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

Boyan T. Torosov and Nikolay V. Vitanov

1Department of Physics, Sofia University, James Bourchier 5 blvd, 1164 Sofia, Bulgaria
2Institute of Solid State Physics, Bulgarian Academy of Sciences, Tsarigradsko chaussée 72, 1784 Sofia, Bulgaria

(Dated: October 6, 2009)

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.

PACS numbers: 03.67.Ac, 32.80.Qk, 32.80.Xx, 03.67.Bg

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 [1,2,3], including Shor’s factorization [4], the 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 [3]. Experimental demonstrations include synthesis of 3-qubit QFT in nuclear magnetic resonance (NMR) systems [3], order finding with NMR [8], 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 Cooley-Tukey’s 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: 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 control-phase gates, which, for large number of qubits, involve very small phases. To this end, an “approximate” QFT has been proposed [3,21,22], 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 [23]. Such a semiclassical QFT has been demonstrated recently with three trapped ions [12].

In the present work, we propose to construct QFT by a novel 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 techniques robust against variations in the interaction parameters. The present paper uses a similar approach as Unanyan et al. [26], who proposed to use circulant Hamiltonians in order to create coherent superpositions of states.

II. BACKGROUND

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

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

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

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

In a matrix form QFT is a square matrix with elements

\[
F^N_{kn} = \frac{1}{\sqrt{N}} e^{2\pi i k n/N}. \tag{3}
\]

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

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

\[
(4)
\]
is called a circulant matrix. It is a special case of a Toeplitz matrix \[27\] 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 \[9\] 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:

\[
\lambda_n = \sum_{k=0}^{N-1} c_k \exp(-12\pi kn/N). \tag{5}
\]

III. DESIGN OF THE HAMILTONIAN

In order to synthesize QFT, we use a special time-dependent Hamiltonian of the form \[21\]

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

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

\[
0 \xrightarrow{\sim} -t \frac{g(t)}{f(t)} \xrightarrow{\sim} \infty. \tag{7}
\]

For instance, we can take

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

Therefore, the Hamiltonian \[13\] has the asymptotics

\[
H_0 \xrightarrow{\sim} -t \quad H(t) \xrightarrow{\sim} \infty \quad H_1. \tag{9}
\]

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

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

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 the Hamiltonian \[13\] 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 a Hamiltonian \[13\], adiabatic evolution will perform the QFT \[11\] (possibly after renumbering of the basis states), but with some additional phases \(\alpha_n\),

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

FIG. 1: Eigenvalues of the Hamiltonian \[9\] as a function of time for \(H_0\) and \(H_1\) given by Eqs. \[14a\] and \[14b\], with \(V = E(1 + 1/3)\), whereas \(g(t)\) and \(f(t)\) are given by Eqs. \[16a\] and \[16b\].

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

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

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 interaction \(V\) is given by the Rabi frequency \(\Omega\): \(V = \frac{1}{2} \hbar \Omega\). Insofar as the eigenvalues of the circulant matrix are given by Eq. \[27\], one has to choose the interaction energy \(V\) in such a way that the eigenenergies have well separated values. Another requirement for adiabatic evolution is that the functions \(f(t)\) and \(g(t)\) change sufficiently slowly, so that the nonadiabatic coupling \(\langle \chi_m(t) | \chi_n(t) \rangle\) between each pair of adiabatic states \(|\chi_m(t)\rangle\) and \(|\chi_n(t)\rangle\) remains negligibly small compared to the separation of the eigenenergies \(\varepsilon_m(t)\) and \(\varepsilon_n(t)\),

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

where \(T\) is the interaction duration.

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

\[
f(t) = \text{sech}(t/\tau)[1 - \tanh(t/T)], \tag{16a}
g(t) = \text{sech}(t/\tau)[1 + \tanh(t/T)]. \tag{16b}
\]
These factors are chosen for implementation feasibility; they do not change the (all-important) asymptotic behaviour of the eigenstates \(|\chi_n(t)\rangle\). Figure 11 shows the evolution of the eigenvalues of the Hamiltonian (6) for \(V = E(1 + i/3)\). For this choice of \(V\) the eigenenergies are non-degenerate (except at infinite times, which is irrelevant because there is no interaction) and the adiabatic evolution is enabled.

IV. QUANTUM PHASE ESTIMATION

We shall show now that the QFT propagator \([11]\), which results from the Hamiltonian \([6]\), can be used to realize quantum algorithms, despite the presence of the adiabatic phase factors \(e^{i\alpha}\). 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-\(U^{2^j}\) 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 successsive powers of two. The final state of the first register is

\[
2^{-r/2}(|0\rangle + e^{2\pi i 2^{-r} \phi}|1\rangle)_{11}(|0\rangle + e^{2\pi i 2^{-r-2} \phi}|1\rangle)_{2} \cdots 
\times (|0\rangle + e^{2\pi i 2^{0} \phi}|1\rangle)_{r} = 2^{-r/2} \sum_{k=0}^{2^r-1} e^{2\pi i k \phi} |k\rangle, \quad (17)
\]

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

\[
\phi = 0.\phi_1\phi_2 \cdots \phi_r = \frac{\phi_1}{2} + \frac{\phi_2}{4} + \cdots + \frac{\phi_r}{2^r}, \quad (18)
\]

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

\[
2^{-r/2}(|0\rangle + e^{2\pi i 0.\phi_r}|1\rangle)_{11}(|0\rangle + e^{2\pi i 0.\phi_{r-1} \cdots \phi_1}|1\rangle)_{2} \cdots 
\times (|0\rangle + e^{2\pi i 0.\phi_1\phi_2 \cdots \phi_r}|1\rangle)_{r} = 2^{-r/2} \sum_{k=0}^{2^r-1} e^{2\pi i k \phi} |k\rangle, \quad (19)
\]

Finally, we apply the inverse QFT in order to obtain the product state \(|\phi_1 \cdots \phi_r\rangle\). In our case we apply the phased inverse QFT \([13]\) and find

\[
e^{-i\alpha(\phi)}|\phi_1 \cdots \phi_r\rangle, \quad (20)
\]

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 \([18]\), 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 \([12]\). This probability is evaluated by solving numerically the Schrödinger equation for the Hamiltonian \([14]\) 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 the 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. 2(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 \((\sigma_+\text{ and } \sigma_-)\). By ordering the magnetic sublevels in the sequence \(|m' = -\frac{1}{2}\rangle, |m' = \frac{1}{2}\rangle, |m'' = \frac{1}{2}\rangle, |m'' = -\frac{1}{2}\rangle\), 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 \([14]\). 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 the 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
Because $m' = 0 \leftrightarrow m'' = 0$ is a dipole forbidden transition. By ordering the magnetic sublevels in the sequence $|m' = -1\rangle$, $|m'' = 0\rangle$, $|m' = 1\rangle$, $|m'' = 1\rangle$, $|m' = 0\rangle$, $|m'' = -1\rangle$ we obtain a Hamiltonian of the type

$$H_1 = \frac{i}{\hbar} \begin{pmatrix}
0 & -\Omega_1 & 0 & 0 & -\Omega_2 & 0 \\
-\Omega_1^* & 0 & \Omega_1 & 0 & 0 & 0 \\
0 & \Omega_1 & 0 & \Omega_2 & 0 & 0 \\
0 & 0 & 0 & -\Omega_1^* & 0 & 0 \\
0 & 0 & 0 & 0 & \Omega_1 & 0 \\
-\Omega_2^* & 0 & 0 & 0 & \Omega_1^* & 0
\end{pmatrix},$$

where $\Omega_1$ and $\Omega_2$ are the Rabi frequencies between, respectively, states with different $m$ and states with the same $m$. 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 non-degenerate 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 enable adiabatic evolution. The resulting unitary transformation, which this Hamiltonian produces, differs from the standard QFT by additional (adiabatic) phase factors in the matrix columns: 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 Bul-
garian NSF grants VU-F-205/06, VU-I-301/07, D002-90/08, and IRC-CoSiM.

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).
[2] R. Jozsa, Proc. R. Soc. Lond. A 454, 323 (1998).
[3] C. M. Bowden, G. Chen, Z. Diao, A. Klappenecker, J. Math. Anal. Appl. 274, 69 (2002).
[4] P.W. Shor, in Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, edited by S. Goldwasser (IEEE Computer Society, Los Alamitos, CA, 1994), p. 124; SIAM J. Sci. Statist. Comput. 26, 1484 (1997); arXiv:quant-ph/9508027v2.
[5] D. Deutsch, Proc. R. Soc. Lond. A 400, 97 (1985); D. Deutsch and R. Jozsa, Proc. R. Soc. Lond. A 439, 553 (1992).
[6] D.R. Simon, in Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, edited by S. Goldwasser (IEEE Computer Society, Los Alamitos, CA, 1994), p. 116; SIAM J. Comput. 26, 1474 (1997).
[7] D. Coppersmith, arXiv:quant-ph/0201067v1 (1994 IBM Internal Report).
[8] Y.S. Weinstein, M.A. Pravia, E.M. Fortunato, S. Lloyd, and D.G. Cory, Phys. Rev. Lett. 86, 1880 (2001).
[9] L.M.K. Vandersypen, M. Steffen, G. Breyta, C.S. Yannoni, R. Cleve, and I.L. Chuang, Phys. Rev. Lett. 85, 5452 (2000).
[10] J.S. Lee, J. Kim, Y. Cheong, and S. Lee, Phys. Rev. A. 66, 042316 (2002).
[11] L.M.K. Vandersypen, M. Steffen, G. Breyta, C.S. Yannoni, M.H. Sherwood, and I.L. Chuang, Nature 414, 883 (2001).
[12] J. Chiaverini, J. Britton, D. Leibfried, E. Knill, M.D. Barrett, R.B. Blakestad, W.M. Itano, J.D. Jost, C. Langer, R. Ozeri, T. Schaetz, D.J. Wineland, Science 308, 997 (2005).
[13] B.P. Lanyon, T.J. Weinhold, N.K. Langford, M. Barbieri, D.F.V. James, A. Gilchrist, and A.G. White, Phys. Rev. Lett. 99, 250505 (2007).
[14] C.-Y. Lu, D.E. Browne, T. Yang, J.-W. Pan, Phys. Rev. Lett. 99, 250504 (2007).
[15] M.O. Scully and M.S. Zubairy, Phys. Rev. A 65, 052324 (2002).
[16] A. Muthukrishnan and C. R. Stroud Jr, J. Mod. Opt. 49, 2115 (2002).
[17] P.A. Ivanov and N.V. Vitanov, Phys. Rev. A 77, 012335 (2008).
[18] R. Barak and Y. Ben-Aryeh, J. Opt. Soc. Am. B 231, 24 (2007).
[19] J. W. Cooley and J. W. Tukey, Math. Comput. 19, 297 (1965).
[20] R. Akis, D. K. Ferry, Appl. Phys. Lett. 79 2823 (2001).
[21] X. Peng, Z. Liao, N. Xu, G. Qin, X. Zhou, D. Suter, and J. Du, Phys. Rev. Lett. 101, 220405 (2008).
[22] D. Beckman, A.N. Chari, S. Devabhaktuni, and J. Preskill, Phys. Rev. A 54, 1034 (1996).
[23] R.B. Griffiths and C.-S. Niu, Phys. Rev. Lett. 76, 3228 (1996).
[24] A. Barenco, A. Ekert, K.-A. Suominen, and P. Törmä, Phys. Rev. A 54, 139 (1996).
[25] D. Cheung, Proc. of the Winter International Symposium of Information and Communication Technologies (WISICT 2004), pp. 192-197; arXiv:quant-ph/0403071v1.
[26] R. G. Unanyan, B. W. Shore, M. Fleischhauer, and N. V. Vitanov, Phys. Rev. A 75, 022305 (2007).
[27] F. R. Gantmacher, *Matrix Theory* (Springer, Berlin, 1986).
[28] A. Messiah, *Quantum Mechanics* (North-Holland, New York, 1962).