Conservation-law-induced quantum limits for physical realizations of the quantum NOT gate

Tokishiro Karasawa* and Masanao Ozawa†
Graduate School of Information Sciences, Tôhoku University, Aoba-ku, Sendai 980-8579, Japan
(Received 28 November 2006; published 19 March 2007)

In recent investigations, it has been found that conservation laws generally lead to precision limits on quantum computing. Lower bounds of the error probability have been obtained for various logic operations from the commutation relation between the noise operator and the conserved quantity or from the recently developed universal uncertainty principle for the noise-disturbance trade-off in general measurements. However, the problem of obtaining the precision limit to realizing the quantum NOT gate has eluded a solution from these approaches. Here, we develop a method for this problem based on analyzing the trace distance between the output state from the realization under consideration and the one from the ideal gate. Using the mathematical apparatus of orthogonal polynomials, we obtain a general lower bound on the error probability for the realization of the quantum NOT gate in terms of the number of qubits in the control system under conservation of the total angular momentum of the computational qubit plus the control system along the direction used to encode the computational basis. The lower bound turns out to be more stringent than one might expect from previous results. Our method is expected to lead to more accurate estimates for physical realizations of various types of quantum computations under conservation laws and to contribute to related problems such as the accuracy of programmable quantum processors.

DOI: 10.1103/PhysRevA.75.032324 PACS number(s): 03.67.Lx, 03.65.Yz, 03.65.Ta

I. INTRODUCTION

Recently, there have been extensive research efforts to explore whether fundamental physical laws put any constraints on realizing scalable quantum computing. Soon after the discovery of Shor's algorithm [1], it was pointed out by several physicists [2–4] that the decoherence, the exponential decay of coherence in time, caused by the coupling between a quantum computer and the environment would cancel out the computational advantage of quantum computers. To overcome this difficulty, quantum error correction was proposed [5,6], and subsequent development has established the so-called threshold theorem: if the error caused by the decoherence in individual quantum gates is below a certain constant threshold, it is possible in principle to efficiently perform an arbitrary scale of fault-tolerant quantum computation with error correction [7]. Thus, the error correction reduces, in principle, the scalability problem to the accuracy problem requiring individual quantum logic gates to clear the error threshold, though being still quite demanding.

In general, decoherence in quantum computer components can be classified into two classes: (i) static decoherence, arising from the interaction between computational qubits, typically in the memory, and the environment, and (ii) dynamical decoherence, arising from the interaction between computational qubits, typically in the register, and the control system of gate operations [8]. The static decoherence may be overcome by developing materials with long decoherence time. On the other hand, dynamical decoherence poses a dilemma between controllability and decoherence; the control needs coupling, whereas the coupling causes decoherence. Thus, even if the interaction with the environment is completely suppressed, the error caused by the dynamical decoherence still remains. Clearly, if the control system is described classically, there is no decoherence. However, this never happens in reality with finite resources.

Barnes and Warren [9], Gea-Banacloche [10], and van Enk and Kimble [11] have focused on the atom-field interaction between atom qubits and control electromagnetic fields, and shown that, when the control field is in a coherent state, the gate error scales as the inverse of the average photon number. In contrast to those model-dependent approaches, one of the current authors [12] explored the physical constraint on the error caused by dynamical decoherence generally imposed by conservation laws and obtained accuracy limits by quantitatively generalizing the so-called Wigner-Araki-Yanase theorem [13,14]: observables which do not commute with bounded additive conserved quantities have no precise and nondisturbing measurements. It is natural to assume that conservation laws are satisfied by the interaction between the qubit and the external control system. If the control system were to be completely described as a classical system, the conservation law would not cause any conflict in realizing a unitary operation on the computational qubit, since the classical interaction causes no decoherence and yet conserves the (infinite) total quantum number. However, in reality, the interaction may cause decoherence and the time evolution operator on the composite system is limited to one commuting with the conserved quantity. Under these conditions, the accuracy of the realized gate operation generally depends on the kind of gate being considered. It has been shown that the SWAP gate can be realized in principle without error [12]. However, the controlled-NOT gate and the Hadamard gate have lower bounds of the error probability that scales as the inverse of the size of the control system, as follows.

The impossibility of precise and nondisturbing measurements under conservation laws was generalized to an inequality for the lower bound of the sum of the noise and

*Electronic address: jidai@ims.is.tohoku.ac.jp
†Electronic address: ozawa@math.is.tohoku.ac.jp

disturbance of the measuring process under a conservation law [8]. This inequality leads to a general lower bound for the error probability of any realization of the controlled-NOT gate under conservation laws [8,12,15]. For single-spin qubits controlled by the N-qubit control system, the angular momentum conservation law leads to the minimum error probability $(4N^2)^{-1}$ [12]. Thus, assuming a threshold error probability $10^{-4}-10^{-5}$ [7], a two-qubit unitary operator needs to be realized by an interaction with more than 100 qubit systems, suggesting the usefulness of schemes based on multiple-spin encoded qubits such as the universal encoding based on decoherence-free subspaces [15–17]. In bosonic controls, such as electromagnetic fields in coherent states, the minimum error probability amounts to $(16\bar{n})^{-1}$ [12], where $\bar{n}$ is the average number of photons. The above result also leads to a conclusion that in any universal set of elementally logic operations there is at least one logic operation that obeys the error limit with the same scaling as above [12].

On the other hand, without assuming the nondisturbing condition the lower bound for the noise in arbitrary measurements under arbitrary conservation laws was derived from the commutation relation for the noise operator and the conserved quantity [18] or simply from the universal uncertainty principle [19]; see Refs. [20–22] for the universal uncertainty principle. This inequality also leads to a general lower bound for the error probability of the realization of the Hadamard gate that amounts to the minimum error probability $(4N^2)^{-1}$ for any N-qubit control system and $(16\bar{n})^{-1}$ for any electromagnetic control field in a coherent state with an average number of photons, $\bar{n}$ [19]. Gea-Banacloche and one of the authors [23] compared the above result for electromagnetic control fields with the previous result obtained by Gea-Banacloche [10] for the Jaynes-Cummings interaction, and it was concluded that the constraint based on the angular momentum conservation law represents an ultimate limit closely related to fluctuations in the quantum field phase. The use of the Jaynes-Cummings model in the above model-dependent approach [10,11] was questioned by Itano [24], and subsequently Silberfarb and Deutsch [25] justified the Jaynes-Cummings model in the limit of small entanglement; see also replies to Itano by van Enk and Kimble [26] and by Gea-Banacloche [27]. The above consistency result between the model-dependent and model-independent approaches enforces the validity of the use of the Jaynes-Cummings model and substantially clarifies the whole situation.

The above methods for deriving conservation-law-induced quantum limits for quantum logic operations are also applicable to the Toffoli gate and the Fredkin gate to obtain similar lower bounds. However, the problem of obtaining the precision limit to realizing the quantum NOT gate has eluded a solution from these approaches, and hence the problem has been open as to how the minimum error for that gate scales with the size of the control system. In this paper, in order to solve this problem we devise a method of deriving the precision limit and show that there exists a nonzero lower bound, which indeed scales as the inverse size of the control system, of the error probability for the quantum NOT gate.

Our formulation has various common features with the formulation of programmable quantum processors [28–30], in which a set of unitary operators is to be realized by selecting a unitary operator on the composite system, the system plus the ancilla, and by selecting a set of ancilla states, whereas in our problem a single unitary operator is to be realized under a conservation law by selecting a unitary operator on the composite system satisfying the conservation laws and by selecting a single ancilla state. In previous investigations the accuracy of programmable quantum computing has been measured by the so-called process fidelity, a fidelity-based distance measure between two operations, whereas here we investigate in the completely bounded (CB) distance or gate trace distance, a trace-distance-based measure. Thus, our method is expected to contribute to the problem of programmable quantum processors and related subjects [31–33] in future investigations.

This paper is organized as follows. Section II gives the basic formulations and main results. We define the error probability in realizing the quantum NOT gate based on the CB distance. We subsequently show that a pure input state gives the worst error probability. This enables us to assume, without loss of generality, that the input state is a pure state. In preparation for deriving the lower bound of the error probability, in Sec. III we generally describe the maximum trace distance between the two output states from the realization and from the ideal quantum NOT gate. In Sec. IV, we introduce the conservation law into the discussion. By minimizing the error probability over arbitrary choices of the evolution operator obeying the conservation law, we give a lower bound which depends only on the ancilla input state. In Sec. V, we optimize the ancilla input state and derive a general lower bound expressed as a function of the size (the number of qubits) of the ancilla. Chebyshev polynomials of the second kind, a family of orthogonal polynomials, are used to solve this problem. To show the tightness of the bound, in Sec. VI, we consider classically complete realizations, realizations which correctly carry out the quantum NOT operation when the input state is a computational basis state. We obtain the attainable lower bound for classically complete realizations. This result also shows that the general lower bound can be attained up to constant factor of the ancilla size. In the final section, we summarize our study and comment on the direction of future studies.

II. FORMULATION AND MAIN RESULTS

A. Qubits and conservation laws

The problem to be considered is formulated as follows. The main system **S** is a single qubit described by a two-dimensional Hilbert space $\mathcal{H}_{\mathbf{S}}$ with a fixed computational basis $\{|0\rangle,|1\rangle\}$. The Pauli operators $X_{\mathbf{S}}$, $Y_{\mathbf{S}}$, and $Z_{\mathbf{S}}$ on $\mathcal{H}_{\mathbf{S}}$ are defined by $X_{\mathbf{S}}=|0\rangle\langle 1|+|1\rangle\langle 0|$, $Y_{\mathbf{S}}=-i|0\rangle\langle 1|+i|1\rangle\langle 0|$, and $Z_{\mathbf{S}}=|0\rangle\langle 0|-|1\rangle\langle 1|$. We refer to $X_{\mathbf{S}}$ as the quantum NOT gate.

We suppose that the computational basis is represented by the z component of spin and consider the constraint on realizing the quantum NOT gate $X_{\mathbf{S}}$ under the angular momentum conservation law. More specifically, we assume that the control system is described as an N-qubit system **A**, also called the ancilla, and that the interaction between **S** and **A** preserves the z component of the angular momentum of the composite system $\mathbf{S}+\mathbf{A}$, and study the unavoidable error probability in realizing the quantum NOT operation.

Each qubit $\mathbf{A}_i$ for $i=1,2,\ldots,N$ in the ancilla $\mathbf{A}$ is described by a two-dimensional Hilbert space $\mathcal{H}_{\mathbf{A}_i}$. Accordingly, the Hilbert space $\mathcal{H}_{\mathbf{A}}$ of the ancilla $\mathbf{A}$ is the tensor product $\mathcal{H}_{\mathbf{A}}=\otimes_{i=1}^{N}\mathcal{H}_{\mathbf{A}_i}$ and the Hilbert space $\mathcal{H}$ of the composite system $\mathbf{S}+\mathbf{A}$ is $\mathcal{H}=\mathcal{H}_{\mathbf{S}}\otimes\mathcal{H}_{\mathbf{A}}$. The observable $Z_{\mathbf{S}}$ on $\mathcal{H}_{\mathbf{S}}$ is identified with $Z_{\mathbf{S}}\otimes I_{\mathbf{A}_1}\otimes I_{\mathbf{A}_2}\otimes\cdots\otimes I_{\mathbf{A}_N}$, where $I_{\mathbf{A}_i}$ for $i=1,2,\ldots,N$ is the identity operator on $\mathcal{H}_{\mathbf{A}_i}$, respectively. Let $Z_{\mathbf{A}_i}$ be the Pauli Z operator on $\mathcal{H}_{\mathbf{A}_i}$, which is also identified with the corresponding operator on $\mathcal{H}$. The sum of Pauli Z operators on $\mathbf{A}$ is denoted by

$$Z_{\mathbf{A}}=\sum_{i=1}^{N} Z_{\mathbf{A}_i},$$

and the corresponding sum of $\mathbf{S}+\mathbf{A}$ is denoted by

$$Z=Z_{\mathbf{S}}+Z_{\mathbf{A}}.$$

Let U be the evolution operator of $\mathbf{S}+\mathbf{A}$ during the interaction between $\mathbf{S}$ and $\mathbf{A}$ to realize the quantum NOT gate on $\mathbf{S}$. We assume that U satisfies the conservation law

$$[U,Z]=0, \tag{1}$$

where $[U,Z]=UZ-ZU$. We shall show that the conservation law (1) causes unavoidable decoherence in realizing $X_{\mathbf{S}}$ by U.

To obtain the error probability, we describe the output state of $\mathbf{S}$ resulting from the evolution of $\mathbf{S}+\mathbf{A}$. Let $\rho_{\mathbf{S}}$ and $\rho_{\mathbf{A}}$ be states of $\mathbf{S}$ and $\mathbf{A}$, respectively, so that the input state of $\mathbf{S}+\mathbf{A}$ is the product state $\rho_{\mathbf{S}}\otimes\rho_{\mathbf{A}}$. Then the output state $\mathcal{E}_{U,\rho_{\mathbf{A}}}(\rho_{\mathbf{S}})$ of $\mathbf{S}$ is given by

$$\mathcal{E}_{U,\rho_{\mathbf{A}}}(\rho_{\mathbf{S}})=\mathrm{Tr}_{\mathbf{A}}[U(\rho_{\mathbf{S}}\otimes\rho_{\mathbf{A}})U^{\dagger}], \tag{2}$$

where $\mathrm{Tr}_{\mathbf{A}}[\cdot]$ is the partial trace over $\mathcal{H}_{\mathbf{A}}$. On the other hand, for the perfect quantum NOT gate, the output state $\mathcal{E}_{X_{\mathbf{S}}}(\rho_{\mathbf{S}})$ of $\mathbf{S}$ would be

$$\mathcal{E}_{X_{\mathbf{S}}}(\rho_{\mathbf{S}})=X_{\mathbf{S}}\rho_{\mathbf{S}}X_{\mathbf{S}}{}^{\dagger}. \tag{3}$$

In the following sections we shall show that there exists an unavoidable error probability of the output state (2) in realizing the output state (3) under the conservation law (1). The unavoidable error probability for any unitary operator U satisfying the conservation law (1) will be evaluated to be at least

$$\frac{1}{2}\left(1-\cos\frac{\pi}{N+2}\right)$$

for the worst input state $\rho_{\mathbf{S}}$ of $\mathbf{S}$ and for the best input state $\rho_{\mathbf{A}}$ of $\mathbf{A}$, and the achievability to this lower bound will be shown asymptotically. This lower bound is much tighter than the lower bound $\frac{1}{16N^2+4}$ anticipated from previous investigations for other gates as to be shown numerically.

B. Error probability and CB distance

To state our results more precisely, we introduce the following definitions. Any pair $(U,\rho_{\mathbf{A}})$ consisting of a unitary operator U on $\mathcal{H}_{\mathbf{S}}\otimes\mathcal{H}_{\mathbf{A}}$ and a state $\rho_{\mathbf{A}}$ on $\mathcal{H}_{\mathbf{A}}$ is called a gate implementation or simply an implementation with ancilla $\mathbf{A}$. Every implementation $(U,\rho_{\mathbf{A}})$ determines the trace-preserving completely positive (CP) map $\mathcal{E}_{U,\rho_{\mathbf{A}}}$ of the states of $\mathbf{S}$ by Eq. (2) called the gate operation determined by $(U,\rho_{\mathbf{A}})$; see Ref. [7] for trace-preserving CP maps in quantum information theory. An implementation $(U,\rho_{\mathbf{A}})$ is said to be conservative if it satisfies Eq. (1). We consider the problem as to how accurately we can make the gate operation $\mathcal{E}_{U,\rho_{\mathbf{A}}}$ to realize the quantum NOT gate $\mathcal{E}_{X_{\mathbf{S}}}$. The worst error probability of this realization is defined by the completely bounded distance [34,35] (the CB distance, or the half-CB-norm distance) between $\mathcal{E}_{U,\rho_{\mathbf{A}}}$ and $\mathcal{E}_{X_{\mathbf{S}}}$, given by

$$D_{\mathrm{CB}}(\mathcal{E}_{U,\rho_{\mathbf{A}}},\mathcal{E}_{X_{\mathbf{S}}})=\sup_{n,\rho} D(\mathcal{E}_{U,\rho_{\mathbf{A}}}\otimes id_n(\rho),\mathcal{E}_{X_{\mathbf{S}}}\otimes id_n(\rho)), \tag{4}$$

where $D(\cdot,\cdot)$ denotes the trace distance (or the half-trace-norm distance) [7] defined by

$$D(\rho_1,\rho_2)=\frac{1}{2}\mathrm{Tr}[|\rho_1-\rho_2|]$$

for any states ρ_1 and ρ_2 of $\mathbf{S}$, id_n is the identity operation on an n-level system $\mathbf{E}$, and ρ runs over the density operators on $\mathbf{S}+\mathbf{E}$. Since the trace distance of the output states can be interpreted as the achievable upper bound on the classical trace distances, or the total-variation distances, between the probability distributions arising from any measurements on those states [7], the CB distance can be interpreted as the ultimate achievable upper bound on those classical trace distances with further allowing measurements over the environment with entangled input states; see, for example, [36] for a discussion on the enhancement of channel discriminations with an entanglement assistance. Thus, we interpret $D_{\mathrm{CB}}(\mathcal{E}_{U,\rho_{\mathbf{A}}},\mathcal{E}_{X_{\mathbf{S}}})$ as the worst error probability of $\mathcal{E}_{U,\rho_{\mathbf{A}}}$ in realizing $\mathcal{E}_{X_{\mathbf{S}}}$. The phrase "error probability" in the following discussion means the CB distance (4). Clearly,

$$D_{\mathrm{CB}}(\mathcal{E}_{U,\rho_{\mathbf{A}}},\mathcal{E}_{X_{\mathbf{S}}})\geqslant\max_{\rho_{\mathbf{S}}} D(\mathcal{E}_{U,\rho_{\mathbf{A}}}(\rho_{\mathbf{S}}),\mathcal{E}_{X_{\mathbf{S}}}(\rho_{\mathbf{S}})),$$

and minimizing $\max_{\rho_{\mathbf{S}}}D(\mathcal{E}_{U,\rho_{\mathbf{A}}}(\rho_{\mathbf{S}}),\mathcal{E}_{X_{\mathbf{S}}}(\rho_{\mathbf{S}}))$ over all the conservative implementations $(U,\rho_{\mathbf{A}})$, we find

$$D_{\mathrm{CB}}(\mathcal{E}_{U,\rho_{\mathbf{A}}},\mathcal{E}_{X_{\mathbf{S}}})\geqslant\min_{(U,\rho_{\mathbf{A}})}\max_{\rho_{\mathbf{S}}} D(\mathcal{E}_{U,\rho_{\mathbf{A}}}(\rho_{\mathbf{S}}),\mathcal{E}_{X_{\mathbf{S}}}(\rho_{\mathbf{S}})). \tag{5}$$

The right-hand side of this inequality can be interpreted as a precision limit of the quantum NOT gate under the conservation law (1). If the limit could take zero, it might be considered that there exists a perfect realization in $\mathcal{E}_{U,\rho_{\mathbf{A}}}$. However, we show that such a realization does not exist because of the conservation law (1).

C. Sufficiency of pure input states

Now, we shall simplify the maximization over the input state $\rho_{\mathbf{S}}$ by showing that it suffices to consider only the pure state $\rho_{\mathbf{S}}$. To show this, we use the fact that the output trace distance is jointly convex in its inputs:

$$D\left(\mathcal{E}_{U,\rho_{\mathbf{A}}}\left(\sum_i p_i\rho_i\right),\mathcal{E}_{X_{\mathbf{S}}}\left(\sum_i p_i\rho_i\right)\right) \leqslant \sum_i p_i D(\mathcal{E}_{U,\rho_{\mathbf{A}}}(\rho_i),\mathcal{E}_{X_{\mathbf{S}}}(\rho_i)), \quad (6)$$

where $\Sigma_i p_i=1$ and $p_i \geqslant 0$. This follows easily from the joint convexity of the trace distance [7] and the linearity of operations $\mathcal{E}_{X_{\mathbf{S}}}$ and $\mathcal{E}_{U,\rho_{\mathbf{A}}}$.

From the above inequality, a pure input state certainly gives the maximum of the trace distance. To see this briefly, let $\rho_{\mathbf{S}}=\Sigma_i q_i|\psi_i\rangle\langle\psi_i|$, where $\Sigma_i q_i=1$ and $q_i \geqslant 0$. Then, there exists a pure state $|\psi_j\rangle$ such that

$$\begin{aligned} D\left(\mathcal{E}_{U,\rho_{\mathbf{A}}}\left(\sum_i q_i|\psi_i\rangle\langle\psi_i|\right),\mathcal{E}_{X_{\mathbf{S}}}\left(\sum_i q_i|\psi_i\rangle\langle\psi_i|\right)\right) &\leqslant \sum_i q_i D(\mathcal{E}_{U,\rho_{\mathbf{A}}}(|\psi_i\rangle\langle\psi_i|),\mathcal{E}_{X_{\mathbf{S}}}(|\psi_i\rangle\langle\psi_i|)) \\ &\leqslant D(\mathcal{E}_{U,\rho_{\mathbf{A}}}(|\psi_j\rangle\langle\psi_j|),\mathcal{E}_{X_{\mathbf{S}}}(|\psi_j\rangle\langle\psi_j|)). \end{aligned} \quad (7)$$

Thus in considering $\max_{\rho_{\mathbf{S}}} D(\mathcal{E}_{U,\rho_{\mathbf{A}}}(\rho_{\mathbf{S}}),\mathcal{E}_{X_{\mathbf{S}}}(\rho_{\mathbf{S}}))$, we shall assume in later discussions without loss of generality that the input state $\rho_{\mathbf{S}}$ is a pure state.

D. Pure conservative implementations

An implementation $(U,\rho_{\mathbf{A}})$ is said to be pure if $\rho_{\mathbf{A}}$ is a pure state. In this case, we shall write $(U,\rho_{\mathbf{A}})=(U,|A\rangle)$ if $\rho_{\mathbf{A}}=|A\rangle\langle A|$. In the following sections, we shall mainly consider the case where the ancilla state is a pure state. Here, we shall show a purification method that makes any general conservative implementation a pure conservative implementation, so that every conservative implementation with N-qubit ancilla has a pure conservative implementation with $\{N+\lceil\log_2 \mathrm{rank}(\rho_{\mathbf{A}})\rceil\}$-qubit ancilla, where $\mathrm{rank}(\rho_{\mathbf{A}})$ denotes the rank of $\rho_{\mathbf{A}}$.

Let $(U,\rho_{\mathbf{A}})$ be a conservative implementation with N-qubit ancilla $\mathbf{A}$. Then, we have the spectral decomposition

$$\rho_{\mathbf{A}} = \sum_{j=1}^{R} p_j|\phi_j\rangle\langle\phi_j|, \quad (8)$$

where $R=\mathrm{rank}(\rho_{\mathbf{A}})$, $\langle\phi_j|\phi_k\rangle=\delta_{jk}$, $p_j>0$ for all $j,k=1,\ldots,R$, and $\Sigma_j p_j=1$. Let $\mathbf{A}'$ be the N'-qubit ancilla system extending $\mathbf{A}$ satisfying $N'=N+\lceil\log_2 R\rceil$. Let $|A'\rangle \in \mathcal{H}_{\mathbf{A}'}$ be such that

$$|A'\rangle = \sum_{j=1}^{R} \sqrt{p_j}|\phi_j\rangle \otimes |\xi_j\rangle, \quad (9)$$

where $|\xi_j\rangle \in \mathcal{H}_{\mathbf{A}'-\mathbf{A}}$, $\langle\xi_j|\xi_k\rangle=\delta_{jk}$ for all $j,k=1,\ldots,R$. We define a unitary operator U' on $\mathcal{H}_{\mathbf{S}}\otimes\mathcal{H}_{\mathbf{A}}\otimes\mathcal{H}_{\mathbf{A}'-\mathbf{A}}$ by $U'=U\otimes I$, where I is the identity operator on $\mathcal{H}_{\mathbf{A}'-\mathbf{A}}$.

Now, we consider the implementation $(U',|A'\rangle)$. It is easy to see that U' satisfies the conservation law $[U',Z]=0$, where Z is the sum of Pauli Z operators in $\mathbf{S}+\mathbf{A}'$. We shall show the relation

$$\mathcal{E}_{U,\rho_{\mathbf{A}}} = \mathcal{E}_{U',|A'\rangle}. \quad (10)$$

Let $\rho_{\mathbf{S}}$ be any input state. Then, by Eq. (9) we have

$$\mathrm{Tr}_{\mathbf{A}'-\mathbf{A}}[\rho_{\mathbf{S}} \otimes |A'\rangle\langle A'|] = \rho_{\mathbf{S}} \otimes \rho_{\mathbf{A}}. \quad (11)$$

We also have

$$\begin{aligned} \mathcal{E}_{U',|A'\rangle}(\rho_{\mathbf{S}}) &= \mathrm{Tr}_{\mathbf{A}'}[U'(\rho_{\mathbf{S}} \otimes |A'\rangle\langle A'|)U'^{\dagger}] \\ &= \mathrm{Tr}_{\mathbf{A}}\mathrm{Tr}_{\mathbf{A}'-\mathbf{A}}[(U\otimes I)(\rho_{\mathbf{S}} \otimes |A'\rangle\langle A'|)(U^{\dagger}\otimes I)] \\ &= \mathrm{Tr}_{\mathbf{A}}[U\mathrm{Tr}_{\mathbf{A}'-\mathbf{A}}[\rho_{\mathbf{S}} \otimes |A'\rangle\langle A'|]U^{\dagger}]. \end{aligned}$$

From Eq. (11), we have

$$\mathcal{E}_{U',|A'\rangle}(\rho_{\mathbf{S}}) = \mathrm{Tr}_{\mathbf{A}}[U(\rho_{\mathbf{S}} \otimes \rho_{\mathbf{A}})U^{\dagger}].$$

Since $\rho_{\mathbf{S}}$ is arbitrary, Eq. (10) follows from Eq. (2).

The implementation $(U',|A'\rangle)$ is a pure conservative implementation and has $\{N'=N+\lceil\log_2 \mathrm{rank}(\rho_{\mathbf{A}})\rceil\}$-qubit ancilla.

E. Gate fidelity and gate trace distance

For any two trace-preserving CP maps $\mathcal{E}_1$ and $\mathcal{E}_2$ their distance measures are defined as follows. The gate fidelity [7] $F(\mathcal{E}_1,\mathcal{E}_2)$ between $\mathcal{E}_1$ and $\mathcal{E}_2$ is defined by

$$F(\mathcal{E}_1,\mathcal{E}_2) = \inf_{\rho_{\mathbf{S}}} F(\mathcal{E}_1(\rho_{\mathbf{S}}),\mathcal{E}_2(\rho_{\mathbf{S}})), \quad (12)$$

where $\rho_{\mathbf{S}}$ varies over all the states of $\mathbf{S}$ and $F(\cdot,\cdot)$ on the right-hand side denotes the fidelity defined by

$$F(\rho_1,\rho_2) = \mathrm{Tr}[(\rho_1^{1/2}\rho_2\rho_1^{1/2})^{1/2}] \quad (13)$$

for all states ρ_1 and ρ_2 of $\mathbf{S}$. By the joint concavity of the fidelity ([7], p. 415) the infimum in Eq. (12) can be replaced by the one over only all the pure states $\rho_{\mathbf{S}}$ of $\mathbf{S}$.

We define the gate trace distance $D(\mathcal{E}_1,\mathcal{E}_2)$ between $\mathcal{E}_1$ and $\mathcal{E}_2$ by

$$D(\mathcal{E}_1,\mathcal{E}_2) = \sup_{\rho_{\mathbf{S}}} D(\mathcal{E}_1(\rho_{\mathbf{S}}),\mathcal{E}_2(\rho_{\mathbf{S}})), \quad (14)$$

where $\rho_{\mathbf{S}}$ varies over all the states of $\mathbf{S}$. By the result obtained in Sec. II C, the supremum in Eq. (14) can be replaced by the one over only all the pure states $\rho_{\mathbf{S}}$ of $\mathbf{S}$.

For any state ρ_1 and any pure state ρ_2, the fidelity and the trace distance are related by

$$D(\rho_1,\rho_2) \geqslant 1 - F(\rho_1,\rho_2)^2$$

[see Eq. (9,111) of Ref. [7]]. Since $\mathcal{E}_{X_{\mathbf{S}}}(\rho_{\mathbf{S}})$ is a pure state provided that $\rho_{\mathbf{S}}$ is pure, we have

$$D(\mathcal{E}_{U,\rho_{\mathbf{A}}}(\rho_{\mathbf{S}}),\mathcal{E}_{X_{\mathbf{S}}}(\rho_{\mathbf{S}})) \geqslant 1 - F(\mathcal{E}_{U,\rho_{\mathbf{A}}}(\rho_{\mathbf{S}}),\mathcal{E}_{X_{\mathbf{S}}}(\rho_{\mathbf{S}}))^2 \quad (15)$$

for any pure state $\rho_{\mathbf{S}}$ of $\mathbf{S}$. Taking the supremum over all the pure states $\rho_{\mathbf{S}}$ of both sides of Eq. (15), for any implementation $(U,\rho_{\mathbf{A}})$ we obtain

$$D_{\mathrm{CB}}(\mathcal{E}_{U,\rho_{\mathbf{A}}},\mathcal{E}_{X_{\mathbf{S}}}) \geq D(\mathcal{E}_{U,\rho_{\mathbf{A}}},\mathcal{E}_{X_{\mathbf{S}}}) \geq 1 - F(\mathcal{E}_{U,\rho_{\mathbf{A}}},\mathcal{E}_{X_{\mathbf{S}}})^2. \tag{16}$$

In Ref. [19], the realization of the Hadamard gate $H_{\mathbf{S}} = (1/\sqrt{2})(|0\rangle\langle 0| + |1\rangle\langle 0| + |0\rangle\langle 1| - |1\rangle\langle 1|)$ has been considered and it has been proved that for any pure conservative implementation $(U,|A\rangle)$ with N-qubit ancilla $\mathbf{A}$, we have

$$1 - F(\mathcal{E}_{U,|A\rangle},\mathcal{E}_{H_{\mathbf{S}}})^2 \geq \frac{1}{4N^2+4}, \tag{17}$$

where $\mathcal{E}_{H_{\mathbf{S}}}(\rho_{\mathbf{S}}) = H_{\mathbf{S}}\rho_{\mathbf{S}}H_{\mathbf{S}}^{\dagger}$.[1] Since any conservative implementation $(U,\rho_{\mathbf{A}})$ with N-qubit ancilla $\mathbf{A}$ can be purified to be a pure conservative implementation $(U',|A'\rangle)$ with $\{N + \lceil \log_2 \mathrm{rank}(\rho_{\mathbf{A}})\rceil\}$-qubit ancilla $\mathbf{A}'$, we have

$$1 - F(\mathcal{E}_{U,\rho_{\mathbf{A}}},\mathcal{E}_{H_{\mathbf{S}}})^2 \geq \frac{1}{4[N + \log_2 \mathrm{rank}(\rho_{\mathbf{A}})]^2 + 4}. \tag{18}$$

Since $N + \lceil \log_2 \mathrm{rank}(\rho_{\mathbf{A}})\rceil \leq 2N$, we conclude that every conservative implementation $(U,\rho_{\mathbf{A}})$ with N-qubit ancilla $\mathbf{A}$ satisfies

$$1 - F(\mathcal{E}_{U,\rho_{\mathbf{A}}},\mathcal{E}_{H_{\mathbf{S}}})^2 \geq \frac{1}{16N^2+4}. \tag{19}$$

In other words, we have

$$\min_{(U,|A\rangle)} \max_{\rho_{\mathbf{S}}} [1 - F(\mathcal{E}_{U,|A\rangle},\mathcal{E}_{H_{\mathbf{S}}})^2] \geq \frac{1}{4N^2+4}, \tag{20}$$

where $(U,|A\rangle)$ varies over all the pure conservative implementations with N-qubit ancilla $\mathbf{A}$, and we have

$$\min_{(U,\rho_{\mathbf{A}})} \max_{\rho_{\mathbf{S}}} [1 - F(\mathcal{E}_{U,\rho_{\mathbf{A}}},\mathcal{E}_{H_{\mathbf{S}}})^2] \geq \frac{1}{16N^2+4}, \tag{21}$$

where $(U,\rho_{\mathbf{A}})$ varies over all the conservative implementations with N-qubit ancilla $\mathbf{A}$.

F. Main results

Unfortunately, the method for deriving Eq. (17) cannot be applied to the quantum NOT gate. In this paper we develop a method for analyzing the gate trace distance $D(\mathcal{E}_{U,\rho_{\mathbf{A}}},\mathcal{E}_{X_{\mathbf{S}}})$ instead of considering the gate fidelity $F(\mathcal{E}_{U,\rho_{\mathbf{A}}},\mathcal{E}_{X_{\mathbf{S}}})$ and we shall prove the following relations. In Sec. V, we shall show that any pure conservative implementation $(U,|A\rangle)$ with N-qubit ancilla satisfies

$$D(\mathcal{E}_{U,|A\rangle},\mathcal{E}_{X_{\mathbf{S}}}) \geq \frac{1}{2}\left(1 - \cos\frac{2\pi}{N+4}\right). \tag{22}$$

It follows from the above that any conservative implementation $(U,\rho_{\mathbf{A}})$ with N-qubit ancilla satisfies

$$D(\mathcal{E}_{U,\rho_{\mathbf{A}}},\mathcal{E}_{X_{\mathbf{S}}}) \geq \frac{1}{2}\left(1 - \cos\frac{2\pi}{N + \log_2 \mathrm{rank}(\rho_{\mathbf{A}}) + 4}\right). \tag{23}$$

An implementation $(U,\rho_{\mathbf{A}})$ is called a classically complete implementation of the quantum NOT gate, or classically complete implementation for short, if it satisfies

$$\mathcal{E}_{U,\rho_{\mathbf{A}}}(|0\rangle\langle 0|) = |1\rangle\langle 1|, \tag{24}$$

$$\mathcal{E}_{U,\rho_{\mathbf{A}}}(|1\rangle\langle 1|) = |0\rangle\langle 0|. \tag{25}$$

In Sec. VI, we shall consider classically complete pure conservative implementations. We shall find the attainable lower bound for this case, so that we obtain

$$\min_{(U,|A\rangle)} \max_{\rho_{\mathbf{S}}} D(\mathcal{E}_{U,|A\rangle}(\rho_{\mathbf{S}}),\mathcal{E}_{X_{\mathbf{S}}}(\rho_{\mathbf{S}})) = \frac{1}{2}\left(1 - \cos\frac{2\pi}{N+2}\right), \tag{26}$$

where $(U,|A\rangle)$ varies over all the classically complete pure conservative implementations with N-qubit ancilla $\mathbf{A}$ provided N is even, and we obtain

$$\min_{(U,|A\rangle)} \max_{\rho_{\mathbf{S}}} D(\mathcal{E}_{U,|A\rangle}(\rho_{\mathbf{S}}),\mathcal{E}_{X_{\mathbf{S}}}(\rho_{\mathbf{S}})) = \frac{1}{2}\left(1 - \cos\frac{2\pi}{N+1}\right), \tag{27}$$

provided N is odd. From the above, any classically complete conservative implementation $(U,\rho_{\mathbf{A}})$ with N-qubit ancilla satisfies

$$D(\mathcal{E}_{U,\rho_{\mathbf{A}}},\mathcal{E}_{X_{\mathbf{S}}}) \geq \frac{1}{2}\left(1 - \cos\frac{2\pi}{N + \log_2 \mathrm{rank}(\rho_{\mathbf{A}}) + 2}\right). \tag{28}$$

Since $N + \log_2 \mathrm{rank}(\rho_{\mathbf{A}}) \leq 2N$, from the above we have

$$\frac{1}{2}\left(1 - \cos\frac{2\pi}{N+1}\right) \geq \min_{(U,\rho_{\mathbf{A}})} \max_{\rho_{\mathbf{S}}} D(\mathcal{E}_{U,\rho_{\mathbf{A}}}(\rho_{\mathbf{S}}),\mathcal{E}_{X_{\mathbf{S}}}(\rho_{\mathbf{S}})) \geq \frac{1}{2}\left(1 - \cos\frac{\pi}{N+1}\right), \tag{29}$$

where $(U,\rho_{\mathbf{A}})$ varies over all the classically complete implementations with N-qubit ancilla. From Eqs. (22) and (27), we have

$$\frac{1}{2}\left(1 - \cos\frac{2\pi}{N+1}\right) \geq \min_{(U,|A\rangle)} \max_{\rho_{\mathbf{S}}} D(\mathcal{E}_{U,|A\rangle}(\rho_{\mathbf{S}}),\mathcal{E}_{X_{\mathbf{S}}}(\rho_{\mathbf{S}})) \geq \frac{1}{2}\left(1 - \cos\frac{2\pi}{N+4}\right), \tag{30}$$

where $(U,|A\rangle)$ varies over all the pure conservative implementations. Finally, from Eqs. (23) and (27), we have

[1] Note that the presentation of Ref. [19] discusses the conservation law for the x component of the spin instead of the z component considered in the present paper. However, in that argument the x component and the z component are completely interchangeable, since we have both relations $H^{\dagger}XH = Z$ and $H^{\dagger}ZH = X$ from $H = H^{\dagger}$.

$$\frac{1}{2}\left(1-\cos\frac{2\pi}{N+1}\right) \geqslant \min_{(U,\rho_{\mathbf{A}})} \max_{\rho_{\mathbf{S}}} D(\mathcal{E}_{U,\rho_{\mathbf{A}}}(\rho_{\mathbf{S}}),\mathcal{E}_{X_{\mathbf{S}}}(\rho_{\mathbf{S}})) \geqslant \frac{1}{2}\left(1-\cos\frac{\pi}{N+2}\right), \quad (31)$$

where $(U,\rho_{\mathbf{A}})$ varies over all the conservative implementations with N-qubit ancilla **A**.

III. LOWER BOUND OF THE GATE TRACE DISTANCE

In this section, we investigate the maximum trace distance over all possible input states of **S** for given U and $\rho_{\mathbf{A}}$ in a general way without considering the conservation law.

A. System input state and trace distance

We start with a description of the output states controlled by any unitary operator U on $\mathcal{H}_{\mathbf{S}}\otimes\mathcal{H}_{\mathbf{A}}$. Any pure input state $|\psi\rangle$ of **S** can be described as

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad (32)$$

where $|\alpha|^2+|\beta|^2=1$. We assume that the input state of **A** is a pure state $|A\rangle$, so that the input state of the composite system **S**+**A** is the product state $|\psi\rangle\otimes|A\rangle$. When $|0\rangle$ or $|1\rangle$ is an input state of **S** the corresponding output state of **S**+**A** can be generally expressed as

$$U(|0\rangle\otimes|A\rangle) = |0\rangle\otimes|A_0^0\rangle + |1\rangle\otimes|A_1^0\rangle,$$

$$U(|1\rangle\otimes|A\rangle) = |0\rangle\otimes|A_0^1\rangle + |1\rangle\otimes|A_1^1\rangle, \quad (33)$$

where $|A_j^i\rangle\in\mathcal{H}_{\mathbf{A}}$ for $i,j=0,1$. Normalizing these states gives

$$\||A_0^0\rangle\|^2 + \||A_1^0\rangle\|^2 = 1, \quad \||A_0^1\rangle\|^2 + \||A_1^1\rangle\|^2 = 1. \quad (34)$$

The output state of **S**+**A** corresponding to $|\psi\rangle$ can then be expressed as

$$U(|\psi\rangle\otimes|A\rangle) = \alpha(|0\rangle\otimes|A_0^0\rangle + |1\rangle\otimes|A_1^0\rangle) + \beta(|0\rangle\otimes|A_0^1\rangle + |1\rangle\otimes|A_1^1\rangle). \quad (35)$$

Normalizing Eq. (35) gives

$$\mathrm{Re}[\alpha^*\beta(\langle A_0^0|A_0^1\rangle + \langle A_1^0|A_1^1\rangle)] = 0. \quad (36)$$

The output state $\mathcal{E}_{U,|A\rangle}(|\psi\rangle) := \mathcal{E}_{U,|A\rangle}(|\psi\rangle\langle\psi|)$ of **S** is given by the partial trace of Eq. (35) with respect to **A** as follows:

$$\begin{aligned}\mathcal{E}_{U,|A\rangle}(|\psi\rangle) &= \mathrm{Tr}_{\mathbf{A}}[U(|\psi\rangle\langle\psi|\otimes|A\rangle\langle A|)U^\dagger] \\ &= (|\alpha|^2\||A_0^0\rangle\|^2 + \alpha\beta^*\langle A_0^1|A_0^0\rangle + \alpha^*\beta\langle A_0^0|A_0^1\rangle \\ &\quad + |\beta|^2\||A_0^1\rangle\|^2)|0\rangle\langle 0| + (|\alpha|^2\langle A_1^0|A_0^0\rangle + \alpha\beta^*\langle A_1^1|A_0^0\rangle \\ &\quad + \alpha^*\beta\langle A_1^0|A_0^1\rangle + |\beta|^2\langle A_1^1|A_0^1\rangle)|0\rangle\langle 1| + (|\alpha|^2\langle A_0^0|A_1^0\rangle \\ &\quad + \alpha\beta^*\langle A_0^1|A_1^0\rangle + \alpha^*\beta\langle A_0^0|A_1^1\rangle + |\beta|^2\langle A_0^1|A_1^1\rangle)|1\rangle\langle 0| \\ &\quad + (|\alpha|^2\||A_1^0\rangle\|^2 + \alpha\beta^*\langle A_1^1|A_1^0\rangle \\ &\quad + \alpha^*\beta\langle A_1^0|A_1^1\rangle + |\beta|^2\||A_1^1\rangle\|^2)|1\rangle\langle 1|. \end{aligned} \quad (37)$$

On the other hand, if the quantum NOT gate were to be perfectly realized, the output state $\mathcal{E}_{X_{\mathbf{S}}}(|\psi\rangle) := \mathcal{E}_{X_{\mathbf{S}}}(|\psi\rangle\langle\psi|)$ would be given by

$$\begin{aligned}\mathcal{E}_{X_{\mathbf{S}}}(|\psi\rangle) &= X_{\mathbf{S}}|\psi\rangle\langle\psi|X_{\mathbf{S}}^\dagger \\ &= |\beta|^2|0\rangle\langle 0| + \alpha^*\beta|0\rangle\langle 1| \\ &\quad + \alpha\beta^*|1\rangle\langle 0| + |\alpha|^2|1\rangle\langle 1|. \end{aligned} \quad (38)$$

We now consider the trace distance between $\mathcal{E}_{U,|A\rangle}(|\psi\rangle)$ and $\mathcal{E}_X(|\psi\rangle)$. Note that the trace distance between two-dimensional states σ^ξ and σ^η can be described as

$$D(\sigma^\xi,\sigma^\eta) = \sqrt{|\sigma_{01}^\xi - \sigma_{01}^\eta|^2 - (\sigma_{00}^\xi - \sigma_{00}^\eta)(\sigma_{11}^\xi - \sigma_{11}^\eta)}, \quad (39)$$

where $\sigma_{ij}^k=\langle i|\sigma^k|j\rangle$ for $k=\xi,\eta$. Using this relation, the trace distance $D(\mathcal{E}_{X_{\mathbf{S}}}(|\psi\rangle),\mathcal{E}_{U,|A\rangle}(|\psi\rangle))$ is

$$\begin{aligned} D(\mathcal{E}_{U,|A\rangle}(|\psi\rangle),\mathcal{E}_{X_{\mathbf{S}}}(|\psi\rangle)) &= \{|\alpha^*\beta - (|\alpha|^2\langle A_1^0|A_0^0\rangle + \alpha\beta^*\langle A_1^1|A_0^0\rangle + \alpha^*\beta\langle A_1^0|A_0^1\rangle \\ &\quad + |\beta|^2\langle A_1^1|A_0^1\rangle)|^2 - [|\beta|^2 - (|\alpha|^2\||A_0^0\rangle\|^2 \\ &\quad + \alpha\beta^*\langle A_0^1|A_0^0\rangle + \alpha^*\beta\langle A_0^0|A_0^1\rangle + |\beta|^2\||A_0^1\rangle\|^2)] \\ &\quad \times [|\alpha|^2 - (|\alpha|^2\||A_1^0\rangle\|^2 + \alpha\beta^*\langle A_1^1|A_1^0\rangle \\ &\quad + \alpha^*\beta\langle A_1^0|A_1^1\rangle + |\beta|^2\||A_1^1\rangle\|^2)]\}^{1/2}. \end{aligned} \quad (40)$$

Let $\epsilon_0=\||A_0^0\rangle\|^2$ and $\epsilon_1=\||A_1^1\rangle\|^2$. Then $\||A_1^0\rangle\|^2=1-\epsilon_0$ and $\||A_0^1\rangle\|^2=1-\epsilon_1$ by Eq. (34). Thus Eqs. (36) and (40) give

$$\begin{aligned} D(\mathcal{E}_{U,|A\rangle}(|\psi\rangle),\mathcal{E}_{X_{\mathbf{S}}}(|\psi\rangle)) &= \{|\alpha^*\beta(1-\langle A_1^0|A_0^1\rangle) + \alpha\beta^*\langle A_1^1|A_0^0\rangle \\ &\quad - |\alpha|^2\langle A_1^0|A_0^0\rangle - |\beta|^2\langle A_1^1|A_0^1\rangle|^2 \\ &\quad + [-|\alpha|^2\epsilon_0 + |\beta|^2\epsilon_1 \\ &\quad - 2\,\mathrm{Re}(\alpha^*\beta\langle A_0^0|A_0^1\rangle)]^2\}^{1/2}. \end{aligned} \quad (41)$$

Clearly $[(-|\alpha|^2\epsilon_0+|\beta|^2\epsilon_1)-2\,\mathrm{Re}(\alpha^*\beta\langle A_0^0|A_0^1\rangle)]^2\geqslant 0$, and hence we obtain

$$\begin{aligned} D(\mathcal{E}_{U,|A\rangle}(|\psi\rangle),\mathcal{E}_{X_{\mathbf{S}}}(|\psi\rangle)) &\geqslant |\alpha^*\beta(1-\langle A_1^0|A_0^1\rangle) + \alpha\beta^*\langle A_1^1|A_0^0\rangle \\ &\quad - |\alpha|^2\langle A_1^0|A_0^0\rangle - |\beta|^2\langle A_1^1|A_0^1\rangle|. \end{aligned} \quad (42)$$

B. Lower bound for maximum trace distance

In the following, we shall prove that for any U and $|A\rangle$, we have

$$\max_{\rho_{\mathbf{S}}} D(\mathcal{E}_{U,|A\rangle}(\rho_{\mathbf{S}}),\mathcal{E}_{X_{\mathbf{S}}}(\rho_{\mathbf{S}})) \geqslant \frac{1}{2}|1-\langle A_1^0|A_0^1\rangle|, \quad (43)$$

by considering the maximization of Eq. (42) over the input state $|\psi\rangle$ of **S**. This means that the output trace distance must satisfy Eq. (43) for any interaction and any input state of **A**.

The proof is as follows. We consider the input state $|\psi'\rangle = \alpha|0\rangle + \beta|1\rangle$ such that $|\alpha| = |\beta| = \frac{1}{\sqrt{2}}$. Let θ be such that $\alpha^*\beta = \frac{1}{2}e^{i\theta}$ and $0 \leqslant \theta < 2\pi$. Then Eq. (42) gives

$$D(\mathcal{E}_{U,|A\rangle}(|\psi'\rangle),\mathcal{E}_{X_{\mathbf{S}}}(|\psi'\rangle)) \geqslant \frac{1}{2}|e^{i\theta}(1-\langle A_1^0|A_0^1\rangle) + e^{-i\theta}\langle A_1^1|A_0^0\rangle - \langle A_1^0|A_0^0\rangle - \langle A_1^1|A_0^1\rangle|. \quad (44)$$

Here three complex numbers $1-\langle A_1^0|A_0^1\rangle$, $\langle A_1^1|A_0^0\rangle$, and $-\langle A_1^0|A_0^0\rangle - \langle A_1^1|A_0^1\rangle$, which are determined by U and $|A\rangle$, can be expressed as

$$1-\langle A_1^0|A_0^1\rangle = r_1 e^{i\phi_1}, \quad \langle A_1^1|A_0^0\rangle = r_2 e^{i\phi_2},$$

$$-\langle A_1^0|A_0^0\rangle - \langle A_1^1|A_0^1\rangle = r_3 e^{i\phi_3}, \quad (45)$$

where $r_i \geqslant 0$ and $0 \leqslant \phi_i < 2\pi$ for $i=1,2,3$. Then $r_1 = |1-\langle A_1^0|A_0^1\rangle|$ and

$$D(\mathcal{E}_{U,|A\rangle}(|\psi'\rangle),\mathcal{E}_{X_{\mathbf{S}}}(|\psi'\rangle)) \geqslant \frac{1}{2}|r_1 + r_2 e^{i(-2\theta-\phi_1+\phi_2)} + r_3 e^{i(-\theta+\phi_3-\phi_1)}|. \quad (46)$$

Note that Eq. (46) is maintained for any θ which is independent of U and $|A\rangle$. Hence, we consider the following two cases. In the first case, suppose that U and $|A\rangle$ satisfy $r_2 \geqslant r_3$. In this case, for the input state $|\psi_a'\rangle$ of $\mathbf{S}$ with $\theta = \frac{1}{2}(\phi_2 - \phi_1)$, we have

$$D(\mathcal{E}_{U,|A\rangle}(|\psi_a'\rangle),\mathcal{E}_{X_{\mathbf{S}}}(|\psi_a'\rangle)) = \frac{1}{2}|r_1 + r_2 + r_3 e^{i\{-(\phi_2-\phi_1)+\phi_3-\phi_1\}/2}| \geqslant \frac{1}{2}|r_1 + r_2 - r_3| \geqslant \frac{1}{2}r_1.$$

Thus, there exists a state $|\psi\rangle$ of $\mathbf{S}$ that satisfies $D(\mathcal{E}_{X_{\mathbf{S}}}(|\psi\rangle),\mathcal{E}_{U,|A\rangle}(|\psi\rangle)) \geqslant \frac{1}{2}r_1$ in the case where $r_2 \geqslant r_3$. In the second case, suppose that U and $|A\rangle$ satisfy $r_2 < r_3$. In this case, for the input state $|\psi_b'\rangle$ with $\theta = \phi_3 - \phi_1$, we have

$$D(\mathcal{E}_{U,|A\rangle}(|\psi_b'\rangle),\mathcal{E}_{X_{\mathbf{S}}}(|\psi_b'\rangle)) = \frac{1}{2}|r_1 + r_2 e^{i\{-2(\phi_3-\phi_1)-\phi_1+\phi_2\}} + r_3| \geqslant \frac{1}{2}|r_1 + r_3 - r_2| \geqslant \frac{1}{2}r_1.$$

Thus, there exists a state $|\psi\rangle$ of $\mathbf{S}$ that satisfies $D(\mathcal{E}_{U,|A\rangle}(|\psi\rangle),\mathcal{E}_{X_{\mathbf{S}}}(|\psi\rangle)) \geqslant \frac{1}{2}r_1$ in the case where $r_2 < r_3$. We therefore conclude that for any U and $|A\rangle$, there exists a state $|\psi\rangle$ of $\mathbf{S}$ such that the input state $\rho_{\mathbf{S}} = |\psi\rangle\langle\psi|$ satisfies

$$D(\mathcal{E}_{U,|A\rangle}(\rho_{\mathbf{S}}),\mathcal{E}_{X_{\mathbf{S}}}(\rho_{\mathbf{S}})) \geqslant \frac{1}{2}|1-\langle A_1^0|A_0^1\rangle|. \quad (47)$$

This completes the proof.

In Eq. (43), if the inner product $\langle A_1^0|A_0^1\rangle$ could take one by a certain choice of U and $|A\rangle$, the lower bound could take zero. This may mean a perfect realization of $\mathcal{E}_{U,|A\rangle}$ exists. However, we will show in the following sections that the inner product cannot take one by assuming the conservation law (1). This result will give us a precision limit of the quantum NOT gate.

IV. PRECISION LIMIT GIVEN THE ANCILLA STATE

In this section, we derive the lower bound which depends on the input state of the ancilla system by minimizing the right-hand side of Eq. (47) over the evolution operator U under the conservation law.

A. Constraints on ancilla input states

We start with the description of the input state of $\mathbf{A}$. The sum of the Pauli Z operators on $\mathbf{A}$ is the operator $Z_{\mathbf{A}}$ on $\mathcal{H}_{\mathbf{A}}$ given by

$$Z_{\mathbf{A}} = \sum_{i=1}^{N} Z_{\mathbf{A}_i}.$$

We denote the eigenspace in $Z_{\mathbf{A}}$ of an eigenvalue ξ by $E_\xi^{Z_{\mathbf{A}}}$. The eigenvalues are $N-2n$, where $n=0,1,2,\ldots,N$. The dimension of the eigenspace of the eigenvalue $N-2n$ is $d_n = \frac{N!}{(N-n)!n!}$. Note that the Hilbert space of $\mathbf{A}$ is the direct sum of the spaces $E_{N-2n}^{Z_{\mathbf{A}}}$ for $n=0,1,\ldots,N$:

$$\mathcal{H}_{\mathbf{A}} = \oplus_{n=0}^{N} E_{N-2n}^{Z_{\mathbf{A}}}. \quad (48)$$

Therefore, for any input state $|A\rangle$ of $\mathbf{A}$ there exist $a_n \in \mathbf{C}$ and $|\phi_n^A\rangle \in E_{N-2n}^{Z_{\mathbf{A}}}$ with $\||\phi_n^A\rangle\| = 1$ satisfying

$$|A\rangle = \sum_{n=0}^{N} a_n |\phi_n^A\rangle. \quad (49)$$

Normalizing Eq. (49) gives

$$\sum_{n=0}^{N} |a_n|^2 = 1. \quad (50)$$

Next we describe the output state of $\mathbf{S}+\mathbf{A}$ under the conservation law. Let $E_m^{Z_{\mathbf{S}}}$ be the eigenspace of an eigenvalue $m=1,-1$ of $Z_{\mathbf{S}}$ and E_λ^{Z} be the eigenspace of an eigenvalue λ of Z, where $Z = Z_{\mathbf{S}} + Z_{\mathbf{A}}$, which has

$$\lambda = N + 1 - 2n, \quad (51)$$

where $n=0,1,\ldots,N,N+1$. The eigenspace E_λ^Z can be expressed by the tensor product of the space $E_1^{Z_{\mathbf{S}}} \otimes E_{N-2n}^{Z_{\mathbf{A}}}$ and the space $E_{-1}^{Z_{\mathbf{S}}} \otimes E_{N-2n}^{Z_{\mathbf{A}}}$ as follows:

$$E_{N+1}^Z = E_1^{Z_{\mathbf{S}}} \otimes E_N^{Z_{\mathbf{A}}},$$

$$E_{N+1-2}^Z = (E_1^{Z_{\mathbf{S}}} \otimes E_{N-2}^{Z_{\mathbf{A}}}) \oplus (E_{-1}^{Z_{\mathbf{S}}} \otimes E_N^{Z_{\mathbf{A}}}),$$

$$E_{N+1-4}^Z = (E_1^{Z_{\mathbf{S}}} \otimes E_{N-4}^{Z_{\mathbf{A}}}) \oplus (E_{-1}^{Z_{\mathbf{S}}} \otimes E_{N-2}^{Z_{\mathbf{A}}}),$$

$$\vdots$$

$$E_{N+1-2n}^Z = (E_1^{Z_{\mathbf{S}}} \otimes E_{N-2n}^{Z_{\mathbf{A}}}) \oplus (E_{-1}^{Z_{\mathbf{S}}} \otimes E_{N-2(n-1)}^{Z_{\mathbf{A}}}),$$

$$\vdots$$

$$E^{Z}_{-N+1} = (E^{Z_S}_{1} \otimes E^{Z_A}_{-N}) \oplus (E^{Z_S}_{-1} \otimes E^{Z_A}_{-N+2}),$$

$$E^{Z}_{-N-1} = E^{Z_S}_{-1} \otimes E^{Z_A}_{-N}. \tag{52}$$

Note that the conservation law (1) can be equivalently expressed by the relation[2]

$$UE^{Z}_{\lambda} \subset E^{Z}_{\lambda} \tag{53}$$

for all λ. Equations (52) and (53) then show that the output state $U(|0\rangle\otimes|\phi^A_n\rangle)$ is an element of the subspace $(E^{Z_S}_{1} \otimes E^{Z_A}_{N-2n}) \oplus (E^{Z_S}_{-1} \otimes E^{Z_A}_{N-2(n-1)})$ for $n=1,2,\ldots,N$, since

$$\begin{aligned} U(|0\rangle \otimes |\phi^A_n\rangle) &\in U(E^{Z_S}_{1} \otimes E^{Z_A}_{N-2n}) \subset UE^{Z}_{N+1-2n} \subset E^{Z}_{N+1-2n} \\ &= (E^{Z_S}_{1} \otimes E^{Z_A}_{N-2n}) \oplus (E^{Z_S}_{-1} \otimes E^{Z_A}_{N-2(n-1)}). \end{aligned} \tag{54}$$

Similarly, the output state $U(|0\rangle\otimes|\phi^A_0\rangle)$ is an element of the subspace $E^{Z_S}_{1}\otimes E^{Z_A}_{N}$, since

$$\begin{aligned} U(|0\rangle \otimes |\phi^A_0\rangle) &\in U(E^{Z_S}_{1} \otimes E^{Z_A}_{N}) = UE^{Z}_{N+1} \subset E^{Z}_{N+1} \\ &= E^{Z_S}_{1} \otimes E^{Z_A}_{N}. \end{aligned} \tag{55}$$

Therefore, by Eqs. (54) and (55), there exist $|(\phi^A_n)^0_0\rangle \in E^{Z_A}_{N-2n}$ and $|(\phi^A_{n-1})^0_1\rangle \in E^{Z_A}_{N-2(n-1)}$ such that

$$U(|0\rangle \otimes |\phi^A_n\rangle) = |0\rangle \otimes |(\phi^A_n)^0_0\rangle + |1\rangle \otimes |(\phi^A_{n-1})^0_1\rangle, \tag{56}$$

where $|(\phi^A_{-1})^0_1\rangle=0$. Normalizing Eq. (56) gives

$$\||(\phi^A_n)^0_0\rangle\|^2 + \||(\phi^A_{n-1})^0_1\rangle\|^2 = 1. \tag{57}$$

Similarly, for the output state $U(|1\rangle\otimes|\phi^A_n\rangle)$, there exist $|(\phi^A_{n+1})^1_0\rangle \in E^{Z_A}_{N-2(n+1)}$ and $|(\phi^A_n)^1_1\rangle \in E^{Z_A}_{N-2n}$ such that

$$U(|1\rangle \otimes |\phi^A_n\rangle) = |0\rangle \otimes |(\phi^A_{n+1})^1_0\rangle + |1\rangle \otimes |(\phi^A_n)^1_1\rangle, \tag{58}$$

where $|(\phi^A_{N+1})^1_0\rangle=0$. Normalizing Eq. (58) gives

$$\||(\phi^A_{n+1})^1_0\rangle\|^2 + \||(\phi^A_n)^1_1\rangle\|^2 = 1. \tag{59}$$

We can now obtain useful relations for the output state of **S+A** under the conservation law. For the output state $U(|0\rangle\otimes|A\rangle)$, Eqs. (49) and (56) give

$$\begin{aligned} &U(|0\rangle \otimes |A\rangle) \\ &= |0\rangle \otimes \left(\sum_{n=0}^{N} a_n|(\phi^A_n)^0_0\rangle\right) + |1\rangle \otimes \left(\sum_{n=0}^{N} a_n|(\phi^A_{n-1})^0_1\rangle\right). \end{aligned} \tag{60}$$

Similarly, for the output state $U(|1\rangle\otimes|A\rangle)$, Eqs. (49) and (58) give

$$\begin{aligned} &U(|1\rangle \otimes |A\rangle) \\ &= |0\rangle \otimes \left(\sum_{n=0}^{N} a_n|(\phi^A_{n+1})^1_0\rangle\right) + |1\rangle \otimes \left(\sum_{n=0}^{N} a_n|(\phi^A_n)^1_1\rangle\right). \end{aligned} \tag{61}$$

Comparing Eq. (33) with Eqs. (60) and (61), we obtain the following relations:

$$|A^0_0\rangle = \sum_{n=0}^{N} a_n|(\phi^A_n)^0_0\rangle, \quad |A^0_1\rangle = \sum_{n=0}^{N} a_n|(\phi^A_{n-1})^0_1\rangle,$$

$$|A^1_0\rangle = \sum_{n=0}^{N} a_n|(\phi^A_{n+1})^1_0\rangle, \quad |A^1_1\rangle = \sum_{n=0}^{N} a_n|(\phi^A_n)^1_1\rangle. \tag{62}$$

B. Optimization of the gate trace distance by ancilla input

We can now estimate the inner product $\langle A^0_1|A^1_0\rangle$. By Eq. (62),

$$\langle A^0_1|A^1_0\rangle = \sum_{n,n'=0}^{N} a_{n'}{}^{*} a_n \langle(\phi^A_{n'-1})^0_1|(\phi^A_{n+1})^1_0\rangle, \tag{63}$$

where the inner product $\langle(\phi^A_{n'-1})^0_1|(\phi^A_{n+1})^1_0\rangle$ is given as

$$\langle(\phi^A_{n'-1})^0_1|(\phi^A_{n+1})^1_0\rangle = \begin{cases} 0 & \text{for } n'-1 \neq n+1, \\ \langle(\phi^A_{n+1})^0_1|(\phi^A_{n+1})^1_0\rangle & \text{for } n'-1 = n+1. \end{cases} \tag{64}$$

Therefore,

$$\langle A^0_1|A^1_0\rangle = \sum_{n=0}^{N-2} a_{n+2}{}^{*} a_n \langle(\phi^A_{n+1})^0_1|(\phi^A_{n+1})^1_0\rangle. \tag{65}$$

By the triangle inequality, we have

$$|\langle A^0_1|A^1_0\rangle| \leqslant \sum_{n=0}^{N-2} |a_{n+2}||a_n||\langle(\phi^A_{n+1})^0_1|(\phi^A_{n+1})^1_0\rangle|. \tag{66}$$

From Eqs. (50), (57), and (59), the Schwarz inequality gives the relations

$$\sum_{n=0}^{N-2} |a_{n+2}||a_n| \leqslant 1, \tag{67}$$

$$|\langle(\phi^A_{n+1})^0_1|(\phi^A_{n+1})^1_0\rangle| \leqslant \||(\phi^A_{n+1})^0_1\rangle\|\||(\phi^A_{n+1})^1_0\rangle\| \leqslant 1. \tag{68}$$

Thus,

$$|\langle A^0_1|A^1_0\rangle| \leqslant \sum_{n=0}^{N-2} |a_{n+2}||a_n| \leqslant 1, \tag{69}$$

[2]To see this, let P_λ be the projection on E^Z_λ. Then, (53) is equivalent to $UP_\lambda=P_\lambda UP_\lambda$ for all λ, whereas (1) is equivalent to $UP_\lambda=P_\lambda U$ for all λ. Thus, (1) implies (53). Conversely, from (53) we also have $U(I-P_\lambda)=(I-P_\lambda)U(I-P_\lambda)$ to obtain $P_\lambda U=P_\lambda UP_\lambda$ for all λ, and consequently (1) follows from (53).

so that the maximum of $|\langle A_1^0|A_0^1\rangle|$ is at most $\Sigma_{n=0}^{N-2}|a_{n+2}||a_n|$. Therefore, the minimum of $\frac{1}{2}|1-\langle A_1^0|A_0^1\rangle|$ on the right-hand side of Eq. (43) is at least $\frac{1}{2}(1-\Sigma_{n=0}^{N-2}|a_{n+2}||a_n|)$. Since in the above argument the unitary operator U was arbitrary but satisfied the conservation law, we have

$$\min_U \max_{\rho_{\mathbf{S}}} D(\mathcal{E}_{U,|A\rangle}(\rho_{\mathbf{S}}),\mathcal{E}_{X_{\mathbf{S}}}(\rho_{\mathbf{S}})) \geqslant \frac{1}{2}\left(1-\sum_{n=0}^{N-2}|a_{n+2}||a_n|\right), \tag{70}$$

where U varies over all the unitary operators on $\mathcal{H}_{\mathbf{S}}\otimes\mathcal{H}_{\mathbf{A}}$ satisfying Eq. (1). This is a useful inequality that allows us to evaluate a lower bound of the quantum NOT gate given the input state of the ancilla system. For example, if a_n is a constant, such as

$$a_n = \frac{1}{\sqrt{N+1}} \tag{71}$$

for all $n=0,1,\ldots,N$, then whatever evolution operator is used, an error probability $\frac{1}{N+1}$ determined by Eq. (70) is unavoidable.

The following questions regarding Eq. (70) still remain: What is the lower bound over the input states of the ancilla system? Can we reduce the lower bound to zero by choosing appropriate input states of **A**? In the next section, we will quantitatively show that there exists a nonzero lower bound of the error probability for any input state of the ancilla system and any evolution operator. In order to obtain the bound, it is necessary to minimize Eq. (70) over the input states of **A** under condition (50).

V. PRECISION LIMIT GIVEN THE ANCILLA SIZE

We consider the maximization of $\Sigma_{n=0}^{N-2}|a_{n+2}||a_n|$ over input states of the ancilla system to minimize the right-hand side of Eq. (70) under condition (50). In the first place, we show that this problem can be reduced to the derivation of the maximum eigenvalue of a symmetric matrix. Second, we explain how to derive the maximum eigenvalue, making use of the recurrence formula of Chebyshev polynomials of the second kind. We finally describe the lower bound of the quantum NOT gate which depends only on the size of the ancilla system.

A. Lower bound and eigenvalue problem

The summation $\Sigma_{n=0}^{N-2}|a_{n+2}||a_n|$ can be divided into two parts: the summation of odd subscripts, such as $|a_0||a_2|$, $|a_2||a_4|,\ldots,$ and that of even subscripts, such as $|a_1||a_3|$, $|a_3||a_5|,\ldots.$ For even N,

$$\sum_{n=0}^{N-2}|a_{n+2}||a_n| = \sum_{r=0}^{(N-4)/2}|a_{2r+1}||a_{2r+3}| + \sum_{r=0}^{(N-2)/2}|a_{2r}||a_{2r+2}|, \tag{72}$$

where $N\geqslant 2$. For odd N,

$$\sum_{n=0}^{N-2}|a_{n+2}||a_n| = \sum_{r=0}^{(N-3)/2}|a_{2r+1}||a_{2r+3}| + \sum_{r=0}^{(N-3)/2}|a_{2r}||a_{2r+2}|, \tag{73}$$

where $N\geqslant 3$. We now assume that N is even for simplicity; we will comment on the case of odd N later. To rewrite the summation, we define an $(N+1)$-dimensional vector $\mathbf{A}^\dagger$ by

$$\mathbf{A}^\dagger = [|a_1|,|a_3|,\ldots,|a_{N-1}|,|a_0|,|a_2|,\ldots,|a_N|], \tag{74}$$

where the odd indexed (even indexed) elements are in the first (second) half elements of the vector and the number of those elements is $\frac{N}{2}$ $(\frac{N}{2}+1)$. The summation can then be expressed by a matrix and the vector **A** as

$$\sum_{n=0}^{N-2}|a_{n+2}||a_n| = \mathbf{A}^\dagger\left[\begin{array}{cccccc|cccccc} 0 & 1 & 0 & \cdots & & & 0 & \cdots & & & & 0 \\ 0 & 0 & 1 & & & & \vdots & & & & & \vdots \\ & & \ddots & \ddots & & & & & & & & \\ & & & 0 & 1 & & & & & & & \\ & & & & 0 & & 0 & \cdots & & & & 0 \\ \hline 0 & \cdots & & & 0 & & 0 & 1 & 0 & \cdots & & \\ \vdots & & & & \vdots & & 0 & 0 & 1 & & & \\ & & & & & & & & \ddots & \ddots & & \\ & & & & & & & & & 0 & 1 & \\ 0 & \cdots & & & 0 & & & & & & 0 & \end{array}\right]\mathbf{A}, \tag{75}$$

where the matrix has four submatrices. The upper left [lower right] submatrix is the $\frac{N}{2}\times\frac{N}{2}$ $[(\frac{N}{2}+1)\times(\frac{N}{2}+1)]$ matrix with all the first subdiagonal entries 1 and all the other entries 0. The upper right [lower left] submatrix is the $\frac{N}{2}\times(\frac{N}{2}+1)$ $[(\frac{N}{2}+1)\times\frac{N}{2}]$ matrix with all the entries zero. Taking the complex conjugate of both sides of Eq. (75) gives

$$\sum_{n=0}^{N-2}|a_{n+2}||a_n| = \mathbf{A}^\dagger\left[\begin{array}{ccccc|ccccc} 0 & 0 & \cdots & & & 0 & \cdots & & & 0 \\ 1 & 0 & & & & \vdots & & & & \vdots \\ 0 & 1 & \ddots & & & & & & & \\ \vdots & & \ddots & 0 & 0 & & & & & \\ & & & 1 & 0 & 0 & \cdots & & & 0 \\ \hline 0 & \cdots & & & 0 & 0 & 0 & \cdots & & \\ \vdots & & & & \vdots & 1 & 0 & & & \\ & & & & & 0 & 1 & \ddots & & \\ & & & & & & & \ddots & 0 & \\ 0 & \cdots & & & 0 & & & & 1 & 0 \end{array}\right]\mathbf{A}. \tag{76}$$

Therefore, adding Eq. (75) to Eq. (76) gives

$$\sum_{n=0}^{N-2} |a_{n+2}||a_n| = \mathbf{A}^\dagger \left[\begin{array}{cccccc|cccccc} 0 & \frac{1}{2} & 0 & \cdots & & 0 & \cdots & & & & & 0 \\ \frac{1}{2} & 0 & \frac{1}{2} & & & & \vdots & & & & & \vdots \\ 0 & \frac{1}{2} & 0 & \ddots & & & & & & & & \\ & & \ddots & \ddots & \frac{1}{2} & 0 & & & & & & \\ & & & \frac{1}{2} & 0 & \frac{1}{2} & & & & & & \\ & & & 0 & \frac{1}{2} & 0 & 0 & \cdots & & & & 0 \\ \hline 0 & \cdots & & & & 0 & 0 & \frac{1}{2} & 0 & \cdots & & \\ \vdots & & & & & \vdots & \frac{1}{2} & 0 & \frac{1}{2} & & & \\ & & & & & & 0 & \frac{1}{2} & 0 & \ddots & & \\ & & & & & & & & \ddots & \ddots & \frac{1}{2} & 0 \\ & & & & & & & & & \frac{1}{2} & 0 & \frac{1}{2} \\ 0 & \cdots & & & & 0 & & & & 0 & \frac{1}{2} & 0 \end{array}\right] \mathbf{A}, \tag{77}$$

where the upper left and lower right submatrices are symmetric with all the first subdiagonal and superdiagonal entries $1/2$ and all the other entries 0. Let $\mathbf{A}_{\text{odd}}^\dagger$ and $\mathbf{A}_{\text{even}}^\dagger$ be two vectors defined by

$$\mathbf{A}_{\text{odd}}^\dagger = [|a_1|,|a_3|,|a_5|, \ldots ,|a_{N-1}|],$$

$$\mathbf{A}_{\text{even}}^\dagger = [|a_0|,|a_2|,|a_4|, \ldots ,|a_N|], \tag{78}$$

and S_l be an $l \times l$ symmetric matrix defined by

$$S_l = \begin{bmatrix} 0 & \frac{1}{2} & 0 & 0 & & \\ \frac{1}{2} & 0 & \frac{1}{2} & 0 & & \\ 0 & \frac{1}{2} & 0 & \ddots & & \\ 0 & 0 & \ddots & \ddots & \frac{1}{2} \\ & & & \frac{1}{2} & 0 \end{bmatrix}. \tag{79}$$

Then, Eq. (77) can be written as

$$\sum_{n=0}^{N-2} |a_{n+2}||a_n| = \mathbf{A}_{\text{odd}}^\dagger S_{N/2} \mathbf{A}_{\text{odd}} + \mathbf{A}_{\text{even}}^\dagger S_{N/2+1} \mathbf{A}_{\text{even}}$$
$$\leqslant \|\mathbf{A}_{\text{odd}}\|^2 s_{N/2} + \|\mathbf{A}_{\text{even}}\|^2 s_{N/2+1}, \tag{80}$$

where s_l is the maximum eigenvalue of the symmetric matrix S_l. Recall that $\|\mathbf{A}_{\text{odd}}\|^2 + \|\mathbf{A}_{\text{even}}\|^2 = \mathbf{A}^\dagger \cdot \mathbf{A} = 1$, and thus

$$\max_{\Sigma|a_n|^2=1} \left[\sum_{n=0}^{N-2} |a_{n+2}||a_n|\right] = \max[s_{N/2}, s_{N/2+1}], \tag{81}$$

where the maximization on the right-hand side means selecting the larger of $s_{N/2}$ and $s_{N/2+1}$.

Taking the difference between Eqs. (72) and (73) into account, we apply the same analysis for odd N. Then, we have

$$\max_{\Sigma|a_n|^2=1} \left[\sum_{n=0}^{N-2} |a_{n+2}||a_n|\right] = s_{(N+1)/2}. \tag{82}$$

In this way, the maximization of the summation $\sum_{n=0}^{N-2} |a_{n+2}||a_n|$ under condition (50) reduces to the derivation of the maximum eigenvalue of the symmetric matrices $S_{N/2}$ and $S_{N/2+1}$.

B. Eigenvalue problem and orthogonal polynomials

Next we shall determine the maximum eigenvalue, as mentioned above, and give the lower bound of the quantum NOT gate. It is well known that the eigenvalues and the eigenvectors of the matrix S_l are obtained from a recurrence formula of orthogonal polynomials as follows [37,38]. Chebyshev polynomials $W_l(x)$ for $l=1,2,\ldots$ of the second kind are defined by the relation

$$W_l(\cos\theta) = \frac{\sin(l+1)\theta}{\sin\theta}, \tag{83}$$

where $0 < \theta < \pi$, and are polynomials of the precise degree l and satisfy the recurrence formula

$$xW_0(x) = \frac{1}{2}W_1(x), \tag{84}$$

$$xW_l(x) = \frac{1}{2}W_{l+1}(x) + \frac{1}{2}W_{l-1}(x), \tag{85}$$

where $l \geqslant 1$. The roots $x = x_{l,k}$ of the equation $W_l(x)=0$ are given by

$$x_{l,k} = \cos\frac{k\pi}{l+1} \tag{86}$$

for $k=1,2,\ldots,l$. Let $\mathbf{W}^\dagger(x_{l,k})$ be an l-dimensional vector defined as

$$\mathbf{W}^{\dagger}(x_{l,k}) = (W_0(x_{l,k}), W_1(x_{l,k}), \ldots, W_{l-1}(x_{l,k})). \quad (87)$$

Since $W_l(x_{l,k})=0$, Eqs. (85) and (84) give

$$S_l\mathbf{W}(x_{l,k}) = \begin{bmatrix} 0 & \frac{1}{2} & 0 & & \\ \frac{1}{2} & 0 & \frac{1}{2} & & \\ 0 & \frac{1}{2} & 0 & \ddots & \\ 0 & 0 & \ddots & \ddots & \frac{1}{2} \\ & & & \frac{1}{2} & 0 \end{bmatrix} \begin{bmatrix} W_0(x_{l,k}) \\ W_1(x_{l,k}) \\ \vdots \\ \vdots \\ W_{l-1}(x_{l,k}) \end{bmatrix} = \begin{bmatrix} \frac{1}{2}W_1(x_{l,k}) \\ \frac{1}{2}W_0(x_{l,k}) + \frac{1}{2}W_2(x_{l,k}) \\ \vdots \\ \frac{1}{2}W_{j-1}(x_{l,k}) + \frac{1}{2}W_{j+1}(x_{l,k}) \\ \vdots \\ \frac{1}{2}W_{l-2}(x_{l,k}) + \frac{1}{2}W_l(x_{l,k}) \end{bmatrix} = x_{l,k}\mathbf{W}(x_{l,k}). \quad (88)$$

Thus, the vector $\mathbf{W}(x_{l,k})$ is an eigenvector of S_l with eigenvalue $x_{l,k}$. Therefore, the maximum eigenvalue of S_l is

$$s_l = x_{l,1} = \cos\frac{\pi}{l+1} \quad (89)$$

and the corresponding eigenvector is given by

$$\mathbf{W}^{\dagger}(x_{l,1}) = \left[\frac{\sin\frac{(j+1)\pi}{l+1}}{\sin\frac{\pi}{l+1}}\right]_{j=0}^{l-1}. \quad (90)$$

C. Derivation of the lower bound given the size of the ancilla

We have found the maximum eigenvalue, and thus we can now describe a lower bound of the error probability in realizing the quantum NOT gate. For even N, Eqs. (81) and (89) give

$$\max_{\Sigma|a_n|^2=1}\sum_{n=0}^{N-2}|a_{n+2}||a_n| = \cos\frac{2\pi}{N+4}. \quad (91)$$

Recall that the minimization of Eq. (70) over the input states of **A** is derived from the maximization of $\Sigma_{n=0}^{N-2}|a_{n+2}||a_n|$. Thus,

$$\min_{(U,|A\rangle)}\max_{\rho_{\mathbf{S}}} D(\mathcal{E}_{U,|A\rangle}(\rho_{\mathbf{S}}),\mathcal{E}_{X_{\mathbf{S}}}(\rho_{\mathbf{S}})) \geqslant \frac{1}{2}\left(1-\cos\frac{2\pi}{N+4}\right). \quad (92)$$

Similarly, for odd N,

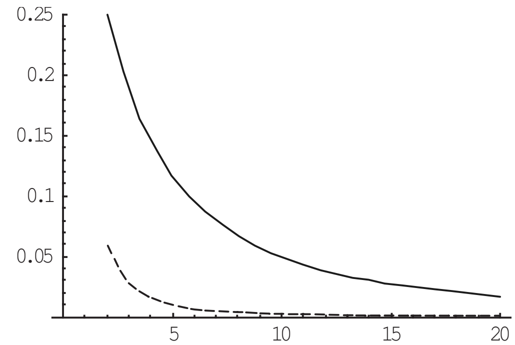

FIG. 1. Plot of the lower bounds as a function of N. The solid line shows the lower bound $\frac{1}{2}(1-\cos\frac{2\pi}{N+4})$ of the quantum NOT gate in Eq. (94). The dashed line shows the lower bound $\frac{1}{4(N^2+1)}$ previously obtained for the Hadamard gate in Ref. [19].

$$\min_{(U,|A\rangle)}\max_{\rho_{\mathbf{S}}} D(\mathcal{E}_{U,|A\rangle}(\rho_{\mathbf{S}}),\mathcal{E}_{X_{\mathbf{S}}}(\rho_{\mathbf{S}})) \geqslant \frac{1}{2}\left(1-\cos\frac{2\pi}{N+3}\right). \quad (93)$$

Here $\cos\frac{2\pi}{N+4}$ is greater than $\cos\frac{2\pi}{N+3}$, and hence we have finally obtained the lower bound for the error probability of any realization of the quantum NOT gate with N-qubit control system under the angular momentum conservation law as

$$\min_{(U,|A\rangle)}\max_{\rho_{\mathbf{S}}} D(\mathcal{E}_{U,|A\rangle}(\rho_{\mathbf{S}}),\mathcal{E}_{X_{\mathbf{S}}}(\rho_{\mathbf{S}})) \geqslant \frac{1}{2}\left(1-\cos\frac{2\pi}{N+4}\right) \quad (94)$$

for any $N(\geqslant 2)$. The bound depends only on the size of the ancilla system: the larger N, the closer to zero is the lower bound.

According to previous works [12,19] based on the uncertainty principle, it may be expected that the lower bound of the quantum NOT gate scales with the inverse of N as $\frac{1}{4(N^2+1)} \approx \frac{1}{4N^2}$. However, the new bound has the leading order $\frac{1}{2}(1-\cos\frac{2\pi}{N+4}) \approx \frac{\pi^2}{N^2}$, so that the lower bound obtained here is really tighter than that as depicted by Fig. 1.

D. Lower bound: General case

We have considered the case where the ancilla state is a pure state. In the following we shall consider the general case. Let $(U,\rho_{\mathbf{A}})$ be a conservative implementation with N qubit ancilla **A**. Then, its purification $(U',|A'\rangle)$ is a conservative pure implementation with $\{N+\lceil\log_2 \mathrm{rank}\rho_{\mathbf{A}}\rceil\}$-qubit ancilla $\mathbf{A}'$ such that $\mathcal{E}_{U,\rho_{\mathbf{A}}}=\mathcal{E}_{U',|A'\rangle}$. Applying Eq. (94) to $\mathcal{E}_{U',|A'\rangle}$, we have

$$\max_{\rho_{\mathbf{S}}} D(\mathcal{E}_{U,\rho_{\mathbf{A}}}(\rho_{\mathbf{S}}),\mathcal{E}_{X_{\mathbf{S}}}(\rho_{\mathbf{S}})) \geqslant \frac{1}{2}\left(1-\cos\frac{2\pi}{N+\log_2 \mathrm{rank}\rho_{\mathbf{A}}+4}\right), \quad (95)$$

and from $N+\log_2 \mathrm{rank}\rho_{\mathbf{A}} \leqslant 2N$, and we conclude

$$\min_{(U,\rho_{\mathbf{A}})} \max_{\rho_{\mathbf{S}}} D(\mathcal{E}_{U,\rho_{\mathbf{A}}}(\rho_{\mathbf{S}}),\mathcal{E}_{X_{\mathbf{S}}}(\rho_{\mathbf{S}})) \geqslant \frac{1}{2}\left(1-\cos\frac{\pi}{N+2}\right), \tag{96}$$

where $(U,\rho_{\mathbf{A}})$ varies over all the conservative implementations with N-qubit ancilla.

VI. LOWER BOUNDS FOR CLASSICALLY COMPLETE IMPLEMENTATIONS AND THEIR ATTAINABILITY

In the preceding section, we have shown that a general lower bound for the error probability in realizing the quantum NOT gate is given by the $1-\cos(1/N)$ scale for the ancilla size N, instead of $1/N^2$ scaling already known for some other gates. Since $2[1-\cos(1/N)]=1/N^2-1/(12N^4)+\cdots$, the new scale has the same leading order as $1/N^2$ up to a constant, but it is natural to ask if the higher-order terms are really meaningful. Here, we shall answer this question, so that the $1-\cos(1/N)$ scale is the best result. To show this, we shall show the attainability of a lower bound with the $1-\cos(1/N)$ scale for classically complete conservative pure implementations. Thus, a classically complete conservative implementation exists even with only 2-qubit ancilla, whereas the substantial error occurs when the input state is a superposition of computational basis states. This result also shows that the general lower bound for conservative implementations with N-qubit ancilla can be reached by a classically complete conservative pure implementations with $2N$-qubit ancilla.

A. Classically complete pure implementations

Let $(U',|A'\rangle)$ be a classically complete conservative pure implementation. Then, we have the following relations:

$$U'(|0\rangle\otimes|A'\rangle)=|1\rangle\otimes|A_1'^0\rangle,$$

$$U'(|1\rangle\otimes|A'\rangle)=|0\rangle\otimes|A_0'^1\rangle, \tag{97}$$

where $|A_1'^0\rangle$ and $|A_0'^1\rangle\in\mathcal{H}_{\mathbf{A}}$.

First, we discuss the constraint on the input state $|A'\rangle$ of $\mathbf{A}$ imposed by the above relations. To illustrate this, we describe $|A'\rangle$ as

$$|A'\rangle=\sum_{n=0}^{N} a_n'|\phi_n^{A'}\rangle, \tag{98}$$

where $|\phi_n^{A'}\rangle$ are normalized vectors in the eigenspaces $E_{N-2n}^{Z_{\mathbf{A}}}$ for all $n=0,1,\ldots,N$ and we have $\sum_{n=0}^{N}|a_n'|^2=1$. Suppose that the input state of $\mathbf{S}$ is $|0\rangle$. Recalling that relation (55) holds by the conservation law, the output state corresponding to the input state $|0\rangle\otimes|\phi_0^{A'}\rangle$ can be written as

$$U'(|0\rangle\otimes|\phi_0^{A'}\rangle)=e^{i\phi'}|0\rangle\otimes|\phi_0^{A'}\rangle, \tag{99}$$

where $e^{i\phi'}$ is a phase factor. Thus the output state corresponding to the input state $|0\rangle\otimes|A'\rangle$ can be expressed as

$$U'(|0\rangle\otimes|A'\rangle)=a_0'e^{i\phi'}|0\rangle\otimes|\phi_0^{A'}\rangle+\sum_{n=1}^{N}a_n'U'(|0\rangle\otimes|\phi_n^{A'}\rangle). \tag{100}$$

Comparing with Eq. (97), a_0' must be zero. Similarly, a_N' must be zero, considering the input state $|1\rangle$.

We now describe the output state in $\mathbf{S}$ from $(U',|A'\rangle)$ for any pure input state $|\psi\rangle$. This is given by the partial trace of the output state in $\mathbf{S}+\mathbf{A}$ with respect to $\mathbf{A}$:

$$\begin{aligned}\mathcal{E}_{U',|A'\rangle}(|\psi\rangle)&=\mathrm{Tr}_{\mathbf{A}}[U'(|\psi\rangle\otimes|A'\rangle)(\langle\psi|\otimes\langle A'|)U'^{\dagger}]\\&=|\beta|^2|0\rangle\langle0|+\alpha^*\beta\langle A_1'^0|A_0'^1\rangle|0\rangle\langle1|\\&\quad+\alpha\beta^*\langle A_0'^1|A_1'^0\rangle|1\rangle\langle0|+|\alpha|^2|1\rangle\langle1|.\end{aligned} \tag{101}$$

Here, we use abbreviations such as $\mathcal{E}(|\psi\rangle):=\mathcal{E}(|\psi\rangle\langle\psi|)$ for any operation $\mathcal{E}$. The trace distance between the ideal quantum NOT operation (38) and $\mathcal{E}_{U',|A'\rangle}(|\psi\rangle)$ is then

$$D(\mathcal{E}_{X_{\mathbf{S}}}(|\psi\rangle),\mathcal{E}_{U',|A'\rangle}(|\psi\rangle))=|\alpha^*\beta||1-\langle A_1'^0|A_0'^1\rangle|. \tag{102}$$

Thus, the derivation of the lower bound for the gate implementation $(U',|A'\rangle)$ can be reduced to estimating the maximum value of $\langle A_1'^0|A_0'^1\rangle$, which is very similar to the general analysis of Sec. IV. However, this case differs from the general analysis in that $a_0=a_N=0$. Taking this condition into account, $|A_1'^0\rangle$ and $|A_0'^1\rangle$ can be written as

$$|A_1'^0\rangle=\sum_{n=1}^{N-1}a_n'|(\phi_{n-1}^{A'})_1^0\rangle,\quad |A_0'^1\rangle=\sum_{n=1}^{N-1}a_n'|(\phi_{n+1}^{A'})_0^1\rangle, \tag{103}$$

where $|(\phi_{n-1}^{A'})_1^0\rangle$ and $|(\phi_{n+1}^{A'})_0^1\rangle$ are normalized vectors in the eigenspaces $E_{N-2(n-1)}^{Z_{\mathbf{A}}}$ and $E_{N-2(n+1)}^{Z_{\mathbf{A}}}$, respectively. Thus,

$$|\langle A_1'^0|A'^1_0\rangle|\leqslant\sum_{n=1}^{N-3}|a_{n+2}'||a_n'|, \tag{104}$$

and therefore,

$$\min_{U'}\max_{\rho_{\mathbf{S}}} D(\mathcal{E}_{U',|A'\rangle}(\rho_{\mathbf{S}}),\mathcal{E}_{X_{\mathbf{S}}}(\rho_{\mathbf{S}}))\geqslant\frac{1}{2}\left(1-\sum_{n=1}^{N-3}|a_{n+2}'||a_n'|\right). \tag{105}$$

Since the discussion in Sec. V can be applied to minimizing Eq. (105) over the input states of $\mathbf{A}$, we see that for even N

$$\min_{(U',|A'\rangle)}\max_{\rho_{\mathbf{S}}} D(\mathcal{E}_{U',|A'\rangle}(\rho_{\mathbf{S}}),\mathcal{E}_{X_{\mathbf{S}}}(\rho_{\mathbf{S}}))\geqslant\frac{1}{2}\left(1-\cos\frac{2\pi}{N+2}\right). \tag{106}$$

This lower bound is slightly larger than the one for the general case; the difference comes close to zero for large N of the ancilla system. We shall comment on the odd N-case later.

B. Attainability of the lower bound for classically complete pure implementations

Next we show that there exists a classically complete implementation $(U',|A'\rangle)$ which attains the lower bound $\frac{1}{2}(1-\cos\frac{2\pi}{N+2})$. We begin by describing the input state $|\widetilde{A}\rangle$ as follows. Let $|(e_n)^i\rangle$ be fixed orthonormal bases in eigenspace $E^{Z_{\mathbf{A}}}_{N-2n}$ as

$$|(e_n)^1\rangle,|(e_n)^2\rangle,\ldots,|(e_n)^k\rangle,\ldots,|(e_n)^{d_n}\rangle, \tag{107}$$

for $n=0,1,\ldots,N$, where $d_n=\frac{N!}{n!(N-n)!}$. In addition, $\widetilde{\mathbf{A}}^\dagger_{\rm odd}$ and $\widetilde{\mathbf{A}}^\dagger_{\rm even}$ are two vectors:

$$\widetilde{\mathbf{A}}^\dagger_{\rm odd}=[\widetilde{a}_1,\widetilde{a}_3,\widetilde{a}_5,\ldots,\widetilde{a}_{N-1}],$$

$$\widetilde{\mathbf{A}}^\dagger_{\rm even}=[\widetilde{a}_2,\widetilde{a}_4,\widetilde{a}_6,\ldots,\widetilde{a}_{N-2}], \tag{108}$$

where $\widetilde{\mathbf{A}}^\dagger_{\rm odd}$ $[\widetilde{\mathbf{A}}^\dagger_{\rm even}]$ is an $(N/2)$ $[(N/2-1)]$ dimensional vector whose entries are indexed by odd [even] numbers. We assume that these vectors satisfy

$$\widetilde{\mathbf{A}}_{\rm odd}=\frac{1}{C_{N/2}}\mathbf{W}(x_{N/2,1}),\quad \widetilde{\mathbf{A}}_{\rm even}=0, \tag{109}$$

where $C_{N/2}=[\mathbf{W}(x_{N/2,1})^\dagger\mathbf{W}(x_{N/2,1})]^{1/2}$. It follows that $\|\widetilde{\mathbf{A}}_{\rm odd}\|^2=1$ by normalization. We assume that the input state $|\widetilde{A}\rangle$ is given by

$$|\widetilde{A}\rangle=\sum_{n=1}^{N-1}\widetilde{a}_n|(e_n)^1\rangle. \tag{110}$$

Recall that $\mathbf{W}(x_{N/2,1})$ is an eigenvector with the maximum eigenvalue of $S_{N/2}$. Then the coefficients $\widetilde{a}_n$ satisfy the following equation:

$$\sum_{n=1}^{N-3}\widetilde{a}_{n+2}\widetilde{a}_n=\widetilde{\mathbf{A}}^\dagger_{\rm odd}S_{N/2}\widetilde{\mathbf{A}}_{\rm odd}=\frac{1}{C^2_{N/2}}\mathbf{W}(x_{N/2,1})^\dagger S_{N/2}\mathbf{W}(x_{N/2,1})$$
$$=s_{N/2}=\cos\frac{2\pi}{N+2}. \tag{111}$$

Constructing the evolution operator $\widetilde{U}$ can be accomplished by determining the transformation for all orthonormal bases. We require that $\widetilde{U}$ satisfy the following conditions. For $n=1,2,\ldots,N$,

$$\widetilde{U}(|0\rangle\otimes|(e_n)^1\rangle)=|1\rangle\otimes|(e_{n-1})^1\rangle,$$

$$\widetilde{U}(|1\rangle\otimes|(e_{n-1})^1\rangle)=|0\rangle\otimes|(e_n)^1\rangle, \tag{112}$$

and for all bases except those that appear in Eq. (112),

$$\widetilde{U}(|0\rangle\otimes|(e_n)^i\rangle)=|0\rangle\otimes|(e_n)^i\rangle,$$

$$\widetilde{U}(|1\rangle\otimes|(e_n)^i\rangle)=|1\rangle\otimes|(e_n)^i\rangle. \tag{113}$$

These requirements determine one-to-one mapping on the orthonormal basis, $\{|0\rangle\otimes|(e_n)^i\rangle,|1\rangle\otimes|(e_n)^i\rangle\}$, and hence there uniquely exists a unitary operator $\widetilde{U}$ fulfilling the above requirements. Note also that $\widetilde{U}$ satisfies the conservation law (1), since from Eqs. (112) and (113) we have the relations $UE^Z_\lambda\subset E^Z_\lambda$ for all λ, which are equivalent to the conservation law, as seen in Eq. (53).

We now describe the output state of $(\widetilde{U},|\widetilde{A}\rangle)$ and the trace distance between the ideal output state and that of $(\widetilde{U},|\widetilde{A}\rangle)$. The output states for $|0\rangle$ and $|1\rangle$ can be generally written as

$$\widetilde{U}(|0\rangle\otimes|\widetilde{A}\rangle)=|0\rangle\otimes|\widetilde{A}^0_0\rangle+|1\rangle\otimes|\widetilde{A}^0_1\rangle,$$

$$\widetilde{U}(|1\rangle\otimes|\widetilde{A}\rangle)=|0\rangle\otimes|\widetilde{A}^1_0\rangle+|1\rangle\otimes|\widetilde{A}^1_1\rangle, \tag{114}$$

respectively, where $|\widetilde{A}^i_j\rangle\in\mathcal{H}_{\mathbf{A}}$ with $i,j=0,1$. On the other hand, by the definitions of $\widetilde{U}$ and $|\widetilde{A}\rangle$, we have

$$\widetilde{U}(|0\rangle\otimes|\widetilde{A}\rangle)=\widetilde{U}\left(|0\rangle\otimes\sum_{n=1}^{N-1}\widetilde{a}_n|(e_n)^1\rangle\right)$$
$$=|1\rangle\otimes\left(\sum_{n=1}^{N-1}\widetilde{a}_n|(e_{n-1})^1\rangle\right),$$

$$\widetilde{U}(|1\rangle\otimes|\widetilde{A}\rangle)=\widetilde{U}\left(|1\rangle\otimes\sum_{n=1}^{N-1}\widetilde{a}_n|(e_n)^1\rangle\right)$$
$$=|0\rangle\otimes\left(\sum_{n=1}^{N-1}\widetilde{a}_n|(e_{n+1})^1\rangle\right). \tag{115}$$

Thus we have the following relations:

$$|\widetilde{A}^0_0\rangle=0,\quad |\widetilde{A}^0_1\rangle=\sum_{n=1}^{N-1}\widetilde{a}_n|(e_{n-1})^1\rangle,$$

$$|\widetilde{A}^1_0\rangle=\sum_{n=1}^{N-1}\widetilde{a}_n|(e_{n+1})^1\rangle,\quad |\widetilde{A}^1_1\rangle=0. \tag{116}$$

Let $\mathcal{E}_{\widetilde{U},|\widetilde{A}\rangle}(|\psi\rangle)$ be the output state of $\mathbf{S}$ from $(\widetilde{U},|\widetilde{A}\rangle)$. The trace distance between $\mathcal{E}_{X_{\mathbf{S}}}(|\psi\rangle)$ and $\mathcal{E}_{\widetilde{U},|\widetilde{A}\rangle}(|\psi\rangle)$ can be expressed in the same way as for Eq. (41) so that we have

$$D(\mathcal{E}_{\widetilde{U},|\widetilde{A}\rangle}(|\psi\rangle),\mathcal{E}_{X_{\mathbf{S}}}(|\psi\rangle))=\{|\alpha^*\beta(1-\langle\widetilde{A}^0_1|\widetilde{A}^1_0\rangle)+\alpha\beta^*\langle\widetilde{A}^1_1|\widetilde{A}^0_0\rangle$$
$$-|\alpha|^2\langle\widetilde{A}^0_1|\widetilde{A}^0_0\rangle-|\beta|^2\langle\widetilde{A}^1_1|\widetilde{A}^1_0\rangle|^2$$
$$+[(-|\alpha|^2\widetilde{\epsilon}_0+|\beta|^2\widetilde{\epsilon}_1)$$
$$-2\,\mathrm{Re}(\alpha^*\beta\langle\widetilde{A}^0_0|\widetilde{A}^1_0\rangle)]^2\}^{1/2}, \tag{117}$$

where $\||\widetilde{A}^0_0\rangle\|^2=\widetilde{\epsilon}_0$, $\||\widetilde{A}^1_1\rangle\|^2=\widetilde{\epsilon}_1$. However, in this case, $\widetilde{\epsilon}_0=\widetilde{\epsilon}_1=0$ from Eq. (116), and therefore

$$D(\mathcal{E}_{\widetilde{U},|\widetilde{A}\rangle}(|\psi\rangle),\mathcal{E}_{X_{\mathbf{S}}}(|\psi\rangle))=|\alpha^*\beta(1-\langle\widetilde{A}^0_1|\widetilde{A}^1_0\rangle)|.$$

Recall that $|(e_n)^1\rangle$ are orthonormal bases. Then, Eq. (111) gives

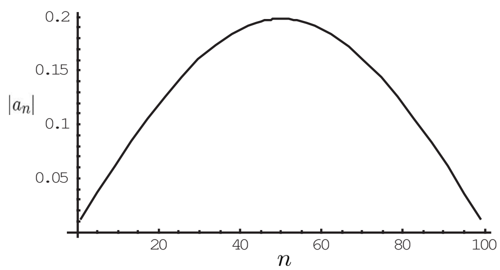

FIG. 2. Distribution of $|a_n|$ with odd subscripts for $N=100$ which gives the lower bound in Eq. (106). This figure shows $\frac{1}{C_{N/2}}W_{(n-1)/2}(x_{N/2,1})$ as a function of odd n.

$$\langle\widetilde{A}_1^0|\widetilde{A}_0^1\rangle = \sum_{n,n'=1}^{N-1}\widetilde{a}_n\widetilde{a}_{n'}\langle(e_{n-1})^1|(e_{n'+1})^1\rangle = \sum_{n'=1}^{N-3}\widetilde{a}_{n'+2}\widetilde{a}_{n'} = \cos\frac{2\pi}{N+2}. \tag{118}$$

Thus,

$$D(\mathcal{E}_{\widetilde{U},|\widetilde{A}\rangle}(|\psi\rangle),\mathcal{E}_{X_{\mathbf{S}}}(|\psi\rangle)) = \left|\alpha^*\beta\left(1-\cos\frac{2\pi}{N+2}\right)\right|.$$

Since the right-hand side is maximized where $|\alpha^*\beta|=\frac{1}{2}$, we have

$$\max_{|\psi\rangle} D(\mathcal{E}_{\widetilde{U},|\widetilde{A}\rangle}(|\psi\rangle),\mathcal{E}_{X_{\mathbf{S}}}(|\psi\rangle)) = \frac{1}{2}\left(1-\cos\frac{2\pi}{N+2}\right). \tag{119}$$

That is, the model $(\widetilde{U},|\widetilde{A}\rangle)$ attains the lower bound in Eq. (106). Notice that our model $(\widetilde{U},|\widetilde{A}\rangle)$ has a distribution of $|a_n|$, as given by Eq. (109). Figure 2 describes the distribution for $N=100$. From a qualitative point of view, in order to reduce the lower bound of the quantum NOT gate, an input state of the ancilla system should be prepared which has a sufficiently thick distribution in the neighborhood of eigenvalue 0, rather than a constant distribution, such as that given by Eq. (71).

For odd N, the lower bound can be given by setting the input state and the evolution operator as those analogous to the case of even N. The bound is $\frac{1}{2}(1-\cos\frac{2\pi}{N+1})$. The attainability of this bound is also proved by the analogous argument.

Thus, we have shown that

$$\min_{(U,|A\rangle)}\max_{\rho_{\mathbf{S}}} D(\mathcal{E}_{U,|A\rangle}(\rho_{\mathbf{S}}),\mathcal{E}_{X_{\mathbf{S}}}(\rho_{\mathbf{S}})) = \frac{1}{2}\left(1-\cos\frac{2\pi}{N+2}\right), \tag{120}$$

if N is even, and

$$\min_{(U,|A\rangle)}\max_{\rho_{\mathbf{S}}} D(\mathcal{E}_{U,|A\rangle}(\rho_{\mathbf{S}}),\mathcal{E}_{X_{\mathbf{S}}}(\rho_{\mathbf{S}})) = \frac{1}{2}\left(1-\cos\frac{2\pi}{N+1}\right), \tag{121}$$

if N is odd, where $(U,|A\rangle)$ varies over all the classical complete pure implementation with N qubit ancilla.

For arbitrary N, we conclude as a common lower bound

$$\min_{(U,|A\rangle)}\max_{\rho_{\mathbf{S}}} D(\mathcal{E}_{U,|A\rangle}(\rho_{\mathbf{S}}),\mathcal{E}_{X_{\mathbf{S}}}(\rho_{\mathbf{S}})) \geqslant \frac{1}{2}\left(1-\cos\frac{2\pi}{N+2}\right), \tag{122}$$

where $(U,|A\rangle)$ varies over all the classically complete pure implementation with N-qubit ancilla.

We have considered the case where the ancilla state is a pure state. The lower bound for the general case is obtained by the previously developed purification argument, and we conclude the following relations. We have

$$\max_{\rho_{\mathbf{S}}} D(\mathcal{E}_{U,\rho_{\mathbf{A}}}(\rho_{\mathbf{S}}),\mathcal{E}_{X_{\mathbf{S}}}(\rho_{\mathbf{S}})) \geqslant \frac{1}{2}\left(1-\cos\frac{2\pi}{N+\log_2\operatorname{rank}\rho_{\mathbf{A}}+2}\right), \tag{123}$$

for any classically complete implementation $(U,\rho_{\mathbf{A}})$ with N-qubit ancilla, and

$$\min_{(U,\rho_{\mathbf{A}})}\max_{\rho_{\mathbf{S}}} D(\mathcal{E}_{U,\rho_{\mathbf{A}}}(\rho_{\mathbf{S}}),\mathcal{E}_{X_{\mathbf{S}}}(\rho_{\mathbf{S}})) \geqslant \frac{1}{2}\left(1-\cos\frac{\pi}{N+1}\right), \tag{124}$$

where $(U,\rho_{\mathbf{A}})$ varies over all the classically complete implementation with N-qubit ancilla.

VII. CONCLUDING REMARKS

In this paper, we have studied the precision limit of the quantum NOT gate or the bit-flip gate, one of the most basic gates in quantum computation, represented on the single-spin computational qubit by considering the angular momentum conservation law obeyed by the interaction between the computational qubit and the control system supposed to comprise many qubits. Actually, we have considered the effect of the angular momentum conservation law only in a direction the same as the computational basis, usually set as the z direction. Then, the conserved quantity and the computational basis are represented by the Pauli Z operator, whereas the quantum NOT gate is represented by the Pauli X operator. Thus, it is expected that this noncommutativity leads to a precision limit of the gate operation.

In the previous method which was used for other gates [12,19], one finds a way in which the gate under consideration is used as a component of a measuring apparatus, applies a quantitative generalization of the Wigner-Araki-Yanase (WAY) theorem to this measuring apparatus, and obtains the lower bound of error probability. For the Hadamard gate, one finds that it is used to convert the Z measurement to the X measurement and that the Z measurement can be done without error under the conservation law of the

z component. Then, one can conclude that the inevitable error of the X measurement, calculated from the quantitative version of the WAY theorem, is yielded from the converter using the Hadamard gate. This and similar arguments cannot be applied to the quantum NOT gate, since the quantum NOT gate does not convert the direction of measurement, but simply flips the measured bit.

In this paper, we have developed a method for obtaining the inevitable error probability by evaluating the maximum trace distance between the output from the gate realization and the output from the ideal gate. The previous method naturally leads to a lower bound for the infidelity (one minus the squared fidelity). Since the infidelity is dominated by the trace distance, our method gives a tighter lower bound for the error probability.

Our method is based on a straightforward evaluation of the trace distance of two output states and enables us to find the precision limit, Eq. (70), explicitly described by the input state of the ancilla system. It is thus possible to obtain information on how much an ancilla input has an inherent error probability in itself. The correspondence between the two methods is not easy to elicit, but it is an interesting problem for future studies, which would lead to a deeper understanding of the precision limits to quantum control systems.

We have also obtained the lower bound (94) expressed by the size of the ancilla system by minimizing Eq. (70) over the input states of **A** using Chebyshev polynomials of the second kind. The lower bound is much tighter than the scaling expected from the previous result based on the WAY theorem. Since the quantitative generalization of the WAY theorem has a close relation to the universal uncertainty principle for measurement and disturbance [19,20], the previous lower bound for pure conservative implementations is based on the variance of the ancilla state and scales as $\frac{1}{4N^2+4} \approx \frac{1}{4N^2}$, whereas our method revealed the lower bound $\frac{1}{2}(1-\cos\frac{2\pi}{N+4}) \approx \frac{\pi^2}{N^2}$ as a tighter bound. The higher-order terms in $\frac{1}{2}(1-\cos\frac{2\pi}{N+4})$ are considered to be meaningful, since the lower bound $\frac{1}{2}(1-\cos\frac{2\pi}{N+2})$ is attained among classically complete pure conservative implementations. Interestingly, the attainability result shows that the best ancilla states to attain the lower bound are not maximum variance states or uniformly distributed states, but those states with the distribution determined by the recurrence relation characterized by Chebyshev polynomials.

Although our study has assumed that the ancilla system consists of N qubits for comparison with the previous research, the present method is not restricted to this particular control system, and it can be readily applied to other control systems, such as atom-field systems, where the present method would lead to a lower bound that scales as the inverse of the photon number [23]. Our method will be also expected to contribute to the problem of programmable quantum processors [28–30] and related subjects [31–33] in future investigations.

ACKNOWLEDGMENTS

The authors thank Hajime Tanaka, Gen Kimura, and Julio Gea-Banacloche for useful discussions and suggestions. This research was partially supported by the SCOPE project of the MIC, a Grant-in-Aid for Scientific Research No. (B)17340021, of the JSPS, and the CREST project of the JST.

[1] P. W. Shor, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, edited by G. Goldwasser (IEEE Computer Society Press, Los Alamitos, CA, 1994), pp. 124–134.
[2] W. G. Unruh, Phys. Rev. A **51**, 992 (1995).
[3] G. M. Palma, K. A. Suominen, and A. K. Ekert, Proc. R. Soc. London, Ser. A **452**, 567 (1996).
[4] S. Haroche and J.-M. Raimond, Phys. Today **49**(8), 51 (1996).
[5] P. W. Shor, Phys. Rev. A **52**, R2493 (1995).
[6] A. M. Steane, Phys. Rev. Lett. **77**, 793 (1996).
[7] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).
[8] M. Ozawa, in *Proceedings of the Sixth International Conference on Quantum Communication, Measurement and Computing*, edited by J. H. Shappiro and O. Hirota (Rinton Press, Princeton, 2003), pp. 175–180.
[9] J. P. Barnes and W. S. Warren, Phys. Rev. A **60**, 4363 (1999).
[10] J. Gea-Banacloche, Phys. Rev. A **65**, 022308 (2002).
[11] S. J. van Enk and H. J. Kimble, Quantum Inf. Comput. **2**, 1 (2002).
[12] M. Ozawa, Phys. Rev. Lett. **89**, 057902 (2002).
[13] E. P. Wigner, Z. Phys. **133**, 101 (1952).
[14] H. Araki and M. M. Yanase, Phys. Rev. **120**, 622 (1960).
[15] M. Ozawa, Phys. Rev. Lett. **91**, 089802 (2003).
[16] D. A. Lidar, Phys. Rev. Lett. **91**, 089801 (2003).
[17] Y. Kawano and M. Ozawa, Phys. Rev. A **73**, 012339 (2006).
[18] M. Ozawa, Phys. Rev. Lett. **88**, 050402 (2002b).
[19] M. Ozawa, Int. J. Quantum Inf. **1**, 569 (2003).
[20] M. Ozawa, Phys. Rev. A **67**, 042105 (2003).
[21] M. Ozawa, Phys. Lett. A **318**, 21 (2003).
[22] M. Ozawa, Ann. Phys. (N.Y.) **311**, 350 (2004).
[23] J. Gea-Banacloche and M. Ozawa, J. Opt. B: Quantum Semiclassical Opt. **7**, S326 (2005).
[24] W. M. Itano, Phys. Rev. A **68**, 046301 (2003).
[25] A. Silberfarb and I. H. Deutsch, Phys. Rev. A **69**, 042308 (2004).
[26] S. J. van Enk and H. J. Kimble, Phys. Rev. A **68**, 046302 (2003).
[27] J. Gea-Banacloche, Phys. Rev. A **68**, 046303 (2003).
[28] M. A. Nielsen and I. L. Chuang, Phys. Rev. Lett. **79**, 321 (1997).
[29] C. Vidal and J. I. Cirac, e-print quant-ph/0012067.
[30] M. Hillery, M. Ziman, and V. Bužek, Phys. Rev. A **73**, 022345 (2006).
[31] G. M. D'Ariano and P. Perinotti, Phys. Rev. Lett. **94**, 090401

(2005).
[32] G. M. D'Ariano and P. Perinotti, e-print quant-ph/0509183.
[33] G. M. D'Ariano and P. Perinotti, e-print quant-ph/0510033.
[34] V. I. Paulsen, *Completely Bounded Maps and Dilations, Pitman Research Notes in Mathematics*, Vol. 146 (Longman, New York, 1986).
[35] V. P. Belavkin, G. M. D'Ariano, and M. Raginsky, J. Math. Phys. **46**, 062106 (2005).
[36] M. Hotta, T. Karasawa, and M. Ozawa, Phys. Rev. A **72**, 052334 (2005).
[37] G. Szego, *Orthogonal Polynomials* (American Mathematical Society, Providence, RI, 1967).
[38] T. S. Chihara, *An Introduction to Orthogonal Polynomials* (Gordon and Breach, New York, 1978).