38**, 9019 (2005). K. Manne and C. Caves, quant-ph/0506151.
[17] D. Gottesman, Ph. D. thesis, California Institute of Technology, Pasadena, California, 1997.
[18] R. Somma, G. Ortiz, H. Barnum, E. Knill, and L. Viola, Phys. Rev. A **70**, 042311 (2004).
[19] R. Somma, H. Barnum, G. Ortiz, and E. Knill, quant-ph/0601030.
[20] J. Joo, Y. Park, S. Oh, and J. Kim, New J. Phys. **5**, 136 (2003).
[21] J. Joo, J. Lee, J. Jang, and Y. Park, J. Korean Phys. Soc. **46**, 763 (2005).
[22] In this framework, it will also be allowed to have stabilizers that are polynomially large (with respect to N) linear combinations of products of Pauli operators.
[23] F. Toscano, D. A. R. Dalvit, L. Davidovich, and W. H. Zurek, Phys. Rev. A **73**, 023803 (2006).
[24] W. M. Zhang, D. H. Feng, and R. Gilmore, Rev. Mod. Phys. **62**, 867 (1990).
[25] H. Barnum, E. Knill, G. Ortiz, and L. Viola, Phys. Rev. A **68**, 032308 (2003).
[26] J. Fuchs, *Affine Lie Algebras and Quantum Groups* (Cambridge University Press, Cambridge, 1992).
[27] J. F. Cornwell, *Group Theory in Physics* (Academic Press, London, 1989).
[28] Z. Hradil, Phys. Rev. A **55**, R1561 (1997).
[29] K. Banaszek, G. M. D'Ariano, M. G. A. Paris, and M. F. Sacchi, Phys. Rev. A **61**, 010304(R) (1999).
[30] It is $\mathcal{O}(3^N X)$ experiments for an ion trap device.
[31] For example, J. R. Taylor, *An Introduction to Error Analysis* (University Science Books, Sausalito, California, 1997).
[32] If X is not large enough, one can use the Chernoff bound to estimate the confidence.
[33] M. Lewenstein, B. Kraus, J. I. Cirac, and P. Horodecki, Phys. Rev. A **62**, 052310 (2000).
[34] M. Bourennane *et al.*, Phys. Rev. Lett. **92**, 087902 (2004).
[35] O. Gühne, P. Hyllus, D. Bruβ, A. Eckert, M. Lewenstein, C. Macchiavello, A. Sanpera, Phys. Rev. A **66**, 062305 (2002).
[36] G. Tòth and O. Gühne, Phys. Rev. Lett. **94**, 060501 (2005).