Signaling versus distinguishing different preparations of same pure quantum state

Chirag Srivastava,[*] Sreetama Das,[†] Aditi Sen(De)[‡] and Ujjwal Sen[§]

Harish-Chandra Research Institute, HBNI,
Chhatnag Road, Jhunsi, Allahabad 211 019, India

Abstract

Different ensembles of quantum states can have the same average nonpure state. Distinguishing between such constructions, via different mixing procedures of the same nonpure quantum state, is known to entail signaling. In parallel, different superpositions of pure quantum states can lead to the same pure state. We show that the possibility of distinguishing between such preparations, via different interferometric setups leading to the same pure quantum state, also implies signaling. The implication holds irrespective of whether the distinguishing procedure is deterministic or probabilistic.

1 Introduction

The state of a quantum system, if it is not pure, always has an infinite number of decompositions into ensembles. It is postulated within quantum mechanics that these decompositions represent the same physical situation. Indeed, it is known that if different decompositions of the same mixed quantum state are distinguishable, it will result in instantaneous communication of information between two spatially separated parties, who can in principle be even space-like separated [1, 2, 3]. In general, it has been found that "tweaking" quantum evolutions, i.e., considering non-quantum evolutions, typically result in signaling [2, 4, 5, 6, 7, 8, 9]. It is interesting to note that the no-signaling constraint has been used with success in several areas. In particular, it has been used to obtain the optimal approximate quantum cloning fidelity [10, 11], and fidelity for optimal quantum state discrimination [12]. Also, there has been an important set of works that considered the security in bit commitment protocols based on the no-signaling principle [13]. Cryptographic protocols have also been considered where the eavesdropper is restrained not by quantum mechanics but by the weaker condition of no-signaling [14]. It is interesting to note here that the no-signaling condition has recently been generalized, leading to interesting consequences [15].

---

[*]E-mail: chiragsrivastava@hri.res.in
[†]E-mail: sreetamadas@hri.res.in
[‡]E-mail: aditi@hri.res.in
[§]E-mail: ujjwal@hri.res.in

If the quantum state of a physical system is pure, it can be represented by superpositions over an infinite number of bases of the corresponding Hilbert space. While different decompositions of the same mixed state can be perceived of as different mixing strategies during the preparation stage of the mixed state, different superpositions of the same pure state can be viewed as different interferometric-type setups during the preparation stage of the pure state. In this paper, we use different representations (superpositions) of the same pure state to indicate that they have been prepared differently, as shown in Fig. 1. Notice that these different preparation procedures of the same state, and an engagement in trying to distinguish between them is an inverse of the attempt to identify and correct errors in the same state in quantum error correction protocols [16]. Error correction codes do exist within the ambit of quantum mechanics.

Here we show that a possibility of discrimination of different preparation procedures of the same pure state, which is postulated in quantum mechanics to be impossible, will result in signaling.
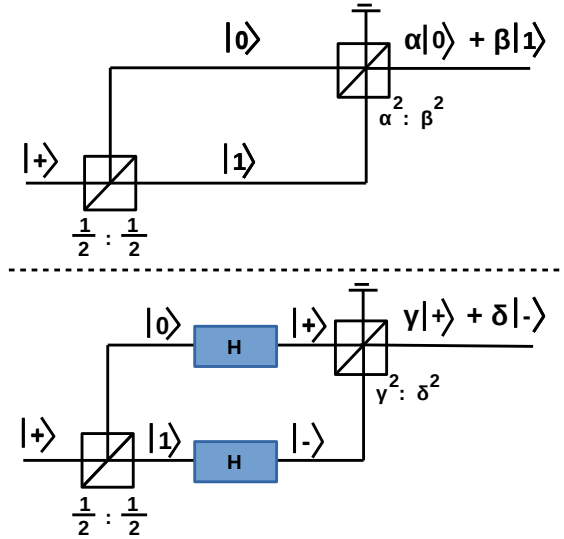

Figure 1: Two preparation procedures of the same state. We consider a photonic set-up, where we denote the horizontal and vertical polarization states as $|0\rangle$ and $|1\rangle$ respectively, and $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. The square boxes represent polarization beam splitters, with their splitting ratios being indicated below them in the figure. The two panels correspond to the two preparation procedures. In both the panels, the input is from the left, and is the state $|+\rangle$. In the upper panel, the vertical final output is discarded, while the state in the horizontal final output channel is $|\psi_{\alpha\beta}\rangle = \alpha|0\rangle + \beta|1\rangle$, where α and β are complex numbers, and $|\alpha|^2 + |\beta|^2 = 1$. In the lower panel, the set-up is otherwise the same, but there are two Hadamard gates inserted, denoted in the figure as rectangular boxes with "H" written on them. Again, the vertical final output is disposed of, and the horizontal final output is in the state $|\psi_{\gamma\delta}\rangle = \gamma|+\rangle + \delta|-\rangle$, where α, β, γ, δ are so chosen that $\alpha|0\rangle + \beta|1\rangle = \gamma|+\rangle + \delta|-\rangle$.

2 The association

Consider two parties, Alice (A) and Bob (B), sharing a pure state,

$$|\Phi\rangle_{AB} = \frac{1}{\sqrt{2}} \left(|\psi_{\alpha\beta}\rangle_A |0\rangle_B + |\psi_{\gamma\delta}\rangle_A |1\rangle_B \right), \tag{1}$$

of two spin-1/2 quantum particles, where

$$|\psi_{\alpha\beta}\rangle = \alpha|0\rangle + \beta|1\rangle \tag{2}$$

is an expansion of the pure spin-1/2 quantum state $|\psi\rangle_A$ in the σ_z basis, and

$$|\psi_{\gamma\delta}\rangle = \gamma|+\rangle + \delta|-\rangle \tag{3}$$

is an expansion of the same state $|\psi\rangle_A$ in the σ_x basis. The two different representations, $|\psi_{\alpha\beta}\rangle$ and $|\psi_{\gamma\delta}\rangle$, are used to imply that they are prepared differently, as shown in Fig. 1. $|0\rangle$ and $|1\rangle$ of Bob's system are again eigenstates of σ_z. All kets and bras in this manuscript are normalized to unity, unless stated otherwise. The state, $|\Phi\rangle_{AB}$, is equivalent to the product (unentangled) state $|\psi\rangle_A \otimes |+\rangle_B$. A potential preparation schematic is presented in Fig. 2.
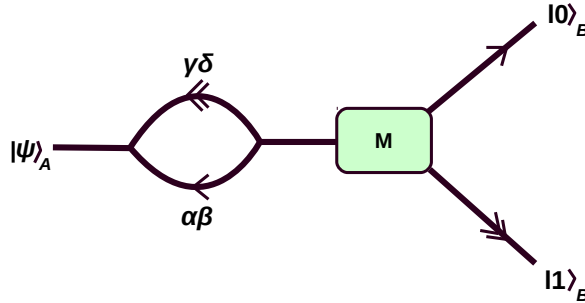

Figure 2: Schematic potential preparation procedure for the state $|\Phi\rangle_{AB}$. The state, $|\Phi\rangle_{AB}$, given in Eq. (1), can in principle be prepared by a machine, $\mathbf{M}$, whose arms on the right represents a qubit, spanned by $|0\rangle_B$ and $|1\rangle_B$, and is in possession of Bob. The output on the left of $\mathbf{M}$ are in possession of Alice. The lower arm on the left represents the preparation procedure of the quantum state $|\psi\rangle$ via the method presented in upper panel in Fig. 1. Parallely, the upper arm on the left represents that via the method presented in lower panel in Fig. 1. Similar to that in, say type-I spontaneous parametric down conversion [17], upper and lower arms respectively on the right and left are correlated, and coherently superposes with instances when the lower and upper arms fire respectively on the right and left.

Let us now assume that Alice has a machine that distinguishes between the two preparation procedures, $|\psi_{\alpha\beta}\rangle$ and $|\psi_{\gamma\delta}\rangle$, of the same pure state $|\psi\rangle_A$. Note that the evolution

(action of the distinguishing machine) is not quantum. But it is assumed that after its application on a situation, it returns some situation of the same physical system. And these situations are still represented by quantum states. Alice and Bob are in two separate locations, say a distance (d) apart, and have had their clocks syncronized. It has also been decided that if it rains at time, t_0, at Alice's location, Alice will apply her machine to her part of the shared state. She won't do anything if it doesn't rain. It takes at least a time $\frac{d}{c}$ for light to travel from Alice's location to Bob's, where c is the speed of light in vacuum. A measurement at Bob's end, say at $t_0 + d/2c$, on his part of the shared state, will reveal whether or not Alice had applied her machine. Indeed, suppose that the distinguishing protocol runs by implementing the transformations

$$
\begin{aligned}
|\psi_{\alpha\beta}\rangle_A |0\rangle_{A_1} &\rightarrow c_{\alpha\beta}|\overline{\psi}_{\alpha\beta}\rangle_{AA_1}, \\
|\psi_{\gamma\delta}\rangle_A |0\rangle_{A_1} &\rightarrow c_{\gamma\delta}|\overline{\psi}_{\gamma\delta}\rangle_{AA_1},
\end{aligned}
\tag{4}
$$

where, for the success of the distinguishing protocol of Alice, we must have $|\langle\overline{\psi}_{\alpha\beta}|\overline{\psi}_{\gamma\delta}\rangle| \neq 1$. $c_{\alpha\beta}$ and $c_{\gamma\delta}$ are arbitrary nonzero complex numbers. A_1 is an auxiliary machine system at Alice's laboratory.

We now assume that the machine is linear on the superposition

$$
\frac{1}{\sqrt{2}}\left(|\psi_{\alpha\beta}\rangle_A |0\rangle_{A_1}|0\rangle_B + |\psi_{\gamma\delta}\rangle_A |0\rangle_{A_1}|1\rangle_B\right),
\tag{5}
$$

although not necessarily on other superpositions. The shared state of the two laboratories (consisting of A, A_1, and B), is exactly in the state in (5), which, after the action of Alice's machine, given by (4), is the unnormalized state

$$
\frac{1}{\sqrt{2}}\left(c_{\alpha\beta}|\overline{\psi}_{\alpha\beta}\rangle_{AA_1}|0\rangle_B + c_{\gamma\delta}|\overline{\psi}_{\gamma\delta}\rangle_{AA_1}|1\rangle_B\right).
\tag{6}
$$

If $|\langle\overline{\psi}_{\alpha\beta}|\overline{\psi}_{\gamma\delta}\rangle| \neq 1$, this state will be entangled [18], in the $AA_1{:}B$ partition, i.e., it cannot be expressed as $\tilde{c}|\chi_{AA_1}\rangle|\chi_B\rangle$, where $\tilde{c}$ is a complex number, and $|\chi_{AA_1}\rangle$ and $|\chi_B\rangle$ are vectors in the Hilbert spaces corresponding to AA_1 and B respectively. Consequently, the local state at Bob's (as well as Alice's) end will possess a nonzero von Neumann entropy, where the von Neumann entropy of a density matrix σ is given by $-\mathrm{tr}(\sigma\log_2\sigma)$. This is the situation if it rained at Alice's location at time t_0. If it didn't, then Alice will not apply the machine corresponding to Eq. (4), and consequently, the von Neumann entropy at Bob's (and Alice's) end will be vanishing, since Bob's state is then pure. To find the von Neumann entropy at Bob's end, Bob can perform a tomography of his part of the shared state, for which we need to assume that there existed several copies of the shared state, and Alice applied the transformation (4), separately, on all copies if it did rain at time t_0. The tomography was performed by Bob at $t_0 + d/2c$. The value of the von Neumann entropy of Bob's state indicates whether it rained or not at Alice's location. We therefore find that the assumption of the possibility of distinguishing between $|\psi_{\alpha\beta}\rangle$ and $|\psi_{\gamma\delta}\rangle$ leads to the signaling, i.e., superluminal transfer of classical information.

To reiterate, we have assumed (a) that a certain machine exists which can distinguish between two superpositions of the same state, and (b) that the machine is linear on

a certain superposition. The conjunction of these two assumptions implies signaling. Assuming that no-signaling is a physical constraint that we wish to adhere to, (a) or (b) or both are wrong. It is true that the machine assumed in (a) is not unitary. Indeed, no unitary machine can distinguish between two different superpositions of the same state. Our argument is that a future non-quantum theory that may allow non-unitary operations, will still have to keep different superpositions of the same state as non-distinguishable, if it is linear on a particular superposition and if we want to adhere to no-signaling.

Suppose now that Alice is able to apply a transformation that only probabilistically (i.e., sometimes) provides her with the possibility of distinguishing between the two superpositions $|\psi_{\alpha\beta}\rangle$ and $|\psi_{\gamma\delta}\rangle$. If that probability is p, then the transformation (4) needs to be replaced by one that implements

$$
\begin{aligned}
|\psi_{\alpha\beta}\rangle_A |0\rangle_{A_1} &\rightarrow \tilde{c}_{\alpha\beta} \left(\sqrt{p} |\overline{\psi}_{\alpha\beta}\rangle_{AA_1} + \sqrt{1-p} |\overline{\chi}_{\alpha\beta}\rangle_{AA_1} \right) \equiv \tilde{c}_{\alpha\beta} |\widetilde{\psi}_{\alpha\beta}\rangle, \\
|\psi_{\gamma\delta}\rangle_A |0\rangle_{A_1} &\rightarrow \tilde{c}_{\gamma\delta} \left(\sqrt{p} |\overline{\psi}_{\gamma\delta}\rangle_{AA_1} + \sqrt{1-p} |\overline{\chi}_{\gamma\delta}\rangle_{AA_1} \right) \equiv \tilde{c}_{\gamma\delta} |\widetilde{\psi}_{\gamma\delta}\rangle,
\end{aligned}
\tag{7}
$$

where the projector onto the span of $|\overline{\psi}_{\alpha\beta}\rangle$ and $|\overline{\psi}_{\gamma\delta}\rangle$ is orthogonal to that onto the span of $|\overline{\chi}_{\alpha\beta}\rangle$ and $|\overline{\chi}_{\gamma\delta}\rangle$. $\tilde{c}_{\alpha\beta}$ and $\tilde{c}_{\gamma\delta}$ are arbitrary nonzero complex numbers. The relative phases on the right-hand-sides of (7) have been absorbed in the definitions of $|\overline{\chi}_{\alpha\beta}\rangle$ and $|\overline{\chi}_{\gamma\delta}\rangle$. Note that the relevant states, $|\overline{\psi}_{\alpha\beta}\rangle$ and $|\overline{\psi}_{\gamma\delta}\rangle$, can be obtained with probability p, assumed to be non-zero, when a measurement, comprising of two projectors, viz. the projector onto the span of $|\overline{\psi}_{\alpha\beta}\rangle$ and $|\overline{\psi}_{\gamma\delta}\rangle$ and that onto the orthogonal complement of that span, is performed. The transformation (7) followed by the measurement is similar to the "unitary-reduction" machines that are used in probabilistic cloning of quantum states [19] and tasks like probabilistic teleportation, dense coding, and masking of quantum information [20]. A difference of our "probabilistic" scheme with the unitary-reduction methods is that instead of a deterministic unitary evolution followed by a measurement, a deterministic non-unitary evolution (7) followed by a measurement is considered here. Such probabilistic machines are different from probabilistic processes where different deterministic processes are applied probabilistically onto an input, e.g. in twirling operations (see e.g. [21]). For the transformation (7) to offer a probabilistic protocol of distinguishing between $|\psi_{\alpha\beta}\rangle$ and $|\psi_{\gamma\delta}\rangle$, one must have $|\langle\overline{\psi}_{\alpha\beta}|\overline{\psi}_{\gamma\delta}\rangle|$ strictly less than unity. In that case, the modulus of the inner product of the normalized portions in the right-hand-sides of the transformation (7) can be bounded above strictly by unity:

$$
\begin{aligned}
|\langle\widetilde{\psi}_{\alpha\beta}|\widetilde{\psi}_{\gamma\delta}\rangle| &\leq p|\langle\overline{\psi}_{\alpha\beta}|\overline{\psi}_{\gamma\delta}\rangle| + (1-p)|\langle\overline{\chi}_{\alpha\beta}|\overline{\chi}_{\gamma\delta}\rangle| \\
&\leq p|\langle\overline{\psi}_{\alpha\beta}|\overline{\psi}_{\gamma\delta}\rangle| + (1-p) < 1.
\end{aligned}
$$

The first inequality follows from the fact that $|a + b| \leq |a| + |b|$ for complex numbers a and b. The second one follows by using $|\langle\overline{\chi}_{\alpha\beta}|\overline{\chi}_{\gamma\delta}\rangle| \leq 1$. The third (strict) inequality follows from the fact that as $|\langle\overline{\psi}_{\alpha\beta}|\overline{\psi}_{\gamma\delta}\rangle| < 1$, and that $p \neq 0$. Even this possibility of distinguishing between the states $|\psi_{\alpha\beta}\rangle$ and $|\psi_{\gamma\delta}\rangle$ with some probability leads to signaling. To see this, apply the transformation (7) to the state $|\Phi\rangle_{AB}|0\rangle_{A_1}$ to find that although

it is a product state, in the $AA_1 : B$ partition, before application of the transformation, it becomes entangled after. Again, a linearity for the superposition in (5) is assumed, although linearity for other superpositions may not hold. The post-transformation state is given by

$$\frac{1}{\sqrt{2}} \left(\tilde{c}_{\alpha\beta} |\widetilde{\psi}_{\alpha\beta}\rangle_{AA_1} |0\rangle_B + \tilde{c}_{\gamma\delta} |\widetilde{\psi}_{\gamma\delta}\rangle_{AA_1} |1\rangle_B \right), \tag{8}$$

which is entangled by virtue of the fact that $|\langle \widetilde{\psi}_{\alpha\beta} | \widetilde{\psi}_{\gamma\delta} \rangle| < 1$, which in turn follows from the assumption that the states $|\psi_{\alpha\beta}\rangle$ and $|\psi_{\gamma\delta}\rangle$ are probabilistically distinguishable.

3   Conclusion

It is postulated in quantum mechanics that different preparation procedures of the same pure state cannot be discriminated. Assuming that a physical situation is always represented by a quantum state, it is shown that the existence of a machine that can discriminate between two preparation procedures of the state leads to signaling.

Note added: We note here that the results of Ref. [22] and of this manuscript were obtained in parallel and in knowledge of all authors of the two manuscripts. Although the results reported in the two manuscripts are similar, they use different proofs for obtaining them. Specifically, the proof in [22] uses an initially entangled state shared between two parties, and tries to prove that different preparation procedures of same pure state leads to signaling. Whereas in the current manuscript, we use a state that is initially unentangled (product). Additionally, and, we feel, importantly, the machine, in the current manuscript, that distinguishes between two preparation procedures of the same pure state uses an operation which is beyond quantum mechanics, and that leads to the distinguishing. The motivation here is to ask whether distinguishing different superpositions of the same pure quantum state through a non-quantum process leads to signaling, just like it is already known that distinguishing different mixtures of the same mixed quantum state through a non-quantum process leads to signaling. The motivation is also to investigate whether tweaking quantum operations even slightly leads to violation of a physical principle like no-signaling, which is independent of quantum theory. Therefore, although the final results claimed in two manuscripts are similar, the perspectives are different. There is a probabilistic version of the distinguishing procedure that we consider in the current manuscript, which is absent in [22].

Acknowledgment.

References

[1] G.-C. Ghirardi, A. Rimini, and T. Weber, Lett. Nuovo Cimento Soc. Ital. Fis. **27**, 293 (1980).

[2] N. Gisin, Helv. Phys. Acta **62**, 363 (1989).

[3] L. P. Hughston, R. Jozsa, and W. K. Wootters Phys. Lett. A **183**, 14 (1993).

[4] N. Gisin, Phys. Lett. A **143**, 1 (1990).

[5] N. Gisin and M. Rigo, J. Phys. A **28**, 7375 (1995).

[6] M. Horodecki, R. Horodecki, A. Sen(De), and U. Sen, arXiv:quant-ph/0306044; Found. Phys. **35**, 2041 (2005).

[7] G. Svetlichny, quant-ph/0410036.

[8] A. Sen(De) and U. Sen, Phys. Rev. A **72**, 014304 (2005).

[9] M. Ferraro, Phys. Rev. A **73**, 034304 (2006).

[10] N. Gisin, Phys. Lett. A **242**, 1 (1998).

[11] D. Bruß, G. M. D'Ariano, C. Macchiavello, and M. F. Sacchi, Phys. Rev. A **62**, 062302 (2000).

[12] W.-Y. Hwang, Phys. Rev. A **71**, 062315 (2005); J. Bae, J.-W. Lee, J. Kim, and W.-Y. Hwang, Phys. Rev. A **78**, 022335 (2008); W.-Y. Hwang and J. Bae, J. Math. Phys. **51**, 022202 (2010); J. Bae, W.-Y. Hwang, and Y.-D. Han, Phys. Rev. Lett. **107**, 170403 (2011).

[13] A. Kent, Phys. Rev. Lett. **83**, 1447 (1999); A. Kent, J. Cryptolog. **18**, 313 (2005); T. Lunghi, J. Kaniewski, F. Bussières, R. Houlmann, M. Tomamichel, A. Kent, N. Gisin, S. Wehner, and H. Zbinden, Phys. Rev. Lett. **111**, 180504 (2013). See also G. M. D'Ariano, D. Kretschmann, D. Schlingemann, and R. F. Werner, Phys. Rev. A **76**, 032328 (2007); A. Peres and D. R. Terno, Rev. Mod. Phys. **76**, 93 (2004); H.-K. Lo and H. F. Chau, Phys. Rev. Lett. **78**, 3410 (1997); D. Mayers, Phys. Rev. Lett. **78**, 3414 (1997).

[14] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991); J. Barrett, L. Hardy, and A. Kent, Phys. Rev. Lett. **95**, 010503 (2005); A. Acín, N. Gisin, and L. Masanes, Phys. Rev. Lett. **97**, 120405 (2006).

[15] M. Pawłowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, and M. Żukowski, Nature **461**, 1101 (2009).

[16] P. W. Shor, in *Proceedings of 37th FOCS* (IEEE Computer Society, Washington, DC, 1996), p. 56; A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098, 1996; A. Steane, Proc. Roy. Soc. Lond. **A452**, 2551 (1996); B. M. Terhal, Rev. Mod. Phys. **87**, 307 (2015).

[17] C. K. Hong and L. Mandel, Phys. Rev. A **31**, 2409 (1985); L. Mandel and E. Wolf, Optical Coherence and Quantum Optics, Cambridge University Press (1995).

[18] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009).

[19] L.-M. Duan and G.-C. Guo, Phys. Lett. A **243**, 261 (1998); Phys. Rev. Lett. **80**, 4999 (1998); A. K. Pati, Phys. Rev. Lett. **83**, 2849 (1999); C.-W. Zhang, Z.-Y. Wang, C.-F. Li, and G.-C. Guo, Phys. Rev. A **61**, 062310 (2000); C.-W. Zhang, C.-F. Li, Z.-Y. Wang, and G.-C. Guo, Phys. Rev. A **62**, 042302 (2000); K. Azuma, J. Shimamura, M. Koashi, and N. Imoto, Phys. Rev. A **72**, 032335 (2005); L. Li and D. Qiu, Phys. Lett. A **362**, 143 (2007); H. Chen, D. Lu, B. Chong, G. Qin, X. Zhou, X. Peng, and J. Du, Phys. Rev. Lett. **106**, 180404 (2011). P. Rui, W. Zhang, Y. Liao, and Z. Zhang, arXiv:1603.07036 [quant-ph]; H. Liu and H. Fan, arXiv:1905.01878 [quant-ph].

[20] T. Mor, arXiv:quant-ph/9608005; T. Mor and P. Horodecki, arXiv:quant-ph/9906039; W.-L. Li, C.-F. Li, and G.-C. Guo, Phys. Rev. A **61**, 034301 (2000); S. Bandyopadhyay, Phys. Rev. A **62**, 012308 (2000); B.-S. Shi, Y.-K. Jiang, and G.-C. Guo, Phys. Lett. A **268**, 161 (2000); J.-C. Hao, C.-F. Li, and G.-C. Guo, Phys. Lett. A **278**, 113 (2000); S. Wu, S. M. Cohen, Y. Sun, and R. B. Griffiths, Phys. Rev. A **73**, 042311 (2006); Y. Feng, R. Duan, and Z. Ji, Phys. Rev. A **74**, 012310 (2006); B. Li, S.-h. Jiang, X.-B. Liang, X. Li-Jost, H. Fan, and S.-M. Fei, Phys. Rev. A **99**, 052343 (2019); C. Srivastava, A. Bera, A. Sen (De), and U. Sen, Phys. Rev. A **100**, 052304 (2019).

[21] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).

[22] A. K. Pati, arXiv:1904.05722 [physics.gen-ph].