Optimal entanglement manipulation via coherent-state transmission

Koji Azuma and Go Kato

1NTT Basic Research Laboratories, 3-1 Morinosato Wakamiya, Atsugi, Kanagawa 243-0198, Japan
2NTT Communication Science Laboratories, 3-1 Morinosato Wakamiya, Atsugi, Kanagawa 243-0198, Japan

(Dated: April 28, 2013)

We derive an optimal bound for arbitrary entanglement manipulation based on the transmission of a pulse in coherent states over a lossy channel followed by local operations and unlimited classical communication (LOCC). This stands on a theorem to reduce LOCC via a local unital qubit channel to local filtering. We also present an optimal protocol based on beam splitters and a quantum nondemolition (QND) measurement on photons. Even if we replace the QND measurement with photon detectors, the protocol outperforms known entanglement generation schemes.

PACS numbers: 03.67.Hk, 03.67.Bg, 03.65.Ud, 03.67.Mn

Entanglement is now well known as an essential resource for quantum communication [1], despite it being found in an attempt to point out a paradoxical nature of quantum mechanics [2]. In fact, it is known that any quantum communication [including quantum key distribution [5]] and entanglement generation protocols in quantum repeaters [6–11] can never be accomplished by distant parties who are not capable of sharing entangled pairs. This implies the importance of evaluating the potential to share entanglement through a given communication channel, which determines its value as a quantum channel. If we look at practical quantum communication such as fiber-based quantum key distribution, free-space quantum communication, entanglement generation in quantum repeaters, quantum communication via superconducting transmission lines, and a quantum memory for bosons (transmission in time), we become aware that all the protocols rely on a lossy bosonic channel. Thus, quantum communication based on this channel is practically the most important class (cf. [4]).

One of the most fundamental protocols in this class is the family of coherent-state-based protocols represented by Bennett 1992 quantum key distribution [3] and entanglement generation protocols in quantum repeaters [6–11]. These protocols are based on the transmission of a pulse in coherent states over a lossy channel, and they are dominated by the following paradigm: (i) A sender prepares an entangled state composed only of beam splitters and a quantum nondemolition (QND) measurement on photons. The derived limit is represented in terms of the total success probability and an average entanglement monotone [14] of the generated entangled states, and it is determined only by the transmittance of the channel. The bound is shown to be accomplished by a simple protocol composed only of beam splitters and a quantum nondemolition (QND) measurement [15] on photons. If we substitute photon-number-resolving detectors for the QND measurement, the protocol can entangle distant qubits with near-optimal performance, which is shown to outperform known protocols [6–11]. Hence, these protocols play the role of an efficient entanglement supplier for various quantum communication schemes.

Coherent-state-based protocols.—We start by defining the protocols considered here: (A-i) A sender called Alice prepares a qubit A and a pulse a in her desired state in the form of \( \sum_{j=0,1} e^{i\theta_j} \sqrt{n_j} |j\rangle_A |\alpha_j\rangle_a \) for a computational basis \( \{ |j\rangle_A \}_{j=0,1} \), coherent states \( \{ |\alpha_j\rangle_a \}_{j=0,1} \), real parameters \( \Theta_j \), and \( q_j \geq 0 \) with \( \sum_{j=0,1} q_j = 1 \); (A-ii) Alice sends the pulse a to a receiver called Bob, through a lossy channel described by an isometry \( |\alpha\rangle_a \rightarrow |\sqrt{T}\alpha\rangle_b |\sqrt{1-T}\rangle_e, \) where \( T \) is the transmittance, b is a mode at Bob’s place, and e is the environment; (A-iii) Then, Alice and Bob manipulate the system \( Ab \) through LOCC to obtain an entangled state \( \tilde{\rho}_{AB} \) between Alice’s system \( A' \) and Bob’s system \( B \), and declare whether they obtain a success outcome k occurring with a probability \( p_k \) or a failure outcome. Note that the output systems \( A'B \) are not limited to qubits [12]. In what follows, the set of all the success events k is denoted by \( \mathcal{S} \).

As a measure of the performance of the protocols, we...
take the total success probability, i.e., \( P_s = \sum_{k \in S} p_k \). We also need to choose an entanglement measure for estimating the value of the obtained entangled states \( \{\tilde{\tau}_{k AB}^A\} \forall k \in S \). Since the output system \( A' B \) has no restrictions in contrast to those described in Refs. \([8, 10, 13]\), the singlet fraction may be unacceptable. Thus, here we take an entanglement monotone \( E \) \([14]\) that is a convex monotonic nondecreasing function of the concurrence \( C \) \([17]\) at least for qubits (cf. \([18]\)). Based on this \( E \), as another measure of the protocols, we adopt the average \( \bar{E} \) of the obtained entangled states \( \{\tilde{\tau}_{k AB}^A\} \forall k \in S \), namely \( \bar{E} = \left( \sum_{k \in S} p_k E(\tilde{\tau}_{k AB}^A) \right) / P_s \).

We also allow Alice and Bob to switch among two or more protocols probabilistically. This corresponds to 13 taking the convex hull of achievable points \( (P_s, P_s E) \).

**Virtual protocol.**—For an actual protocol, we define the virtual protocol \([10]\) that works in the same way as the actual protocol but simplifies the analysis significantly. Steps (A-i) and (A-ii) indicate that, when the pulse arrives at Bob’s site, the state of the total system \( AB \) is prepared in the form

\[
|\psi\rangle_{AB} = \sum_{j=0,1} \sqrt{p_j} |j\rangle_A |u_j\rangle_B \quad \text{for states } \{ |u_j\rangle \}_{j=0,1}
\]

and \( \{ |v_j\rangle \}_{j=0,1} \) with \( |\langle v_1|u_0 \rangle|^2 = T > 0 \). Thus, for a state \( |\psi\rangle_{AB} = \sum_{j=0,1} \sqrt{p_j} |j\rangle_A |u_j\rangle_B \) with \( 2 \xi := |\langle v_1|u_0 \rangle|^2 > 0 \) and for a phase-flip channel \( \Lambda^A_\rho := f_\rho \hat{Z}^A \), where \( \hat{Z}^A := |0\rangle\langle 0| - |1\rangle\langle 1| \) and \( f_\rho := (1 + u \hat{Z}^A) / 2 \), we have \( \text{Tr}_B[|\psi\rangle_\langle\psi|_{AB} \Lambda^A_\rho] = \Lambda^A_\rho(|\psi\rangle_\langle\psi|_{AB}) \). Hence, we can consider any protocol to have the following sequence: (V-i) System \( A \) is prepared in \( |\psi\rangle_{AB} \); (V-ii) \( \Lambda^A_{|\psi\rangle_\langle\psi|_{AB}} \) is applied on qubit \( A \); (V-iii) Alice and Bob perform an LOCC, which provides \( \tilde{\tau}_{k AB}^A \). We call this sequence “the virtual protocol.”

We introduce a proposition that enables us to derive an optimal bound in more general settings (cf. \([22]\)).

**Proposition.**—Let \( (P_s, E) \) be the performance of an LOCC protocol starting with qubits \( AB \) in state \( \mathcal{E}(\varphi, \langle\varphi|_{AB}) \) where \( \mathcal{E} \) is a random local unitary channel \([20]\) defined by \( \mathcal{E}(\rho_{AB}) := \sum_l q_l U_l^A \rho_{AB} U_l^A \). Then, there is a protocol that is not less efficient than \( (P_s, E) \) but that is based only on Bob’s measurement.

In addition, for Schmidt coefficients \( \lambda_0 \) and \( \lambda_1 \leq \lambda_0 \) of \( |\varphi\rangle_{AB} \), the achievable region of \( (P_s, E) \) is described by the convex hull of \( \{ (P_s, E) | 0 \leq P_s < 1, 0 \leq E \leq E(\mathcal{E}_{\max}(P_s)) \} \) with \( E(\mathcal{E}_{\max}(P_s)) = (2\sqrt{\lambda_0 \lambda_1})^{-1} C(\mathcal{E}(\langle\varphi|_{AB})) \) for \( P_s = 2 \lambda_1 \) and \( E(\max(P_s)) = P_s^{-1} (\sqrt{2 - \lambda_1}) / \lambda_0 C(\mathcal{E}(\langle\varphi|_{AB})) \) for \( P_s \geq 2 \lambda_1 \).

**Proof.** Let Kraus operators \( \{M_k^A \otimes N_k^B\} \forall k \in S \) be Alice and Bob’s successful measurement in step (V-iii). Without loss of generality, the input spaces of \( M_k^A \) and \( N_k^B \) can be assumed to be qubit spaces. If Alice and Bob can achieve the measurement \( \{M_k^A \otimes N_k^B\} \forall k \in S \), they can always, in principle, obtain a state \( \hat{\tau}_{k AB}^A \) by \( (M_k^A \otimes N_k^B) \mathcal{E}(\varphi, \langle\varphi|_{AB}) (M_k^A \otimes N_k^B) \). From the convexity of the entanglement monotone \( E \) \([14]\), the performance of this protocol is not less than protocols where, for a set \( S' \subseteq S \), they provide a mixture of the states \( \{\hat{\tau}_{k AB}^A\} \forall k \in S' \). Thus, we can assume that Alice and Bob return the state \( \hat{\tau}_{k AB}^A \) with probability \( P_k \). Note that the range of \( \hat{\tau}_{k AB}^A \) can be assumed to be qubit spaces.

From Proposition 1 in Ref. \([23]\), for any \( U_A \), there exist unitary operators \( \{V_k^A\} \forall k \) and Kraus operators \( \{\hat{O}_{k AB}\} \) that satisfy \( \{M_k^A \hat{U}_k^A \otimes \hat{N}_k^B\} |\varphi\rangle_{AB} = (V_k^A \hat{U}_k^A \otimes \hat{O}_{k AB}) |\varphi\rangle_{AB} \) with \( \hat{d}_k := \det(M_k^A) \det(M_k^A) \det(\hat{N}_k^B) \det(\hat{N}_k^B) = \det(\hat{O}_{k AB}) \det(\hat{O}_{k AB}) \). On the other hand, using the formula \([17]\), we can show that the concurrence \( C \) for the state \( \hat{\tau}_{k AB}^A \) is described by \( p_k C(\hat{\tau}_{k AB}^A) = \sqrt{\det(C(\mathcal{E}(\langle\varphi|_{AB}) \)). Thus, if Bob performs \( \{\hat{O}_{k AB}\} \forall k \), he obtains a state

\[
\hat{\tau}_{k AB}^A := \hat{O}_{k AB} \mathcal{E}(\langle\varphi|_{AB}) \hat{O}_{k AB}^\dagger \quad \text{with probability } p_k
\]

by considering the mixture of \( \{\hat{O}_{k AB}\} \), with the convexity of \( C(\mathcal{E}(\langle\varphi|_{AB}) \), the original LOCC protocol is concluded to be outperformed by a protocol that performs only Bob’s measurement \( \{\hat{O}_{k AB}\} \) with probability \( s \) and returns and \( \hat{\tau}_{k AB}^A \) as the outcome.

Thus, we focus on a protocol that is based on Bob’s measurement \( \{\hat{O}_{k AB}\} \forall k \in S \) and returns state \( \hat{\rho}_{k AB} := \hat{O}_{k AB} \mathcal{E}(\langle\varphi|_{AB}) \hat{O}_{k AB}^\dagger \quad \text{with probability } p_k \). We note that there are Kraus operators \( \hat{\Omega}_k \) and \( \{\hat{L}_k^B\} \forall k \in S \) satisfying \( \hat{L}_k^B \hat{\Omega}_k = \hat{\Omega}_k^\dagger \). In fact, if we define them as

\[
\hat{\Omega}_k = \left[ \sum_{s \in S} \hat{p}_k \hat{L}_s^B \right] \quad \text{and} \quad \hat{L}_k^B := \hat{\Omega}_k^{-1} \hat{\Omega}_k^B
\]

where \( \hat{\Omega}_k^{-1} \) is the inverse of \( \hat{\Omega}_k \) in its range, the operators satisfy \( \hat{\Omega}_k \hat{\Omega}_k^B = \hat{1} \) and \( \sum_{s \in S} \hat{L}_s^B \hat{L}_s^B \leq \hat{1} \) from \(\sum_{s \in S} \hat{\Omega}_s^B \hat{\Omega}_s \leq \hat{1} \). Hence, we can regard Bob’s measurement \( \{\hat{L}_k^B\} \forall k \in S \) as a sequential measurement of \( \mathcal{E}(\mathcal{E}(\langle\varphi|_{AB}) \hat{\Omega}_k \hat{\Omega}_k^B \hat{\Omega}_k) \) for a fixed \( P_s \). On the other hand, for the Schmidt decomposition of \( |\varphi\rangle_{AB} = \sum_{j=0,1} \sqrt{\lambda_j} |j\rangle_A \otimes |j\rangle_B \) and \( \hat{p}_k \mathcal{E}(\tau_{k AB}^A) = (\hat{p}_k \mathcal{E}(\tau_{k AB}^A))^{1/2} \mathcal{E}(\langle\varphi|_{AB}) \langle\varphi|_{AB}) \langle\varphi|_{AB}) \), the equalities hold by choosing \( \hat{\Omega}_k \) with \( \langle 0 | \hat{\Omega}_k^B \hat{\Omega}_k = 0 \). Combined with \( \hat{\Omega}_k \hat{\Omega}_k^B \leq \hat{1} \), this shows that \( \mathcal{E}(\langle\varphi|_{AB}) \langle\varphi|_{AB}) \langle\varphi|_{AB}) \) is the maximum of \( C(\tau_{k AB}^A) \). By considering the mixture of
protocols. The overall statement becomes the proposition.

Optimal bound. Let us apply the proposition to our problem. Schmidt coefficients of $|\psi\rangle_{AB}$ are $\lambda_{\pm} := [1 \pm \sqrt{1-x^2}]/2$, and the concurrence of the input state is $C(A_{(u_1|u_0)}) = \max(1-|u_1|^2, 1-|u_0|^2)$ from Ref. [2], where $x := 2\sqrt{q_0q_1(1-|u_1|^2)}$. Hence, $C_{\text{max}}(P_s) = \max(1-|u_1|^2, 1-|u_0|^2)$ for $P_s < 1 - \sqrt{1-x^2}$ and $C_{\text{max}}(P_s) = P_s^{-1}(1-|u_1|^2, 1-|u_0|^2)$ for $P_s \geq 1 - \sqrt{1-x^2}$. Since $C_{\text{max}}(P_s)$ is a monotonically nondecreasing function of $x$, the choice of $q_0 = q_1 = 1/2$ gives the maximum value of $C_{\text{max}}(P_s)$, which is further bounded by an achievable concurrence $C^\text{opt}_{\text{a}}(P_s)$ with

$$C^\text{opt}_{\text{a}}(P_s) := \frac{u^{1/2} \sqrt{(1-u)(2P_s + u - 1)}}{P_s}$$

(1)

for $u^* := \frac{1}{2} \left[ (1-P_s)(2-T) + \sqrt{4T^2(1-T) + (1-P_s)^2T^2} \right]$ satisfying $1 - P_s \leq u^* \leq 1$. Therefore, the performance $(P_s, P_s, E)$ of any protocol must be in the convex hull of $(\{P_s, P_s, E\} : 0 \leq P_s \leq 1, 0 \leq E \leq E(C^\text{opt}_{\text{a}}(P_s)))$.

Optimal protocol. We have shown that the achievable region of an arbitrary protocol is described by Eqs. (1) and (2). Here we present a specific protocol achieving the optimal bound $C^\text{opt}_{\text{a}}(P_s)$ except for a trivial point $P_s = 1$. We allow Alice and Bob to use a realizable [7] interaction between an off-resonance laser pulse in a coherent state $|\alpha\rangle_a$ and a matter qubit $A$, which is described by a unitary operation $\hat{U}(\theta, |j\rangle_A |\alpha\rangle_a = |j\rangle_A |\alpha e^{i\theta}/\sqrt{2}\rangle_a$ for $j = 0, 1$. $\theta$ depends on the strength of the interaction ($\theta \sim 0.01$). Let us consider the following protocol [see Fig. 1 (a)]: (1) Alice makes a probe pulse in a coherent state $|\alpha\sqrt{T}\rangle_a (\alpha \geq 0)$ interact with her qubit $A$ in a state $\Sigma_{j=1}^{\infty} e^{-i(j-1)\zeta_{\text{c}}/\sqrt{2}} |j\rangle_B$ with $\zeta_{\text{c}} := (1/2)\alpha^2 \sin \theta = \hat{U}_{\theta}$, and she applies a displacement operation $\hat{D}_{-\alpha/\sqrt{T}\cos(\theta/2)}$ to the pulse $a$; (2) Alice sends the pulse to Bob through a lossy channel $a \rightarrow b_1$ (with transmittance $T$) together with the local oscillator (LO); (3) On receiving the pulse $b_1$ and the LO, Bob generates a second probe pulse $b_2$ in a coherent state $|\beta\rangle_b$ with $\beta \geq \alpha$ from the LO, and he makes the pulse $b_2$ interact with his qubit $B$ in state $\Sigma_{j=1}^{\infty} e^{-i(j-1)\zeta_{\text{c}}/\sqrt{2}} |j\rangle_B$ with $\zeta_{\text{c}} := (1/2)\beta^2 \sin \theta = \hat{U}_{\theta}$; (4) Bob applies a displacement operation $\hat{D}_{-\beta \cos(\theta/2)}$ to the pulse $b_2$; (5) Bob further applies a 50/50 beam splitter described by $|\alpha_1\rangle_b |\alpha_2\rangle_b \rightarrow |(\alpha_1 + \alpha_2)/\sqrt{2}\rangle_b |(\alpha_1 - \alpha_2)/\sqrt{2}\rangle_b$ to the pulses in modes $b_1$ and $b_2$; (6) Bob applies a QND measurement to pulses $b_3$ and $b_4$ in order to execute a projective measurement $\{Q_{b_3b_4}, \hat{1}_{b_3b_4} - Q_{b_3b_4}\}$ with $Q_{b_3b_4} := \hat{1}_{b_3b_4} - \sum_{n=0}^{\infty} \langle n|b_3 \otimes \langle n|b_4 \rangle$; (7) If Bob receives an outcome corresponding to the projection $Q_{b_3b_4}^+$, Bob declares the success of the protocol.

In the virtual protocol for this scheme, since Bob’s operations in steps (3)-(7) commute with the phase-flip channel $A_{(u_1|u_0)}$, the operations are assumed to be directly applied to the state $|\psi\rangle_{AB}$. In this sense, the state after step (6) is described by $|\psi\rangle_{AB} = |00\rangle_{AB} |\beta\rangle_{b_1} |\beta\rangle_{b_2} + |01\rangle_{AB} |i\beta\gamma\rangle_{b_1} |\beta\gamma\rangle_{b_2} + |10\rangle_{AB} |\beta\gamma\rangle_{b_1} |\beta\rangle_{b_2} + |11\rangle_{AB} |\beta\gamma\rangle_{b_1} |\beta\rangle_{b_2} /2$ with $\gamma_{\pm} := \sqrt{(\beta \pm \alpha) \sin(\theta/2)}/\sqrt{2}$. This state can be represented, in the respective phase spaces of modes $b_3$ and $b_4$, by $|\psi\rangle_{AB} = \psi_{\text{opt}}$ in Fig. 1 (a). This figure suggests an intuitive reason why this protocol can generate entanglement between qubits $AB$: If there are more photons in mode $b_3 (b_4)$ than in mode $b_2 (b_3)$, the possibility that the state has lived in the subspace spanned by $\{|00\rangle_{AB}, |11\rangle_{AB}\}$ is higher. A direct calculation shows $|\langle A|(|j\rangle \langle 0| \otimes \hat{Q}^{b_3b_4}_{j})|b_3b_4\rangle| \geq \left| 1 - e^{-\gamma^2 - \gamma^2} I_0(2\gamma\sin(\theta)/2) \right|$ for $j = 0, 1$.

Near-optimal protocol. We have shown that a protocol employing the QND measurement on incoming pulses can optimally generate entanglement between Alice’s qubit $A$ and Bob’s entire system $B_{b_3b_4}$ including pulses $b_3b_4$. However, in practice, it is difficult to achieve such a QND measurement, and the pulses $b_3b_4$ are unsuitable for storing the entangled state for a long time. Therefore, it is important to find a protocol that does not need to use a QND measurement and produces entanglement between Alice and Bob’s qubits $AB$ instead of $A$ and $B_{b_3b_4}$. One such protocol can be obtained by replacing steps (6) and (7) in the optimal protocol with the following steps [see Fig. 1 (a)]; (6') Bob counts the number of photons by using photon-number-resolving detectors in modes $b_3$ and $b_4$, respectively; (7') If the outcomes $m$ and $n$ of the two detectors are different, Bob declares the success of the protocol. We consider this modified protocol below.

From the definition, the success probability $P_s$ must be the same as Eq. (3). In the virtual protocol for this scheme, with probability $P_{mn} := e^{-\gamma^2 - \gamma^2} (\gamma_{+}^{2m} \gamma_{+}^{2n} + \gamma_{-}^{2m} \gamma_{-}^{2n})/(2m!n!)$, the protocol returns outcomes $m$ and $n$, and provides a final state $A_{(u_1|u_0)} (\phi_{mn} |\psi_{mn}\rangle_{AB}$ for state

$$P_s = 1 - (\beta^2 + \alpha^2)^2 \sin^2(\theta/2) = I_0((\beta^2 - \alpha^2)^2 \sin^2(\theta/2)).$$

(3)
tical devices in quantum communication can become as optimal performance. This suggests that quantum operations on the optimal protocol [Fig. 1 (a)] with almost entanglement manipulation via coherent-state transmission [7].

Probes [8, 9], and (v) a homodyne-detection-based single-probe protocol [10].

In conclusion, we have provided an optimal bound $E(C)_{\alpha=0}$ for arbitrary entanglement manipulation via coherent-state transmission. In addition, we have presented a simple optimal scheme and its practical version [Fig. 1 (a)] with almost optimal performance. This suggests that quantum optical devices in quantum communication can become as powerful as arbitrary operations. The setting of the problem respects a shared nature of known realistic schemes [11], but we believe that our solution to the problem will provide new insights into fundamental theories such as those in Refs. [4, 12] and into limits on other quantum communication protocols as in Refs. [25, 26].

We thank M. Koashi, who pointed out the possibility of simplifying the proof of our proposition, W. J. Munro, M. Owari, and K. Tamaki, whose comments helped us to improve this paper, and K. Igeta, N. Matsuda, F. Morikoshi, N. Sota, and Y. Tokura for helpful discussions. K.A. is supported by a MEXT Grant-in-Aid for Scientific Research on Innovative Areas 21102008.

FIG. 1: (a) Schematic of near-optimal protocol. If we replace the photon detectors D1 and D2 with the QND measurement to perform the projection $Q_{bs}$, we can reduce the protocol to the optimal one. (b) Performance of various protocols: The average concurrence $\bar{C}$ as a function of the success probability $P_s$ when $T=\frac{e^{-1/\theta}}{t_{th}}$ with $t_{th}=25$ km ($\sim 0.17$ dB/km attenuation) and $\theta=0.01$, for (i) the optimal protocol, (ii) the near-optimal protocol, (iii) a photon-detector-based two-probe protocol [10] that achieves a tight bound [13] for single-error-type entanglement generation, (iv) a photon-detector-based single-probe protocol [8, 9], and (v) a homodyne-detection-based single-probe protocol [7].

$$|\phi_{mn}\rangle_{AB} := \frac{1}{\sqrt{\sum_{mn} C_{mn}}} \sum_{mn} C_{mn} |\phi_{mn}\rangle_{AB} = \frac{1}{\sqrt{\sum_{mn} C_{mn}}} \sum_{mn} C_{mn} |\phi_{mn}\rangle_{AB}$$

Parameters $\alpha$ and $\beta$ (determining $\gamma_{\pm}$) should be chosen to maximize $E$ with $P_s$ fixed.

In Fig. 1 (b), we show the performance of several known protocols [8–11] as well as the optimal and near-optimal protocols in terms of the average concurrence $\bar{C}$. For comparison, we assume that all the devices used in the protocols are ideal. From the figures, we can confirm that the near-optimal protocol performs similarly to the optimal protocol and it outperforms the existing protocols [8–11]. Through the relation $E=E(C)$ for qubits, one could also easily estimate the performance even in terms of the entanglement monotone $E$.

In conclusion, we have provided an optimal bound $E(C)_{\alpha=0}$ for arbitrary entanglement manipulation via coherent-state transmission. In addition, we have presented a simple optimal scheme and its practical version [Fig. 1 (a)] with almost optimal performance. This suggests that quantum optical devices in quantum communication can become as powerful as arbitrary operations.
[23] H.-K. Lo and S. Popescu, Phys. Rev. A 63, 022301 (2001).

[24] If we input $|\omega\rangle_{AB} = \sum_{j=0,1} \sqrt{p_j}|j\rangle_A|\phi_j\rangle_B$ to a phase flip channel $\Lambda^A(\hat{\rho}) := f\hat{\rho} + (1-f)\hat{Z}A\hat{\rho}\hat{Z}A$ with $1/2 \leq f \leq 1$, the concurrence $C$ of the output state $\Lambda^A(|\omega\rangle\langle\omega|_{AB})$ is $2(2f - 1)\sqrt{p_0p_1(1 - |\langle\phi_1|\phi_0\rangle|^2)}$ from the formula [17].

[25] L. Praxmeyer and P. van Loock, Phys. Rev. A 81, 060303(R) (2010).

[26] N. Sangouard et al., Rev. Mod. Phys. 83, 33 (2011).