Quantum fast Fourier transform and quantum computation by linear optics

Ronen Barak and Yacob Ben-Aryeh

Department of Physics, Technion - Israel Institute of Technology, Haifa 32000, Israel

Received May 2, 2006; revised August 21, 2006; accepted August 23, 2006;
posted September 7, 2006 (Doc. ID 70512); published January 26, 2007

Using the quantum fast Fourier transform in linear optics the input mode annihilation operators $\{\hat{a}_0,\hat{a}_1,\ldots,\hat{a}_{s-1}\}$ are transformed into output mode annihilation operators $\{\hat{b}_0,\hat{b}_1,\ldots,\hat{b}_{s-1}\}$. We show how to implement experimentally such transformations based on the Cooley–Tukey algorithm, by the use of beam splitters and phase shifters in a linear optical system. Optical systems implementing 1,2, and 3 qubits discrete Fourier transform (DFT) are described, and a general method for implementing the n-qubit DFT is analyzed. These transformations are used on various input radiation states by which phase estimation and order finding can be computed. © 2007 Optical Society of America

OCIS codes: 270.0270, 200.0200.

1. INTRODUCTION

Optics interferometry has been used in various works to simulate quantum computations.[1–14] In the present work we discuss the use of the fast Fourier transform[15–21] (FFT) in linear optics for quantum computation. While most of the literature exploiting the use of FFT is for classical states, quantum FFT has been shown to be effective for computing phase estimation and prime factorization[22–25] among other quantum computation algorithms.[26]

The realizations of linear optics transformations by beam splitters (BSs) have been analyzed in previous works.[19–21] It has been shown[2,20] that by using a multiport BS configurations one can realize any unitary operator in Hilbert spaces of arbitrary finite dimension. Various Einstein–Podolsky–Rosen correlations have been analyzed for these systems by Zukowski *et al.*[20] A generalization of the standard four-port BS to a $2N$ multiport (N input ports and N output ports) has been described, and novel quantum mechanical interference phenomena of two-photon states has been analyzed.[21] A realization for totally symmetric mode couplers, for which the discrete Fourier transform (DFT) is a special case, has been described by Törmä *et al.*,[19] where the number of BSs needed for its implementation has been estimated. The main issue of the present paper, which is different from those cited above, is to describe a general algorithm for the implementation of the DFT using the Cooley–Tukey algorithm with single-photon states and to discuss some of its applications.

Classically, an s-dimensional vector $\{a_j\}$ of complex numbers can be transformed by the unitary DFT into

$$b_k = \frac{1}{s^{1/2}}\sum_{j=0}^{s-1} a_j \exp(2\pi ijk/s), \qquad (1)$$

where the integers j and k represent the indices for the components of the vectors. To apply the DFT to quantum optical systems (a quantum DFT) we apply Eq. (1) to a set of commuting annihilation operators $\{\hat{a}_0,\hat{a}_1,\ldots,\hat{a}_{s-1}\}$ so that Eq. (1) becomes

$$\hat{b}_k = \frac{1}{s^{1/2}}\sum_{j=0}^{s-1} \hat{a}_j \exp(2\pi ijk/s). \qquad (2)$$

The inverse DFT is, of course, the same with $\hat{a}$ and $\hat{b}$ replaced and with a negative exponent.

In Section 2 we show how to implement experimentally, using linear optics, a DFT where the set of output annihilation operators $\{\hat{b}_0,\hat{b}_1,\ldots,\hat{b}_{s-1}\}$ is a DFT of the input annihilation operators $\{\hat{a}_0,\hat{a}_1,\ldots,\hat{a}_{s-1}\}$. Such a transformation can be accomplished by using only BSs and phase shifters (PSs) without the use of nonlinear optics. Any pure input electromagnetic (EM) state which is represented by series expansion of the input creation operators operating on the vacuum state $|0\rangle$ leads by this transformation to an output EM state described by the output creation operators, operating on the vacuum, which are the DFT of the input ones.[27] We show in Section 2 how to implement experimentally the DFT using linear optics operators. Only then we apply in Section 3 the general transform to specific input states that can be used in quantum computation. The possibilities of using measurements in the quantum DFT with nonclassical input states are enormous relative to the classical description, and some of such transforms are useful for quantum computation. One should notice that the unitary matrix for DFT of the set of commuting operators $\{\hat{a}_0,\hat{a}_1,\ldots,\hat{a}_{s-1}\}$ is also used for the DFT of the orthogonal computational basis of quantum states.

In Section 3 we use Eq. (2) for analyzing the transformations of certain nonclassical input states that might be used for phase estimation. In Section 4 we describe certain phase estimation procedures that can be used for order finding, which is an essential component in prime factorization. Our results are summarized in Section 5.

2. EXPERIMENTAL REALIZATION OF FAST FOURIER TRANSFORM OF LINEAR OPTICS OPERATORS

A unitary transformation, represented by the $U(2)$ group operating on a 2D vector (such as a single qubit) can be given by the matrix

$$U(\alpha,\beta,\gamma,\delta)=e^{-i\alpha}\begin{bmatrix}\cos(\beta)e^{i(\gamma+\delta)} & \sin(\beta)e^{i(-\gamma+\delta)}\\ -\sin(\beta)e^{i(\gamma-\delta)} & \cos(\beta)e^{i(-\gamma-\delta)}\end{bmatrix}, \quad (3)$$

where $\alpha,\beta,\gamma,\delta$ are four independent parameters.[28] By multiplying the vector of input parameters $\hat{a}_1$, $\hat{a}_2$ from the left by the unitary matrix $U(\alpha,\beta,\gamma,\delta)$ they are transformed into the two output operators $\hat{b}_1$, $\hat{b}_2$:

$$\begin{pmatrix}\hat{b}_1\\ \hat{b}_2\end{pmatrix}=U(\alpha,\beta,\gamma,\delta)\begin{pmatrix}\hat{a}_1\\ \hat{a}_2\end{pmatrix}. \quad (4)$$

In this paper we shall use a quantum optical implementation for the qubits using the dual-rail construction, and the unitary transformations using BSs and PSs.[25] The two orthogonal states of the qubit, $|0\rangle_L$ and $|1\rangle_L$, are represented by the two input or output ports of each BS in an optical circuit, and the unitary transformation the qubits go through is represented by an optical circuit containing a BS and PS alone. A photon in input port $\hat{a}_1$ of the BS represents the state $|0\rangle_L$, and a photon in input port $\hat{a}_2$ represents the state $|1\rangle_L$. Any superposition of the two is also possible. The balanced BS and $\pi/2$ PS in Fig. 1 represent the Hadamard gate.

A transformation $U(\alpha,\beta,\gamma,\delta)$ could thus be implemented using one BS, which has three independent variables, and one PS, which has one independent variable.[2] A BS can be described as a four-port device (with two input ports and two output ports), where any incident beam goes through a phase shift γ, then the amplitudes are rotated by β, and finally the phases are shifted again by an angle δ.[28] A unitary matrix describing the action of a BS would therefore be $U(0,\beta,\gamma,\delta)$. The transformation of Eq. (4) can therefore be implemented by using one BS and one PS.[2] One should notice that the transformation matrix $U(\alpha,\beta,\gamma,\delta)$ used here for the qubit operators $\hat{a}_1$,$\hat{a}_2$ can be used for qubit states as well (2D orthogonal quantum states).

The DFT is widely used in quantum computation algorithms, and so a fast algorithm for implementing it has great significance. A FFT algorithm for a DFT was suggested approximately four decades ago and is known as the Cooley–Tukey algorithm.[15] It has also been shown that any unitary matrix of dimension d can be simply decomposed to a multiplication of at most $d(d-1)/2$ unitary matrices that act nontrivially on only two or fewer vector components.[26] These matrices, representing single qubit and CNOT gates, can be implemented using at most one BS and one PS acting on two qubit components, not necessarily from the same qubit. Thus it is shown that any n qubit unitary transformation can be implemented by at most $2^{n-1}(2^n-1)$ BS and PS combinations. The Cooley–Tukey algorithm improves such a relation as it breaks down the $2^n\times 2^n$ unitary matrix into $n2^{n-1}$-qubit transformations that can be realized by using linear optics by the use of BS and PS. The Cooley–Tukey algorithm for the $2^n\times 2^n$ unitary matrix is the decomposition of this matrix using n stages of 2^{n-1} transformations, where in each stage the input is given by the output of the previous stage. The mixing of the mode operators (or the computational basis of states) is arranged such that the final transformation will give the DFT.

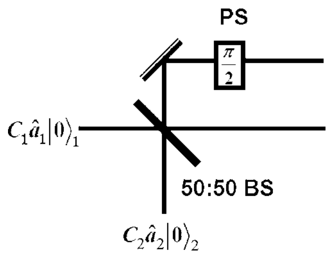

Fig. 1. Quantum optical circuit representing a qubit $(C_1\hat{a}_1^{\dagger}|0\rangle_1+C_2\hat{a}_2^{\dagger}|0\rangle_2)$ going through a Hadamard gate (balanced BS and $\pi/2$ PS). The Hadamard gate and its realization are well known from the basic literature on quantum computation (Ref. 26).

A DFT implemented by using quantum states is called a quantum Fourier transform (QFT). For 2^n commuting operators or 2^n computational quantum states that represent n qubits, the 2^n-dimensional DFT matrix is represented by the unitary matrix

$$\mathrm{QFT}(n)=\frac{1}{2^{n/2}}\times\begin{bmatrix}1 & 1 & 1 & 1 & \cdots & 1\\ 1 & u & u^2 & u^3 & \cdots & u^{2^n-1}\\ 1 & u^2 & u^4 & u^6 & \cdots & u^{2(2^n-1)}\\ 1 & u^3 & u^6 & u^9 & \cdots & u^{3(2^n-1)}\\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots\\ 1 & u^{2^{n-1}} & u^{2(2^n-1)} & u^{3(2^n-1)} & \cdots & u^{n(2^n-1)}\end{bmatrix}, \quad (5)$$

where $u=\exp(2\pi i/2^n)$.

We demonstrate the following algorithm, which includes an implementation of the Cooley–Tukey algorithm,[15,29] for the design of optical circuits performing the DFT:

1. The matrix representation of the n-qubit–2^n-dimensional DFT is calculated from Eq. (5).
2. Using the Cooley–Tukey algorithm[15,29] this matrix is broken down into a multiplication of n matrices $S_k^{(n)}$, where n is the number of qubits in the DFT and k ($k=1,\ldots,n$) is associated with the stage of the Cooley–Tukey algorithm. Each matrix represents 2^{n-1} BS–PS components.
3. Using the Cooley–Tukey algorithm the graphical representation of the optical circuit can be found.
4. Using the matrices $S_k^{(n)}$ and the graphical representation of the optical circuit the properties of each BS–PS component is calculated.

A. Two-Dimensional Discrete Fourier Transform

A single-qubit–2D DFT is simply represented by the Hadamard gate.[26]

1. In matrix representation this would simply be

$$\mathrm{QFT}(1) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{6}$$

2. This matrix represents one BS–PS component, therefore $\mathrm{QFT}(1) = S_1^{(1)}$, where the upper index represents the 1-qubit–2D DFT, and the lower index represents the only stage in the Cooley–Tukey algorithm.

3. The graphical representation of the optical circuit is given in Fig. 1.

4. Using the notation of Eq. (3) (or the graphical representation of the optical circuit in Fig. 1) one can easily find that the single-qubit–2D DFT (or the Hadamard gate) consists of a balanced BS ($\beta = \pi/4$), a $\pi/2$ PS, and an unimportant phase ($\alpha = \pi/2$):

$$\mathrm{BS}_1^{(1)} = U\left(\frac{\pi}{2}, \frac{\pi}{4}, 0, \frac{\pi}{2}\right) \quad \text{or} \quad \mathrm{BS}_1^{(1)} = U\left(\frac{\pi}{2}, \frac{\pi}{4}, \frac{4\pi}{2}, \frac{\pi}{2}\right), \tag{7}$$

where the upper index represent the 1-qubit–2D DFT, and the lower index represents the only BS–PS component in the system.

B. Four-Dimensional Discrete Fourier Transform

1. By using the matrix in Eq. (5) it is easily shown that the matrix representation of a 2-qubit–4D DFT is simply

$$\mathrm{QFT}(2) = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & \mathrm{i} & -1 & -\mathrm{i} \\ 1 & -1 & 1 & -1 \\ 1 & -\mathrm{i} & -1 & \mathrm{i} \end{bmatrix}. \tag{8}$$

2. Using the Cooley–Tukey algorithm (represented in Fig. 2) this transformation matrix for the input operators $\{\hat{a}_0, \hat{a}_1, \hat{a}_2, \hat{a}_3\}$ breaks down to the multiplication of two matrices $\mathrm{QFT}(2) = S_2^{(2)} S_1^{(2)}$ (the upper index represents the 2-qubit–4D DFT). The first matrix ($S_1^{(2)}$) represents the first stage of the Cooley–Tukey algorithm where two BS–PS components combine operators $\hat{a}_0, \hat{a}_2$ and $\hat{a}_1, \hat{a}_3$. The second matrix ($S_2^{(2)}$) represents the second stage of the Cooley–Tukey algorithm where two BS–PS components combine the operators $\hat{a}_0 + \hat{a}_2$, $\hat{a}_1 + \hat{a}_3$ and the operators $\hat{a}_0 - \hat{a}_2$, $\hat{a}_1 - \hat{a}_3$.

$$S_1^{(2)} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix};$$

$$S_2^{(2)} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & \mathrm{i} \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & -\mathrm{i} \end{bmatrix}, \tag{9}$$

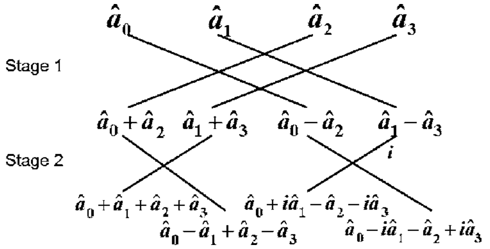
$\hat{a}_0$
$\hat{a}_1$
$\hat{a}_2$
$\hat{a}_3$
Stage 1
$\hat{a}_0 + \hat{a}_2$
$\hat{a}_1 + \hat{a}_3$
$\hat{a}_0 - \hat{a}_2$
$\hat{a}_1 - \hat{a}_3$
i
Stage 2
$\hat{a}_0 + \hat{a}_1 + \hat{a}_2 + \hat{a}_3$
$\hat{a}_0 + i\hat{a}_1 - \hat{a}_2 - i\hat{a}_3$
$\hat{a}_0 - \hat{a}_1 + \hat{a}_2 - \hat{a}_3$
$\hat{a}_0 - i\hat{a}_1 - \hat{a}_2 + i\hat{a}_3$

Fig. 2. Graphical representation of the transformation using BS–PS components (represented by the intersection of the lines) of input operators $\hat{a}_0$, $\hat{a}_1$, $\hat{a}_2$, and $\hat{a}_3$, to get the output operators defining the DFT. The line indicated by the letter i has an extra PS on it. This schematic represents the Cooley–Tukey algorithm based on two stage (Refs. 15–18).

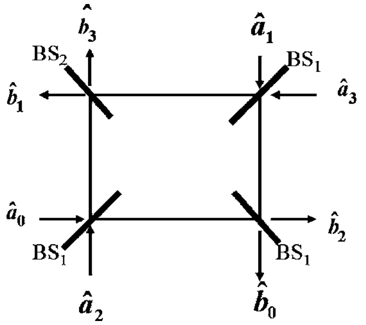

Fig. 3. Optical circuit representing a two-qubit DFT [all BSs have an upper index (2) though not explicitly written]. The 4D circuit is composed of twice the previous 2D DFT circuits connected through two other BS–PS components one of which is the same as a 2D DFT and one new BS–PS component. The use of multiport beam splitters for quantum computation has been analyzed in the literature [i.e., Ref. 20].

3. Each line intersection represents a BS–PS component (actually all represent the balanced BS–PS component $\mathrm{BS}_1^{(1)}$ from Subsection 2.A except for one intersection in which an extra phase $\pm i$, is introduced). Thus the optical DFT circuit is composed of twice the previous 2D DFT circuits (a BS–PS component), where the output of each is connected to the output of the other through a BS–PS component (one of which is the same as a 2D DFT and one new BS–PS component). This optical circuit is depicted in Fig. 3.[30]

4. Three of the four BS–PS components are exactly the same as those of the 2D DFT ($\mathrm{BS}_1^{(1)} = \mathrm{BS}_1^{(2)}$), but the fourth BS–PS component is different in the sense that a different PS has been introduced (the BS is still balanced) with half the phase shift compared to the others:

$$\mathrm{BS}_2^{(2)} = U\left(\frac{\pi}{4}, \frac{\pi}{4}, \frac{7\pi}{4}, \frac{\pi}{2}\right). \tag{10}$$

In this notation $\mathrm{BS}_1^{(2)} = \mathrm{BS}_1^{(1)} = U(2\pi/4, \pi/4, 8\pi/4, \pi/2)$, where the upper index represents the number of qubits in the DFT, and the lower index represents the different BS–PS components.

Using this method we have implemented the 2-qubit–4D DFT using only four BS–PS components, as opposed to the method devised by Reck *et al.*[2] for the linear optical implementation of any unitary operation, in which six BS–PS components are necessary.

C. Eight-Dimensional Discrete Fourier Transform

1. For the 3-qubit–8D DFT we find by using Eq. (5):

$$\mathrm{QFT}(3)=\frac{1}{2\sqrt{2}}\begin{bmatrix}1 & 1 & 1 & 1 & 1 & 1 & 1 & 1\\ 1 & e^{i(\pi/4)} & i & e^{i(3\pi/4)} & -1 & e^{i5(\pi/4)} & -i & e^{i(7\pi/4)}\\ 1 & i & -1 & -i & 1 & i & -1 & -i\\ 1 & e^{i(3\pi/4)} & -i & e^{i(\pi/4)} & -1 & e^{i(7\pi/4)} & i & e^{i(5\pi/4)}\\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1\\ 1 & e^{i(5\pi/4)} & i & e^{i(7\pi/4)} & -1 & e^{i(\pi/4)} & -i & e^{i(3\pi/4)}\\ 1 & -i & -1 & i & 1 & -i & -1 & i\\ 1 & e^{i(7\pi/4)} & -i & e^{i(5\pi/4)} & -1 & e^{i(3\pi/4)} & i & e^{i(\pi/4)}\end{bmatrix}. \quad (11)$$

2. Using the Cooley–Tukey algorithm (represented in Fig. 4) this transformation matrix breaks down to the multiplication of three matrices $\mathrm{QFT}(3)=S_3^{(3)}S_2^{(3)}S_1^{(3)}$. Each matrix (lower index i) represents a different stage i in the Cooley–Tukey algorithm:

$$S_3^{(3)}=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 1 & e^{i\frac{\pi}{4}} & 0 & 0\\ 0 & 0 & 1 & i & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & e^{i(3\pi/4)}\\ 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 1 & -e^{i(\pi/4)} & 0 & 0\\ 0 & 0 & 1 & -i & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -e^{i(3\pi/4)}\end{bmatrix}, \quad (12)$$

$$S_2^{(3)}=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 0 & 1 & 0 & 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0\\ 1 & 0 & -1 & 0 & 0 & 0 & 0 & 0\\ 0 & 1 & 0 & -1 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 1 & 0 & i & 0\\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & i\\ 0 & 0 & 0 & 0 & 1 & 0 & -i & 0\\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & -i\end{bmatrix}, \quad (13)$$

$$S_1^{(3)}=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 0 & 0 & 0 & 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1\\ 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0\end{bmatrix}. \quad (14)$$

3. The optical circuit performing the 3-qubit–8D DFT is composed as follows: Each intersection represents a BS–PS component multiplied by a phase factor. Thus the circuit is composed of two 4D DFT circuits (four BS–PS components) where the four outputs are combined with each other through a BS–PS component (two of these BS–PS components are the same as a those from the 4D DFT, and two are new BS–PS components). The circuit is depicted in Fig. 5.

4. All of the BS–PS components required consist of balanced BS ($\beta=\pi/4$) but different PS that must reach the resolution of at least $\pi/8$. For the 3-qubit–8D DFT one finds both the components of $\mathrm{BS}_1^{(1)}$ of Subsection 2.A found in the 2D DFT and of $\mathrm{BS}_2^{(2)}$ of Subsection 2.C found in the 4D DFT, but also two new components, which contain a balanced BS but a different PS:

$$BS_3^{(3)}=U\left(\frac{3\pi}{8},\frac{\pi}{4},\frac{15\pi}{8},\frac{\pi}{2}\right). \quad (15)$$

$$BS_4^{(3)}=U\left(\frac{\pi}{8},\frac{\pi}{4},\frac{13\pi}{8},\frac{\pi}{2}\right). \quad (16)$$

Once again, in the notation where the upper index describes the number of qubits and the lower index representing the different BS–PS components, $\mathrm{BS}_1^{(3)}=\mathrm{BS}_1^{(2)}=\mathrm{BS}_1^{(1)}=U(4\pi/8,\pi/4,16\pi/8,\pi/2)$ and $\mathrm{BS}_2^{(3)}=\mathrm{BS}_2^{(2)}=U(2\pi/8,\pi/4,14\pi/8,\pi/2)$.

D. n-Qubit–2^n Dimensional Discrete Fourier Transform

1. An n-qubit–2^n-dimensional DFT can be represented by the $2^n \times 2^n$ unitary matrix of Eq. (5).

2. The Cooley–Tukey algorithm breaks down the $2^n \times 2^n$ unitary matrix into n unitary matrices, each representing a different stage in the Cooley–Tukey algorithm where in each stage 2^n inputs are combined using 2^{n-1} BS–PS components. Thus the algorithm requires $n2^{n-1}$ BS–PS components instead of the 2^{2n} components required for any unitary matrix.

Stage k $(1 \le k \le n)$ can be divided into 2^{k-1} groups of 2^{n-k+1} inputs, where for group m the input j is combined (using a balanced BS) with input $j+2^{n-k}$ of the same group, which is multiplied by a phase factor $\phi = e^{(\pi i/2^k)f(k,m)}$ (using a PS). For the group m of stage k the function $f(k,m)$ is defined as the number m represented in k bits (base 2) where its digits are reversed, so that, for example, for group $m=100$ (4 in base 2) in stage $k=3$ the reversed order is 001 (1 in base 2) and thus the function $f(3,4)=1$. Another way of defining $f(k,m)$ recursively would be

$$f(1,1) = 0. \tag{17}$$

$$f(k,m) = 2f(k-1,m) \quad \text{for } m \in \{1, \ldots, 2^{k-2}\}. \tag{18}$$

$$f(k,m) = 2f(k-1,m-2^{k-2}) + 1 \quad \text{for } m \in \{2^{k-2} + 1, \ldots, 2^{k-2}\}. \tag{19}$$

Another stage should be added at the end to rearrange the order of the outputs.

For example, in the third stage $(k=3)$ of a 4-qubit–16D DFT $(n=4)$ the 16 inputs are divided into four groups of four inputs where the combinations are between inputs 0 and 2, 1 and 3; 4 and 6, 5 and 7; 8 and 10, 9 and 11; 12 and 14, 13 and 15. Inputs 6 and 7 are multiplied by the phase $e^{(\pi i/8)4}$, inputs 10 and 11 are multiplied by the phase $e^{(\pi i/8)2}$, and inputs 14 and 15 are multiplied by the phase $e^{(\pi i/8)6}$.

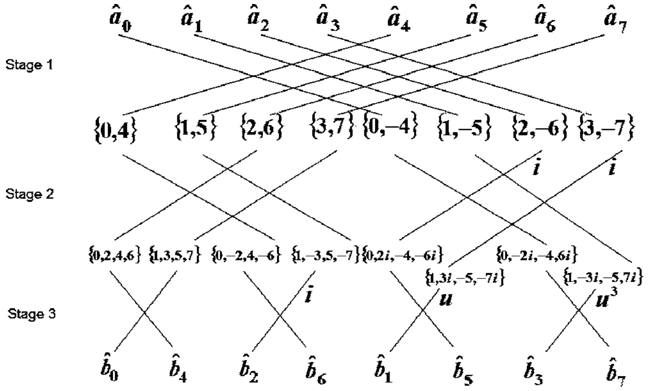
$\hat{a}_0$ $\hat{a}_1$ $\hat{a}_2$ $\hat{a}_3$ $\hat{a}_4$ $\hat{a}_5$ $\hat{a}_6$ $\hat{a}_7$
Stage 1
{0,4} {1,5} {2,6} {3,7} {0,−4} {1,−5} {2,−6} {3,−7}
Stage 2
i i
{0,2,4,6} {1,3,5,7} {0,−2,4,−6} {1,−3,5,−7} {0,2i,−4,−6i} {0,−2i,−4,6i}
{1,3i,−5,−7i} {1,−3i,−5,7i}
Stage 3
i u u^3
$\hat{b}_0$ $\hat{b}_4$ $\hat{b}_2$ $\hat{b}_6$ $\hat{b}_1$ $\hat{b}_5$ $\hat{b}_3$ $\hat{b}_7$

Fig. 4. Graphical representation of the transformation using BS–PS components (represented by the intersection of the lines) of input operators $\hat{a}_i$ with $i=0,\ldots,7$, to get the output operators $\hat{b}_i$ with $i=0,\ldots,7$. The lines indicated by the letter i, u, u^3 have an extra PS on them with phase $\pi/2$, $\pi/4$, and $3\pi/4$, respectively. (In the intermediate stage, for the use of short notation, only the subscripts, signs and phases of the annihilation operators are denoted). This schematic represents the Cooley–Tukey transform (Refs. 15–18) based on three stages.

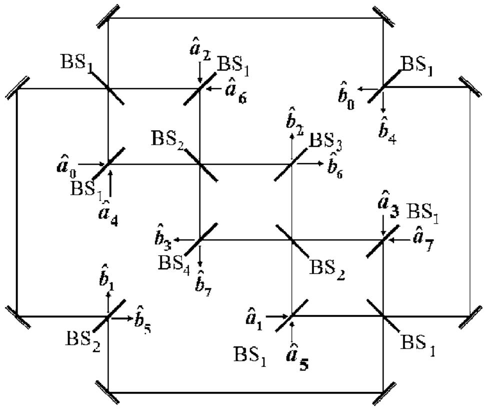

Fig. 5. Optical circuit representing a three-qubit DFT [all BSs have an upper index (3) though not explicitly written]. The circuit is composed of two 4D DFT circuits where the outputs are combined through two BS–PS components, two of which are the same as a those from the 4D DFT and two are new BS–PS components. In this figure the multiport BSs (Ref. 20) realize the Cooley–Tukey transform (Refs. 15–18) for an 8D DFT.

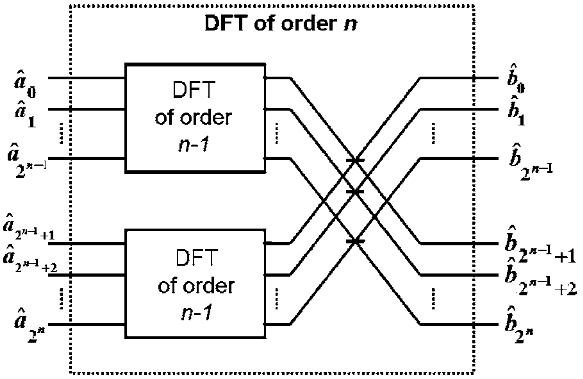

Fig. 6. Optical circuit representing an n-qubit–2^n-dimensional DFT composed recursively using two 2^{n-1}-dimensional DFTs. Each of the outputs of one of these circuits is combined with the outputs of the other using BS–PS components such that they consist of a series of 2^{n-2} components similar to those used in the 2^{n-1}-dimensional DFT and 2^{n-2} components that differ by a phase factor of $\pi/2^n$.

From the graphical representation we can easily find the matrices $S_k^{(n)}$. The combination of any two inputs p and q (e.g., 12 and 14 from the above example) where $q > p$ contributes four elements to the matrices. The value of the matrix elements $(p+1,p+1)$ and $(q+1,p+1)$ are $1/\sqrt{2}$ [e.g., (13,13) and (15,13) for the above example], while the value of elements $(p+1,q+1)$ and $(q+1,q+1)$ are $\phi/\sqrt{2}$ and $-\phi/\sqrt{2}$, respectively [e.g., (13,15) and (15,15) are $e^{(3\pi i/4)}$ and $-e^{(3\pi i/4)}$ for the above example]. All other elements are 0. Thus one finds

$$\mathrm{QFT}(n) = R^{(n)} S_n^{(n)} S_{n-1}^{(n)}, \ldots, S_2^{(n)} S_1^{(n)}, \tag{20}$$

where $R^{(n)}$ is the matrix rearranging the order of outputs from $\{\hat{b}_{i_j}\}$ to $\{\hat{b}_j\}$ with $j=0,\ldots,2^{n-1}-1$ and $i_j \in \{0,\ldots,2^{n-1}-1\}$ (notice that Eqs. (9) and (12) include $R^{(2)}$ and $R^{(3)}$ already multiplied into $S_2^{(2)}$ and $S_3^{(3)}$, respectively).

In the example where $n=4$ we find

$$S_3^{(4)} = \frac{1}{\sqrt{2}}\begin{bmatrix}
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & i & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & i & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & -i & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & -i & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & e^{(\pi i/4)} & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & e^{(\pi i/4)} & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & -e^{(\pi i/4)} & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & -e^{(\pi i/4)} & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & e^{3(\pi i/4)} & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & e^{3(\pi i/4)} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & -e^{3(\pi i/4)} & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & -e^{3(\pi i/4)}
\end{bmatrix}. \tag{21}$$

3. An n-qubit–2^n dimensional DFT optical circuit can easily be recursively assembled out of two $(n-1)$-qubit–2^{n-1}-dimensional DFT optical circuits where each of the outputs of one of these circuits is combined with the outputs of the other using one BS–PS component as depicted in Fig. 6. The combining BS–PS components consist of a series of 2^{n-2} components similar to those used in the $(n-1)$-qubit–2^{n-1}-dimensional DFT, and the 2^{n-2} components that differ by a phase factor of $\pi/2^n$.

4. All of the BS–PS components required consist of a balanced BS ($\beta=\pi/4$), but different PS that must reach the resolution of at least $\pi/2^n$. Thus

$$\mathrm{BS}_j^{(n)} = U\left(\frac{(2^{n-1}-j+1)\pi}{2^n}, \frac{\pi}{4}, \frac{(2^{n+1}-j+1)}{2^n}\pi, \frac{\pi}{2}\right), \tag{22}$$

where $j=0,1,\ldots,2^n-1$.

Reck *et al.*[2] showed that any unitary transformation of 2^n optical modes could be implemented with a 2^n port interferometer. Their method gave a general description for a transformation using $2^n(2^n-1)/2$ BS–PS elements. The method explained above, though relevant to the special case of the QFT uses only $n2^n$ BS–PS elements. Thus for large numbers of qubits we find a large saving by a factor of $2^n/n$ of the number of BS–PS elements. The lower number of BS–PS components is the same as the one calculated by Törmä *et al.*[19] for the general case of an N-dimensional DFT (where N does not necessarily equal 2^n).

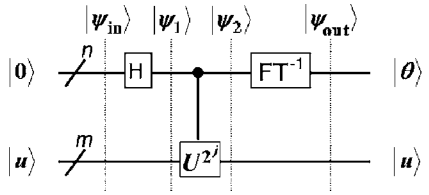

Fig. 7. A quantum circuit used to find an n qubit estimation of the phase θ of the eigenvalue $e^{i\theta}$ of a unitary operator U with an m qubit representation of the eigenvector $|u\rangle$. $|\psi_i\rangle$ are the intermediate quantum states. This schematic is a standard figure in quantum computation (Ref. 26).

3. PHOTON STATES AND PHASE ESTIMATION MEASUREMENTS

The objective of phase estimation is to find an n-qubit estimation of the phase θ of the eigenvalue $e^{i\theta}$ of a unitary operator U with an m-qubit representation of the eigenvector $|u\rangle$. We assume that we can prepare the state $|u\rangle$ and the operator-controlled U^{2^j} $(c-U^{2^j})$ where j is a nonnegative integer. The well-known quantum circuit solving this problem is given in Fig. 7, with an output given by[31]

$$|0\rangle^n|u\rangle \rightarrow \frac{1}{2^{n/2}}\sum_{y=0}^{2^n-1} e^{i\theta y}|y\rangle|u\rangle. \tag{23}$$

As shown in Fig. 7 the input to the system is

$$|\psi_{\text{in}}\rangle = |0\rangle^n|u\rangle. \tag{24}$$

This circuit can be divided into several steps. The first is performing a Hadamard transformation on $|0\rangle^n$:

$$|\psi_1\rangle = H^n|0\rangle^n|u\rangle = (H^n \otimes I^m)|0\rangle^n|u\rangle. \tag{25}$$

The second step includes the correlation between the register with $|0\rangle^n$ and the one with $|u\rangle$ that is achieved by using a $c-U^{2^j}$ gate. Owing to Eq. (23) the register containing $|u\rangle$ could be considered unchanged and even though the phase ϕ is determined by it, it could be perceived that the transformation is performed on the first register alone. Thus we find that

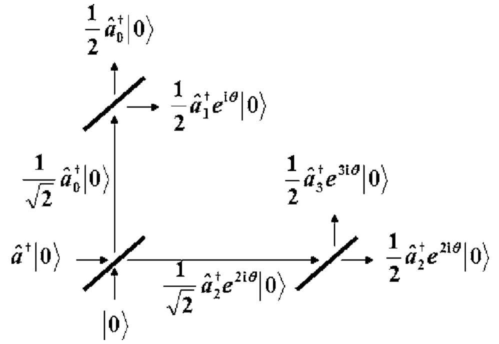
$\frac{1}{2}\hat{a}_0^\dagger|0\rangle$
$\frac{1}{2}\hat{a}_1^\dagger e^{i\theta}|0\rangle$
$\frac{1}{\sqrt{2}}\hat{a}_0^\dagger|0\rangle$
$\frac{1}{2}\hat{a}_3^\dagger e^{3i\theta}|0\rangle$
$\hat{a}^\dagger|0\rangle$
$\frac{1}{2}\hat{a}_2^\dagger e^{2i\theta}|0\rangle$
$\frac{1}{\sqrt{2}}\hat{a}_2^\dagger e^{2i\theta}|0\rangle$
$|0\rangle$

Fig. 8. Experimental setup transforming the operator $\hat{a}^\dagger$ into $\frac{1}{2}(\hat{a}_0^\dagger+\hat{a}_1^\dagger e^{i\theta}+\hat{a}_2^\dagger e^{2i\theta}+\hat{a}_3^\dagger e^{3i\theta})$ [any one photon state could be produced by just a BSs setup (Ref. 26)]. For one photon inserted into the optical system the state given by Eq. (32), corresponding to $s=4$, is produced (using a balanced BS and relevant PS).

$$|\psi_2\rangle = R_\theta^n|\psi_1\rangle = (R_\theta^n \otimes I^m)|\psi_1\rangle, \tag{26}$$

where

$$R_\theta^n = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & e^{i\theta} & 0 & \cdots & 0 \\ 0 & 0 & e^{2i\theta} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & e^{(2^n-1)i\theta} \end{bmatrix}. \tag{27}$$

The final step of the algorithm includes an inverse FT on the first register alone:

$$|\psi_{\text{out}}\rangle = \text{FT}_n^{-1}|\psi_2\rangle = (\text{FT}_n^{-1} \otimes I^m)|\psi_2\rangle. \tag{28}$$

The output of the whole algorithm is given by

$$|\psi_{\text{out}}\rangle = (\text{FT}_n^{-1} \otimes I^m)(R_\theta^n \otimes I^m)(H^n \otimes I^m)|0^n|u\rangle = P_n^m|0\rangle^n|u\rangle. \tag{29}$$

Notice that even though it seems $|u\rangle$ does not explicitly contribute to the algorithm, the phase θ is determined by it. Thus for the case where $n,m=1$:

$$P_n^m = \begin{bmatrix} 1+e^{i\theta} & 1-e^{i\theta} & 0 & 0 \\ 1-e^{i\theta} & 1+e^{i\theta} & 0 & 0 \\ 0 & 0 & 1+e^{i\theta} & 1-e^{i\theta} \\ 0 & 0 & 1-e^{i\theta} & 1+e^{i\theta} \end{bmatrix}. \tag{30}$$

In the following examples we show measurements of the phase shift introduced by a linear optical system. Although other methods for measuring phase shifts will be more effective and simpler, the present method of measuring phase shifts is introduced as a simple example for phase estimation by photons that can lead to order finding as will be analyzed in the next section. This method should therefore be important as it is an essential component in prime factorization.

Let us assume that we have a linear optical system that leads to a phase shift θ that can be expressed as

$$\theta = 2\pi\left(\frac{\theta_1}{2}+\frac{\theta_2}{4}+\frac{\theta_3}{8}+\cdots+\frac{\theta_n}{2^n}\right), \tag{31}$$

where $0_i \in \{0,1\}$. For very large values of n Eq. (31) can be used as a good approximation for θ but for the simplicity of the calculation we assume that the expression of Eq. (31) is exact. Our first aim is to show how θ can be measured by the DFT.

We assume that a one-photon state of order s, given by

$$\frac{1}{s^{1/2}}\sum_{j=0}^{s-1}\hat{a}_j^\dagger \exp(\mathrm{i}j\theta)|0\rangle. \tag{32}$$

can be produced. This state can be introduced by inserting the one-photon state $(\hat{a}^\dagger|0\rangle)$ in an optical system composed of BS–PS components. In states given by Eq. (32) the rail associated with the photon (the j port) is correlated to its phase $\exp(\mathrm{i}j\theta)$.[32] Figure 8 describes the experimental setup for producing the state given by Eq. (32) for $s=4$ $(n=2)$.

Using the methods described in Section 2 we can find the phase of the state given by Eq. (32) by using the DFT experimental scheme of order s where the component j of the state is inserted into the input port j. The output operatoric vector $\vec{\hat{b}}$ is given by multiplying the operatoric vector $\vec{\hat{a}}$ from the left by the matrix QFT(n) given by Eq. (5) (where $s=2^n$). Due to the special form of the input state given by Eqs. (31) and (32) the DFT of Eq. (32) would lead to only one component of the operatoric vector $\vec{\hat{b}}$ [assuming n is finite in Eq. (31)] so that the one photon will be measured only in one output port, and there will be a one-to-one correspondence between the set of numbers $\theta_i \in \{0,1\}$ describing θ and the corresponding output port. We give, however, a more general procedure for obtaining the output for the input state described by Eq. (32) by the use of the DFT. This procedure is not limited to the special form of θ described above.

To find the output of this scheme using the DFT we express the operatoric vector $\vec{\hat{a}}$ using the operatoric vector $\vec{\hat{b}}$ multiplied on the left by the inverse of Eq. (5):

$$\begin{pmatrix} \hat{a}_0^\dagger \\ \hat{a}_1^\dagger \\ \vdots \\ \hat{a}_{2^n-1}^\dagger \end{pmatrix} = \text{QFT}^{-1}(n)\begin{pmatrix} \hat{b}_0^\dagger \\ \hat{b}_1^\dagger \\ \vdots \\ \hat{b}_{2^n-1}^\dagger \end{pmatrix}. \tag{33}$$

Using Eq. (33) the operators $\hat{a}_j$ of Eq. (32) can be expressed as linear combinations of the operators $\vec{b}_k$ $(k=1,2,\ldots,2^n-1)$. For the special cases where the input states are given by Eqs. (31) and (32) the photon has the probability to be measured in only one output port j where there will be a one-to-one correspondence between the set of numbers $\theta_i \in \{0,1\}$ describing θ and the corresponding output port. We demonstrate this effect for $n=2$:

$$\begin{pmatrix}\hat a_0^\dagger\\ \hat a_1^\dagger\\ \hat a_2^\dagger\\ \hat a_3^\dagger\end{pmatrix}=\frac{1}{2}\begin{bmatrix}1 & 1 & 1 & 1\\ 1 & -\mathrm{i} & -1 & \mathrm{i}\\ 1 & -1 & 1 & -1\\ 1 & \mathrm{i} & -1 & -\mathrm{i}\end{bmatrix}\begin{pmatrix}\hat b_0^\dagger\\ \hat b_1^\dagger\\ \hat b_2^\dagger\\ \hat b_3^\dagger\end{pmatrix}$$

$$=\begin{bmatrix}\hat b_0^\dagger+\hat b_1^\dagger+\hat b_2^\dagger+\hat b_3^\dagger\\ \hat b_0^\dagger-i\hat b_1^\dagger-\hat b_2^\dagger+i\hat b_3^\dagger\\ \hat b_0^\dagger-\hat b_1^\dagger+\hat b_2^\dagger-\hat b_3^\dagger\\ \hat b_0^\dagger+i\hat b_1^\dagger+\hat b_2^\dagger-i\hat b_3^\dagger\end{bmatrix}. \qquad (34)$$

We therefore find that

$$\sum_{j=0}^{3}\hat a_j^\dagger e^{ij\theta}\rightarrow\frac{1}{2}(\hat b_0^\dagger+\hat b_1^\dagger+\hat b_2^\dagger+\hat b_3^\dagger)+(\hat b_0^\dagger-i\hat b_1^\dagger-\hat b_2^\dagger+i\hat b_3^\dagger)e^{i\theta}$$
$$+(\hat b_0^\dagger-\hat b_1^\dagger+\hat b_2^\dagger-\hat b_3^\dagger)e^{2i\theta}+(\hat b_0^\dagger+i\hat b_1^\dagger+\hat b_2^\dagger-i\hat b_3^\dagger)e^{3i\theta}. \qquad (35)$$

For the special cases of Fig. 8 where $s=4$ we obtain

$$\frac{1}{2}\sum_{j=0}^{3}\hat a_j^\dagger e^{ij\theta}\rightarrow\begin{bmatrix}\hat b_0^\dagger \text{ for } \theta=0 & (\theta_1=0;\theta_2=0)\\ \hat b_1^\dagger \text{ for } \theta=\pi/2 & (\theta_1=1;\theta_2=0)\\ \hat b_2^\dagger \text{ for } \theta=\pi & (\theta_1=0;\theta_2=1)\\ \hat b_3^\dagger \text{ for } \theta=3\pi/2 & (\theta_1=1;\theta_2=1)\end{bmatrix}. \qquad (36)$$

One should notice that because of the use of operatoric vectors rather than the vectors of the computational basis states the above formalism is more general but reduces to the conventional one for a one-photon state. Instead of using a one-photon state as given by Eq. (32) we can use the n-photon state given by

$$\frac{1}{s^{1/2}}\sum_{j=0}^{s-1}\frac{(\hat a_j^\dagger \exp(\mathrm{i}j\theta))^n}{\sqrt{n!}}|0. \qquad (37)$$

For example, if instead of inserting the one-photon state into the experimental scheme of Fig. 8 we insert an n-photon number state, we produce the state

$$\frac{1}{2}\sum_{j=0}^{3}\frac{(\hat a_j^\dagger)^n\exp(\mathrm{i}jn\theta)}{\sqrt{n!}}|0\rangle. \qquad (38)$$

Repeating the calculation of Eq. (36) for the special values of θ given by Eq. (31) we find that the n photons will be measured in one output port. Once again we get a one-to-one correspondence between the set of numbers $\theta_i \in \{0,1\}$ describing θ and the corresponding output port for the measured photons that is the same as that obtained for the one-photon case.

Although the above methods can be used for measuring the phase shift of a linear optical system, the additional advantages of using this method are for order finding in a prime factorization scheme, or more generally to obtain the period of a function $f(x)$ $(x=0,1,2,3,\ldots)$, as will be analyzed in Section 4. We point out that our analysis has been limited by the special form of θ given by Eq. (31). In the case where such a relation is not accurate, but still a good approximation for large values of n, there is a certain probability that the photon instead of being measured in the expected port j will be measured in port $\tilde{j}$ where $|j-\tilde{j}|$ should be very small.

4. IMPLEMENTATION OF ORDER FINDING BY THE USE OF LINEAR OPTICS

The search for a polynomial algorithm for the prime factorization problem has been going on for several centuries with no classical results. Shor's quantum factoring algorithm has solved this problem thus potentially speeding up such algorithms exponentially. The algorithm for factoring an integer N is based on calculating the period r of the function $F^j \pmod N$ $(j=0,1,2,\ldots)$ for a randomly selected integer F between 1 and N such that the greatest common devisor of F and N equals 1.[22,23] Once the period r is known two of the factors of N are obtained by calculating the great common divisor of N and $F^{r/2}\pm 1$ (The process fails if r is odd or r is even but gives a trivial solution[22,23]).

We assume that by using BS–PS components we can build the one-photon state (where $s=2n$):

$$|\psi\rangle=\frac{1}{s^{1/2}}\sum_{j=0}^{s-1}\hat a_j^\dagger e^{if_j}|0\rangle=\frac{1}{\sqrt{s}}(\hat a_0^\dagger e^{if_0}+\hat a_1^\dagger e^{if_1}+\hat a_2^\dagger e^{if_2}$$
$$+\cdots+\hat a_{s-1}^\dagger e^{if_{s-1}})|0\rangle, \qquad (39)$$

where the function f_j can be related to $F^j \pmod N$ by

$$f_j=2\pi\frac{F^j(\operatorname{mod} N)}{N}, \qquad (40)$$

so that by finding the periodicity of e^{if_j} we can find the period of the function $F^j \pmod N$ or any other periodic function modulo N.

In the state of Eq. (39) the rail associated with the photon is correlated to its phase e^{if_j}. The state in Eq. (39) can be prepared by using methods similar to those presented in Section 3. The system suggested here for period finding uses correlations between the photon phase and its associated rail as opposed to physical systems suggested previously for this purpose,[26] where a nonlinear medium was used to perform $c-U$ operations by facilitating an interaction between the photons. One should notice that a wave function of the one-photon state can be prepared as represented in Eq. (39) or this equation can be generalized to s photons by assuming

$$|\psi\rangle=\frac{1}{s^{1/2}}\sum_{j=0}^{s-1}\frac{(a_j^\dagger)^n}{(n\,!\,)^{1/2}}\exp(\mathrm{i}f_j)|0\rangle. \qquad (41)$$

To measure the periodicity of f_j we operate with the DFT on the operators $\hat a_j^\dagger$. They are transformed to operators $\hat b_k^\dagger$ as

$$\hat a_j^\dagger\rightarrow\frac{1}{s^{1/2}}\sum_{k=0}^{s-1}\exp(2\pi\mathrm{i}jk/s)\hat b_k^\dagger. \qquad (42)$$

Using Eq. (42) the state $|\psi\rangle$ of Eq. (39) is transformed into

$$|\psi'\rangle = \frac{1}{s}\sum_{j=0}^{s-1}\sum_{k=0}^{s-1}\exp(2\pi \mathrm{i}jk/s)\hat{b}_k^\dagger \exp(\mathrm{i}f_j)|0\rangle. \quad (43)$$

According to Shor's algorithm adapted to the state of Eq. (43), we can find the period of e^{if_j} by measuring the output port of the photons. The periodicity of the function e^{if_j} can be related to the periodicity of the output ports in which the photons are measured.

We demonstrate this effect by using the explicit expression of $|\psi'\rangle$ for $s=8$:

$$\begin{aligned}8|\psi'\rangle = (&\hat{b}_0^\dagger[e^{if_0}+e^{if_1}+e^{if_2}+\cdots+e^{if_7}]\\ &+\hat{b}_1^\dagger[e^{if_0}+e^{(2\pi/8)if_1}+e^{2(2\pi/8)if_2}+\cdots+e^{7(2\pi/8)if_7}]\\ &+\hat{b}_2^\dagger[e^{if_0}+e^{2(2\pi/8)if_1}+e^{4(2\pi/8)if_2}+\cdots+e^{14(2\pi/8)if_7}]\\ &\vdots\\ &+\hat{b}_7^\dagger[e^{if_0}+e^{7(2\pi/8)if_1}+e^{14(2\pi/8)if_2}+\cdots+e^{49(2\pi/8)if_7}])|0\rangle.\end{aligned} \quad (44)$$

An example that is expressed in a way similar to Eq. (44) has been described and analyzed by Berman *et al.*[33] We follow their example described for entangled atomic states but adapt the formalism to the present photon states. Assuming in this example [Ref. 33, Eq. 45] that the function f_j has the period $T=2$, i.e., $f_0=f_2=f_4=f_6$, and $f_1=f_3=f_5=f_7$, then the function $|\psi'\rangle$ can be written as

$$\begin{aligned}8|\psi'\rangle = (&\hat{b}_0^\dagger[4e^{if_0}+4e^{if_1}]+\hat{b}_1^\dagger[e^{if_0}(1+e^{i\pi/2}+e^{i\pi}+e^{3i\pi/2})\\ &+e^{if_1}(e^{i\pi/4}+e^{3i\pi/4}+e^{5i\pi/4}+e^{7i\pi/4})]\\ &+\hat{b}_2^\dagger[e^{if_0}(1+e^{i\pi}+1+e^{i\pi})\\ &+e^{if_1}(e^{i\pi/2}+e^{3i\pi/2}+e^{i\pi/2}+e^{3i\pi/2})]\\ &\vdots\\ &+\hat{b}_7^\dagger[e^{if_0}(1+e^{3i\pi/2}+e^{i\pi}+e^{i\pi/2})\\ &+e^{if_1}(e^{7i\pi/4}+e^{5i\pi/4}+e^{3i\pi/4}+e^{i\pi/4})]]|0\rangle.\end{aligned} \quad (45)$$

The complex amplitudes of $\hat{b}_1^\dagger e^{if_0}$ that are given in the brackets have the phases 0, $\pi/2$, π, and $3\pi/2$. Consequently, these amplitudes cancel each other. The complex amplitudes corresponding to $\hat{b}_1^\dagger e^{if_1}$ have the phases $\pi/4$, $3\pi/4$, $5\pi/4$, and $7\pi/4$, which also cancel each other. Following in a straightforward way we find that the complex amplitudes corresponding to $\hat{b}_2^\dagger$, $\hat{b}_3^\dagger$, $\hat{b}_5^\dagger$, $\hat{b}_6^\dagger$, and $\hat{b}_7^\dagger$ also vanish. However, those of $\hat{b}_0^\dagger$ and $\hat{b}_4^\dagger$ do not, and we find

$$|\psi'\rangle = \frac{1}{2}(\hat{b}_0^\dagger[e^{if_0}+e^{if_1}]+\hat{b}_4^\dagger[e^{if_0}+e^{i\pi}e^{if_1}])|0\rangle. \quad (46)$$

Using the above analysis we find that owing to the periodicity of the function the photon will be measured only in the output ports 0 and 4. The probabilities for the one photon to be measured in the output ports 0 and 4 are easily seen from Eq. (46) to be

$$\frac{|e^{if_0}+e^{if_1}|^2}{4} = \frac{1+\cos(f_0-f_1)}{2},$$

$$\frac{|e^{if_0}-e^{if_1}|^2}{4} = \frac{1-\cos(f_0-f_1)}{2}. \quad (47)$$

According to Shor's algorithm the photon will be measured in the output ports given by $k=m(D/T)$ with $m=0,1,\ldots,T-1$ where D is the number of output ports, and T is the periodicity of the function e^{if_j}. In the present simple example $D=8$ and $T=2$ so that $k=0,4$. Vice versa, from the knowledge of $k=0,4$ and $D=8$, one finds the periodicity $T=2$.

Our aim in analyzing the above specific example and in the above general analysis is to show a general method by which period finding can be realized in experimental linear optics. One should take into account that we have not changed the principles on which Shor's algorithm is based so that when we try to apply this specific experimental method to more general cases of order finding we should use general methods that have been developed in Shor's algorithm,[22,23,26] and we refer to the literature for this purpose. One should also take into account that order finding is only one component in Shor's prime factorization algorithm.

5. SUMMARY AND DISCUSSION

We have shown that the DFT of any n qubits can be realized in a linear optics system with a lower amount of BS–PS components than needed in the general case. The lower number of BS–PS components is the same as the one calculated by Törmä *et al.*[19] The difference between our work and theirs is that we give a specific algorithm to find the linear optical circuit by following the Cooley–Tukey algorithm and by using BS–PS optical components. An explicit evaluation of this general method for 1, 2, and 3 optical qubits has been described and analyzed in Section 2.

To implement quantum computation one needs to use interference and entanglement processes. While it is relatively easy to obtain the interference effects, the entanglement processes needed in quantum computation are difficult to achieve. The present work is based on the idea that by using BS–PS components in an optical system photon states can be produced in which the photons' associated rails (e.g., the input or output port) are correlated with their phase. We use such states for obtaining phase estimation and order finding.

In Section 3 it is shown how these states can be related to the phases of any linear optical system. Period finding is shown in Section 4 and is related to the measurement of these photon states. We believe that there is an advantage in the present approach since BS–PS optical components have been used extensively in quantum optics, and we do not need to use nonlinear media based quantum gates.

ACKNOWLEDGMENTS

We thank Ophir Topf for enlightening discussions and for drawing the graphical representations of optical circuits.

The corresponding author Y. Ben-Aryeh can be reached by e-mail at phr65yb@physics.technion.ac.il.

REFERENCES

1. A. Ekert, "Quantum interferometers as quantum computers," Phys. Scr. **1**, 218–222 (1998).
2. M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani, "Experimental realization of any discrete unitary operator," Phys. Rev. Lett. **73**, 58–61 (1994).
3. D. Bouwmeester, J. C. Howell, and A. Lamas-Linares, "Quantum information science using photons," in *Fundamentals of Quantum Information: Quantum Computation, Communication, Decoherence, and All That*, D. Heiss, ed. (Springer, 2002), pp. 149–197.
4. N. J. Cerf, C. Adami, and P. G. Kwiat, "Optical simulation of quantum logic," Phys. Rev. A **57**, R1477–R1480 (1998).
5. G. M. D'Ariano, C. Macchiavello, and L. Maccone, "Quantum computations with polarized photons," Fortschr. Phys. **48**, 573–577 (2000).
6. J. C. Howell and J. A. Yeazell, "Quantum computation through entangling single photons in multipath interferometers," Phys. Rev. Lett. **85**, 198–201 (2000).
7. S. Takeuchi, "A simple quantum computer: experimental realization of quantum computation algorithms with linear optics," Electron. Commun. Jpn. Part 3 **84**, 52–60 (2001).
8. S. Takeuchi, "Analysis of errors in linear-optics quantum computational," Phys. Rev. A **61**, 052302 (2000).
9. H. F. Hofmann and S. Takeuchi, "Quantum phase gate for photonic qubits using only beam splitters and postselection," Phys. Rev. A **66**, 024308/1–3 (2002).
10. T. C. Ralph, A. G. White, W. J. Munro, and G. J. Milburn, "Simple scheme for efficient linear optics quantum gates," Phys. Rev. A **65**, 012314 (2001).
11. G. J. Milburn, T. Ralph, A. White, E. Knill, and R. Laflamme, "Efficient linear optics quantum computation," Quantum Inf. Comput. **1**, 13–19 (2001).
12. E. Knill, R. Laflamme, and G. J. Milburn, "A scheme for efficient quantum computation with linear optics," Nature **409**, 46–52 (2001).
13. J. L. O'Brien, G. J. Pryde, A. G. White, T. C. Ralph, and D. Branning, "Demonstration of an all-optical quantum controlled-NOT gate," Nature **426**, 264–267 (2003).
14. N. Yoran and B. Reznik, "Deterministic linear optics quantum computation with single photon qubits," Phys. Rev. Lett. **91**, 037903/1–4 (2003).
15. J. W. Cooley and J. W. Tukey, "An algorithm for the machine calculation of complex Fourier series," Math. Comput. **19**, 297–301 (1965).
16. E. O. Brigham, *The Fast Fourier Transform* (Prentice-Hall, 1975).
17. H. J. Nussbaumer, *Fast Fourier Transform and Convolution Algorithms* (Springer, 1981).
18. J. S. Walker, *Fast Fourier Transforms*, (CRS Press, l996).
19. P. Törmä, I. Jex, and S. Stenholm, "Beam splitter realizations of totally symmetric mode couplers," J. Mod. Opt. **43**, 245–251 (1996).
20. M. Zukowski, A. Zeilinger, and M. A. Horne, "Realizable higher-dimensional two-particle entanglements via multiport beam splitters," Phys. Rev. A **55**, 2564–2579 (1997).
21. K. Mattle, M. Michler, H. Weinfurter, A. Zeilinger, and M. Zukowski, "Nonclassical statistics at multiport beam splitters," Appl. Phys. B **60**, S111–S117 (1995).
22. P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM J. Comput. **26**, 1484–1509 (1997).
23. A. Ekert and R. Jozsa, "Quantum computation and Shor's factoring algorithm," Rev. Mod. Phys. **68**, 733–753 (1996).
24. A. Ekert, P. Hayden, H. Inamori, and D. K. L. Oi, "What is quantum computation?" Int. J. Mod. Phys. A **16**, 3335–3363 (2001).
25. R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca, "Quantum algorithms revisited," Proc. R. Soc. London Ser. A **454**, 339–354 (1998).
26. M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge U. Press, 2000).
27. A. E. Siegman, "Fiber Fourier optics," Opt. Lett. **26**, 1215–1217 (2001).
28. U. Leonhardt, *Measuring the Quantum State of Light* (Cambridge U. Press, l997).
29. G. D. Bergland, "A guided tour of the fast Fourier transforms," IEEE Spectrum **6**, 41–52 (1969).
30. N. G. Walker, "Quantum theory of multiport optical homodyning," J. Mod. Opt. **34**, 15–60 (1987).
31. G. Benenti, G. Casati, G. Strini, *Principles of Quantum Computation and Information, Volume I: Basic Concepts* (World Scientific, 2004).
32. V. Vedral, "The role of relative entropy in quantum information theory," Rev. Mod. Phys. **74**, 197–234 (2002).
33. G. P. Berman, G. D. Doolen, R. Mainieri, and V. I. Tsifrinovich, *Introduction to Quantum Computers* (World Scientific, l998).