Counterfactual quantum indistinguishability

Vinod N. Rao,1,2,∗ Anindita Banerjee,3 and R. Srikanth1,†
1Theoretical Sciences Division, Poornaprajna Institute of Scientific Research, Bengaluru - 562164, India
2Graduate Studies, Manipal Academy of Higher Education, Manipal - 576104, India
3Centre of Development of Advanced Computing, Corporate Research and Development, Pune - 411008, India

Quantum indistinguishability and counterfactuality are two counterintuitive features of quantum mechanics. The latter refers to the possibility of detecting a particle without an interaction, whilst the former to the indistinguishability of identical particles. In this work, we describe a phenomenon, that we call “counterfactual indistinguishability”, which combines these two features, and whereby the detection of a particle at a given station indicates a blockade on an indistinguishable particle elsewhere. From a foundational perspective, it is of interest to note that despite being a multi-particle phenomenon, this is ideally realized using single-photon (rather than multi-photon) interference.

I. INTRODUCTION

Interaction-free measurement (IFM) is a counterintuitive feature of quantum mechanics that enables detecting the presence of an object without interacting with it [1]. Since its discovery, various applications of IFM have been identified in quantum information processing, leading to so-called counterfactual quantum key distribution [2–5], direct communication [6, 7], quantum computation [8], certificate authorization [9] and others [10].

The basic principle behind IFM is paradigmatically explained using the Mach-Zehnder (MZ) interferometer. A photon incident on the MZ interferometer is split at a beam-splitter, and re-interfered at a second splitter, leading to a detection at a specific output port owing to destructive interference. However, if an obstacle is inserted in one of the arms, the consequent disruption of the destructive interference leads to a possible detection at the other output port. Counterfactuality or IFM refers to this feature whereby the presence of an obstacle on one interferometric arm is revealed by a measuring device placed elsewhere.

Yet another counterintuitive feature of quantum mechanics is the indistinguishability of identical particles, which is responsible for the Hong-Ou-Mandel effect [11], bosonic stimulation [12], boson sampling [13], among others. Here, the indistinguishability is enforced through the (anti-)symmetrization conditions \( \{ a_j, a_k \} = \delta_{j,k} \) (resp., \( \{ a_j, a_k^\dagger \} = \delta_{j,k} \)) in the case of bosons (resp., fermions), where the subscripts \( j \) and \( k \) refer to the two modes of the quantum field.

In this work, we propose the idea of “IFM-by-proxy”, which is a fundamental modification of IFM that combines counterfactuality and indistinguishability. Under IFM-by-proxy, the presence of an obstacle on a particle’s path is revealed by a measurement made elsewhere, on another particle that is indistinguishable with the first particle. Even though IFM-by-proxy involves two or more particles, yet paradoxically it turns out to be a single-particle interference effect in the ideal case. We refer to this aspect of quantum indistinguishability brought forth by IFM-by-proxy as counterfactual indistinguishability, which will be distinguished from the usual aspect of indistinguishability, mentioned in the preceding paragraph.

This article is organized as follows. A practical scheme for observing IFM-by-proxy using attenuated coherent pulses is presented in Sec. II. An idealization thereof is explored in Sec. III. A generalization of the experimental idea to a three-pulse interference and beyond is given in Section IV. Finally, we present discussions and conclusions in Sec. V, where we briefly indicate potential experimental parameters that are suitable to realize the proposed experiment.

II. INTERACTION-FREE MEASUREMENT BASED ON INDISTINGUISHABILITY

We consider the following variant of IFM involving a modified MZ interferometer, as depicted in Fig. 1. One of the arms (labelled \( l \)) is longer than the other (labelled \( s \)), with the path length difference between the two denoted \( \delta \). A retractable obstacle \( O \) is present in the long arm. The condition \( \delta > 0 \) ensures that when a light pulse is incident on the first beam-splitter BS₁, the resulting two partial waves will not recombine at the second beam-splitter BS₂. Thus, the conventional IFM is ruled out.

Suppose a train of \( N \) identical, attenuated coherent pulses, labelled with time stamp \( t_n \), where \( n = \{ 1, 2, 3, \ldots, N \} \), is incident on BS₁. Consecutive pulses are spaced by a constant interval of \( \delta \), which ensures that the partial wave of \( (j) \)-th pulse traveling via the short arm and that of \( (j-1) \)-th pulse traveling via the long arm, are incident at the same time on BS₂.

The state of the train is given by:

\[
|\Psi\rangle = \bigotimes_{j=1}^{N} |\alpha e^{i\phi_j}\rangle,
\]

where \(|\alpha|^2\) is the mean photon number of the train and...
\( \phi_j \) is the initial phase of the state, which we set to \( \phi_j = 0 \) to begin with. If \( \hat{a}^\dagger \) denotes the creation operator for the input mode, then the transformation at BS1 is given by:

\[
\hat{a}^\dagger_n \rightarrow \frac{1}{\sqrt{2}} (\hat{b}^\dagger_n + i\hat{s}^\dagger_n),
\]

where \( \hat{b}_n^\dagger \) and \( \hat{s}_n^\dagger \) are the creation operators of the respective arms of the interferometer. Similarly, the transformations at BS2 are

\[
\hat{b}^\dagger_n \rightarrow \frac{1}{\sqrt{2}} (\hat{c}^\dagger_n + i\hat{d}^\dagger_n),
\]

and \( \hat{s}^\dagger_n \rightarrow \frac{1}{\sqrt{2}} (\hat{c}^\dagger_n + i\hat{d}^\dagger_n) \), where \( \hat{c}_n^\dagger \) and \( \hat{d}_n^\dagger \) are the creation operators of the respective output ports.

The action of a beam-splitter on coherent states \(|\alpha\rangle\) and \(|\beta\rangle\) incident on its two input ports is given by

\[
|\alpha\rangle|\beta\rangle \xrightarrow{\text{BS}} \frac{1}{\sqrt{2}} (|\alpha + i\beta\rangle + |\alpha - i\beta\rangle).
\]

Accordingly, at BS1, for the \(j\)-th pulse, we have \(|\alpha\rangle_j |\text{vac}\rangle \xrightarrow{\text{BS}1} |\alpha\rangle_{j,c} |\text{vac}\rangle_{j,d} \).

Consider the case when obstacle \(O\) (Fig. 1) is absent in the arm \(l\). On account of the path difference, the partial waves of two consecutive pulses meet, and we have

\[
|\alpha\rangle_{j,s} |\text{vac}\rangle_{j-1,l} \xrightarrow{\text{BS}2} |\alpha\rangle_{j,c} |\text{vac}\rangle_{j,d}, \tag{2}
\]

implying that there can be a detection at detector \(D_1\) and none at \(D_2\). We note that in Eq. (2) the interfering partial waves at BS2 belong to two consecutive pulses. Therefore, the quantum indistinguishability of the photons in the pulses is crucial for this interference to happen.

If obstacle \(O\) is inserted, then the pulse amplitude in arm \(l\) is blocked. Therefore, in place of Eq. (2), we have

\[
|\alpha\rangle_{j,s} |\text{vac}\rangle_{j-1,l} \xrightarrow{\text{BS}2} \frac{|\alpha\rangle}{\sqrt{2}}_{j,c} |\text{vac}\rangle_{j,d}, \tag{3}
\]

showing that there could be a detection at detector \(D_2\) as well. This measurement of \(O\) is indeed counterfactual in the sense that the detection at \(D_2\) entails the presence of a blocking action elsewhere. Letting \(|\alpha|^2 \ll 1\), typically \(|\alpha|^2 = 0.1\), the probability \(P_0\) that there is no detection at \(O\) conditioned on a detection at \(D_2\), is given by \(P_0 \approx 1 - \frac{1}{2}|\alpha|^2 = 0.95\). Thus, strictly speaking, the measurement of \(O\) is not interaction-free.

In conventional IFM, the detection of a particle at one place indicates its blocking elsewhere. Indeed, this non-local element is present here also. Additionally, the measurement of the \((j)\)-th pulse can indicate the blocking (elsewhere) of another pulse, namely the \((j-1)\)-th. As noted earlier, it seems natural to refer to this type of measurement as “IFM-by-proxy” or “proxy counterfactual”, in that the measured \((j)\)-th pulse acts as a proxy for another \((j-1)\)-th pulse, such that the measurement of the former pulse could indicate the presence of a blockade in the path of the latter pulse.

If the two converging partial waves at BS2 were distinguishable (say, possessing different wavelengths, or one particle being a photon and the other a neutron), then they would not interfere at BS2, and therefore lead to any of the four possible detections (namely, both at \(D_1\) or both at \(D_2\) or one at each). Thus, the interference in Eq. (2) implies that the photons of the two pulses meeting at BS2 are indistinguishable. This aspect of quantum indistinguishability that is responsible for IFM-by-proxy constitutes counterfactual indistinguishability, a simple but intimate union of quantum indistinguishability and quantum counterfactuality.

### III. TOWARDS AN IDEAL IFM-BY-PROXY

We noted in the preceding section that there is a non-zero probability of detection both at \(D_2\) (this being counterfactual) and also at obstacle \(O\), owing to the presence of multiphotons in the coherent pulse. As a result, the measurement here is not strictly interaction-free. We now point out how one may in principle realize an ideal IFM-by-proxy.

It is not hard to show that the ideal IFM-by-proxy can be realized if the train of \(N\) pulses in Eq. (1) is replaced by the following “tensor sum” train:

\[
\hat{Q}_N |\text{vac}\rangle \equiv \frac{1}{\sqrt{N}} \sum_{n=1}^{N} \hat{a}^\dagger_n |\text{vac}\rangle. \tag{4}
\]

If this state is input into the setup of Fig. 1, then it outputs a photon at \(D_1\) with unit probability in the absence of \(O\), and with probability \(1/2\) if \(O\) is inserted. Moreover, in the latter case a detection at \(O\) and at \(D_1\) or \(D_2\) is mutually exclusive. Thus this setup realizes an ideal IFM-by-proxy.

The state Eq. (4) can be engineered from the state Eq. (1) by means of suitable nonlinear filtering, as explained below. We note that Eq. (1) can be written as

\[
|\Psi\rangle = \sum_{j=0}^{\infty} \frac{N^{j/2}}{\sqrt{j!}} |\alpha|^j (\hat{Q}_N)^j |\text{vac}\rangle. \tag{5}
\]
It follows that the required filtering operation is one that takes a train of $N$ pulses initially in the state Eq. (1), and probabilistically outputs the state Eq. (4) by eliminating the terms corresponding to $j = 0$ (vacuum) and $j > 1$ (higher-order excitations).

Interestingly, the (ideal) IFM-by-proxy can be understood using just “first quantization” arguments. In particular, the statement of quantum indistinguishability based on the commutation relation $\{c_n^\dagger, d_m\} = 0$ doesn’t need to be invoked. Let the electric field operators corresponding to detectors $D_1$ and $D_2$ be given by (up to a global phase)

\[
\begin{align*}
\hat{c}_n(t_n) &= \frac{1}{\sqrt{2}}(i\hat{d}_{n-1}e^{i(k\delta-\omega t_{n-1})} + i\hat{s}_ne^{-i\omega t_n}), \\
\hat{d}_n(t_n) &= \frac{1}{\sqrt{2}}(i\hat{d}_{n-1}e^{i(k\delta-\omega t_{n-1})} + \hat{s}_ne^{-i\omega t_n}),
\end{align*}
\]

where $\omega$ and $k$ denote the angular frequency and wave number of the mode, respectively. The probability of detection of a photon at detector $D_1$ at time $t_n$ is given by

\[
\langle \hat{c}_n(t_n)\hat{c}_n^\dagger(t_n) \rangle = \frac{1}{2}(1 + \cos \left[k\delta - \omega(t_{n-1} - t_n)\right]).
\]

Since $k\delta = \omega(t_{n-1} - t_n)$, this interference is like that in a conventional MZ interferometer, except that the two partial waves that converge at BS$_2$ belong to two distinct (consecutive) pulses.

In this sense, even though we have here a two-photon situation, the ideal IFM-by-proxy realizes single-photon interference, rather than two-photon interference. In this light, it seems more apt to attribute counterfactual indistinguishability to photonic non-individuality within the mode, and not to (anti-)symmetrization condition. This type of indistinguishability may be differentiated from the “conventional” photonic indistinguishability indicated, for example, in the Hong-Ou-Mandel effect or bosonic sampling, where there is a genuine two-photon or multi-photon interference. In the former case, there is a cancellation of the two-photon amplitude for both particles being transmitted through a beam-splitter and that for both being reflected.

In place of the train of coherent pulses as in Eq. (1), suppose we have a train of single photons. This would be described by the state:

\[
|\Phi\rangle = \bigotimes_{n=1}^N \hat{d}_n^\dagger \ket{\text{vac}}
\]

in place of the state Eq. (4) i.e., replacing the tensor sum with a tensor product (apart from the normalization factor). The state Eq. (9) leads to a probabilistic Hong-Ou-Mandel effect, and not to the “single-particle” interference that is the basis of the IFM-by-proxy.

### IV. COUNTERFACTUAL QUANTUM INDISTINGUISHABILITY WITH MULTIPLE CONSECUTIVE PULSES

The principle of IFM-by-proxy can be straightforwardly extended to a situation where multiple pulses interfere in an interferometric setup. Consider the case of an analogous single-photon interference in a 3-pulse scenario. A similar setup as in Fig. 1 can be considered, but with three consecutive pulses being interfered. For example, the beam-splitters of Fig. 1 are replaced by triters (three-way beam-splitters) described by the unitary action

\[
U_3 = \begin{pmatrix}
\frac{1}{\sqrt{2}} & i & -\frac{1}{\sqrt{2}} \\
\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\
0 & 0 & \frac{1}{\sqrt{2}}
\end{pmatrix}.
\]

In general, any $n$-input $n$-output splitter can be realized by a cascaded setup of $U_2$ [14]. A proxy counterfactual setup incorporating the tritter transformation of Eq. (10) realized through a two-interferometer cascaded setup is depicted in Fig. 2.

In the absence of a retractable obstacle $O$, only a $D_1$ detection occurs for the train of pulses given in Eq. (1). To show this, note that the state of the fields after BS$_1$ and BS$_2$ is given by:

\[
|\psi\rangle = \left| \frac{\alpha}{\sqrt{2}} \right\rangle_{j,s} \left| -\frac{\alpha}{2} \right\rangle_{j-1,m} \left| \frac{\alpha}{2} \right\rangle_{j-2,l}
\]

\[
\xrightarrow{\text{BS}_3} \left| \frac{\alpha}{\sqrt{2}} \right\rangle_{j,s} \left| -\frac{\alpha}{\sqrt{2}} \right\rangle_{j,s} |\text{vac}\rangle_{s,b}
\]

\[
\xrightarrow{\text{BS}_4} |\text{vac}\rangle_{s,e} |\alpha\rangle_{s,d},
\]

where * indicates the superposition of two or more consecutive pulses. Eq. (11a) shows that three sequential pulses are involved in the interference. A phase of $e^{i\pi/2}$ (via a half-wave plate) is assumed to be introduced in the arm $s$ prior to the action of BS$_4$. As follows from Eq. (11), in the absence of the obstacle $O$, detection may happen only at detector $D_1$ and not at $D_2$ or $D_3$.

It follows that a detection at detector $D_2$ or $D_3$ indicates the presence of $O$ on path $l$. This corresponds to a counterfactual measurement of the obstacle. Similarly, an obstacle placed at arm $m$ can also be counterfactually measured. The counterfactual detection is interaction-free with probability $\approx 1 - |\alpha|^2 \approx 0.9$, letting $|\alpha|^2 = 0.1$.

As in the previous case, one may observe ideal IFM-by-proxy by employing the state Eq. (4), rather than a train of coherent pulses.

A potential application of this kind of setup is checking for misalignment or defects in a quantum circuit. For example, suppose we require a quantum circuit that builds on the one given in Fig. 2. Then, before placing the necessary optical elements (such as gates, polarizers, half/full wave plates etc.), one can check for the above interference patterns, such as a detection only at $D_1$ in
the absence of any path defects in arm $l$ or $m$. One can run a defect diagnostics on the circuit by introducing obstacles or certain phase fluctuations and monitoring the detector clicks.

V. DISCUSSION AND CONCLUSION

Interaction-free measurement (IFM) is a counterintuitive feature of quantum interference in which the blocking action by an object is indicated by a measurement outcome elsewhere. Here we have proposed a twist to this situation in which the partial waves in the two interferometric arms belong to two distinct but indistinguishable photons. The IFM in this case is such that the detection pattern pertaining to one photon is able to indicate the presence of an obstacle in the path of another, indistinguishable photon—a case of IFM mediated by a proxy. As the IFM wouldn’t be possible if the interfering particles were distinguishable, this effect corresponds to what may be called counterfactual indistinguishability.

Although this interference effect involves two photons, it does not constitute a two-photon interference, such as occurs in the Hong-Ou-Mandel effect. Instead, paradoxically, it constitutes a single-photon interference effect in that it can be fully described employing only the first-quantization formalism. The aspect of indistinguishability highlighted here is not the exchange symmetry between two or more identical particles, but rather a kind of photonic non-individuality of the particles belonging to a given mode. Finally, we point out that counterfactual indistinguishability is not limited to the case of re-interference of only two pulses, but can be extended to multiple pulses as well.

The experimental setup of Fig. 1 to realize counterfactual quantum indistinguishability is well within the scope of current technology. In particular, it can be built employing the same setup that implements differential-phase-shift (DPS) cryptography, barring the retractable obstacle. We outline a few details of a potential experiment to realize it.

It would incorporate a fiber-coupled laser as the source of coherent light, and one-bit delay line MZ interferometer followed by two single-photon detectors. The path-length difference in the delay-line based MZ interferometer will introduce a one-bit delay corresponding to the $\delta$ value. The choice of the source wavelength is vital to the design of the entire optical path. The source could be a continuous wave (cw) laser diode equipped with an external cavity of 810 nm. This is converted into a pulsed light source by means of a high-speed amplitude modulator placed just behind the cw light source [15]. We may as well employ 1550 nm telecom wavelength, which may be considered mainly for the availability of InGaAs detectors. However, SiAPD may be preferable thanks to its better performance, specifically its higher efficiency of 70%, lower dead-time of 50 ns, etc [16]. Further, the light source should be greatly attenuated using fixed and variable attenuators to the required mean photon number of $|\alpha|^2 \approx 0.1$, which translates to a single detection over 10 consecutive pulses. This degree of attenuation ensures that there is a much higher probability for single-photon events over multi-photon events. The light source is then linked to the MZ interferometer through a single-mode fiber about 2 m long.

In case of the pulsed laser source the interferometer introduces a delay equal to the interval of the neighboring pulses. The stability of the MZ interferometer is a critical part in differential phase detection. The path delay relies upon the characteristics of the light source such as frequency and optical path. It should be tuned to achieve good spatial matching such that most of the time there is at most a single detection event, at one of the detectors or obstacle.

In the context of Fig. 1, the detection occurs at $D_2$ instead of $D_1$ (in the absence of $O$), if the phase difference between two consecutive pulses, $\phi = \pi$. This fact forms the basis of DPS QKD [17], which was an inspiration for the present work. However, DPS QKD does not involve counterfactual measurements, and a key bit is generated conditioned on a detection at $D_1$ or $D_2$. The security of DPS QKD is based on the fact that by choosing very small $|\alpha|^2$, the two possible encoding states can be made sufficiently non-orthogonal, as $\langle \alpha | - \alpha \rangle = e^{-2|\alpha|^2}$ [18, 19]. By contrast, here we require small $|\alpha|^2$ to ensure that the counterfactual effect reduces to IFM proper.

It is known that multiphoton, linear interference can be the basis of a powerful, albeit non-universal, model of quantum computing, since it can be used to sample a probability distribution that is known to be hard to calculate. In particular, the distribution requires calculating the permanent of a matrix based on the unitary that describes a multiport interferometer used for the i-
terference, a problem known to be \#P-hard [13]. By contrast, the single-photon interference that leads to IFM-by-proxy is not expected to give a greater than quadratic speedup, as in Grover search [20], since it can be described by first-quantization principles.

ACKNOWLEDGMENTS

V.N.R. and R.S. acknowledge the support from Interdisciplinary Cyber Physical Systems (ICPS) program of the Department of Science and Technology (DST), India, Grant No. DST/ICPS/QuST/Theme-1/2019/14. V.N.R. acknowledges the support and encouragement from Admar Mutt Education Foundation.

[1] Avshalom C Elitzur and Lev Vaidman, “Quantum mechanical interaction-free measurements,” Foundations of Physics **23**, 987–997 (1993).
[2] Guang-Can Guo and Bao-Sen Shi, “Quantum cryptography based on interaction-free measurement,” Physics Letters A **256**, 109–112 (1999).
[3] Tae-Gon Noh, “Counterfactual quantum cryptography,” Physical Review Letters **103**, 230501 (2009).
[4] H Akshata Shenoy, R Srikanth, and T Srinivas, “Semi-counterfactual cryptography,” Europhysics Letters **103**, 60008 (2013).
[5] Vinod N Rao and R Srikanth, “Noiseless attack and counterfactual security of quantum key distribution,” Physical Review A **104**, 022424 (2021).
[6] Hatim Salih, Zheng-Hong Li, Mohammad Al-Amri, and M Suhail Zubairy, “Protocol for direct counterfactual quantum communication,” Physical review letters **110**, 170502 (2013).
[7] Yakir Aharonov and Lev Vaidman, “Modification of counterfactual communication protocols that eliminates weak particle traces,” Physical Review A **99**, 010103 (2019).
[8] Zhu Cao, “Counterfactual universal quantum computation,” Physical Review A **102**, 052413 (2020).
[9] Akshata Shenoy, R Srikanth, and T Srinivas, “Counterfactual quantum certificate authorization,” Physical Review A **89**, 052307 (2014).
[10] Akshata Shenoy-Hejamadi, Anirban Pathak, and Srikanth Radhakrishna, “Quantum cryptography: key distribution and beyond,” Quanta **6**, 1–47 (2017).
[11] Chong-Ki Hong, Zhe-Yu Ou, and Leonard Mandel, “Measurement of subpicosecond time intervals between two photons by interference,” Physical Review Letters **59**, 2044 (1987).
[12] H Akshata Shenoy, R Srikanth, and T Srinivas, “Efficient quantum random number generation using quantum indistinguishability,” Fluctuation and Noise Letters **12**, 1350020 (2013).
[13] Scott Aaronson and Alex Arkhipov, “The computational complexity of linear optics,” in *Proceedings of the forty-third annual ACM symposium on Theory of computing* (2011) pp. 333–342.
[14] Michael Reck, Anton Zeilinger, Herbert J Bernstein, and Philip Bertani, “Experimental realization of any discrete unitary operator,” Physical review letters **73**, 58 (1994).
[15] Qiang Zhang, Hiroki Takesue, Toshimori Honjo, Kai Wen, Toru Hirohata, Motohiro Suyama, Yoshihiro Takiguchi, Hidehiko Kamada, Yashuhiro Tokura, Osamu Tadanaga, *et al.*, “Megabits secure key rate quantum key distribution,” New Journal of Physics **11**, 045010 (2009).
[16] Hiroki Takesue, Eleen Diamanti, Carsten Langrock, MM Fejer, and Yoshihisa Yamamoto, “10-gghz clock differential phase shift quantum key distribution experiment,” Optics express **14**, 9522–9530 (2006).
[17] K Inoue, E Waks, and Y Yamamoto, “Differential-phase-shift quantum key distribution using coherent light,” Physical Review A **68**, 022317 (2003).
[18] Edo Waks, Hiroki Takesue, and Yoshihisa Yamamoto, “Security of differential-phase-shift quantum key distribution against individual attacks,” Physical Review A **73**, 012344 (2006).
[19] Tobias Moroder, Marcos Curty, Charles Ci Wen Lim, Hugo Zbinden, and Nicolas Gisin, “Security of distributed-phase-reference quantum key distribution,” Physical review letters **109**, 260501 (2012).
[20] Charles H Bennett, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani, “Strengths and weaknesses of quantum computing,” SIAM journal on Computing **26**, 1510–1523 (1997).