Design of quantum Fourier transforms and quantum algorithms by using circulant Hamiltonians

Boyan T. Torosov\textsuperscript{1} and Nikolay V. Vitanov\textsuperscript{1,2}

\textsuperscript{1}Department of Physics, Sofia University, James Bourchier 5 Boulevard, 1164 Sofia, Bulgaria
\textsuperscript{2}Institute of Solid State Physics, Bulgarian Academy of Sciences, Tsarigradsko Chaussee 72, 1784 Sofia, Bulgaria

We propose a technique for design of quantum Fourier transforms, and ensuing quantum algorithms, in a single interaction step by engineered Hamiltonians of circulant symmetry. The method uses adiabatic evolution and is robust against fluctuations of the interaction parameters as long as the Hamiltonian retains a circulant symmetry.

DOI: 10.1103/PhysRevA.80.022329  PACS number(s): 03.67.Ac, 32.80.Qk, 32.80.Xx, 03.67.Bg

\section{I. INTRODUCTION}

Quantum information processing is built upon sequences of special unitary transformations. One of the most important of these is the quantum (discrete) Fourier transform (QFT), which is a key ingredient of many quantum algorithms [1–3], including Shor’s factorization [4], algorithms of Deutsch [5] and Simon [6], order finding, discrete logarithms, quantum phase estimation, etc. [1].

Traditionally, QFT on \( r \) qubits is implemented by a quantum circuit consisting of \( O(r) \) Hadamard gates and \( O(r^2) \) controlled-phase gates [7]. Experimental demonstrations include synthesis of three-qubit QFT in nuclear magnetic resonance (NMR) systems [8], order finding with NMR [9], phase estimation with NMR [10], Shor’s factorization in NMR [11], in ion traps [12], and using a “compiled version” of Shor’s algorithm with photonic qubits [13,14]. Further theoretical proposals for implementations of QFT include atoms in cavity QED [15], entangled multilevel atoms [16], trapped ions with Householder reflections [17], linear optics [18] with the Cooley-Tukey algorithm [19], waveguide arrays [20], etc.

The largest numbers factorized experimentally by Shor’s algorithm hitherto are 15 [11,12] and 21 [21]. The primary obstacle for demonstration of Shor’s factorization for larger numbers is the large number of one- and two-qubit gates required. A “general-purpose” Shor’s algorithm for an \( L \)-bit number demands \( L^3 \) gates and \( 5L+1 \) qubits [22]; an implementation using a linear ion trap would require about 396\( L^3 \) laser pulses [22]. “Special-purpose” algorithms that exploit special properties of the input number are much faster (but still demand a great number of steps): the number 15 can be factored with 6 qubits and 38 pulses only [22].

Another practical difficulty of the QFT algorithm is the use of two-qubit controlled-phase gates, which, for large number of qubits, involve very small phases. To this end, an “approximate” QFT has been proposed \cite{7,23,24}, in which the phase shift gates requiring highest precision are omitted.

Griffiths and Niu proposed a “semiclassical” QFT, wherein the costly two-qubit gates are replaced by serial single-qubit rotations supplemented with classical measurements \cite{25}. Such a semiclassical QFT has been demonstrated recently with three trapped ions [12].

In the present work, we propose to construct QFT by an approach which uses a special class of Hamiltonians, having a circulant symmetry. Such Hamiltonians have the advantage that their eigenvectors are the columns of the QFT (hence the latter diagonalizes the Hamiltonian), and they do not depend on the particular elements of the Hamiltonian, as far as the circulant symmetry is conserved. This important feature allows one to construct QFT in a single interaction step; it also makes this technique robust against variations in the interaction parameters. The present paper uses a similar approach as Unanyan \textit{et al.} \cite{26}, who proposed to use circulant Hamiltonians in order to create coherent superpositions of states.

\section{II. BACKGROUND}

\textbf{Quantum Fourier transform.} The \( N \)-dimensional QFT is defined with its action on an orthonormal basis \( |0\rangle, |1\rangle, \ldots, |N-1\rangle \),

\begin{equation}
F^N|n\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i nk/N} |k\rangle.
\end{equation}

It transforms a single state into an equal superposition of states with specific phase factors. The inverse QFT is

\begin{equation}
(F^N)^{-1}|n\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{-2\pi i nk/N} |k\rangle.
\end{equation}

In a matrix form QFT is a square matrix with elements

\begin{equation}
F^N_{kn} = \frac{1}{\sqrt{N}} e^{2\pi i kn/N}.
\end{equation}

\textbf{Circulant matrix.} An \( N \times N \) matrix \( C \) of the form

\begin{equation}
C = \begin{bmatrix}
    c_0 & c_{N-1} & c_{N-2} & \cdots & c_1 \\
    c_1 & c_0 & c_{N-1} & \cdots & c_2 \\
    c_2 & c_1 & c_0 & \cdots & c_3 \\
    \vdots & \vdots & \vdots & \ddots & \vdots \\
    c_{N-1} & c_{N-2} & c_{N-3} & \cdots & c_0
\end{bmatrix}
\end{equation}

is called a circulant matrix. It is a special case of a Toeplitz matrix \cite{27} and it is completely defined by its first vector column (or row). The other columns (rows) are just cyclic permutations of it. The circulant matrices have some very interesting properties. The most important one in the present context is that the eigenvectors of a circulant matrix of a
given size are the vector columns of the discrete Fourier transform [Eq. (3)] of the same size; hence they do not depend on the elements of the circulant matrix. The eigenvalues \( \lambda_n \) of the circulant matrix, though, are phased sums of the matrix elements,

\[
\lambda_n = \sum_{k=0}^{N-1} c_k \exp(-i2\pi nk/N). \tag{5}
\]

III. DESIGN OF THE HAMILTONIAN

In order to synthesize QFT, we use a special time-dependent Hamiltonian of the form [26]

\[
H(t) = f(t)H_0 + g(t)H_1, \tag{6}
\]

where \( f(t) \) and \( g(t) \) are (generally pulse-shaped) real-valued functions, such that \( f(t) \) precedes \( g(t) \) in time, i.e.,

\[
\frac{8-\infty}{-\infty} \frac{g(t)}{f(t)} \to \infty. \tag{7}
\]

For instance, we can take

\[
f(t) = \frac{1 - \tanh(t/T)}{2}, \tag{8a}
\]

\[
g(t) = \frac{1 + \tanh(t/T)}{2}. \tag{8b}
\]

Therefore, Hamiltonian (6) has the asymptotics

\[
H_0 \leftarrow H(t) \to H_1. \tag{9}
\]

We demand \( H_0 \) to be a diagonal matrix in which the energies of all states (the diagonal elements) are nondegenerate,

\[
H_0 = \text{diag}(E_1, E_2, \ldots, E_N). \tag{10}
\]

For \( H_1 \) we choose a circulant matrix, with the condition that the eigenvalues should be well separated from each other. Because the Hamiltonian has to be Hermitian, \( H_1 \) is not a most general circulant matrix but a Hermitian circulant matrix.

Because Hamiltonian (6) at \( t \to \infty \) has a circulant symmetry, its eigenvectors are the vector columns of QFT. However, each eigenvector \( |n\rangle \) may have an adiabatic phase factor \( e^{i\alpha_n} \), acquired in the end of the evolution, which may be different for each \( |n\rangle \). This means that for such Hamiltonian (6), adiabatic evolution will perform QFT (1) (possibly after renumbering of the basis states) but with some additional phases \( \alpha_n \),

\[
|\mathbf{F}^N|n\rangle = \frac{1}{\sqrt{N}} e^{i\alpha_n} \sum_{k=0}^{N-1} e^{2\pi ik/N}|k\rangle. \tag{11}
\]

The phases \( \alpha_n \) are just integrals over the quasienergies, as follows from the adiabatic theorem [28]. The inverse Fourier transform is

\[
(\mathbf{F}^N)^{-1}|n\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{-i\alpha_k} e^{-2\pi ik/N}|k\rangle, \tag{12}
\]

and it can be accomplished by adiabatic evolution with the Hamiltonian

\[
H(t) = g(t)H_0 + f(t)H_1. \tag{13}
\]

For example, for \( N=4 \) we can have

\[
H_0 = \text{diag}(-E, -E/3, -E/3, E), \tag{14a}
\]

\[
H_1 = \begin{bmatrix} 0 & V & 0 & V \\ V & 0 & V & 0 \\ 0 & V^* & 0 & V \\ V & 0 & V^* & 0 \end{bmatrix}. \tag{14b}
\]

For laser-driven atomic and molecular transitions, the inter-

\[
\text{action} V \text{ is given by the Rabi frequency } \Omega: V=\Omega/\hbar. \text{ Insofar as the eigenvalues of the circulant matrix are given by Eq. (5), one has to choose the interaction energy } V \text{ in such a way that the eigenenergies have well separated values. Another requirement for adiabatic evolution is that the functions } f(t) \text{ and } g(t) \text{ change sufficiently slowly, so that the nonadiabatic coupling } \langle \chi_m(t)|\chi_n(t) \rangle \text{ between each pair of adiabatic states } |\chi_m(t)\rangle \text{ and } |\chi_n(t)\rangle \text{ remains negligibly small compared to the separation of the eigenenergies } e_m(t) \text{ and } e_n(t),
\]

\[
|e_m(t) - e_n(t)| \gg |\langle \chi_m(t)|\chi_n(t) \rangle| \sim \frac{1}{T}, \tag{15}
\]

where \( T \) is the interaction duration.

In the numeric examples we use a hyperbolic-secant mask for the functions \( f(t) \) and \( g(t) \),

\[
f(t) = \text{sech}(t/T)[1 - \tanh(t/T)], \tag{16a}
\]

\[
g(t) = \text{sech}(t/T)[1 + \tanh(t/T)]. \tag{16b}
\]

These factors are chosen for implementation feasibility; they do not change the (all-important) asymptotic behavior of the eigenstates \( |\chi_m(t)\rangle \). Figure 1 shows the evolution of the eigenvalues of Hamiltonian (6) for \( V=E(1+i/3) \). For this choice of \( V \) the eigenenergies are nondegenerate (except at infinite times, which is irrelevant because there is no inter-

IV. QUANTUM PHASE ESTIMATION

We shall show now that QFT propagator (11), which results from Hamiltonian (6), can be used to realize quantum
algorithms despite the presence of the adiabatic phase factors $e^{ia\phi}$. We consider the quantum phase estimation algorithm [1], which is the key for many other algorithms, such as Shor’s factorization. We briefly summarize here the essence of this algorithm.

Let us consider a unitary operator $U$, which has an eigenvector $|u\rangle$ and a corresponding eigenvalue $\exp(2\pi i \phi)$, where $\phi \in [0,1)$. We assume that we are able to prepare state $|u\rangle$ and to perform the controlled-$U^m$ operation for non-negative integer $j$. The goal of the algorithm is to estimate $\phi$. To this end, the algorithm uses two registers. The first register contains $r$ qubits initially in state $|0\rangle$ and the second one starts in state $|u\rangle$, containing as many qubits as needed to store $|u\rangle$.

The procedure starts with the application of a Hadamard transform [1] to the first register, followed by the application of controlled-$U$ operations on the second register, with $U$ raised to successive powers of 2. The final state of the first register is

$$2^{-r/2}(|0\rangle + e^{2\pi i 2^{-3/2} \phi}|1\rangle)|0\rangle + e^{2\pi i 2^{-3/2} \phi}|1\rangle|1\rangle + \ldots (0)$$

and the second register stays in state $|u\rangle$. Now let us suppose that $\phi$ can be expressed using a $r$-bit expansion,

$$\phi = 0, \phi_1 \phi_2 \ldots \phi_r = \frac{\phi_1}{2} + \frac{\phi_2}{4} + \cdots + \frac{\phi_r}{2^r},$$

where $0, \phi_1, \phi_2 \ldots \phi_r$ represents a binary fraction. Then state (17) can be written as

$$2^{-r/2}(|0\rangle + e^{2\pi i 0.\phi_1}|1\rangle)|0\rangle + e^{2\pi i 0.\phi_1}|1\rangle|1\rangle + \ldots (0)$$

Finally, we apply the inverse QFT in order to obtain the product state $|\phi_1 \ldots \phi_r\rangle$. In our case we apply the phased inverse QFT [Eq. (11)] and find

$$e^{-i\alpha(\phi)} |\phi_1 \ldots \phi_r\rangle,$$

where $\alpha(\phi)$ is an adiabatic phase that depends on $\phi$. Since this global phase $\alpha$ has no physical meaning, a measurement in the computational basis would give us exactly $\phi$. We note that if $\phi$ cannot be written as a $r$-bit expansion [Eq. (18)], this procedure can still produce a good approximation to $\phi$ with high probability [1].

In Fig. 2 we plot the probability of state (20) during the inverse Fourier transformation [Eq. (12)]. This probability is evaluated by solving numerically the Schrödinger equation for Hamiltonian (13) and is used as a measure of the fidelity. The figure shows that when the phase $\phi$ has an exact expansion as a binary fraction, the final probability tends to unity.

**V. IMPLEMENTATIONS**

In this section we discuss a few simple systems, which can be used for implementing Hamiltonian (6).

$J'=\frac{1}{2} \leftrightarrow J''=\frac{1}{2}$ system. As a first example we consider the system formed of the magnetic sublevels in a $J'=\frac{1}{2} \leftrightarrow J''=\frac{1}{2}$ transition shown in Fig. 3(a), where $J$ is the total angular momentum of each level. We apply two linearly polarized fields (the two polarization directions being perpendicular), the second one seen as a superposition of two circularly polarized fields ($\sigma_+$ and $\sigma_-$). By ordering the magnetic sublevels in the sequence $|m'=-\frac{1}{2}\rangle$, $|m'=\frac{1}{2}\rangle$, and by suitably tuning the strengths and the relative phase of the two independent fields, we can adjust the interaction elements of the Hamiltonian and produce the desired circulant form [Eq. (14b)]. We note that because of the different signs of some of the Clebsch-Gordan coefficients, one should redefine one of the probability amplitudes by changing its sign.

As we want to implement full Hamiltonian (6), we also need to realize its first part $H_0$. It is especially important to remove the degeneracies between the magnetic sublevels. This can be accomplished by using a magnetic field, which induces $m$-dependent Zeeman shifts, and a far-off resonant laser pulse, which will cause Stark shifts. Let the energy
splitting due to Zeeman shift be $E_Z$ (the same for both ground and excited levels). The Stark shifts are generally different for the two levels: $E_{g,S}$ and $E_{e,S}$, where “g” and “e” stand for ground and excited, respectively. Hence, in order to realize Hamiltonian (14a), we need to solve the following algebraic system:

\[
\begin{align*}
-\frac{1}{2}E_Z + E_{g,S} &= -E, \\
\frac{1}{2}E_Z + E_{g,S} &= -E/3, \\
-\frac{1}{2}E_Z + E_{e,S} &= E/3, \\
\frac{1}{2}E_Z + E_{e,S} &= E,
\end{align*}
\]

which gives $E_Z = E_{g,S} = -E_{e,S} = \frac{1}{2}E$. Moreover, because the energies of $H_0$ need not be exactly evenly separated, our method is robust against fluctuations in the field parameters. Making a reference to Eq. (6) and Fig. 2, we conclude that the Stark and Zeeman fields, with the time dependence $f(t)$, have to be applied before the polarized laser fields, with time dependence $g(t)$.

$J'=0 \leftrightarrow J'=1 \leftrightarrow J''=0$ system. Another system with $N=4$ is the diamond system depicted in Fig. 3(b). Here again two linearly polarized laser fields are needed, but now they have parallel polarization directions. One advantage of this system is that only magnetic fields are sufficient to realize the first part of the Hamiltonian. The disadvantage is that the two independent fields generally come from two different lasers because of the different frequencies of the transitions.

$J'=1 \leftrightarrow J'=1$ system. The $J'=1 \leftrightarrow J'=1$ system, depicted in Fig. 3(c), contains six coupled $m$ sublevels. In this system the circulant symmetry occurs because $m'=0 \leftrightarrow m''=0$ is a dipole forbidden transition. By ordering the magnetic sublevels in the sequence $|m'=1, |m''=0, |m'=1, |m''=1, |m'=0, |m''=1\rangle$ we obtain a Hamiltonian of the type

\[
H_1 = \frac{\hbar}{2} \begin{bmatrix}
0 & -\Omega_1 & 0 & 0 & 0 & -\Omega_2 \\
-\Omega_1^* & 0 & \Omega_1^* & 0 & 0 & 0 \\
0 & \Omega_1 & 0 & \Omega_2 & 0 & 0 \\
0 & 0 & \Omega_2^* & 0 & -\Omega_1^* & 0 \\
0 & 0 & 0 & -\Omega_1 & 0 & \Omega_1 \\
-\Omega_2^* & 0 & 0 & 0 & \Omega_1^* & 0
\end{bmatrix},
\]

where $\Omega_1$ and $\Omega_2$ are the Rabi frequencies between states with different $m$ and states with the same $m$, respectively. Each Clebsch-Gordan coefficient is incorporated in the respective Rabi frequency. The Rabi frequencies are complex (needed to avoid eigenvalue degeneracies), with a phase difference between the left and right circularly polarized components. After a phase transformation of the amplitudes, $c_n \rightarrow e^{i\beta_n}c_n$, with suitably chosen phase factors $\beta_n$ we can make the Hamiltonian take the form of a circulant matrix. The selection of the phases $\beta_n$ amounts to solving a simple linear algebraic system.

The first part of the Hamiltonian $H_0$ can be realized with auxiliary magnetic and electric fields, as for the $J'=\frac{1}{2} \leftrightarrow J''=\frac{1}{2}$ system.

VI. CONCLUSIONS

The intrinsic symmetry of circulant matrices allows one to design Hamiltonians that can produce a discrete Fourier transform on a set of quantum states in a natural manner and in a single step, without the need to apply a large number of consecutive quantum gates. The designed Hamiltonian has different asymptotics: it is a nondegenerate diagonal matrix in the beginning and a circulant matrix in the end (or vice versa); the time dependence that connects the two should be sufficiently slow in order to allow adiabatic evolution. The resulting unitary transformation, which this Hamiltonian produces, differs from the standard QFT by additional (adiabatic) phase factors in the matrix rows: we show, however, that one can still construct the quantum phase estimation algorithm, which is an essential subroutine in many quantum algorithms. We have presented examples of simple atomic systems, the Hamiltonians of which can be tailored to obtain circulant symmetry. The construction of large-scale systems with circulant symmetry requires the design of a closed-loop linkage pattern; for instance, a chain of nearest-neighbor interactions supplemented with a (direct or effective) interaction between the two ends of the chain.

ACKNOWLEDGMENTS

This work has been supported by the European Commission projects EMALI and FASTQUAST and the Bulgarian NSF Grant No. VU-F-205/06, No. VU-I-301/07, No. D002-90/08, and No. IRC-CoSiM.


