Front. Phys. 13(5), 130318 (2018)
https://doi.org/10.1007/s11467-018-0825-8

RESEARCH ARTICLE

Degradation of Grover's search under collective phase flips in queries to the oracle

Alexey E. Rastegin

Department of Theoretical Physics, Irkutsk State University, Irkutsk, Russia
E-mail: alexrastegin@mail.ru
Received February 4, 2018; accepted June 17, 2018

We address the case in which querying the oracle in Grover's algorithm is exposed to noise including phase distortions. The oracle-box wires can be altered by an opposing party that tries to prevent reception of correct data from the oracle. This situation reflects an experienced truth that any access to prophetic knowledge cannot be common and direct. To study this problem, we introduce a simple model of collective phase distortions on the basis of a phase-damping channel. In the model, the probability of success is not altered via the oracle-box wires *per se*. Phase distortions of the considered type can hardly be detected via any one-time query to the oracle. However, the probability of success is significantly changed when such errors are introduced as an intermediate step in the Grover iteration. We investigate the probability of success with respect to variations of the parameter that characterizes the amount of phase errors. It turns out that the probability of success decreases significantly even if the error is not very high. Moreover, this probability quickly reduces to the value of one half, which corresponds to the completely mixed state. We also study trade-off relations between quantum coherence and the probability of success in the presence of noise of the considered type.

Keywords Grover's algorithm, phase noise, relative entropy of coherence

PACS numbers 03.67.-a, 03.67.Ac, 03.65.Yz

1 Introduction

In the last few decades, quantum effects have found a new field of applications for information processing [1]. Shor's discovery [2] famously led to numerous quantum algorithms for algebraic problems [3–5]. Grover's search algorithm [6–8] is another fundamental result. The amplitude amplification technique that it inspired is widely used as one of the primary tools in building quantum algorithms [9]. The Shor's and Grover's algorithms may be more closely related than they initially seem [10]. The study of quantum algorithms is a part of recent efforts to realize emerging technologies in quantum information processing. The Grover algorithm is optimal for searching by means of queries to the oracle [11, 12]. The user invokes the oracle to process any item, whereas the database itself is not represented explicitly. The original formulation has been modified with particular blocks of a more general kind. In addition, the amplification process may start with an arbitrary initial distribution of amplitudes. Generalized versions of Grover's algorithm have been analyzed thoroughly [13–16].

Algorithms of amplitude amplification are related to the case when users access the so-called oracle. The oracle denotes some black box that is able to calculate values of the desired Boolean function. Users query the box by inputting concrete values of the argument. In reality, access to the oracle may be impeded and unreliable. Because of the wide applicability of amplitude amplification techniques, this problem merits detailed investigation. The oracle-box wires are inevitably exposed to noise, even if the amount is low. In addition, the wires may be affected due to activity of an opposing party. There are many possible scenarios in which the above questions could be examined. In this work, we address one such scenario. In spite of its simplicity, we disclose some unexpected corollaries of the collective phase flips in the oracle-box wires. In the model considered, queries to the oracle are exposed to phase flips described similarly to the phase damping of a qubit. We also discuss the relative entropy of coherence from the viewpoint of

*arXiv: 1708.09060 [quant-ph].

its trade-off with the probability of success.

The paper is organized as follows. The preliminary material is given in Section 2. In Section 3, we introduce the model of collective flips that occurs in the oracle-box wires. The used model leads to the recursion equation in terms of the effective Bloch vector. From the viewpoint of noise amount, two certain cases should be distinguished. In Section 4, we examine changes of the probability of success after repeated Grover's iterations under collective phase flips. It was found that the Grover search algorithm is very sensitive to distortions of the considered type. Using the relative entropy of coherence, we further study the trade-off relations with the probability of success. In Section 5, we conclude the paper with a summary of our results. Appendix A is devoted to solutions of the derived recursion equation.

2 Preliminaries

In this section, the required material will be reviewed. We begin with linear algebra. Some aspects of the Grover search algorithm, quantum noise, and coherence measures will also be presented. The singular values of a rectangular $m \times n$ matrix Z, $s_j(\mathsf{Z})$, are defined as the square roots of the eigenvalues of the positive semidefinite matrix $\mathsf{Z}^\dagger\mathsf{Z}$ [17]. The number of non-zero singular values is equal to $\mathrm{rank}(\mathsf{Z}) \leq \min\{m,n\}$. The matrices $\mathsf{Z}^\dagger\mathsf{Z}$ and $\mathsf{Z}\mathsf{Z}^\dagger$ have the same non-zero eigenvalues. For $q \in [1;\infty]$, the Schatten q-norm is defined as [17]

$$\|\mathsf{Z}\|_q := \left(\sum_{j=1}^{\mathrm{rank}(\mathsf{Z})} s_j(\mathsf{Z})^q \right)^{1/q}. \tag{1}$$

In the following, we will use the Frobenius norm $\|\mathsf{Z}\|_2 := \sqrt{\mathrm{tr}(\mathsf{Z}^\dagger\mathsf{Z})}$ and the spectral norm $\|\mathsf{Z}\|_\infty := \max s_j(\mathsf{Z})$. One of the important properties of the Schatten norm is expressed by the inequality (see, e.g., formula (1.175) in [17])

$$\|\mathsf{XYZ}\|_q \leq \|\mathsf{X}\|_\infty \|\mathsf{Y}\|_q \|\mathsf{Z}\|_\infty. \tag{2}$$

Let us recall the original formulation of Grover's search algorithm. The search space contains $N = 2^n$ items denoted by binary n-string $x = (x_1 \cdots x_n)$ with $x_j \in \{0,1\}$ such that $x \in \{0,1,\ldots,N-1\}$. The problem is to find one of the marked items that form some set $\mathcal{M}$. By $\mathcal{M}^\mathsf{c}$, we mean the complement of this set. Without loss of generality, we can assume $1 \leq |\mathcal{M}| \leq N/2$.

Checking items, the algorithm appeals to the so-called "oracle." For the each given x, the oracle returns the value of Boolean function $x \mapsto F(x)$ such that $F(x) = 1$ for $x \in \mathcal{M}$ and $F(x) = 0$ for $x \in \mathcal{M}^\mathsf{c}$. The algorithm initializes the n-qubit register to $|0\rangle$. Applying the Hadamard transform, one obtains the distribution with equal amplitudes, namely

$$\mathsf{H}|0\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle. \tag{3}$$

Such superpositions are used to realize the quantum parallelism [18]. Furthermore, we repeat the Grover iteration involving two steps. The first step of querying the oracle can be represented by the rotation operator

$$\mathsf{J} = \sum_{x=0}^{N-1} (-1)^{F(x)} |x\rangle\langle x|. \tag{4}$$

By (4), the amplitudes of marked states are all multiplied by the phase factor $\exp(\mathtt{i}\pi) = -1$. This step has been generalized to other values of the phase [13, 15]. Because we shall focus on the influence of noise, such generalizations are not considered in the following. The second step of the Grover iteration realizes the inversion about the mean [19]. It is described by the operator

$$\mathsf{K} = 2\mathsf{H}|0\rangle\langle 0|\mathsf{H} - \mathbb{1}_N, \tag{5}$$

where $\mathbb{1}_N$ is the identity operator of the corresponding size. We can sometimes replace (5) with a more general block. Such algorithms were analyzed in [13, 15]. Thus, the standard Grover iteration is written as

$$\mathsf{G} = \mathsf{K}\mathsf{J}. \tag{6}$$

In the standard formulation, the initial distribution of the amplitudes is taken in the form (3). Then, the evolution of amplitudes can be described within the two-dimensional picture. Let us define the normalized superpositions of the unmarked and marked states as

$$|w\rangle := \frac{1}{\sqrt{N-M}} \sum_{x \in \mathcal{M}^\mathsf{c}} |x\rangle, \tag{7}$$

$$|m\rangle := \frac{1}{\sqrt{M}} \sum_{x \in \mathcal{M}} |x\rangle. \tag{8}$$

We will also use the parameter $\theta \in (0;\pi/2)$ such that $\cos\theta = 1 - 2M/N$, whence

$$\sin^2\frac{\theta}{2} = \frac{M}{N}, \quad \cos^2\frac{\theta}{2} = 1 - \frac{M}{N}. \tag{9}$$

Writing operators as matrices in the basis $\{|w\rangle, |m\rangle\}$, we have $\mathsf{J} = \mathrm{diag}(+1,-1) = \boldsymbol{\sigma}_z$ and

$$\mathsf{K} = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}. \tag{10}$$

Hence, the operator (6) is simply represented as [19]

$$\mathsf{G} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}. \tag{11}$$

Thus, each Grover iteration rotates the register state by θ towards the superposition $|m\rangle$. We wish to address the case when querying the oracle is exposed to noise. To obtain explicit results, we restrict the consideration to sufficiently simple models of errors.

Entanglement is a key resource in quantum computations. Due to findings of the papers [20, 21], quantum speed-up without entanglement is hardly possible. To analyze the nature of quantum algorithms, we should think about correlations in the context of prescribed bases. This question is related to changes of quantum coherence of the register during computational processes. The framework for studies of coherence as purely quantum feature was developed recently [22, 23]. Concerning amplitude amplification, trade-off relations between quantum coherence and the probability of success is an important questions. We shall address this question in the case, when queries to the oracle are exposed to phase flips of certain type. To do so, the relative entropy of coherence will be utilized.

In general, various approaches to measure quantum correlations were discussed [23–26]. The authors of [22] developed a list of axioms that should be satisfied by any proper quantifier of coherence. As a rule, each candidate to quantify the amount of coherence is associated with some distinguishability measure. Let us take the set $\mathcal{I}$ of all diagonal density matrices such that

$$\boldsymbol{\delta} = \sum_{x=0}^{N-1} b(x)|x\rangle\langle x|, \quad \sum_{x=0}^{N-1} b(x) = 1. \tag{12}$$

We question how far the given state is from the states that are completely incoherent in the computational basis. Using the quantum relative entropy as a measure of distinguishability leads to the relative entropy of coherence. The quantum relative entropy of $\boldsymbol{\rho}$ with respect to $\boldsymbol{\omega}$ is defined as [17, 27]

$$D_1(\boldsymbol{\rho}||\boldsymbol{\omega}) := \begin{cases} \mathrm{tr}(\boldsymbol{\rho}\ln\boldsymbol{\rho} - \boldsymbol{\rho}\ln\boldsymbol{\omega}), & \text{if } \mathrm{ran}(\boldsymbol{\rho}) \subseteq \mathrm{ran}(\boldsymbol{\omega}), \\ +\infty, & \text{otherwise.} \end{cases} \tag{13}$$

By $\mathrm{ran}(\boldsymbol{\rho})$, we mean here the range of $\boldsymbol{\rho}$. Based on the quantity (13), the corresponding coherence measure is introduced as [22]

$$C_1(\boldsymbol{\rho}) := \min_{\boldsymbol{\delta}\in\mathcal{I}} D_1(\boldsymbol{\rho}||\boldsymbol{\delta}). \tag{14}$$

The minimization has led to the expression [22]

$$C_1(\boldsymbol{\rho}) = S_1(\boldsymbol{\rho}_{\mathrm{diag}}) - S_1(\boldsymbol{\rho}), \tag{15}$$

where $S_1(\boldsymbol{\rho}) = -\mathrm{tr}(\boldsymbol{\rho}\ln\boldsymbol{\rho})$ is the von Neumann entropy of $\boldsymbol{\rho}$, and

$$\boldsymbol{\rho}_{\mathrm{diag}} := \sum_{x=0}^{N-1} p(x)|x\rangle\langle x|, \quad p(x) = \langle x|\boldsymbol{\rho}|x\rangle.$$

The entropy $S(\boldsymbol{\rho}_{\mathrm{diag}})$ is equal to the Shannon entropy calculated with the probabilities $p(x)$. The basic properties of (14) are considered in [22, 23]. The generalized entropic functions have found use in quantum information theory. It is for this reason that we designate the above quantities by the subscript 1. Coherence quantifiers induced by quantum divergences of the Tsallis type were addressed in [28]. In contrast to (15), such quantifiers do not allow a simple additive expression. Coherence monotones based on Rényi divergences were considered in [29–31]. Other candidates to quantify the amount of coherence were also examined [32, 33]. The geometric coherence is an interesting quantifier of different characters [23]. Two-sided estimates on the geometric coherence were obtained in [34].

Complementarity relations for quantum coherence can be formulated in several ways [35–39]. Duality relations between the coherence and path information were analyzed in [40–42]. From the viewpoint of quantum computations, the concept of quantum coherence was studied in [43–45]. In particular, the authors of [44] reported on coherence depletion in the original Grover algorithm. In [46], we studied relations between the coherence and probability of success in generalized amplitude amplification. Some of these results will be used in studies of Grover's search in the presence of phase flips.

3 Collective flips introduced by phase damping

There are infinitely many scenarios of interaction with the environment. We will consider a model with phase damping. Such processes describe the loss of quantum information without losses of energy [19]. Phase damping provides the grounds for understanding the physical effects in quantum systems, similar to the Schrödinger cat–atom system. Let us focus on those density matrices that are effectively two-dimensional with respect to the basis $\{|w\rangle, |m\rangle\}$. In other words, they can be represented via the usual Bloch vector $\mathbf{r} = (r_x, r_y, r_z)$, namely

$$\boldsymbol{\rho} = \frac{1}{2}\begin{pmatrix} 1+r_z & r_x - \mathrm{i}r_y \\ r_x + \mathrm{i}r_y & 1-r_z \end{pmatrix}. \tag{16}$$

With positive parameter $\eta \le 1$, we introduce the following Kraus operators:

$$\mathsf{E}_0 := \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{\eta} \end{pmatrix}, \quad \mathsf{E}_1 := \begin{pmatrix} 0 & 0 \\ 0 & \sqrt{1-\eta} \end{pmatrix}. \tag{17}$$

These operators prescribe the action of phase damping Φ_{E} on density matrices of the above type. It is well known that this action reads as [19]

$$(r_x, r_y, r_z) \overset{\Phi_{\mathsf{E}}}{\longmapsto} \left(\sqrt{\eta}r_x, \sqrt{\eta}r_y, r_z\right). \tag{18}$$

Initializing yields the density matrix $\boldsymbol{\rho}(0) = \mathsf{H}|0\rangle\langle 0|\mathsf{H}$ with the Bloch vector $\mathbf{r}(0) = (\sin\theta, 0, \cos\theta)$. After t iterations, the probability of success is written as

$$P_{\mathrm{suc}}(t) = \langle m|\boldsymbol{\rho}(t)|m\rangle = \frac{1 - r_z(t)}{2}. \tag{19}$$

It must be stressed that the channel Φ_{E} itself cannot alter the probability of success. We immediately see this fact from (18). Nevertheless, the probability of success will be changed in the case where this channel acts as an intermediate point in the amplitude amplification process.

We will investigate the following scheme. Each iteration transforms the density matrices of the register according to the formula

$$\boldsymbol{\rho}(t) \mapsto \boldsymbol{\rho}(t+1) = \Upsilon_{\mathsf{K}} \circ \Phi_{\mathsf{E}} \circ \Upsilon_{\mathsf{J}} \circ \Phi_{\mathsf{E}}\big(\boldsymbol{\rho}(t)\big), \tag{20}$$

where the two unitary channels are defined as

$$\Upsilon_{\mathsf{J}}(\boldsymbol{\varrho}) = \mathsf{J}\boldsymbol{\varrho}\mathsf{J}^{\dagger}, \quad \Upsilon_{\mathsf{K}}(\boldsymbol{\varrho}) = \mathsf{K}\boldsymbol{\varrho}\mathsf{K}^{\dagger}. \tag{21}$$

For $\eta = 1$, the map Φ_{E} reduces to the identical one, such that the right-hand side of (20) takes the form

$$\boldsymbol{\rho}(t+1) = \Upsilon_{\mathsf{K}} \circ \Upsilon_{\mathsf{J}}\big(\boldsymbol{\rho}(t)\big) = \mathsf{G}\boldsymbol{\rho}(t)\mathsf{G}^{\dagger}. \tag{22}$$

If the initialized state is pure, then the register will remain in the pure state under the action of the map (22). This is not the case for the altered map (20).

The above model deals with collective phase distortions that are simply expressed in the computational basis. It allows us to formulate results in a closed analytical form. Under some circumstances, the considered picture concerns the case when phase flips occur solely in a single qubit. The phase flip channel has Kraus operators $\sqrt{\alpha}\mathbb{1}_2$ and $\sqrt{1-\alpha}\boldsymbol{\sigma}_z$ [19]. This channel is actually equivalent to the phase damping channel whenever

$$2\alpha = 1 + \sqrt{\eta}. \tag{23}$$

If only one qubit is affected, we can split the total Hilbert space into two subspaces $\mathcal{H}_0$ and $\mathcal{H}_1$. These subspaces are spanned by canonical states that have in their binary notation either 0 or 1 in the position of the noised qubit, respectively. Any density matrix $\boldsymbol{\rho}$ can then be written as a block 2×2-matrix $[[\boldsymbol{\rho}_{ij}]]$. Due to phase flips in the noised qubit, we have $\boldsymbol{\rho}_{ij} \mapsto \sqrt{\eta}\,\boldsymbol{\rho}_{ij}$ for $i \neq j$. The diagonal submatrices $\boldsymbol{\rho}_{00}$ and $\boldsymbol{\rho}_{11}$ are not changed. Suppose that errors occur in each query to the oracle. In general, a complete analysis is complicated [47]. However, the situation can sometimes be reduced to our model. When one subspace consists of only marked states, we really deal with the channel Φ_E, per (18). Our scenario does not mean that phase distortions act in all qubits simultaneously. Dephasing noise may be treated as a result of the existence of "damaged" vertices in a quantum-walk search [47]. Because of the interferometric picture of quantum walks [48], one can therefore provide an example of phase errors in realistic systems.

Interpreting (20) as a matrix relation, we will solve it via diagonalization. This approach is somewhat similar to the treatment of [15]. On the other hand, we deal with the recursion equation for components of the actual Bloch vector. The authors of [15] used the recursion equation for components of the wave function. In our case, only two of the components of the Bloch vector are non-zero. Hence, we will further treat $\mathbf{r}(t)$ as a column with two entries, namely $r_x(t)$ and $r_z(t)$. In terms of the Bloch vector components, the action of operation Φ_{E} is represented by the matrix $\mathrm{diag}(\sqrt{\eta}, +1)$. We also have

$$\begin{aligned} 2\mathsf{J}\boldsymbol{\rho}\mathsf{J}^{\dagger} &= \boldsymbol{\sigma}_z(\mathbb{1}_2 + r_x\boldsymbol{\sigma}_x + r_z\boldsymbol{\sigma}_z)\boldsymbol{\sigma}_z \\ &= \mathbb{1}_2 - r_x\boldsymbol{\sigma}_x + r_z\boldsymbol{\sigma}_z, \end{aligned} \tag{24}$$

whence the operation Υ_{J} acts on the Bloch vectors as the matrix $\mathrm{diag}(-1, +1)$. Using (10), we obtain $\mathsf{K}\mathbb{1}_2\,\mathsf{K}^{\dagger} = \mathbb{1}_2$,

$$\begin{aligned} \mathsf{K}\boldsymbol{\sigma}_x\mathsf{K}^{\dagger} &= -\cos 2\theta\boldsymbol{\sigma}_x + \sin 2\theta\boldsymbol{\sigma}_z, \\ \mathsf{K}\boldsymbol{\sigma}_z\mathsf{K}^{\dagger} &= \sin 2\theta\boldsymbol{\sigma}_x + \cos 2\theta\boldsymbol{\sigma}_z, \end{aligned}$$

such that $r_x \mapsto -\cos 2\theta r_x + \sin 2\theta r_z$ and $r_z \mapsto \sin 2\theta r_x + \cos 2\theta r_z$ due to the operation Υ_{K}. Hence, this operation acts on the Bloch vectors as the matrix

$$\begin{pmatrix} -\cos 2\theta & \sin 2\theta \\ \sin 2\theta & \cos 2\theta \end{pmatrix}. \tag{25}$$

Finally, the recursion equation is written in terms of the effective Bloch vector as

$$\mathbf{r}(t+1) = \mathsf{L}\mathbf{r}(t), \tag{26}$$

where the matrix L reads as

$$\mathsf{L} = \begin{pmatrix} \eta\cos 2\theta & \sin 2\theta \\ -\eta\sin 2\theta & \cos 2\theta \end{pmatrix}. \tag{27}$$

Thus, we obtain the equation $\mathbf{r}(t) = \mathsf{L}^t\mathbf{r}(0)$, which is solved explicitly in Appendix A. The singular values of L are equal to 1 and η, whence $\|\mathsf{L}\|_{\infty} = 1$. Combining the latter with (2) implies that the 2-norm of the Bloch vector cannot increase, i.e., $\|\mathbf{r}(t)\|_2 \leq \|\mathbf{r}(0)\|_2$.

It will be convenient to apply three positive parameters, viz.

$$A_{\pm} := \frac{1 \pm \eta}{2}\cos 2\theta, \tag{28}$$

$$B := \begin{cases} \sqrt{\eta - A_+^2}, & \text{if } \eta > A_+^2, \\ 0, & \text{if } \eta = A_+^2, \\ \sqrt{A_+^2 - \eta}, & \text{if } \eta < A_+^2. \end{cases} \tag{29}$$

The characteristic equation is written as

$$\lambda^2 - 2A_+\lambda + \eta = 0. \tag{30}$$

We will further assume that $A_+^2 - \eta \neq 0$. Then, the eigenvalues λ_+ and λ_- differ such that the matrix L is certainly diagonalizable. The following two cases should be mentioned: (i) $\eta > A_+^2$, (ii) $\eta < A_+^2$. In Appendix A, we examine them separately. In the first case,

$$r_z(t) = \frac{\eta^{t/2}}{B}\Big(-\eta \sin\varphi t \sin 2\theta \sin\theta + (B\cos\varphi t + A_- \sin\varphi t)\cos\theta\Big), \tag{31}$$

$$P_{\text{suc}}(t) = \frac{1}{2B}\Big(B + \eta^{1+t/2}\sin\varphi t \sin 2\theta \sin\theta - \eta^{t/2}(B\cos\varphi t + A_- \sin\varphi t)\cos\theta\Big). \tag{32}$$

In the second case,

$$r_z(t) = \frac{\eta^{t/2}}{B}\Big(-\eta \sinh\phi t \sin 2\theta \sin\theta + (B\cosh\phi t + A_- \sinh\phi t)\cos\theta\Big), \tag{33}$$

$$P_{\text{suc}}(t) = \frac{1}{2B}\Big(B + \eta^{1+t/2}\sinh\phi t \sin 2\theta \sin\theta - \eta^{t/2}(B\cosh\phi t + A_- \sinh\phi t)\cos\theta\Big). \tag{34}$$

4 Dynamics of the probability of success and quantum coherence

In this section, we will use the solutions of (32) and (34) to study a vulnerability of Grover's search with respect to phase flips in the oracle-box wires. In principle, they may be inspired by an opposing party that tries to prevent correct querying to the oracle. To input collective phase flips, the opponent should be aware of the details of the Boolean function $x \mapsto F(x)$.

To study the significance of collective phase flips, we visualize $P_{\text{suc}}(t)$ versus t for several values of the parameter η. We begin with case (i), when $\eta > A_+^2$. As was mentioned above, this case includes the standard situation $\eta = 1$. In Fig. 1, we take $N = 64$, $M = 1$, and show the lines for the four values of η. Although t takes integer values, lines may be drawn continuously for the sake of visibility. Even if the amount of errors is low, values of the probability of success are still reduced. Without distortions, when $\eta = 1$, the dependence of $P_{\text{suc}}(t)$ on t is almost periodic. A noticeable decrease in $P_{\text{suc}}(t)$ due to $\eta < 1$ is observed, even in the first cycle of amplitude amplification. After several cycles, the curve $P_{\text{suc}}(t)$ asymptotically degenerates to a constant equal to 1/2. The same result was later reported for a particular case of decoupling noise in [47].

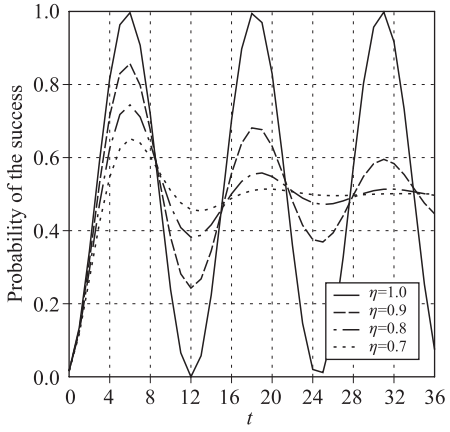

Fig. 1 In case (i), $P_{\text{suc}}(t)$ is shown for $N = 64$, $M = 1$, and the four values of η.

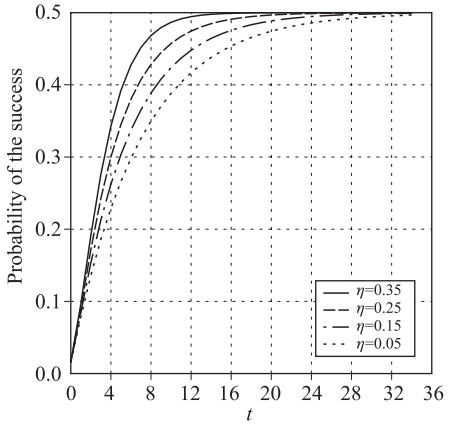

Fig. 2 In case (ii), $P_{\text{suc}}(t)$ is shown for $N = 64$, $M = 1$, and the four values of η.

For completeness, we also show an example of $P_{\text{suc}}(t)$ for case (ii), when $\eta < A_+^2$. In Fig. 2, we set $N = 64$, $M = 1$, and show the lines for the four low values of η. Here, the dependence $P_{\text{suc}}(t)$ is of a completely different character. Instead of decaying cycles with some peaks, we observe that the lines smoothly and quickly saturate the constant equal to 1/2. This behavior cannot be treated as amplitude amplification of any kind. When the oracle-box wires are exposed to the channel Υ_{K} with such low values of η, legitimate users are able to detect this fact. Therefore, we further return to case (i) and address the trade-off relations between the quantum coherence and probability of success.

The relative entropy of coherence satisfies [46]

$$h_1(P_{\text{suc}}) \leq C_1(\boldsymbol{\rho}) + S_1(\boldsymbol{\rho}) \leq P_{\text{suc}} \ln\left(\frac{M}{P_{\text{suc}}}\right) + (1 - P_{\text{suc}}) \ln\left(\frac{N-M}{1-P_{\text{suc}}}\right), \tag{35}$$

where $h_1(P_{\text{suc}})$ is the binary Shannon entropy. In calculating $C_1\big(\boldsymbol{\rho}(t)\big)$, we examine it from the viewpoint of (35).

To do so, we recall the complete form of $\boldsymbol{\rho}(t)$, namely

$$\boldsymbol{\rho}(t) = \frac{1+r_z(t)}{2}\,|w\rangle\langle w| + \frac{r_x(t)}{2}\big(|w\rangle\langle m| + |m\rangle\langle w|\big) + \frac{1-r_z(t)}{2}\,|m\rangle\langle m|. \tag{36}$$

In the computational basis, the diagonal part of $\boldsymbol{\rho}(t)$ can be written as a diagonal matrix that has the value $\big(1-P_{\rm suc}(t)\big)/(N-M)$ with multiplicity $N-M$ and the value $P_{\rm suc}(t)/M$ with multiplicity M. For $t>0$, the nonzero eigenvalues of $\boldsymbol{\rho}(t)$ are obtained as

$$\frac{1\pm\|\mathbf{r}(t)\|_2}{2}, \quad \|\mathbf{r}(t)\|_2 = \sqrt{r_x(t)^2+r_z(t)^2} < 1. \tag{37}$$

Of course, with the initial distribution (3), we have $\|\mathbf{r}(0)\|_2 = 1$. Due to (A10), we have $\|\mathbf{r}(t)\|_2 \propto \eta^{t/2}$. In the considered case of amplitude amplification, we have the equality

$$C_1\big(\boldsymbol{\rho}(t)\big) = P_{\rm suc}(t)\ln\left(\frac{M}{P_{\rm suc}(t)}\right) + \big(1-P_{\rm suc}(t)\big)\ln\left(\frac{N-M}{1-P_{\rm suc}(t)}\right) - S_1\big(\boldsymbol{\rho}(t)\big).$$

That is, the upper bound of the right-hand side of (35) is saturated here. For the given $P_{\rm suc}$, this upper bound approves the maximal possible value of $C_1(\boldsymbol{\rho})$. We see that trade-offs between $C_1\big(\boldsymbol{\rho}(t)\big)$ and $P_{\rm suc}(t)$ follow the mentioned line. Let us exemplify the dependence of the relative entropy of coherence on the step number t. In Fig. 3, we take $N=64$, $M=1$, and show $C_1\big(\boldsymbol{\rho}(t)\big)$ for the four values of η. Except for when $\eta=1.0$, the curves asymptotically lie on the constant line. This constant is generally written as $(1/2)\ln\big(MN-M^2\big)$. Substituting $N=64$ and $M=1$, we have the value $\ln 63/2 \approx 2.072$, which is also seen in Fig. 3. For the value $\eta=1$, we may compare the two curves in Figs. 1 and 3. One observes that the peaks of $P_{\rm suc}(t)$ correspond to valleys of $C_1\big(\boldsymbol{\rho}(t)\big)$, and *vice versa*. In detail, this property was discussed in [44]. We also observe that the curves for $\eta<1$ reveal a similar behavior, but now with decay. Even if the amount of phase noise is low, oscillations in the relative entropy are reduced sufficiently quickly. These results additionally maintain the conclusions previously reported in [46]. Namely, even a tight trade-off relation between coherence and the probability of success does not imply a high quality of amplitude amplification. This question merits further investigation.

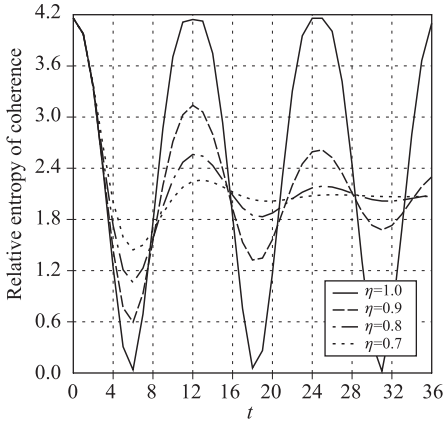

Fig. 3 In case (i), $C_1\big(\boldsymbol{\rho}(t)\big)$ is shown for $N=64$, $M=1$, and the four values of η.

5 Conclusions

We have examined the case in which queries to the oracle in Grover's search algorithm are exposed to phase distortions of a specific type. Another possibility is that the oracle-box wires are altered due to intrusion of an opposing party. The model of collective phase flips is similar to the phase damping channel. Despite its simplicity, this model allows us to observe some genuine features of the amplitude amplification processes. We have concluded that Grover's search algorithm is actually sensitive to collective phase flips occurring in the oracle-box wires. This feature also provides an opposing party with chances to prevent proper queries of legitimate users to the oracle. At the same time, phase flips are such that the probability of success is not changed during transfer via these wires. Even if the user has been ensured with testing states, he is hardly able to detect such distortions by means of one-time queries to the oracle. We also investigated the trade-off relation between the coherence and probability of success under noise of the considered type. Our findings further support the conclusions obtained previously.

Appendix A Solutions of the recursion equation

To solve (26), we calculate the eigenvalues and the corresponding eigenvectors. We begin with the case (i), when $\eta > A_+^2$. By calculations, one has

$$\cos 2\theta = 1 - \frac{8M}{N} + \frac{8M^2}{N^2}. \tag{A1}$$

The most interesting case occurs, when $M \ll N$ and the term $\cos 2\theta$ is sufficiently close to 1. The condition of the case (i),

$$\frac{2\sqrt{\eta}}{1+\eta} > \cos 2\theta, \tag{A2}$$

will be fulfilled for $\eta_{\min} < \eta < 1$ with

$$\sqrt{\eta_{\min}} = \frac{1-\sin 2\theta}{\cos 2\theta}.$$

The value $\eta_{\min}$ does not approach 1 with necessity, whence the above range may be wide enough. Say, for $M = 1$ and $N = 64$ we get $\cos 2\theta \approx 0.877$ and $\eta_{\min} \approx 0.351$. Due to $B^2 = \eta - A_+^2$, the eigenvalues are written in the form

$$\lambda_{\pm} = A_+ \pm \mathtt{i}B. \tag{A3}$$

Using $A_+^2 + B^2 = \eta$, put positive angle φ such that

$$\frac{A_+}{\sqrt{\eta}} = \cos\varphi, \quad \frac{B}{\sqrt{\eta}} = \sin\varphi, \tag{A4}$$

$$\varphi = \arctan\left(\frac{B}{A_+}\right). \tag{A5}$$

The eigenvalues are rewritten as $\lambda_{\pm} = \sqrt{\eta}\exp(\pm\mathtt{i}\varphi)$. Calculating the corresponding eigenvectors, we further obtain

$$\mathsf{X}^{-1}\mathsf{L}\mathsf{X} = \mathsf{D}, \tag{A6}$$

where $\mathsf{D} = \mathrm{diag}(\lambda_+, \lambda_-)$ and

$$\mathsf{X} = \begin{pmatrix} \sin 2\theta & \sin 2\theta \\ A_- + \mathtt{i}B & A_- - \mathtt{i}B \end{pmatrix}, \tag{A7}$$

$$\mathsf{X}^{-1} = \frac{1}{2\mathtt{i}B\sin 2\theta}\begin{pmatrix} \mathtt{i}B - A_- & \sin 2\theta \\ \mathtt{i}B + A_- & -\sin 2\theta \end{pmatrix}. \tag{A8}$$

Calculations of the matrix $\mathsf{L}^t = \mathsf{X}\mathsf{D}^t\mathsf{X}^{-1}$ finally give

$$\frac{\eta^{t/2}}{B}\begin{pmatrix} B\cos\varphi t - A_-\sin\varphi t & \sin\varphi t\sin 2\theta \\ -\eta\sin\varphi t\sin 2\theta & B\cos\varphi t + A_-\sin\varphi t \end{pmatrix}.$$

Due to $r_x(0) = \sin\theta$ and $r_z(0) = \cos\theta$, the above formulas result in (31) and (32). For $\eta = 1$, we have $A_+ = \cos 2\theta$, $A_- = 0$, $B = \sin 2\theta$, and $\varphi = 2\theta$. Then the expression (32) is reduced to

$$P_{\mathrm{suc}}(t) = \frac{1-\cos(2\theta t + \theta)}{2} = \sin^2\big[\theta(t+1/2)\big]. \tag{A9}$$

The latter is well known for the original Grover algorithm. It is seen from the formula for L^t that components of the Bloch vector are proportional to the factor $\eta^{t/2}$, namely

$$r_x(t) \propto \eta^{t/2}, \quad r_z(t) \propto \eta^{t/2}. \tag{A10}$$

Except for the value $\eta = 1$, these components asymptotically tends to zero. Hence, the probability $P_{\mathrm{suc}}(t)$ goes to 1/2.

Let us proceed to the case (ii), when $\eta < A_+^2$. Due to $B^2 = A_+^2 - \eta$, the eigenvalues are expressed as

$$\lambda_{\pm} = A_+ \pm B. \tag{A11}$$

For $\eta > 0$, the eigenvalues are both strictly positive and $\lambda_- < \lambda_+ \le A_+ + A_- = \cos 2\theta < 1$. So, the matrix L describes a contracting map. Due to $A_+^2 - B^2 = \eta$, we can write

$$\frac{A_+}{\sqrt{\eta}} = \cosh\phi, \quad \frac{B}{\sqrt{\eta}} = \sinh\phi, \tag{A12}$$

where positive parameter ϕ reads as

$$\phi = \frac{1}{2}\ln\left(\frac{A_+ + B}{A_+ - B}\right). \tag{A13}$$

Hence, we can write $\lambda_{\pm} = \sqrt{\eta}\exp(\pm\phi)$. Similarly to the case (i), we diagonalize L according to (A6). Now, the matrix of column eigenvectors and its inverse are represented as

$$\mathsf{X} = \begin{pmatrix} \sin 2\theta & \sin 2\theta \\ A_- + B & A_- - B \end{pmatrix}, \tag{A14}$$

$$\mathsf{X}^{-1} = \frac{1}{2B\sin 2\theta}\begin{pmatrix} B - A_- & \sin 2\theta \\ B + A_- & -\sin 2\theta \end{pmatrix}. \tag{A15}$$

Calculating the matrix $\mathsf{L}^t = \mathsf{X}\mathsf{D}^t\mathsf{X}^{-1}$, we have

$$\frac{\eta^{t/2}}{B}\begin{pmatrix} B\cosh\phi t - A_-\sinh\phi t & \sinh\phi t\sin 2\theta \\ -\eta\sinh\phi t\sin 2\theta & B\cosh\phi t + A_-\sinh\phi t \end{pmatrix},$$

since $A_-^2 - B^2 = \eta\sin^2 2\theta$. Due to $r_x(0) = \sin\theta$ and $r_z(0) = \cos\theta$, we finally get (33) and (34). The original Grover search is beyond the case (ii). Indeed, for $1 \le M \le N/2$ we have $\cos 2\theta < 1$, so that the condition $2\sqrt{\eta} < (1+\eta)\cos 2\theta$ is certainly violated with $\eta = 1$.

References

1. A. Galindo and M. A. Martin-Delgado, Information and computation: Classical and quantum aspects, *Rev. Mod. Phys.* 74(2), 347 (2002)
2. P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM J. Comput.* 26(5), 1484 (1997)
3. D. Haase and H. Maier, Quantum algorithms for number fields, *Fortschr. Phys.* 54(8–10), 866 (2006)
4. S. Hallgren, Polynomial-time quantum algorithms for Pell's equation and the principal ideal problem, *J. Assoc. Comput. Mach.* 54(1), 1 (2007)
5. A. M. Childs and W. van Dam, Quantum algorithms for algebraic problems, *Rev. Mod. Phys.* 82(1), 1 (2010)

6. L. K. Grover, Quantum mechanics helps in searching for a needle in a haystack, *Phys. Rev. Lett.* 79(2), 325 (1997)
7. L. K. Grover, Quantum computers can search arbitrarily large databases by a single query, *Phys. Rev. Lett.* 79(23), 4709 (1997)
8. L. K. Grover, Quantum computers can search rapidly by using almost any transformation, *Phys. Rev. Lett.* 80(19), 4329 (1998)
9. A. D. Patel and L. K. Grover, Quantum search, in: M.-Y. Kao (Ed.), Encyclopedia of Algorithms, New York: Springer, 2016, pp 1707–1716
10. S. J. Jr Lomonaco and L. H. Kauffman, Is Grover's algorithm a quantum hidden subgroup algorithm? *Quantum Inform. Process.* 6(6), 461 (2007)
11. C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, Strengths and weaknesses of quantum computing, *SIAM J. Comput.* 26(5), 1510 (1997)
12. C. Zalka, Grover's quantum searching algorithm is optimal, *Phys. Rev. A* 60(4), 2746 (1999)
13. E. Biham, O. Biham, D. Biron, M. Grassl, and D. A. Lidar, Grover's quantum search algorithm for an arbitrary initial amplitude distribution, *Phys. Rev. A* 60(4), 2742 (1999)
14. A. Galindo and M. A. Martin-Delgado, Family of Grover's quantum-searching algorithms, *Phys. Rev. A* 62(6), 062303 (2000)
15. E. Biham, O. Biham, D. Biron, M. Grassl, D. A. Lidar, and D. Shapira, Analysis of generalized Grover quantum search algorithms using recursion equations, *Phys. Rev. A* 63(1), 012310 (2000)
16. E. Biham and D. Kenigsberg, Grover's quantum search algorithm for an arbitrary initial mixed state, *Phys. Rev. A* 66(6), 062301 (2002)
17. J. Watrous, The Theory of Quantum Information, Cambridge: Cambridge University Press, 2018
18. D. Deutsch, Quantum theory, the Church–Turing principle and the universal quantum computer, *Proc. R. Soc. Lond. A* 400(1818), 97 (1985)
19. M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information, Cambridge: Cambridge University Press, 2000
20. S. L. Braunstein and A. K. Pati, Speed-up and entanglement in quantum searching, *Quantum Inf. Comput.* 2, 399 (2002)
21. R. Jozsa and N. Linden, On the role of entanglement in quantum-computational speed-up, *Proc. R. Soc. Lond. A* 459(2036), 2011 (2003)
22. T. Baumgratz, M. Cramer, and M. B. Plenio, Quantifying coherence, *Phys. Rev. Lett.* 113(14), 140401 (2014)
23. A. Streltsov, G. Adesso, and M. B. Plenio, Quantum coherence as a resource, *Rev. Mod. Phys.* 89(4), 041003 (2017)
24. G. Adesso, T. R. Bromley, and M. Cianciaruso, Measures and applications of quantum correlations, *J. Phys. A Math. Theor.* 49(47), 473001 (2016)
25. M. L. Hu and H. Fan, Relative quantum coherence, incompatibility, and quantum correlations of states, *Phys. Rev. A* 95(5), 052106 (2017)
26. M.L. Hu, X. Hu, Y. Peng, Y.R. Zhang, and H. Fan, Quantum coherence and quantum correlations, arXiv: 1703.01852 [quant-ph] (2017)
27. V. Vedral, The role of relative entropy in quantum information theory, *Rev. Mod. Phys.* 74(1), 197 (2002)
28. A. E. Rastegin, Quantum-coherence quantifiers based on the Tsallis relative a entropies, *Phys. Rev. A* 93(3), 032136 (2016)
29. E. Chitambar and G. Gour, Comparison of incoherent operations and measures of coherence, *Phys. Rev. A* 94(5), 052336 (2016)
30. L. H. Shao, Y. Li, Y. Luo, and Z. Xi, Quantum coherence quantifiers based on the Rényi a-relative entropy, *Commum. Theor. Phys.* 67(6), 631 (2017)
31. A. Streltsov, H. Kampermann, S. Wölk, M. Gessner, and D. Bruß, Maximal coherence and the resource theory of purity, *New J. Phys.* 20(5), 053058 (2018)
32. L. H. Shao, Z. Xi, H. Fan, and Y. Li, Fidelity and tracenorm distances for quantifying coherence, *Phys. Rev. A* 91(4), 042120 (2015)
33. S. Rana, P. Parashar, and M. Lewenstein, Trace-distance measure of coherence, *Phys. Rev. A* 93(1), 012110 (2016)
34. H. J. Zhang, B. Chen, M. Li, S. M. Fei, and G. L. Long, Estimation on geometric measure of quantum coherence, *Commum. Theor. Phys.* 67(2), 166 (2017)
35. S. Cheng and M. J. W. Hall, Complementarity relations for quantum coherence, *Phys. Rev. A* 92(4), 042101 (2015)
36. U. Singh, A. K. Pati, and M. N. Bera, Uncertainty relations for quantum coherence, *Mathematics* 4(3), 47 (2016)
37. Y. Peng, Y.R. Zhang, Z.Y. Fan, S. Liu, and H. Fan, Complementary relation of quantum coherence and quantum correlations in multiple measurements, arXiv: 1608.07950 [quant-ph] (2016)
38. X. Yuan, G. Bai, T. Peng, and X. Ma, Quantum uncertainty relation using coherence, *Phys. Rev. A* 96(3), 032313 (2017)
39. A. E. Rastegin, Uncertainty relations for quantum coherence with respect to mutually unbiased bases, *Front. Phys.* 13(1), 130304 (2018)
40. M. N. Bera, T. Qureshi, M. A. Siddiqui, and A. K. Pati, Duality of quantum coherence and path distinguishability, *Phys. Rev. A* 92(1), 012118 (2015)
41. E. Bagan, J. A. Bergou, S. S. Cottrell, and M. Hillery, Relations between coherence and path information, *Phys. Rev. Lett.* 116(16), 160406 (2016)

42. T. Qureshi and M. A. Siddiqui, Wave-particle duality in N-path interference, *Ann. Phys.* 385, 598 (2017)

43. M. Hillery, Coherence as a resource in decision problems: The Deutsch-Jozsa algorithm and a variation, *Phys. Rev. A* 93(1), 012111 (2016)

44. H. L. Shi, S. Y. Liu, X. H. Wang, W. L. Yang, Z. Y. Yang, and H. Fan, Coherence depletion in the Grover quantum search algorithm, *Phys. Rev. A* 95(3), 032307 (2017)

45. N. Anand and A. K. Pati, Coherence and entanglement monogamy in the discrete analogue of analog Grover search, arXiv: 1611.04542 [quant-ph] (2016)

46. A. E. Rastegin, On the role of dealing with quantum coherence in amplitude amplification, *Quantum Inf. Progress* 17(7), 179 (2018)

47. D. Reitzner and M. Hillery, Grover search under localized dephasing, arXiv: 1712.06558 [quant-ph] (2017)

48. M. Hillery, J. Bergou, and E. Feldman, Quantum walks based on an interferometric analogy, *Phys. Rev. A* 68(3), 032314 (2003)