SWAP test and Hong-Ou-Mandel effect are equivalent

Juan Carlos Garcia-Escartin* and Pedro Chamorro-Posada

Universidad de Valladolid, Departamento Teoría de la Señal e Ingeniería Telemática, Paseo Belén No. 15, 47011 Valladolid, Spain

(Received 27 March 2013; published 29 May 2013)

We show that the Hong-Ou-Mandel effect from quantum optics is equivalent to the SWAP test, a quantum information primitive which compares two arbitrary states. We first derive a destructive SWAP test that does not need the ancillary qubit that appears in the usual quantum circuit. Then we study the Hong-Ou-Mandel effect for two photons meeting at a beam splitter and prove it is, in fact, an optical implementation of the destructive SWAP test. This result offers both an interesting simple realization of a powerful quantum information primitive and an alternative way to understand and analyze the Hong-Ou-Mandel effect.

DOI: 10.1103/PhysRevA.87.052330 PACS number(s): 03.67.Ac, 42.50.Ex

I. INTRODUCTION

Quantum information has provided a new way to think about quantum mechanics. Its formalism draws heavily from quantum optics and many interesting results come from the interplay between both disciplines. Bell inequalities and Bell tests can be more clearly understood in a computational framework [1]. Simple quantum information protocols, such as quantum cryptography, are naturally realized with optical systems [2,3]. Many quantum algorithms are also directly inspired by physical phenomena. For instance, Grover's algorithm for quantum search is based on Schrödinger's equation [4].

In this paper, we show how quantum information has "rediscovered" the Hong-Ou-Mandel effect of quantum optics under the name of SWAP test. We show there is a deep connection between these two concepts. On the way, we propose a SWAP test circuit that does not need any ancillary input and suggest practical realizations of this test using photons, a beam splitter, and two detectors.

The paper has five main sections. In Sec. II, we describe the SWAP test and its uses in state comparison. In Sec. III, we review the Hong-Ou-Mandel effect for two photons and give a formulation that highlights the role of the information the photons carry. In Sec. IV, we derive a destructive SWAP test circuit with no ancillas. Section V shows that the Hong-Ou-Mandel effect corresponds to a destructive, simplified optical SWAP test circuit. Finally, in Sec. VI, we outline the possible applications of these results and propose experimental systems that put these connections into practical use.

II. THE SWAP TEST

When working with quantum information, the question often arises of whether two states $|\phi\rangle$ and $|\psi\rangle$ are equal or not. The SWAP test is a procedure from which we can determine with certainty that two states are different. Equality can be inferred with high probability if we have multiple copies of the states. The quantum circuit used in the test, introduced in the context of quantum fingerprinting [5], is shown in Fig. 1. The inputs are two states $|\psi\rangle$ and $|\phi\rangle$ of equal dimension and an ancillary qubit in the $|0\rangle$ state. There are three gates, two Hadamard gates, H, and a controlled SWAP gate, CSWAP. The Hadamard gates convert the $|0\rangle$ state into a superposition $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|1\rangle$ into $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$. The controlled SWAP operation interchanges the states $|\phi\rangle$ and $|\psi\rangle$ if the ancillary qubit is in state $|1\rangle$. When the ancillary qubit is $|0\rangle$, the other states keep their order. The evolution through this circuit is

$$\begin{aligned}|0\rangle|\phi\rangle|\psi\rangle &\xrightarrow{H} \frac{|0\rangle+|1\rangle}{\sqrt{2}}|\phi\rangle|\psi\rangle \xrightarrow{\text{CSWAP}} \frac{|0\rangle|\phi\rangle|\psi\rangle+|1\rangle|\psi\rangle|\phi\rangle}{\sqrt{2}}\\ &\xrightarrow{H} \frac{|0\rangle[|\phi\rangle|\psi\rangle+|\psi\rangle|\phi\rangle]+|1\rangle[|\phi\rangle|\psi\rangle-|\psi\rangle|\phi\rangle]}{2}.\end{aligned} \tag{1}$$

At the end of the circuit, the state of the ancillary qubit is measured. We call outcome 0 the case where the $|0\rangle$ state is found and outcome 1 when $|1\rangle$ is measured. If the states are equal, $|\phi\rangle=|\psi\rangle$, the outcome is 0 with probability 1. Swapping the positions has no effect and there is no entanglement with the ancillary qubit. For different states both outcomes are possible. Outcome 1 can only happen for different states. In that case, we say the states "fail" the test. If two states fail the test, we know with certainty they are different. If the states "pass" the test (outcome 0), they are not necessarily equal. From Eq. (1), we can find that the probability of passing the test is

$$\begin{aligned}P_p &= \frac{1}{4}(\langle\phi|\langle\psi|+\langle\psi|\langle\phi|)(|\phi\rangle|\psi\rangle+|\psi\rangle|\phi\rangle)\\ &= \frac{1+|\langle\psi|\phi\rangle|^2}{2}.\end{aligned} \tag{2}$$

The probability of failure is the complementary $P_f=\frac{1-|\langle\psi|\phi\rangle|^2}{2}$. The test is valid only as a comparison of independent input states. If the inputs are entangled, the state must be taken as a whole and it makes no sense to speak of a comparison.

The probability of passing the test depends on the overlap $|\langle\psi|\phi\rangle|^2$ of the input states. The overlap gives a good estimate of how close two states are. For two orthogonal states, $|\langle\psi|\phi\rangle|^2=0$ and $P_p=P_f=\frac{1}{2}$. For nonorthogonal states, the closer they are, the greater the probability of passing the test. If we have n copies of the two input states, we can repeat the test. The probability of passing the n rounds is

$$\left(\frac{1+|\langle\psi|\phi\rangle|^2}{2}\right)^n. \tag{3}$$

*juagar@tel.uva.es

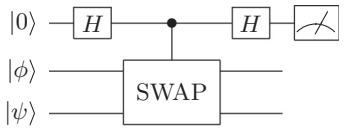

FIG. 1. Quantum circuit implementing the SWAP test.

If the state passes the test multiple times, we can infer with high probability they are equal or, at least, have a large overlap. We can estimate the number of tests we need to tell apart two states which are arbitrarily close so that $|\langle\psi|\phi\rangle|^2 = 1-\epsilon$, with $\epsilon \ll 1$. With this overlap, $P_p = \frac{2-\epsilon}{2}$ and the probability of passing n tests is $(1-\frac{\epsilon}{2})^n \approx 1-\frac{n\epsilon}{2}$.

One important detail of the SWAP test is the output state after measuring the ancillary qubit. For outcome 0, we have an entangled state $|0\rangle\frac{|\phi\rangle|\psi\rangle+|\psi\rangle|\phi\rangle}{\sqrt{2}}$ and for outcome 1, $|1\rangle\frac{|\phi\rangle|\psi\rangle-|\psi\rangle|\phi\rangle}{\sqrt{2}}$. In both cases, it is impossible to completely separate the input states again. If it were possible, the SWAP test could be repeated as many times as desired. This would make it possible to distinguish arbitrarily close states. It is easy to see why this must be wrong. If the states could be recycled, we could choose a set of states $\{|\psi_1\rangle,|\psi_2\rangle,\ldots,|\psi_N\rangle\}$ as large as we want and, for an unknown state $|\psi_i\rangle$, we could try each of them until we find an outcome 1. After a defined number of tries, the index i of the chosen state could be deduced with high probability. This method makes it possible to send an arbitrarily large amount of information encoded in a state of a finite dimension. This violates the Holevo bound, which gives a limit of $\log_2 d$ bits for a d-dimensional system [6,7].

Due to this confusion of states at the output, the protocols that use the SWAP test do no further work on them. The output can be measured without any effect on the protocol. This motivates our search for a simpler test with no ancillary qubit and where the output is measured destroying any superposition. In Sec. IV, we describe an ancilla-free test using standard quantum gates, but, first, we show a simple optical system which already gives a destructive quantum state comparison.

III. THE HONG-OU-MANDEL EFFECT

The Hong-Ou-Mandel (HOM) effect of quantum optics offers a straightforward way to compare the state of two photons. The phenomenon was originally proposed as a way to find nanosecond time shifts between two photons [8], but, in its full generality, it can help to detect any other difference, like frequency shifts or other changes in the wave function.

We can describe the phenomenon by looking at the behavior of photons when they cross a beam splitter. We imagine a photon in state $|1^s\rangle$ which can take two paths, up and down. We use the notation $|n^s\rangle_p$ to denote a photon number state $|n\rangle$ in mode s_p. Mode s_p describes a photon with a certain state $|s\rangle$ which can include polarization or frequency, while subindex p is reserved to specify the path (spatial mode), which can be up $|1^s\rangle_U$ or down $|1^s\rangle_D$. The vacuum state (zero photon number) is represented as $|0\rangle_U$ or $|0\rangle_D$. All the modes s have the same vacuum state (all empty modes are the same).

For a 50:50 beam splitter we have the evolution

$$|1^s\rangle_U|0\rangle_D \longrightarrow \frac{|1^s\rangle_U|0\rangle_D + |0\rangle_U|1^s\rangle_D}{\sqrt{2}} \tag{4}$$

and

$$|0\rangle_U|1^s\rangle_D \longrightarrow \frac{|1^s\rangle_U|0\rangle_D - |0\rangle_U|1^s\rangle_D}{\sqrt{2}}. \tag{5}$$

For single photons, this is the equivalent to an H gate where we replace logic states $|0\rangle$ and $|1\rangle$ with $|1^s\rangle_U|0\rangle_D$ and $|0\rangle_U|1^s\rangle_D$, respectively. If we place two detectors D_1 and D_2, one up and one down, each can "click" (find the photon) with a probability $\frac{1}{2}$.

If we have two photons in orthogonal modes $|1^s\rangle$ and $|1^t\rangle$, with $\langle 1^s|1^t\rangle = 0$, that enter the beam splitter one up and one down, they evolve independently. The final click statistics in the detectors can be deduced from those of the individual photons. When D_1 and D_2 click at the same time, or, in practice, in the same short time window, we say there is a *coincidence*. An interesting phenomenon appears when the input photon states have an overlap $\langle 1^s|1^t\rangle \neq 0$. Photons in the same state bunch together at the output. The simplest case occurs for two indistinguishable input photon states.

We can describe the general evolution inside a beam splitter or any other linear optics element from its scattering matrix. We use photon creation operators $\hat{a}^\dagger_{s,p}$ such that

$$\hat{a}^\dagger_{s,p}|n^s\rangle_p = \sqrt{n+1}|n+1^s\rangle_p. \tag{6}$$

A state $|n^s\rangle_p$ can be written as [9]

$$|n^s\rangle_p = \frac{(\hat{a}^\dagger_{s,p})^n}{\sqrt{n!}}|0\rangle_p. \tag{7}$$

The creation operators of independent modes (orthogonal photon states) commute. In the Heisenberg picture, we can study the evolution of a quantum system from the evolution of an operator acting on the same initial state. If the evolution is defined by a unitary operator U and we have an input photon in state $|1^s\rangle_p = \hat{a}^\dagger_{s,p}|0\rangle_p$, the output after the beam splitter can be written as $(U\hat{a}^\dagger_{s,p}U^\dagger)|0\rangle_p$. We concentrate on the evolution of the operator. From the scattering matrix of a 50:50 beam splitter, it can be shown that the creation operators evolve as [10]

$$U\hat{a}^\dagger_{s,U}U^\dagger \longrightarrow \frac{1}{\sqrt{2}}\hat{a}^\dagger_{s,U} + \frac{1}{\sqrt{2}}\hat{a}^\dagger_{s,D}, \tag{8}$$

$$U\hat{a}^\dagger_{s,D}U^\dagger \longrightarrow \frac{1}{\sqrt{2}}\hat{a}^\dagger_{s,U} - \frac{1}{\sqrt{2}}\hat{a}^\dagger_{s,D}. \tag{9}$$

For two equal photons giving an input state

$$|1^s\rangle_U|1^s\rangle_D = \hat{a}^\dagger_{s,U}\hat{a}^\dagger_{s,D}|0\rangle_U|0\rangle_D, \tag{10}$$

we have at the output

$$\begin{aligned} U\hat{a}^\dagger_{s,U}\hat{a}^\dagger_{s,D}U^\dagger|0\rangle_U|0\rangle_D &= (U\hat{a}^\dagger_{s,U}U^\dagger)(U\hat{a}^\dagger_{s,D}U^\dagger)|0\rangle_U|0\rangle_D \\ &= \tfrac{1}{2}[(\hat{a}^\dagger_{s,U})^2 - \hat{a}^\dagger_{s,U}\hat{a}^\dagger_{s,D} + \hat{a}^\dagger_{s,D}\hat{a}^\dagger_{s,U} \\ &\quad - (\hat{a}^\dagger_{s,D})^2]|0\rangle_U|0\rangle_D. \end{aligned} \tag{11}$$

For modes U and D the creation operators commute and the output state is

$$\frac{(\hat{a}^\dagger_{s,U})^2-(\hat{a}^\dagger_{s,D})^2}{2}|0\rangle_U|0\rangle_D, \tag{12}$$

which, from (6), is

$$\frac{|2^s\rangle_U|0\rangle_D-|0\rangle_U|2^s\rangle_D}{\sqrt{2}}. \tag{13}$$

Due to interference, both photons leave the beam splitter through the same port. Both detectors have an equal probability of clicking, but the number of coincidences becomes zero.

For photons with continuous wave-packet amplitude functions $\xi_1(t)$ and $\xi_2(t)$ at the input of a 50:50 beam splitter, the probability of finding a coincidence is known to be [9]

$$\frac{1-|\int \xi_1(t)^*\xi_2(t)\,dt|^2}{2}. \tag{14}$$

The term $|\int \xi_1(t)^*\xi_2(t)\,dt|$ is the overlap of the two photon states. The photons are found in the same output port with the same probability,

$$\frac{1+|\int \xi_1(t)^*\xi_2(t)\,dt|^2}{4}, \tag{15}$$

for each detector. The photons have the same behavior as the input states in the SWAP test. In the following section, we derive the same results for discrete systems which correspond naturally to the qubit or qudit case. Later, we discuss the equivalence of the discrete case to the general expression with the wave-packet amplitude functions. We study the system from the point of view of discrete photon creation operators. An alternative general proof with density matrices which includes mixed states can be found in [11].

A. Discrete systems: HOM for d-dimensional systems

We want to consider now *single-photon states*,

$$|\phi\rangle=\sum_{i=0}^{d-1}\alpha_i|i\rangle \quad \text{and} \quad |\psi\rangle=\sum_{j=0}^{d-1}\beta_j|j\rangle, \tag{16}$$

with

$$\sum_{i=0}^{d-1}|\alpha_i|^2=1 \quad \text{and} \quad \sum_{i=0}^{d-1}|\beta_i|^2=1. \tag{17}$$

States $|i\rangle$ from $\{|0\rangle,|1\rangle,\ldots,|d-1\rangle\}$ are orthogonal and can correspond to photons with different frequencies, orbital angular momentum values [12], or wave functions in different time windows like in time-bin encoding [13]. We can also add different polarizations to double the number of possible orthogonal states or combine any of the mentioned degrees of freedom.

We have now creation operators $\hat{a}^\dagger_{i,p}$, as we still allow each of these photon states to be in the upper and lower ports. The evolution through a 50:50 beam splitter is

$$\begin{aligned}
|\phi\rangle_U|\psi\rangle_D &= \sum_i^{d-1}\sum_j^{d-1}\alpha_i\beta_j\hat{a}^\dagger_{i,U}\hat{a}^\dagger_{j,D}|0\rangle_U|0\rangle_D\\
&\to U\left(\sum_i\sum_j\alpha_i\beta_j\hat{a}^\dagger_{i,U}\hat{a}^\dagger_{j,D}\right)U^\dagger|0\rangle_U|0\rangle_D\\
&=\sum_i\sum_j\alpha_i\beta_j(U\hat{a}^\dagger_{i,U}U^\dagger)(U\hat{a}^\dagger_{j,D}U^\dagger)|0\rangle_U|0\rangle_D\\
&=\sum_i\sum_j\frac{\alpha_i\beta_j}{2}(\hat{a}^\dagger_{i,U}\hat{a}^\dagger_{j,U}-\hat{a}^\dagger_{i,U}\hat{a}^\dagger_{j,D}\\
&\quad+\hat{a}^\dagger_{i,D}\hat{a}^\dagger_{j,U}-\hat{a}^\dagger_{i,D}\hat{a}^\dagger_{j,D})|0\rangle_U|0\rangle_D.
\end{aligned} \tag{18}$$

There are two parts with different behavior

$$\begin{aligned}
&\sum_i\alpha_i\beta_i\frac{|2^i\rangle_U|0\rangle_D-|0\rangle_U|2^i\rangle_D}{\sqrt{2}}\\
&\quad+\sum_i\sum_{j\neq i}\frac{\alpha_i\beta_j}{2}[|1^i,1^j\rangle_U|0\rangle_D\\
&\quad-|1^i\rangle_U|1^j\rangle_D+|1^j\rangle_U|1^i\rangle_D-|0\rangle_U|1^i,1^j\rangle_D].
\end{aligned} \tag{19}$$

We use $|1^i,1^j\rangle_p$ to denote two photons that coexist in the same path but are in different states i and j.

We can consider the setting as a test. The photons pass the test if only one detector fires. A coincidence is detected as a failure. The probabilities of each event are related to the overlap of the two input states, with $\langle\psi|\phi\rangle=\sum_i\alpha_i\beta_i^*$ and

$$|\langle\psi|\phi\rangle|^2=\langle\psi|\phi\rangle\langle\psi|\phi\rangle^*=\sum_i\sum_j\alpha_i\alpha_j^*\beta_i^*\beta_j. \tag{20}$$

The part of the superposition in (19) which corresponds to a coincidence is

$$\sum_i\sum_{j\neq i}\frac{\alpha_i\beta_j}{2}[-|1^i\rangle_U|1^j\rangle_D+|1^j\rangle_U|1^i\rangle_D]. \tag{21}$$

The terms can be rearranged taking into account the interference between indistinguishable photon states to give

$$-\sum_i\sum_j\frac{1}{2}(\alpha_i\beta_j-\alpha_j\beta_i)|1^i\rangle_U|1^j\rangle_D. \tag{22}$$

The probability of finding a coincidence and failing the test is

$$\begin{aligned}
&\sum_i\sum_j\frac{1}{4}(\alpha_i\beta_j-\alpha_j\beta_i)(\alpha_i\beta_j-\alpha_j\beta_i)^*\\
&\quad=\sum_i\sum_j\frac{1}{4}(|\alpha_i|^2|\beta_j|^2+|\alpha_j|^2|\beta_i|^2\\
&\qquad-\alpha_i\alpha_j^*\beta_i^*\beta_j-\alpha_i^*\alpha_j\beta_i\beta_j^*).
\end{aligned} \tag{23}$$

We can group the terms and see the failure probability is

$$\begin{aligned}
P_f&=\frac{\sum_i\sum_j|\alpha_i|^2|\beta_j|^2-\sum_i\sum_j\alpha_i\alpha_j^*\beta_i^*\beta_j}{2}\\
&=\frac{1-|\langle\phi|\psi\rangle|^2}{2},
\end{aligned} \tag{24}$$

where we use Eqs. (17) and (20).

The probability of passing the test is, as it should be, $\frac{1+|\langle\phi|\psi\rangle|^2}{2}$ for any pair of input states $|\phi\rangle$ and $|\psi\rangle$. This shows the HOM circuit performs a SWAP test. The formal equivalence permits an optical implementation in many applications where the SWAP test is used (see Sec. VI).

IV. DESTRUCTIVE SWAP TESTS

The HOM effect proves no ancillary photon is needed to perform a SWAP test. In this section, we present a destructive SWAP test with no ancillas.

The gates in our quantum circuits are best described by their effects on the states $|0\rangle$ and $|1\rangle$. They form what is usually called the computational basis. Operations on states $|x\rangle$ with $x = 0$ and $x = 1$ can be explained in terms of simple primitives. The generalization to arbitrary quantum states is simple. Any arbitrary qubit state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is a superposition of states from the computational basis. The output after a gate presents the same superposition of the transformed $|0\rangle$ and $|1\rangle$ inputs. α and β are the complex probability amplitudes associated to $|0\rangle$ and $|1\rangle$, respectively, and, as such, $|\alpha|^2 + |\beta|^2 = 1$.

We can derive a destructive SWAP test circuit from an implementation of the SWAP gate which only uses CNOT and Toffoli gates. Both are based on the binary exclusive OR function (XOR). The XOR of two binary values is only true if one, and only one, of them is true. In particular, we use that $x \oplus x = 0$ and $x \oplus 0 = x$ for any input. The XOR function can be seen as both a modulo 2 addition and a modulo 2 complement. In higher dimensions these operations correspond to separate functions.

The basic gate, the NOT or X gate, takes $|0\rangle$ into $|1\rangle$ and $|1\rangle$ into $|0\rangle$. In terms of the XOR operation

$$X|x\rangle = \text{NOT}|x\rangle = |x \oplus 1\rangle. \tag{25}$$

In the CNOT and Toffoli gates, we define target and control qubits represented by the XOR symbol ($\oplus$) and a black dot, respectively. The CNOT gate is a controlled NOT operation that flips the target value if the control is in state $|1\rangle$. We have

$$\text{CNOT}|x\rangle|y\rangle = |x\rangle|x \oplus y\rangle. \tag{26}$$

The Toffoli gate is a controlled-controlled-NOT. The target is only flipped if both control qubits are $|1\rangle$, with evolution

$$\text{CCNOT}|x\rangle|y\rangle|z\rangle = |x\rangle|y\rangle|(x \cdot y) \oplus z\rangle, \tag{27}$$

where $x \cdot y$ is the binary AND of x and y. From the properties of the XOR function, we can see both gates are their own inverses. They cancel if applied twice in a row.

A. Comparison of one-qubit states

We start with a CSWAP circuit inspired by classical XOR swapping. When we have two registers, we can switch their contents without any additional memory bits with the circuit of Fig. 2.

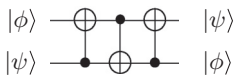

FIG. 2. XOR swapping circuit.

The step-by-step evolution is

$$\begin{aligned}|x\rangle|y\rangle &\xrightarrow{\text{CNOT}(2,1)} |x \oplus y\rangle|y\rangle \xrightarrow{\text{CNOT}(1,2)} |x \oplus y\rangle|y \oplus x \oplus y\rangle \\ &= |x \oplus y\rangle|x\rangle \xrightarrow{\text{CNOT}(2,1)} |x \oplus y \oplus x\rangle|x\rangle = |y\rangle|x\rangle.\end{aligned} \tag{28}$$

We call CNOT(i, j) the CNOT gate with control qubit i and target qubit j. We have described the classical setting, but the results can also be generalized to arbitrary quantum superpositions.

We can introduce an additional control in the middle gate of the SWAP circuit of Fig. 2 to build a CSWAP gate. Figure 3 shows the corresponding SWAP test circuit. If the ancillary control qubit is $|0\rangle$, the middle gate has no effect and the first and last CNOT cancel. If the ancillary qubit is $|1\rangle$, we recover the SWAP operation.

We are going to find equivalent circuits that show the ancillary qubit can be replaced by measurement on the tested states. We need to introduce two additional gates. The first is the Z gate, which performs the conditional sign shift

$$Z|x\rangle = (-1)^x|x\rangle. \tag{29}$$

The second is its controlled version

$$\text{CZ}|x\rangle|y\rangle = (-1)^{x \cdot y}|x\rangle|y\rangle. \tag{30}$$

The only input state $|x\rangle|y\rangle$ from the computational basis for which the CZ gate introduces a sign shift is $|1\rangle|1\rangle$.

In our proof, we are going to use the circuit equivalences shown in Fig. 4. The basic step is the decomposition of the X gate into the sequence HZH. For a state $|x\rangle$ from the computational basis

$$H|x\rangle = \frac{|0\rangle + (-1)^x|1\rangle}{\sqrt{2}}. \tag{31}$$

The effect of the gate sequence HZH on an input $|x\rangle$ is

$$|x\rangle \xrightarrow{H} \frac{|0\rangle + (-1)^x|1\rangle}{\sqrt{2}} \xrightarrow{Z} \frac{|0\rangle + (-1)^{x+1}|1\rangle}{\sqrt{2}} \xrightarrow{H} |x \oplus 1\rangle, \tag{32}$$

which is also the result of the operation $X|x\rangle$.

If we replace the Z gate with a CZ gate, the resulting circuit acts as a CNOT gate. If the control qubit is $|1\rangle$, we have the operation sequence $HZH = X$ on the target. If it is $|0\rangle$, we

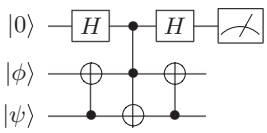

FIG. 3. SWAP test circuit for qubit states with CNOT, Toffoli, and H gates. The measured qubit is taken into a superposition $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$, which controls the Toffoli gate in the middle. Only the parts of the superposition corresponding to control qubit state $|1\rangle$ are swapped. The final state is the same as in the circuit of Fig. 1.

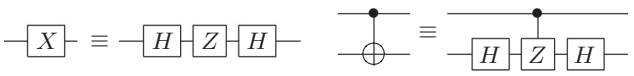

FIG. 4. Equivalent circuits for the X and Z gates and their controlled versions.

have two H gates, which cancel. We can similarly define a controlled-controlled-Z gate, CCZ, with

$$\mathrm{CCZ}|x\rangle|y\rangle|z\rangle = (-1)^{x\cdot y\cdot z}|x\rangle|y\rangle|z\rangle. \tag{33}$$

With these equivalences, we can proceed to simplify the SWAP test circuit.

Figure 5 shows our starting circuit. We have taken the SWAP test circuit of Fig. 3 and replaced the Toffoli gate in the center with a CCZ gate that has two H gates around the target qubit. The combination of these gates produces the CCNOT operation of the Toffoli gate, with an evolution similar to that described in Eq. (32). In Fig. 5 we have also included a measurement on all qubits at the end of the test. The tested qubits have no use after the comparison. We can suppose they are measured at the end of the protocol.

We can reduce the number of gates if we notice that the ancillary qubit which carries the answer to the test is not affected by operations on the tested qubits after the CCZ gate. We are not interested in the outcomes of the measurements on the qubits under test. We can just as well get rid of the last H and CNOT gates and measure directly after the CCZ gate with no effect on the ancillary qubit and the result of the SWAP test.

We can also move the target in the CCZ operation. All the qubits can be equally said to be a control or a target. The sign shift takes place only when the three qubits are $|1\rangle$. The result of advancing the measurement and reinterpreting the roles of target and control in the CCZ gate is the circuit of Fig. 6.

After this rearrangement, we use the equivalences in Fig. 4 to rewrite the circuit as in Fig. 7 and make the ancillary qubit the target of a CCNOT gate.

The test will fail if, after the CCNOT gate, the original ancillary $|0\rangle$ qubit has become $|1\rangle$. That happens only when both control qubits are $|1\rangle$. We get the same measurement statistics if we just measure the qubits under test and then perform an X gate on the ancillary qubit only if we find two 1 outcomes. This fact is sometimes called the principle of deferred measurement [14]. We can just ignore the ancillary qubit and perform a SWAP test with the circuit in Fig. 8.

The order of the input states is not relevant. The SWAP test should return the same results for $|\phi\rangle|\psi\rangle$ and for $|\psi\rangle|\phi\rangle$, giving us two equivalent circuits. The result of the SWAP test is the NAND function of the outcomes, $\mathrm{NAND}(O_1, O_2)$. Only if both outcomes are 1, $O_1 \cdot O_2 = 1$, we get a failure.

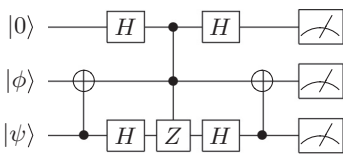

FIG. 5. SWAP test circuit with a CCZ gate. The Toffoli gate which controls the SWAP gate can be decomposed into a CCZ gate with two H gates around the target qubit.

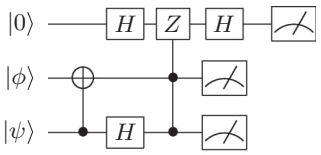

FIG. 6. SWAP test advancing the measurement. We can ignore the gates that are not relevant to the state comparison test and measure just after the CCZ gate. The CCZ operation changes only the $|1\rangle|1\rangle|1\rangle$ state. Because of this symmetry, we can interchange the roles of target and control qubits.

For the rest of the paper, we work with the last circuit in Fig. 8. This circuit is, in fact, a measurement in the Bell basis. The gates take inputs from the Bell basis

$$\left\{\frac{|00\rangle+|11\rangle}{\sqrt{2}}, \frac{|01\rangle+|10\rangle}{\sqrt{2}}, \frac{|00\rangle-|11\rangle}{\sqrt{2}}, \frac{|01\rangle-|10\rangle}{\sqrt{2}}\right\} \tag{34}$$

into the computational basis for two qubits $\{|00\rangle,|01\rangle,|10\rangle,|11\rangle\}$. This is quite relevant, as both the SWAP test and the HOM effect have a peculiar behavior when the inputs are entangled. Take state $\frac{|01\rangle+|10\rangle}{\sqrt{2}}$. After the change of basis, it becomes $|01\rangle$ and passes the test. This is correct because the entangled input state is the right level of description, but runs against our intuition that it should fail because the first and the second qubit are always different. State comparison is valid only for an input $|\phi\rangle|\psi\rangle = |\phi\rangle \otimes |\psi\rangle$, where $\otimes$ is a tensor product.

We can do a quick check to find the test is still valid after all the simplifications. For two arbitrary single qubit input states $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ and $|\psi\rangle = \gamma|0\rangle + \delta|1\rangle$, the input state goes from

$$\alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle \tag{35}$$

to

$$\alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|11\rangle + \beta\delta|10\rangle \tag{36}$$

after the CNOT. After the H gate and before measurement we have

$$\frac{1}{\sqrt{2}}[\alpha\gamma|00\rangle + \alpha\gamma|10\rangle + \alpha\delta|01\rangle + \alpha\delta|11\rangle + \beta\gamma|01\rangle - \beta\gamma|11\rangle + \beta\delta|00\rangle - \beta\delta|10\rangle]. \tag{37}$$

The probability of failure,

$$P_f = \frac{|\alpha\delta-\beta\gamma|^2}{2} = \frac{(\alpha\delta-\beta\gamma)(\alpha\delta-\beta\gamma)^*}{2}, \tag{38}$$

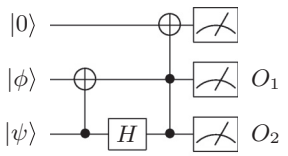

FIG. 7. SWAP test where the ancillary qubit is the target of a CCNOT gate.

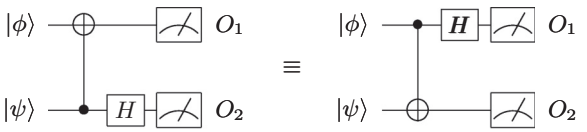

FIG. 8. Quantum circuits for a destructive SWAP test.

comes from considering the probability of measuring the $|11\rangle$ state. The complementary probability of success is

$$P_p = \frac{2 - |\alpha|^2|\delta|^2 - |\beta|^2|\gamma|^2 + \alpha\beta^*\gamma^*\delta + \alpha^*\beta\gamma\delta^*}{2}. \quad (39)$$

Taking into account that the probability amplitudes in the input qubits obey $|\alpha|^2 + |\beta|^2 = 1$ and $|\gamma|^2 + |\delta|^2 = 1$, we obtain

$$P_p = \frac{1 + |\alpha|^2|\gamma|^2 + |\beta|^2|\delta|^2 + \alpha\beta^*\gamma^*\delta + \alpha^*\beta\gamma\delta^*}{2}. \quad (40)$$

The overlap of the input states is $|\langle\psi|\phi\rangle|^2 = (\alpha\gamma^* + \beta\delta^*)(\alpha^*\gamma + \beta^*\delta) = |\alpha|^2|\gamma|^2 + |\beta|^2|\delta|^2 + \alpha\beta^*\gamma^*\delta + \alpha^*\beta\gamma\delta^*$. We can see the probability of success of the SWAP test $P_p = \frac{1+|\langle\psi|\phi\rangle|^2}{2}$ from Eq. (2) corresponds to that in Eq. (40).

B. Generalization to *n* qubits

The destructive SWAP test can be extended to any number of qubits with little additional effort. We take two n-qubit states $|\phi\rangle$ and $|\psi\rangle$ so that $|\phi\rangle|\psi\rangle = |\phi\rangle \otimes |\psi\rangle$. The qubits that form each input state can be entangled.

If we swap the qubits of $|\phi\rangle$ and $|\psi\rangle$ one by one, we have an n-qubit SWAP gate. Figure 9 shows the corresponding SWAP test circuit where all the qubits are explicitly shown.

We can repeat the steps of the one-qubit states example and get the circuit of Fig. 10. The ancillary qubit sees n CCZ gates. The total phase shift can be perfectly determined from the outcomes of the measurements $O_1^1, \ldots, O_n^1, O_1^2, \ldots, O_n^2$. O_i^1 is the result of the measurement on the ith qubit of the first tested state. O_i^2 is the corresponding result for the second state. The total phase shift is $\pi \sum_{i=1}^n O_i^1 \cdot O_i^2$. The qubit output is 1 (failed test) only if we have an odd number of sign shifts.

We can ignore the ancillary qubit altogether and obtain the same answer from the measurement outcomes (Fig. 11). If we call O_1 and O_2 to the bit strings with all the measurements

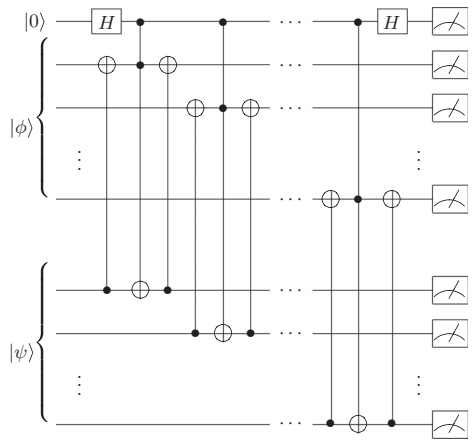

FIG. 9. SWAP test for n-qubit states.

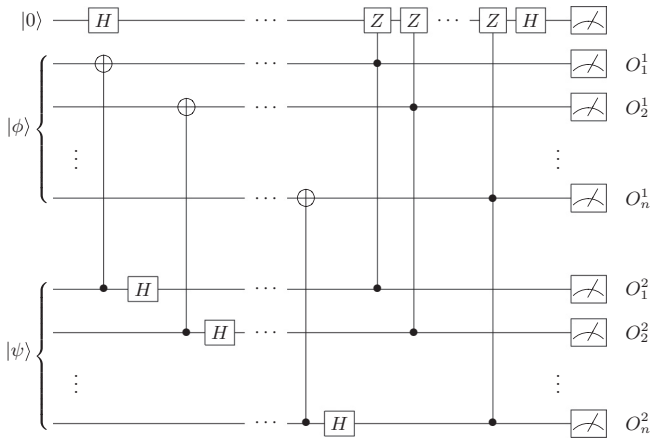

FIG. 10. SWAP test for n-qubit states advancing the measurement.

corresponding to all the O_i^1 and O_i^2, the test succeeds if the bitwise AND of O_1 and O_2 has an even parity.

We wish to point out that, while for quantum systems with a dimension that is a power of two there is a natural destructive circuit, the decomposition of the SWAP test circuit for general d-dimensional states $|\phi\rangle$ and $|\psi\rangle$ (qudits) poses certain challenges. Complements to d and modulo d are not the same operation as in the $d = 2$ case.

V. AN OPTICAL SWAP CIRCUIT

We can also check that the optical circuit of the HOM effect not only performs the same operation as the SWAP test, but is also completely equivalent to the destructive SWAP test of Sec. IV.

A. Optical SWAP test

The optical setup of the HOM effect is just a destructive version of the complete optical implementation of the SWAP test. To prove it, we start with the controlled optical SWAP gate in Fig. 12. The system is a modified interferometer.

The gate has two 50:50 beam splitters and a π phase shifter. We add a control bit b that activates the phase shifter when its value is 1. Physically, it can correspond to a Pockels cell, a typical element to manipulate single photons in optical quantum computation [15]. Pockels cells introduce a π phase shift between the upper and lower arms of the interferometer.

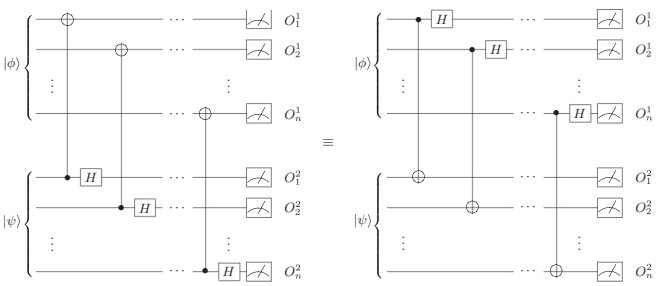

FIG. 11. SWAP test for n-qubit states. We can, as in the single-qubit SWAP test, change the input state order to obtain the last equivalence.

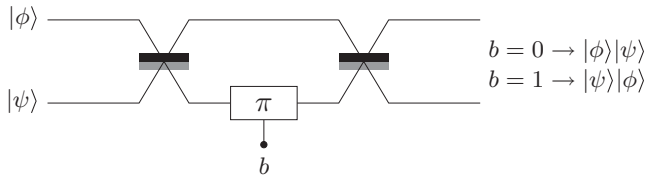

FIG. 12. Optical SWAP gate with a classical control bit, b. The system could correspond to a Mach-Zehnder interferometer with a settable phase in the lower arm.

When $b = 0$, we have two beam splitters which cancel each other (they apply two H operations in a row). For independent, orthogonal photons, at the second beam splitter, there is a constructive interference in the up or down port the photon came in and a destructive interference in the other port. Taking equations (8) and (9), we can also see that indistinguishable photons are separated again after the second beam splitter. The total evolution is

$$|1^s\rangle_U|1^s\rangle_D \xrightarrow{\text{BS}_1} \frac{|2^s\rangle_U|0\rangle_D - |0\rangle_U|2^s\rangle_D}{\sqrt{2}} \xrightarrow{\text{BS}_2} |1^s\rangle_U|1^s\rangle_D. \tag{41}$$

Both equal and different components have the same behavior. We can establish that the two beam splitters perform an identity operation.

When there is a π phase shift ($b = 1$), we have a typical interferometric setup where the port with the constructive and destructive interference change. For orthogonal photons, we can see from each individual photon's evolution that

$$\begin{aligned} |1^s\rangle_U|0\rangle_D &\xrightarrow{\text{BS}_1} \frac{|1^s\rangle_U|0\rangle_D + |0\rangle_U|1^s\rangle_D}{\sqrt{2}} \\ &\xrightarrow{\pi} \frac{|1^s\rangle_U|0\rangle_D - |0\rangle_U|1^s\rangle_D}{\sqrt{2}} \xrightarrow{\text{BS}_2} |0\rangle_U|1^s\rangle_D \end{aligned} \tag{42}$$

and

$$\begin{aligned} |0\rangle_U|1^s\rangle_D &\xrightarrow{\text{BS}_1} \frac{|1^s\rangle_U|0\rangle_D - |0\rangle_U|1^s\rangle_D}{\sqrt{2}} \\ &\xrightarrow{\pi} \frac{|1^s\rangle_U|0\rangle_D + |0\rangle_U|1^s\rangle_D}{\sqrt{2}} \xrightarrow{\text{BS}_2} |1^s\rangle_U|0\rangle_D. \end{aligned} \tag{43}$$

For photons in the same state, we always have 0 or 2 photons going through the phase shifter. This makes a total phase shift of 0 or 2π for the joint system, which does not alter the global state. Equation (41) is still valid. Either way, for indistinguishable photons, the output can be equally said to be the same or swapped.

We can now add an ancillary photon to perform a full SWAP test (Fig. 13). This setup is an optical implementation of the circuit in Fig. 1.

We put a photon in any state we want in the upper port of an interferometer with two 50:50 beam splitters in the place of the H gates. The most complicated part is the control of the SWAP gate. The logical $|1\rangle$ state, the $|0\rangle_U|1^s\rangle_D$ term after the first beam splitter, must activate the π phase shift that triggers the SWAP operation. This is a CZ operation for photons, which, given that we can build H gates with beam splitters, is also a photonic CNOT gate. There have been many proposals in that direction, like using the nonlinearities

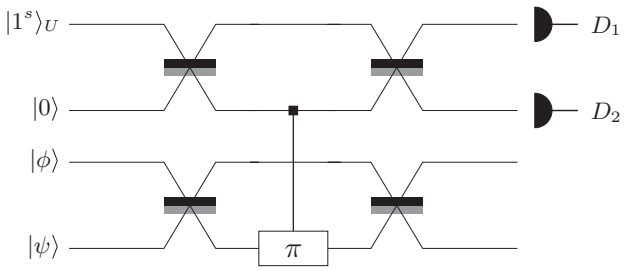

FIG. 13. Optical SWAP test with an interferometric setup and an optical CZ gate.

inside Kerr media, or making the photons interact with atomic systems or introducing measurement-assisted systems [16]. Photonic interaction at the quantum level is challenging and it still remains a major roadblock for scalable optical quantum computation. However, we only need the gate as an intermediate step in our proof. We assume it is possible to build one and do not really worry about its efficiency.

Now that we have all the elements in place, we can proceed in the same way we did in Sec. IV. The input photons pass the SWAP test if detector D_1 in Fig. 13 clicks. The two-photon state at the output of the lower interferometer is not used. We could just as well take out the last beam splitter and the SWAP test would be unaffected. We can also add two detectors D_3 and D_4 (Fig. 14).

As we commented in Sec. IV, in a CZ gate the roles of the control and the target states can be reversed. We can suppose the optical CZ gate is controlled by the existence of photons in the lower arm of the lower interferometer. The input photons under comparison fail the test only if there is a π phase shift in the lower path of the ancillary photon. Imagine D_4 could count photons. For 0 or 2 photons there has been no change in the ancillary photon's phase and we know the SWAP test has been successful. For one photon the input states fail the test. The output state up in the ancillary interferometer is then correlated to the measurement outcomes from detectors D_3 and D_4.

The optical CZ gate does not change the number of photons. We can perform the measurement before the gate and get the same measurement statistics (Fig. 15). We do not really need to be able to count photons. The total photon number is conserved in the passive, lossless, linear optics beam splitter we are assuming. For two input photons, we have two output photons. The only way to have one photon in D_4 is if we get a coincidence count. If only D_3 fires, we have two photons up. If only D_4 fires, both photons are down. The AND of the outcomes of both detectors, being 0 no click and 1 a click, gives

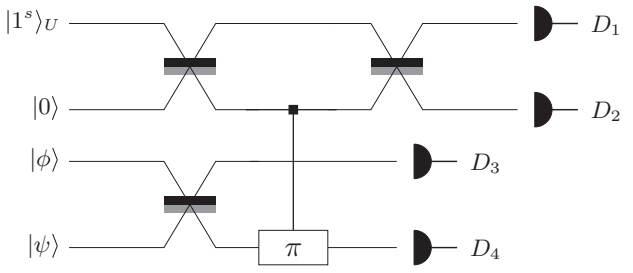

FIG. 14. Simplified optical SWAP test.

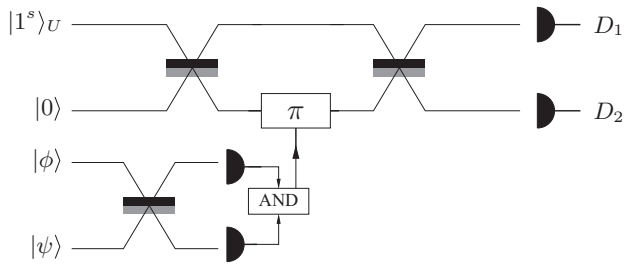

FIG. 15. Optical SWAP test without the CZ gate.

the control bit for the SWAP gate in the upper interferometer. The output of the SWAP test is the NAND of the outcomes. The test fails (outcome 0) only if there is a coincidence count.

That means we can just ignore the ancillary photon and work directly with the detectors' outcomes. The usual HOM setup (Fig. 16) with simple binary photodetectors that click or not, such as avalanche photodiodes, is enough to perform a SWAP test. All the steps in the proof are valid regardless of the dimension of the photon states $|\phi\rangle$ and $|\psi\rangle$. A beam splitter and two photodetectors is all we need to perform a SWAP test on any two photon states.

VI. APPLICATIONS AND FUTURE LINES

We have shown the HOM effect and the SWAP test are formally equivalent. The proof offers simpler implementations of the SWAP test which can be interesting in quantum information protocols.

Equation (14) captures how photons can be used in a SWAP test in quantum information. We only need to find orthogonal wave functions. The most obvious examples are frequency and time-bin qudits. The wave functions of photons of different frequencies can be thought of as orthogonal sine functions. Time-bin qudits are just wave functions with separate, nonoverlapping supports. There are also wave functions which are orthogonal in space like, for instance, optical vortices carrying orbital angular momentum (OAM).

There is a caveat in this last case. Reflection from the beam splitter performs a left-to-right inversion. If we want to preserve proper interference, the reflection must be compensated. Imagine we have single-photon input states $|1^\ell\rangle$ which carry an orbital angular momentum of $\ell\hbar$. In a 50:50 beam splitter the evolution is

$$|1^\ell\rangle_U|0\rangle_D \longrightarrow \frac{|1^{-\ell}\rangle_U|0\rangle_D + |0\rangle_U|1^\ell\rangle_D}{\sqrt{2}}, \tag{44}$$

$$|0\rangle_U|1^\ell\rangle_D \longrightarrow \frac{|1^\ell\rangle_U|0\rangle_D - |0\rangle_U|1^{-\ell}\rangle_D}{\sqrt{2}}. \tag{45}$$

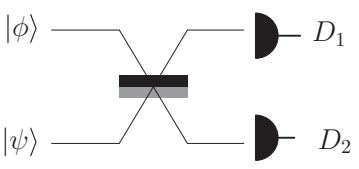

FIG. 16. Destructive SWAP test with a HOM configuration.

Due to the symmetry of the OAM wave fronts, reflection from a mirror results in a change of the sign of the winding number ℓ. A simple mirror in the lower port can compensate for that. An input $|1^\ell\rangle_U|1^{-\ell}\rangle_D$ becomes, at the output of the beam splitter, the entangled state

$$\frac{|2^{-\ell}\rangle_U|0\rangle_D - |0\rangle_U|2^\ell\rangle_D}{\sqrt{2}}, \tag{46}$$

where the interference in the HOM effect is still present and the photons in the upper output port are in the reflected state. A similar analysis can be made for any spatially modulated photon.

One possible application is quantum fingerprinting. Two users, Alice with a string x and Bob with a string y, both n qubits long, want to know whether x and y are equal or different. Alice could send her string to Bob, who would answer if they are equal or not. The cost would be communicating $n+1$ classical bits. Alternatively, they could send shorter strings, called fingerprints, which are a function of x and y and, with high probability, are only equal when $x = y$. In the simultaneous message passing model, if Alice and Bob do not have any previously shared information, they need fingerprints of a size proportional to $\sqrt{n}$ bits [17]. Quantum fingerprints of size of the order of $\log_2(n)$ qubits are enough for the same task [5]. This exponential reduction in communication complexity is based on the comparison of quantum fingerprint states. For a string x, the fingerprint is a superposition of $m = cn$ states of the form

$$|h_x\rangle = \frac{1}{\sqrt{m}}\sum_{i=1}^{m}(-1)^{E_i(x)}|i\rangle, \tag{47}$$

where $E(x)$ is the code word corresponding to x in a binary error correcting code and $E_i(x)$ the ith bit of that code word. c is a constant related to the chosen code. For certain error-correcting codes, like Justesen codes [18], we can guarantee $\langle h_x|h_y\rangle \leqslant \delta$ for a $\delta > 0$. Repetitions of the SWAP test make it possible to detect different strings with high probability. In the limit of large n, the total communication complexity is of the order of $\log_2(n)$ qubits.

We can perform the test with a HOM setup. In fact, the equivalence of the SWAP test and the HOM effect has already been noticed in the single-qubit case and has been put to use in a quantum fingerprinting scheme with one-qubit fingerprints, which still has some advantages with respect to any classical method [19]. The equivalence can be extended to arbitrary mixed single-photon input states with density matrices ρ_A and ρ_B. For them, the HOM effect provides a SWAP test that succeeds with probability $P_p = \frac{1+\mathrm{Tr}(\rho_A\rho_B)}{2}$ [11].

Our circuits also show that the results can be extended to qudits as long as we can still use a single photon for each fingerprint. The fingerprint can be encoded in a single photon with a method similar to the single-photon fingerprinting scheme of Massar [20]. Imagine we take a photon source with a long coherence time. A photon wave function of length T s can be divided into m parts of duration $\frac{T}{m}$. We can number the portions from 1 to m and define states $|i\rangle$ corresponding to a photon found in the ith segment. The fingerprint state of Eq. (47) can be generated with a phase shifter which selectively

introduces a π shift in the portions for which $E_i(x)$ is 1. Bob can do the same to produce a state $|h_y\rangle$.

While m is of the order of n, the photon state can only convey $\log_2 c + \log_2 n$ bits. The Holevo bound makes it impossible to recover more bits [6]. We can reach the bound if we determine the time segment in which the photon arrives. This gives us one number from 1 to m (about $\log_2 n$ bits). This kind of test would prove the principle of quantum fingerprinting.

However, there are two details that make the system impractical. First, we could use the T s to send x directly with classical light using a phase modulation encoding where 0 corresponds to a null phase shift and 1 to a phase π. The number of bits is greater, but we avoid dealing with single photons and the total transmission time is still T. In a practical system, there is no real advantage in using the quantum scheme. Second, in order to obtain a small probability of error the fingerprints have to be sent multiple times. If we want to outperform the communication complexity of classical methods, proportional to $\sqrt{n}$, we would need strings with a large number of bits. While asymptotically the quantum system is exponentially better, it will work more efficiently only for long strings of around $10^{10} \approx 2^{33}$ bits [20], which poses experimental challenges.

The first problem can be solved using better encodings. Hyperentangled photons are a good example [21]. We could use a combination of polarization, OAM, and temporal degrees of freedom. For two polarization states, M OAM states and B time bins, we have $2MB$ orthogonal states. A complete decoding would be difficult, but it is not needed for a SWAP test. Single photon fingerprints in such an encoding would take only B time segments. If B and M are of the same order, close to $\sqrt{\frac{n}{2}}$, we can compete with the classical scheme in terms of the transmission time.

In that sense, we advocate for spatial encoding schemes. Let us take a spatial light modulator, SLM, with $N \times N$ transmissive pixels which either do nothing or introduce a π phase shift. This SLM can produce up to 2^{N^2} different wave fronts for a single photon. We can search for a subset of those wave functions which have a bounded overlap $\langle h_x|h_y\rangle \leqslant \delta$ for any x and y. This is a generalization of what is done to produce OAM states with SLMs [22]. Similarly, d states can be encoded in the transverse spatial profile of a single photon [23]. If a good family of codes is found, it would make it possible to send single photon fingerprints in a reasonable time. Spatial precision needs not to be so good as in a classical spatial encoding method. We just need a binary equal or not-equal measurement from the coincidence count. The quantum fingerprinting system is practical as long as we can make the photons interfere (arrange the times of arrival and correct for the effects of reflection in the wave front). This kind of system would permit many interesting experiments with the SWAP test, not only as used in quantum fingerprinting, but also as used in other applications such as entanglement detection [24].

Photons seem an ideal support with many accessible time and spatial modes. Photonic technology is mature. We can prepare two photons in the same time and spatial mode and compare them with a HOM SWAP test. Nevertheless, the photon interference we have described for a beam splitter is valid also for any boson. Similar schemes could be implemented with bosonic atoms or Bose-Einstein condensates. The HOM effect also appears in these cases, with a small probability of collision, which can be reduced if we have long wave packets [25].

We have shown that the HOM effect permits us to compare photon states and provides an optical implementation of the SWAP test for simple quantum communication protocols. Reciprocally, the formal equivalence of the SWAP test and the HOM effect gives us a computational point of view to analyze and understand interference in quantum optics. We have used this equivalence to show that the usual SWAP test circuit can be simplified if we allow for a destructive test. This simplification can be extended to other implementations of the SWAP test outside quantum optics.

ACKNOWLEDGMENTS

This work has been funded by Projects No. VA342B11-2 (Junta de Castilla y León) and No. TEC2010-21303-C04-04 (MICINN).

[1] H. Buhrman, R. Cleve, S. Massar, and R. de Wolf, Rev. Mod. Phys. **82**, 665 (2010).
[2] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.
[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[4] L. K. Grover, Am. J. Phys. **69**, 769 (2001).
[5] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf, Phys. Rev. Lett. **87**, 167902 (2001).
[6] A. Holevo, Probl. Inf. Transm. **9**, 177 (1973).
[7] A. Holevo, IEEE Trans. Inf. Theory **44**, 269 (1998).
[8] C. K. Hong, Z. Y. Ou, and L. Mandel, Phys. Rev. Lett. **59**, 2044 (1987).
[9] R. Loudon, *The Quantum Theory of Light*, 3rd ed. (Oxford University Press, Oxford, UK, 2000).
[10] J. Skaar, J. C. G. Escartín, and H. Landro, Am. J. Phys. **72**, 1385 (2004).
[11] L. Schwarz and S. J. van Enk, Phys. Rev. Lett. **106**, 180501 (2011).
[12] G. Molina-Terriza, J. P. Torres, and L. Torner, Phys. Rev. Lett. **88**, 013601 (2001).
[13] D. Stucki, H. Zbinden, and N. Gisin, J. Mod. Opt. **52**, 2637 (2005).
[14] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, 1st ed. (Cambridge University Press, Cambridge, UK, 2000).
[15] T. B. Pittman, B. C. Jacobs, and J. D. Franson, Phys. Rev. A **66**, 052305 (2002).

[16] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn, Rev. Mod. Phys. **79**, 135 (2007).
[17] A. Ambainis, Algorithmica **16**, 298 (1996).
[18] J. Justesen, IEEE Trans. Inf. Theory **18**, 652 (1972).
[19] R. T. Horn, S. A. Babichev, K.-P. Marzlin, A. I. Lvovsky, and B. C. Sanders, Phys. Rev. Lett. **95**, 150502 (2005).
[20] S. Massar, Phys. Rev. A **71**, 012310 (2005).
[21] J. T. Barreiro, N. K. Langford, N. A. Peters, and P. G. Kwiat, Phys. Rev. Lett. **95**, 260501 (2005).
[22] M. Stütz, S. Gröblacher, T. Jennewein, and A. Zeilinger, Appl. Phys. Lett. **90**, 261114 (2007).
[23] S. P. Walborn, D. S. Lemelle, M. P. Almeida, and P. H. Souto Ribeiro, Phys. Rev. Lett. **96**, 090501 (2006).
[24] A. W. Harrow and A. Montanaro, in *51st Annual IEEE Symposium on Foundations of Computer Science (FOCS), 2010* (IEEE Computer Society, Piscataway, NJ, 2010), pp. 633–642.
[25] S. Popescu, Phys. Rev. Lett. **99**, 130503 (2007).