Near-optimal quantum circuit for Grover's unstructured search using a transverse field

Zhang Jiang, Eleanor G. Rieffel, and Zhihui Wang

Near-optimal quantum circuit for Grover's unstructured search using a transverse field

Zhang Jiang,[1,2,*] Eleanor G. Rieffel,[1] and Zhihui Wang[1,3]

[1]*Quantum Artificial Intelligence Laboratory (QuAIL),*
NASA Ames Research Center, Moffett Field, California 94035, USA
[2]*Stinger Ghaffarian Technologies Inc., 7701 Greenbelt Rd., Suite 400, Greenbelt, MD 20770*
[3]*Universities Space Research Association, 615 National Ave, Mountain View, CA 94043*

(Dated: May 4, 2017)

Inspired by a class of algorithms proposed by Farhi *et al.* [arXiv:1411.4028 (2014)], namely the quantum approximate optimization algorithm (QAOA), we present a circuit-based quantum algorithm to search for a needle in a haystack, obtaining the same quadratic speedup achieved by Grover's original algorithm. In our algorithm, the problem Hamiltonian (oracle) and a transverse field are applied alternately to the system in a periodic manner. We introduced a novel technique, a spin-coherent-state approach, to analyze the composite unitary in a single period. This composite unitary drives a closed transition between two states that have high degrees of overlap with the initial state and the target state, respectively. The transition rate in our algorithm is of order $\Theta(1/\sqrt{N})$, and the overlaps are of order $\Theta(1)$, yielding a nearly optimal query complexity of $T \simeq \sqrt{N}(\pi/2\sqrt{2})$. Our algorithm is the first example of a QAOA circuit that demonstrates a quantum advantage with large number of iterations that is not derived from Trotterization of an adiabatic quantum optimization (AQO) algorithm. It also suggests that the analysis required to understand QAOA circuits involves a very different process from estimating the energy gap of a Hamiltonian in AQO.

I. INTRODUCTION

Recently, Farhi *et al.* [1, 2] proposed a new class of quantum heuristic algorithms, the quantum approximate optimization algorithm (QAOA). We present a novel algorithm for Grover's unstructured search problem [9] inspired by QAOA. This algorithm is the first within the QAOA framework to show a quantum advantage for a number of iterations p in the intermediate range between $p = 1$ and $p \to \infty$. We also introduce a novel tool, a representation based on spin coherent states, for the design and analysis of the QAOA-type circuits. Using this tool, we prove a $\Theta(\sqrt{N})$ query complexity for our algorithm. The algorithm has the advantage of requiring fewer 2-qubit gates than Grover's original algorithm, because we use the transverse field in place of Grover's original diffusion operator. With increasing number of iterations p, exhaustive search of the QAOA parameters often becomes inefficient due to the curse of dimensionality. Our method avoids this difficulty by restricting the parameters to be periodic. The approach suggests a potential route for parameter optimization for QAOA-based quantum heuristic algorithms more generally.

In our algorithm, mixing and problem (oracle) Hamiltonians are applied to the system in a sequence that is periodic in time. The long-time dynamics of a periodically driven quantum system can be profoundly different from a time-homogeneous one [3]. To analyze the outcome after $\Theta(\sqrt{N})$ periods, we solve the relevant eigenvalues and eigenvectors of the composite (effective) unitary in a single period to exponential precision $\mathcal{O}(1/\sqrt{N})$. This analysis gives further evidence that, while the initial mo-

tivation for Farhi *et al.*'s design of QAOA circuits may have come from Trotterization of adiabatic quantum optimization (AQO), the analysis required to understand QAOA circuits involves a very different process from estimating an exponentially small energy gap of a Hamiltonian.

Instead, the intuition for this algorithm comes from a novel phase-space representation based on spin-coherent states in which both the unitaries generated by the mixing and the oracle Hamiltonians take simple forms. We find that the composite unitary generates a closed transition between two states that have high degrees of overlap with the initial state and the target state, respectively. The transition rate in our algorithm is of order $\Theta(1/\sqrt{N})$, and the overlaps are of order $\Theta(1)$, yielding a nearly optimal query complexity of $T \simeq \sqrt{N}(\pi/2\sqrt{2})$.

We begin, in Sec. II, by briefly reviewing QAOA circuits, providing context and inspiration for our construction. In Sec. III, we briefly review prior approaches to Grover's problem. In Sec. IV, we introduce our algorithm. Section V gives an intuitive picture, using a representation based on spin coherent states, for why the algorithm works. The most straightforward application of this picture results in a query complexity that is close to optimal, up to a polylog factor. We then refine the algorithm, removing the polylog factor, to obtain a query complexity within a small constant of optimal. This improvement makes use of the novel phase-space representation we describe in Sec. VI. Section VII shows how we use this phase space representation to derive analytical results, including the success probability and the query complexity of our algorithm. In Sec. VIII, we briefly comment on how to check whether the correct solution has been found. We conclude in Sec. IX with thoughts on future directions.

* zhang.jiang@nasa.gov

II. REVIEW OF QAOA CIRCUITS

QAOA circuits iteratively alternate between a classical Hamiltonian (usually the problem Hamiltonian derived from a cost function) and a mixing term (often the transverse field) [1, 2]. Farhi *et al.* proposed these circuits to tackle approximate optimization of challenging combinatorial problems, with the approximation ratio improving (or at least not decreasing) as the number of iterations p increases. We will refer to circuits with the above structure as QAOA circuits whether or not they are used for approximate optimization or for some other purpose. Since Farhi *et al.*'s original work, QAOA circuits have also been applied for exact optimization [4] and sampling [5]. Further, Farhi and Harrow [5] argued, under reasonable complexity theoretic assumptions, that it is not possible for any classical algorithm to produce samples according to the output distribution of QAOA circuits with even a single iteration ($p = 1$). Their results suggest that QAOA circuits applied to sampling are among the most promising candidates for early demonstrations of "quantum supremacy" [6, 7]. It remains an open question whether QAOA circuits provide a quantum advantage for approximate optimization.

Trotterization of adiabatic quantum optimization (AQO) implies that QAOA can always achieve the optimum in the limit of infinite iterations ($p \to \infty$). At the other end of the spectrum, Farhi *et al.* [2] proved that a QAOA circuit with $p = 1$ beat the best classical approximation ratio for MaxE3Lin2 at the time (which inspired a new classical approach that currently hold the record [8]). The parameters for these circuits are the times β_i and γ_i, $1 \le i \le p$, for which the mixing and classical Hamiltonian, respectively, are applied. Farhi *et al.* show that, for a fixed p, the optimal parameters can be computed in time polynomial in the number of qubits n. If we discretize so that each parameter can take on m values, exhaustive search of the optimum takes exponential steps in p as m^{2p}.

For this reason, prior to this work, there were no results for QAOA circuits with an intermediate number of iterations $1 \ll p < \infty$. Here, we give the first such algorithm. Our approach suggests that considering QAOA circuits with periodic parameters may be a profitable way to parameter setting for QAOA circuits with $1 \ll p < \infty$.

III. REVIEW OF PRIOR QUANTUM ALGORITHMS FOR GROVER'S PROBLEM

Grover's algorithm [9] has attracted much attention, because it has been proven that it outperforms any classical algorithm. It searches for a needle in a haystack, achieving a query complexity of $\Theta(\sqrt{N})$, where $N = 2^n$ is the size of the search space. Grover's algorithm is optimal among quantum algorithms for such a task [10–12]. It offers a modest quadratic speedup over any classical counterpart, though even quadratic speedup is consider-

able when N is large.

Grover's algorithm selectively alters the phase of the target state given by the oracle, at each iteration. While this operation on its own would not change the probability of reading out the target state, it sets the stage for the next operation which takes advantage of the phase difference to increase the probability of the system being in that state. This effect would be impossible were quantum amplitudes not able to store phase information as well as the probability. This step is carried out by Grover's diffusion operator, which applies a phase of π to the even superposition state and does nothing to any state orthogonal to it. It requires $\Theta(n)$ two-qubit gates to implement Grover's diffusion operator [13].

Grover's unstructured search problem can also be solved by adiabatic quantum computation, where a mixing Hamiltonian (typically a transverse field) is gradually replaced by the problem Hamiltonian that encodes the answer in its ground state. The minimum gap of the total Hamiltonian is crucial to the time complexity of the algorithm and was first given by Farhi *et al.* [14]. Recently, the exponential scaling of this minimum gap was rederived using an instanton approach, without solving the eigenvalue equation (see supplementary material in [15]). By adjusting the evolution rate of the Hamiltonian, Roland and Cerf [16] recover the quadratic advantage of Grover's original algorithm over classical search. Roland and Cerf do not use the standard mixing operator, the transverse field, but rather a Hamiltonian related to Grover's diffusion operator.

A natural question is whether it is possible to implement unstructured quantum search in the circuit model using the transverse field instead of Grover's diffusion operator. Here, we give an affirmative answer to this question.

IV. OUR ALGORITHM

Here, we give a high-level view of the algorithm. Sec. V describes the intuition behind our algorithm, based on a picture using spin-coherent states.

Grover's problem.—Suppose we are given a problem Hamiltonian (oracle)

$$C_{\boldsymbol{u}} = -|\,\boldsymbol{u}\,\rangle\langle\,\boldsymbol{u}\,|\,, \tag{1}$$

that encodes an unknown bit string $\boldsymbol{u}$ of length n (n even, for simplicity). The aim is to find $\boldsymbol{u}$ using as few calls to this oracle as possible.

Our algorithm uses the transverse field operator B as the driver (mixing term),

$$B = \sum_{j=1}^{n} X_j\,, \tag{2}$$

where X_j is the Pauli-X operator of the j-th qubit. An advantage of using B over Grover's diffusion operator
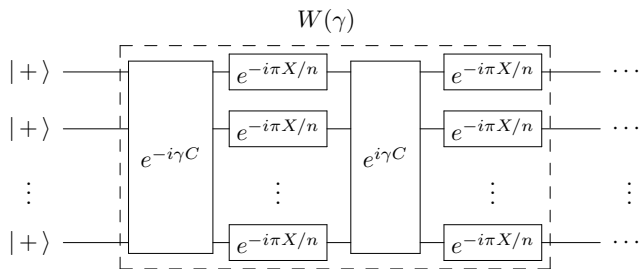
$$W(\gamma)$$

FIG. 1. To map the input state to a state having large overlap with the target, the unitary $W(\gamma)$ is repeated for $\mathcal{O}(N^{1/2})$ times.

is that B acts only on individual spins, so it is easier and more efficient to implement. The input state of our algorithm is the usual one, the tensor product $|+\rangle^{\otimes n}$, the joint $+1$ eigenstate of all the X_j operators, and the even superposition of all bit strings,

$$|\psi_{\rm in}\rangle = |+\rangle^{\otimes n} = \frac{1}{\sqrt{N}} \sum_{s\in\{0,1\}^n} |s\rangle. \qquad (3)$$

We can simplify the analysis, following Farhi *et al.* [14], by working in a basis in which the target state is $|\mathbf{0}\rangle = |0\cdots00\rangle$. Since the driver B and the initial state $|\psi_{\rm in}\rangle$ remain the same when any subset of the n qubits are flipped, the problem can be converted to finding the bit string $\mathbf{0}$ using the oracle $C_\mathbf{0}$ with the same driver B. Doing so drastically simplifies our analysis: the state $|\mathbf{0}\rangle$, and the initial state $|+\rangle^{\otimes n}$, are in the $(n+1)$-dimensional symmetric subspace (under permutations of qubits), and the evolution under both B and $C_\mathbf{0}$ preserves this subspace, so we only need to consider that $(n+1)$-dimensional subspace instead of the whole Hilbert space of dimension 2^n. To simplify notation, we will omit the subscript in $C_\mathbf{0}$ hereafter, i.e., $C \equiv C_\mathbf{0}$.

The building block of our algorithm is a simple product of unitaries generated by B and C,

$$W(\gamma) = e^{-i\pi B/n} e^{i\gamma C} e^{-i\pi B/n} e^{-i\gamma C}, \qquad (4)$$

where $\gamma \in (0, \pi]$ is a free parameter. The intuition that we choose the angle of the rotation $e^{-i\pi B/n}$ can be found in Sec. V. The algorithm repeatedly applies the unitary $W(\gamma)$ for $\Theta(\sqrt{N})$ times (see Fig. 1). The relevant eigenvalues of the unitary $W(\gamma)$ determine the query complexity of our algorithm, while the corresponding eigenvectors determine the probability of success. We will show that the relevant eigenvalues are the ones closest to 1, but not equal to 1.

The unitary $W(\gamma)$ has a time-reversal-like symmetry

$$\Lambda W(\gamma)\Lambda^\dagger = W^\dagger(\gamma), \qquad (5)$$

where $\Lambda = e^{-i\pi B/n} Z_1 Z_2 \cdots Z_n$ with Z_j being the Pauli-Z operator of the j-th qubit. Equation (5) holds generally for Hamiltonians based on classical cost functions, Hamiltonians diagonal in the computational basis. This

symmetry implies that if α is an eigenvalue of $W(\gamma)$, then its complex conjugate α^* is also an eigenvalue of $W(\gamma)$; the corresponding eigenstates are denoted by $|w_\alpha\rangle$ and $|w_{\alpha^*}\rangle$, respectively. When restricted to the 2-dimensional subspace $\mathcal{S}_\alpha$ spanned by $\{|w_\alpha\rangle, |w_{\alpha^*}\rangle\}$, and written in the basis $\{|w_+\rangle, |w_-\rangle\}$, where

$$|w_\pm\rangle = \frac{1}{\sqrt{2}} \Big(|w_\alpha\rangle \pm |w_{\alpha^*}\rangle \Big), \qquad (6)$$

$W(\gamma)$ has the matrix representation

$$W\big|_{\mathcal{S}_\alpha}(\gamma) = \exp\left[-i \begin{pmatrix} 0 & \arg(\alpha) \\ \arg(\alpha) & 0 \end{pmatrix} \right]. \qquad (7)$$

The unitary $W(\gamma)$ thus drives a closed transition between $|w_\pm\rangle$ with the transition rate $\arg(\alpha)$. To drive a full transition, one needs to repeat $W(\gamma)$ for roughly $\pi/(2\arg(\alpha))$ times.

Let $|b_\pm\rangle = \frac{1}{\sqrt{2}}(|+\rangle^{\otimes n} \pm |-\rangle^{\otimes n})$. We show in Sec. VII that for the eigenvalues α and α^* exponentially close to 1 but not equal to 1, $|w_\alpha\rangle$ and $|w_{\alpha^*}\rangle$ have large overlaps with $\frac{1}{\sqrt{2}}(|\mathbf{0}\rangle \pm i|b_+\rangle)$, respectively. In other words, $|w_+\rangle$ and $|w_-\rangle$ have large overlaps with $|\mathbf{0}\rangle$ and $i|b_+\rangle$, respectively, so the algorithm drives $|b_+\rangle$ close to the target state $|\mathbf{0}\rangle$. The value of $\arg(\alpha)$ has to be exponentially small in n, otherwise, our algorithm would have beaten the optimal query complexity of Grover's algorithm. Hereafter, α will refer to this specific eigenvalue. The initial state (3) can be written as

$$|\psi_{\rm in}\rangle = |+\rangle^{\otimes n} = \frac{1}{\sqrt{2}} \Big(|b_+\rangle + |b_-\rangle \Big); \qquad (8)$$

note that $|b_-\rangle$ is a dark state, i.e., $W(\gamma)|b_-\rangle = |b_-\rangle$. For $|\langle \mathbf{0}|w_+\rangle| \simeq |\langle b_+|w_-\rangle| \simeq 1$, the output state is approximately

$$|\psi_{\rm out}\rangle \simeq \frac{1}{\sqrt{2}} \Big(|\mathbf{0}\rangle + |b_-\rangle \Big), \qquad (9)$$

and the probability of finding the target state $|\mathbf{0}\rangle$ is approximately $1/2$.

In Sec. VII, we derive approximate results for our algorithm in the large-n limit. For $\gamma = \pi$, we find that $|\langle \mathbf{0}|w_+\rangle| \simeq (1 - \pi^2/2n)^{1/4}$ in Eq. (58) (the fidelity is smaller for $\gamma \neq \pi$). See Fig. 2(a) for a comparison of analytical and numerical results. We also find that $|\langle b_+|w_-\rangle| \simeq 1 - N^{-1}$ in Eq. (67). See Fig. 2(b) for a comparison of analytical and numerical results. Furthermore, we calculate that $\arg(\alpha) \simeq 4\sqrt{2}\,N^{-1/2}(1 - \pi^2/2n)^{1/4}$ in Eq. (66). Figure 3(a) shows a comparison of analytic and numerical results. Considering that the success probabilities of our algorithm is about $1/2$ and each iteration $W(\gamma)$ calls the oracle twice, the average query complexity of our algorithm is

$$T(n) \simeq \frac{2\pi}{\arg(\alpha)} \simeq \frac{\pi}{2\sqrt{2}} 2^{n/2}, \qquad (10)$$

which differs from the optimal value presented in Ref. [12] by a factor of $\sqrt{2}$.
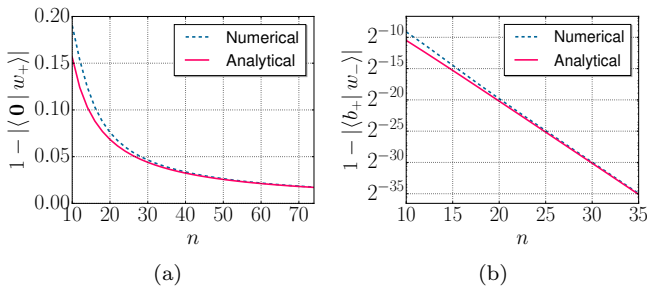
FIG. 2. (a) Numerical and analytical (large-n limit) results for the infidelity $1-|\langle \mathbf{0} | w_+ \rangle|$ as a function of the number of qubits for $\gamma = \pi$, which vanishes polynomially as n increases. The numerical results are calculated by direct diagonalization of the matrix $W(\pi)$ in the symmetric subspace; the analytical results use Eq. (58), $|\langle \mathbf{0} | w_+ \rangle| \simeq (1 - \pi^2/2n)^{1/4}$. (b) Numerical and analytical (large-n limit) results for the infidelity $1-|\langle b_+ | w_- \rangle|$ as a function of the number of qubits n for $\gamma = \pi$, which decreases exponentially as n increases. The numerical results come from direct diagonalization, and the analytical results from Eq. (63), $\langle b_+ | w_- \rangle \simeq i\sqrt{2d/n}\,(1-\pi^2/2n)^{1/4}$.
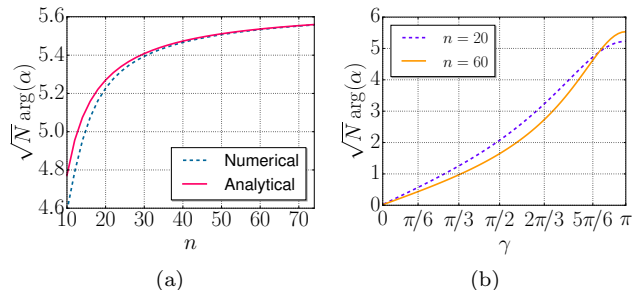

FIG. 3. (a) Numerical and analytical (large-n limit) results for $\sqrt{N}\arg(\alpha)$ as a function of n for $\gamma = \pi$; (b) Numerical results for $\sqrt{N}\arg(\alpha)$ as a function of γ. The numerical results are computed using exact diagonalization. The analytical results are from Eq. (66) and Eq. (66), respectively.

V. AN INTUITIVE PICTURE USING SPIN COHERENT STATES

This section gives intuition behind our algorithm. A representation using spin coherent states [17, 18] is useful for understanding why the algorithm works. Consider spin coherent states of the form

$$| \psi(\theta) \rangle = e^{-i\theta B/2}| \mathbf{0} \rangle, \qquad (11)$$

where $\theta \in [0, 2\pi)$; these states form an over-complete basis for the symmetric subspace $\mathcal{H}_S$. We pay particular attention to a set of discrete angles $\theta_k = k\Delta\theta$, where $k = 0, 1, \ldots, n-1$ and $\Delta\theta = 2\pi/n$. Along with the dark state $| b_- \rangle$, this set of discrete spin coherent states form a complete basis of $\mathcal{H}_S$. The state $| b_+ \rangle$ can be expanded

as (see Fig. 4a),

$$| b_+ \rangle = \frac{1}{n\langle b_+ | \mathbf{0} \rangle} \sum_{k=0}^{n-1}(-1)^k e^{-ik\pi B/n}| \mathbf{0} \rangle, \qquad (12)$$

where $\langle b_+ | \mathbf{0} \rangle = \sqrt{2/N}$ is exponentially small in n. The normalization factor can be derived by noticing

$$\sum_{k=0}^{n-1}(-1)^k\langle b_+ | e^{-ik\pi B/n}| \mathbf{0} \rangle = n\langle b_+ | \mathbf{0} \rangle, \qquad (13)$$

where we used the identity

$$e^{-i\pi B/n}| b_\pm \rangle = -| b_\pm \rangle. \qquad (14)$$

The expansion coefficient in Eq. (12) can be derived by noticing that $| b_+ \rangle$ is orthogonal to any eigenstate of B with an eigenvalue other than $\pm n$. We will also need the eigenstate of B with eigenvalue 0,

$$| b_0 \rangle \propto P_S\left(| + \rangle^{\otimes \frac{n}{2}} \otimes | - \rangle^{\otimes \frac{n}{2}}\right), \qquad (15)$$

where P_S is the projector onto $\mathcal{H}_S$. In other words, $| b_0 \rangle$ is proportional to the sum of the $\binom{n}{n/2}$ terms that are tensor products of the single-qubit states $| + \rangle$ and $| - \rangle$ with the same number of occurrences, i.e., Hamming weight $n/2$ strings in the Hadamard basis. The overlap of this state with the target state is

$$|\langle b_0 | \mathbf{0} \rangle|^2 = \frac{n!}{(n/2)!(n/2)!}\frac{1}{2^n} \simeq \sqrt{\frac{2}{\pi n}}, \qquad (16)$$

which is only polynomially small. This state has the following expansion using the discrete spin coherent states [see Fig. 4(b)],

$$| b_0 \rangle = \frac{1}{n\langle b_0 | \mathbf{0} \rangle} \sum_{k=0}^{n-1} e^{-ik\pi B/n}| \mathbf{0} \rangle, \qquad (17)$$

where $\langle b_0 | \mathbf{0} \rangle$ is of order $n^{-1/4}$. It remains the same under the discrete rotation

$$e^{-i\pi B/n}| b_0 \rangle = | b_0 \rangle. \qquad (18)$$

The unitary generated by the oracle takes the following form for $\gamma \ll 1$,

$$e^{-i\gamma C}| \psi \rangle = | \psi \rangle + i\gamma \langle \mathbf{0} | \psi \rangle| \mathbf{0} \rangle + \mathcal{O}(\gamma^2), \qquad (19)$$

where $| \psi \rangle$ is an arbitrary state. Putting Eqs. (4), (14), (18), and (19) together, we have

$$W(\gamma)^{\frac{n}{2}}| b_+ \rangle \simeq | b_+ \rangle + i\gamma\eta| b_0 \rangle, \qquad (20)$$

$$W(\gamma)^{\frac{n}{2}}| b_0 \rangle \simeq | b_0 \rangle + i\gamma\eta| b_+ \rangle, \qquad (21)$$

where

$$\eta = n\langle b_+ | \mathbf{0} \rangle\langle b_0 | \mathbf{0} \rangle \simeq \sqrt[4]{2/\pi}\,n^{3/4}N^{-1/2}. \qquad (22)$$
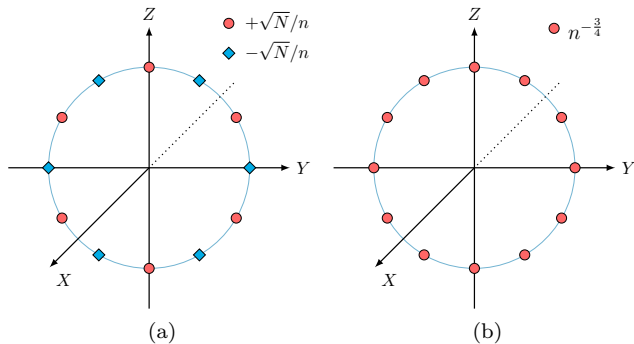
FIG. 4. Spin coherent state representation: (a) for $|b_+\rangle$, where $\sqrt{N}/n$ is the order of the expansion coefficients in Eq. (12); (b) for $|b_0\rangle$, where $n^{-3/4}$ is the order of the expansion coefficients in Eq. (17).

Thus, the unitary $W(\gamma)^{n/2}$ approximately drives a transition between $|b_+\rangle$ and $|b_0\rangle$ with the rate $\gamma\eta$. Applying the unitary $W(\gamma)$ for order $n/\gamma\eta$ times, one can drive the state $|b_+\rangle$ to a state close to $|b_0\rangle$. The probability of finding the target state with $|b_0\rangle$ is only polynomially small in n as opposed to the exponentially small value with $|b_+\rangle$, achieving the quadratic speedup in Grover's algorithm up to a logarithmic factor.

Although the case $\gamma \ll 1$ is illustrative, it requires a logarithmically many more calls to the oracle than Grover's original algorithm, and the probability of finding the target state is small. Since η is exponentially small in n, both $|b_+\rangle$ and $|b_0\rangle$ are close to eigenvectors for eigenvalues exponentially close to 1. This analysis suggests concentrating on the subspace spanned by $\{|w_\alpha\rangle, |w_{\alpha^*}\rangle\}$, where α and α^* are the eigenvalues closest to 1. Indeed, we show in Sec. VII that one can increase the success probability and reduce the number of calls to the oracle by setting $\gamma = \pi$. In Fig. 3(b), $\arg(\alpha)$ is plotted as a function of γ. The reason behind why $\gamma = \pi$ performs the best (or why it even works) seems unclear without a tedious calculation. We give this calculation in Sec. VII, after introducing a "phase space" representation that will be useful in that analysis.

VI. PHASE SPACE REPRESENTATIONS

We introduce a novel phase space representation in this section, which is essential in the following section to the analytical solution of the success probability and the query complexity of our algorithm. The phase space representation is based on the inner products of a quantum state with the spin coherent states we introduced in Sec. V.

Any state $|\psi\rangle \in \mathcal{H}_S$ can be uniquely determined by the inner products $\langle \mathbf{0}|e^{i\theta B/2}|\psi\rangle$. The χ function

$$\chi(|\psi\rangle, \theta) = \langle \mathbf{0}|e^{i\theta B/2}|\psi\rangle. \quad (23)$$

fully determines the state $|\psi\rangle$, since the spin coherent states $e^{-i\theta B/2}|\mathbf{0}\rangle$ for $\theta \in [0, 2\pi)$ are over-complete for the symmetric subspace; the advantage of this representation is that both B and C can be expressed concisely. For even n, the χ function satisfies the periodic boundary condition

$$\begin{aligned}\chi(|\psi\rangle, 2\pi) &= \langle \mathbf{0}|e^{i\pi B}|\psi\rangle \\ &= (-1)^n\langle \mathbf{0}|\psi\rangle = \chi(|\psi\rangle, 0).\end{aligned} \quad (24)$$

For the initial state in Eq. (3), we have

$$\chi(|\psi_{\text{in}}\rangle, \theta) = \langle \mathbf{0}|e^{i\theta B/2}|\psi_{\text{in}}\rangle = \frac{e^{-in\theta/2}}{\sqrt{N}}. \quad (25)$$

For the target state $|\mathbf{0}\rangle$, we have

$$\chi(|\mathbf{0}\rangle, \theta) = \langle \mathbf{0}|e^{i\theta B/2}|\mathbf{0}\rangle = \cos(\theta/2)^n. \quad (26)$$

The unitaries $e^{-i\phi B/2}$ and $e^{-i\gamma C}$ take simple forms,

$$\chi(e^{-i\phi B/2}|\psi\rangle, \theta) = \chi(|\psi\rangle, \theta - \phi), \quad (27)$$

$$\begin{aligned}&\chi(e^{-i\gamma C}|\psi\rangle, \theta) \\ &= \chi(|\psi\rangle, \theta) + (e^{i\gamma} - 1)\chi(|\psi\rangle, 0)\cos(\theta/2)^n.\end{aligned} \quad (28)$$

For the discrete angles $\theta_k = 2k\pi/n$, we introduce the notation

$$\chi_k(|\psi\rangle) = \langle \mathbf{0}|e^{ik\pi B/n}|\psi\rangle. \quad (29)$$

The χ function of $|\mathbf{0}\rangle$ will be used frequently, and we denote it as

$$\xi_k \equiv \chi_k(|\mathbf{0}\rangle) = \cos(k\pi/n)^n. \quad (30)$$

We will used the following identity repeatedly,

$$\sum_{k=0}^{n-1}(-1)^k\xi_k = n\langle \mathbf{0}|b_+\rangle^2 = \frac{2n}{N}. \quad (31)$$

For discrete angles, Eqs. (27) and (28) becomes

$$\chi_k(e^{-i\pi B/n}|\psi\rangle) = \chi_{k-1}(|\psi\rangle), \quad (32)$$

$$\chi_k(e^{-i\gamma C}|\psi\rangle) = \chi_k(|\psi\rangle) + (e^{i\gamma} - 1)\chi_0(|\psi\rangle)\xi_k. \quad (33)$$

For the eigenstates of B with eigenvalues $\pm n$, we have

$$\chi_k(|b_n\rangle) = \chi_k(|b_{-n}\rangle) = (-1)^k N^{-1/2}, \quad (34)$$

where $|b_n\rangle = |\psi_{\text{in}}\rangle = |+\rangle^{\otimes n}$ and $|b_{-n}\rangle = |-\rangle^{\otimes n}$. Since the discrete χ function of the states $|b_n\rangle$ and $|b_{-n}\rangle$ are the same, it does not uniquely determine a state in the symmetric subspace with dimension $n + 1$. The discrete χ function, however, is unique in the orthogonal space of $|b_-\rangle = \frac{1}{\sqrt{2}}(|b_n\rangle - |b_{-n}\rangle)$. We will restrict our discussions in that subspace, and $|b_-\rangle$ is a dark state anyway. For $|b_+\rangle = \frac{1}{\sqrt{2}}(|b_n\rangle + |b_{-n}\rangle)$, we have

$$\chi_k(|b_+\rangle) = \sqrt{2}(-1)^k N^{-1/2}. \quad (35)$$

The state $|b_0\rangle$ remains the same under $e^{-i\theta B/2}$, and its χ function is a constant

$$\chi_k(|b_0\rangle) = \chi_0(|b_0\rangle) \simeq \sqrt[4]{2/\pi n}\,, \qquad (36)$$

using the approximation in Eq. (16). To calculate the normalization factor of the χ representation, we need the Fourier component

$$\tilde{\chi}_j(|\psi\rangle) = \frac{1}{n}\sum_{k=0}^{n-1} \chi_k(|\psi\rangle)\, e^{ijk\pi/n}\,, \qquad (37)$$

where $j \in J \equiv \{-n, \ldots, -2, 0, 2, \ldots, n\}$. The normalization condition is

$$|\langle\psi\,|\,\psi\rangle|^2 = \frac{N}{2}\left|\tilde{\chi}_n(|\psi\rangle)\right|^2 + \sum_{j\in J'}\frac{\left|\tilde{\chi}_j(|\psi\rangle)\right|^2}{|\langle\mathbf{0}\,|\,b_j\rangle|^2}\,, \qquad (38)$$

where J' denotes the set $J\backslash\{\pm n\}$, and $|b_j\rangle$ is the eigenstate of B whose eigenvalue is j, i.e. $B|b_j\rangle = j|b_j\rangle$.

VII. ANALYTICAL SOLUTIONS

In this section, we solve the case $\gamma = \pi$ analytically using the phase space representation introduced in Sec. VI. Because $e^{-i\pi C} = e^{i\pi C}$, it suffices to consider

$$V \equiv e^{-i\pi B/n}\, e^{i\pi C} = \sqrt{W(\pi)}\,. \qquad (39)$$

The state $|w_\alpha\rangle$, an eigenstate of W, is also an eigenstate of V. The new eigenvalue is $\beta = \alpha^{1/2}$ (β is close to -1). The remainder of this section is devoted to finding the relevant eigenvalues and eigenstates of V. The eigenvalues determine the query complexity of our algorithm, while the corresponding eigenvectors determine the probability of success.

We introduce the unnormalized χ functions of the eigenstate $|w_\alpha\rangle$,

$$\varphi_k \equiv \chi_k(|w_\alpha\rangle)/\chi_0(|w_\alpha\rangle)\,, \qquad (40)$$

which satisfies $\varphi_0 = 1$. Using Eqs. (32) and (33), we have

$$\varphi_k = \beta^k + 2\sum_{\ell=1}^{k}\beta^{k-\ell}\xi_\ell\,, \qquad (41)$$

where ξ_ℓ is defined in Eq. (30). The periodic boundary condition $\varphi_n = \varphi_0$ gives the eigenvalue equation for β,

$$(1 + \beta^n)/2 + \beta^{n-1}\xi_1 + \cdots + \beta^2\xi_{n-2} + \beta\xi_{n-1} = 0\,. \quad (42)$$

Because Eq. (42) only contains real coefficients, β^* is also an solution to it [comes from the symmetry (5)]. For $\beta \simeq -1$, we have

$$\beta = -\sqrt{1-\delta^2} - i\delta \simeq -1 - i\delta + \delta^2/2\,, \qquad (43)$$

where $\delta > 0$ is a small real parameter of order $1/\sqrt{N}$. Putting Eq. (43) into Eq. (42) and only keeping terms up to order δ^2, we have

$$0 = 1 + in\delta/2 - n^2\delta^2/4 + \sum_{k=1}^{n-1}(-1)^k\left(1 + (n-k)\big[i\delta - (n-k)\delta^2/2\big]\right)\xi_k + \mathcal{O}(\delta^3)$$

$$= \sum_{k=0}^{n-1}(-1)^k\xi_k + i\delta\left(\frac{n}{2} + \sum_{k=1}^{n-1}(-1)^k(n-k)\,\xi_k\right) - \frac{\delta^2}{2}\left(\frac{n^2}{2} + \sum_{k=1}^{n-1}(-1)^k(n-k)^2\,\xi_k\right) + \mathcal{O}(\delta^3)\,. \qquad (44)$$

The coefficient of the term with $i\delta$ in Eq. (44) is

$$\frac{n}{2} + \sum_{k=1}^{n-1}(-1)^k(n-k)\,\xi_k = \frac{n}{2}\sum_{k=0}^{n-1}(-1)^k\xi_k = \frac{n^2}{N}\,, \quad (45)$$

where we have used Eq. (31); therefore, the pure imaginary term in Eq. (44) is of order δ^3 and can be neglected. Comparing the real parts at both sides of Eq. (44), we have

$$\delta^2 \simeq \frac{2\sum_{k=0}^{n-1}(-1)^k\xi_k}{n^2/2 + \sum_{k=1}^{n-1}(-1)^k(n-k)^2\,\xi_k}\,. \qquad (46)$$

While the numerator in Eq. (46) has already been solved in Eq. (31), the denominator is harder to calculate. We

write the denominator as

$$d = n^2/2 + \sum_{k=1}^{n-1}(-1)^k(n-k)^2\,\xi_k\,, \qquad (47)$$

and we will solve it later (but remember $d \sim n$). Putting Eqs. (31) and (47) into Eq. (46), we have the formal solution

$$\delta = 2\sqrt{n/d}\,N^{-1/2}\,, \qquad (48)$$

where d is to be determined.

Let φ_k^+ and φ_k^- be the real and imaginary parts of the function φ_k defined in Eq. (40), we have

$$\varphi_k^+ = \chi_k(|w_+\rangle)/\chi_0(|w_+\rangle)\,, \qquad (49)$$

$$\varphi_k^- = \chi_k(|w_-\rangle)/\chi_0(|w_+\rangle)\,, \qquad (50)$$

where we use the identity $\chi_0(|w_+\rangle) = \sqrt{2}\,\chi_0(|w_\alpha\rangle)$. The normalization factor $\chi_0(|w_+\rangle) = |\langle \mathbf{0}|w_+\rangle|$ determines the overlap and can be calculated by using Eq. (38). Separating the real and imaginary parts in the expansion (41), we have

$$\varphi_k^+ \simeq (-1)^k + 2\sum_{\ell=1}^{k}(-1)^{k-\ell}\xi_\ell\,, \tag{51}$$

$$\varphi_k^- \simeq i\delta\Big((-1)^k k + 2\sum_{\ell=1}^{k}(-1)^{k-\ell}(k-\ell)\xi_\ell\Big)\,, \tag{52}$$

where higher-order terms in δ are neglected. The j-th Fourier component of φ^+ is

$$\tilde{\varphi}_j^+ = \frac{2}{n(1+e^{ij\pi/n})}\sum_{k=0}^{n-1}\xi_k\Big(e^{ijk\pi/n}-(-1)^k\Big)$$
$$\simeq \frac{2}{1+e^{ij\pi/n}}\,|\langle\mathbf{0}|b_j\rangle|^2\,, \tag{53}$$

where $j \in J \equiv \{-n,\ldots,-2,0,2,\ldots,n\}$. Using the normalization condition (38), we have

$$\frac{1}{|\langle\mathbf{0}|w_+\rangle|^2} \simeq \sum_{j\in J'}\frac{|\tilde{\varphi}_j^+|^2}{|\langle\mathbf{0}|b_j\rangle|^2} \simeq \sum_{j\in J'}\frac{2\,|\langle\mathbf{0}|b_j\rangle|^2}{1+\cos(j\pi/n)}\,, \tag{54}$$

where $J' = J\backslash\{\pm n\}$ and the exponentially small term proportional to $|\tilde{\varphi}_n^+|^2$ is neglected. For $|j| \ll n$, we have

$$\frac{2}{1+\cos(j\pi/n)} \simeq 1+\pi^2\tau^2 \simeq e^{\pi^2\tau^2}\,, \tag{55}$$

where $\tau \equiv j/2n$. The squared fidelity $|\langle\mathbf{0}|b_j\rangle|^2$ can also be approximated by a Gaussian for $\tau \ll 1$,

$$|\langle\mathbf{0}|b_j\rangle|^2 = \frac{n!}{n_+!\,n_-!}\frac{1}{2^n} \simeq \frac{2e^{-2n\tau^2}}{\sqrt{2\pi n}}\,, \tag{56}$$

where $n_\pm = (n\pm j)/2 = n(1/2\pm\tau)$. The term in Eq. (55) modifies the variance of the Gaussian (56) by a factor of $2n/(2n-\pi^2)$, and thus we have

$$\sum_j \frac{2\,|\langle\mathbf{0}|b_j\rangle|^2}{1+\cos(j\pi/n)} \simeq \sqrt{\frac{2n}{2n-\pi^2}}\,, \tag{57}$$

where we used the condition $\sum_{j\in J'}|\langle\mathbf{0}|b_j\rangle|^2 \simeq 1$. Putting Eq. (57) into Eq. (54), we have

$$|\langle\mathbf{0}|w_+\rangle| \simeq \left(1-\pi^2/2n\right)^{1/4}\,, \tag{58}$$

which becomes arbitrarily close to 1 for large n, see Fig. 2(a) for a comparison to numerics.

To derive the fidelity $|\langle b_+|w_-\rangle|$, we notice

$$\varphi_k^- + \varphi_{k+1}^- = -i\delta\varphi_k^+\,, \tag{59}$$

which is proportional to the χ function of $|w_+\rangle$. Because $|w_+\rangle \simeq e^{-i\pi B/n}|w_+\rangle$, Eq. (59) implies that

$$|w_-\rangle \simeq \langle b_+|w_-\rangle|b_+\rangle - \frac{i\delta}{2}|w_+\rangle\,. \tag{60}$$

Thus, we can estimate the fidelity

$$|\langle b_+|w_-\rangle| \simeq 1-\delta^2/8\,, \tag{61}$$

which is exponentially close to 1 ($\delta^2 \sim N^{-1}$).

The value of δ, however, is only formally solved in Eq. (48). We still need to determine the value of d defined in Eq. (47). The Fourier component of φ^- corresponding to $|b_+\rangle$ is

$$\frac{1}{n}\sum_{k=0}^{n-1}(-1)^k\varphi_k^- = \frac{i\delta}{n}\sum_{k=0}^{n-1}(-1)^k\Big((-1)^k k + 2\sum_{\ell=1}^{k}(-1)^{k-\ell}(k-\ell)\xi_\ell\Big)$$
$$= \frac{i\delta}{n}\Big(\frac{1}{2}n(n-1)+2\sum_{\ell=1}^{n-1}\sum_{k=\ell}^{n-1}(-1)^\ell(k-\ell)\xi_\ell\Big)$$
$$= \frac{i\delta}{n}\Big(\frac{n^2}{2}+\sum_{\ell=1}^{n-1}(-1)^\ell(n-\ell)^2\xi_\ell - \frac{n}{2} - \sum_{\ell=1}^{n-1}(-1)^\ell(n-\ell)\xi_\ell\Big) = i\delta\big(d/n - n/N\big)\,, \tag{62}$$

where we used Eqs. (45) and (47) in the last step. By neglecting the higher order term in Eq. (62), we have

$$\langle b_+|w_-\rangle \simeq i\delta(d/n)\sqrt{N/2}\,|\langle\mathbf{0}|w_+\rangle|$$
$$\simeq i\,\sqrt{2d/n}\left(1-\pi^2/2n\right)^{1/4}\,. \tag{63}$$

where we used Eqs. (48) and (58). Comparing Eq. (63) with Eq. (61), we have

$$d \simeq \frac{n}{2}\left(1 - \pi^2/2n\right)^{-1/2}. \tag{64}$$

Putting this result into Eq. (48), we have

$$\delta \simeq 2\sqrt{2}\, N^{-1/2}\left(1 - \pi^2/2n\right)^{1/4}. \tag{65}$$

The argument of α thus takes the form

$$\arg(\alpha) \simeq 2\delta \simeq 4\sqrt{2}\, N^{-1/2}\left(1 - \pi^2/2n\right)^{1/4}, \tag{66}$$

which conforms with the numerical result in Fig. 3(a). Putting Eq. (65) into Eq. (61), we have the fidelity

$$|\langle\, b_+\,|\,w_-\,\rangle| \simeq 1 - N^{-1}, \tag{67}$$

where we drop the factor $(1 - \pi^2/2n)^{1/2}$, because it is of the same order as the approximation made in Eq. (60).

We calculate the fidelities $|\langle\, \mathbf{0}\,|\,w_+\,\rangle|$ and $|\langle\, b_+\,|\,w_-\,\rangle|$ numerically for $\gamma \neq \pi$ and find that they are always less than the corresponding values at $\gamma = \pi$. The alternating signs in $e^{i\gamma C}$ and $e^{-i\gamma C}$ are important for $\gamma \neq \pi$; the probability of finding the target state almost vanishes when the same sign are used (localized eigenstates).

VIII.   CHECK THE SOLUTION

Because the success probability of our algorithm is about $1/2$, it may not be very efficient to use a majority vote approach to find the marked bit string with high probability. Here, we describe a method to check whether the marked bit string has been found systematically.

Suppose that one has found the bit string $|\,s\,\rangle$ at the output of the circuit. Apply a $\pi/2$ pulse on an arbitrary qubit, creating an even superposition of the bit string $|\,s\,\rangle$ and a flipped bit sting $|\,s'\,\rangle$. Then apply the unitary $e^{i\pi C}$ to the system; this step flips the sign of the target bit string. Finally, apply a $-\pi/2$ pulse to the selected qubit and measure in the computational basis. One of the two bit stings $|\,s\,\rangle$ and $|\,s'\,\rangle$ must be the target if the measurement outcome is the bit sting $|\,s'\,\rangle$, otherwise, neither of the two bit strings is the target. To distinguish whether the bit string $|\,s\,\rangle$ or $|\,s'\,\rangle$ is the target, do the whole procedure over again on a different qubit.

IX.   CONCLUSION

Inspired by the QAOA proposed by Farhi *et al.* [1, 2], we present a circuit-based quantum algorithm to search for a needle in a haystack. We show that Grover's diffusion operator can be replaced by the transverse field, which only requires single-qubit gates, without sacrificing the quadratic quantum speedup. As single-qubit gates can usually be carried out much more efficiently than multi-qubit gates in practice, our algorithm offers a mild implementation advantage for Grover's unstructured search and its variants. This circuit model approach can take advantage of fault-tolerant error-correcting schemes; it is not known how, and could be impossible, to achieve fault tolerance in a purely adiabatic model [19].

We construct a simple periodic sequence of gates that induces a closed transition between two states which have large overlaps with the initial and the target states, respectively. The query complexity of our algorithm is $T(n) \simeq (\pi/2\sqrt{2})\, 2^{n/2}$, differing from the optimal value proved in [12] only by a constant factor of $\sqrt{2}$. Our algorithm provides the first example of a QAOA circuit that exhibits a quantum advantage at an intermediate number of iterations p, $p \gg 1$ and the algorithm is not derived from Trotterization of an AQO algorithm, demonstrating the breadth of the QAOA framework. It remains an open question whether QAOA circuits provide a quantum advantage for approximate optimization.

It is generally hard to find the optimal parameters in the QAOA when the number of iterations of the algorithm is large. Our work demonstrates that even simple periodic dynamics generated by the transverse field and the problem Hamiltonian can induce interesting transitions between a problem-independent state and an approximate target state. It offers a strategy to drastically simplify the optimization of the parameters in QAOA by restricting them to be periodic. For Grover's unstructured search, such simplification yields a near optimal solution to the problem. It will be interesting to see how well this strategy works for more general cases.

Our algorithm can be understood intuitively using a spin-coherent-state representation, where the weights of the basis states evolve in a simple way under the unitaries generated by the driver and the oracle. We also use a novel phase-space representation based on spin-coherent states to analyze the composite unitary in our algorithm. The eigenstates (up to normalization factors) of the composite unitary take explicit forms in this representation, and the eigenvalue equation can be readily derived using the periodic boundary condition. This enables us to solve the eigenstates and eigenvalues to exponential precision in n. It is worth exploring the extent to which such a representation is effective for more general quantum heuristic algorithms.

[1] Edward Farhi, Jeffrey Goldstone, and Sam Gutmann, "A Quantum Approximate Optimization Algorithm," arXiv:1411.4028 (2014).

[2] Edward Farhi, Jeffrey Goldstone, and Sam Gutmann, "A Quantum Approximate Optimization Algorithm Applied to a Bounded Occurrence Constraint Problem," arXiv:1412.6062 (2014).

[3] N. Goldman and J. Dalibard, "Periodically Driven Quantum Systems: Effective Hamiltonians and Engineered Gauge Fields," Physical Review X 4, 031027 (2014).

[4] Dave Wecker, Matthew B Hastings, and Matthias Troyer, "Training a quantum optimizer," Physical Review A 94, 022309 (2016).

[5] Edward Farhi and Aram W. Harrow, "Quantum Supremacy through the Quantum Approximate Optimization Algorithm," arXiv:1602.07674 (2016).

[6] John Preskill, "Quantum computing and the entanglement frontier," arXiv:1203.5813 (2012).

[7] Sergio Boixo, Sergei V. Isakov, Vadim N. Smelyanskiy, Ryan Babbush, Nan Ding, Zhang Jiang, John M. Martinis, and Hartmut Neven, "Characterizing Quantum Supremacy in Near-Term Devices," arXiv:1608.00263 (2016).

[8] Boaz Barak, Ankur Moitra, Ryan O'Donnell, Prasad Raghavendra, Oded Regev, David Steurer, Luca Trevisan, Aravindan Vijayaraghavan, David Witmer, and John Wright, "Beating the random assignment on constraint satisfaction problems of bounded degree," in APPROX-RANDOM (2015) pp. 110–123, arXiv:1505.03424.

[9] Lov K. Grover, "A Fast Quantum Mechanical Algorithm for Database Search," in Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing, STOC '96 (ACM, New York, NY, USA, 1996) pp. 212–219.

[10] C. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, "Strengths and Weaknesses of Quantum Computing," SIAM Journal on Computing 26, 1510–1523 (1997).

[11] Edward Farhi and Sam Gutmann, "Analog analogue of a digital quantum computation," Phys. Rev. A 57, 2403–2406 (1998).

[12] Christof Zalka, "Grover's quantum searching algorithm is optimal," Physical Review A 60, 2746–2751 (1999).

[13] Zijian Diao, M. Suhail Zubairy, and Goong Chen, "A Quantum Circuit Design for Grover's Algorithm," Zeitschrift für Naturforschung A 57, 701–708 (2014).

[14] Edward Farhi, Jeffrey Goldstone, Sam Gutmann, and Michael Sipser, "Quantum Computation by Adiabatic Evolution," arXiv:0001106 (2000).

[15] Sergei V. Isakov, Guglielmo Mazzola, Vadim N. Smelyanskiy, Zhang Jiang, Sergio Boixo, Hartmut Neven, and Matthias Troyer, "Understanding Quantum Tunneling through Quantum Monte Carlo Simulations," Physical Review Letters 117, 180402 (2016).

[16] Jérémie Roland and Nicolas J. Cerf, "Quantum search by local adiabatic evolution," Physical Review A 65, 042308 (2002).

[17] J. M. Radcliffe, "Some properties of coherent spin states," Journal of Physics A: General Physics 4, 313 (1971).

[18] Askold Perelomov, Generalized Coherent States and Their Applications (Springer Berlin Heidelberg, Berlin, Heidelberg, 1986).

[19] Kevin C. Young, Mohan Sarovar, and Robin Blume-Kohout, "Error suppression and error correction in adiabatic quantum computation: Techniques and challenges," Physical Review X 3, 041013 (2013).