scientific reports

Check for updates

OPEN

Quantum teleportation with one classical bit

Abhishek Parakh

Quantum teleportation allows one to transmit an arbitrary qubit from point A to point B using a pair of (pre-shared) entangled qubits and classical bits of information. The conventional protocol for teleportation uses two bits of classical information and assumes that the sender has access to only one copy of the arbitrary qubit to be sent. Here, we ask whether we can do better than two bits of classical information if the sender has access to multiple copies of the qubit to be teleported. We place no restrictions on the qubit states. Consequently, we propose a modified quantum teleportation protocol that allows Alice to reset the state of the entangled pair to its initial state using only local operations. As a result, the proposed teleportation protocol requires the transmission of only one classical bit with a probability greater than one-half. This has implications for efficient quantum communications and the security of quantum cryptographic protocols based on quantum entanglement.

Quantum teleportation[1,2] is a strikingly curious quantum phenomenon with myriads of applications ranging from secure quantum communication to distributed quantum computing[3–7]. First presented by Bennett et al.[1], quantum teleportation allows one to recreate an arbitrary qubit from just two bits of classical information. The precondition is that the two communicating parties share an entangled pair of qubits. Entanglement, essentially, transmits the raw values of amplitudes present in the arbitrary qubit and the classical bits provide a final "correction" to these values. Quantum teleportation has proven to be an invaluable tool in quantum information science[8–10]. Quantum teleportation enables the development of quantum repeaters[3,11], a pivotal technology for the establishment of quantum communication networks[12], and in general the framework of quantum Internet. Quantum teleportation has been implemented in lab setting using a number of different resources[13,14]. Lastly, a number of cryptographic protocols use shared entangled qubits and operations equivalent to teleportation to produce random numbers and encryption keys[15].

It is known that, given a pre-shared Bell pair, the teleportation of an unknown qubit, requires the transmission of two classical bits[1]. More generally, the teleportation of an N-state requires $2log_2N$ classical bits[16]. This, however, assumes that the sender has access to only one copy of the arbitrary unknown qubit that she is teleporting. Kak investigated the minimum number of classical bits required for teleportation[17]. In turn, he proposed three variations on Bennett's protocol that required fewer than two qubits. Two of these variations, however, use a non-traditional setup where the entangled qubits are not pre-shared between the communicating parties but transmitted along with the classical bits of information. This change in the setup can be looked upon as an encryption system where the classical bit of information acts as the encryption key for the qubit and multipath routing can be used for their transmission. From the viewpoint of teleportation, nevertheless, if the qubits are to be transmitted along with classical bits, then one could transmit the arbitrary qubit directly at that time without the need to resorting to teleportation. However, it does point out to the possibility of some "non-standard" setting of quantum teleportation having lower classical cost of communication. One such "non-standard" setting was investigated by Pati[18] where the teleported qubit arose from a specific portion of the Bloch sphere leading to a one-bit classical communication cost. This was further investigated by Lo as remote state preparation[19].

In this paper, we too consider a somewhat non-standard setting but in terms of resources. Like the traditional teleportation protocol, we assume that the communicating parties pre-share entangled qubits. However, we consider the case when the sender has more than one copy of an (unknown) arbitrary qubit $|\phi\rangle = a|0\rangle + b|1\rangle$, $|a|^2 + |b|^2 = 1$. We do not place any other restrictions on the qubits. Such a possibility has not been investigated before. Our result shows that under such as setting, we can do better than two classical bits of communication. A sender may have multiple copies of the qubit to be teleported in many practical situations where the unknown qubit is either the result of a periodic or on-demand natural process or output of a quantum algorithm. One may need to send this (unmeasured) output to the receiver for further processing. We show that the teleportation of such a qubit requires the transmission of only one classical bit with a probability greater than one-half. In order to do so, we propose a *reset* procedure that allows for the recreation of the original shared Bell state using only local operations at the sender's end and no consumption of resources at receiver's end. In the proposed reset procedure,

University of Nebraska, Omaha, NE 68116, USA. email: aparakh@unomaha.edu

as with conventional teleportation protocol, we begin with maximally entangled qubits. At the first stage of the protocol, if this maximally entangled qubit enters into a desired state we move on to the second stage of the protocol. If, on the other hand, the entangled part ends up in an undesired state we reset it back to the original state using only local operations at the sender's end. The cost of doing so is one copy of the arbitrary qubit, $|\phi\rangle$.

Furthermore, if the amplitudes a and b are known and/or the qubit, $|\phi\rangle$, generated on demand, then the *reset* operation may be attempted many times over.

The result presented in this paper, we believe, represents a fundamental advance in the classical burden of teleportation, since it was proposed by Bennett et al.[1], because we do not restrict the states of the qubit and allow the parties to pre-share entangled pairs as in the traditional setting. The presented result also has widespread consequences for quantum cryptographic protocols that use entangled pairs and assume a symmetric power between communicating parties.

Result

It is useful to think of the conventional teleportation protocol as a two stage system[19]. We start with a shared Bell pair $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$ between sender, Alice, and receiver, Bob. The first stage of the teleportation protocol introduces the amplitudes a and b into the entangled pair. However, the locations of the amplitudes maybe flipped and is corrected with the application of Pauli X gate by both the sender and the receiver. This requires the transmission of 1-bit of classical information to Bob. In the second stage of the protocol, Alice terminates the entanglement by measuring her qubit of the Bell pair in the Hadamard basis. This introduces another undesirable error into the state of the qubit that Bob holds corresponding to the Pauli Z gate. This is corrected by the transmission of another classical bit of information to Bob.

To be more precise, in Bennett's protocol[1] at the end of the first stage the two parties share the state $a|00\rangle + b|11\rangle$ or $b|00\rangle + a|11\rangle$. The first of these states is desirable and the second one is converted to the first one with the application of a bi-local unitary transformation $|0\rangle \rightarrow |1\rangle$. This requires one bit to be sent to Bob. In the second stage of the protocol, Bob ends up with $a|0\rangle + b|1\rangle$ or $a|0\rangle - b|1\rangle$. The correction of the last state requires the other bit of information to be sent to Bob. In the end Bob is left with $a|0\rangle + b|1\rangle$, which corresponds to the unknown state $|\phi\rangle$ that Alice wanted to teleport.

In this paper, we ask a simple question: if Alice ends up in the undesired state at the end of the first stage, i.e. $b|00\rangle + a|11\rangle$, can she using only local transformations reset the state of the shared entanglement to the original state $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$? If so, she can reattempt the teleportation protocol.

Resetting the entangled state. In order to reset the entangled state, Alice introduces an ancillary qubit $|\theta\rangle = c|0\rangle + d|1\rangle$ into the system. It will become apparent through the following discussion that $|\theta\rangle = |\phi\rangle$. The resulting system state is given by $|\psi\rangle$,

$$\begin{aligned} |\psi\rangle &= |\theta\rangle(a|1_A 1_B\rangle + b|0_A 0_B\rangle) \\ &= (c|0_l\rangle + d|1_l\rangle)(a|1_A 1_B\rangle + b|0_A 0_B\rangle) \\ &= ca|0_l 1_A 1_B\rangle + cb|0_l 0_A 0_B\rangle + da|1_l 1_A 1_B\rangle + db|1_l 0_A 0_B\rangle \end{aligned} \tag{1}$$

Qubits with subscripts l and A are with Alice and the qubit denoted by subscript B is with Bob. Now, Alice applies CNOT with the ancillary qubit (the first qubit) as the control qubit and second qubit as the target qubit. The state then becomes,

$$\begin{aligned} |\psi\rangle &= ca|0_l 1_A 1_B\rangle + cb|0_l 0_A 0_B\rangle + da|1_l 0_A 1_B\rangle + db|1_l 1_A 0_B\rangle \\ &= |1_A\rangle(ca|0_l 1_B\rangle + db|1_l 0_B\rangle) + |0_A\rangle(cb|0_l 0_B\rangle + da|1_l 1_B\rangle) \end{aligned} \tag{2}$$

In Eq. (2) above, we have removed the second qubit as the common qubit for simplification of the expression. We see that $|0_A\rangle(cb|0_l 0_B\rangle + da|1_l 1_B\rangle)$ is closest to the desired state $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$. If we set $c = a$ and $d = b$ then we get,

$$|\psi\rangle = |1_A\rangle(aa|0_l 1_B\rangle + bb|1_l 0_B\rangle) + |0_A\rangle(ab|0_l 0_B\rangle + ba|1_l 1_B\rangle) \tag{3}$$

Alice now measures the second qubit.

She will see $|0\rangle$ with probability $2|ab|^2$ and the shared entangled qubits end up in state $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$. *This constitutes a successful reset by Alice*. Note that, setting $c = a$ and $d = b$ means that Alice is simply using a copy of the original qubit $|\phi\rangle$ for the reset operation and does not need to create any new special ancillary qubits. Once a reset to the original Bell state is achieved, Alice reinitiates the teleportation protocol using a fresh copy of $|\phi\rangle$.

On the other hand, Alice's measurement results in $|1\rangle$ with probability $|a^2|^2 + |b^2|^2$. This takes the system to the state $\frac{a^2|01\rangle+b^2|10\rangle}{\sqrt{|a^2|^2+|b^2|^2}}$. Alice can apply the X gate to her qubit and reattempt the reset operation with $\frac{a^2}{\sqrt{|a^2|^2+|b^2|^2}}$ and $\frac{b^2}{\sqrt{|a^2|^2+|b^2|^2}}$ as the new a and b values, respectively.

At this point, Alice has consumed two copies of $|\phi\rangle$. One during stage one of the teleportation protocol and second as the ancillary qubit introduced into the system during the reset operation. Figure 1 shows the branches that a teleportation attempt with the proposed reset procedure can follow.

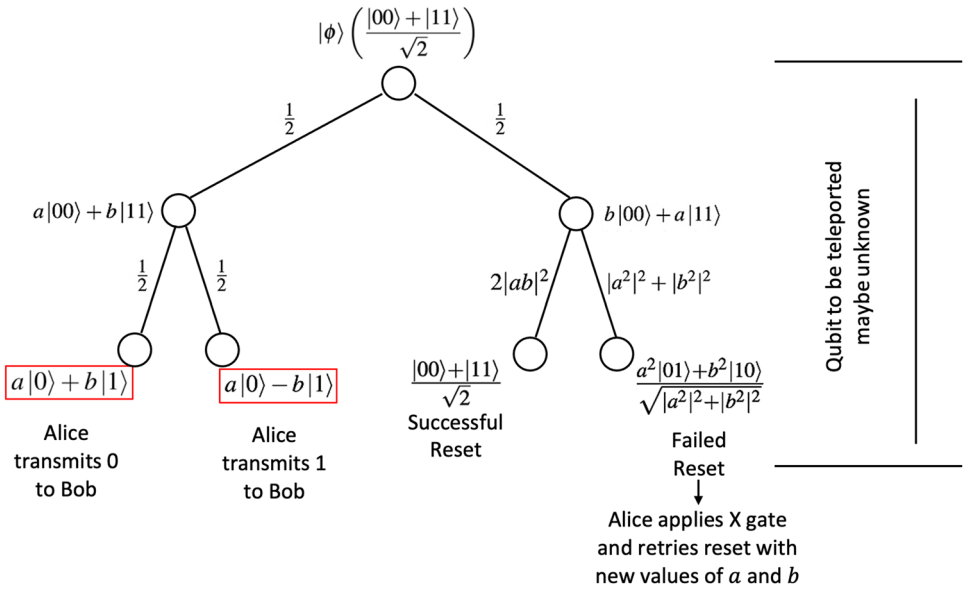

Figure 1. Decision tree at Alice's end for teleportation with the proposed reset operation. Probabilities are shown along the arms between the nodes. States in the red boxes reside with Bob.

Discussion

The probability of success of the reset attempts vary with the values of amplitudes a and b, in the state $|\phi\rangle$, and is given by $2|ab|^2$ for the first reset attempt. Since, $|ab|^2 = |a|^2|b|^2 = |a|^2(1-|a|^2) = |a|^2 - |a|^4$ and $0 \leq |a|^2 \leq 1$, we get $|ab|^2 \leq \frac{1}{4}$ and $2|ab|^2 \leq \frac{1}{2}$.

For example, when $a = \frac{i}{\sqrt{2}}$ and $b = \frac{1}{2} + \frac{i}{2}$, the probability that the first reset attempt will succeed is $\frac{1}{2}$. After a successful reset, Alice makes a second attempt to teleport the qubit. The probability that entangled qubits will collapse into the desirable state $(a|00\rangle + b|11\rangle)$ is again $\frac{1}{2}$. Therefore, with probability $\frac{1}{2} + \frac{1}{4}$ Alice would transmit just one bit for teleportation but must have at least three copies of $|\phi\rangle$ at her disposal.

Remarkably, the qubit $|\phi\rangle$ remains unknown and arbitrary.

Consequently, in general, considering only the first reset attempt and an unknown qubit $|\phi\rangle$ the probability of ending up in the desired state $(a|00\rangle + b|11\rangle)$, that is a successful teleportation with only one-classical bit, is $\frac{1}{2} + \frac{1}{2} \cdot 2|ab|^2 = \frac{1}{2} + |ab|^2$. Note, this probability is always set to $\frac{1}{2}$ in Bennett et al.'s quantum teleportation[1] protocol which always requires two bits of information to be transmitted.

Alice, however, does require the values of a and b for the reset attempts beyond the first one; in the case of a reset failure. This latter case is useful when the precision required for classical representation of the a and b values exceeds the available bandwidth or resources available on the classical channel. In other words, if the values of a and b are known, Alice can pursue the reset attempts until it succeeds. Note that once a reset attempt succeeds, the probability that we will end up in the desired entangled state is again $\frac{1}{2}$. Therefore, the expected number of attempts, given a successful reset, is 2.

The reset procedure presented above, when successful, reduces the teleportation protocol to one stage protocol under the standard setting of pre-shared Bell states. Furthermore, Alice knows at each stage whether the reset has succeeded or not. In the worst case, if the values of a and b are not known and the reset fails, she can abandon that particular pair of entangled qubits and use another. The computational burden of teleportation with reset can then be stated as,

$$H(T) = \left[\left(\frac{1}{2} + |ab|^2\right)(1) + \left(\frac{1}{2} - |ab|^2\right)(2)\right] \text{ bits} \tag{4}$$

It is easy to see that $1.25 \leq H(T) \leq 1.5$ depending on the values of a and b. For comparison, one of the protocols by Kak[17] reduces the computational burden to 1.5 bits when the Bell states are pre-shared. The cost of reducing the computational burden to 1.25 bits, therefore, is the expenditure of extra copies of the unknown qubit $|\phi\rangle$. In other words, the probability $\frac{1}{2} + |ab|^2$ only represents the average case. Given that the proposed protocol is probabilistic in nature and if Alice has several qubits to teleport, she may end up with a situation where all her reset attempts may succeed resulting in a 1 bit per qubit for teleportation even for a completely arbitrary unknown qubit!

One may argue that even in Bennett's original teleportation protocol[1], Alice and Bob may agree on a scheme such as the follows: if stage one of the protocol succeeds in creating $a|00\rangle + b|11\rangle$ then they will proceed with stage two and if stage one results in $a|11\rangle + b|00\rangle$, they will abandon the entangled pair. Such a modification would also be probabilistic and result in 1 bit per qubit for teleportation. However, we point out that the probability of 1 bit per qubit in such a modified Bennett's protocol would be stuck at $\frac{1}{2}$. Whereas, our reset procedure allows this probability to be $\frac{1}{2} + |ab|^2$ which is greater than $\frac{1}{2}$ for all practical purposes.

The probability of success for the reset operation at every attempt changes with the amplitudes a and b and is given by a recursive relationship. If $R_0, R_1, R_2, \ldots$ represent successive reset attempts then the probability of success of each reset is given by,

$$\begin{aligned} P(R_0) &= 2|ab|^2 \\ P(R_1) &= 2|a_1 b_1|^2 \text{ where } a_1 = \frac{a^2}{\sqrt{|a^2|^2 + |b^2|^2}} \text{ and } b_1 = \frac{b^2}{\sqrt{|a^2|^2 + |b^2|^2}} \\ P(R_2) &= 2|a_2 b_2|^2 \text{ where } a_2 = \frac{a_1^2}{\sqrt{|a_1^2|^2 + |b_1^2|^2}} \text{ and } b_2 = \frac{b_1^2}{\sqrt{|a_1^2|^2 + |b_1^2|^2}} \\ &\text{and so on.} \end{aligned} \tag{5}$$

Therefore, the probability that Alice would *need* three reset attempts is given by $(1 - P(R_0))(1 - P(R_1))P(R_2)$. For a state such as $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ this would be $(1 - \frac{1}{2})(1 - \frac{1}{2})(\frac{1}{2}) = \frac{1}{8}$.

An important implication of Eq. (4) is that when $|ab|^2 > 0$ there is a non-zero probability of a successful reset. The equality, $|ab|^2 = 0$, holds only when one of the amplitudes a or $b = 0$, a corner case. As a result, the above protocol breaks the symmetry between the four cases of the conventional teleportation protocol[1]. More precisely, in the conventional teleportation protocol, there is an equal probability for Bob to end up in any of the four states: $|\phi_0\rangle = a|0\rangle + b|1\rangle, |\phi_1\rangle = a|0\rangle - b|1\rangle, |\phi_2\rangle = b|0\rangle + a|1\rangle$, and $|\phi_3\rangle = b|0\rangle - a|1\rangle$. Consequently, two classical bits were needed for teleportation. However, with the proposed reset operation the relationship between the probabilities of the states that Bob sees is given by,

$$P(|\phi_0\rangle) + P(|\phi_1\rangle) > P(|\phi_2\rangle) + P(|\phi_3\rangle) \tag{6}$$

For a moment only consider the first stage of the teleportation protocol and the reset operation. Assume that Alice has not transmitted any information to Bob. We see that, the reset operation also implies that when $a, b \neq 0$, Alice can unilaterally force the shared entanglement, $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$ to be converted to $a|00\rangle + b|11\rangle$ with a probability higher than $\frac{1}{2}$ and no communication with Bob. If the qubit $|\phi\rangle$ is deliberately constructed by Alice and the information Alice wants to transmit is encoded in the values of a and b rather than the phase difference between them, then Alice has successfully induced a bias in Bob's qubit.

The ability of one party to, unilaterally, induce a bias in a shared entangled pair gives a party wanting to cheat, in a cryptographic protocol, an advantage. For example, several quantum key agreement protocols have been proposed in literature[20–25]. These protocols are designed such that both the communicating parties make equal contribution to the final agreed key. This is in contrast to traditional quantum key distribution protocols such as BB84 where one party determines the entire key and securely distributes it to the other party. If the quantum key agreement protocol is based on entanglement then one of the cheating parties can induce a bias in the final key stream by introducing an appropriate $|\phi\rangle$ in the system. The simplest example of a weak quantum key agreement protocol is the E91 protocol where both parties make random measurements on maximally entangled pairs of qubits. If these maximally entangled pairs are distributed by a central authority then Alice (cheating party) can introduce $|\phi\rangle = a|0\rangle + b|1\rangle$ such that $|a|^2 \neq |b|^2$ resulting in a biased measurement result, at Bob's end, of her own choosing. Therefore, the asymmetry caused by the reset operation gives Alice more power than Bob and is devastating for cryptographic protocols that use entanglement and rely on the powers of the communicating parties being symmetric for security.

In this paper, we have only considered the ideal case where the shared entangled pair is maximally entangled. Investigation into how the reset procedure would proceed in the case of non-maximally entangled states, mixed states, non-ideal measurements and channel errors are left as future work. Entanglement distillation[26] could be used to mitigate the effects of these non-ideal cases.

Received: 21 October 2021; Accepted: 7 February 2022
Published online: 01 March 2022

References

1. Bennett, C. H. *et al.* Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.* **70**, 1895–1899. https://doi.org/10.1103/PhysRevLett.70.1895 (1993).
2. Gauthier, D. J. *Superluminal Communication in Quantum Mechanics* 766–769 (Springer, 2009). https://doi.org/10.1007/978-3-540-70626-7_217.
3. Briegel, H.-J., Dür, W., Cirac, J. I. & Zoller, P. Quantum repeaters: The role of imperfect local operations in quantum communication. *Phys. Rev. Lett.* **81**, 5932–5935. https://doi.org/10.1103/PhysRevLett.81.5932 (1998).
4. Gottesman, D. & Chuang, I. L. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature* **402**, 390–393 (1999).
5. Raussendorf, R. & Briegel, H. J. A one-way quantum computer. *Phys. Rev. Lett.* **86**, 5188–5191. https://doi.org/10.1103/PhysRevLett.86.5188 (2001).
6. Kimble, H. J. The quantum internet. *Nature* **453**, 1023–1030 (2008).
7. Gottesman, D. & Chuang, I. L. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature* **402**, 390–393. https://doi.org/10.1038/46503 (1999).
8. Weedbrook, C. *et al.* Gaussian quantum information. *Rev. Mod. Phys.* **84**, 621–669. https://doi.org/10.1103/RevModPhys.84.621 (2012).
9. Braunstein, S. L. & van Loock, P. Quantum information with continuous variables. *Rev. Mod. Phys.* **77**, 513–577. https://doi.org/10.1103/RevModPhys.77.513 (2005).
10. Wilde, M. M. *Quantum Information Theory* 2nd edn. (Cambridge University Press, 2017).

11. Ghalaii, M. & Pirandola, S. Capacity-approaching quantum repeaters for quantum communications. *Phys. Rev. A* **102**, 062412. https://doi.org/10.1103/PhysRevA.102.062412 (2020).
12. Stephen Binkley, J., Carl Williams, S. J. & Tahan, C. A coordinated approach to quantum networking research. https://www.quantum.gov/wp-content/uploads/2021/01/A-Coordinated-Approach-to-Quantum-Networking.pdf (2021).
13. Llewellyn, D. *et al.* Chip-to-chip quantum teleportation and multi-photon entanglement in silicon. *Nat. Phys.* **16**, 148–153. https://doi.org/10.1038/s41567-019-0727-x (2020).
14. Khatri, S., Brady, A. J., Desporte, R. A., Bart, M. P. & Dowling, J. P. Spooky action at a global distance: Analysis of space-based entanglement distribution for the quantum internet. *npj Quantum Inf.* **7**, 4. https://doi.org/10.1038/s41534-020-00327-5 (2021).
15. Shenoy-Hejamadi, A., Pathak, A. & Radhakrishna, S. Quantum cryptography: Key distribution and beyond. *Quanta* **6**, 1–47 (2017).
16. Chau, H. F. & Lo, H.-K. How much does it cost to teleport? In *4th Workshop on Physics and Computation (PhysComp 96)* (1996). arXiv:quant-ph/9605025.
17. Kak, S. C. Teleportation protocols requiring only one classical bit. *arXiv* (2003). arXiv:quant-ph/0305085.
18. Pati, A. K. Minimum classical bit for remote preparation and measurement of a qubit. *Phys. Rev. A* **63**, 014302. https://doi.org/10.1103/PhysRevA.63.014302 (2000).
19. Lo, H.-K. Classical-communication cost in distributed quantum-information processing: A generalization of quantum-communication complexity. *Phys. Rev. A* **62**, 012313. https://doi.org/10.1103/PhysRevA.62.012313 (2000).
20. Zhou, N. Quantum key agreement protocol. *Electron. Lett.* **40**, 1149–1150 (2004).
21. Cao, H. & Ma, W. Multiparty quantum key agreement based on quantum search algorithm. *Sci. Rep.* **7**, 45046 (2017).
22. Yin, X., Ma, W. & Liu, W. Y. Three-party quantum key agreement with two-photon entanglement. *Int. J. Theor. Phys.* **52**, 3915–3921 (2013).
23. Huang, W.-C., Yang, Y.-K., Jiang, D. & Chen, L. Efficient travelling-mode quantum key agreement against participant's attacks. *Sci. Rep.* **9**, 16421 (2019).
24. Chong, S.-K., Tsai, C.-W. & Hwang, T. Improvement on "quantum key agreement protocol with maximally entangled states". *Int. J. Theor. Phys.* **50**, 1793–1802 (2011).
25. Shi, R.-H. & Zhong, H. Multi-party quantum key agreement with bell states and bell measurements. *Quantum Inf. Process.* **12**, 921–932 (2013).
26. Bennett, C. H., Bernstein, H. J., Popescu, S. & Schumacher, B. Concentrating partial entanglement by local operations. *Phys. Rev. A* **53**, 2046–2052. https://doi.org/10.1103/PhysRevA.53.2046 (1996).

Author contributions
I am the sole author of the paper.

Competing interests
The authors declare no competing interests.

Additional information
Correspondence and requests for materials should be addressed to A.P.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.