Restoring broken symmetries using oracles

Edgar Andres Ruiz Guzman† and Denis Lacroix‡
Université Paris-Saclay, CNRS/IN2P3, IJCLab, 91405 Orsay, France
(Dated: October 21, 2022)

We present a new method to perform variation after projection in many-body systems on quantum computers that does not require performing explicit projection. The technique employs the notion of “oracle”, generally used in quantum search algorithms. We show how to construct the oracle and the projector associated with a symmetry operator. The procedure is illustrated for the parity, particle number, and total spin symmetries. The oracle is used to restore symmetry by indirect measurements using a single ancillary qubit. An illustration of the technique is made to obtain the approximate ground state energy for the pairing model Hamiltonian.

I. INTRODUCTION

Quantum computers promise to speed up the computation of some selected problems that are hard to solve on classical computers [1,2]. One of the opportunities offered by quantum technologies is the simulation of many-body quantum systems with a large number of particles, where the exponential scaling of their Hilbert space prevents their ab-initio description in classical computers as the number of degrees of freedom increases. Assuming we can describe the physical system accurately in the quantum computer, multiple methods have been designed to estimate the ground state energy of a Hamiltonian, e.g., [3–8]. We are now in the Noisy intermediate-scale quantum (NISQ) computers era [9,10]: in this period, the algorithms should be tailor-made to handle a limited number of gates and qubits and the presence of noise. The variational quantum eigensolver (VQE) [3–8] is one of the currently used best candidates to fill the requirements listed above due (i) to its comparatively short coherence time and (ii) to the possibility of customizing the ansatz to the physical problem at hand.

Because of the inherent noise of current quantum processors, the symmetry that a wave function should respect when solving a physical problem will most likely be broken accidentally. A possible way to control the errors is eventually to enforce the symmetry with specific algorithms [12–14,16–19]. In some cases, like when a system encounters a spontaneous symmetry breaking, it can also be helpful to break some symmetries on purpose [20,21]. In both cases, wanted or unwanted symmetry-breaking (SB), specific methods should be designed to restore the symmetry (SR) in quantum computations. In the many-body context, this avenue has been recently explored, requiring [22] or not [23] the explicit construction of the symmetry projected wave function. The method proposed in [23] applies to any symmetries, including spin projection problems [24]. The symmetry projection was used in addition to classical optimization post-processing calculations in Refs. [25,26] to obtain ground state and excited states in many-body systems. In particular, in [26], the equivalent to the Variation-After-Projection, called Q-VAP, has been applied to superfluid systems. This method is based on the Quantum-Phase-Estimation (QPE) algorithm, using the indirect measurements of a set of ancillary qubits with a large set of quantum operations to perform in the circuit. This resource demand limited us to only testing the method on quantum emulators, which will probably be usable on quantum platforms after the NISQ period. Alternative methods to restore symmetries, eventually with lower circuit depths and lengths, have been discussed recently in Refs. [30,31].

One of the promising methods evoked in Ref. [31] is those based on oracles. Oracles are specific operators that have been introduced in quantum search algorithms. Among these algorithms, one can mention the Grover method [32,33] that has been recognized as optimal for specific query problems [34,35]. The practical use of oracles depends strongly on the difficulty of constructing them. We analyze how oracles can be implemented to restore symmetries in the Quantum-Variation After Projection (Q-VAP) method of Ref. [29].

The procedure reduces the cost of the indirect measurements compared to the QPE to that of a single qubit. It can also continuously monitor symmetry restoration during the variational optimization process. In particular, it can avoid explicitly projecting the variational state each time the energy is estimated. Illustrations of the oracle construction are given for the parity, particle number, and total spin symmetries. Applications are performed on the pairing model.

II. QUANTUM VARIATION-AFTER-PROJECTION WITH ORACLE

Similarly to the Variation-After-Projection (VAP) performed on a classical computer, in the Q-VAP approach, a symmetry-breaking state $|\Psi (\{\theta_i\})\rangle$ is considered where $\{\theta_i\}$ are a set of parameters that are varied to minimize
the energy:

$$E (\{\theta_i\}) = \frac{\langle \Psi (\{\theta_i\}) | \hat{H} \hat{P}_S | \Psi (\{\theta_i\}) \rangle}{\langle \Psi (\{\theta_i\}) | \hat{P}_S \Psi (\{\theta_i\}) \rangle}.$$  \hspace{1cm} (1)$$

Here, $\hat{H}$ denotes the Hamiltonian, and $\hat{P}_S$ is a projector onto the subspace $\mathcal{H}_S$, which respects a given set of symmetries of the Hamiltonian, denoted generically by $S$. In Eq. (1), we used the fact that $\hat{P}_S^2 = \hat{P}_S$ and $[\hat{H}, \hat{P}_S] = 0$.

The method proposed in Ref. [25] to perform symmetry restoration combines the QPE approach and takes advantage of the fact that the eigenvalues of symmetry operators are known. Although this method applies to any symmetry problem, one of its inconveniences is that it relies on two steps to estimate the energy in Eq. (1). In the first step, the SR state is obtained by projection, and in the second step, this projected state is used to compute the expectation value of $\hat{H}$. Possible ways to reduce the circuit to perform the projection have been discussed in Ref. [31]. Depending on the projection method, this can lead to quite significant coherence time requirements. In most of the techniques discussed in [31], the projection is achieved by indirect measurements of a set of ancillary qubits. Because of this, and possible small improvements in the number of operations to perform the projection, the first step often remains probabilistic. This implies that only part of the events and, depending on the unprojected state properties, a possibly significant fraction of the runs could be thrown away, leading to waste in the use of quantum platforms. An extreme situation would be where the SB state has a very small or zero fraction of states belonging to $\mathcal{H}_S$. Thus, the probability of the states with the correct symmetry is too low or zero in the parametric symmetry-breaking wave function. In that case, we could find ourselves in a situation where the projector rarely or never projects in the correct subspace. To address this issue, we explore below an alternative method where we can directly access the energy in Eq. (1) without performing the explicit projection.

A. Using oracle for symmetry restoration

An oracle [31–33], denoted hereafter by $\hat{O}$, is an operator able to classify the total Hilbert space $\mathcal{H}$ into two subspaces. In one subspace, states have a specific property we are interested in. These states are the Good states and correspond, in our case, to states that respect the symmetry $S$. The other states are Bad states and are the ones that do not respect the symmetry. They belong to the complementary subspace of $\mathcal{H}_S$, denoted hereafter by $\mathcal{H}_B$.

A second property of the oracle is that it acts differently on the good and bad states. In general, the action is relatively simple. Here, we assume that the oracle multiplies by the same phase $\varphi$ (resp. $\mu$) states that do (resp. do not) respect a symmetry, i.e.:

$$\hat{O} |\psi_k\rangle = \begin{cases} e^{i\varphi} |\psi_k\rangle & \text{if } |\psi_k\rangle \in \mathcal{H}_S, \\ e^{i\mu} |\psi_k\rangle & \text{if } |\psi_k\rangle \in \mathcal{H}_B. \end{cases}$$  \hspace{1cm} (2)$$

We consider below $\varphi \neq \mu$. Note that standard search algorithms usually assume $e^{i\varphi} = -1$ and $e^{i\mu} = +1$. Here, we define the oracle in a more general way because using phases different from the standard choice will be useful for certain calculations shown below. The states $\{|\psi_k\rangle\}$ correspond here to a complete general basis that spans the entire Hilbert space. Then, the oracle applied to a general wave function $|\Psi\rangle = \sum_k c_k |\psi_k\rangle$ gives:

$$\hat{O} |\Psi\rangle = e^{i\varphi} \sum_{\psi_k \in \mathcal{H}_S} c_k |\psi_k\rangle + e^{i\mu} \sum_{\psi_k \in \mathcal{H}_B} c_k |\psi_k\rangle.$$  \hspace{1cm} (3)$$

We have that $|\Psi\rangle = (|\Psi_G\rangle + |\Psi_B\rangle$ where $|\Psi_G\rangle$ (resp. $|\Psi_B\rangle$) corresponds to the projection of the state onto the good (resp. bad) subspace.

![FIG. 1: Hadamard test to get the expectation value of the operator $\hat{U}$ in a determined subspace defined by $\hat{O}$ (see text and Eq. (2)). $\hat{O}$ stands for the oracle operator. In this circuit, one ancillary qubit is used. The repeated measurements of 0 and 1 of the ancillary qubit give access to the real part (or to the imaginary part if a phase gate of phase $-\pi/2$ is added after the first Hadamard gate on the ancilla qubit) of the expectation value given by Eq. (4).](image)

We then perform a Hadamard test using a generic operator $\hat{U}$ and the oracle. The corresponding circuit is shown in Fig 1. The choice of the operator $\hat{U}$ is discussed below. The Hadamard test gives access to the following expectation value:

$$\langle \Psi | \hat{U} \hat{O} | \Psi \rangle = \left( \langle \Psi_G | + \langle \Psi_B | \right) \hat{U} \left( e^{i\varphi} \langle \Psi_G | + e^{i\mu} \langle \Psi_B | \right) ,$$

$$= e^{i\varphi} \left( \langle \Psi_G | \hat{U} | \Psi_G \rangle + \langle \Psi_B | \hat{U} | \Psi_G \rangle \right) + e^{i\mu} \left( \langle \Psi_G | \hat{U} | \Psi_B \rangle + \langle \Psi_B | \hat{U} | \Psi_B \rangle \right).$$  \hspace{1cm} (4)$$

This expression simplifies if $\hat{U}$ also preserves the symmetry $S$, so that we have $\hat{U} |\Psi_G\rangle \in \mathcal{H}_S$ and $\hat{U} |\Psi_B\rangle \in \mathcal{H}_S$. Accordingly, we deduce

$$\langle \Psi_B | \hat{U} | \Psi_G \rangle = \langle \Psi_G | \hat{U} | \Psi_B \rangle = 0.$$  \hspace{1cm} (5)$$

With the use of the Hadamard test, we can retrieve the real or imaginary part of the expectation value:

$$\langle \Psi | \hat{O} \hat{U} | \Psi \rangle = e^{i\varphi} \langle \Psi_G | \hat{U} | \Psi_G \rangle + e^{i\mu} \langle \Psi_B | \hat{U} | \Psi_B \rangle.$$  \hspace{1cm} (6)$$
An interesting situation is the case where \( \hat{U} \) is Hermitian and where we set \( \varphi = 0 \) and \( \mu = \pi/2 \). Then, the Hadamard test used for obtaining the real part gives the expectation value of the operator \( \hat{U} \) on the state of interest, i.e.,

\[
p_0 - p_1 = \langle \Psi_G | \hat{U} | \Psi_G \rangle.
\]

where \( p_0 \) (resp. \( p_1 \)) denotes the probability to measure 0 or 1 in the ancillary qubit. Therefore, we see that the method provides direct access to the expectation value of any operator \( \hat{U} \) taken on the “Good” state, i.e., symmetry restored part of the initial wave function.

An illustration of the use of Eq. (7) using the probability \( p_0 \) and \( p_1 \) with a limited set of measurements \( N_e \) is shown in Fig. 2. This figure illustrates that an approximate value of the left-hand side of Eq. (7) can be obtained even if a limited number of measurements is performed. An important aspect is that no event is rejected contrary to methods usually based on the iterative use of Hadamard tests (see for instance discussion in [31]).

![FIG. 2: Illustration of the use of an oracle to obtain \( \langle \Psi_G | \hat{U} | \Psi_G \rangle \) for the specific case \( \hat{U} = I \) and \( (\varphi, \mu) = (\pi/2) \) in which case the oracle gives the amplitude of the initial state belonging to \( \mathcal{H}_G \). The initial state is encoded here on 8 qubits, and it corresponds to the equiprobable state \( |\Psi\rangle = \frac{1}{\sqrt{2^N}} \sum_k |k\rangle \) where \( |k\rangle \) should be interpreted as the binary representation of the integer \( k \) encoded on the 8 register qubits. In this example, the “Good” states were defined as the states with four 1 in their binary representation. Suppose the initial state represents a many-body system encoded on the quantum register using the Jordan-Wigner fermion to qubit mapping [5] [38] [40]. Then, the projected state will correspond to a many-body system with exactly 4 particles while the initial state mixes all possible particle numbers. The green horizontal line is the exact value of \( \langle \Psi_G | \hat{U} | \Psi_G \rangle \), while the red dots correspond to the value \( p_0 - p_1 \) deduced from a set of \( N_e \) measurements. The error bars in blue shown in the figure are taken as \( 1/\sqrt{N_e} \). The oracle is constructed using the method discussed in section [31].

We also note in passing that the Eq. (6) is a rather simple trigonometric function of the angles \( (\varphi, \mu) \). It only depends on the two parameters \( \langle \Psi_G | \hat{U} | \Psi_G \rangle \) and \( \langle \Psi_B | \hat{U} | \Psi_B \rangle \). Therefore, we see that the knowledge of \( \langle \Psi | \hat{O} | \Psi \rangle \) given by Eq. (4) for few selected values of \( (\varphi, \pi) \) give access to the same expectation values for all values of these angles. For the case presented in Fig. 2 for \( \hat{U} = I \), a single pair of angles is sufficient since:

\[
\langle \Psi_G | \hat{O} | \Psi_G \rangle = \langle \Psi_B | \hat{O} | \Psi_B \rangle = 1.
\]

The corresponding function \( \text{Re}[\langle \Psi | \hat{O}(\varphi, \mu) | \Psi \rangle] \) is illustrated in Fig. 3 as well as few remarkable sets of angles.

![FIG. 3: Contour plot of the \( \text{Re}[\langle \Psi | \hat{O}(\varphi, \mu) | \Psi \rangle] \) quantities deduced from Eq. (4) as function of the angles \( \varphi \) and \( \mu \in [0, 2\pi] \) for the same initial state and oracle considered in Fig. 2. The symbols highlight specific angles: the angles used in Fig. 2 [red filled circles], the case \( (\varphi = \pi/2, \mu = 0) \) that leads to \( p_0 - p_1 = \langle \Phi_B | \Phi_B \rangle \) [blue filled square] and the standard prescription for the oracle generally used in Grover search algorithm, i.e. \( (\varphi = \pi, \mu = 0) \) [orange cross].

In addition to the advantage, compared to the method proposed in [25] [29], that the circuit depth is reduced by using a single ancillary qubit, we see that repeated measurements of this qubit will rapidly enable us to identify if the initial state has a significant amplitude belonging to the space \( \mathcal{H}_S \). In the opposite case, i.e., if \( p_0 \approx p_1 \), the initial state can be monitored to increase this amplitude variationally. Last, we mention that there are no wasted events in the approach, contrary to most of the methods discussed in [31].

Up to now, we have not discussed the operator \( \hat{U} \) itself. We will typically be interested in using \( \hat{U} = I \) or \( \hat{U} = \hat{H} \) for many-body systems. The former gives access to the norm of the state \( \langle \Psi_G | \hat{H} | \Psi_G \rangle \) while the latter provides the expectation value of the Hamiltonian over the “Good” space. The ratio of the two quantities gives the projected energy (1) for the symmetry-restored state.

Since \( \hat{H} \) is hermitian but not unitary, it might be helpful to use \( \hat{U}(t) = e^{-it\hat{H}} \) instead of \( \hat{H} \) itself. We can extract the energy using the generating function method discussed in details in Ref. [25], i.e.:

\[
\langle \Psi_G | \hat{H} | \Psi_G \rangle \equiv i \frac{dF_G(t)}{dt} |_{t=0},
\]
where \( F_G(t) = \langle \Psi_G | e^{-iHt} | \Psi_G \rangle \) is obtained using the oracle technique. Given that, in this case, we would be interested in the imaginary part of \( F_G(t) \), we can use a modified Hadamard test to get the imaginary part of the expected value (see Fig. 1 of ref. [28]). In practice, the first derivative of \( F_G(t) \) can be evaluated using a simple finite-difference method, in which case only short-time propagation (short circuit length) is required. Alternatively, to reduce the numerical noise of this derivative, one can use the parameter-shift rule technique [41, [42].

Each expectation value on the right-hand side can be separately obtained in a quantum computer, and the sum can be reconstructed on a classical computer. An illustration of this technique can be found in Ref. [29]. The possible advantages of using the LCU decomposition will be discussed below in more detail.

As underlined in Ref. [31], once we have a usable form for a projector, one can deduce a similar form for the oracle. The oracle operator, as defined in Eq (2), can be constructed from the projector as:

\[
\hat{O}_\alpha = e^{i\mu} \hat{I} + e^{i\varphi} \hat{P}_\alpha.
\]

Using Eq (9), we get:

\[
\hat{O}_\alpha = e^{i\mu} \hat{I} + (e^{i\varphi} - e^{i\mu}) \hat{P}_\alpha \equiv \sum_{k=0}^{M} \beta_k(\phi, \varphi)e^{i\phi_k S}.
\]

If an operator \( \hat{A} \) respects the symmetry, we can show that its expectation value on a projected normalized state verifies:

\[
\frac{\langle \hat{A} \hat{P}_\alpha \rangle}{\langle \hat{P}_\alpha \rangle} = \frac{\langle \hat{A} \hat{O}_\alpha \rangle - e^{i\mu} \langle \hat{A} \rangle}{\langle \hat{O}_\alpha \rangle - e^{i\mu}},
\]

where we used the compact notation \( \langle \Psi | . | \Psi \rangle = \langle . \rangle \) and assumed that the state \( | \Psi \rangle \) is normalized to 1. It is interesting to note that the above equality holds whatever is the retained value of \( \varphi \) and \( \mu \) provided that \( \varphi \neq \mu \). This flexibility could be used to reduce the numerical cost. We mention the special case where \( \hat{A} \) is a hermitian operator. In this case, we can set \( \varphi = 0 \) and \( \mu = \pi/2 \), and we would only need to compute the real part of \( \langle \hat{A} \hat{O}_\alpha \rangle \) and \( \langle \hat{O}_\alpha \rangle \).

### III. ORACLE CONSTRUCTION FOR SYMMETRY-RESTORATION

The approach presented above strongly relies on the possibility of efficiently constructing the oracle associated with the symmetry restoration problem. A SB problem’s specificity is that the eigenvalues of the symmetry operator \( S \) are usually known. We restrict the discussion here to the case where the eigenvalues are discrete.

Because the number of qubits \( n_q \) that describe the system is finite in practice, these eigenvalues are bound from below and above. We denote them by \( \lambda_1 < \cdots < \lambda_Q \) where \( \Omega \) depends on \( n_q \). In the following, we define the set of values \( \xi_\alpha = \lambda_\alpha - \lambda_1 \) and assume that we can write \( \xi_\alpha = \alpha \tau \lambda_1 \) where \( \alpha \) is a constant that depends on the symmetry considered and \( \{m_\alpha\}_{\alpha=1}^{\Omega} \) correspond to a set of positive integers in the interval \([0, M]\). The projector \( \hat{P}_\alpha \) that projects onto the subspace associated with the eigenvalue \( \lambda_\alpha \) can then be written as:

\[
\hat{P}_\alpha = \sum_{k=0}^{M} \alpha_k e^{i\phi_k S},
\]

with

\[
\begin{align*}
\alpha_k &= \frac{1}{M+1} e^{-i\phi_k (\xi_\alpha + \lambda_1)} \\
\phi_k &= \frac{2\pi k}{\alpha (M+1)}
\end{align*}
\]

and \( M = m_\Omega \). This generic form of a projector is particularly interesting for quantum computing since the non-unitary projector is written as a linear combination of unitary (LCU) operators. This form could be advantageously used to reduce the cost of performing expectation values of operators. For instance, an operator’s projected expectation value of an operator \( \hat{A} \) verifies:

\[
\langle \hat{A} \hat{P}_\alpha \rangle = \sum_k \alpha_k \langle \hat{A} e^{i\phi_k S} \rangle.
\]

### A. Example of projectors and oracle for selected symmetries

We consider here some example of common symmetries that are standardly respected by many-body Hamiltonians.

**Parity:** One of the simplest symmetries is the one associated with parity; its operator is denoted hereafter as \( \hat{\pi} \). We consider below a set of computational states \( | m \rangle \) with \( m = 0, 2^n s - 1 \) mapped to a qubit register with \( n_q \) qubits.

---

1 The proof can be made using simply the identity:

\[
\frac{1}{M+1} \sum_{k=0}^{M} e^{2i\pi \frac{2(m-n)}{(M+1)}} = \delta_{mn}
\]

that is correct provided that \( m, n \in [0, M] \).
such that $|m\rangle = |\delta_{x_{m-1}}, \ldots, \delta_0\rangle$ with $m = \sum_{i=0}^{n_q-1} \delta_i 2^i$. Such states are eigenstates of $\hat{\pi}$ with eigenvalues +1 (resp. −1) if the number of $\delta$’s equal to 1 is even (resp. odd).

For many-body Fermi systems, if one uses the Jordan-Wigner Transformation (JWT) to map the Fock space to the qubit space, the occupation probability of a particle in a particular state becomes equivalent to the probability of measuring the state |1⟩ in the corresponding qubit. Then the qubit parity identifies with the many-body state’s parity and separates the total Hilbert space into odd and even particle number subspaces. For the special case $(\varphi, \mu) = (0, \pi)$ in Eq. (2), the parity case is very peculiar because the parity operator is itself the oracle $\hat{O}_\pi = \hat{\pi}$. In the following, we use the notation $(X_m, Y_m, Z_m)$ for the Pauli matrices acting on the $m^{th}$ qubit. The parity operator can be written as $\hat{\pi} = \otimes_{m=0}^{n_q-1} Z_m$; this operator was used in [15] to mitigate the error in quantum computers, and a low-cost method, similar to Eq. (10) was proposed in Ref. [14] to get the parity projected densities. Denoting by $\varepsilon_\pi = \pm 1$ the eigenvalues of the parity operator, the projector is given by:

$$P_{\varepsilon_\pi} = \frac{1}{2} (I + \varepsilon_\pi \hat{\pi})$$

(17)

The generalized form of the oracle for the parity operator as given in Eq. (2) is:

$$O_{\varepsilon_\pi} = \frac{1}{2} (e^{i\varphi} + e^{i\mu}) I + \frac{1}{2} (e^{i\varphi} - e^{i\mu}) \varepsilon_\pi \hat{\pi}$$

(18)

**Particle number:** If we use again the JWT encoding for fermions, the particle number operator $\hat{N}$ is given by $\hat{N} = \sum_{m=0}^{n_q-1} (I - Z_m)/2$. States of the computational basis are again eigenstates of this operator with eigenvalues $N = 0, \ldots, n_q$ that correspond to the number of 1 in the binary representation of the states. Projection on particle number with the QPE approach was illustrated in ref. [25, 29]. For this operator, the decomposition for the projection $\hat{P}_A$ onto a given particle number $A$ is obtained by using $a = 1$, $\lambda_1 = 0$ and $m_a = A$, while $M$ should verify $M \geq n_q$ in Eq. (11). The different unitary operators entering in Eq. (9) can be implemented using the tensor decomposition [28]:

$$e^{i\phi_k \hat{N}} = \bigotimes_{m=0}^{n_q-1} \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi_k} \end{pmatrix}_m$$

(19)

where the set of $2 \times 2$ matrix on the right side corresponds to phase gates acting on the set of qubits.

**Total spin operator:** We now consider a slightly more complex situation where the qubit register corresponds to a set of spins. We use the same mapping from spins to qubits as in Ref. [27], and we consider $n_q$ spins encoded on a $n_q$ qubits register with the convention \{0,1\} with the convention \{0,1\} = {0 \uparrow, 1 \downarrow} \{0,\ldots, n_q - 1\}. The spin vector for the qubit $m$ is directly denoted as $\hat{S}_m = \frac{1}{2} (X_m, Y_m, Z_m)$. The QPE method was employed in [27] to project a state simultaneously onto a given value of the total spin and its $z$-component. Hereafter, we denote by $S(S+1)$ and $S_z$ the corresponding eigenvalues (note that here we use the convention $\hbar = 1$). As shown in Ref. [27], the projection on a given eigenstate of $\hat{S}_z$ is equivalent to the projection on particle $\hat{N}$ discussed above. Therefore, we only discuss the projection on eigenstates of $\hat{S}_z^2$. It is first helpful to write this operator as [53]:

$$\hat{S}_z^2 = n_q \left( \frac{4 - n_q}{4} \right) + \sum_{i<j} \hat{P}_{ij}$$

(20)

where $\hat{P}_{ij} = \frac{1}{2} (I_i I_j + X_i X_j + Y_i Y_j + Z_i Z_j)$ are the permutation operators that invert two qubits values, i.e. $\hat{P}_{ij} |\delta_i \delta_j\rangle = |\delta_j \delta_i\rangle$.

The case of $\hat{S}_z^2$ slightly differs from the particle number since this operator has non-equidistant eigenvalues $S(S+1)$. Its possible values depend on the number of qubits $n_q$; more precisely, we have:

- For even $n_q$, we have $S = 0, 1, \ldots, n_q/2$ leading to $S(S+1) = 0, 2, \ldots, n_q(n_q + 2)/4$; from which we deduce $\lambda_1 = 0$. Then to reduce the number of phase operators in Eq. (9) one can assume $a = 2$, so that $m_a = 0, 1, \ldots, k_q(k_q+2)/2$ with $k_q = n_q/2$.

- For odd $n_q$, we have $S = 1, \frac{3}{2}, \ldots, n_q/2$ leading to $\lambda_1 = \frac{1}{2}$ and $S(S+1) - \lambda_1 = 0, 3, 8, \ldots, k_q(k_q+2)$ with $n_q = 2k_q + 1$. Given this sequence, $a$ should be set to 1 and the possible values of $m_a$ directly identifies with those reported for $S(S+1) - \lambda_1$.

To implement the circuit associated with the different phase operators $e^{i\phi_k \hat{S}_z^2}$ we directly used here Eq. (20) together with the Trotter-Suzuki method [4] [55]. Technical aspects and related quantum circuits are given in appendix A. We note that for the total spin, we can also use the method of Ref. [36], where the discretization of the projector is written as an integral over spherical coordinate angles. The latter method gives an alternative approximate LCU decomposition of the total spin projector with the advantage of only needing one-body operators in each exponential term.

**B. Practical aspects for the oracle application**

In the above discussion, we have shown how the oracle can be used for restoring symmetries and how it can be decomposed systematically in the LCU form using Eq. (9). Here, we discuss in more detail how, starting from the LCU decomposition of oracles, they can be implemented on quantum computers. Two methods are presented, one that can be readily applied on NISQ platforms and the second based on the LCU algorithm [43].
1. Implementation of oracle on NISQ devices

One standard approach to reduce the numerical cost associated with an operator is to separate its expectation values into a set of independent evaluations requiring a lower cost. From Eq. (16), we see that the expectation value of an operator \( \hat{A} \) on the projected state can already be decomposed either directly as \((\hat{A}\hat{P}) = \sum_k \alpha_k \hat{A} e^{i\phi_k} \) and \((\hat{P}_\alpha) = \sum_k \alpha_k e^{i\phi_k} \hat{S}\) or into the expectation values of \( \langle \hat{A} \rangle, \langle \hat{O}_\alpha \hat{A} \rangle \); this illustrates that the projected state itself does not need to be explicitly constructed.

Provided that the operator \( \hat{A} \) can also be written as an LCU, we deduce:

\[
\langle \hat{A} \rangle = \sum_j \gamma_j \langle \hat{A}_j \rangle, \quad \langle \hat{O}_\alpha \hat{A} \rangle = \sum_{k,j} \beta_k \gamma_j \langle \hat{V}_k \hat{A}_j \rangle,
\]

where we used Eq. (14) with the notations \( \hat{V}_k = e^{i\phi_k} \hat{S} \) and \( \beta_k = \beta_k(\phi, \varphi) \). A standard pragmatic approach to reduce the cost of the evaluation of these expected values is to use a Hadamard test to evaluate each expectation among the set \{\( \langle \hat{A}_j \rangle, \langle \hat{V}_k \rangle, \langle \hat{V}_k \hat{A}_j \rangle \}\}. We also mention that given the appropriate decomposition of \( \hat{A} \) and \( \hat{O} \), it is possible to use classical shadows \([57]\) to reduce even more the amount of QC resources used. It is worth noting that such expectation values are independent of the choice \( (\mu, \varphi) \) used in the general definition (2) and can be made only once to get access to the whole family of operators \( \hat{O}_\alpha(\mu, \varphi) \). An illustration of this aspect is given in Fig. 3.

2. Oracle or projector construction with a simplified LCU algorithm

We now discuss a general approach to applying a non-unitary operator written as an LCU on a quantum computer. Given an operator written as a linear combination of unitary operators \( \hat{G} = \sum_{k=0}^{k_{\max}-1} g_k \hat{G}_k \), the LCU algorithm \([13]\) gives a method to perform the following operation:

\[
|\Psi\rangle \rightarrow \hat{G}|\Psi\rangle.
\]

This method has been extensively used for Hamiltonian simulation \([44, 46]\). The LCU method might be somewhat demanding regarding ancillary qubits to be added to the system description and the number of operations to implement it. Nevertheless, it remains an excellent candidate for implementing projectors for symmetry-restoration and associated oracles in quantum computers beyond the NISQ period. We use the implementation proposed in \([48]\), shown in Fig. 4 to do the operation (21). We need to introduce a set of \( n_{\text{LCU}} \) ancillary qubits such that \( 2^{n_{\text{LCU}}} \geq k_{\max} \). Then, an operator \( \hat{B} \) acting on the ancillary qubits is defined as:

\[
\hat{B}|0\rangle^{\otimes n_{\text{LCU}}} = \frac{1}{N} \sum_{k=0}^{2^{n_{\text{LCU}}} - 1} g_k |k\rangle^{\otimes n_{\text{LCU}}}
\]

with \( g_k \geq k_{\max} = 0 \) and where we introduced the normalization constant \( N = \sqrt{\sum_k |g_k|^2} \). Here \( \hat{G} \) can be any of the operators discussed above, e.g., the projector \( |0\rangle \) or the associated oracle \( |1\rangle \).

After applying the operation (22) to the ancillary register, a set of states \( \hat{G}_k|\Psi\rangle \) are sequentially associated with the different computational states of the ancillary register using controlled operations as shown in Fig. 4. Finally, the operation \( H^{\otimes n_{\text{LCU}}} \) is applied to the ancillary register. By measuring the qubits in the ancillary register and selecting the events where the state \( |0\rangle^{\otimes n_{\text{LCU}}} \) is measured, we obtain that the system state, after each of these measurements, collapses to the desired \( \hat{G}|\Psi\rangle \) state.

For the parity or particle number projection, the operators \( \hat{G}_k \) as defined in Eq. (19) are diagonal in the computational basis. A general implementation of a diagonal operator that can be applied in the case of these two types of oracles is presented in Refs. \([49, 50]\). These works showed that the optimal gate count for an arbitrary diagonal operator was \( 2^{n_{\text{LCU}}} + 3 \) where \( n_{\text{LCU}} \) is the number of qubits. However, for these cases, each operator \( \hat{G}_k \) controlled by the \( n_{\text{LCU}} \) qubits in the ancilla register can be implemented using a linear number of gates in \( n_{\text{LCU}} \) and \( n_q \). This linear dependence in \( n_{\text{LCU}} \) originates from the fact that a single qubit unitary gate controlled by \( n_q \) qubits can be decomposed in single qubits gates and CNOTS whose number depends linearly in \( n \) \([17]\).

The use of the set of Hadamard gates \( H^{\otimes n_{\text{LCU}}} \) in Fig 4 leads to an exponential decrease in the probability of measuring precisely zero in all ancillary qubits, i.e., \( p_{|0\rangle}^{\otimes n_{\text{LCU}}} \approx 1/\sqrt{2^{n_{\text{LCU}}}} \), which leads to a large set of rejected events. To avoid this unwanted feature, we replace the set of Hadamard gates with an operator \( \hat{E} \), where \( \hat{E} \) is the operator that initialize an equiprobable distribution in the ancillary register up to the state \( k_{\max} \), i.e.:

\[
\hat{E}|0\rangle^{\otimes n_{\text{LCU}}} = \frac{1}{\sqrt{k_{\max}}} \sum_{k=0}^{k_{\max}-1} |k\rangle^{\otimes n_{\text{LCU}}}.
\]

This replacement can be done because the only requirement for an arbitrary operator \( \hat{M} \) to be able to replace the set of Hadamard gates is to have equal components in its \( M_{0,j} \leq k_{\max} \) entries. Using \( \hat{M} = \hat{E} \), defined in Eq. (23), the probability \( p_{|0\rangle}^{\otimes n_{\text{LCU}}} \) now scales as \( 1/\sqrt{k_{\max}} \) and leads to a significant reduction of the number of rejected events compared to the initial proposal shown in Fig. 4.

We mention that the construction of such an operator is polynomial in the number of qubits \( O\left(L n^2_{\text{LCU}}\right) \) \([52]\).
FIG. 4: Simplified LCU circuit with $n_{\text{LCU}}$ ancilla qubits. This circuit can implement a linear combination of up to $2^{n_{\text{LCU}}}$ unitary operators. The filled circles (resp. open) are controlled operations by the $|1\rangle$ (resp. $|0\rangle$) state. We use the Qiskit convention in all the text, where the uppermost qubit corresponds to the least significant bit in the binary representation.

IV. EXAMPLE OF APPLICATIONS

Some illustrations of applications of the oracle techniques for projection as an alternative to the previously proposed methods of Refs. [25, 27, 29] are given in this section. In Fig 5, we show examples of how by only computing the expected values $\langle A e^{i\phi_k} S \rangle$ from Eq. (12) we have access to all the projected expectation values over the ensemble of eigenvalues of the symmetry operator. For the particle number symmetry, we use the same initial states as the one used in Figs. [2] and [3] that corresponds to an equiprobable mixing of all possible states of the total qubit space basis. Assuming the Jordan-Wigner mapping, these states mix different particle numbers. We show in panel (a) of Fig. 5 the amplitudes of the initial state obtained for different particle number $A = 0, \cdots, 8$. The simulations have been obtained using the LCU decomposition of the operator $P_A$ with varying particle numbers. All the simulations were made using the Qiskit package [55].

A second illustration is given in panel (b) of Fig. 5 where the projection of the total spin is performed for different values of $S$. In this case, similarly to the encoding of spins used in Ref. [27] and discussed previously, the spin components ($|\uparrow\rangle, |\downarrow\rangle$) of a particle is directly mapped to the states ($|0\rangle, |1\rangle$) of a given qubit. Accordingly, possible values of $S$ ranges from 0 to 4. Since here we performed the calculation onto a quantum computer emulator, i.e. without noise, we deduce that the amplitudes decompositions matches the exact amplitudes.

We finally repeated the calculation performed in Ref. [29] where the Q-VAP approach was applied to a set of fermions with equidistant level spacing $\epsilon_i = i \Delta \epsilon$, interacting with each other through a pairing interaction whose strength was denoted by $g$. In this reference, a BCS state parameterized with a set of parameters $\{\theta_i\}_{i=1,8}$ was prepared on a quantum register. This state was then projected onto a given particle number using the method proposed in Ref. [25] based on measuring a set of ancillary qubits. The projected state was then optimized using quantum-classical hybrid calculations leading to the Q-VAP minimum of energy. The Q-VAP procedure was repeated here using the oracle method for projecting the particle number symmetry. The previous and new results are compared in Fig. 6. All details regarding the superfluid system encoding, state preparation, and optimization technique are given in Ref. [29]. We see that the energies obtained with the two projection techniques perfectly match, with the advantage that the oracle-based approach requires only one ancillary qubit and that there are no rejected measurements.

V. CONCLUSION

In the present exploratory study, we discuss the possibility of using the concept of an oracle for the restoration of symmetries in many-body systems. We illustrate using examples that the indirect measurement technique used in Ref. [29] to perform the Quantum Variation After projection can be replaced by the oracle projection method. These examples put on evidence that the oracle also provides an accurate technique to perform projection with the advantage of not requiring the explicit construction of the projected state, reducing the number of ancillary
qubits and avoiding rejecting unwanted events.

Additionally, we show how oracles and projectors associated with symmetries can be constructed in practice on a quantum computer by first decomposing the projectors into a weighted sum of unitary operators. Once such decomposition is achieved, a standard technique based on the LCU method can be envisaged for implementing projectors or oracles. If we consider using the LCU technique, it is advisable to directly use the projector given by Eq. (28) and associated with symmetries can be constructed in practice on a quantum computer by first decomposing the projectors into a weighted sum of unitary operators.

We finally mention that the construction of an oracle associated with projectors either by the LCU method or by the direct encoding of a diagonal operator remains a challenge for current noisy machines and that the method will only be applicable in the post-NISQ period.

Acknowledgments

This project has received financial support from the CNRS through the 80Prime program and is part of the QC2I project. We acknowledge the use of IBM Q cloud as well as use of the Qiskit software package for performing the quantum simulations.

Appendix A: Technical aspects for the total spin projection

To implement the circuit associated with the spin projection, we first rewrite $\hat{S}^2$ given by Eq. (20) as:

$$\hat{S}^2 = \frac{3n_q}{4} + \frac{1}{2} \sum_{i<j,j=0}^{n_q-1} (X_iX_j + Y_iY_j + Z_iZ_j). \quad (A1)$$

The projector given in Eq. (9), written in the specific case where we project on the spin value $S'$ becomes:

$$\tilde{P}_{S'} = \sum_{k=0}^{n_q} \alpha_k e^{\frac{\phi_k}{\hbar} \sum_{i<j,j=0}^{n_q-1} (X_iX_j + Y_iY_j)} e^{\frac{\phi_k}{\hbar} \sum_{i<j,j=0}^{n_q-1} (Z_iZ_j)}$$

$$= \sum_{k=0}^{n_q} \alpha_k e^{\frac{\phi_k}{\hbar} \sum_{i<j,j=0}^{n_q-1} (X_iX_j + Y_iY_j)} \prod_{i<j,j=0}^{n_q-1} e^{\frac{\phi_k}{\hbar} Z_iZ_j}$$

with $\alpha_k = e^{i\alpha_k \frac{3n_q - \xi_{S', \lambda_1}}{M+1}}$ and $\phi_k = \frac{2\pi k}{\alpha(M+1)}$. We recognize the $R_{ZZ}(\theta) = e^{-i\frac{\theta}{2} Z \otimes Z}$ gate; a decomposition of this gate in elemental gates is shown in Fig. 7. Since the terms $X_iX_j + Y_iY_j$ do not commute; we use the Trotter-Suzuki approximation as:

$$e^{i\frac{\phi_k}{\hbar} \sum_{i<j,j=0}^{n_q-1} (X_iX_j + Y_iY_j)} \approx \left( \prod_{i<j,j=0}^{n_q-1} e^{i\frac{\phi_k}{\hbar} (X_iX_j + Y_iY_j)} \right)^{n_t}$$

where $n_t$ is the number of Trotter-Suzuki steps. A circuit to implement an operator $e^{-i\frac{\theta}{2} (X \otimes X + Y \otimes Y)}$ is shown in Fig. 8. $\theta$ should be equal to $\frac{2\alpha_k}{\alpha}$ in order to implement the gates in Eq. (A2).

![Fig. 7: Decomposition of the $R_{ZZ}(\theta) = e^{-i\frac{\theta}{2} Z \otimes Z}$ gate.](image)

![Fig. 8: Circuit to implement the operator $e^{-i\frac{\theta}{2} (X \otimes X + Y \otimes Y)}$.](image)
ble models of an antiferromagnetic chain, Ann. of Phys. 16, 407 (1961).

[40] R. Somma, G. Ortiz, J. E. Gubernatis, E. Knill, and R. Laflamme, Simulating physical phenomena by quantum networks, Phys. Rev. A 65, 042323 (2002).

[41] K Mitarai, M Negoro, M Kitagawa, and K Fujii. Quantum circuit learning, Phys. Rev. A, 98, 32309 (2018).

[42] M. Schuld, V. Bergholm, C. Gogolin, J. Izaac, and N. Killoran, Evaluating analytic gradients on quantum hardware. Phys. Rev. A, 99, 032331 (2019).

[43] G.L. Long. General quantum interference principle and duality computer. Common. Theor. Phys. 45, 825-844 (2006).

[44] A.M. Childs and N. Wiebe, Hamiltonian simulation using linear combinations of unitary operations, Quant. Inf. and Comp. 12, 901 (2012).

[45] D.W. Berry, A.M. Childs, R. Cleve, R. Kothari, and R.D. Somma. Exponential improvement in precision for simulating sparse Hamiltonians. Proceedings of the Annual ACM Symposium on Theory of Computing, 283-292 (2014).

[46] D. Berry, A. Childs, and R. Kothari. Hamiltonian Simulation with Nearly Optimal Dependence on all Parameters. Proceedings of the 56th IEEE Symposium on Foundations of Computer Science, (2015).

[47] A.J. da Silva1, and D.K. Park. Linear-depth quantum circuits for multi-qubit controlled gates. arxiv.org/pdf/2203.11882, (2022).

[48] S. Wei, H. Li, and G. Long A Full Quantum Eigensolver for Quantum Chemistry Simulations. Research, 2020, (2020).

[49] S.S. Bullock and I.L. Markov, Smaller Circuits for Arbitrary n-qubit Diagonal Computations, Quant. Inf. and Comp., 4, 027 (2004).

[50] Jonathan Welch, Daniel Greenbaum, Sarah Mostame, and Alan Aspuru-Guzik, Efficient quantum circuits for diagonal unitaries without ancillas, New J. Phys. 16, 033040 (2014)

[51] K. Choi, D. Lee, J. Bonitati, Z. Qian, and J. Watkins. Rodeo Algorithm for Quantum Computing. Phys. Rev. Lett. 16, 40505 (2021).

[52] G. Long and Y. Sun. Efficient scheme for initializing a quantum register with an arbitrary superposed state. Phys. Rev. A, 64 (1):14303, (2001).

[53] V. Shende, S. Bullock, and I. Markov. Synthesis of Quantum Logic Circuits. Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions, 25 1000-1010, (2006).

[54] P. L"owdin and Osvaldo Goscinski. The exchange phenomenon, the symmetric group, and the spin degeneracy problem. International Journal of Quantum Chemistry, 4(3B) 533-591, (1969).

[55] H. F. Trotter, On the product of semi-groups of operators, Proc. Am. Math. Soc. 10, 545 (1959).

[56] Takashi Tsuchimochi and Yuto Mori, Spin-projection for quantum computation: A low-depth approach to strong correlation, Phys. Rev. Research 2, 043142 (2020).

[57] HY. Huang, R.Kueng, and J. Preskill. Predicting many properties of a quantum system from very few measurements, Nat. Phys. 127, 1050-1057 (2020).

[58] IBM. Qiskit: An Open-source Framework for Quantum Computing,