

Coherence and decoherence in generalized Shor's algorithm

Linlin Ye(叶琳琳), Zhaoqi Wu(吴照奇), and Nanrun Zhou(周南润)

Citation: Chin. Phys. B, 2026, 35 (**6**): 060304. DOI: 10.1088/1674-1056/ae445e
http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Probing dephasing and non-Markovian effects on three-qubit states

Muhammad Noman, Aqsa Mushtaq, and Wei Cui(崔巍)
Chin. Phys. B, 2026, 35 (**5**): 050302. DOI: 10.1088/1674-1056/ae1822

Generation of cross-cross resonance gates with two fluxonium qubits

Xinpeng Chen(陈鑫鹏) and Zeliang Xiang(项泽亮)
Chin. Phys. B, 2026, 35 (**4**): 040308. DOI: 10.1088/1674-1056/ae13ea

Estimating quantum coherence using limited quantum resources

Bin Zou(邹斌), Kai Wu(吴凯), and Zhihua Chen(陈芝花)
Chin. Phys. B, 2026, 35 (**3**): 030301. DOI: 10.1088/1674-1056/adfb56

Impact of decoherence on the metrological advantage of weak-value amplification

Yu-Han Yan(严雨涵), Yan-Ping Tan(谭艳萍), Yan-Yan Lu(陆艳艳), Shao-Jie Xiong(熊少杰), and Zhe Sun(孙哲)
Chin. Phys. B, 2026, 35 (**1**): 010307. DOI: 10.1088/1674-1056/ae29fe

Realization of *t*-bit semiclassical quantum Fourier transform on IBM's quantum cloud computer

Xiang-Qun Fu(付向群), Wan-Su Bao(鲍皖苏), He-Liang Huang(黄合良), Tan Li(李坦), Jian-Hong Shi(史建红), Xiang Wang(汪翔), Shuo Zhang(张硕), Feng-Guang Li(李风光)
Chin. Phys. B, 2019, 28 (**2**): 020302. DOI: 10.1088/1674-1056/28/2/020302

Coherence and decoherence in generalized Shor's algorithm

Linlin Ye(叶琳琳)[1], Zhaoqi Wu(吴照奇)[1,†], and Nanrun Zhou(周南润)[2,3]

[1] *Department of Mathematics, Nanchang University, Nanchang* 330031, *China*
[2] *School of Electronic and Electrical Engineering, Shanghai University of Engineering Science, Shanghai* 201620, *China*
[3] *Department of Electronic Information Engineering, Nanchang University, Nanchang* 330031, *China*

(Received 11 November 2025; revised manuscript received 8 January 2026; accepted manuscript online 11 February 2026)

Quantum coherence constitutes a fundamental physical mechanism essential to the study of quantum algorithms. We study coherence and decoherence in the generalized Shor's algorithm where the register A is initialized in an arbitrary pure state, or the combined register AB is initialized in a pseudo-pure state, which encompasses the standard Shor's algorithm as a special case. We derive both lower and upper bounds on the performance of the generalized Shor's algorithm, and establish the relation between the probability of calculating the order r when register AB is initialized in a pseudo-pure state and that when register A is initialized in an arbitrary pure state. Moreover, we study coherence and decoherence in the noisy Shor's algorithm and give a lower bound on the probability that we can calculate the order r.

Keywords: Shor's algorithm, coherence, decoherence, success probability

PACS: 03.67.Ac, 03.65.Yz, 03.67.–a

DOI: 10.1088/1674-1056/ae445e **CSTR:** 32038.14.CPB.ae445e

1. Introduction

Quantum coherence represents a fundamental resource in quantum information processing, derived from the quantum superposition principle, a concept originally formulated to explain interference phenomena in light.[1–3] The rigorous quantification of coherence has been systematically formalized through comprehensive theoretical frameworks,[4,5] which have subsequently facilitated the development of diverse coherence measures with distinct operational interpretations.[6–11] As a quantifiable resource closely connected to other ones, coherence finds many applications in other fields.[12–16] Significant progress has been made in the systematic investigation of coherence manipulation, evolving from fundamental studies on coherence transformations under incoherent operations to sophisticated protocols for multi-mode quantum systems.[17–20] Furthermore, quantum coherence has been extended from orthonormal basis-based to POVM-based.[21–23]

Fisher information stands as a fundamental concept in quantum metrology.[24–26] Using operator monotone metrics, Hansen[27] introduced a class of quantum Fisher information known as metric-adjusted skew information, which encompasses notable examples such as the Wigner–Yanase skew information and the quantum Fisher information based on the symmetric logarithmic derivative. Owing to its versatility and theoretical importance, metric-adjusted skew information has found widespread applications across various domains, including uncertainty relations[28,29] and asymmetry.[30] Sun[31] further demonstrated its utility by quantifying the coherence of quantum states relative to channels using metric-adjusted skew information.

Shor's algorithm[32] enables the efficient factorization of large integers, posing a significant threat to RSA encryption security. Accordingly, great attention has been paid to optimizing its circuit and architectural design to reduce qubit requirements.[33–35] It has been clarified how Shor's algorithm can be implemented in realistic quantum models to break RSA, underscoring the vulnerability of conventional public-key cryptosystems.[36] Despite these advances, resource estimates indicate that breaking standard 2048-bit RSA with Shor's algorithm would still require fault-tolerant quantum hardware with on the order of millions of physical qubits.[37,38] In parallel with large-scale assessments, proof-of-principle demonstrations have also been reported, including implementations based on a single photon encoded in a 32-dimensional quantum state[39] and Qiskit-based circuit realizations for factoring small integers.[40]

Quantum coherence has emerged as a critical resource underpinning the efficacy of quantum algorithms.[41–49] Studies have demonstrated that the Deutsch–Jozsa algorithm's precision correlates directly with recoverable coherence.[50,51] Extensive research has been conducted to elucidate the coherence dynamics in Grover's search algorithm under both ideal and noise-affected conditions, establishing significant correlations between coherence measures and algorithmic success probability.[52–61] Similarly, coherence establishes both upper and lower bounds on Shor's algorithm's performance.[62] More recently, Zhou showed that the generalized Grover algorithm's success probability depends not only on oracle queries

†Corresponding author. E-mail: wuzhaoqi_conquer@163.com

© 2026 Chinese Physical Society and IOP Publishing Ltd. All rights, including for text and data mining, AI training, and similar technologies, are reserved.

but also on the coherence fraction.[63] In this work, we investigate quantum coherence within the framework of a generalized Shor's algorithm.

The remainder of this paper is organized as follows. In Section 2, we review Shor's algorithm and define coherence and decoherence based on the generalized metric-adjusted skew information of ρ with respect to a channel Φ. In Section 3, we investigate the coherence and decoherence dynamics in generalized Shor's algorithm. We derive both lower and upper bounds on the performance of generalized Shor's algorithm when the register is initialized in an arbitrary pure state and derive the relation between the probability of calculating r for an initial arbitrary pure state in register A and for an initial pseudo-pure state in register AB. In Section 4, we study the coherence and decoherence in noisy Shor's algorithm. Finally, we summarize the results in Section 5.

2. Shor's algorithm and coherence quantifiers

In this section, we recall Shor's algorithm and the coherence measures that will be used in this paper.

Given an odd composite positive integer N, the prime factorization problem requires finding its prime factors. It is widely recognized that the factorization of a composite number can be reduced to the problem of order finding. Specifically, for an integer N and a coprime integer x where $x < N$ and $\gcd(x,N) = 1$, the order-finding task involves determining the smallest positive integer r satisfying $x^r \equiv 1 \pmod N$. The algorithm employs a quantum system of n qubits structured into two registers: register A containing t qubits (where $Q = 2^t$) and register B. The composite system AB is initialized in the state $|0\rangle_A^{\otimes t}|1\rangle_B$, establishing the foundation for the quantum computation. The principal steps of Shor's algorithm proceed as follows:[32]

(i) Impose the Hadamard gate

$$H^{\otimes t} = \frac{1}{\sqrt{2^t}}\sum_{x,y}(-1)^{xy}|y\rangle\langle x|$$

on the qubits in register A. This yields the state

$$|\psi_1\rangle = \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle_A|1\rangle_B, \tag{1}$$

and $|\psi_1\rangle$ can be rewritten as $|+\rangle_A^{\otimes t}|1\rangle_B$.

(ii) Consider the unitary operator $U = \sum_{m=0}^{2^t-1}|m\rangle\langle m|_A \otimes U_B^m$ acting on the state $|\psi_1\rangle$, where $U_B|m\rangle_B = |xm \bmod N\rangle_B$ and $U|j\rangle_A|m\rangle_B = |j\rangle_A|x^j m \bmod N\rangle_B$. Then we have

$$|\psi_2\rangle = \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle_A|x^j \bmod N\rangle_B. \tag{2}$$

The eigenvectors of U_B, denoted as $|u_s\rangle_B$, are given by

$$|u_s\rangle_B = \frac{1}{\sqrt{r}}\sum_{a=0}^{r-1}\exp\left(-\frac{2\pi i a s}{r}\right)|x^a \bmod N\rangle_B,$$

where $0 \le s \le r-1$. These eigenvectors correspond to eigenvalues $e^{2\pi i s/r}$, and they satisfy the relation

$$\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|u_s\rangle_B = |1\rangle_B.$$

The state $|\psi_2\rangle$ can be rewritten as

$$\begin{aligned} U|\psi_1\rangle &= \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle_A U_B^j\left(\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|u_s\rangle_B\right) \\ &= \frac{1}{\sqrt{2^t r}}\sum_{s=0}^{r-1}\sum_{j=0}^{2^t-1}\exp\left(2\pi i j\frac{s}{r}\right)|j\rangle_A|u_s\rangle_B. \end{aligned} \tag{3}$$

(iii) By applying the inverse Fourier transform $F^\dagger$ to register A, we obtain

$$\begin{aligned} |\psi_3\rangle &= (F_A^\dagger \otimes \boldsymbol{I}_B)\frac{1}{\sqrt{2^t r}}\sum_{s=0}^{r-1}\sum_{j=0}^{2^t-1}\exp\left(2\pi i j\frac{s}{r}\right)|j\rangle_A|u_s\rangle_B \\ &= \frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}\left(F_A^\dagger\frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}\exp\left(2\pi i j\frac{s}{r}\right)|j\rangle_A\right)(\boldsymbol{I}_B|u_s\rangle_B) = \frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|\psi_s\rangle_A|u_s\rangle_B, \end{aligned} \tag{4}$$

where

$$\begin{aligned} |\psi_s\rangle_A &= \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}\exp\left(2\pi i j\frac{s}{r}\right)(F_A^\dagger|j\rangle_A) \\ &= \frac{1}{2^t}\sum_{j=0}^{2^t-1}\sum_{k=0}^{2^t-1}\exp\left[2\pi i j\left(\frac{s}{r}-\frac{k}{Q}\right)\right]|k\rangle_A \end{aligned}$$

and $\boldsymbol{I}_B$ is the identity operator of register B. The measurement of the first register yields an approximation $k/Q \approx s/r$ where $s \in \{0,1,\ldots,r-1\}$. Here, $|k\rangle_A$ represents a t-bit string that serves as an estimate of the fraction s/r for some s. The probability of measuring outcome k in the first register at step (iii) is given by

$$P_k = \frac{1}{r}\sum_{s=0}^{r-1}\left|\frac{1}{Q}\sum_{j=0}^{2^t-1}\exp\left[2\pi i j\left(\frac{s}{r}-\frac{k}{Q}\right)\right]\right|^2. \tag{5}$$

In essence, the order-finding algorithm randomly selects a value $s \in \{0,1,\ldots,r-1\}$ and generates an approximation to s/r expressed as k/Q. Subsequently, the order r is determined

by employing the continued fraction algorithm.

Denote by $\mathbb{R}^+$ the set of all nonnegative real numbers, and let $f:\mathbb{R}^+\to\mathbb{R}^+$ be an operator monotone function that satisfies $f(0)>0$ and $xf(1/x)=f(x)$. The corresponding Morozova–Chentsov function is then defined as $c_f(x,y)=1/[yf(x/y)]$.[64] For any quantum state ρ and operator K, the generalization of metric-adjusted skew information is defined by[27]

$$F_f(\rho,K)=\frac{f(0)}{2}\langle \mathrm{i}[\rho,K],\mathrm{i}[\rho,K]\rangle_{\rho,f}, \tag{6}$$

where $\langle A,B\rangle_{\rho,f}=\mathrm{tr}[A^\dagger c_f(L_\rho R_\rho)(B)]$ for any operators A and B. Here $L_\rho(A)=\rho A$, $R_\rho(A)=A\rho$, and $[A,B]=AB-BA$ is the commutator between operators A and B. For a pure state $\rho=|\psi\rangle\langle\psi|$ and any operator K, $F_f(\rho,K)$ simply reduces to

$$I(|\psi\rangle\langle\psi|,K)=\frac{1}{2}[\langle\psi|K^\dagger K|\psi\rangle+\langle\psi|KK^\dagger|\psi\rangle]-|\langle\psi|K|\psi\rangle|^2, \tag{7}$$

which reveals that $F_f(\rho,K)$ becomes independent of the function f for any pure state ρ, where $I(\rho,K):=\frac{1}{2}\mathrm{tr}[\sqrt{\rho},K][\sqrt{\rho},K]^\dagger$ is the modified Wigner–Yanase skew information.[65–67]

A quantum channel is a trace-preserving completely positive mapping, which has the following Kraus representation

$$\Phi(\rho)=\sum_{l=1}^m K_l\rho K_l^\dagger,$$

where the set $\{K_l\}_{l=1}^m$ comprises the Kraus operators characterizing the channel, satisfying the completeness relation $\sum_{l=1}^m K_l^\dagger K_l=\boldsymbol{I}$. A key focus in quantum information theory is the quantification of coherence in relation to quantum channels. Suppose that the density matrix ρ has the spectral decomposition $\rho=\sum_i\lambda_i|\phi_i\rangle\langle\phi_i|$. The generalized metric-adjusted skew information of ρ with respect to a channel Φ is given by [31]

$$\begin{aligned}F_f(\rho,\Phi)&=\sum_l F_f(\rho,K_l)\\&=\frac{f(0)}{2}\sum_{ij}\frac{(\lambda_i-\lambda_j)^2}{\lambda_j f(\lambda_i/\lambda_j)}\langle\phi_i|\Phi(|\phi_j\rangle\langle\phi_j|)|\phi_i\rangle.\end{aligned} \tag{8}$$

When ρ in Eq. (8) is a pure state, *i.e.*, $\rho=|\psi\rangle\langle\psi|$, $F_f(\rho,\Phi)$ reduces to

$$F_f(|\psi\rangle\langle\psi|,\Phi)=\frac{1}{2}+\frac{1}{2}\sum_{l=1}^m\langle\psi|K_lK_l^\dagger|\psi\rangle-\sum_{l=1}^m|\langle\psi|K_l|\psi\rangle|^2. \tag{9}$$

In particular, when f in Eq. (8) is chosen as the operator monotone function

$$f(x)=\left(\frac{1+\sqrt{x}}{2}\right)^2,$$

$F_f(\rho,\Phi)$ reduces to the modified Wigner–Yanase skew information [65]

$$I(\rho,\Phi)=\frac{1}{2}\sum_{l=1}^m\mathrm{tr}\,[\sqrt{\rho},K_l]\,[\sqrt{\rho},K_l]^\dagger$$

$$=\frac{1+\mathrm{tr}(\rho\Phi(\boldsymbol{I}))}{2}-\mathrm{tr}(\sqrt{\rho}\Phi(\sqrt{\rho})). \tag{10}$$

Specifically, when ρ in Eq. (10) is a pure state, *i.e.*, $\rho=|\psi\rangle\langle\psi|$, one can find that $I(|\psi\rangle\langle\psi|,\Phi)$ coincides with $F_f(|\psi\rangle\langle\psi|,\Phi)$.

Rather than relying on a single quantity such as the relative entropy of coherence, metric-adjusted skew information offers a more flexible and fine-grained characterization by exploiting the family structure induced by operator monotone functions. Moreover, these quantities admit a clear physical interpretation in parameter estimation,[24,25] quantum metrology,[26] and asymmetry.[30] Owing to their intrinsic connection with quantum Fisher information, they can be viewed not only as quantifiers of decoherence induced by quantum channels, but also as measures directly linked to metrological precision and sensitivity to parameter variations.[31] In contrast, the relative entropy of coherence can be interpreted as the optimal rate for distilling a maximally coherent state from given states.[12]

In Shor's algorithm or the generalized Shor's algorithm, we investigate the coherence of the final state ρ' with respect to the von Neumann measurement $\Pi=\{|i\rangle\langle i|_{AB}\}_{i=0}^{d-1}$, constructed from the orthonormal basis $\{|i\rangle_{AB}\}_{i=0}^{d-1}$ of the d-dimensional Hilbert space as

$$C_f(\rho',\Pi)\triangleq F_f(\rho',\Pi). \tag{11}$$

Correspondingly, the decoherence of the initial state ρ induced by the unitary transformation $\mathcal{S}$ is characterized by

$$D_f(\rho,\mathcal{S})\triangleq F_f(\rho,\mathcal{S}), \tag{12}$$

where $\mathcal{S}(\cdot)=(F_A^\dagger\otimes\boldsymbol{I}_B)U(\cdot)((F_A^\dagger\otimes\boldsymbol{I}_B)U)^\dagger$ represents the composite unitary evolution conducted in Shor's algorithm. When ρ' and ρ are pure states, the coherence of the final state ρ' with respect to the von Neumann measurement is

$$C(\rho',\Pi)\triangleq I(\rho',\Pi), \tag{13}$$

and the decoherence of the initial state ρ induced by the unitary transformation $\mathcal{S}$ is

$$D(\rho,\mathcal{S})\triangleq I(\rho,\mathcal{S}). \tag{14}$$

3. Coherence and decoherence in generalized Shor's algorithm

In Subsection 3.1, we investigate the coherence and decoherence dynamics and derive both lower and upper bounds on the performance of Shor's algorithm when the register A is initialized in an arbitrary pure state. In Subsection 3.2, we investigate the coherence and decoherence dynamics in Shor's algorithm when the register AB is initialized in a pseudo-pure state. We also derive the relationship between the probability of successfully calculating r for an initial pure state in register A and for an initial pseudo-pure state in the combined register AB.

3.1. Coherence and decoherence in Shor's algorithm for arbitrary pure state

Instead of applying the Hadamard gate to obtain

$$|\psi_1\rangle = \frac{1}{\sqrt{Q}} \sum_{j=0}^{Q-1} |j\rangle_A |1\rangle_B,$$

we impose an arbitrary unitary quantum gate U' on the initial state $|0\rangle^{\otimes t}$ of register A, yielding the state in the composite system AB as

$$|\phi_1\rangle = \sum_{j=0}^{Q-1} \alpha_j |j\rangle_A |1\rangle_B, \tag{15}$$

where α_j are complex amplitudes satisfying $\sum_{j=0}^{Q-1} |\alpha_j|^2 = 1$.

Applying the unitary transformation $U = \sum_{n=0}^{Q-1} |n\rangle\langle n|_A \otimes U_B^n$, we then have

$$|\phi_2\rangle = U\left(\sum_{j=0}^{Q-1} \alpha_j |j\rangle_A |1\rangle_B\right) = \sum_{j=0}^{Q-1} \alpha_j |j\rangle_A |x^j \bmod N\rangle_B. \tag{16}$$

Noting that the eigenvectors of U_B are $|u_s\rangle_B$, $|\phi_2\rangle$ can be rewritten as

$$\begin{aligned} U|\phi_1\rangle &= \sum_{j=0}^{2^t-1} \alpha_j |j\rangle_A U_B^j \left(\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle_B\right) \\ &= \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \sum_{j=0}^{2^t-1} \alpha_j \exp\left(2\pi \mathrm{i} j \frac{s}{r}\right) |j\rangle_A |u_s\rangle_B. \end{aligned} \tag{17}$$

Since

$$F_A^\dagger |j\rangle_A = \frac{1}{\sqrt{Q}} \sum_{k=0}^{Q-1} \exp\left(\frac{-2\pi \mathrm{i} jk}{Q}\right) |k\rangle,$$

the state of AB after the inverse Fourier transform $F_A^\dagger$ is imposed on register A is

$$\begin{aligned} |\phi_3\rangle &= (F_A^\dagger \otimes \boldsymbol{I}_B)\left[\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \sum_{j=0}^{2^t-1} \alpha_j \exp\left(2\pi \mathrm{i} j \frac{s}{r}\right) |j\rangle_A |u_s\rangle_B\right] \\ &= \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \sum_{j=0}^{2^t-1} \alpha_j \exp\left(2\pi \mathrm{i} j \frac{s}{r}\right) (F_A^\dagger |j\rangle_A)(\boldsymbol{I}_B |u_s\rangle_B) \\ &= \frac{1}{\sqrt{2^t r}} \sum_{s=0}^{r-1} \sum_{j,k=0}^{2^t-1} \alpha_j \exp\left[2\pi \mathrm{i} j \left(\frac{s}{r} - \frac{k}{Q}\right)\right] |k\rangle_A |u_s\rangle_B. \end{aligned} \tag{18}$$

Note that by applying the inverse Fourier transform $F_A^\dagger$ to Eq. (16), we also obtain

$$\begin{aligned} |\phi_3\rangle &= (F_A^\dagger \otimes \boldsymbol{I}_B)\left(\sum_{j=0}^{Q-1} \alpha_j |j\rangle_A |x^j \bmod N\rangle_B\right) \\ &= \frac{1}{\sqrt{Q}} \sum_{k=0}^{Q-1} \sum_{j=0}^{Q-1} \alpha_j \exp\left(-2\pi \mathrm{i} jk/Q\right) |k\rangle_A |x^j \bmod N\rangle_B. \end{aligned} \tag{19}$$

When measuring register A, the probability of obtaining outcome k is

$$P(k) = \frac{1}{Qr} \sum_{s=0}^{r-1} \left| \sum_{j=0}^{2^t-1} \alpha_j \mathrm{e}^{2\pi \mathrm{i} j(s/r - k/Q)} \right|^2. \tag{20}$$

The quantum circuit for Shor's algorithm in this scenario is illustrated in Fig. 1.

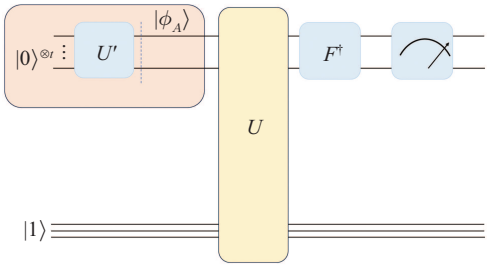


Fig. 1. Quantum circuit for Shor's algorithm when the register A is initialized in an arbitrary pure state.

To simplify the subsequent analysis, we assume that $Q = rm$, where m is a positive integer. Then it follows that

$$\left\lfloor \frac{Q-1}{r} \right\rfloor = m - 1.$$

By decomposing the index j in the form $j = a + br$, where a and b serve as the remainder and quotient respectively, we can reformulate the quantum state $|\phi_3\rangle$, that is,

$$|\phi_3\rangle = \frac{1}{\sqrt{Q}} \sum_{k=0}^{Q-1} \sum_{a=0}^{r-1} \sum_{b=0}^{m-1} \alpha_{a+br} \mathrm{e}^{-2\pi \mathrm{i}(a+br)k/Q} |k\rangle_A |x^a \bmod N\rangle_B,$$

where $0 \le a \le r-1$ and $0 \le b \le m-1$. The probability of obtaining the measurement result k can be rewritten as

$$P(k) = \frac{1}{Q} \sum_{a=0}^{r-1} \left| \sum_{b=0}^{m-1} \alpha_{a+br} \mathrm{e}^{-2\pi \mathrm{i} brk/Q} \right|^2. \tag{21}$$

Denote

$$A_{a,k} = \sum_{b=0}^{m-1} \alpha_{a+br} \mathrm{e}^{-2\pi \mathrm{i} brk/Q}.$$

Then we have

$$P(k) = \frac{1}{Q} \sum_{a=0}^{r-1} |A_{a,k}|^2.$$

Remark 1 When $k = s \cdot (Q/r) = sm$, $s = \{0, 1, \ldots, r-1\}$, we have $\mathrm{e}^{-2\pi \mathrm{i} brk/Q} = \mathrm{e}^{-2\pi \mathrm{i} bs} = 1$, and the formula simplifies to

$$P(k) = \frac{1}{Q} \sum_{a=0}^{r-1} \left| \sum_{b=0}^{m-1} \alpha_{a+br} \right|^2. \tag{22}$$

We now proceed to investigate coherence and decoherence in a generalized Shor's algorithm when the register A is initialized in an arbitrary pure state.

Theorem 1 For the generalized Shor's algorithm with the register A initialized in an arbitrary pure state, the coherence of state $|\phi_3\rangle$ with respect to the von Neumann measurement Π in the computational basis is quantified by

$$C(\rho_3', \Pi) = 1 - \sum_{a=0}^{r-1} \sum_{k=0}^{Q-1} \frac{|A_{a,k}|^4}{Q^2}, \tag{23}$$

where $\Pi(\cdot)=\sum_i K_i(\cdot)K_i^\dagger$, $K_i=|i\rangle\langle i|_{AB}$, ρ_3' represent the density operators of $|\phi_3\rangle$ and $A_{a,k}=\sum_{b=0}^{m-1}\alpha_{a+br}\mathrm{e}^{-2\pi\mathrm{i}brk/Q}$, and the decoherence of the initial state ρ_1' induced by the unitary transformation $\mathcal{S}$ is characterized by

$$D(\rho_1',\mathcal{S})=1-\frac{1}{Q}\left|\sum_{k=0}^{Q-1}\alpha_k A_{0,k}\right|^2, \tag{24}$$

where ρ_1' represents the density operator of $|\phi_1\rangle$ and $A_{0,k}=\sum_{b=0}^{m-1}\alpha_{br}\mathrm{e}^{-2\pi\mathrm{i}brk/Q}$.

Proof Let the density matrix of $|\phi_3\rangle$ be ρ_3'. According to Eqs. (9), (13), and (19), by letting

$$A_{a,k}=\sum_{b=0}^{m-1}\alpha_{a+br}\mathrm{e}^{-2\pi\mathrm{i}brk/Q},$$

we have

$$C(\rho_3',\Pi)=1-\sum_{a=0}^{r-1}\sum_{k=0}^{Q-1}\left|\frac{1}{Q}\sum_{b=0}^{m-1}\sum_{b'=0}^{m-1}\alpha_{a+br}\alpha_{a+b'r}\mathrm{e}^{-2\pi\mathrm{i}(b-b')rk/Q}\right|^2=1-\sum_{a=0}^{r-1}\sum_{k=0}^{Q-1}\frac{|A_{a,k}|^4}{Q^2}.$$

Let the density matrix of $|\phi_1\rangle$ be ρ_1'. According to Eqs. (9), (14), and (15), by letting $A_{0,k}=\sum_{b=0}^{m-1}\alpha_{br}\,\mathrm{e}^{-2\pi\mathrm{i}brk/Q}$, we have

$$D(\rho_1',\mathcal{S})=1-\frac{1}{Q}\left|\sum_{k=0}^{Q-1}\sum_{b=0}^{m-1}\alpha_k\alpha_{br}\mathrm{e}^{-2\pi\mathrm{i}brk/Q}\right|^2=1-\frac{1}{Q}\left|\sum_{k=0}^{Q-1}\alpha_k A_{0,k}\right|^2.$$

Theorem 1 characterizes coherence and decoherence of arbitrary pure initial states in quantum systems. It precisely quantifies the coherence of state ρ_3' under von Neumann measurements and the decoherence of the quantum operation $\mathcal{S}(\cdot)$ on the initial state ρ_1'.

Theorem 2 For the generalized Shor's algorithm with the register A initialized in an arbitrary pure state, the probability that we can calculate r satisfies

$$P>\frac{4Q|\alpha_{\min}|^2\phi(r)}{r\pi^2}, \tag{25}$$

where $|\alpha_{\min}|^2=\min_j|\alpha_j|^2$, ϕ is Euler's totient function, and $\phi(r)$ is the number of integers s that are less than and coprime to r.

Proof According to Eq. (20), the probability of obtaining outcome k in register A satisfies

$$P(k)>\frac{|\alpha_{\min}|^2}{Qr}\sum_{s=0}^{r-1}\left|\sum_{j=0}^{2^t-1}\mathrm{e}^{2\pi\mathrm{i}j(s/r-k/Q)}\right|^2,$$

where $|\alpha_{\min}|^2=\min_j|\alpha_j|^2$. Denote $\sum_{j=0}^{2^t-1}\mathrm{e}^{2\pi\mathrm{i}j(s/r-k/Q)}$ by $\mathcal{S}$. Since $\mathcal{S}$ represents an arithmetic progression, the magnitude squared $|\mathcal{S}|^2$ can be effectively bounded as

$$|\mathcal{S}|^2>\frac{4Q^2}{\pi^2}\quad\text{for}\quad\left|\frac{s}{r}-\frac{k}{Q}\right|<\frac{1}{2Q}.$$

Since the condition $Q>N^2$ holds, this constitutes a sufficient condition ensuring that, given the ratio k/Q, there exists exactly one fraction s/r with $r<N$ that satisfies the aforementioned condition. Thus the probability that k/Q is the best estimate of a fraction with denominator r is

$$P'(k)>\frac{|\alpha_{\min}|^2}{Qr}\cdot\frac{4Q^2}{\pi^2}=\frac{4Q|\alpha_{\min}|^2}{r\pi^2}.$$

For the algorithm to function correctly, we impose the constraint that the numerator s is coprime to r. This requirement is essential because, in the absence of this condition, cancellation of common factors would occur in the fraction s/r, thereby compromising the algorithm's effectiveness.

The number of values of s that satisfy both conditions, being less than r and coprime to r, is given by Euler's totient function $\phi(r)$.[68] Consequently, the probability of successfully calculating r can be estimated by Eq. (25).

Specifically, Hardy and Wright's theorem provides the asymptotic bound $\phi(r)/r>\delta/\log\log r$,[68] where δ is a positive constant. Therefore, by Theorem 2, we can further derive that

$$P>\frac{4Q|\alpha_{\min}|^2\delta}{\pi^2\log\log r}.$$

To obtain an upper bound for the probability that we can calculate r, we first estimate the probability of obtaining outcome k.

Lemma 1 The probability of obtaining outcome k in register A satisfies the following relation:

$$1-C(\rho_3',\Pi)\le\sum_k P(k)^2\le r(1-C(\rho_3',\Pi)), \tag{26}$$

where the upper bound is saturated when the initial state of register A is

$$|\phi\rangle_A=|+\rangle_A^{\otimes t}=\sum_{j=0}^{Q-1}\frac{1}{\sqrt{Q}}|j\rangle_A,$$

and the lower bound is saturated when the initial state of register A is $|\phi\rangle_A=|j\rangle_A$.

Proof From Theorem 1 and Eq. (21), we have

$$\sum_{a=0}^{r-1}|A_{a,k}|^2=QP(k),$$

$$\sum_{a=0}^{r-1}\sum_{k=0}^{Q-1}|A_{a,k}|^4 = Q^2(1-C(\rho_3',\Pi)).$$

By applying the Cauchy–Schwartz inequality for the sequence $\{|A_{a,k}|\}$, we have

$$\left(\sum_{a=0}^{r-1}|A_{a,k}|^2\right)^2 \le r\sum_{a=0}^{r-1}|A_{a,k}|^4.$$

Since $\left(\sum_{a=0}^{r-1}|A_{a,k}|^2\right)^2 = Q^2P(k)^2$, we obtain

$$Q^2P(k)^2 \le r\sum_{a=0}^{r-1}|A_{a,k}|^4.$$

Summing over k yields

$$Q^2\sum_{k=0}^{Q-1}P(k)^2 \le r\sum_{k=0}^{Q-1}\sum_{a=0}^{r-1}|A_{a,k}|^4 = rQ^2\left(1-C(\rho_3',\Pi)\right),$$

which gives an upper bound for $\sum_k P(k)^2$ as

$$\sum_k P(k)^2 \le r(1-C(\rho_3',\Pi)).$$

We next prove the corresponding lower bound. From Eq. (21), we can obtain

$$P(k)^2 = \frac{1}{Q^2}\left(\sum_a |A_{a,k}|^2\right)^2.$$

Expanding the squared term yields

$$\begin{aligned}\left(\sum_a |A_{a,k}|^2\right)^2 &= \sum_a\sum_{a'}|A_{a,k}|^2|A_{a',k}|^2\\ &= \sum_a |A_{a,k}|^4 + \sum_{a\neq a'}|A_{a,k}|^2|A_{a',k}|^2.\end{aligned}$$

Substituting this expansion into the expression for $P(k)^2$ and summing over all k, we obtain

$$\sum_k P(k)^2 = \frac{1}{Q^2}\sum_k\left(\sum_a |A_{a,k}|^4 + \sum_{a\neq a'}|A_{a,k}|^2|A_{a',k}|^2\right).$$

Noting that

$$1-C(\rho_3',\Pi) = \frac{1}{Q^2}\sum_k\sum_a |A_{a,k}|^4,$$

we get

$$\sum_k P(k)^2 \ge 1-C(\rho_3',\Pi).$$

Thus we have derived Eq. (26).

Note that $\sum_k P(k)^2 = r(1-C(\rho_3',\Pi))$ if and only if for any given k, $|A_{a,k}| = \alpha$ for all $a\in\{0,1,\ldots,r-1\}$, where α is a constant. It is easy to check that the upper bound is saturated when the initial state of register A is

$$|\phi\rangle_A = |+\rangle_A^{\otimes t} = \sum_{j=0}^{Q-1}\frac{1}{\sqrt{Q}}|j\rangle_A.$$

On the other hand, $\sum_k P(k)^2 = 1-C(\rho_3',\Pi)$ if and only if for each k, $|A_{a,k}| = 0$ or $|A_{a',k}| = 0$ for $a\neq a'$. It is easy to check that the lower bound is saturated when the initial state of register A is $|\phi\rangle_A = |j\rangle_A$.

Remark 2 From Lemma 1, the lower and upper bounds of the sum of $P(k)^2$ are closely related to the coherence $C(\rho_3',\Pi)$, indicating that $\sum_k P(k)^2$ cannot be too large if the coherence $C(\rho_3',\Pi)$ is large and it cannot be arbitrarily small when the coherence $C(\rho_3',\Pi)$ is very small.

Theorem 3. For the generalized Shor's algorithm with the register A initialized in an arbitrary pure state, the probability of calculating r satisfies the following relation:

$$P^2 < r(1-C(\rho_3',\Pi))\phi^2(r). \tag{27}$$

Proof The probability that k/Q is the best estimate of a fraction with denominator r, *i.e.*,

$$\left|\frac{s}{r}-\frac{k}{Q}\right| < \frac{1}{2Q}$$

satisfies

$$P'^2(k) < \sum_k P(k)^2.$$

We now require that the numerator, s, be coprime to r. Then, the probability of the generalized Shor's algorithm that we can calculate r is $P^2 < \phi^2(r)\sum_k P(k)^2$.

According to Lemma 1, $\sum_k P(k)^2 \le r(1-C(\rho_3',\Pi))$, and thus we get Eq. (27).

We now consider a special case of the global unitary operation U', that is, the local unitary operation acting on an t-qubit quantum register as

$$U' = \left(U'(\alpha,\beta,\theta)\right)^{\otimes t}.$$

Here, the single-qubit unitary gate $U'(\alpha,\beta,\theta)$ is parameterized by three real parameters α, β, and θ, where $\alpha,\beta,\theta\in[0,\pi/2]$, which is of the form

$$U'(\alpha,\beta,\theta) = \begin{bmatrix} e^{i\alpha}\cos\theta & e^{-i\beta}\sin\theta \\ e^{i\beta}\sin\theta & -e^{-i\alpha}\cos\theta\end{bmatrix}.$$

It is worth noting that when $\alpha=\beta=0$ and $\theta=\pi/4$, this gate reduces to the well-known Hadamard operator. When we apply this unitary gate to the single-qubit state $|0\rangle$, the resulting state is

$$\begin{aligned}|\phi(\alpha,\beta,\theta)\rangle &= U'(\alpha,\beta,\theta)|0\rangle\\ &= e^{i\alpha}\cos\theta|0\rangle + e^{i\beta}\sin\theta|1\rangle.\end{aligned}$$

In this case, the initial state and the final state of the register AB respectively are

$$|\phi_1\rangle = |\phi(\alpha,\beta,\theta)\rangle_A^{\otimes t}|1\rangle_B = \sum_{j=0}^{Q-1}\left(\mathrm{e}^{\mathrm{i}\alpha}\cos\theta\right)^{x_j}\left(\mathrm{e}^{\mathrm{i}\beta}\sin\theta\right)^{t-x_j}|j\rangle_A|1\rangle_B,$$

$$|\phi_3\rangle = \frac{1}{\sqrt{Q}}\sum_{k=0}^{Q-1}\sum_{j=0}^{Q-1}\left(\mathrm{e}^{\mathrm{i}\alpha}\cos\theta\right)^{x_j}\left(\mathrm{e}^{\mathrm{i}\beta}\sin\theta\right)^{t-x_j}\mathrm{e}^{-2\pi\mathrm{i}jk/Q}|k\rangle_A|x^j \bmod N\rangle_B,$$

where x_j denotes the number of zeros in the binary representation of $j = j_1 j_2 \cdots j_t$. Moreover, the coherence of state $|\phi_3\rangle$ with respect to the von Neumann measurement Π is

$$C(\rho_3', \Pi) = 1 - \sum_{a=0}^{r-1}\sum_{k=0}^{Q-1}\frac{|E_{a,k}|^4}{Q^2}, \tag{28}$$

where

$$E_{a,k} = \sum_{b=0}^{m-1}\left(\mathrm{e}^{\mathrm{i}\alpha}\cos\theta\right)^{x_{a+br}}\left(\mathrm{e}^{\mathrm{i}\beta}\sin\theta\right)^{t-x_{a+br}}\mathrm{e}^{-2\pi\mathrm{i}brk/Q},$$

and the decoherence of the initial state ρ_1' induced by $\mathcal{S}$ is

$$D(\rho_1', \mathcal{S}) = 1 - \frac{1}{Q}\left|\sum_{k=0}^{Q-1}\left(\mathrm{e}^{\mathrm{i}\alpha}\cos\theta\right)^{x_k}\left(\mathrm{e}^{\mathrm{i}\beta}\sin\theta\right)^{t-x_k}G_{0,k}\right|^2, \tag{29}$$

where

$$G_{0,k} = \sum_{b=0}^{m-1}\left(\mathrm{e}^{\mathrm{i}\alpha}\cos\theta\right)^{x_b r}\left(\mathrm{e}^{\mathrm{i}\beta}\sin\theta\right)^{t-x_b r}\mathrm{e}^{-2\pi\mathrm{i}brk/Q}.$$

When $\theta < \pi/4$, we have $|\alpha_{\min}|^2 = \min_j|\alpha_j|^2 = \sin^{2t}\theta$, and the probability that we can calculate r is

$$P > \frac{4Q\sin^{2t}\theta\phi(r)}{r\pi^2}.$$

When $\theta > \pi/4$, we have $|\alpha_{\min}|^2 = \min_j|\alpha_j|^2 = \cos^{2t}\theta$, and the probability that we can calculate r is

$$P > \frac{4Q\cos^{2t}\theta\phi(r)}{r\pi^2}.$$

When $\theta = \pi/4$, we have $|\alpha_{\min}|^2 = \min_j|\alpha_j|^2 = 1/Q$, and the probability that we can calculate r is

$$P > 4\phi(r)/r\pi^2.$$

Note that the state $|\phi_1\rangle$ here corresponds to the state in Eq. (15) in which $\alpha_j = \left(\mathrm{e}^{\mathrm{i}\alpha}\cos\theta\right)^{x_j}\left(\mathrm{e}^{\mathrm{i}\beta}\sin\theta\right)^{t-x_j}$. So when $\alpha = \beta = 0$ and $\theta = \pi/4$, $U'(\alpha,\beta,\theta)$ reduces to the Hadamard operator, which corresponds to the original Shor's algorithm where all $\alpha_j = 1/\sqrt{Q}$. This leads to the following result.

Corollary 1 The coherence of state $|\psi_3\rangle$ with respect to the von Neumann measurement Π in the computational basis is given by

$$C(\rho_3, \Pi) = 1 - \frac{1}{r^2}, \tag{30}$$

where ρ_3 is the density operator of $|\psi_3\rangle$ and r is the order of Shor's algorithm, and the decoherence of the initial state ρ_1' induced by $\mathcal{S}$ is

$$D(\rho_1, \mathcal{S}) = 1 - 1/Q, \tag{31}$$

where ρ_1 is the density operator of $|\psi_1\rangle$ and $Q = 2^t$ is the dimension of register A.

3.2. Coherence and decoherence in Shor's algorithm for any pseudo-pure state

Pseudo-pure states can be effectively prepared using existing techniques,[69–71] and play a crucial role in quantum computation in the presence of noise. Indeed, the utility of pseudo-pure states for nuclear magnetic resonance (NMR) quantum computation has been recognized.[72] It is shown that an entanglement-free version of the Bernstein–Vazirani (BV) algorithm on an NMR ensemble quantum computer can be implemented,[73] and for a given bounded purity, pseudo-pure states are the quantum states that achieve optimal performance in the probabilistic BV algorithm.[48]

Consider Shor's algorithm with the register AB initialized in a pseudo-pure state[70]

$$\rho_1^{\varepsilon} = (1-\varepsilon)|\phi_1\rangle\langle\phi_1| + (\varepsilon/d)\boldsymbol{I}_{AB}, \tag{32}$$

where $0 \le \varepsilon \le 1$, $|\phi_1\rangle = \sum_{j=0}^{Q-1}\alpha_j|j\rangle_A|1\rangle_B$, and $d = 2^n$ denote the dimension of the composite system AB. It is one of the simplest models for mixed-state quantum computation. After applying the unitary transformation

$$U = \sum_{n=0}^{Q-1}|n\rangle\langle n|_A \otimes U_B^n,$$

the resulting state becomes

$$\rho_2^{\varepsilon} = (1-\varepsilon)|\phi_2\rangle\langle\phi_2| + \frac{\varepsilon}{d}\boldsymbol{I}_{AB}, \tag{33}$$

where

$$|\phi_2\rangle = \sum_{j=0}^{Q-1}\alpha_j|j\rangle_A|x^j \bmod N\rangle_B.$$

Applying the inverse Fourier transform $F^{\dagger}$ to register A yields

$$\rho_3^{\varepsilon} = (1-\varepsilon)|\phi_3\rangle\langle\phi_3| + \frac{\varepsilon}{d}\boldsymbol{I}_{AB}, \tag{34}$$

where

$$|\phi_3\rangle = \frac{1}{\sqrt{Q}}\sum_{k=0}^{Q-1}\sum_{j=0}^{Q-1}\alpha_j\mathrm{e}^{-2\pi\mathrm{i}jk/Q}|k\rangle_A|x^j \bmod N\rangle_B.$$

When measuring register A, the probability of obtaining outcome k is

$$P_{\varepsilon}(k) = (1-\varepsilon)P(k) + \varepsilon/Q. \tag{35}$$

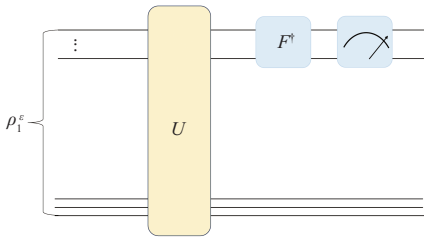


Fig. 2. Quantum circuit for Shor's algorithm when the register AB is initialized in a pseudo-pure state.

For large Q, the probability of obtaining outcome k with the register AB initialized in a pseudo-pure state is approximately proportional to the probability of obtaining outcome k with the register A initialized in an arbitrary pure state. The quantum circuit for Shor's algorithm in this scenario is illustrated in Fig. 2.

Theorem 4 For the generalized Shor's algorithm with the register AB initialized in a pseudo-pure state, the coherence of the state ρ_3^ε with respect to the von Neumann measurement Π in the computational basis is quantified by

$$C_f(\rho_3^\varepsilon,\Pi)=\frac{f(0)(1-\varepsilon)^2C(\rho_3',\Pi)}{2}\left[\frac{d}{\varepsilon\cdot f\left(\frac{d-(d-1)\varepsilon}{\varepsilon}\right)}+\frac{d}{(d-(d-1)\varepsilon)\cdot f\left(\frac{\varepsilon}{d-(d-1)\varepsilon}\right)}\right], \tag{36}$$

where $0<\varepsilon\leq 1$ and $C(\rho_3',\Pi)$ represent the coherence of $|\phi_3\rangle$, and the decoherence of the initial state ρ_1^ε induced by the unitary transformation $\mathcal{S}$ is

$$D_f(\rho_1^\varepsilon,\mathcal{S})=\frac{f(0)(1-\varepsilon)^2D(\rho_1',\Pi)}{2}\left[\frac{d}{\varepsilon\cdot f\left(\frac{d-(d-1)\varepsilon}{\varepsilon}\right)}+\frac{d}{(d-(d-1)\varepsilon)\cdot f\left(\frac{\varepsilon}{d-(d-1)\varepsilon}\right)}\right], \tag{37}$$

where $0<\varepsilon\leq 1$ and $D(\rho_1',\Pi)$ represent the decoherence of $|\phi_1\rangle$.

Proof The spectral decomposition of the state ρ_3^ε takes the form

$$\rho_3^\varepsilon=\lambda_1|\phi_3\rangle\langle\phi_3|+\sum_{j=2}^{d}\lambda_j|\varphi_j\rangle\langle\varphi_j|,$$

where $\lambda_1=1-\frac{(d-1)\varepsilon}{d}$ and $\lambda_j=\frac{\varepsilon}{d}$ $(j\in\{2,3,\ldots,d\})$. Here, $\{|\varphi_j\rangle\}_{j=1}^d$ represents the orthonormal basis, where $|\varphi_1\rangle=|\phi_3\rangle$ and the remaining states $|\varphi_j\rangle$ satisfy $\langle\varphi_j|\phi_3\rangle=0$ for $j\geq 2$. Utilizing the orthogonality relation $\sum_{j=2}^d|\varphi_j\rangle\langle\varphi_j|=\boldsymbol{I}_{AB}-|\phi_3\rangle\langle\phi_3|$, we can rewrite this as

$$\rho_3^\varepsilon=\left(1-\frac{(d-1)\varepsilon}{d}\right)|\phi_3\rangle\langle\phi_3|+\frac{\varepsilon}{d}\left(\boldsymbol{I}_{AB}-|\phi_3\rangle\langle\phi_3|\right).$$

According to Eqs. (8) and (11), the coherence of state ρ_3^ε with respect to the von Neumann measurement Π is

$$C_f(\rho_3^\varepsilon,\Pi)=\sum_i F_f(\rho,K_i)=\frac{f(0)}{2}\sum_{jk}\frac{(\lambda_j-\lambda_k)^2}{\lambda_k f(\lambda_j/\lambda_k)}\langle\varphi_j|\Pi(|\varphi_k\rangle\langle\varphi_k|)|\varphi_j\rangle.$$

After algebraic manipulation, the result of $C_f(\rho_3^\varepsilon,\Pi)$ is

$$\frac{f(0)(1-\varepsilon)^2}{2}\left[\frac{d}{\varepsilon\cdot f\left(\frac{d-(d-1)\varepsilon}{\varepsilon}\right)}+\frac{d}{(d-(d-1)\varepsilon)\cdot f\left(\frac{\varepsilon}{d-(d-1)\varepsilon}\right)}\right]\left(1-\sum_{i=0}^{d-1}|\langle i|\phi_3\rangle|^4\right),$$

where $0<\varepsilon\leq 1$, and $\langle i|$ denotes $\langle i|_{AB}$ for the sake of simplicity. The coherence of $|\phi_3\rangle$ with respect to the von Neumann measurement Π is $1-\sum_{i=0}^{d-1}|\langle i|\phi_3\rangle|^4$. Thus we can derive Eq. (36). The spectral decomposition of the state ρ_1^ε takes the form $\rho_1^\varepsilon=\lambda_1|\phi_1\rangle\langle\phi_1|+\sum_{j=2}^d\lambda_j|\varphi_j'\rangle\langle\varphi_j'|$, where $\lambda_1=1-\frac{(d-1)\varepsilon}{d}$ and $\lambda_j=\frac{\varepsilon}{d}$ $(j\in\{2,3,\ldots,d\})$. Here, $\{|\varphi_j'\rangle\}_{j=1}^d$ is an orthonormal basis with $|\varphi_1'\rangle=|\phi_1\rangle$ and $\langle\varphi_j'|\phi_1\rangle=0$ for $j\geq 2$.

According to Eqs. (8) and (12), the decoherence of the initial state ρ_1^ε induced by the unitary transformation $\mathcal{S}$ is shown below:

$$D_f(\rho_1^\varepsilon,\mathcal{S})=F_f(\rho_1^\varepsilon,\mathcal{S})=\frac{f(0)}{2}\sum_{jk}\frac{(\lambda_j-\lambda_k)^2}{\lambda_k f(\lambda_j/\lambda_k)}\langle\varphi_j'|S(|\varphi_k'\rangle\langle\varphi_k'|)|\varphi_j'\rangle.$$

The value of decoherence $D_f(\rho_1^\varepsilon,\mathcal{S})$ is

$$\frac{f(0)(1-\varepsilon)^2}{2}\left[\frac{d}{\varepsilon\cdot f\left(\frac{d-(d-1)\varepsilon}{\varepsilon}\right)}+\frac{d}{(d-(d-1)\varepsilon)\cdot f\left(\frac{\varepsilon}{d-(d-1)\varepsilon}\right)}\right]\left(1-|\langle\phi_1|\phi_3\rangle|^2\right),$$

where $0 < \varepsilon \leq 1$. Noting that the decoherence of the initial state ρ_1' induced by the unitary transformation $\mathcal{S}$ is $1 - |\langle\phi_1|\phi_3\rangle|^2$, we obtain Eq. (37).

After algebraic manipulation, the square root is given by

$$\sqrt{\rho_3^\varepsilon} = \sqrt{\frac{\varepsilon}{d}}\boldsymbol{I}_{AB} + \left(\sqrt{1-\frac{(d-1)\varepsilon}{d}} - \sqrt{\frac{\varepsilon}{d}}\right)|\phi_3\rangle\langle\phi_3|.$$

Let the operator monotone function be $f(x) = \left(\frac{1+\sqrt{x}}{2}\right)^2$. Then we can obtain the following result.

Corollary 2 The coherence of state ρ_3^ε with respect to the von Neumann measurement Π is given by

$$C(\rho_3^\varepsilon, \Pi) = \left(\sqrt{1-\frac{(d-1)\varepsilon}{d}} - \sqrt{\frac{\varepsilon}{d}}\right)^2 C(\rho_3', \Pi), \quad (38)$$

where $C(\rho_3', \Pi)$ represents the coherence of $|\phi_3\rangle$, and the decoherence of the initial state ρ_1^ε induced by the unitary transformation $\mathcal{S}$ is

$$D(\rho_1^\varepsilon, \mathcal{S}) = \left(\sqrt{1-\frac{(d-1)\varepsilon}{d}} - \sqrt{\frac{\varepsilon}{d}}\right)^2 D(\rho_1', \mathcal{S}), \quad (39)$$

where $D(\rho_1', S)$ represents the decoherence of $|\phi_1\rangle$.

Theorem 5 The probability that we can calculate r when the register AB is initialized in a pseudo-pure state and the one when the register A is initialized in an arbitrary pure state exhibit the following relation:

$$P(\rho_3^\varepsilon) = (1-\varepsilon)P + \frac{\varepsilon\phi(r)}{Q}. \quad (40)$$

Proof According to Eq. (35), the probability that k/Q is the best estimate of a fraction with denominator r, *i.e.*,

$$\left|\frac{s}{r} - \frac{k}{Q}\right| < \frac{1}{2Q},$$

satisfies

$$P_\varepsilon'(k) = (1-\varepsilon)P'(k) + \frac{\varepsilon}{Q}.$$

We now require that the numerator s is coprime to r. There are $\phi(r)$ values of s which are less than and coprime to r. Then, the probability that we can calculate r when the register AB is initialized in a pseudo-pure state is

$$P(\rho_3^\varepsilon) = P_\varepsilon'(k)\phi(r) = (1-\varepsilon)P'(k)\phi(r) + \frac{\varepsilon\phi(r)}{Q}.$$

Since $P'(k)\phi(r) = P$, we obtain Eq. (40).

4. Coherence and decoherence in noisy Shor's algorithm

In the real world, quantum systems cannot be completely isolated from their environment and are subject to various noise influences. Furthermore, quantum systems inevitably interact with their surrounding environments, leading to decoherence phenomena. In this section, we investigate coherence and decoherence in noisy Shor's algorithm.

Now we consider an important channel Φ acting on a d-dimensional quantum system called the depolarizing channel,[74–76]

$$\Phi(\rho) = \lambda V\rho V^\dagger + (1-\lambda)\frac{\boldsymbol{I}_{AB}}{d}, \quad \frac{-1}{d^2-1} \leq \lambda \leq 1,$$

where V represents an arbitrary unitary operator. The parameter λ is chosen to ensure that the channel Φ maintains complete positivity, which is essential for physical realizability. Since all depolarizing channels satisfy the unitality condition ($\Phi(\boldsymbol{I}) = \boldsymbol{I}$), the set of depolarizing channels constitutes a proper subset of the broader class of unital channels. When $\lambda = 0$, Φ reduces to the completely depolarizing channel, which maps any input state to the maximally mixed state $\boldsymbol{I}_{AB}/d$.

The depolarizing channel exhibits the fundamental property of unitary invariance and constitutes a significant subclass of commutativity-preserving channels. It possesses the remarkable characteristic of never increasing quantumness between any two quantum states. When $\lambda \neq 0$, the depolarizing channel stands as one of the few channel types incapable of creating quantum discord in zero quantum discord states. Moreover, for quantum systems with dimension $n \geq 3$, it occupies a privileged position due to its unique bidirectional property of preserving quantum correlations, distinguishing it from other quantum channels in the context of quantum information theory.

Here, we discuss the case $V = W_A \otimes \boldsymbol{I}_B$ where $W_A = \sum_x e^{i\theta_x}|x\rangle\langle x|$ is an arbitrary diagonal unitary matrix. This specific scenario allows us to examine the properties and implications of diagonal unitarity within quantum computational frameworks. Let Φ be the noise channel. Then the noisy Shor's algorithm can be described as

$$\mathcal{E} = (\mathcal{F}^\dagger \otimes \mathbb{I}) \circ \Phi \circ \mathcal{U} \circ \Phi, \quad (41)$$

where $\Phi(\rho) = \lambda(W_A \otimes \boldsymbol{I}_B)\rho(W_A \otimes \boldsymbol{I}_B) + (1-\lambda)(\boldsymbol{I}_{AB}/d)$, $(\mathcal{F}^\dagger \otimes \mathbb{I})(\rho) = (F_A^\dagger \otimes \boldsymbol{I}_B)\rho(F_A \otimes \boldsymbol{I}_B)$, and $\mathcal{U} = U\rho U^\dagger$. By applying the Hadamard gate, we obtain the initial state

$$|\psi_1\rangle = \frac{1}{\sqrt{Q}}\sum_{j=0}^{Q-1}|j\rangle_A|1\rangle_B.$$

Subsequently, applying the operator $W_A \otimes \boldsymbol{I}_B$ to this state yields

$$(W_A \otimes \boldsymbol{I}_B)|\psi_1\rangle = \frac{1}{\sqrt{Q}}\sum_j e^{i\theta_j}|j\rangle_A|1\rangle_B.$$

Next, we consider the unitary transformation U acting on the previously obtained state, and obtain

$$|\psi_2'\rangle = U(W_A \otimes \boldsymbol{I}_B)|\psi_1\rangle = \frac{1}{\sqrt{Q}}\sum_j e^{i\theta_j}|j\rangle_A|x^j \bmod N\rangle_B.$$

By applying the operator $W_A \otimes \boldsymbol{I}_B$ to the state $|\psi_2'\rangle$, we obtain

$$(W_A \otimes \boldsymbol{I}_B)U(W_A \otimes \boldsymbol{I}_B)|\psi_1\rangle = \frac{1}{\sqrt{Q}}\sum_j e^{2i\theta_j}|j\rangle_A|x^j \bmod N\rangle_B.$$

Finally, by using the inverse Fourier transform $F_A^\dagger \otimes \boldsymbol{I}_B$, we get

$$|\psi_3'\rangle = (F_A^\dagger \otimes \boldsymbol{I}_B)(W_A \otimes \boldsymbol{I}_B)U(W_A \otimes \boldsymbol{I}_B)|\psi_1\rangle = \frac{1}{Q}\sum_{j,k} \mathrm{e}^{2\mathrm{i}\theta_j} \exp\left(\frac{-2\pi \mathrm{i} jk}{Q}\right)|k\rangle_A |x^j \bmod N\rangle_B.$$

Then the state after the noisy Shor's algorithm can be described as

$$\begin{aligned}\mathcal{E}(|\psi_1\rangle\langle\psi_1|) &= (\mathcal{F}^\dagger \otimes \boldsymbol{I}) \circ \Phi \circ \mathcal{U}\left(\lambda (W_A \otimes \boldsymbol{I}_B)|\psi_1\rangle\langle\psi_1|(W_A^\dagger \otimes \boldsymbol{I}_B) + (1-\lambda)\frac{\boldsymbol{I}_{AB}}{d}\right) \\ &= \lambda^2 |\psi_3'\rangle\langle\psi_3'| + (1-\lambda^2)\frac{\boldsymbol{I}_{AB}}{d}.\end{aligned}$$

Theorem 6 For the noisy Shor's algorithm caused by the depolarizing channel where $W_A = \sum_x \exp(\mathrm{i}\pi x/Q)|x\rangle\langle x|$, the coherence of state σ_3 with respect to the von Neumann measurement Π is quantified by

$$C_f(\sigma_3, \Pi) = \frac{f(0)\lambda^4}{2}\left(1 - \frac{1}{r^2}\right)\left[\frac{d}{(1-\lambda^2)\cdot f\left(\frac{\lambda^2(d-1)+1}{1-\lambda^2}\right)} + \frac{d}{(\lambda^2(d-1)+1)\cdot f\left(\frac{1-\lambda^2}{\lambda^2(d-1)+1}\right)}\right], \tag{42}$$

where $\frac{-1}{d^2-1} \le \lambda < 1$ and $d = 2^n$ are the dimensions of the composite system AB, and the decoherence of the initial state ρ_1 induced by the quantum channel $\mathcal{E}$ during noisy Shor's algorithm is characterized by

$$D(\rho_1, \mathcal{E}) = \lambda^2\left(\frac{1}{d} - \frac{1}{Q}\right) + \frac{d-1}{d}. \tag{43}$$

Proof Let $\sigma_3 = \mathcal{E}(|\psi_1\rangle\langle\psi_1|)$. The spectral decomposition of the state σ_3 takes the form

$$\sigma_3 = \lambda_1 |\psi_3'\rangle\langle\psi_3'| + \sum_{j=2}^{d} \lambda_j |\varphi_j''\rangle\langle\varphi_j''|,$$

where $\lambda_1 = 1 - \frac{(d-1)(1-\lambda^2)}{d}$ and $\lambda_j = \frac{1-\lambda^2}{d}$ $(j \in \{2,3,\ldots,d\})$. Here, $\{|\varphi_j''\rangle\}_{j=1}^d$ represents the orthonormal basis, where $|\varphi_1''\rangle = |\psi_3'\rangle$ and $\langle\varphi_j''|\psi_3'\rangle = 0$ for $j \ge 2$. According to Eqs. (8) and (11), the coherence of the state σ_3 with respect to the von Neumann measurement Π is

$$C_f(\sigma_3, \Pi) = \sum_i F_f(\sigma_3, K_i) = \frac{f(0)}{2}\sum_{jk}\frac{(\lambda_j - \lambda_k)^2}{\lambda_k f(\lambda_j/\lambda_k)}\langle\varphi_j''|\Pi(|\varphi_k''\rangle\langle\varphi_k''|)|\varphi_j''\rangle.$$

Utilizing the relation $\sum_{j=2}^d |\varphi_j''\rangle\langle\varphi_j''| = \boldsymbol{I}_{AB} - |\psi_3'\rangle\langle\psi_3'|$, after algebraic manipulation, the value of $C_f(\sigma_3, \Pi)$ is

$$\frac{f(0)\lambda^4}{2}\left[\frac{d}{(1-\lambda^2)\cdot f\left(\frac{\lambda^2(d-1)+1}{1-\lambda^2}\right)} + \frac{d}{(\lambda^2(d-1)+1)\cdot f\left(\frac{1-\lambda^2}{\lambda^2(d-1)+1}\right)}\right]\left(1 - \sum_{i=0}^{d-1}|\langle i|\psi_3'\rangle|^4\right),$$

where $\lambda \ne 1$ and $\langle i|$ denote $\langle i|_{AB}$ for the sake of simplicity. To simplify the analysis, we set $Q = rm$ where m is a positive integer, which implies that $\left\lfloor \frac{Q-1}{r} \right\rfloor = m-1$. Decomposing the index j as $j = a + br$, where a is the remainder and b is the quotient, we can rewrite the state $|\psi_3'\rangle$ as

$$|\psi_3'\rangle = \frac{1}{Q}\sum_{k=0}^{Q-1}\sum_{a=0}^{r-1}\sum_{b=0}^{m-1} \mathrm{e}^{2\mathrm{i}\theta_{a+br}} \exp\left(\frac{-2\pi\mathrm{i}(a+br)k}{Q}\right)|k\rangle_A |x^a \bmod N\rangle_B.$$

The coherence of $|\psi_3'\rangle$ with respect to the von Neumann measurement Π is $1 - \sum_{i=0}^{d-1}|\langle i|\psi_3'\rangle|^4$. When $W_A = \sum_x \mathrm{e}^{\frac{\mathrm{i}\pi x}{Q}}|x\rangle\langle x|$, we obtain

$$\begin{aligned}1 - \sum_{i=0}^{d-1}|\langle i|\psi_3'\rangle|^4 &= 1 - \frac{1}{Q^4}\sum_{k=0}^{Q-1}\sum_{a=0}^{r-1}\left|\sum_{b=0}^{m-1} \mathrm{e}^{2\mathrm{i}\theta_{a+br}} \exp\left(\frac{-2\pi\mathrm{i}kbr}{Q}\right)\right|^4 \\ &= 1 - \frac{1}{Q^4}\sum_{k=0}^{Q-1}\sum_{a=0}^{r-1}\left|\sum_{b=0}^{m-1} \exp\left(\frac{-2\pi\mathrm{i}b(k-1)}{m}\right)\right|^4 = 1 - \frac{1}{r^2}.\end{aligned}$$

Thus we can derive Eq. (42). According to Eqs. (10) and (14), we have

$$D(\rho_1, \mathcal{E}) = \frac{1 + \mathrm{tr}(\rho_1 \mathcal{E}(\boldsymbol{I}_{AB}))}{2} - \mathrm{tr}(\rho_1 \mathcal{E}(\rho)) = \frac{d - 1 + \lambda^2}{d} - \lambda^2 |\langle\psi_1|\psi_3'\rangle|^2.$$

Direct calculations show that

$$\begin{aligned}&\left|\langle\psi_1|\psi_3'\rangle\right|^2\\&=\frac{1}{Q^3}\left|\sum_{k=0}^{Q-1}\sum_{b=0}^{m-1}\mathrm{e}^{2\mathrm{i}\theta_{br}}\exp\left(\frac{-2\pi\mathrm{i}brk}{Q}\right)\right|^2\\&=\frac{1}{Q^3}\left|\mathrm{e}^{2\mathrm{i}\theta_0}Q\right|^2=\frac{1}{Q}.\end{aligned}$$

Therefore, Eq. (43) holds.

Taking $f(x)=\left(\frac{1+\sqrt{x}}{2}\right)^2$, we immediately obtain the following result.

Corollary 3 For the noisy Shor's algorithm caused by the depolarizing channel where $W_A=\sum_x \mathrm{e}^{\mathrm{i}\pi x/Q}|x\rangle\langle x|$, the coherence of state σ_3 with respect to the von Neumann measurement Π is given by

$$\begin{aligned}&C(\sigma_3,\Pi)\\&=\left(\sqrt{1-\frac{(d-1)(1-\lambda^2)}{d}}-\sqrt{\frac{1-\lambda^2}{d}}\right)^2\left(1-\frac{1}{r^2}\right).\end{aligned}\tag{44}$$

Since $-1/(d^2-1)\le\lambda\le 1$, we can obtain $1-1/Q\le D(\rho_1,\mathcal{E})\le 1-1/d$ and $0\le C(\sigma_3,\Pi)\le 1-1/r^2$. When $\lambda=0$, Φ reduces to the completely depolarizing channel, which maps any input state to the maximally mixed state $\boldsymbol{I}_{AB}/d$, resulting in the complete loss of information from the original state. In this scenario, the decoherence induced on the state $|\psi_1\rangle$ by the channel $\mathcal{E}$ reaches its maximum value, quantified as $D(\rho_1,\mathcal{E})=1-1/d$. However, the coherence of state σ_3 with respect to Π reaches its minimum value of 0 when $W_A=\sum_x \mathrm{e}^{\mathrm{i}\pi x/Q}|x\rangle\langle x|$.

When $\lambda=1$, Φ reduces to a unitary channel, which merely performs a unitary transformation while perfectly preserving the quantum state information. Under these conditions, the decoherence induced on the state $|\psi_1\rangle$ by the channel $\mathcal{E}$ attains its minimum value, represented as $D(\rho_1,\mathcal{E})=1-1/Q$. When $W_A=\sum_x \mathrm{e}^{\mathrm{i}\pi x/Q}|x\rangle\langle x|$, the coherence of state σ_3 with respect to Π reaches its maximum value of $1-1/r^2$. Furthermore, $\lambda=-1/(d^2-1)$ represents the critical parameter value for maintaining complete positivity of the channel. Any value of λ smaller than this threshold would cause the channel to lose its complete positivity property. At this critical point, the decoherence and coherence are given by

$$\begin{aligned}&D(\rho_1,\mathcal{E})=\frac{1}{(d^2-1)^2}\times(1/d-1/Q)+(d-1)/d,\\&C(\sigma_3,\Pi)=\left(\sqrt{1-\frac{d(d-1)(d^2-2)}{(d^2-1)^2}}-\sqrt{\frac{d(d^2-2)}{(d^2-1)^2}}\right)^2\\&\qquad\times\left(1-\frac{1}{r^2}\right).\end{aligned}$$

Since the eigenvectors of U_B are $|u_s\rangle$, $|\psi_2'\rangle$ can be rewritten as follows:

$$\begin{aligned}&U\frac{1}{\sqrt{Q}}\sum_{j=0}^{2^t-1}\mathrm{e}^{\mathrm{i}\theta_j}|j\rangle_A|1\rangle_B\\&=\sum_{j=0}^{2^t-1}\frac{1}{\sqrt{Q}}\mathrm{e}^{\mathrm{i}\theta_j}|j\rangle_A U_B^j\left(\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|u_s\rangle_B\right)\\&=\frac{1}{\sqrt{Qr}}\sum_{j=0}^{2^t-1}\sum_{s=0}^{r-1}\mathrm{e}^{\mathrm{i}\theta_j}\exp\left(2\pi\mathrm{i}j\frac{s}{r}\right)|j\rangle_A|u_s\rangle_B.\end{aligned}\tag{45}$$

We then apply the operator $W_A\otimes\boldsymbol{I}_B$ and the inverse Fourier transform $F^\dagger$; $|\psi_3'\rangle$ can be rewritten as

$$\begin{aligned}&(F_A^\dagger\otimes\boldsymbol{I}_B)\left(\frac{1}{\sqrt{Qr}}\sum_{j=0}^{2^t-1}\sum_{s=0}^{r-1}\mathrm{e}^{2\mathrm{i}\theta_j}\exp\left(2\pi\mathrm{i}j\frac{s}{r}|j\rangle_A|u_s\rangle_B\right)\right)\\&=\frac{1}{Q\sqrt{r}}\sum_{j,k=0}^{2^t-1}\sum_{s=0}^{r-1}\mathrm{e}^{\mathrm{i}\theta_j}\exp\left[2\pi\mathrm{i}j\left(\frac{s}{r}-\frac{k}{Q}\right)\right]|k\rangle_A|u_s\rangle_B.\end{aligned}\tag{46}$$

When measuring register A, the probability of obtaining outcome k is

$$P_\lambda(k)=\sum_{j=0}^{2^{n-t}-1}\left\langle k,j\left|\left[\lambda^2|\psi_3'\rangle\langle\psi_3'|+(1-\lambda^2)\frac{\boldsymbol{I}_{AB}}{d}\right]\right|k,j\right\rangle.\tag{47}$$

Theorem 7 When $W_A=\sum_x \mathrm{e}^{\mathrm{i}\pi x/6Q}|x\rangle\langle x|$, the probability that we can calculate r in noisy Shor's algorithm is

$$P_\lambda>\frac{27\lambda^2\phi(r)}{16r\pi^2}+\frac{(1-\lambda^2)\phi(r)}{Q}.\tag{48}$$

Proof Let $P_{|\psi_3'\rangle}(k)=\sum_{j=0}^{2^{n-t}-1}\langle k,j|\psi_3'\rangle\langle\psi_3'|k,j\rangle$. Through rigorous calculations, we have

$$P_{|\psi_3'\rangle}(k)=\frac{1}{Q^2r}\sum_{s=0}^{r-1}\left|\sum_{j=0}^{2^t-1}\mathrm{e}^{2\mathrm{i}\theta_j}\exp\left[2\pi\mathrm{i}j\left(\frac{s}{r}-\frac{k}{Q}\right)\right]\right|^2.$$

When

$$W_A=\sum_x\exp(\mathrm{i}\pi x/6Q)\,|x\rangle\langle x|,$$

we have

$$P_{|\psi_3'\rangle}(k)=\frac{1}{Q^2r}\sum_{s=0}^{r-1}\left|\sum_{j=0}^{2^t-1}\exp\left[2\pi\mathrm{i}j\left(\frac{s}{r}-\frac{k}{Q}+\frac{1}{6Q}\right)\right]\right|^2.$$

Denote

$$\sum_{j=0}^{2^t-1}\exp\left[2\pi\mathrm{i}j\left(\frac{s}{r}-\frac{k}{Q}+\frac{1}{6Q}\right)\right]$$

by R. Specifically, we have

$$|R|^2>\frac{27Q^2}{16\pi^2}\quad\text{for}\quad\left|\frac{s}{r}-\frac{k}{Q}\right|<\frac{1}{2Q}.$$

According to Eq. (47), we obtain that the probability of obtaining outcome k is

$$P_\lambda(k)=\lambda^2P_{|\psi_3'\rangle}(k)+\frac{1-\lambda^2}{Q}.$$

For any given ratio k/Q, there exists a unique fraction s/r with $r<N$ satisfying this condition. Consequently, the probability

that k/Q serves as the optimal approximation to a fraction with denominator r satisfies

$$P'_\lambda(k) > \frac{27\lambda^2}{16r\pi^2} + \frac{1-\lambda^2}{Q}.$$

The algorithm requires that the numerator s be coprime to r, preventing cancellation of common factors that would otherwise reduce the fraction s/r. Then the probability of successfully calculating r becomes

$$P_\lambda > \frac{27\lambda^2\phi(r)}{16r\pi^2} + \frac{(1-\lambda^2)\phi(r)}{Q}.$$

Remark 3 When $W_A = \sum_x \exp(\mathrm{i}\pi x/Q)\,|x\rangle\langle x|$, the probability of obtaining outcome k with decoherence of the initial state ρ_1 satisfies the following relation:

$$D(\rho_1,\mathcal{E}) - P_\lambda(k) = \gamma(\lambda), \tag{49}$$

where

$$\gamma(\lambda) = \lambda^2\left(\frac{1}{d} - \frac{1}{r}\right) + 1 - \frac{1}{d} - \frac{1}{Q}.$$

Since

$$\frac{-1}{d^2-1} \le \lambda \le 1,$$

we obtain

$$1 - \frac{1}{r} - \frac{1}{Q} \le D(\rho_1,\mathcal{E}) - P_\lambda(k) \le 1 - \frac{1}{d} - \frac{1}{Q}.$$

5. Discussion and conclusion

In this study, we have systematically analyzed the coherence and decoherence dynamics in Shor's algorithm under both noiseless and noisy conditions and established lower and upper bounds for the probability of successfully determining the order r. For the generalized Shor's algorithm, we have shown that the upper bound of the probability that we can calculate r exhibits a negative correlation with the coherence of state ρ'_3 relative to the von Neumann measurement. The lower bound of the probability that we can calculate r increases with increasing Q. When the register is initialized in a pseudo-pure state, we have investigated the coherence and decoherence dynamics in Shor's algorithm. For large values of Q, the probability that we can calculate r when the register is initialized in a pseudo-pure state is approximately proportional to the probability that we can calculate r when the register is initialized in an arbitrary pure state.

In addition, we have investigated coherence and decoherence dynamics in noisy Shor's algorithm. It has been revealed that while the coherence of state σ_3 relative to the von Neumann measurement depends on the order r, the decoherence induced on state $|\psi_1\rangle$ by the quantum channel $\mathcal{E}$ remains independent of r. For the specific case where $W_A = \sum_x \exp(\mathrm{i}\pi x/6Q)\,|x\rangle\langle x|$, we have rigorously proven that the lower bound of the success probability is determined by the parameters Q, r, and $\phi(r)$, where $\phi(r)$ denotes Euler's totient function. Our results may offer new insights into the study of resources in quantum algorithms.

In Ref. [52], the authors investigated the Grover search algorithm with an arbitrary pure initial state or in a pseudo-pure state, and showed that the coherence, quantified by the Wigner–Yanase skew information, satisfies a complementary relation or an approximate one with the success probability. Moreover, the relation between decoherence and success probability under single-qubit noise was analyzed. In this work, we shift our focus to Shor's algorithm in both the pure state and pseudo-pure state cases. Instead of deriving complementary relations, we have deduced both upper and lower bounds on the success probability by employing metric-adjusted skew information of coherence, a class of more general coherence quantifiers, which can also be interpreted as a measure of quantum uncertainty or asymmetry in the state-channel interplay.[65] This highlights the generality and applicability of our approach. In addition, we obtain a lower bound on the success probability under depolarizing channels in d dimensional systems.

Grover's algorithm was also considered in the arbitrary pure initial state scenario, and the average success probability is shown to exhibit a strict linear dependence on the coherence fraction of the initial state, while the maximum coherence fraction corresponds to the highest success probability.[63] We found that the probability of obtaining the outcome k in the generalized Shor's algorithm reaches the maximum when the algorithm reduces to the original one, where similar arguments have been elucidated for Grover's algorithm in Ref. [63].

We restrict attention to pseudo-pure states, and our main conclusions rely on their form. For general mixed input states, quantifying coherence in Shor's algorithm becomes computationally intractable and analytically challenging due to the algorithm's intrinsic complexity, which makes a systematic characterization of the performance difficult. It is revealed that under a fixed admixture, purer inputs tend to yield higher success probabilities. Structured mixed inputs have been considered, and the robustness of coherence has been related to the performance of the probabilistic BV algorithm.[48] However, most quantum algorithms are designed to operate on pure input states.

Acknowledgements

Project supported by the National Natural Science Foundation of China (Grant Nos. 12561084 and 12161056) and the Natural Science Foundation of Jiangxi Province, China (Grant No. 20232ACB211003).

References

[1] Sudarshan E C G 1963 *Phys. Rev. Lett.* **10** 277
[2] Glauber R J 1963 *Phys. Rev.* **131** 2766
[3] Scully M O and Zubairy M S 1997 *Quantum Optics* (Cambridge: Cambridge University Press)
[4] Baumgratz T, Cramer M and Plenio M B 2014 *Phys. Rev. Lett.* **113** 140401
[5] Yu X, Zhang D, Xu G and Tong D 2016 *Phys. Rev. A* **94** 060302
[6] Xu J 2020 *Chin. Phys. B* **29** 010301
[7] Bu K, Singh U, Fei S M, Pati A K and Wu J 2017 *Phys. Rev. Lett.* **119** 150405
[8] Yu C 2017 *Phys. Rev. A* **95** 042337
[9] Zhu X, Jin Z and Fei S M 2019 *Quantum Inf. Process.* **18** 179
[10] Shao L, Li Y, Luo Y and Xi Z 2017 *Commun. Theor. Phys.* **67** 631
[11] Wu Z, Zhang L, Fei S M and Li-Jost X 2020 *Quantum Inf. Process.* **19** 125
[12] Winter A and Yang D 2016 *Phys. Rev. Lett.* **116** 120404
[13] Liu S Y and Fan H 2023 *Chin. Phys. B* **32** 110304
[14] Huang S Y, Gao J, Ren Z C, et al. 2024 *Chin. Phys. Lett.* **41** 074205
[15] Streltsov A, Adesso G and Plenio M B 2017 *Rev. Mod. Phys.* **89** 041003
[16] Hu M L, Hu X, Wang J, Peng Y, Zhang Y R and Fan H 2018 *Phys. Rep.* **762** 1
[17] Du S, Bai Z and Guo Y 2015 *Phys. Rev. A* **91** 052120
[18] Du S, Bai Z and Qi X 2019 *Phys. Rev. A* **100** 032313
[19] Du S and Bai Z 2022 *Phys. Rev. A* **105** 022412
[20] Du S and Bai Z 2023 *Phys. Rev. A* **107** 012407
[21] Bischof F, Kampermann H and Bruß D 2019 *Phys. Rev. Lett.* **123** 110402
[22] Guo M L, Liang J M, Li B, Fei S M and Wang Z X 2023 *Chin. Phys. B* **32** 050302
[23] Melo L F, Jimenez O and Neves L 2025 *Phys. Rev. A* **111** 012403
[24] Holevo A S 1973 *J. Multivar. Anal.* **3** 337
[25] Braunstein S L and Caves C M 1994 *Phys. Rev. Lett.* **72** 3439
[26] Giovannetti V, Lloyd S and Maccone L 2006 *Phys. Rev. Lett.* **96** 010401
[27] Hansen F 2008 *Proc. Natl. Acad. Sci. USA* **105** 9909
[28] Luo S 2005 *Phys. Rev. A* **72** 042110
[29] Ren R, Li P, Ye M and Li Y 2021 *Phys. Rev. A* **104** 052414
[30] Takagi R 2019 *Sci. Rep.* **9** 14562
[31] Sun Y, Li N and Luo S 2022 *Phys. Rev. A* **106** 012436
[32] Shor P W 1997 *SIAM J. Comput.* **26** 1484
[33] Beauregard S 2003 *Quantum Inf. Comput.* **3** 175
[34] Haner T, Roetteler M and Svore K M 2017 *Quantum Inf. Comput.* **17** 673
[35] Parker S and Plenio M B 2000 *Phys. Rev. Lett.* **85** 3049
[36] Kute S, Desai C and Jadhav M 2024 *AIP Conf. Proc.* **3156** 0227773
[37] Gidney C and Ekera M 2021 *Quantum* **5** 433
[38] Gidney C 2025 arXiv: 2505.15917
[39] Weng H C and Chuu C S 2024 *Phys. Rev. Appl.* **22** 034003
[40] Gharbi I E, Gueddana A, Eleuch H and Lakshminarayanan V 2024 *Proc. SPIE* **13148** 1314809
[41] Fu S, He J, Li X and Luo S 2023 *Phys. Scr.* **98** 045114
[42] Rall P 2021 *Quantum* **5** 566
[43] Mahdian M and Yeganeh H D 2020 *Quantum Inf. Process.* **19** 285
[44] Cirstoiu C, Holmes Z, Iosue J, Cincio L, Coles P J and Sornborger A 2020 *NPJ Quantum Inf.* **6** 82
[45] Ye L, Wu Z and Fei S M 2023 *Phys. Scr.* **98** 125104
[46] Ye L, Wu Z and Fei S M 2023 *Commun. Theor. Phys.* **75** 085101
[47] Ye L, Wu Z and Fei S M 2023 *Europhys. Lett.* **144** 18001
[48] Naseri M, Kondra T V, Goswami S, Fellous-Asiani M and Streltsov A 2022 *Phys. Rev. A* **106** 062429
[49] Feng C, Chen L and Zhao L J 2023 *Phys. A* **626** 129048
[50] Hillery M 2016 *Phys. Rev. A* **93** 012111
[51] Matera J M, Egloff D, Killoran N and Plenio M B 2016 *Quantum Sci. Technol.* **1** 01
[52] Sun Y 2024 *Quantum Inf. Process.* **23** 5
[53] Pan M and Qiu D 2019 *Phys. Rev. A* **100** 012349
[54] Pan M, Situ H and Zheng S 2022 *Europhys. Lett.* **138** 48002
[55] Anand N and Pati A K 2016 arXiv: 1611.04542
[56] Shi H L, Liu S Y, Wang X H, Yang W L, Yang Z Y and Fan H 2017 *Phys. Rev. A* **95** 023307
[57] Chin S 2017 *Phys. Rev. A* **96** 042336
[58] Rastegin A E 2018 *Front. Phys.* **13** 130318
[59] Rastegin A E 2018 *Quantum Inf. Process.* **17** 179
[60] Liu Y C, Shang J and Zhang X 2019 *Entropy* **21** 260
[61] Rastegin A E and Sazhenova A M 2023 *Mod. Phys. Lett. A* **38** 2350030
[62] Ahnefeld F, Theurer T, Egloff D, Matera J M and Plenio M B 2022 *Phys. Rev. Lett.* **129** 120501
[63] Zhou S Q, Jin H, Liang J M, Fei S M, Xiao Y and Ma Z 2024 *Phys. Rev. A* **110** 062429
[64] Petz D 1996 *Linear Algebra Appl.* **244** 81
[65] Luo S and Sun Y 2018 *Phys. Rev. A* **98** 012113
[66] Fan Y J, Cao H X, Wang W H, Meng H X and Chen L 2018 *Quantum Inf. Process.* **17** 157
[67] Wu Z, Zhang L, Wang J, Jiang W and Li J 2020 *Int. J. Theor. Phys.* **59** 704
[68] Hardy G H and Wright E M 1984 *An Introduction to the Theory Of Numbers,* 6th edn. (Oxford: Oxford University Press)
[69] Linden N and Popescu S 2001 *Phys. Rev. Lett.* **87** 047901
[70] Cory D G, Fahmy A F and Havel T F 1997 *Proc. Natl. Acad. Sci. USA* **94** 1634
[71] Sharf Y, Havel T F and Cory D G 2000 *Phys. Rev. A* **62** 052314
[72] Braunstein S L, Caves C M, Jozsa R, Linden N, Popescu S and Schack R 1999 *Phys. Rev. Lett.* **83** 1054
[73] Du J, Shi M, Zhou X, Fan Y, Ye B J, Han R and Wu J 2001 *Phys. Rev. A* **64** 042306
[74] Hu X, Fan H, Zhou D L and Liu W M 2012 *Phys. Rev. A* **85** 032102
[75] Guo Y and Hou J 2013 *J. Phys. A: Math. Theor.* **46** 155301
[76] Li N, Luo S and Song H 2019 *Phys. Rev. A* **99** 052114