Deterministic Grover search with a restricted oracle

Tanay Roy[1]* and Liang Jiang[2], David I. Schuster[1]
[1]*Department of Physics and James Franck Institute, University of Chicago, Chicago, Illinois 60637, USA and*
[2]*Pritzker School of Molecular Engineering, University of Chicago, Chicago, Illinois 60637, USA*
(Dated: January 4, 2022)

Grover's quantum search algorithm provides a quadratic quantum advantage over classical algorithms across a broad class of unstructured search problems. The original protocol is probabilistic, returning the desired result with significant probability on each query, but in general, requiring several iterations of the algorithm. We present a modified version to return the correct result with certainty without having user control over the quantum search oracle. Our deterministic, two-parameter "D2p" protocol utilizes generalized phase rotations replacing the phase inversions after a standard oracle query. The D2p protocol achieves a 100% success rate in no more than one additional iteration compared to the optimal number of steps in the original Grover's search enabling the same quadratic speed up. We also provide a visualization using the Bloch sphere for enhanced geometric intuition.

I. INTRODUCTION

An efficient algorithm to search a large unstructured search space has a wide range of applications. While the time complexity of a classical search algorithm scales linearly with the size of the space, Grover's quantum search algorithm [1] provides a quadratic speedup. Though the quantum advantage is not exponential as in some quantum algorithms it can be applied very broadly, to any problem whose result can be verified efficiently. The search is performed by an "oracle", a quantum algorithm that the user may not have access to. The oracle could be a quantum random access memory [2, 3] to access an unstructured classical or quantum database. Alternatively, the oracle could be a quantum version of a one-way function such as a hash, symmetric key encryption, or number theory conjecture, etc. Given a space with N unsorted inputs and quantum oracle that identifies M marked states, Grover's search algorithm is guaranteed to produce better than 50% success probability with $\mathcal{O}(\sqrt{N/M})$ oracle queries, whereas a classical algorithm needs on average $N/(2M)$ interrogations.

Grover's algorithm is composed of two steps — the oracle query, which flips the phase of the marked states, and the application of the diffusion operator (also known as the reflection or inversion operator) that amplifies the amplitude of the marked states. In the original protocol [1], both steps use a phase-flip operator that restricts the evolution of the initial superposition state in a way that the success is probabilistic. One can achieve the target state with certainty by controlling the phases of the phase-flip and diffusion operators when the ratio $\lambda = M/N$ is known [4]. Other works aim to improve the success rate for an unknown λ (with a modest guess of the lower bound) by performing multi-phase matching [5–7]. However, these protocols require one to control the phase of the oracle, which might not always be plausible as the user may not have knowledge of or access to the oracle. Practically, the search oracle should be treated as a fixed unitary determined by some physical process with no user-tunable parameters.

In this work, we present an algorithm to find a marked state *deterministically* with the constraint that the user does not have control over the oracle phase. We show that only two phase parameters for the consecutive diffusion operators are sufficient to find a target state with certainty by making $k_{\text{opt}} = \left\lceil \frac{\pi}{4\sin^{-1}\sqrt{\lambda}} - \frac{1}{2} \right\rceil$ oracle queries for a given λ.

II. OVERVIEW OF GROVER'S ALGORITHM

The original Grover's algorithm constitutes of successive application of the oracle and diffusion operators on the initial equal-superposition state (containing mostly unmarked states) that is transformed into a superposition of mostly marked states. Assuming $N = 2^n$ as the number of total states, one can prepare an equal-superposition state $|\psi_0\rangle$ by applying a Walsh-Hadamard transformation individually to all the qubits initiated to $|0\rangle$. Instead of using the full 2^n-dimensional Hilbert space, it is more convenient to map the system to a two-dimensional sub-space spanned by the orthogonal vectors $|T\rangle$ and $|R\rangle$, where $|T\rangle\,(|R\rangle)$ represents the equal-superposition of all marked (unmarked) states $|t_j\rangle\,(|r_j\rangle)$,

$$|T\rangle = \frac{1}{\sqrt{M}} \sum_{j=1}^{M} |t_j\rangle\,, \tag{1a}$$

$$|R\rangle = \frac{1}{\sqrt{N-M}} \sum_{j=1}^{N-M} |r_j\rangle\,. \tag{1b}$$

* Corresponding author: roytanay@uchicago.edu

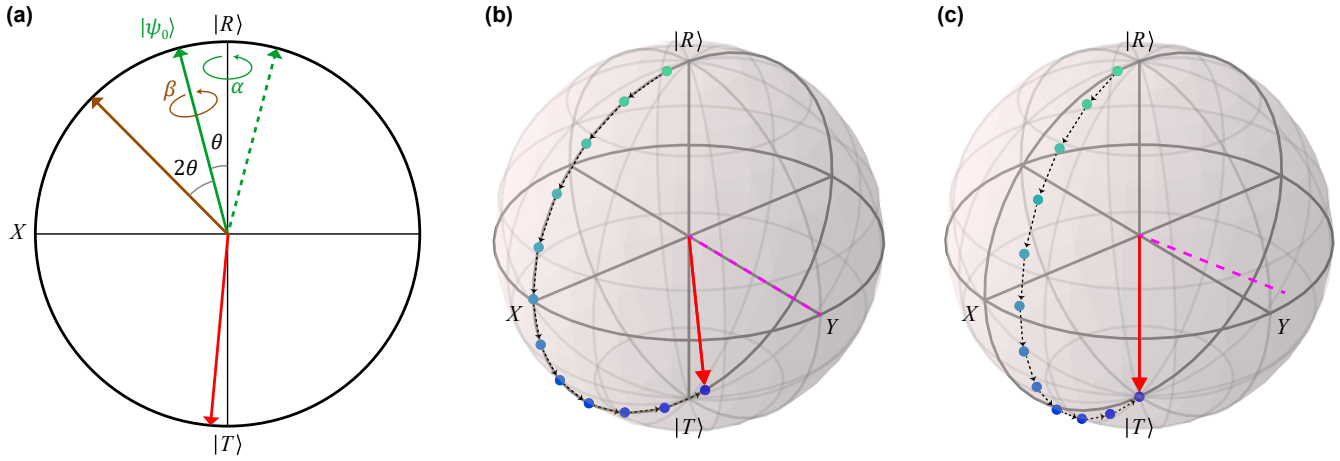

FIG. 1. Trajectory of the state vector on a Bloch sphere spanned by the equal-superposition of marked states $|T\rangle$ (south pole) and unmarked states $|R\rangle$ (north pole). (a) The initial equal superposition state $|\psi_0\rangle$ (solid green arrow) makes a polar angle θ determined by the ratio of marked to unmarked state counts λ. The plane containing the vectors $|\psi_0\rangle$ and $|R\rangle$ is assumed to be the ZX plane of the Bloch sphere. The generalized oracle operator $S_0(\alpha)$ (see Eq. (3)) rotates the state vector about z-axis by an angle α. Similarly, the generalized reflection operator $S_r(\beta)$ (see Eq. (4)) performs a rotation of the state vector about the direction of $|\psi_0\rangle$ by an angle β. The oracle in the original Grover's algorithm with $\alpha = \pm\pi$ flips the phase of $|T\rangle$ resulting in the dashed green vector and then the reflection operator (with $\beta = \pm\pi$) inverts the state with respect to $|\psi_0\rangle$ leading to the brown vector when starting from $|\psi_0\rangle$. As a result, a single Grover iterate effectively rotates the state vector by 2θ about the y-axis in each iteration. (b) Consequently, the trajectory of the state vector is always confined in the ZX plane, perpendicular to the y-axis (dashed magenta line) in the original Grover's algorithm and the final state (red arrow) doesn't always end up along the south pole after an integer number of steps. (c) The protocol in Ref. 4 achieves zero theoretical failure rate by rotating the state vector in a plane such that it always lands along the south pole. The corresponding axis of rotation (dashed magenta line) is carefully chosen and doesn't lie along the y-axis in general. In this case, the user is assumed to have control over both the oracle and the reflection operator steps so that one can set $\alpha = \beta = \theta_0$ (see Eq. (6)).

Then the initial state can be expressed in the new basis $|R\rangle = \binom{1}{0}$ and $|T\rangle = \binom{0}{1}$ as

$$|\psi_0\rangle = \sqrt{1-\lambda}\,|R\rangle + \sqrt{\lambda}\,|T\rangle = \begin{pmatrix}\sqrt{1-\lambda}\\ \sqrt{\lambda}\end{pmatrix}. \tag{2}$$

The evolution of $|\psi_0\rangle$ can be visualized as a moving unit vector on the Bloch sphere spanned by $|R\rangle$ (north pole) and $|T\rangle$ (south pole) as shown in Fig. 1(a). The initial state (solid green arrow) lies in the ZX plane making an angle $\theta = 2\sin^{-1}\sqrt{\lambda}$ with the z-axis. The oracle is a unitary operator

$$S_o(\alpha) = I - (1-e^{i\alpha})\,|T\rangle\langle T| = \begin{pmatrix}1 & 0\\ 0 & e^{i\alpha}\end{pmatrix} \tag{3}$$

representing a generalized controlled-phase gate — rotation of the vector about z-axis by an angle α with I being the identity operator. The special case of $S_o(\pi)$ on $|\psi_0\rangle$ can be simply thought as a reflection with respect to the vertical axis.

Next, we define the generalized Grover's reflection following the convention used in Ref. 6 (up to a global phase)

$$\begin{aligned} S_r(\beta) &= e^{i\beta}\left(I - (1-e^{-i\beta})\,|\psi_0\rangle\langle\psi_0|\right)\\ &= \begin{pmatrix} 1-(1-e^{i\beta})\lambda & (1-e^{i\beta})\sqrt{\lambda(1-\lambda)}\\ (1-e^{i\beta})\sqrt{\lambda(1-\lambda)} & 1-(1-e^{i\beta})(1-\lambda)\end{pmatrix}, \end{aligned} \tag{4}$$

which represents a rotation of the state about $|\psi_0\rangle$ by an angle β (see Fig. 1(a)). The product of the oracle and the reflection operator is often called the Grover's iterate $G(\alpha,\beta) = -S_r(\beta)S_o(\alpha)$. The original Grover's iterate with $\alpha = \pm\pi$ and $\beta = \pm\pi$ rotates the state vector by 2θ about the y-axis (dashed pink line in Fig. 1(b)), restricting the trajectory in the ZX plane. Since the angular distance of $|\psi_0\rangle$ from the south pole is $\pi - \theta$, the number of steps needed to reach $|T\rangle$ becomes $(\pi-\theta)/(2\theta)$, which is, in general, a fractional number. Therefore, the optimal number of steps for the original Grover's search becomes the nearest integer [4]

$$k'_{\rm opt} = \left\lfloor \frac{\pi}{2\theta} - \frac{1}{2} \right\rfloor = \left\lfloor \frac{\pi}{4\sin^{-1}\sqrt{\lambda}} - \frac{1}{2} \right\rfloor. \tag{5}$$

In general the final state vector (red arrow in Fig. 1 (b)) will not always align with south pole providing a maximum success probability of $\sin[(k'_{\rm opt}+1/2)\theta]^2$. This situation of undershooting (overshooting) the target state is often called "undercooking (overcooking)". One can, however, cleverly choose a different plane of rotation so that the final state always lands on the south pole in $k \geq k_{\rm opt}$ steps as shown in Fig. 1 (c). The corresponding Grover's iterate needs $\alpha = \beta = \theta_0$ with [4]

$$\theta_0 = 2\sin^{-1}\left(\frac{1}{\sqrt{\lambda}}\sin\left(\frac{\pi}{4k+2}\right)\right), \tag{6}$$

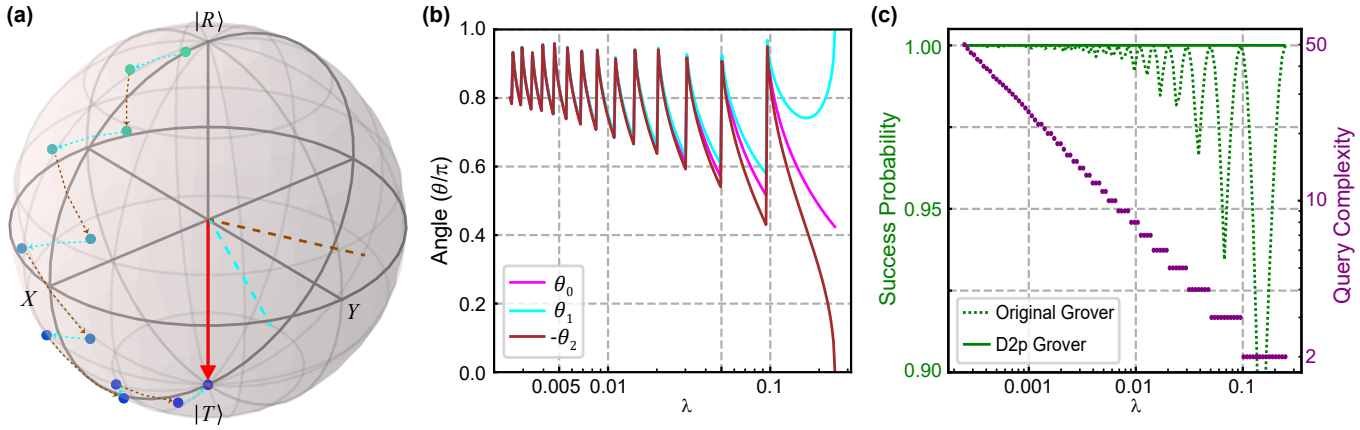

FIG. 2. The D2p Grover's search protocol. (a) The state vector is rotated about two axes (cyan and brown dashed lines) alternatively by amounts θ_1 and θ_2. One can always find parameters $\{\theta_1, \theta_2\}$ such that the final state (red arrow) ends up along the south pole providing zero failure rate for $\lambda \leq 1/4$ when the number of iterations $k \geq k_{\rm opt}$. (b) The values of θ_1 (cyan curve) and θ_2 (brown curve) are plotted as a function of λ obtained by numerically solving Eq. (8) when $k_{\rm opt}$ is even and a similar equation when $k_{\rm opt}$ is odd (see Appendix A). A plot of θ_0 is also shown for reference. (c) Comparison of success rate between the original Grover's search (dashed green curve) and our D2p protocol (solid green line). The corresponding query complexity $k_{\rm opt}$ of the D2p protocol is shown (purple curve) which is at maximum one extra step compared to the optimal number of steps $k'_{\rm opt}$ for the original Grover's search.

which corresponds to an axis of rotation (dashed pink line in Fig. 1(c)) not parallel to the y-axis in general.

III. THE D2P PROTOCOL

The success of the protocol in Ref. 4 relies on the fact that the oracle is user-controllable which might not be always feasible. In this paper, we explore the possibility of deterministic outcome using a fixed oracle. In particular, we consider the standard phase flip operator with $\alpha = \pi$. We show that, interestingly enough, only two phase parameters are needed to obtain zero failure rate, i.e., we apply Grover iterates $G(\pi, \theta_1) = G_d(\theta_1)$ and $G(\pi, \theta_2) = G_d(\theta_2)$ alternatively to the initial state $|\psi_0\rangle$ until $k_{\rm opt}$ oracle queries are made. We call it deterministic 2-parameter (D2p) Grover's search algorithm. The requirement of only two phase parameters can be very intuitively understood from the fact that one needs only two non-colinear axes of rotation to span the full $SU(2)$ space. An example of the resulting trajectory for $\lambda = 0.005$ is illustrated in Fig. 2 (a).

The goal of this protocol then reduces to determining the phases that will ensure landing of the final state along the south pole. We first consider the case when the number of queries k is an even number, so that the final state is

$$|\psi_f\rangle = (G_d(\theta_2) \cdot G_d(\theta_1))^{k/2} |\psi_0\rangle . \tag{7}$$

Imposing the condition $\langle R|\psi_f\rangle = 0$ leads to the following two equations

$$1 + 4\lambda(1-2\lambda) \sin\left(\frac{\theta_1}{2}\right) \sin\left(\frac{\theta_2}{2}\right) \frac{\tan(k\phi)}{\sin(\phi)} = 0, \tag{8a}$$

$$(1-4\lambda) \tan\left(\frac{\theta_1}{2}\right) + \tan\left(\frac{\theta_2}{2}\right) = 0, \tag{8b}$$

where

$$\cos(\phi) = \cos\left(\frac{\theta_1+\theta_2}{2}\right) + 8\lambda(1-\lambda) \sin\left(\frac{\theta_1}{2}\right) \sin\left(\frac{\theta_2}{2}\right). \tag{9}$$

These equations can always be solved for $\{\theta_1, \theta_2\}$ when $k \geq k_{\rm opt}$ and $\lambda \leq 1/4$.

When k is odd, the final state is

$$|\psi_f\rangle = G_d(\theta_1) \cdot (G_d(\theta_2) \cdot G_d(\theta_1))^{\lfloor k/2 \rfloor} |\psi_0\rangle , \tag{10}$$

and one can find two equations similar to Eq. (8) that can be solved to obtain the optimal phase parameters (see Appendix A for explicit equations). Figure 2 (b) plots θ_0, θ_1 and θ_2 as a function of λ with $k = k_{\rm opt}$. The sharp jumps occur when the query complexity $k_{\rm opt}$ changes by one as depicted in Fig. 2(c). Note that for sufficiently small λ, $\theta_1 \approxeq -\theta_2 \approxeq \theta_0$. A comparison of the success probabilities between the standard Grover's search (green dashed line) and the D2p protocol (solid green line) is also shown in Fig. 2(c).

Next, we turn to the circuit implementation of the D2p protocol as depicted in Fig. 3(a). Hadamard gates are applied to individual qubits (initialized to $|0\rangle$) to prepare the equal-superposition state $|\psi_0\rangle$. The modified Grover's iterates $G_d(\theta)$ are applied alternatively with $\theta = \theta_1$ and $\theta = \theta_2$ for $k_{\rm opt}$ times. The last iterate is

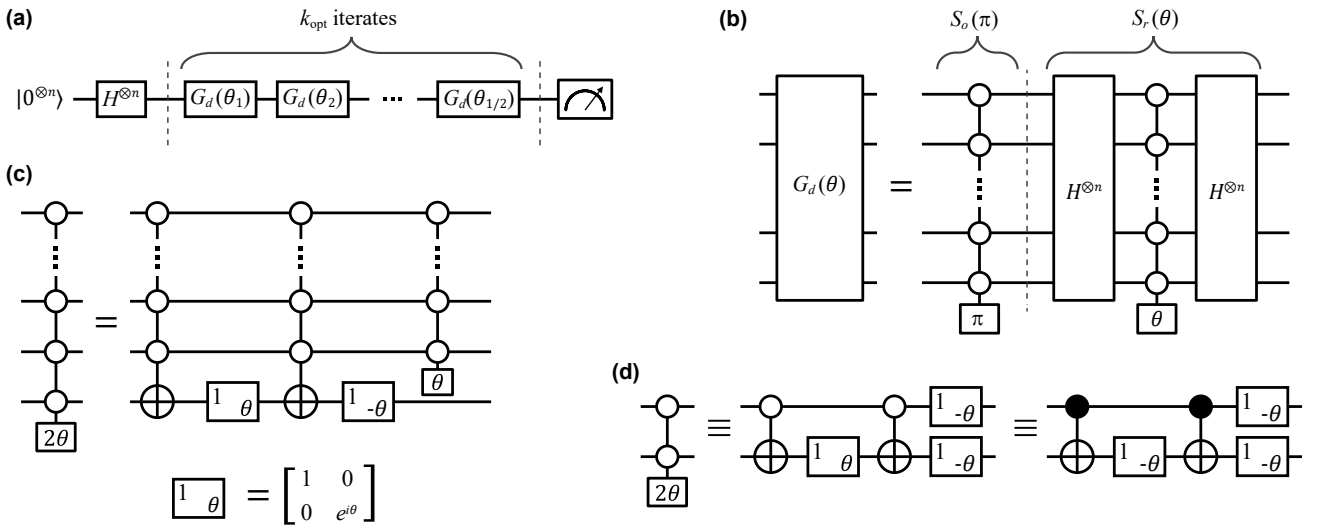

FIG. 3. Circuit implementation of the D2p Grover's search protocol without any ancillary qubit. (a) A schematic of the quantum circuit showing alternate application of the Grover iterate $G_d(\theta)$ on the equal-superposition state $|\psi_0\rangle$ obtained by applying Walsh-Hadamard transformation on individual qubits initialized to $|0\rangle$. After k_{opt} iterations a final projective measurement is performed to retrieve one of the marked states with certainty. (b) Decomposition of one Grover iterate using generalized multiply-controlled phase gate and Walsh-Hadamard gates. It consists of the standard oracle operator $S_o(\pi)$ and the generalized reflection operator $S_r(\theta)$. (c) A method to construct the generalized multiply-controlled phase gate using multiply-controlled NOT gates and single-qubit Z-rotations. The matrix at the bottom panel represents shifting phase of the $|1\rangle$ component by θ. (d) Break down of the generalized two-qubit phase gate using CNOT gates single-qubit rotations up to a global phase.

$G_d(\theta_{1(2)})$ if k_{opt} is an odd (even) number and the final state becomes an equal superposition of the marked states guaranteeing a success when a projective measurement is performed. Each Grover iterate $G_d(\theta)$ is composed of two generalized multiply-controlled phase gates and Hadamard gates as shown in Fig. 3(b). A generalized multiply-controlled phase gate involving n qubits can be deconstructed using two generalized multiply-controlled NOT gates involving n qubits and one generalized multiply-controlled phase gate involving $(n-1)$ qubits along with two single-qubit phase gates as displayed in Fig. 3(c). This decomposition can be inductively applied to construct the target gate using $\mathcal{O}(n^2)$ controlled NOT gates and single qubit rotations [8]. The final two-qubit generalized controlled-phase gate in this decomposition method can be constructed using two two-qubit gates and three single-qubit Z rotations as shown in Fig. 3(d).

IV. CONCLUSION

We have presented a modified version of Grover's search algorithm to find the correct answer with zero failure rate without having user control over the oracle implementation. The main advantage of our D2p protocol is that it requires only two phase parameters to be used in the generalized multiply-controlled phase gates. The phases can be numerically determined for any marked-to-total number of states ratio $\lambda \leq 1/4$. Efficient classical algorithms exist for $1/4 \leq \lambda \leq 1$ and thus it is justified to omit that range with no significant quantum advantage. The visual representation of this protocol using the Bloch-sphere picture makes it very intuitive and can be adapted to other phase-matching protocols [5–7].

The D2p protocol can also be readily applied to any framework where the quantum amplitude amplification [9–11], a generalization of the Grover's search, is used. A few examples include element distinctness problem [12, 13], minima finding [14, 15] and collision problems [16]. One drawback is, however, the requirement of accurate knowledge of λ, which is true for other deterministic search algorithms as well [4]. There are attempts to bound the failure rate when λ is unknown by using multiple phase matching [6] albeit at the expense of using more oracle queries than the standard optimal number k_{opt} and having control over the oracle operator. Another possible extension for our protocol would be to address the same problem without user-controlled oracles.

V. ACKNOWLEDGEMENTS

This work was supported by the Army Research Office under Grant No. W911NF-18-1-0125, National Science Foundation Grant No. PHY-1653820, Air Force Office of Scientific Research under Grant No. FA9550-21-1-0209, Depart of Energy Q-NEXT Center, NTT Research, and the Packard Foundation. .

Appendix A: Equations when k_{opt} is odd

$$2\lambda + (1-2\lambda)\cos(\theta_1) - (1-2\lambda)\sin\left(\frac{\theta_1}{2}\right)\left[\sin(\theta_1)\cos\left(\frac{\theta_2}{2}\right) + (1+4\lambda-8\lambda^2+(1-8\lambda+8\lambda^2)\cos(\theta_1))\sin\left(\frac{\theta_2}{2}\right)\right]\frac{\tan(k\phi)}{\sin(\phi)} = 0, \tag{A1a}$$

$$(1-2\lambda)\sin(\theta_1) + \left[(1-2\lambda)\left(8\lambda(1-\lambda)\sin\left(\frac{\theta_1}{2}\right)\right)\sin(\theta_1)\sin\left(\frac{\theta_2}{2}\right) - \cos(\theta_1)\sin\left(\frac{\theta_1+\theta_2}{2}\right) - 2\lambda\sin\left(\frac{\theta_1-\theta_2}{2}\right)\right]\frac{\tan(k\phi)}{\sin(\phi)} = 0. \tag{A1b}$$

[1] L. K. Grover, Phys. Rev. Lett. **79**, 325 (1997).
[2] V. Giovannetti, S. Lloyd, and L. Maccone, Phys. Rev. Lett. **100**, 160501 (2008).
[3] V. Giovannetti, S. Lloyd, and L. Maccone, Phys. Rev. A **78**, 052310 (2008).
[4] G. L. Long, Phys. Rev. A **64**, 022307 (2001).
[5] F. M. Toyama, W. van Dijk, Y. Nogami, M. Tabuchi, and Y. Kimura, Phys. Rev. A **77**, 042324 (2008).
[6] T. J. Yoder, G. H. Low, and I. L. Chuang, Phys. Rev. Lett. **113**, 210501 (2014).
[7] P. Li and S. Li, Physics Letters A **366**, 42 (2007).
[8] M. Saeedi and M. Pedram, Phys. Rev. A **87**, 062318 (2013).
[9] L. K. Grover, Phys. Rev. Lett. **80**, 4329 (1998).
[10] G. Brassard, P. Hoyer, M. Mosca, and A. Tapp, Contemporary Mathematics **305**, 53 (2002).
[11] A. Ambainis, ACM SIGACT News **35**, 22 (2004).
[12] H. Buhrman, C. Durr, M. Heiligman, P. Hoyer, F. Magniez, M. Santha, and R. De Wolf, in *Proceedings 16th Annual IEEE Conference on Computational Complexity* (IEEE, 2001) pp. 131–137.
[13] A. Ambainis, SIAM Journal on Computing **37**, 210 (2007).
[14] C. Durr and P. Hoyer, arXiv preprint quant-ph/9607014 (1996).
[15] S. Aaronson, SIAM Journal on Computing **35**, 804 (2006).
[16] G. Brassard, P. Hoyer, and A. Tapp, arXiv preprint quant-ph/9705002 (1997).