Quantum Counterfactual Communication Without a Weak Trace

D. R. M. Arvidsson-Shukur and C. H. W. Barnes
Cavendish Laboratory, Department of Physics, University of Cambridge, Cambridge CB3 0HE, United Kingdom
(Dated: May 17, 2017)

The classical theories of communication rely on the assumption that there has to be a flow of particles from Bob to Alice in order for him to send a message to her. We develop a quantum protocol that allows Alice to perceive Bob’s message “counterfactually”. That is, without Alice receiving any particles that have interacted with Bob. By utilising a setup built on results from interaction-free measurements, we outline a communication protocol whereby the information travels in the opposite direction of the emitted particles. In comparison to previous attempts on such protocols, this one is such that a weak measurement at the message source would not leave a weak trace that could be detected by Alice’s receiver. Whilst some interaction-free schemes require a large number of carefully aligned beam-splitters, our protocol is realisable with two or more beam-splitters. We demonstrate this protocol by numerically solving the time-dependent Schrödinger Equation (TDSE) for a Hamiltonian that implements this quantum counterfactual phenomenon.

PACS numbers: 03.65.Ta, 03.67.Hk, 03.67.Ac

I. INTRODUCTION

A century ago, the discovery of quantum mechanics caused a renaissance of physics as a subject. The view of the fundamental nature of physical phenomena was drastically changed. During the following century the scientific community saw several ideas put forward of how to manifest the novelties of quantum mechanics.\textsuperscript{1,2} Furthermore, the novelties of quantum mechanics led to the development of quantum technologies, which can provide solutions to problems that classical systems cannot solve.\textsuperscript{3–8}

A physical novelty that quantum mechanics provide, is the interaction-free measurement (IFM), first developed by Elitzur and Vaidman.\textsuperscript{9} An IFM uses a probing interrogating particle sent through a quantum self-interference device, such as a Mach-Zehnder Interferometer (MZI), in order to obtain information about whether or not an object exists at a certain location. By utilising the postulate of wavefunction collapse\textsuperscript{10}, the protocol can be carried out such that the interrogating particle never directly interacts with or is deflected by the object of interest. These types of non-interacting interrogations are also referred to as counterfactual processes.\textsuperscript{11–13}

Significant improvements to classical information theory have also been attributed to quantum mechanics. Classically, Shannon showed how many bits have to travel from Bob to Alice in order for Bob to provide Alice with a message containing certain information.\textsuperscript{14} The classical assumption that one bit of information had to be carried by a one bit particle, was challenged by the quantum concept of superdense coding, put forward by Bennett and Weišner in 1992. Superdense coding allows Bob to send two classical bits encoded in only one quantum particle (qubit).\textsuperscript{15} Schumacher then extended many ideas from classical information theory to the quantum mechanical scenario, showing how classical information can be efficiently encoded in qubit particles and sent from Bob to Alice over a quantum channel.\textsuperscript{16}

Moreover, quantum information theory led to the development of unconditionally secure quantum key distribution (QKD) schemes.\textsuperscript{5,6,15–17} It was later shown that the distribution process of secret keys in QKD protocols can be realised with counterfactual phenomena, without the secret key particles ever traveling between the communicating parties. Such schemes have been experimentally realised,\textsuperscript{20–22} and their security advantages over other QKD protocols have been studied.\textsuperscript{23–25} Whilst the secret key is generated counterfactually, the classical public channel communication of these schemes requires particle transfer.

Classically, the exchange of physical particles in the direction of the message has been assumed necessary for information transfer between two communicating parties, Alice and Bob.\textsuperscript{14} However, could it be possible that quantum mechanics enables counterfactual transfer (without any particle exchange) of messages from Bob to Alice?

Salih et al. have previously\textsuperscript{12} attempted to produce methods for such counterfactual communication, using schemes similar to those presented in Ref.\textsuperscript{11}. These methods crucially depend on nested MZI devices. However, such devices have been the subject of intense debate in recent years.\textsuperscript{12,13,20,32} The criticism put forward—primarily by Vaidman—highlights the dilemma of welcher Weg (“which path”) determination of quantum particles. By exploring the “weak trace”\textsuperscript{26} introduced by weak measurements in different spatial locations of the protocol—Vaidman shows how significant parts of wavepackets actually travel from Bob to Alice in the protocol of Salih et al.\textsuperscript{28,29}

In this paper we adopt the role of quantum diplomats and present a novel quantum mechanical communication protocol, which avoids the weak trace implications of previous works. We outline how the theory of interaction-free measurements can be utilised to create a protocol for direct information transfer. Whilst our protocol does not alter the limits of bit transfer outlined by Shannon, Bennett, Weišner and Schumacher, it does...
significantly alter the role of the physical particles in the transmission scheme. Our protocol contradicts the intuitive idea and tenet of information theory, that the particles that carry a message of information ought to travel in the same direction as the message. We introduce a novel concept of weak-trace-free counterfactual communication, which allows for the non-local acquiring of information about distant systems. Furthermore, we present a numerical demonstration of the protocol by solving the time-dependent Schrödinger equation (TDSE) of a tailored massive particle Hamiltonian.

II. BACKGROUND

The methods presented by Salih et al. make use of a complicated IFM device, constructed from stacked nested MZIs. The nature of their protocol presents two problems for the realisation of counterfactual communication. Firstly, owing to the structure of the nested IFM device, their protocol fails to eliminate the weak-trace impact in the laboratory of Bob (the sender). Secondly, owing to the experimental difficulties with the realisation of high-efficiency interaction-free measurements and the fact that a success probability of > 95% relies on the perfect alignment of over 60000 beam-splitters with precise transmission and reflection coefficients, we deem the high-fidelity physical implementation of their protocol unlikely.

In order to avoid the implications of the stacked nested IFMs for interaction-freeness and experimental feasibility, we seek to make use of stacked non-nested MZI devices, as originally developed by Kwiat et al. (shown in FIG. 1). Whether or not the particle will be detected at the lower or upper output is determined by the number of beam-splitters, $N$ (with reflection coefficient $\cos\left(\frac{\pi}{2N}\right)$), and whether or not there are detectors present in the upper path. In the scenario of $N$ perfect beam-splitters, the particle will end up in the upper output path with probability 1 if the path is free, and in the lower path with probability $\cos\left(\frac{\pi}{2N}\right)^N$ (1 in the limit of large $N$) if the upper path is blocked by detectors. If the lower path was assigned to Alice’s Laboratory and the upper path to Bob’s, the process with detectors present would generate a counterfactual detection for Alice. However, the scenario of an empty upper path would not, as the wavefunction of the particle would travel back and forth between the two laboratories. Nevertheless, we shall see that it is possible to avoid the exchange of wavefunction from Bob to Alice by a clever spatial arrangement of the Transmission Line and Alice’s and Bob’s respective laboratories (see FIG. 2).

We introduce the bosonic creation and annihilation operators of the respective spatial domains: $a_{A, Tr, B}^\dagger$ and $a_{A, Tr, B}$. The basis states of a restricted one-particle system can then be expressed as:

$$a_{(A)}^\dagger |0\rangle_{(A)} |0\rangle_{(Tr)} |0\rangle_{(B)} \rangle = |1\rangle_{(A)} |0\rangle_{(Tr)} |0\rangle_{(B)} \rangle \, ,$$
$$a_{(Tr)}^\dagger |0\rangle_{(A)} |0\rangle_{(Tr)} |0\rangle_{(B)} \rangle = |0\rangle_{(A)} |1\rangle_{(Tr)} |0\rangle_{(B)} \rangle \, ,$$
$$a_{(B)}^\dagger |0\rangle_{(A)} |0\rangle_{(Tr)} |0\rangle_{(B)} \rangle = |0\rangle_{(A)} |0\rangle_{(Tr)} |1\rangle_{(B)} \rangle \, .$$

We also introduce a number of beam-splitters, $N$, that act between the Transmission Line and Bob’s Laboratory. They implement a transformation such that:

$$\begin{pmatrix} a_{Tr}' \\ a_{B}' \end{pmatrix} = \begin{pmatrix} \cos(N\theta) & i \sin(N\theta) \\ i \sin(N\theta) & \cos(N\theta) \end{pmatrix} \begin{pmatrix} a_{Tr} \\ a_{B} \end{pmatrix} \, , \quad (1)$$

where the primed and un-primed operators denote the output and input operators respectively.

III. THE COUNTERFAC TUAL COMMUNICATION PROTOCOL

In this section we outline the binary quantum counterfactual direct communication protocol of this paper. Firstly, we denote the respective Hilbert spaces of Alice’s, Bob’s and the Transmission Line’s spatial occupation as $H^{(A)}$, $H^{(B)}$ and $H^{(Tr)}$, such that the total Hilbert space becomes $H^{(A)} \oplus H^{(Tr)} \oplus H^{(B)}$. Each of these Hilbert spaces have the occupation number as their degree of freedom. Alice’s Hilbert space, $H^{(A)}$, contains the lower
output and input ports of the stacked IFM. Bob’s space, \( \mathcal{H}^{(B)} \), contains the upper path of the IFM device and the upper output port. Finally, The Transmission Line’s space, \( \mathcal{H}^{(Tr)} \), contains the lower part of the IFM device and all the beam-splitters. See Fig. [2]

In the following two subsections we outline the two processes that make up the communication protocol. In both bit processes Bob and Alice have pre-determined time-intervals during which Alice is to make particles available to the Transmission Line. Moreover, below we omit the prime-notation as it simply indicates smaller subspaces of the defined Hilbert spaces.

(a) The 0-Bit Process:

**Step 1:** The protocol starts with Alice creating a particle in the initial vacuum state:

\[
|0\rangle^{(A)}|0\rangle^{(Tr)}|0\rangle^{(B)} \rightarrow a_0^\dagger|1\rangle^{(A)}|0\rangle^{(Tr)}|0\rangle^{(B)} = |1\rangle^{(A)}|0\rangle^{(Tr)}|0\rangle^{(B)}. \tag{2}
\]

**Step 2:** Alice sends her particle to the Transmission Line with the pre-determined frequency:

\[
a_{(Tr)}^\dagger a_0|1\rangle^{(A)}|0\rangle^{(Tr)}|0\rangle^{(B)} = |0\rangle^{(A)}|1\rangle^{(Tr)}|0\rangle^{(B)}. \tag{3}
\]

**Step 3:** If Bob wishes to transmit a 0-bit, he makes sure that there are no detectors in the upper paths of the IFM device, i.e. in his laboratory. After the particle has entered the Transmission Line it hits a beam-splitter, after which some of the wavefunction travels to Bob’s Laboratory. The beam-splitter angle is set to \( \theta = \pi/2N \). The wavepacket falls on the beam-splitter \( N \) times and the following evolution takes place:

\[
a_{(Tr)}^\dagger |0\rangle^{(A)}|0\rangle^{(Tr)}|0\rangle^{(B)} \rightarrow \frac{1}{\sqrt{2N}} i a_{(B)}^\dagger |0\rangle^{(A)}|0\rangle^{(Tr)}|1\rangle^{(B)}.
\]

**Step 4:** The protocol transfers whatever is left in the Transmission Line back to Alice’s Laboratory by applying the operator \( a_{(Tr)}^\dagger a_{(Tr)}^\dagger \). In this scenario that leads to:

\[
a_{(Tr)}^\dagger a_{(Tr)}^\dagger |0\rangle^{(A)}|0\rangle^{(Tr)}|1\rangle^{(B)} = 0.
\]

**Step 5:** Alice applies a number operator, \( a_{(A)}^\dagger a_{(A)} \), to her state and notes down the outcome. She will find that there is no particle in her domain. Bob empties his laboratory.

(b) The 1-Bit Process:

If Bob instead wishes to transmit a 1-bit to Alice, the step after **Step 2** is instead given by:

**Step 3:** Bob inserts detectors in his laboratory i.e. in the upper IFM path. This causes collapse of the parts of the wavefunction that enter Bob’s Laboratory and dist-
ables the self-interference of the interrogating particle.

\[
a_{(Tr)}^\dagger |0\rangle^{(A)}|0\rangle^{(Tr)}|0\rangle^{(B)} \rightarrow \frac{1}{\sqrt{2N}} i a_{(B)}^\dagger |0\rangle^{(A)}|0\rangle^{(Tr)}|1\rangle^{(B)}.
\]

In order to evaluate the interaction-freeness of our protocol, we can ask ourselves: How does a quantum particle travel through the Hilbert space, \( \mathcal{H}^{(A)} \oplus \mathcal{H}^{(Tr)} \oplus \mathcal{H}^{(B)} \), during our protocol? To answer this question we numerically solve the TDSE of a massive one-particle Hamiltonian that has been tailored to implement the above outlined scheme. The solution is obtained using an accelerated Staggered Leapfrog algorithm as in Ref. [30]. The wavefunction evolution is outlined in Fig. [3]

The wavepacket is plotted at successive time frames (top to bottom). The particle is initialised in Alice’s

**IV. NUMERICAL DEMONSTRATION**
FIG. 3. (color online) This figure outlines the quantum evolution of the probability density distribution (solid red curve) of the 0-bit and 1-bit process in (a) and (b) respectively. The yellow line (at \( x = 3.5 \)) indicates the beam-splitter, the dotted green line shows the potential and the black dashed lines show the spatial divisions. The figure is further explained in the text.

It becomes evident that, unless an error occurs, the wavefunction never evolves from Bob’s space into Alice’s. In the scenario of perfect channels and beam-splitters, weak measurements at any part of Bob’s Laboratory will leave a measurable impact on the particles used in the 0-bit process. However, for weak measurements, such particles still end up at Bob’s Laboratory with a probability approaching unity. We thus conclude that the protocol is fully interaction-free from Alice’s perspective. Furthermore, we coin the term “Weak-Trace-Free Quantum Counterfactual Communication” to describe this phenomenon. A summary is given in FIG. 4.

We wish to highlight the fact that the previous attempt to realise counterfactual communication by Salih et al. [12] aimed at excluding any particles travelling between Alice and Bob. Our scheme does not do that. Particles do travel from Alice to Bob. However, Bob’s message and Alice’s particles are counterpropagating. We use Penrose’s original definition (that counterfactuals are “things that might have happened, although they did not in fact happen”) [41] and thus conclude that: from the receiver’s perspective our protocol should be considered as fully counterfactual, as no particles actually traveled to it from the message source.

V. ERRORS AND VIOLATIONS OF INTERACTION-FREEDOM

It is experimentally challenging to stack a large number of beam-splitters. Furthermore, these beam-splitters naturally suffer from uncertainties in the unitary evolution. Hence, we now address the issue of the failure probabilities of the 0-bit and 1-bit processes: \( P_{\text{fail}}^0 \) and \( P_{\text{fail}}^1 \). For reasonable values of \( N \) and high-fidelity beam-splitters, the nature of these probabilities causes the failure rate of the 1-bit to be substantial and that \( P_{\text{fail}}^0 < P_{\text{fail}}^1 \). However, we suggest an encoding such that a detection of one or more particles in Alice’s Laboratory, out of \( M \) processes, would constitute a logical 1. The logical 0 would be the scenario of no detections. The respective failure probabilities will then change such that \( P_{\text{fail},M}^0 = (P_{\text{fail}}^0)^M \) and \( P_{\text{fail},M}^1 = (P_{\text{fail}}^1)^M \). Whilst the failure probability of the logical 0-process increases with increasing \( M \), that of the logical 1-process falls. Both failures generate bit errors, however, only the logical 0-process failure generates a violation to the interaction-freeness of the protocol. Their respective sig-
FIG. 4. (color online) The flow of particles and information in (a) classical communication schemes and in (b) weak-trace-free quantum counterfactual communication. The two parts of the Transmission Line are separated by a beam-splitter. In both cases information flows from Bob to Alice.

FIG. 5. (color online) Bit error rate (solid) and interaction-free violation rate (dotted) as functions of the process encoding number, $M$. The beam-splitter angle, $\theta = \pi/2N$, was given a standard deviation of $\sigma_\theta = 0.01$ rad. (a) and (b) shows simulations of devices with $N = 2$ and $N = 7$ beam-splitters respectively.

VI. CONCLUDING REMARKS

In this paper we have outlined a weak-trace-free quantum counterfactual communication protocol that contradicts the classical perception of communication [14], by enabling the travel of information from Bob to Alice without any wavefunction travelling from Bob to Alice. Our protocol builds on interaction-free measurement devices [9, 37] and by numerically solving the Schrödinger equation we have demonstrated how it is realistically implementable with just a few beam-splitters. The protocol does not utilise nested MZIs as in previous [12] controversial suggestions for counterfactual communication. Numerical simulations show that—in the limit of perfect beam-splitters—our protocol does not have even infinitesimal parts of the wavefunction travelling from Bob’s Laboratory to Alice’s. Hence, it is immune to the weak-trace criticism of previous protocols [26]. Furthermore, whilst a substantial fraction of the individual 1-bit processes might fail, we show how the logical bits can be redefined in terms of many processes such that the failure probability is only limited by the fidelity of the quantum channels and the unitary operations of the beam-splitters. The protocol is well within the realisable scope of quantum optics and we highly recommend experimental groups to pursue our work.

The authors would like to express their gratitude towards Edmund Owen and Jacek Mosakowski for helpful discussions. This work was supported by the EPSRC and the Cambridge Laboratory of Hitachi Limited via Project for Developing Innovation Systems of the MEXT in Japan.

[1] J. S. Bell, Physics 1, 195 (1964).
[2] L. Hardy, Phys. Rev. Lett. 68, 2981 (1992).
[3] S. Wiesner, SIGACT News 15, 78 (1983).
[4] R. P. Feynman, International Journal of Theoretical Physics 21, 467 (1982).
[5] *Quantum cryptography: Public key distribution and coin tossing*, Vol. 175 (1984).
[6] A. K. Ekert, Phys. Rev. Lett. 67, 661 (1991).
[7] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, (1993).
