A circuit-based quantum algorithm driven by transverse fields for Grover's problem

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: October 6, 2016)

We designed a quantum search algorithm, giving the same quadratic speedup achieved by Grover's original algorithm; we replace Grover's diffusion operator (hard to implement) with a product diffusion operator generated by transverse fields (easy to implement). In our algorithm, the problem Hamiltonian (oracle) and the transverse fields are applied to the system alternatively. We construct such a sequence that the corresponding unitary generates a closed transition between the initial state (even superposition of all states) and a modified target state, which has a high degree of overlap with the original target state. Let $N = 2^n$ be the size of the search space. The transition rate is of order $\mathcal{O}(1/\sqrt{N})$, and the overlap is of order $\mathcal{O}(1/\sqrt{n})$, yielding a $\mathcal{O}(\sqrt{N})$ algorithm up to $\log(N)$ factors. Our algorithm belongs to a class of algorithms proposed by Farhi *et al.* [1–3], namely the Quantum Approximate Optimization Algorithm (QAOA).

I. INTRODUCTION

Grover's algorithm searches for a specified entry in an unstructured database, achieving a quadratic speedup over the best classical algorithms [4]. It is optimal for any quantum algorithm performing such a task [5]. Searching for an unique element in an unstructured database has many applications, such as the problem of boolean satisfiability (SAT). The time complexity of Grover's algorithm is $\Theta(\sqrt{N})$, offering a modest quadratic speedup over any classical counterpart, however, even quadratic speedup is considerable when N is large. If there are t solutions then Grover's algorithm can be modified to find all the answers with time complexity $\Theta(\sqrt{N/t})$ [6]. Grover's algorithm is probabilistic in the sense that it gives the correct answer with a probability of less than 1. To get the error probability down to ϵ one can do $\mathcal{O}(\log(1/\epsilon))$ repetitions (does not grow with N) and output the most frequent outcome.

Recently, Farhi *et al.* [1–3] proposed a new class of algorithms—the Quantum Approximate Optimization Algorithm (QAOA)—to tackle with challenging combinatorial optimization problems. In such algorithms, a mixing term (usually the transverse field) and the problem Hamiltonian are implemented alternatively to the system; the time sequence of implementing the two Hamiltonians are optimized, such that the averaged performance of the algorithm—measured by the expectation value of the problem Hamiltonian at the output—is minimized (or maximized).

Inspired by the circuits used in QAOA, we propose a quantum algorithm based on the principle of amplitude amplification to search a unique entry in an unstructured database consist of n qubits ($N = 2^n$). In our algorithm, the mixing term and the problem Hamiltonian are applied to the system alternatively; the time sequence of applying these Hamiltonians are selected carefully such that it generates a closed transition between the initial state (even superposition of all bit strings) and a modified target state, which has a high degree of overlap with the original target state. The transition rate is of order $\mathcal{O}(1/\sqrt{N})$, and the overlap is large $\mathcal{O}(1/\sqrt{n})$, yielding a $\mathcal{O}(\sqrt{N})$ algorithm up to $\log(N)$ factors.

II. GROVER'S ALGORITHM

Grover's algorithm has attracted many attentions by affirmatively demonstrating that a quantum computer can outperform any classical computer. A technique known as amplitude amplification is used in Grover's algorithm, which then inspired a class of quantum algorithms. The key to such technique is to selectively shift the phase of the particular quantum state given by the oracle, at each iteration. The amplitude of that state changes after the phase shift, however, the probability the system being in that state is unchanged. Subsequent operations on the system take advantage of the difference in amplitude to increase the probability of the system being in that state. This would be impossible if the amplitudes did not hold the extra phase information in addition to the probability. Amplitude amplification is unique to quantum computing because it has no analog in classical probabilities. Our algorithm is based on this principle.

A crucial component of Grover's algorithm is the Grover's diffusion operator. Such operator adds a phase of π to the even superposition state (same amplitude for all the basis states) and does nothing to all the orthogonal states. The Grover diffusion operator is quite hard to implement in a quantum circuit, because it correlates all the qubits under consideration. It requires $\mathcal{O}(\log N)$ two-qubit gates to implement the Grover's diffusion operator [7]. This is a drawback in practice, because two-

[*] zhang.jiang@nasa.gov

qubit gates are very expansive. One way to circumvent that difficulty is to use a transverse field (acting only on individual qubits) instead of Grover's diffusion operator. The same quadratic speedup in Grover's algorithm is believed to be achievable in Adiabatic Quantum Computation (AQC) [8, 9], where the a transverse filed is gradually replaced by the problem Hamiltonian that encodes the answer. A natural question to ask is whether it is possible to implement quantum search in the circuit model only using the transverse field. Here, we give an affirmative answer to this question.

III. PROBLEM SETUP

Suppose we are given a problem Hamiltonian (oracle)

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

that encodes an unknown bit string $\boldsymbol{\mu}$ of length n (n is even for simplicity). Our aim is to find out $\boldsymbol{\mu}$ using as few as possible calls of the oracle. We will also use the following transverse field operator

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

where X_j is the Pauli-X operator on the j-th qubit. The advantage of using the B operator over Grover's diffusion operator is that B (acts only on individual spins) is much easier to implement. The input state of our algorithm is the $+1$ eigenstate of all the X_j operators

$$|\,\Psi_0\,\rangle = \frac{1}{\sqrt{N}} \sum_{\boldsymbol{\nu}\in\{0,1\}^n} |\,\boldsymbol{\nu}\,\rangle = |+\rangle^{\otimes n}\,. \tag{3}$$

The unitary operator that flips a subset of qubits $S \subseteq \{1, 2, \ldots, n\}$ reads

$$F_S = F_S^{\dagger} = \prod_{j\in S} X_j\,. \tag{4}$$

Letting S be the set of bits whose value is 0 in the bit string $\boldsymbol{\mu}$, we have

$$F_S|\,\boldsymbol{\mu}\,\rangle = |\,\mathbf{1}\,\rangle\,, \quad F_S\,C_{\boldsymbol{\mu}}F_S^{\dagger} = C_{\mathbf{1}}\,, \tag{5}$$

where $\mathbf{1} \equiv (1, 1, \ldots, 1)$. Because F_S commutes with B and stabilizes the initial state $|\,\Psi_0\,\rangle$, it can be used to convert our problem of finding the bit string $\boldsymbol{\mu}$ to finding the bit string $\mathbf{1}$ with the oracle $C_{\mathbf{1}}$ and the operator B. This drastically simplified our problem, because one only needs to consider the symmetric subspace of dimension $n+1$ instead of the whole Hilbert space of dimension 2^n. To simplify notation, we will omit the subscript in $C_{\mathbf{1}}$ thereafter, i.e., $C \equiv C_{\mathbf{1}}$.

To find the target bit string $\mathbf{1}$, we construct a unitary—described by a sequence of elementary unitaries generated by B and C—such that it drives a closed transition between the initial state $|\,\Psi_0\,\rangle$ and a modified target state $|\,\Psi_1\,\rangle$ which has a big overlap with $|\,\mathbf{1}\,\rangle$. We choose the state $|\,\Psi_1\,\rangle$ as the eigenstate of B with eigenvalue 0 (for even n),

$$|\,\Psi_1\,\rangle \propto P_{\text{sym}}\Big(|+\rangle^{\otimes\frac{n}{2}} \otimes |-\rangle^{\otimes\frac{n}{2}}\Big)\,, \tag{6}$$

where P_{sym} is the projector into the symmetric subspace. The probability that one finds the target state $|\,\mathbf{1}\,\rangle$ with $|\,\Psi_1\,\rangle$ is

$$|\langle\,\mathbf{1}\,|\,\Psi_1\,\rangle|^2 = \frac{n!}{(n/2)!(n/2)!}\,\frac{1}{2^n} \simeq \sqrt{\frac{2}{\pi n}}\,, \tag{7}$$

which scales as $1/\sqrt{n}$. Thus, one simply needs to repeat the experiment for order $\sqrt{n}$ times to find the target state with high probability.

IV. SPIN COHERENT STATES

It turns out that spin coherent states [10, 11] is especially convenient for our problem. We will only need spin coherent states on the Y-Z plane,

$$\Psi(\theta) = e^{-i\theta B/2}|\,\mathbf{1}\,\rangle\,, \tag{8}$$

where $\theta \in [\,0, 2\pi)$. These states already form an overcomplete basis for the symmetric subspace. We pay particular attention to a set of discrete values of angles $\theta = k\Delta\theta$, where $k = 0, 1, \ldots, n-1$ is an integer and $\Delta\theta = 2\pi/n$. Note that these n spin coherent states do not form a complete basis of the symmetric subspace (with dimension $n+1$). The modified target state $|\,\Psi_1\,\rangle$ can be represented using these discrete spin coherent states,

$$|\,\Psi_1\,\rangle = \frac{1}{a_1}\sum_{k=0}^{n-1} e^{-ik\pi B/n}|\,\mathbf{1}\,\rangle\,, \tag{9}$$

where the normalization factor is

$$a_1 = \sum_{k=0}^{n-1}\langle\,\Psi_1\,|e^{-ik\pi B/n}|\,\mathbf{1}\,\rangle = n\langle\,\Psi_1\,|\,\mathbf{1}\,\rangle \sim n^{3/4}\,. \tag{10}$$

We will need the following states

$$|\,\Psi_0^{\pm}\,\rangle = \frac{1}{\sqrt{2}}\Big(|\,\Psi_0\,\rangle \pm |\,\bar{\Psi}_0\,\rangle\Big) \tag{11}$$

where $|\,\bar{\Psi}_0\,\rangle = |-\rangle^{\otimes n}$. While $\langle\,\Psi_0^-\,|e^{-ik\pi B/n}|\,\mathbf{1}\,\rangle = 0$ for all integer k, $|\,\Psi_0^+\,\rangle$ has the representation

$$|\,\Psi_0^+\,\rangle = \frac{1}{a_0}\sum_{k=0}^{n-1}(-1)^k e^{-ik\pi B/n}|\,\mathbf{1}\,\rangle\,, \tag{12}$$

where the normalization factor is

$$a_0 = n\,\langle\,\Psi_0^+\,|\,\mathbf{1}\,\rangle = \sqrt{2}\,n\,\langle\,\Psi_0\,|\,\mathbf{1}\,\rangle \sim \frac{n}{\sqrt{N}}\,, \tag{13}$$

which is exponentially small. From Eqs. (9) and (11), one can verify the following eigenvalue equations

$$e^{-i\pi B/n}|\,\Psi_0^{\pm}\,\rangle = -|\,\Psi_0^{\pm}\,\rangle\,, \quad e^{-i\pi B/n}|\,\Psi_1\,\rangle = |\,\Psi_1\,\rangle\,. \tag{14}$$

For any state $|\,\Psi\,\rangle$ and a small angel γ, we have

$$\begin{aligned} e^{-i\gamma C}|\,\Psi\,\rangle &= |\,\Psi\,\rangle + \big(e^{i\gamma}-1\big)\langle\,\mathbf{1}\,|\,\Psi\,\rangle|\,\mathbf{1}\,\rangle \\ &= |\,\Psi\,\rangle + i\gamma\,\langle\,\mathbf{1}\,|\,\Psi\,\rangle|\,\mathbf{1}\,\rangle + \mathcal{O}(\gamma^2)\,. \end{aligned} \tag{15}$$

V. THE ALGORITHM

Having equipped with the basics of the spin-coherent state representation, we introduce the unitary that is close in the subspace spanned by $|\,\Psi_0^{\pm}\,\rangle$ and $|\,\Psi_1\,\rangle$. We introduce the following unitary

$$U_\gamma = \big(e^{-i\pi B/n}e^{i\gamma C}e^{-i\pi B/n}e^{-i\gamma C}\big)^{n/2}\,, \tag{16}$$

where γ is a small angle. Using the first identity in Eq. (14) and noticing $e^{-i\gamma C}|\,\Psi_0^-\,\rangle = |\,\Psi_0^-\,\rangle$, we have

$$U_\gamma|\,\Psi_0^-\,\rangle = |\,\Psi_0^-\,\rangle\,. \tag{17}$$

We also notice that

$$\begin{aligned} U_\gamma|\,\Psi_0^+\,\rangle &\simeq |\,\Psi_0^+\,\rangle + i\gamma\,\langle\,\mathbf{1}\,|\,\Psi_0^+\,\rangle\sum_{k=0}^{n-1}e^{-ik\pi B/n}|\,\mathbf{1}\,\rangle \\ &= |\,\Psi_0^+\,\rangle + i\gamma n\,\langle\,\mathbf{1}\,|\,\Psi_0^+\,\rangle\langle\,\Psi_1\,|\,\mathbf{1}\,\rangle\,|\,\Psi_1\,\rangle\,, \end{aligned} \tag{18}$$

and

$$\begin{aligned} U_\gamma|\,\Psi_1\,\rangle &\simeq |\,\Psi_1\,\rangle + i\gamma\,\langle\,\mathbf{1}\,|\,\Psi_1\,\rangle\sum_{k=0}^{n-1}(-1)^k e^{-ik\pi B/n}|\,\mathbf{1}\,\rangle \\ &= |\,\Psi_1\,\rangle + i\gamma n\,\langle\,\mathbf{1}\,|\,\Psi_1\,\rangle\langle\,\Psi_0^+\,|\,\mathbf{1}\,\rangle\,|\,\Psi_0^+\,\rangle\,. \end{aligned} \tag{19}$$

Thus, the unitary U_γ drives a closed transition between $|\,\Psi_0^+\,\rangle$ and $|\,\Psi_1\,\rangle$, and the transition rate is

$$r = \gamma n\,\langle\,\mathbf{1}\,|\,\Psi_1\,\rangle\langle\,\Psi_0^+\,|\,\mathbf{1}\,\rangle \simeq \sqrt[4]{2/\pi}\,\gamma\,n^{3/4}N^{-1/2}\,. \tag{20}$$

Applying the unitary U_γ for $M = \lfloor\pi/2r\rfloor$ times on the initial state $|\,\Psi_0\,\rangle$, we have

$$|\,\Psi_{\rm out}\,\rangle = U_\gamma^M|\,\Psi_0\,\rangle \simeq \frac{1}{\sqrt{2}}\Big(|\,\Psi_1\,\rangle + |\,\Psi_0^-\,\rangle\Big)\,. \tag{21}$$

Because $\langle\,\mathbf{1}\,|\,\Psi_0^-\,\rangle = 0$, the probability that we find the target state $|\,\mathbf{1}\,\rangle$ in the output state is

$$P_{\mathbf{1}} \simeq |\langle\,\mathbf{1}\,|\,\Psi_1\,\rangle|^2/2 \simeq 1/\sqrt{2\pi n}\,. \tag{22}$$

The success of our algorithm, however, is based on the assumption that γ is small; we still need to know how small that γ should be. The whole algorithm could be slower than its classical counterparts if γ was exponentially small. A crucial criteria to choose γ is that the output state $|\,\Psi_{\rm out}\,\rangle$ should be mainly in the subspace spanned by $|\,\Psi_0^{\pm}\,\rangle$ and $|\,\Psi_1\,\rangle$. This condition can be translated to

$$\big(e^{-ik\pi B/n} - I\big)|\,\Psi_{\rm out}\,\rangle \simeq 0\,, \tag{23}$$

for $k = 0, 2, \ldots, n-2$. The condition (23) says that the output state $|\,\Psi_{\rm out}\,\rangle$ does not change under rotations by any angle that is a multiple of π/n, and a simple way to guarantee that is to set $\gamma \lesssim 1/\sqrt{n}$. In Appendix B, we argue that our algorithm even works for γ of order $\Theta(1)$.

To "find" the bit string $\mathbf{1}$ in the output, we can apply the unitary $e^{-i\theta B/2}$ with a random angle $\theta \in [0, 4\pi/n)$. This step maps the output state to a mixed state of $|\,\Psi_0\,\rangle\langle\,\Psi_0\,|$, $|\,\bar{\Psi}_0\,\rangle\langle\,\bar{\Psi}_0\,|$, and $|\,\Psi_1\,\rangle\langle\,\Psi_1\,|$. One then makes a measurement in the computational basis. For roughly half of the times, he get a random string due to the contributijon from $|\,\Psi_0\,\rangle$ and $|\,\bar{\Psi}_0\,\rangle$. For the other half times, he finds the solution with a polynomially small probability $\mathcal{O}(1/\sqrt{n})$. He then test the result by applying a $\pi/2$ pulse on an arbitrary qubit, creating an even superposition of the initial bit string and a flipped bit sting. Then he applies the unitary $e^{i\pi C}$ to the system, this step flips the sign of the target bit string. He then apply a $-\pi/2$ pulse and measure in the computational basis. One of the two bit stings must be the target if he finds the measurement outcome is the flipped bit sting. Otherwise, neither of the two bit strings is the target. To distinguish the two possible target bit strings, he only needs to flip another qubit in the initial bit string.

The complexity of our algorithm is $\Theta\big(n\sqrt{n}\,M\big)$, or equivalently, $\Theta\big(n^{3/4}N^{1/2}\big)$. While the scaling of $N^{1/2}$ cannot be be improved, the scaling of n might be improved.

VI. ROBUSTNESS

We have assumed that the implementation of the quantum gates are perfect, however, no quantum gate is perfect in reality. One of the most detrimental noise in our algorithm is the uncertainly in the transverse field B. This kind of noises destroy the relative phase between the states $|\,\Psi_0^+\,\rangle$ and $|\,\Psi_1\,\rangle$. Because our algorithm engages amplitude amplification, it stops working when phase coherence is destroyed. It is crucial to design a method to stabilize the relative phase of the two states, and quantum control might be useful for that purpose.

Another kind of important noises is decoherence on individual spins. There is no easy way to deal with these noises without a fault-tolerant computer, and one simply need to finish the computation before the qubit decohered. Luckily for us, we only need deal with two very special states. Maybe there is a way to find a decoherence free subspace for the two states.

VII. CONCLUSION

We have proposed a quantum algorithm to search a unique entry in an unstructured database using amplitude amplification. We show that Grover's diffusion operator can be replaced by the transverse field without sacrificing the quadratic speedup. Although this modification does not offer more insights to complexity theory, it is important to the realization of the quantum search algorithms as single-qubit gates can usually be implemented much more precisely and faster than multi-qubit gates. Our algorithm is based on constructing a closed transition between the initial state and a modified target state; the probability of finding the solution in the modified target state is $\mathcal{O}(1/\sqrt{n})$. In Grover's algorithm, one has to change the basis back and forth to implement the diffusion term and the oracle term. Our algorithm does not require changing between basis, and thus might be easier to made more robust to errors. It is also interesting to compare our algorithm to AQC, since the same elements are used therein. A potential advantage of using circuit model instead of the adiabatic model is the flexibility of implementing quantum error-correcting and control protocols.

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

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

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

[4] 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.

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

[6] Michel Boyer, Gilles Brassard, Peter Hyer, and Alain Tapp, "Tight Bounds on Quantum Searching," Fortschritte der Physik **46**, 493–505 (1998).

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

[8] Kostyantyn Kechedzhi and Vadim N. Smelyanskiy, "Open-System Quantum Annealing in Mean-Field Models with Exponential Degeneracy," Physical Review X **6**, 021028 (2016).

[9] Zhang Jiang, Vadim N. Smelyanskiy, Sergei V. Isakov, Sergio Boixo, Guglielmo Mazzola, Matthias Troyer, and Hartmut Neven, "Scaling analysis and instantons for thermally-assisted tunneling and Quantum Monte Carlo simulations," arXiv:1603.01293 (2016).

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

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

Appendix A: Phase space representations

Any state in the symmetric subspace can be uniquely determined by its inner products with spin coherent states, and we introduce the following representation of a quantum state $|\,\Psi\,\rangle$ in the symmetric subspace,

$$\chi\big(|\,\Psi\,\rangle,\theta\big) = \langle\,\mathbf{1}\,|e^{i\theta B/2}|\,\Psi\,\rangle\,. \tag{1}$$

The χ function fully determines the state $|\,\Psi\,\rangle$, since the spin-coherent states $e^{-i\theta B/2}\,|\,\mathbf{1}\,\rangle$ for $\theta \in [\,0,2\pi)$ are overcomplete. Its advantage is to represent both the B and C operations in concise forms. For the initial state in Eq. (3), we have

$$\chi\big(|\,\Psi_0\,\rangle,\theta\big) = \langle\,\mathbf{1}\,|e^{i\theta B/2}|\,\Psi_0\,\rangle = \frac{e^{-in\theta/2}}{\sqrt{N}}\,. \tag{2}$$

For the modified target state $|\,\mathbf{1}\,\rangle$, we have

$$\chi\big(|\,\mathbf{1}\,\rangle,\theta\big) = \langle\,\mathbf{1}\,|e^{i\theta B/2}|\,\mathbf{1}\,\rangle = \cos(\theta/2)^n\,. \tag{3}$$

Note that $\chi\big(|\,\mathbf{1}\,\rangle,\theta\big)$ is peaked at $\theta = 0$, whose width is of order $1/\sqrt{n}$. It is convenient to represent the unitary $e^{-i\phi B/2}$ using the χ function,

$$\chi\big(e^{-i\phi B/2}|\,\Psi\,\rangle,\theta\big) = \chi\big(|\,\Psi\,\rangle,\theta-\phi\big)\,. \tag{4}$$

The action of the unitary generated by C on an arbitrary state is also simple

$$\begin{aligned}&\chi\big(e^{-i\gamma C}|\,\Psi\,\rangle,\theta\big)\\ &\quad= \chi\big(|\,\Psi\,\rangle,\theta\big) + (e^{i\gamma}-1)\cos(\theta/2)^n\,\chi\big(|\,\Psi\,\rangle,0\big)\,.\end{aligned} \tag{5}$$

For $\theta = 2k\pi/n$, we use the following notation for the χ function,

$$\chi_k\big(|\,\Psi\,\rangle\big) = \langle\,\mathbf{1}\,|e^{ik\pi B/n}|\,\Psi\,\rangle\,. \tag{6}$$

For $k = n$ (n even), we have

$$\begin{aligned}\chi_n\big(|\,\Psi\,\rangle\big) &= \langle\,\mathbf{1}\,|e^{i\pi B}|\,\Psi\,\rangle\\ &= (-1)^n\langle\,\mathbf{1}\,|\,\Psi\,\rangle = \langle\,\mathbf{1}\,|\,\Psi\,\rangle = \chi_0\big(|\,\Psi\,\rangle\big)\,.\end{aligned} \tag{7}$$

We will use the relation

$$\chi_k\big(e^{-i\pi B/n}|\,\Psi\,\rangle\big) = \chi_{k-1}\big(|\,\Psi\,\rangle\big)\,. \tag{8}$$

For the initial state, we have

$$\chi_k\big(|\,\Psi_0\,\rangle\big) = \chi_k\big(|\,\bar{\Psi}_0\,\rangle\big) = \frac{(-1)^k}{\sqrt{N}}\,, \tag{9}$$

where $|\,\bar{\Psi}_0\,\rangle = |\,-\,\rangle^{\otimes n}$. The above equation says that the values $\chi_1, \chi_2, \ldots, \chi_{n-1}$ do not uniquely determine a quantum state in the symmetric subspace, because the dimension of the Hilbert space is $n+1$. Since the state $|\,\Psi_1\,\rangle$ remain the same under the rotation $e^{-i\theta B/2}$, its χ function is simply

$$\chi_k\big(|\,\Psi_1\,\rangle\big) = \chi_0\big(|\,\Psi_1\,\rangle\big) \simeq \sqrt[4]{2/\pi n}\,. \tag{10}$$

Appendix B: Large angles

Here, we discuss the case of large γ with the representation introduced in Section A. The advantage of using larger γ is to shorten the circuit depth as well as reducing implementation errors.

We will need the elementary building block of our algorithm,

$$V_\gamma = e^{-i\pi B/n} e^{i\gamma C} e^{-i\pi B/n} e^{-i\gamma C}\,, \tag{1}$$

where γ is not necessary small. Applying V_γ for ℓ times on the state $|\,\Psi_0^+\,\rangle$, we have

$$|\,\Phi_\ell\,\rangle = V_\gamma^\ell |\,\Psi_0^+\,\rangle\,. \tag{2}$$

where ℓ is a positive integer. Because V_γ commutes with V_γ^ℓ, we have

$$\big|\big(V_\gamma^k - I\big)|\,\Phi_\ell\,\rangle\big| = \big|\big(V_\gamma^k - I\big)|\,\Psi_0^+\,\rangle\big| \sim 1/\sqrt{N}\,, \quad \forall \ell\,, \tag{3}$$

where $k = 1, \ldots n-1$. For any normalized state $|\,\Psi\,\rangle$, we have

$$\langle\,\Psi\,|\big(V_\gamma^k - I\big)|\,\Phi_\ell\,\rangle \sim 1/\sqrt{N}\,, \quad \forall \ell\,. \tag{4}$$

Using the phase space representation, it can be proved that $\langle\,\Psi\,|\big(V_\gamma^k - I\big)|\,\Psi\,\rangle \gtrsim 1/n$ if the normalized state $|\,\Psi\,\rangle$ is orthogonal to both $|\,\Psi_0^\pm\,\rangle$ and $|\,\Psi_1\,\rangle$. Thus, the output state can only have exponentially small support in that subspace. The transition rate between the state $|\,\Psi_0^+\,\rangle$ and $|\,\Psi_1\,\rangle$ can be calculated by using the phase space representation.