Remote control of restricted sets of operations: Teleportation of angles

S. F. Huelga,[1] M. B. Plenio,[2] and J. A. Vaccaro[1]
[1]*Department of Physical Sciences, Division of Physics and Astronomy, University of Hertfordshire, Hatfield, Herts AL10 9AB, United Kingdom*
[2]*QOLS, Blackett Laboratory, Imperial College of Science, Technology and Medicine, London, SW7 2BW, United Kingdom*
(Received 28 August 2001; published 2 April 2002)

We study the remote implementation of a unitary transformation on the state of a qubit. We show the existence of nontrivial protocols (i.e., using less resources than bidirectional state teleportation) that allow the perfect remote implementation of certain continuous sets of quantum operations. We prove that, up to a local change of basis, only two subsets exist that can be implemented remotely with a nontrivial protocol: Arbitrary rotations around a fixed direction $\vec{n}$ and a π rotation about an arbitrary direction lying in a plane orthogonal to $\vec{n}$. The former operations effectively constitute the teleportation of arbitrary angles. The overall classical information and distributed entanglement cost required for the remote implementation depends on whether it is known, *a priori*, in which of the two teleportable subsets the transformation belongs. If it is known, the optimal protocol consumes one *e*-bit of entanglement and one *c*-bit in each direction. If it is not known in which subset the transformation belongs, two *e*-bits of entanglement need to be consumed and the classical channel becomes asymmetric with two *c*-bits being conveyed from Alice to Bob but only one from Bob to Alice.

DOI: 10.1103/PhysRevA.65.042316 PACS number(s): 03.67.−a, 03.65.Ta

I. INTRODUCTION

Using entanglement as a resource is a common feature of many tasks in quantum-information processing [1]. A canonical example of entanglement-assisted processes is provided by quantum-state teleportation [2], where an arbitrary qubit state can be transferred with perfect fidelity among distant parties with the sole use of two classical bits (*c*-bits) and the consumption of a distributed maximally entangled state, i.e., one *e*-bit of shared entanglement. Recently we have addressed a related problem where the aim is to *teleport* across distant parties not a quantum state but a *quantum operation* [3]. By this we mean the following. Alice and Bob are set in remote locations and one of the parties, say Alice, is given a black box with the ability of performing a very large set of unitary transformations U on a qubit. The requirement of the set of allowed transformations being very large is imposed with the aim of excluding, by construction, the possibility of teleporting the full black box to Bob, which would exhaust entanglement resources very quickly. We will say that the operation U has been teleported to Bob, or equivalently, it has been remotely implemented if, for any qubit state Bob may hold, a protocol involving only local quantum operations and exchange of classical communication (LQCC) can yield a final global state where Bob holds the state transformed by the operation U disentangled from any other system (see below for a quantitative formulation).

Our previous results show that if we want the transformation U to be an arbitrary element of the group SU(2), then Bob's state must be teleported to Alice's site where it is acted upon by U and then the transformed state is teleported back to Bob. Essentially Alice's black box can only control Bob's state if the state is *local* to the box. This is hardly *remote* control. We can illustrate this problem in a classical remote-control analogy where an operation at Alice's armchair is required to control, via some device, the tuning circuit in Bob's television set. The requirement that Bob's state be teleported to Alice's site is equivalent, in this analogy, to requiring the tuning circuit to be brought to Alice for the channel to be changed. The culprit of this result is linearity. Our *no-remote-control-theorem*, therefore, belongs to the family of no-go results imposed by the linear structure of quantum mechanics and exemplified, for instance, by the non-cloning theorem [4].

However, the no-cloning theorem only forbids the cloning of *arbitrary* unknown states; cloning is possible for restricted classes containing mutually orthogonal states. What happens if the requirement of being able to implement *any* U is relaxed? The bidirectional quantum-state teleportation (BQST) of every state, which is needed for implementing the operation of Alice's black box on Bob's qubit, consumes two *e*-bits of shared entanglement and two classical bits in either direction (Bob to Alice and Alice to Bob). Can we find families of operators that can be implemented consuming less overall resources than the BQST of every state? We should stress that we are interested here in exploiting entanglement, therefore any strategy that attempts the local reconstruction of U [5] is excluded from our valid protocols. (Indeed, in our classical analogy, the local reconstruction of U at Bob's site represents Alice moving to the television set to change the channel; this is not remote control.) In addition, we want to keep to a minimum the available *a priori* information about U. Note, in particular, that if both the form of U and Bob's initial state are completely known, the posed problem reduces to remote-state preparation [6]. Finally, we want the procedure to work with perfect efficiency. Imperfect storage of quantum operations has been recently discussed by Vidal *et al.* [7].

We will show that there are indeed just two restricted classes of operations that can be implemented remotely using less overall resources than BQST (up to a local change of basis). These are arbitrary rotations around a fixed direction

$\vec{n}$ and π rotation about an arbitrary direction lying in a plane orthogonal to $\vec{n}$. As a result, once the direction $\vec{n}$ is fixed, Alice can effectively teleport an arbitrary angle to Bob. We have organized the paper into seven further sections. Section II revises the necessary resources for achieving the remote implementation of an arbitrary U. As opposed to the completely general scenario analyzed in [3], we concentrate here on the case of a macroscopic black box, and therefore we exclude teleportation of the controlling device as a possible strategy. This will allow us to set a new bound for the amount of classical information that Bob needs to transfer to Alice. In Sec. III, a LQCC protocol exhausting these resources and achieving the maximum probability of success allowed for arbitrary U is constructed. Remarkably, two possible sets of transformations could be implemented accurately with this procedure, as discussed in Sec. IV. A geometrical picture of why it is possible to engineer a final correction step in these cases is presented in Sec. V. The uniqueness of the subsets is proven in Sec. VI, the technical bulk of this paper. Section VII deals with the resources trade-off when some *a priori* information about the functional form of the transformation U is provided. The final Sec. VIII summarizes the results and proposes an experimental scenario where the teleportation of *angles* could be demonstrated.

II. REMOTE IMPLEMENTATION OF AN ARBITRARY *U*: NECESSARY RESOURCES

Assuming the black box to be a classical system, we are seeking a protocol with the following structure [3]:

$$G_2 U G_1(|\chi\rangle_{aAB}\otimes|\psi\rangle_b)=|\Phi(\chi)\rangle_{aAB}\otimes U|\psi\rangle_b, \qquad (1)$$

where certain fixed operations G_1 and G_2 are performed, respectively, prior to and following the action of the arbitrary U on a qubit a on Alice's side. The fact that the operation G_1 has to be nontrivial follows from the results of Nielsen and Chuang when analyzing universal programmable gates [8]. We assume that Alice and Bob share initially some entanglement, represented by the joint state $|\chi\rangle_{aAB}$. The purpose of the protocol is to end up with Bob holding a qubit in the transformed state $U|\psi\rangle_b$, for any initial state $|\psi\rangle_b$ and with perfect efficiency. Note that the final distributed state involving the remaining subsystems aAB is independent of both U and $|\psi\rangle_b$ [3]. As in [3], it will convenient to use a nonlocal unitary representation of the transformation, with G_1 and G_2 being unitary operators acting on possibly all subsystems. Their dimensionality will depend on the specific protocol. For instance, a possible solution, while, in principle, not necessarily optimal, corresponds to each G_i being a state teleportation process. In the following we will establish lower bounds on the amount of classical communication and the amount of entanglement required for the teleportation of an arbitrary unitary transformation. Our argument employs the principle that entanglement cannot be increased under LQCC to show that two *e*-bits are necessary and it uses the impossibility of superluminal communication to demonstrate that two classical bits have to be sent from Alice to Bob and at least one bit has to be transferred from Bob to Alice.

Assume that we could teleport any arbitrary operation U from Alice to Bob. Therefore, a universal protocol involving operations G_1 and G_2 would yield the outcome $|\Phi(\chi)\rangle_{aAB}\otimes U|\psi\rangle_b$, independently of the actual form of U. It is easy to show that then it would also be possible to implement remotely an arbitrary *controlled*-U gate. By this we mean that the remote implementation of U is performed conditionally on the state of a certain control qubit c, so that the action of the black box is to apply the identity if the control qubit is state $|0\rangle_c$ and to apply U when the control bit is state $|1\rangle_c$. That is, Eq. (1) is replaced by

$$G_2 U_c G_1(|c\rangle_c\otimes|\chi\rangle_{aAB}\otimes|\psi\rangle_b)=|\Phi(\chi)\rangle_{aAB}\otimes(c_0|0\rangle_c\otimes\mathbb{1}|\psi\rangle_b + c_1|1\rangle_c\otimes U|\psi\rangle_b), \qquad (2)$$

where

$$U_c=|0\rangle_{cc}\langle 0|\otimes\mathbb{1}+|1\rangle_{cc}\langle 1|\otimes U, \qquad (3)$$

and $|c\rangle_c=c_0|0\rangle_c+c_1|1\rangle_c$ is an arbitrary state of the control qubit, which, without loss of generality, can be assumed to be part of the black box and therefore unaffected by the action of the operations G_i, $(i=1,2)$. Let us decompose the global state after the application of G_1 as follows:

$$|c\rangle_c\otimes G_1(|\chi\rangle_{aAB}\otimes|\psi\rangle_b)=(c_0|0\rangle_c+c_1|1\rangle_c)\otimes(|0\rangle_a|\xi_0\rangle_{ABb} + |1\rangle_a|\xi_1\rangle_{ABb}), \qquad (4)$$

where the, possibly distributed, states $|\xi_i\rangle_{ABb}$ are neither necessarily orthogonal not normalized. The action of U_c brings this state onto

$$\begin{aligned} U_c(c_0|0\rangle_c+c_1|1\rangle_c)\otimes(|0\rangle_a|\xi_0\rangle_{ABb}+|1\rangle_a|\xi_1\rangle_{ABb}) &= c_0|0\rangle_c(\mathbb{1}|0\rangle_a|\xi_0\rangle_{ABb}+\mathbb{1}|1\rangle_a|\xi_1\rangle_{ABb}) \\ &\quad + c_1|1\rangle_c(U|0\rangle_a|\xi_0\rangle_{ABb}+U|1\rangle_a|\xi_1\rangle_{ABb}). \end{aligned} \qquad (5)$$

Now, the subsequent action of the operation G_2 gives the transformation law Eq. (2) provided that Eq. (1) holds for every qubit transformation U.

A simple controlled-U operation is not yet sufficient for our argument but we have to introduce a slightly more involved gate. Assume now that we have two control qubits, c and c', on Alice's side and consider again Bob's qubit as the target. We will apply a particular operation, which we call a controlled Pauli gate (CP gate). This gate applies one of the four Pauli spin operators on the target qubit depending on the state of the two control qubits and can be written as

$$U_{CP}=|00\rangle\langle 00|\otimes\mathbb{1}+|01\rangle\langle 01|\otimes\sigma_x+|10\rangle \times\langle 10|\otimes\sigma_y+|11\rangle\langle 11|\otimes\sigma_z, \qquad (6)$$

where we have omitted the subscripts cc' to make the notation lighter. Given that we are assuming that Alice can teleport any unitary operation to Bob, we can therefore implement a CP gate between Alice and Bob with Alice acting as the control. We will demonstrate that the CP gate can be used to establish, starting from a product state between Alice and Bob, a state that contains two shared *e*-bits. To this end, assume that Bob holds two particles in the maximally entangled state $|\phi^{+}\rangle_B = |00\rangle_B + |11\rangle_B$ and that Alice holds her two control particles in the state $|00\rangle + |01\rangle + |10\rangle + |11\rangle$. The result of the CP operation is

$$\begin{aligned} U_{CP}(|00\rangle+|01\rangle+|10\rangle+|11\rangle)_{cc'} \otimes (|00\rangle+|11\rangle)_B \\ = |00\rangle_{cc'}(|00\rangle+|11\rangle)_B + |01\rangle_{cc'}(|01\rangle+|10\rangle)_B \\ + i|10\rangle_{cc'}(|01\rangle-|10\rangle)_B + |11\rangle_{cc'}(|00\rangle-|11\rangle)_B, \end{aligned} \tag{7}$$

which contains two *e*-bits of entanglement shared between Alice and Bob. As entanglement does not increase under LQCC, and the teleportation of U has been done using only LQCC, we conclude that the teleportation of a general U requires at least two *e*-bits.

Now let us proceed to show that the teleportation of an unknown U also requires the transmission of two classical bits from Alice to Bob. The idea of the proof is to show that for each application of the CP gate, Alice can transmit two classical bits of information. This implies that the implementation of the CP gate requires two bits of classical communication between Alice and Bob as otherwise we would be able to establish a superluminal channel between the two parties following an argument analogous to that presented in the original teleportation paper [2]. Imagine the following protocol. Alice encodes four messages in binary notation as $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ in two of her control qubits. Assume that Bob holds two particles in state $|\phi^{+}\rangle_B = |00\rangle + |11\rangle$ as before. The CP gate is applied between Alice's particle and the first of Bob's particles (using the teleportation procedure of an unknown operation). Depending on the state in which Alice has prepared her two control qubits, Bob will subsequently hold one of the four Bell states, which are mutually orthogonal. Therefore he is able to infer Alice's message and two classical bits have been transmitted. As a result, the implementation of the teleportation of an unknown U has to include the transmission of two bits of classical information from Alice to Bob. Consider now the case when the first of Alice's qubits is kept in a fixed state, for instance, in state $|0\rangle$. The implementation of a controlled Pauli operation is now equivalent to implementing a controlled-NOT gate between Alice's second qubit and Bob's qubit [9]. When Alice prepares the state $|+\rangle_c = |0\rangle + |1\rangle$, the action of a controlled-NOT gate with Bob's qubit being in either state $|+\rangle_B$ or in state $|-\rangle_B$ is given by

$$\begin{aligned} |+\rangle_c|+\rangle_B \mapsto |+\rangle_c|+\rangle_B, \\ |+\rangle_c|-\rangle_B \mapsto |-\rangle_c|-\rangle_B. \end{aligned} \tag{8}$$

Therefore, this operation allows Bob to transmit one bit of information to Alice and, as a consequence, the teleportation of U requires at least one bit of communication from Bob to Alice. Summarizing, the physical principles of nonincrease of entanglement under LQCC and the impossibility of superluminal communication allow us to establish lower bounds in the resources required for teleporting an unknown quantum operation on a qubit. At least two *e*-bits of entanglement have to be consumed. In addition, this quantum channel has to be supplemented by a *two-way* classical communication channel, which, in principle, could be nonsymmetric. While consistency with causality requires two classical bits being transmitted from Alice to Bob, the lower bound for the amount of classical information transmitted from Bob to Alice has been found to be one bit. Note that the arguments used in [3] did not yield a nonzero lower bound for the amount of classical information conveyed from Bob to Alice. This situation would correspond to a strategy where the teleportation of the whole controlling device is a possible solution. Obviously, in this case, Bob does not need to communicate with Alice. One of the consequences of the main result in [3] is that the transmission of just one classical bit from Bob to Alice is not sufficient if the protocol is meant to work for an arbitrary U. We showed that each operation G_i necessarily involves a state transfer between the remote parties and therefore, given that quantum-state teleportation can be proven to be optimal, the classical communication cost of the remote control process is two bits in each direction. We will analyze now what happens if the requirement of universality is removed and characterize the sets of transformations that can be implemented remotely without resorting to BQST.

III. OPTIMAL NONTRIVIAL PROTOCOL FOR THE IMPLEMENTATION OF AN ARBITRARY *U*

As explained in detail above, the basic principles establishing the impossibility of superluminal communication and the impossibility of increasing entanglement under LQCC allow us to set the necessary resources for implementing a universal remote-control protocol: Two shared *e*-bits between Alice and Bob, two *c*-bits conveyed from Alice to Bob, one *c*-bit conveyed from Bob to Alice.

We will now show that a protocol can be built, which saturates these bounds and achieves 50% efficiency for the remote implementation of an arbitrary U. Given that the optimal protocol consumes two classical bits from Bob to Alice, this is the maximum probability of success if only one bit is conveyed in that direction.

Our starting point can, therefore, be chosen as a pure state of the form

$$\begin{aligned} |\chi\rangle_{AB} = |\phi^{+}\rangle_{AB} \otimes |\phi^{+}\rangle_{AB} \otimes |\psi\rangle_b \\ = \frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)_{AB} \otimes \frac{1}{\sqrt{2}}(|00\rangle \\ +|11\rangle)_{AB} \otimes (\alpha|0\rangle+\beta|1\rangle)_b, \end{aligned} \tag{9}$$

where Alice and Bob share two maximally entangled states and Bob holds a qubit in an arbitrary state $|\psi\rangle_b = \alpha|0\rangle_b + \beta|1\rangle_b$. In the following we may omit at times the subscripts referring to the parties A and B as well as global normalization factors to make notation lighter whenever there is no risk of confusion. The aim of the protocol is to end up with Bob holding the transformed state $U|\psi\rangle_b$, the operation U being applied only on Alice's side.

A. Local actions on Bob's side

Let us keep, for the moment, one of the shared *e*-bits intact. The remaining part of the initial state can be rewritten as

$$\alpha|0\rangle_A|00\rangle_{Bb}+\beta|0\rangle_A|01\rangle_{Bb}+\alpha|1\rangle_A|10\rangle_{Bb}+\beta|1\rangle_A|11\rangle_{Bb},$$

where the first qubit belongs to Alice and the other two to Bob. We now perform a controlled-NOT operation on Bob's side using his shared part of the *e*-bit as a control. After this operation, they share the joint state

$$(\alpha|00\rangle_{AB}+\beta|11\rangle_{AB})\otimes|0\rangle_b+(\alpha|11\rangle_{AB}+\beta|00\rangle_{AB})\otimes|1\rangle_b.$$

Bob now measures his second qubit in the computational basis. If the result is 0, they do nothing, if it is 1, both Alice and Bob perform a spin flip on their qubits. As a result, Alice and Bob now share the partially entangled state

$$\alpha|00\rangle_{AB}+\beta|11\rangle_{AB}.$$

In this way we have managed to make the coefficients α, β "visible" to Alice's side or, in other words, we have distributed the amplitudes α and β onto the channel. Note that this part of the protocol has already made use of one *e*-bit. In addition, one classical bit of information has been conveyed from Bob to Alice.

B. Local actions on Alice's side

We now make use of the extra *e*-bit we have kept alone so far. The global state of the system can be written as

$$(\alpha|00\rangle_{AB}+\beta|11\rangle_{AB})\otimes(|00\rangle_{AB}+|11\rangle_{AB}).$$

Alice applies the transformation U to one of her qubits. With this, the global state reads

$$[\alpha(U|0\rangle_A)|0\rangle_B+\beta(U|1\rangle_A)|1\rangle_B]\otimes(|00\rangle_{AB}+|11\rangle_{AB}). \tag{10}$$

The remaining part of the protocol mimics quantum-state teleportation with Alice performing a Bell measurement on her side. This procedure makes use of the extra *e*-bit and involves the transmission of two classical bits of information from Alice to Bob. We will see in the following that as a result of this protocol, Bob ends up holding a two-qubit state of the form

$$\begin{aligned}(\alpha U|0\rangle+\beta U|1\rangle)\otimes|0\rangle+(\alpha U|0\rangle-\beta U|1\rangle)\otimes|1\rangle\\ =U(|\psi\rangle)\otimes|0\rangle+U(\sigma_z|\psi\rangle)\otimes|1\rangle.\end{aligned} \tag{11}$$

A final projective measurement on Bob's side yields the correct transformed state with 50% probability, the maximum allowed when the transformation U is completely arbitrary and only one bit is conveyed from Alice to Bob.

1. Detailed steps

For our purposes, it suffices to parametrize the transformation U as a generic unimodular matrix, i.e., an arbitrary rotation on a qubit of the form

$$U=\begin{pmatrix} a & b\\ -b^* & a^*\end{pmatrix}, \tag{12}$$

where the coefficients a and b obey the unimodular constraint $|a|^2+|b|^2=1$. Using the Bell basis $|\phi^{\pm}\rangle_A=|00\rangle_A\pm|11\rangle_A$, $|\psi^{\pm}\rangle_A=|01\rangle_A\pm|10\rangle_A$ for Alice's qubits, we can rewrite the joint state given by Eq. (10) as follows:

$$\begin{aligned}&|\phi^+\rangle_A\otimes(\alpha|0\rangle_BU|0\rangle_B+\beta|1\rangle_BU|1\rangle_B)\\ &\quad+|\phi^-\rangle_A\otimes(\mathbb{1}\otimes\sigma_z)(\alpha|0\rangle_BU|0\rangle_B+\beta|1\rangle_BU|1\rangle_B)\\ &\quad+|\psi^+\rangle_A\otimes(\mathbb{1}\otimes\sigma_x)(\alpha|0\rangle_BU|0\rangle_B+\beta|1\rangle_BU|1\rangle_B)\\ &\quad+|\psi^-\rangle_A\otimes(\mathbb{1}\otimes\sigma_x\sigma_z)(\alpha|0\rangle_BU|0\rangle_B+\beta|1\rangle_BU|1\rangle_B).\end{aligned} \tag{13}$$

Alice now performs a Bell measurement on her two qubits and informs of her results to Bob using a classical channel. Accordingly to Alice's measurement outcomes, Bob performs on his second qubit the same operations as those corresponding to the protocol of quantum-state teleportation. As a result of this procedure, he always ends up holding the following two-qubit pure state (dropping the subscripts B):

$$\alpha|0\rangle(a|0\rangle+b|1\rangle)+\beta|1\rangle(-b^*|0\rangle+a^*|1\rangle),$$

which, after a local Hadamard transformation on the first qubit, reads

$$|0\rangle\otimes(\alpha U|0\rangle+\beta U|1\rangle)+|1\rangle\otimes(\alpha U|0\rangle-\beta U|1\rangle).$$

A final projective measurement on the first qubit leaves Bob holding the correct transformed state by U whenever the measurement outcome is 0. However, in the case that the local measurement throws the outcome 1, Bob would hold the wrong state $\alpha U|0\rangle-\beta U|1\rangle$ and, provided that U is completely arbitrary, he cannot restore this state to the correct form. As a result, the protocol is successful in 50% of the cases. Note that this is the maximum efficiency we can expect when only one bit is conveyed from Bob to Alice. It is a remarkable fact, and a direct consequence of the linearity of quantum mechanics [3], that no protocol different from bidirectional quantum-state teleportation can achieve the remote implementation of any arbitrary operation on a qubit. But, are there sets of transformations for which it is possible for Bob to restore the final state to the correct form $\alpha U|0\rangle+\beta U|1\rangle$?

IV. RESTRICTED SET OF OPERATIONS

As discussed in detail in the preceding section, with probability 50%, Bob is left holding the wrong transformed state

$$\alpha U|0\rangle-\beta U|1\rangle=U\sigma_z|\psi\rangle. \tag{14}$$

Given that the transformation U given by Eq. (12) is completely unknown to him, no subsequent local action can yield the correct transformed state $U(|\psi\rangle)$ for every U. However, it is clear from the above expression that there are cases

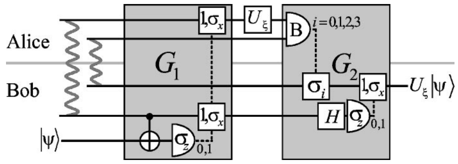

FIG. 1. Quantum circuit illustrating the protocol for the remote implementation of the operator U_ξ, which is either $U_{\rm com}$ or $U_{\rm anti}$, on the state of Bob's qubit. Wiggly lines represent shared entanglement and dotted lines stand for the exchange of classical information following the measurement of the observable enclosed in the half-ovoid symbol. Operations implemented after classical information has been exchanged are represented by squared boxes. Bell measurements are denoted by B and Hadamard transformations by H. The whole protocol prior to and following the action of U_ξ has a unitary representation $G_i (i=1,2)$.

where implementing a universal correction operation V is possible. Formally, we are seeking an operator V such that

$$VU\sigma_z|\psi\rangle = e^{i\delta}U|\psi\rangle \tag{15}$$

for any $|\psi\rangle$, γ being a real parameter. Therefore, the following operator identity must hold:

$$VU = e^{i\delta}U\sigma_z. \tag{16}$$

We can immediately identify a set of transformations that can be remotely implemented. If we set $V=\sigma_z$, the two possible unimodular solutions to Eq. (16) are given by (up to a local change of basis) [10]

$$U_{\rm com} = \begin{pmatrix} a & 0 \\ 0 & a* \end{pmatrix} = e^{i\phi\sigma_z}, \tag{17}$$

with $a=e^{i\phi}$, that is, the set of operations that commute with σ_z, or transformations of the form

$$U_{\rm anti} = \begin{pmatrix} 0 & b \\ -b* & 0 \end{pmatrix} = \sigma_x e^{i(\phi+\pi/2)\sigma_z}, \tag{18}$$

with $b=e^{i\phi}$, which anticommutes with σ_z, i.e., are linear combinations of the Pauli operators σ_x and σ_y. Any operation within this family can be teleported with 100% efficiency using a protocol that employs less resources than BQST. We can physically interpret the set of allowed transformations as arbitrary rotations around the z axis and rotations by π around any axis lying within the equatorial plane.

The complete protocol is illustrated in Fig. 1. We will illustrate in the following section, using the Bloch-sphere representation for qubits, how it can be easily visualized why a universal correction by means of the application of the operator σ_z is possible is these cases.

There is still an important question that remains to be addressed. Are the sets of operations we have just described the only ones that can be implemented remotely by nontrivial means? We will postpone the issue of uniqueness till Sec. VI.

V. GEOMETRICAL INTERPRETATION

The aim of this section is just to provide an intuitive geometrical picture in order to visualize which transformations can be implemented remotely by nontrivial means and illustrate the role of the final restoration step on Bob's side. Let us consider first a very simple scenario in which Bob is holding a qubit state lying in the equatorial plane of the Bloch sphere,

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\zeta}|1\rangle). \tag{19}$$

Imagine now that the transformation we want to implement remotely is just a spin flip, i.e., $U=\sigma_x$ (obviously Alice does not know this). In this case, given that the Pauli operator anticommutes with σ_z, the protocol described in the preceding section will result in Bob holding the correct transformed state $\sigma_x|\psi\rangle$. If Bob follows the prescribed rules, prior to the final correction step with 50% probability he holds the correct transformed state $U|\psi\rangle$ and with 50% probability he holds the erroneous state

$$\alpha U|0\rangle - \beta U|1\rangle = U\left[\frac{1}{\sqrt{2}}(|0\rangle - e^{i\zeta}|1\rangle)\right]. \tag{20}$$

Therefore, we can also consider the erroneous transformed state as the transform by U of the qubit state $|\overline{\psi}\rangle = \sigma_z|\psi\rangle$. Which state Bob ends up holding depends on a certain measurement outcome and therefore he knows whether a subsequent correction step is necessary or not. The relative position of the Bloch vectors representing the initial states $|\psi\rangle$ and $|\overline{\psi}\rangle$ and their transformed vectors by U are shown in Fig. 1. In this case, states $|\psi\rangle$ and $|\overline{\psi}\rangle$ are orthogonal and their associated Bloch vectors lie opposite in the equatorial plane of the Bloch sphere. The action of U preserves the relative orientation and the Bloch vectors associated with the transformed states by U, dashed lines in the figure, are opposite as well. The key point is that a subsequent application of the operation σ_z onto the wrong transformed state just flips its Bloch vector and yields the correct state. These considerations may sound rather trivial but it is all we need to intuitively understand how the protocol works in the general case.

Imagine now that the transformation U is not simply a Pauli operator but a transformation of the general form given by Eq. (12). Assuming that Bob's state lies initially in the equatorial plane, as before, the Bloch vector corresponding to the state transformed by U no longer lies on the equator of the Bloch sphere and has, in general, a nonzero z component $S_z=|\alpha|^2-|\beta|^2$ (we have defined $S_i=\mathrm{tr}\,\rho\sigma_i$). However, this component is equal to zero if the transformation U either commutes or anticommutes with σ_z (operations of the form $U_{\rm com}$ or $U_{\rm anti}$). In this case, we recover the situation discussed before. The transformed Bloch vectors lie opposite along some direction contained in the equatorial plane and a final step via the application of σ_z restores the wrong transformed state to the correct one.

What happens in general? The easiest way to analyze the general case, where Bob holds an arbitrary qubit state, is to parametrize it as a generic spinor and split the representation in terms of the associated Bloch vectors into two components as follows:

$$\rho=|\psi\rangle\langle\psi|=\frac{1}{2}(\mathbb{1}+S_x\sigma_x+S_y\sigma_y+S_z\sigma_z). \quad (21)$$

Analogously, the wrong transformed state can be thought of as obtained from U acting upon the state

$$\overline{\rho}=|\overline{\psi}\rangle\langle\overline{\psi}|=\frac{1}{2}(\mathbb{1}-S_x\sigma_x-S_y\sigma_y+S_z\sigma_z), \quad (22)$$

so we can write the erroneous transformed state as

$$U\overline{\rho}U^{\dagger}=\frac{1}{2}[\mathbb{1}-U(S_x\sigma_x+S_y\sigma_y)U^{\dagger}+US_z\sigma_zU^{\dagger}]. \quad (23)$$

Consider the case where the transformation U commutes with the action of σ_z. When Bob applies the final correction step, the transformed state reads

$$\begin{aligned}\sigma_zU\overline{\rho}U^{\dagger}\sigma_z&=\frac{1}{2}[\mathbb{1}-\sigma_zU(S_x\sigma_x+S_y\sigma_y)U^{\dagger}\sigma_z\\&\quad+\sigma_zUS_z\sigma_zU^{\dagger}\sigma_z]\\&=\frac{1}{2}[\mathbb{1}+U(S_x\sigma_x+S_y\sigma_y)U^{\dagger}+US_z\sigma_zU^{\dagger}]\\&=U\rho U^{\dagger},\end{aligned} \quad (24)$$

where we have taken into account that Pauli operators anticommute among themselves and that $\sigma^2=\mathbb{1}$. A similar argument holds for the case where U anticommutes with σ_z. Resuming our geometrical picture, in the general case, the corresponding Bloch vectors associated with the states $|\psi\rangle$ and $|\overline{\psi}\rangle$ have the same z component while the corresponding projections onto the equatorial plane lie opposite. Therefore, under the action of a transformation U, which either commutes or anticommutes with σ_z, we recover the situation discussed at the beginning of this section and a final correction by means of applying the operation σ_z restores the correct transformed state.

VI. CHARACTERIZATION OF SETS THAT ALLOW REMOTE IMPLEMENTATION WITHOUT BIDIRECTIONAL STATE TELEPORTATION

So far we have identified two sets of transformations that can be implemented remotely without resorting to BQST of every state. However, the procedure by which they have been identified does not allow one to draw any conclusion as far as their uniqueness is concerned. This is the aim of this section. To do this we first establish necessary conditions for avoiding BQST and then we show the uniqueness of the two sets of transformations.

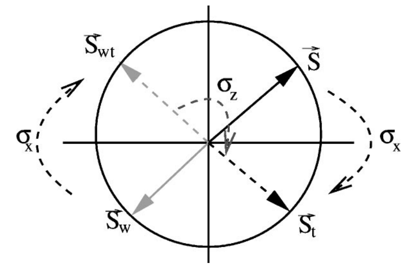

FIG. 2. Geometrical interpretation of the restoration to the correct transformed state when the transformation U belongs to a restricted set. Subindex t refers to the transformed states by the unitary transformation while subindex w refers to the erroneous state. See the text for details.

A. Necessary conditions for avoiding BQST

Let the set of operators that can be remotely implemented on Bob's qubit be labeled as $\mathcal{U}$. We know [3] that if $\mathcal{U}$ is the full set of unimodular operations on a qubit, the protocol necessarily teleports the state of Bob's qubit to Alice, that is, every state undergoes BQST. In contrast, in the protocol described in Sec. III, where $\mathcal{U}$ contains operators of the form Eqs. (17) and (18), it is easy to show that only the two orthogonal states $|0\rangle$ and $|1\rangle$ undergo BQST. In this section we examine the relationship between the size of the set $\mathcal{U}$ and the number of states that undergo BQST. From this we show that if Bob is restricted to sending one c-bit to Alice, then the set $\mathcal{U}$ comprises two particular subsets.

1. Subsets of operators

In [3] we showed that if the teleported operation U is arbitrary, that is, $\mathcal{U}$ is the full set of unimodular operations, then the final state of the ancilla is independent of U. However, here the set of operators is restricted and so the final state of the ancilla may depend on which operation is teleported. Hence we reexpress the operation of the black box as [cf. Eq. (1)]

$$G_2U_nG_1(|\chi\rangle_{aAB}|\psi\rangle_b)=|\Phi(\chi,U_n)\rangle_{aAB}U_n|\psi\rangle_b \quad (25)$$

for $U_n\in\mathcal{U}$. We know that the final state $|\Phi(\chi,U_n)\rangle_{aAB}$ is independent of $|\psi\rangle_b$ by the same arguments presented in our previous work [3].

Consider action of the gate for a linear combination of operators $U=\Sigma_nc_nU_n$, where $U,U_n\in\mathcal{U}$,

$$\begin{aligned}G_2U_nG_1|\chi\rangle_{aAB}|\psi\rangle_b&=\sum_n c_nG_2U_nG_1|\chi\rangle_{aAB}|\psi\rangle_b\\&=\sum_n c_n|\Phi(\chi,U_n)\rangle_{aAB}U_n|\psi\rangle_b,\end{aligned}$$

which equals $|\Phi(\chi,U)\rangle_{aAB}U|\psi\rangle_b$ only if $|\Phi(\chi,U_n)\rangle_{aAB}$ is independent of U_n. In other words, linearly dependent operators share the same final state. This final state may depend on set of linearly dependent control operators, however. Indeed, we subdivide the set $\mathcal{U}$ into subsets

$$\mathcal{U}=\mathcal{U}^{(1)}\cup\mathcal{U}^{(2)}\cup\cdots,$$

which leave the state of the ancilla in the same final state, that is, the set $\mathcal{U}^{(n)}$ only contains operators $U_i^{(n)}$ indexed by i, for which

$$|\Phi(\chi,U_k^{(n)})\rangle=|\Phi(\chi,U_j^{(n)})\rangle=|\Phi^{(n)}(\chi)\rangle.$$

Here, and in the remainder of this section, we use the superscript "(n)" to label a subset and its elements. It follows that the subsets $\mathcal{U}^{(n)}$ are linearly independent in the sense that an operator in one subset cannot be written as a linear combination of operators from it and other sets. Also, the subsets are clearly disjoint as each operator $U\in\mathcal{U}$ belongs to one and only one subset $\mathcal{U}^{(n)}$. Since there are a maximum of four linearly independent operators on the two-dimensional state space, there are thus a maximum of four subsets $\mathcal{U}^{(n)}\subset\mathcal{U}$.

2. Special case $G_1=\mathbb{1}$

It is interesting to consider the special case where $G_1=\mathbb{1}$. We show that for this case there are a maximum of four operators that can be teleported. Consider two operators $U_1^{(n)}$ and $U_2^{(m)}$ and choose an orthogonal pair of states $\langle\psi|\psi_\perp\rangle=0$ such that

$$U_1^{(n)}|\psi\rangle=|\phi\rangle, \tag{26}$$

$$U_2^{(m)}|\psi_\perp\rangle=|\phi'\rangle, \tag{27}$$

where $\langle\phi|\phi'\rangle\neq 0$ and $U_i^{(k)}\in\mathcal{U}^{(k)}$. The fact that this is possible is proved in the Appendix. Thus, we can write

$$\begin{aligned}U_1^{(n)}|\chi\rangle_{aAB}|\psi\rangle_b&=G_2^\dagger|\Phi^{(n)}(\chi)\rangle_{aAB}U_1^{(n)}|\psi\rangle_b\\&=G_2^\dagger|\Phi^{(n)}(\chi)\rangle_{aAB}|\phi\rangle_b,\end{aligned} \tag{28}$$

$$\begin{aligned}U_2^{(m)}|\chi\rangle_{aAB}|\psi_\perp\rangle_b&=G_2^\dagger|\Phi^{(m)}(\chi)\rangle_{aAB}U_1^{(m)}|\psi_\perp\rangle_b\\&=G_2^\dagger|\Phi^{(m)}(\chi)\rangle_{aAB}|\phi'\rangle_b.\end{aligned} \tag{29}$$

The inner product of the left-hand sides of Eqs. (28) and (29) is zero and so

$$0=\langle\Phi^{(n)}(\chi)|\Phi^{(m)}(\chi)\rangle_{aAB}\langle\phi|\phi'\rangle_b. \tag{30}$$

But if $n=m$, then $\langle\Phi^{(n)}(\chi)|\Phi^{(m)}(\chi)\rangle_{aAB}=1$ and Eq. (30) cannot be satisfied. We conclude that each subset contains only one operator.

Also, if $n\neq m$ (i.e., different subsets) then Eq. (30) implies $\langle\Phi^{(n)}(\chi)|\Phi^{(m)}(\chi)\rangle_{aAB}=0$ and so the final ancilla states are orthogonal. The number of operators that can be teleported therefore depends on the dimension of the ancilla state space. Provided this can be made large enough, there will be a maximum of four operators that can be teleported with $G_1=\mathbb{1}$ (because there are a maximum of four linearly independent subsets).

The fact that the final states of the ancilla are orthogonal for different operators means that the operators themselves are orthogonal. Imagine that Alice has a son called Bobby in her laboratory. She teleports the operator to Bobby and together they examine the final state of their (local) ancilla. From this they can determine which operator Alice teleported. Alice can communicate this to Bob using two classical bits of information, and Bob can then carry out locally the corresponding operation on his qubit.

Hence the special case $G_1=\mathbb{1}$ leads to a trivial, classical remote-control scenario. For the remainder of this paper we only consider the case where $G_1\neq\mathbb{1}$.

3. Conditions for the BQST of a state

We now look at a sufficient condition on the set $\mathcal{U}$ for the BQST of a state. This will give us a necessary condition for avoiding BQST for a set of states. Choose $U^{(n)}\in\mathcal{U}^{(n)}$ and let

$$U^{(n)}|\psi\rangle=|\phi\rangle. \tag{31}$$

Thus we have

$$\begin{aligned}G_2U^{(n)}G_1|\chi\rangle_{aAB}|\psi\rangle_b&=|\Phi^{(n)}(\chi)\rangle_{aAB}U^{(n)}|\psi\rangle_b\\&=|\Phi^{(n)}(\chi)\rangle_{aAB}|\phi\rangle_b\end{aligned} \tag{32}$$

and so

$$G_1|\chi\rangle_{aAB}|\psi\rangle_b=[U^{(n)}]^\dagger G_2^\dagger|\Phi^{(n)}(\chi)\rangle_{aAB}|\phi\rangle_b. \tag{33}$$

Next we construct the unimodular operator $Q(\theta,|\xi\rangle)$ as follows:

$$Q(\theta,|\xi\rangle)\equiv e^{i\theta}|\xi\rangle\langle\xi|+e^{-i\theta}(\mathbb{1}-|\xi\rangle\langle\xi|) \tag{34}$$

for $\theta\neq 0,\pi,2\pi,\ldots$ and an arbitrary (normalized) state $|\xi\rangle$. This operator has the property that

$$Q(\theta,|\phi\rangle)U^{(n)}=U^{(n)}Q(\theta,|\psi\rangle).$$

If $U^{(n)}Q(\theta,|\psi\rangle)\in\mathcal{U}^{(n)}$ then we can replace $U^{(n)}$ in Eq. (32) with $U^{(n)}Q(\theta,|\psi\rangle)$ and obtain from Eq. (33)

$$\begin{aligned}Q(\theta,|\phi\rangle_a)G_1|\chi\rangle_{aAB}|\psi\rangle_b&=[U^{(n)}]^\dagger G_2^\dagger|\Phi^{(n)}(\chi)\rangle_{aAB}U^{(n)}\\&\quad\times Q(\theta,|\psi\rangle_b)|\psi\rangle_b\\&=e^{i\theta}[U^{(n)}]^\dagger G_2^\dagger|\Phi^{(n)}(\chi)\rangle_{aAB}|\phi\rangle_b.\end{aligned} \tag{35}$$

Comparing Eq. (33) with Eq. (35) shows that $G_1|\chi\rangle_{aAB}|\psi\rangle_b$ is an eigenstate of $Q(\theta,|\psi\rangle_a)$, i.e.,

$$G_1|\chi\rangle_{aAB}|\psi\rangle_b=|\psi\rangle_a\otimes\cdots$$

or, in other words, that the state of Bob's qubit is necessarily teleported to Alice by the operation of G_1. Note that if $U^{(n)}Q(\theta,|\psi\rangle)$ belongs to a different subset, say $\mathcal{U}^{(m)}$ with $m\neq n$, then instead of Eq. (35) we get

$$\begin{aligned}Q(\theta,|\phi\rangle_a)G_1|\chi\rangle_{aAB}|\psi\rangle_b&=[U^{(n)}]^\dagger G_2^\dagger|\Phi^{(m)}(\chi)\rangle_{aAB}U^{(n)}\\&\quad\times Q(\theta,|\psi\rangle_b)|\psi\rangle_b\\&=e^{i\theta}[U^{(n)}]^\dagger G_2^\dagger|\Phi^{(m)}(\chi)\rangle_{aAB}|\phi\rangle_b\\&\neq e^{i\theta}[U^{(n)}]^\dagger G_2^\dagger|\Phi^{(n)}(\chi)\rangle_{aAB}|\phi\rangle_b\end{aligned}$$

and so the state of Bob's qubit is *not* teleported by G_1 to the qubit operated on by $U^{(n)}$. Hence we can state a sufficient condition for BQST as follows: BQST occurs for a state $|\psi\rangle$ when at least one value of $\theta\neq 0,\pi,2\pi,\ldots$ can be found such that $U^{(n)}Q(\theta,|\psi\rangle)\in\mathcal{U}^{(n)}$ for at least one operator $U^{(n)}\in\mathcal{U}^{(n)}$ for any $\mathcal{U}^{(n)}\subset\mathcal{U}$.

Consider, for the moment, the case where we insist that *none* of the states $|\psi\rangle$ undergo BQST. This requires that $U^{(n)}Q(\theta,|\psi\rangle)\notin\mathcal{U}^{(n)}$ for all $|\psi\rangle$, all $U^{(n)}\in\mathcal{U}^{(n)}$, all $\mathcal{U}^{(n)}\in\mathcal{U}$, and all $\theta\neq 0,\pi,2\pi,\ldots$. The set of $Q(\theta,|\psi\rangle)$ for all $|\psi\rangle$ and all $\theta\neq 0,\pi,2\pi,\ldots$ is the set of all unimodular operators minus the set of operators that are proportional to the identity. Assume for the moment that $\mathcal{U}^{(n)}$ contains the two operators $U_1^{(n)}$, $U_2^{(n)}$ where $U_1^{(n)}\neq e^{i\vartheta}U_2^{(n)}$ for any real ϑ. We can set $Q(\theta,|\psi\rangle)=[U_1^{(n)}]^\dagger U_2$ for an appropriate choice of $|\psi\rangle$ and θ, and so $U_1^{(n)}Q(\theta,|\psi\rangle)=U_2^{(n)}\in\mathcal{U}^{(n)}$. This means that the state $|\psi\rangle$ would be BQST contradicting our starting point. Clearly if no states are to undergo BQST then each subset $\mathcal{U}^{(n)}$ cannot contain more than one operator (up to an imaginary phase factor). Hence, for the case where no states are BQST, $\mathcal{U}$ contains at most four linearly independent operators. We note that if the four operators are orthogonal (i.e., related to the identity operator and four Pauli operators by a fixed transformation) Alice may distinguish between them using local means and thus send two classical bits to Bob who could then implement locally the appropriate operation on his qubit. This, like the $G_1=\mathbb{1}$ case, is trivial, classical remote control and so we do not consider it further.

Returning to the more general case, one can see from Eq. (34) that $Q(\theta,|\psi\rangle)=Q(-\theta,|\psi_\perp\rangle)$ where $\langle\psi_\perp|\psi\rangle=0$ and so if $|\psi\rangle$ undergoes BQST then so too are the states orthogonal to $|\psi\rangle$. Nontrivial remote control therefore necessarily incurs BQST for at least one pair of orthogonal states. Bob can communicate one classical bit to Alice by preparing his qubit in one of a pair of orthogonal states and stopping the protocol after G_1. The scheme we are most interested in is where Bob sends exactly one classical bit of information to Alice. Henceforth we only consider the case where exactly one pair of orthogonal states undergo BQST with all other states avoiding BQST.

4. BQST of a single pair of states

For brevity we take the pair of orthogonal states that are BQST to be the computational basis states: $|0\rangle$, $|1\rangle$. (It is straightforward to generalize our analysis to an arbitrary pair.) All other states $|\psi'\rangle$, arbitrary normalized superpositions of $|0\rangle$ and $|1\rangle$, do not undergo BQST. We can write this as

$$U_i^{(n)}Q(\theta,|\psi'\rangle)\notin\mathcal{U}^{(n)},$$

or, equivalently,

$$Q(\theta,|\psi'\rangle)\notin[U_i^{(n)}]^\dagger\mathcal{U}^{(n)}$$

for all $\theta\neq 0,\pi,2\pi,\ldots$, all $|\psi'\rangle\neq|0\rangle,|1\rangle$, all $U_i^{(n)}\in\mathcal{U}^{(n)}$, and all subsets $\mathcal{U}^{(n)}\subset\mathcal{U}$. The set of operators $\{Q(\theta,|\psi'\rangle)\}$ here is the set of all unimodular operators *not* diagonalized by $|0\rangle,|1\rangle$. Hence each set $[U_i^{(n)}]^\dagger\mathcal{U}^{(n)}$ contains operators that *are* diagonalized by $|0\rangle,|1\rangle$. Thus all elements of each subset $\mathcal{U}^{(n)}\subset\mathcal{U}$ have the form

$$\begin{aligned}U_\varphi^{(n)}&=U_0^{(n)}(e^{i\varphi}|0\rangle\langle 0|+e^{-i\varphi}|1\rangle\langle 1|)\\&=U_0^{(n)}Q(\varphi,|0\rangle)\\&=U_0^{(n)}e^{i\varphi\sigma_z}.\end{aligned}\tag{36}$$

If the subsets $\mathcal{U}^{(n)}$ are the largest possible (i.e., $\mathcal{U}^{(n)}$ contains the operators $U_\varphi^{(n)}$ for all φ) then there are a maximum of two subsets $\mathcal{U}^{(n)}\subset\mathcal{U}$. To see this consider an arbitrary, unimodular, linear combination of the elements of two subsets $\mathcal{U}^{(1)}$ and $\mathcal{U}^{(2)}$,

$$U=xU_0^{(1)}e^{i\varphi\sigma_z}+yU_0^{(2)}e^{i\gamma\sigma_z},$$

where x and y are real numbers. We can write this as

$$[U_0^{(1)}]^\dagger U=xe^{i\varphi\sigma_z}+y[U_0^{(1)}]^\dagger U_0^{(2)}e^{i\gamma\sigma_z}$$

or, in matrix form, as

$$\begin{bmatrix}c & d\\ -d^* & c^*\end{bmatrix}=x\begin{bmatrix}e^{i\varphi} & 0\\ 0 & e^{-i\varphi}\end{bmatrix}+y\begin{bmatrix}ae^{i\gamma} & be^{-i\gamma}\\ -b^*e^{i\gamma} & a^*e^{-i\gamma}\end{bmatrix},$$

where

$$[U_0^{(1)}]^\dagger U=\begin{bmatrix}c & d\\ -d^* & c^*\end{bmatrix},$$

$$[U_0^{(1)}]^\dagger U_0^{(2)}=\begin{bmatrix}a & b\\ -b^* & a^*\end{bmatrix}.$$

Clearly, $ye^{-i\gamma}=d/b$ and $xe^{i\varphi}=c-yae^{i\gamma}$, which can be solved for real values of x, y, φ, and γ for arbitrary c and d satisfying $|c|^2+|d|^2=1$. This shows that every unimodular operator $U'=[U_0^{(1)}]^\dagger U$, and hence every unimodular operator $U=U_0^{(1)}U'$, can be written in terms of a linear combination of operators in the subsets $\mathcal{U}^{(1)}$ and $\mathcal{U}^{(2)}$. These two subsets are, therefore, the only linearly independent subsets. We note that choosing $U_0^{(1)}=\mathbb{1}$ and $U_0^{(2)}=\sigma_x$ in Eq. (36) yields the two sets of operators defined in Eqs. (17) and (18).

We sum up this section: To avoid BQST for all states, the set of control operators must be restricted to a set of a maximum of four linearly independent operators; if one state undergoes BQST then so are the states orthogonal to it; if Bob is restricted to sending one classical bit to Alice then only one pair of orthogonal states can undergo BQST and the set of control operations $\mathcal{U}$ can be divided into a maximum of four subsets $\mathcal{U}^{(n)}\subset\mathcal{U}$ whose elements have the form Eq. (36); if the subsets $\mathcal{U}^{(n)}$ in Eq. (36) contain operators $U_\beta^{(n)}$ for all β then only two subsets are possible.

Finally, we note that these conditions on the set $\mathcal{U}$ of controlled operators are *necessary* for avoiding the BQST of various states. They are not *sufficient* conditions because G_1 and G_2 can be chosen to perform BQST for all states, irrespective of the restrictions on $\mathcal{U}$.

B. Full characterization of classes of operators allowing for nontrivial remote implementation

In this section we now complete the characterization of the classes of transformations that can be implemented without BQST. We will show that a protocol that consumes two shared *e*-bits plus two bits of classical communication from *A* to *B* plus one bit of classical communication from *B* to *A* (i.e., a "221" protocol) for teleportation of unitary operations is only possible when the operations are drawn from the following two sets:

$$\left[\begin{pmatrix} e^{i\phi} & 0 \\ 0 & e^{-i\phi}\end{pmatrix}, \phi\in\mathbb{R}\right], \quad \text{set A}, \tag{37}$$

$$\left[\begin{pmatrix} a & b \\ -b^* & a^*\end{pmatrix}\begin{pmatrix} e^{i\phi} & 0 \\ 0 & e^{-i\phi}\end{pmatrix}, \phi\in\mathbb{R}\right], \quad \text{set B} \tag{38}$$

under the constraint that either $|a|=1$ (trivial) or $|b|=1$. Any other choices will require more resources.[1] Together with the results from the preceding section this then concludes our characterization of those operations that allow for nontrivial remote implementation.

As outlined in Sec. II and used throughout this paper the most general protocol is given by

$$G_2UG_1|\chi\rangle_{aAB}|\psi\rangle_b = |\overline{\chi}\rangle_{aAB}(U|\psi\rangle)_b, \tag{39}$$

where without loss of generality the state $|\chi\rangle$ is a tensor-product state. For whatever form of G_1 we can always write Eq. (39) as

$$G_2UG_1|\chi\rangle_{aAB}|\psi\rangle_b = G_2((U|0\rangle_a)|\Phi_0\rangle_{AB} + (U|1\rangle_a)|\Phi_1\rangle_{AB}) = |\overline{\chi}\rangle_{aAB}(U|\psi\rangle)_b. \tag{40}$$

We chose the notation $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ and note that $|\overline{\chi}\rangle$ is independent from both ϕ and $|\psi\rangle$, but may of course depend on a and b. From normalization we have $\langle\Phi_0|\Phi_0\rangle + \langle\Phi_1|\Phi_1\rangle = 1$. If we now evaluate Eq. (40) for two unitaries U_1, U_2 from the above sets, Eqs. (37) and (38), we can obtain the following scalar product:

$$\sum_{ij}\langle i|U_2^\dagger U_1|j\rangle\langle\Phi_i|\Phi_j\rangle = (|\alpha|^2\langle 0|U_2^\dagger U_1|0\rangle + |\beta|^2\langle 1|U_2^\dagger U_1|1\rangle + \alpha\beta^*\langle 1|U_2^\dagger U_1|0\rangle + \alpha^*\beta\langle 0|U_2^\dagger U_1|1\rangle)\langle\overline{\chi_2}|\overline{\chi_1}\rangle. \tag{41}$$

The proof proceeds in essentially two steps. First we will demonstrate that in the protocol the operation G_1 will generally create an entangled state between the qubit U is acting upon the rest of the systems. Up to local rotations any entangled state is of the form $r|00\rangle + s|11\rangle$. In the basis where the entangled state can be written like this we will then show that when U acts on it we can only find a G_2 that recovers $U|\psi\rangle$ if either $|a|=1$ or $|b|=1$. This then concludes the proof.

Step 1. We assume that there is no entanglement generated by G_1. Given that the set of transformations that we want to teleport is nontrivial, i.e., they are generally nonorthogonal, the transformation G_1 has to be nontrivial. This implies, in particular, that a strategy of distinguishing the unitaries is not possible. Therefore we cannot have the situation that $|\Phi_0\rangle = |\Phi_1\rangle = |\psi\rangle$ for all unitaries U.[2]

Now let us assume that G_1 does not generate an entangled state, which requires that

$$|\Phi_0\rangle = \frac{x'}{y'}|\Phi_1\rangle. \tag{42}$$

Under this assumption we will now demonstrate that then $x'/y' = \alpha/\beta$. To this end let us make the special choice $U_2 = \mathbf{1}$, which simplifies the analysis and is sufficient to generate the desired result. Then we have

$$\langle 0|U_1|0\rangle|x'|^2 + \langle 1|U_1|1\rangle|y'|^2 + \langle 0|U_1|1\rangle(x')^*y' + \langle 1|U_1|0\rangle x'(y')^* = (|\alpha|^2\langle 0|U_1|0\rangle + |\beta|^2\langle 1|U_1|1\rangle + \alpha\beta^*\langle 1|U_1|0\rangle + \alpha^*\beta\langle 0|U_1|1\rangle)g, \tag{43}$$

where g depends on whether U_1 is chosen from set $A(g=1)$ or set B (g to be determined below). Therefore,

$$\langle 0|U_1|0\rangle(|x'|^2 - g|\alpha|^2) + \langle 1|U_1|1\rangle(|y'|^2 - g|\beta|^2) + \langle 0|U_1|1\rangle[(x')^*y' - g\alpha^*\beta] + \langle 1|U_1|0\rangle[x'(y')^* - g\alpha\beta^*] = 0. \tag{44}$$

If we chose

$$\begin{pmatrix} e^{i\phi} & 0 \\ 0 & e^{-i\phi}\end{pmatrix} \tag{45}$$

with $\phi=0$ and $\phi=\pi/2$ (which means $g=1$) then we get two equations and with the resulting condition

$$|x'| = |\alpha| \quad \text{and} \quad |y'| = |\beta|. \tag{46}$$

Now we chose two matrices from the set B to determine g. From Eq. (44) we then find that

$$a^*(1-g)|\beta|^2 + b(x'^*y' - \alpha^*\beta g) = 0, \tag{47}$$

[1] Of course we have, in addition, the freedom of choice of basis, i.e., we can change all the above sets jointly by a fixed basis change, but that is a trivial freedom.

[2] This remark is relevant because for the case of four orthogonal transformations the following argument does not hold, because we assume that $|\chi\rangle$ is independent of U, which only needs to hold when one wishes to teleport nonorthogonal transformations.

$$a(1-g)|\alpha|^2 - b^*(x'y'^* - \alpha\beta^* g) = 0, \tag{48}$$

as coefficients in front of $e^{i\phi}$ and $e^{-i\phi}$ have to vanish. As a, b, and g are fixed, we can now only vary α and β. We know that $|\overline{\chi}\rangle$, and therefore g, do not depend on the choice of α and β. To determine g let us now choose a special case, namely, $\alpha=0$. In that case we see from Eq. (48) that

$$b^* x' y'^* = 0 \tag{49}$$

and therefore from Eq. (47) we find

$$a^*(1-g) = 0. \tag{50}$$

Now we can consider three cases.

(a) $a\neq 0, b\neq 0$: Then $g=1$.

(b) $|a|=1$. Then $g=0$, but in that case the sets A and B are identical and we already know the optimal protocol.

(c) $|b|=1$. Again we know the optimal protocol already.

Therefore, we only need to consider the case where $|g|=1$ and $a\neq 0, b\neq 0$. Then we have that $x'^* y' = \alpha^*\beta$. Dividing both sides by $|x'|^2$ gives

$$\frac{y'}{x'} = \frac{\alpha^*\beta}{|x'|^2} = \frac{\alpha^*\beta}{|\alpha|^2} = \frac{\beta}{\alpha}. \tag{51}$$

This implies

$$|0\rangle|\Phi_0\rangle + |1\rangle|\Phi_1\rangle = \frac{1}{\beta}(\alpha|0\rangle + \beta|1\rangle)|\Phi_1\rangle. \tag{52}$$

As the state $|\psi\rangle$ is general, this implies that G_1 is a state transfer from Bob to Alice and the resource cost is two bits from Bob to Alice. If we only wish to expend one bit from Bob to Alice, then this is not a valid option and we can then, therefore, say that, in general, G_1 will produce an entangled state.

Step 2. Now we can assume that there is a state $|\psi\rangle$ such that G_1 acting on $|\chi\rangle|\psi_1\rangle$ generates an entangled state. Let us now make a basis change such that we can write

$$G_1|\chi\rangle|\psi_1\rangle = r|0\rangle|0\rangle + s|1\rangle|1\rangle. \tag{53}$$

Now we have to show that when a U from any of the sets A or B acts on one half of the state (53), it is not possible to find a G_2 (unless either $|a|=1$ or $|b|=1$) such that

$$G_2(U\otimes 1(r|00\rangle + se^{i\phi}|11\rangle)) = U\begin{pmatrix}1 & 0\\ 0 & e^{i\phi}\end{pmatrix}|\psi\rangle|\chi_U\rangle, \tag{54}$$

$$G_2(r|00\rangle + se^{i\eta}|11\rangle) = U\begin{pmatrix}1 & 0\\ 0 & e^{i\eta}\end{pmatrix}|\psi\rangle|\chi\rangle. \tag{55}$$

First, we note again that the state $|\chi\rangle$ cannot depend on ϕ or η, as otherwise the transformation G_2 would not be linear. However, it may depend on the choice of U. Now let us take the scalar product between Eqs. (54) and (55). Again G_2 drops out due to its unitarity and if we use $g=\langle\chi_U|\chi\rangle=1$, we find

$$|r|^2 a + |s|^2 e^{i(\phi-\eta)} a^* = (a|\alpha|^2 + a^*|\beta|^2 e^{i(\phi-\eta)} + b\alpha^*\beta e^{i\phi} - b^*\alpha\beta^* e^{-i\eta}) \tag{56}$$

or

$$(|r|^2 - |\alpha|^2)a + (|s|^2 - |\beta|^2)e^{i(\phi-\eta)}a^* - b\alpha^*\beta e^{i\phi} + b^*\alpha\beta^* e^{-i\eta} = 0 \tag{57}$$

for all ϕ,η. This implies that

$$|r|^2 - |\alpha|^2 = |s|^2 - |\beta|^2 = 0 \quad \text{and} \quad b\alpha^*\beta = 0. \tag{58}$$

Because both r and s are nonzero, we find that also α and β are nonzero, which implies that $b=0$ [11]. Therefore the only two possible values for a and b are $|a|=1$ and $|b|=1$ and this finishes the proof.

VII. TRADE-OFF IN RESOURCES

The results of the preceding section allows us to establish the uniqueness of the two teleportable sets, which arise in Sec. IV as the two possible cases where the transmission of just one bit from Alice to Bob was sufficient to design a protocol for perfect remote implementation. It should be stressed that the procedure works independently of which particular subset the transformation belongs to. Imagine now that Alice is given the promise that her apparatus can implement transformations within a particular subset, for instance, any unitary transformation that commutes with the action of the Pauli operator σ_z. In other words, she is provided with a machine that can implement arbitrary rotations around the z axis. As before, the aim is to implement remotely any such transformation on Bob's side, provided that he may hold a qubit state in an arbitrary state $|\psi\rangle_b$. We will show in the following that a variation of the protocol discussed in Sec. III allows the implementation of an arbitrary rotation on Bob's side consuming just one e-bit and one c-bit in each direction. In contrast, BQST would consume one e-bit and two c-bits per state-teleportation step. We start with Alice and Bob sharing an e-bit, which for concreteness we assume to be the maximally entangled state $|\phi\rangle_{AB}^+$. Bob holds a qubit system in an arbitrary state $|\phi\rangle_b = \alpha|0\rangle_b + \beta|1\rangle_b$. We carry out the same local operations on Bob's side described in Sec. III A, that is, a controlled-NOT between Bob's qubits with the unknown state acting as the control qubit followed by a projective measurement of the target qubit in the computational basis. This sequence consumes one c-bit from Bob to Alice and ends up with both parties sharing the, in general, partially entangled, state $\alpha|00\rangle_{AB} + \beta|11\rangle_{AB}$. Alice now applies the operation $U_{\rm com}$ onto her qubit followed by a Hadamard transformation. No extra shared entanglement will be required. The global (unnormalized) state of the distributed system after this action can be written as

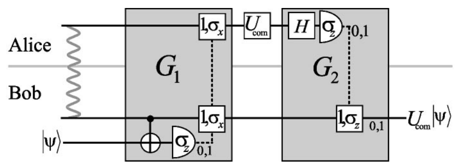

FIG. 3. Quantum circuit illustrating the protocol for the remote implementation of U_{com} on the state of Bob's qubit. Symbolic representations as in Fig. 1.

$$
\begin{aligned}
|\lambda\rangle_{AB} &= \alpha a(|0\rangle_A + |1\rangle_A)|0\rangle_B + \beta a^\star(|0\rangle_A - |1\rangle_A)|1\rangle_B \\
&= |0\rangle_A(\alpha a|0\rangle_B + \beta a^\star|1\rangle_B) + |1\rangle_A(\alpha a|0\rangle_B - \beta a^\star|1\rangle_B) \\
&= |0\rangle_A[\alpha U(|0\rangle_B) + \beta U(|1\rangle_B)] + |1\rangle_A[\alpha U(|0\rangle_B) \\
&\quad - \beta U(|1\rangle_B)]. \qquad (59)
\end{aligned}
$$

A projective measurement in the computational basis on Alice's side yields a collapsed state on Bob's side, which is either the correct transformed state by U_{com}, whenever the measurement outcome is $|0\rangle_A$, or a state that can be locally transformed into the correct one (Fig. 2). If the measurement outcome is $|1\rangle_A$, all Bob has to do is apply the correcting operation σ_z. Bob needs to know the measurement outcome of Alice's measurement and therefore a further *c*-bit is consumed in the second part of the protocol. The complete protocol is illustrated in Fig. 3.

Identical results follow if Alice is given the promise that the transformation U anticommutes with σ_z. The only difference is that Bob gets the correct transformed state via the application of different correction steps, σ_x for outcome $|0\rangle_A$ and $\sigma_z\sigma_x$ for outcome $|1\rangle_A$.

The explicit construction of a protocol that achieves the remote implementation of any unitary operation of the form U_c or U_a proves that consuming one *e*-bit and one *c*-bit in each direction is sufficient. The necessity can be derived from the following argument. Assume that we can teleport any transformation U, which either commutes or anticommutes with σ_z. We can then assume that we could also implement any controlled U of that form and, in particular, we could implement a controlled-NOT operation. But it is known that the nonlocal implementation of a controlled-NOT requires one *e*-bit and two classical bits in each direction [9], therefore the protocol we have described is optimal.

VIII. CONCLUSIONS AND PROSPECTS

We have analyzed the problem of performing quantum remote control of a state. The principles of nonincrease of entanglement under LQCC and the impossibility of superluminal communication allows one to establish lower bounds on the amount of entanglement and the classical communication cost of a universal remote-control protocol: Alice and Bob need to share at least two *e*-bits and need to communicate no less than two *c*-bits from Alice to Bob and one *c*-bit from Bob to Alice. This asymmetry in the communication cost opens the possibility of a different strategy than resorting to BQST. While the protocol cannot work perfectly for an arbitrary transformation on a qubit, we have shown here that there are restricted sets of *teleportable* operations, i.e., operations that can be implemented remotely consuming less overall resources than BQST. Remarkably, up to a local change of basis, only two *teleportable* subsets exist: Arbitrary rotations around a fixed direction $\vec{n}$, and π rotations about an arbitrary direction lying in a plane orthogonal to $\vec{n}$.

We end by describing a possible experimental scenario where the ideas we have developed could be demonstrated. From the practical point of view, the most challenging requirement arises from the distribution of a highly entangled state between two remote parties. Nevertheless, theoretical proposals have been made for establishing a maximally entangled state of two separate trapped ions, each one surrounded by an optical cavity [12]. Let us then assume that a maximally entangled state can be created using these techniques. In addition, Bob's cavity holds a second ion initially prepared in a state that for simplicity we will suppose to be an equally weighted superposition of levels $|0\rangle$ and $|1\rangle$. Transformations that either commute or anticommute with the action of σ_z can be easily realized by means of irradiating Alice's particle with laser light with a suitable value of the ratio Δ/Ω, where Δ is the detuning from the atomic transition $|0\rangle \rightarrow |1\rangle$ and Ω is the laser Rabi frequency. Applying the protocol described in Sec. VII leads to Bob holding a state of the form

$$
|\psi\rangle = \frac{1}{2}(|0\rangle + e^{-i\vartheta}|1\rangle), \qquad (60)
$$

where ϑ will be a function of the laser parameters. Therefore, a subsequent measurement of Bob's particle in the $|\pm\rangle$ basis yields a probability for the ion to be found in the $|+\rangle$ state,

$$
P_{|+\rangle} = \frac{1+\cos\vartheta}{2}. \qquad (61)
$$

In other words, under repeated measurements following laser irradiations of different duration on Alice's side, Bob's particle, in a remote location, will exhibit Ramsey fringes. This effect is a nice illustration of how quantum nonlocality can be exploited and should lie among the near future experimental capabilities in quantum optics. Applications in quantum-communication protocols are foreseeable.

Note added. Recently, we have learned of related results obtained independently by Chui-Ping Yang and J. Gea-Banacloche [13] and by B. Reznik, Y. Aharonov, and B. Groisman [14].

ACKNOWLEDGMENTS

We acknowledge discussions with Benni Reznik. This work was supported by the UK Engineering and Physical Sciences Research Council (EPSRC), by the EQUIP project of the European Union and the European Science Foundation Programme on ‘‘Quantum Information Theory and Quantum Computing,’’ and by the ESF-QIT conference ‘‘Quantum Information Theory: Theory, Experiment and Perspectives’’ in Gdansk, 2001.

APPENDIX

Here we give the proof that states $|\psi\rangle$ and $|\psi_\perp\rangle$ can be found to satisfy Eqs. (26) and (27) for $\langle\psi|\psi_\perp\rangle=0$ and $\langle\phi|\phi'\rangle\neq 0$. We drop the superscripts $(n),(m)$ from the operators in these equations and diagonalize the unimodular product $U_2^\dagger U_1$,

$$U_2^\dagger U_1|\lambda_\pm\rangle = e^{i(\gamma\pm\lambda)}|\lambda_\pm\rangle$$

for real γ and λ. Note that $\lambda\neq 0,\pi,2\pi,\ldots$ for otherwise $U_2^\dagger U_1=\pm(|\lambda_+\rangle\langle\lambda_+|+|\lambda_-\rangle\langle\lambda_-|)$, which is proportional to the identity, and so the operators would be trivially related, $U_2=\pm U_1$ forcing $|\phi\rangle$ and $|\phi'\rangle$ to be orthogonal. Let

$$|\psi\rangle=(|\lambda_+\rangle+|\lambda_-\rangle)/\sqrt{2},$$

$$|\psi_\perp\rangle=(|\lambda_+\rangle-|\lambda_-\rangle)/\sqrt{2}, \tag{A1}$$

then from Eq. (26)

$$U_2^\dagger|\phi\rangle=U_2^\dagger U_1|\psi\rangle=e^{i\gamma}(e^{i\lambda}|\lambda_+\rangle+e^{-i\lambda}|\lambda_-\rangle)/\sqrt{2}$$

from which we find

$$|\phi\rangle=U_2 e^{i\gamma}(e^{i\lambda}|\lambda_+\rangle+e^{-i\lambda}|\lambda_-\rangle)/\sqrt{2}. \tag{A2}$$

From Eq. (27) we also have

$$U_2|\psi_\perp\rangle=|\phi'\rangle. \tag{A3}$$

Thus from Eqs. (A2), (A3), and (A1) we get

$$\langle\phi'|\phi\rangle=\langle\psi_\perp|U_2^\dagger U_2 e^{i\gamma}(e^{i\lambda}|\lambda_+\rangle+e^{-i\lambda}|\lambda_-\rangle)/\sqrt{2}$$
$$=ie^{i\gamma}\sin(\lambda),$$

which is nonzero (because $\lambda\neq 0,\pi,2\pi,\ldots$).

[1] M. B. Plenio and V. Vedral, Contemp. Phys. **39**, 431 (1998).

[2] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).

[3] S. F. Huelga, J. A. Vaccaro, A. Chefles, and M. B. Plenio, Phys. Rev. A **63**, 042303 (2001); e-print quant-ph/0005061.

[4] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).

[5] A. Acín, E. Jané, and G. Vidal, e-print quant-ph/0012015.

[6] A. K. Pati, e-print quant-ph/9907022; H.-K. Lo, e-print quant-ph/9912009; C. H. Bennett *et al.*, e-print quant-ph/0006044.

[7] G. Vidal, L. Masanes, and J. I. Cirac, e-print quant-ph/0102037.

[8] M. A. Nielsen and I. L. Chuang, Phys. Rev. Lett. **79**, 321 (1997).

[9] J. Eisert, K. Jacobs, P. Papadopoulos, and M. B. Plenio, Phys. Rev. A **62**, 052317 (2000); D. Collins, N. Linden, and S. Popescu, e-print quant-ph/0005102.

[10] The final correction operation V can be written as $V=W\sigma_z W^{-1}$, where W is a generic unimodular transformation. Equation (16) can now be rewritten as $\sigma_z W^{-1}U=e^{i\gamma}W^{-1}U\sigma_z$ and the two possible solutions are given by operations of the form $WU_{\rm com}$ or $WU_{\rm anti}$. However, this amounts to the trivial degree of freedom of performing a basis change.

[11] Note that the fact that G_1 generates an entangled state was used explicitly, i.e., that r and s are nonzero.

[12] S. van Enk, J. I. Cirac, and P. Zoller, Science **279**, 205 (1998); S. Bose, P. L. Knight, M. B. Plenio, and V. Vedral, Phys. Rev. Lett. **83**, 5158 (1999); L.-M. Duan, M. Lukin, J. I. Cirac, and P. Zoller, e-print quant-ph/0105105.

[13] Chui-Ping Yang and J. Gea-Banacloche, e-print quant-ph/0107100.

[14] B. Reznik, Y. Aharonov, and B. Groisman, e-print quant-ph/0107143.