Approximate quantum Fourier transform and decoherence

Adriano Barenco and Artur Ekert
Clarendon Laboratory, Department of Physics, University of Oxford, Parks Road, OX1 3PU Oxford, United Kingdom

Kalle-Antti Suominen
Theoretical Physics Division, Department of Physics, University of Helsinki, PL 9, 00014 Helsingin yliopisto, Finland

Päivi Törmä
Research Institute for Theoretical Physics, University of Helsinki, PL 9, 00014 Helsingin yliopisto, Finland
(Received 17 January 1996)

We discuss the advantages of using the approximate quantum Fourier transform (AQFT) in algorithms which involve periodicity estimations. We analyze quantum networks performing AQFT in the presence of decoherence and show that extensive approximations can be made before the accuracy of AQFT (as compared with regular quantum Fourier transform) is compromised. We show that for some computations an approximation may imply a better performance. [S1050-2947(96)05307-3]

PACS number(s): 03.65.−w, 89.70.+c, 42.50.Lc

I. INTRODUCTION

In the course of history many ingenious mechanical, acoustic, and optical devices have been invented for performing Fourier transforms [1] (including nature's own such as the human ear). Most of them are now of merely historical interest since the arrival of the computer-based algorithm known as the fast Fourier transform (FFT) [2,3], which efficiently computes the discrete Fourier transform. The FFT algorithm can also be phrased in terms of quantum dynamics, i.e., in terms of unitary operations performed by a quantum computer on quantum registers. Indeed, all known quantum algorithms employ the quantum version of Fourier transforms, either explicitly or indirectly. It is used for the periodicity estimation in the Shor algorithm [4] and its approximate version (the Hadamard transform) is commonly used to prepare quantum registers in coherent superpositions of different values.

In this paper we analyze the performance of the quantum Fourier transform (QFT) in the presence of decoherence. In particular we show that as far as the periodicity estimation is concerned the approximate quantum Fourier transform (AQFT) can yield better results than the full Fourier transform.

In the following we use some terms which were originally adopted from the classical theory of information and computer science and became standard in the lore of quantum computation. More detailed descriptions can be found, e.g., in Refs. [5–7] and in some recent reviews [8].

A *quantum bit* (*qubit*) is a two-state quantum system; it has a chosen ''computational basis'' $\{|0\rangle,|1\rangle\}$ corresponding to the classical bit values 0 and 1. Boolean operations which map sequences of 0's and 1's into another sequences of 0's and 1's are defined with respect to this computational basis. A collection of L qubits is called a *register* of size L.

Information is stored in the registers in binary form. For example, number 6 is represented by a register in state $|1\rangle\otimes|1\rangle\otimes|0\rangle$. In more compact notation: $|a\rangle$ stands for the direct product $|a_{L-1}\rangle\otimes|a_{L-2}\rangle\otimes\cdots\otimes|a_1\rangle\otimes|a_0\rangle$ which represents a quantum register prepared with the value $a=2^0a_0+2^1a_1+\cdots+2^{L-1}a_{L-1}$.

A *quantum logic gate* is an elementary quantum computing device which performs a fixed unitary operation on selected qubits in a fixed period of time.

A *quantum network* is a quantum computing device consisting of quantum logic gates whose computational steps are synchronised in time. The outputs of some of the gates are connected by wires to the inputs of others. The *size* of the network is its number of gates.

A *quantum computer* will be viewed here as a quantum network (or a family of quantum networks). Quantum computation is defined as a unitary evolution of the network which takes its initial state ''input'' into some final state ''output.''

Our presentation starts with a brief mathematical introduction to the approximate discrete Fourier transform which is followed by the description of its quantum implementation in terms of quantum networks. Then we analyze how the performance of the QFT in the periodicity estimation is affected by the approximations in the algorithms and by decoherence. We also comment on possible simplifications in practical implementations of quantum networks effecting the QFT and AQFT. The quantum algorithm for the fast Fourier transform which we use in this paper was originally proposed by Coppersmith and by Deutsch (independently) [9].

II. DISCRETE FOURIER TRANSFORMS

The discrete Fourier transform is a unitary transformation of an s-dimensional vector $(f(0),f(1),f(2),\ldots,f(s-1))$ defined by:

$$\tilde{f}(c)=\frac{1}{\sqrt{s}}\sum_{a=0}^{s-1}e^{2\pi iac/s}f(a), \tag{1}$$

where $f(a)$ and $\tilde{f}(c)$ are in general complex numbers. It can also be represented as a unitary matrix

$$\frac{1}{\sqrt{s}}\begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{(s-1)} \\ 1 & \omega^2 & \omega^4 & \dots & \omega^{2(s-1)} \\ 1 & \omega^3 & \omega^6 & \dots & \omega^{3(s-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{(s-1)} & \omega^{2(s-1)} & \dots & \omega^{(s-1)^2} \end{pmatrix}, \tag{2}$$

where $\omega=\exp(2\pi i/s)$ is the sth root of unity. In the following we assume that s is a power of 2, i.e., $s=2^L$ for some L; this is a natural choice when binary coding is used. The approximate discrete Fourier transform can be conveniently described when we write the product ac in the exponent on the r.h.s. of Eq. (1) in the binary notation. Writing

$$a=\sum_{i=0}^{L-1} a_i 2^i; \quad c=\sum_{i=0}^{L-1} c_i 2^i, \tag{3}$$

we obtain

$$ac=a_0c_0+(a_0c_1+a_1c_0)2+(a_0c_2+a_1c_1+a_2c_0)2^2+\dots +(a_0c_{L-1}+\dots+a_{L-1}c_0)2^{L-1}+O(2^L). \tag{4}$$

Because $\omega^x=1$ for $x\geqslant s$, the terms $O(2^L)$ do not contribute to the transform, and the term $\exp(2\pi iac/2^L)$ in Eq. (1) can be expressed as

$$\exp(2\pi iac/2^L)=\exp[2\pi i(a_0c_0)/2^L]\times\exp[2\pi i(a_0c_1+a_1c_0)/2^{L-1}]\dots\times\exp[2\pi i(a_0c_{L-1}+\dots+a_{L-1}c_0)/2]. \tag{5}$$

Beginning from the right of this expression, the arguments in the exponentials become smaller and smaller. In the approximate Fourier transform parametrized by an integer m, the $L-m$ smallest terms are neglected. In all the remaining terms the arguments are then multiples of $2\pi/2^m$. The 2^mth root of unity becomes the basic element of the approximate Fourier transform as opposed to 2^Lth root of unity which used in the ordinary Fourier transform. (The ordinary Fourier transform is obtained for $m=L$; when $m=1$ we obtain the Hadamard transform, for which all terms but the last one are dropped.)

The quantum version of the discrete Fourier transform is a unitary transformation which can be written in a chosen computational basis $\{|0\rangle,|1\rangle,\dots,|s-1\rangle\}$ as

$$(\mathrm{QFT})_s:|a\rangle\mapsto\frac{1}{\sqrt{s}}\sum_{c=0}^{s-1}\exp(2\pi iac/s)|c\rangle. \tag{6}$$

More generally, $(\mathrm{QFT})_s$ effects the discrete Fourier transform of the input amplitudes. If

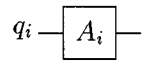
$$(\mathrm{QFT})_s:\sum_a f(a)|a\rangle\mapsto\sum_c \tilde{f}(c)|c\rangle, \tag{7}$$

then the coefficients $\tilde{f}(c)$ are the discrete Fourier transforms of $f(a)$'s. This definition can be trivially extended to cover the approximate quantum Fourier transform (AQFT). We will analyze the approximations involved in the AQFT in terms of computational networks.

III. QUANTUM NETWORKS FOR AQFT

Quantum networks for AQFT can be constructed following the description of the fast Fourier transform algorithm (as described by Knuth [10]). This efficient classical algorithm needs to be reexpressed in terms of unitary operations [9]. The construction requires only two basic unitary operations. The first operation is a one-bit transformation A_i (one-bit gate) that acts on a qubit q_i of the register and effects

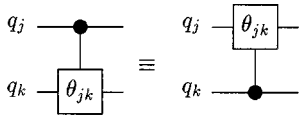
$$|0\rangle \longrightarrow \tfrac{1}{\sqrt{2}}(|0\rangle+|1\rangle),$$
$$|1\rangle \longrightarrow \tfrac{1}{\sqrt{2}}(|0\rangle-|1\rangle).$$



(8)

The diagram on the right provides a schematic representation of the gate acting on a qubit q. The second operation is a two-bit gate B_{jk} that effects

$$|00\rangle \longrightarrow |00\rangle,$$
$$|01\rangle \longrightarrow |01\rangle,$$
$$|10\rangle \longrightarrow |10\rangle,$$
$$|11\rangle \longrightarrow \exp(i\theta_{jk})|11\rangle,$$



(9)

where θ_{jk} depends on the qubits j and k on which the gate acts and equals $\theta_{jk}=\pi/2^{k-j}$. The transformation B_{jk} is an elementary two-qubit operation which affects only states with a 1 in both position j and k regardless the state of the remaining qubits.

The QFT on a register of size 1 reduces to a single operation A performed on a single qubit [cf. Eq. (6) for $s=2$]. The extension of the QFT network to a register of any

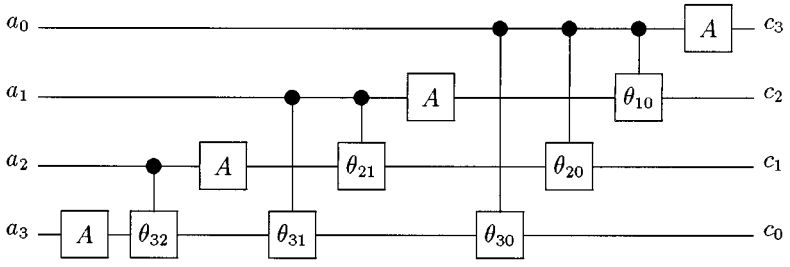


FIG. 1. QFT network operating on a four-bit register. The phases θ_{jk} that appear in the operations B_{jk} are related to the ''distance'' of the qubits $(j-k)$ and are given by $\theta_{jk}=\pi/2^{j-k}$. The network should be read form the left to the right: first the gate A is effected on the qubit a_3, then $B(\phi_{32})$ on a_2 and a_3, and so on.

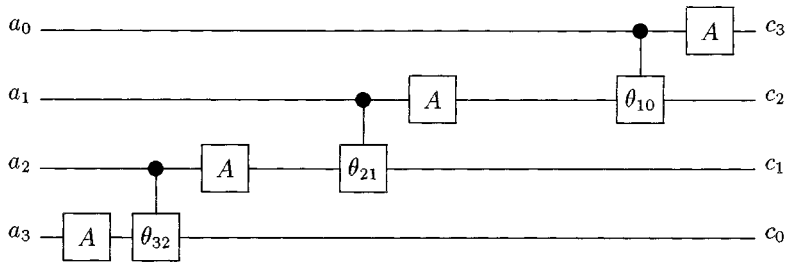


FIG. 2. AQFT network operating on a four-bit register when $m=2$.

size L follows a simple pattern of gates A and B which can be seen in Fig. 1. It shows the QFT network operating on four qubits which can be written as the sequence of the following 10 elementary operations (read from left to right)

$$(A_3)(B_{23}A_2)(B_{13}B_{12}A_1)(B_{03}B_{02}B_{01}A_0). \tag{10}$$

The bit values at the output should be read in the reversed order (see Fig. 1).

The number of gates needed to complete the QFT grows only as a quadratic function of the size of the register: for a transformation on a L qubit register, we require L operations A and $L(L-1)/2$ operations B, in total $L(L+1)/2$ elementary operations. Thus the quantum QFT can be performed efficiently.

The AQFT of degree m is represented by a similar network in which the two-bit gates that act on qubits which are far apart (in the register) are neglected, i.e., those operations B_{jk} for which the phase shift $\theta_{jk}\equiv\pi/2^{k-j}<\pi/2^m$ for some m such that $1\leqslant m\leqslant L$ are dropped [cf. Eq. (5)]. In that case, we need L operations A, and $(2L-m)(m-1)/2$ operations B, which is an improvement on the QFT case since $m<L$. In Fig. 2 we show the $m=2$ AQFT network counterpart to the QFT network shown in Fig. 1. The matrix elements of the QFT and the AQFT differ by a multiplicative factors of the form $\exp(i\epsilon)$ with $|\epsilon|\leqslant 2\pi L/2^m$. The execution time of the AQFT grows as $\sim Lm$.

IV. ESTIMATING PERIODICITY

The quantum Fourier transform, like the ordinary Fourier transform, is a powerful tool for uncovering periodicities. Any periodicity in probability amplitudes describing a quantum state of a register in a computational basis can be estimated (with some probability of success) by performing the QFT followed by a measurement of the register in the computational basis. The result is obtained by reading the qubits of the register in the reversed order.

For example, an interesting periodic state which plays an important role in Shor's quantum factoring algorithm can be written as

$$|\Psi\rangle=\frac{1}{\sqrt{\mathcal{N}}}\sum_{a=0}^{2^L-1} f(a)|a\rangle, \tag{11}$$

where $\mathcal{N}$ is an appropriate normalization factor and

$$f(a)=\delta_{l,a \bmod r}. \tag{12}$$

It is the state of a quantum register of size L in which the probability amplitudes $f(a)$ occur with periodicity r and offset l. If this offset is unknown, a measurement performed in the computational basis cannot reveal r or any of its integer multiples directly. This is illustrated in Fig. 3(a). However, if we perform the QFT on the register first and subsequently measure its state we obtain number $\overline{c}$ which, with probability greater than $4/\pi^2$, is a multiple of $2^L/r$ regardless the offset l (cf. Appendix). The probability is not equal to unity, because the finite size of the register leads to a ''broadening'' of the Fourier-transformed data, as illustrated in Fig. 3(b). (This is because $2^L/r$ is not necessarily an integer, and the quantum register can have only integer values; this is discussed in detail in the Appendix.)

For the AQFT the corresponding probability, in the limit of large L, satisfies

$$\mathrm{Prob}_A\geqslant\frac{8}{\pi^2}\sin^2\left(\frac{\pi}{4}\frac{m}{L}\right). \tag{13}$$

This result is derived in the Appendix. The effect of the approximation is illustrated in Fig. 4 where we plot the modulus of the amplitude of the transformed state $|\Psi\rangle$ (with $l=9$ and $r=10$) for the AQFT of different orders m. Figure 5 shows how the phase of the transformed state becomes corrupted when m becomes smaller.

If the quantum Fourier transform forms a part of a randomised algorithm then the computation can be repeated several times in order to amplify the probability of the correct result. In such cases the performance of the AQFT is only polynomially less efficient than that of the QFT. For example, consider Shor's quantum factoring algorithm and substitute the AQFT for the QFT. In order to obtain a correct factor with a prescribed probability of success, we have to repeat the computation several times. Let k and k' be the number of runs, respectively, with the QFT and the AQFT so that we obtain the same probability of getting at least one correct result, i.e.,

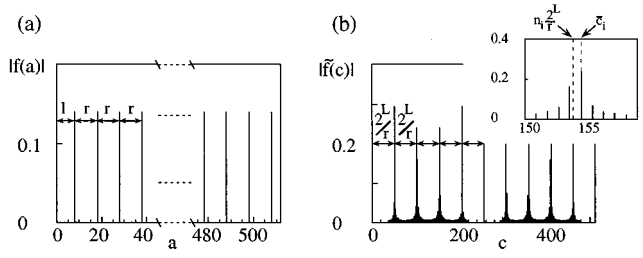


FIG. 3. (a) Function $f(a)$ in Eq. (12). The parameters are $l=8$, $r=10$ and the number of bits in the calculation is $L=9$ so that numbers up to $2^L-1=511$ can be encoded. (b) $|\tilde{f}(c)|$, obtained from $f(a)$ by a QFT. The inset shows $\overline{c_3}=155$ which is the closest integer to $3\times 512/10=153.6$. (See the Appendix for more details.)

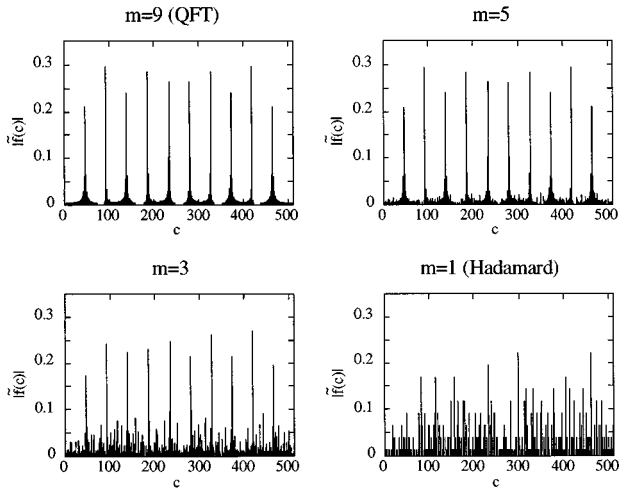


FIG. 4. Different orders of approximation in the AQFT performed on a state $|\Psi\rangle$ for which $f(a)=\delta_{9,a \bmod 10}$.

$$1-(1-p)^k=1-(1-p')^{k'}. \tag{14}$$

Here $p=4/\pi^2$ and $p'=(8/\pi^2)\sin^2[(4/\pi)(m/L)]$ are the corresponding probabilities of success in a single run. The ratio k'/k scales as

$$\frac{k'}{k}=\frac{\ln\left(1-\frac{4}{\pi^2}\right)}{\ln\left[1-\frac{8}{\pi^2}\sin^2\left(\frac{4}{\pi}\frac{m}{L}\right)\right]}<C\left(\frac{L}{m}\right)^3 \tag{15}$$

for some C (the upper bound is found graphically). This shows that in the quantum factoring algorithm the AQFT is not less efficient than the ordinary QFT, i.e., the ratio k'/k scales only polynomially with L/m. Moreover, we will show that in the presence of decoherence the AQFT can perform better than the QFT even in a single computational run.

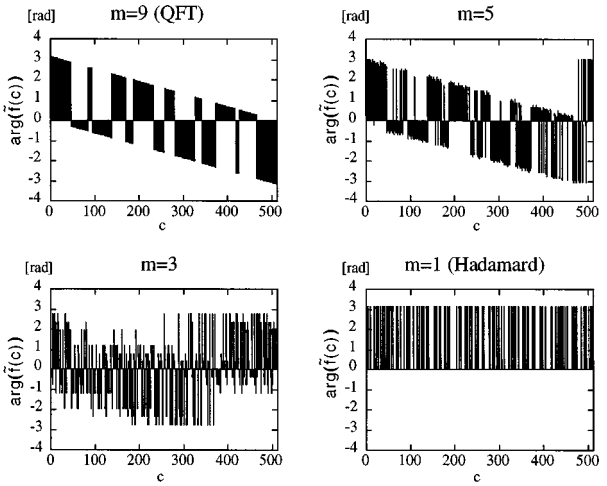


FIG. 5. As Fig. 4, but showing the phase of the amplitudes, i.e., $\arg(\tilde{f}(c))$.

V. DECOHERENCE

Quantum computation requires a controlled, quantum-mechanically coherent evolution at the level of individual quantum systems such as atoms or photons. This imposes severe requirements on quantum computer hardware. If we are to harness the unique power of quantum computers, such systems will have to be manufactured with unprecedented tolerances and shielded from noise to an unprecedented degree. Even a minute interaction with the environment will lead to a nonunitary evolution of the computer and its state will, in general, evolve into a mixed state described by a reduced density operator ρ, which is obtained from the density operator ρ_{total} of the total computer plus environment system by taking a trace over all the quantum states of the environment:

$$\rho=\mathrm{Tr}_{\text{environment}}(\rho_{\text{total}}). \tag{16}$$

Consider, for example, a quantum register of size L which is prepared initially in some pure state and then left on its own. As time goes by, the qubits become entangled with the environment. Both the diagonal and the off-diagonal elements of the density matrix ρ (expressed in a computational basis) are usually affected by this process (cf. [11,12]). The rate of change of the diagonal and the off-diagonal elements depends on the type of coupling to the environment, however, there are realistic cases where the dissapearance of the off-diagonal elements, known as decoherence, takes place on much faster time scale. In this case a simple mathematical model of decoherence has been proposed [13]. It assumes that the environment effectively acts as a measuring apparatus, i.e., a single qubit in state $c_0|0\rangle+c_1|1\rangle$ evolves together with the environment as

$$(c_0|0\rangle+c_1|1\rangle)|a\rangle\rightarrow c_0|0\rangle|a_0\rangle+c_1|1\rangle|a_1\rangle, \tag{17}$$

where states $|a\rangle,|a_0\rangle,|a_1\rangle$ are the states of the environment and $|a_0\rangle,|a_1\rangle$ are usually not orthogonal ($\langle a_0|a_1\rangle\neq 0$). The elements of the density matrix evolve as

$$\rho_{ij}(0)=c_i(0)c_j^*(0)\rightarrow\rho_{ij}(t)=c_i(t)c_j^*(t)\langle a_i(t)|a_j(t)\rangle,$$
$$i,j=0,1. \tag{18}$$

States $|a_0\rangle$ and $|a_1\rangle$ become more and more orthogonal to each other while the coefficients $\{c_i\}$ remain unchanged. Consequently the off-diagonal elements of ρ disappear due to the $\langle a_0(t)|a_1(t)\rangle$ factor and the diagonal elements are not affected.

There is an alternative way of thinking about this process. The environment is regarded as a bosonic heat bath, which introduces phase fluctuations to the qubit states, i.e., it induces random phase fluctuations in the coefficients c_0 and c_1 such that

$$c_0|0\rangle+c_1|1\rangle\rightarrow c_0e^{-i\phi}|0\rangle+c_1e^{i\phi}|1\rangle. \tag{19}$$

The direction and the magnitude of each phase fluctuation ϕ is chosen randomly following the Gaussian distribution

$$P(\phi)d\phi=\frac{1}{\sqrt{2\pi}\delta}\exp\left[-\frac{1}{2}\left(\frac{\phi}{\delta}\right)^2\right]d\phi, \tag{20}$$

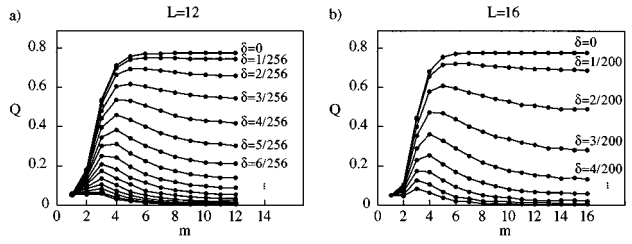


FIG. 6. The quality factor Q as a function of m for selected values of δ. The register sizes are (a) $L=12$ and (b) $L=16$. Statistical errors are too small to be represented on the graph.

where the distribution width δ defines the strength of the coupling to the quantum states of the environment. The elements of the density matrix ρ are then reconstructed as $\rho_{ij}=\langle c_i c_j^* \rangle$, where the average $\langle\ \rangle$ is taken over different realizations of the phase fluctuations within a given period of time (cf [12].). The diagonal elements do not depend on ϕ, whereas the off-diagonal term $\langle c_0 c_1 e^{i2\phi} \rangle$ averages to zero for a sufficiently long period of time.

The latter approach to decoherence is very convenient for numerical simulations and was chosen for the purpose of this paper. It is similar to the Monte Carlo wave function method used in quantum optics [14].

VI. AQFT AND DECOHERENCE

We have analyzed decoherence in the AQFT networks assuming that the environment introduces a random phase fluctuation in a qubit probability amplitudes each time the qubit is affected by gate B. In our model we have not attached any decoherence effects to gate A. In most of the suggested physical realizations the single qubit operations are quite fast, whereas the conditional logic needed in two-qubit operations is often much harder to produce, which makes these operations slower than the single qubit ones, and often much more susceptible to decoherence. For instance, in the ion trap model proposed by Cirac and Zoller [15] single qubit operations require only one laser pulse interacting with one atom, whereas in a two−qubit operation two subsequent laser pulses are needed, and the atoms involved must form an entangled state with a trap phonon mode between the pulses. It should also be noted that there are as many one-qubit gates in the QFT network as there are

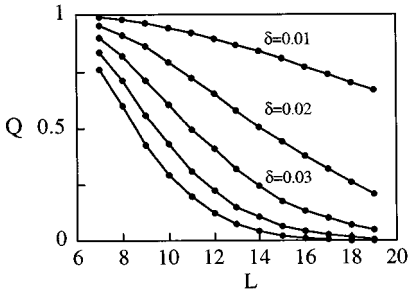


FIG. 7. The quality factor Q as a function of the register size L for QFT, with varying levels of decoherence, from $\delta=0.1$ (top line) to $\delta=0.5$ (bottom line). Statistical errors are too small to be represented on the graph.

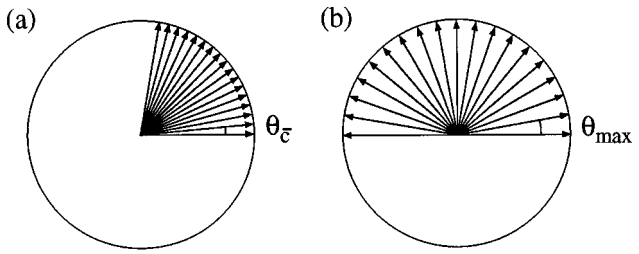


FIG. 8. (a) Argand diagram corresponding to the sum of the phases that appear in the expression of $f(\overline{c})$ for $\overline{c}$ close to one of the values $n2^L/r$. Prob$(\overline{c})$ is the norm of the vector resulting from the sum of each vector in the diagram. (b) Prob$(\overline{c})$ is bounded by the worst-case situation in which we have taken $\theta_{\max}$ instead of $\theta_{\overline{c}}$, in this case the phases lie on an interval $[0,\pi]$ on the Argand diagram and a closed form expression can be found.

input qubits. This number of the one-qubit gates is unchanged when the approximate QFT is performed and the noise due to decoherence of the one-qubit gates is the same regardless of the degree of the approximation. Our considerations do not depend on the level of this constant noise, so for the sake of convenience we can set it to zero.

We have quantified the performance of the AQFT by introducing the quality factor Q. It is simply the probability of obtaining an integer which is closest to any integer multiple of $2^L/r$, when the state of the register is measured after the transformation. In the decoherence-free environment analyzed in Sec. IV we obtain $Q=1$ for integer values of $2^L/r$ and for a randomly selected r the quality factor Q is of the order $4/\pi^2$ for the QFT and of the order of $(8/\pi^2)\sin^2[(4/\pi)(m/L)]$ for the AQFT of degree m.

In Fig. 6 we show how the quality factor Q behaves as a function of m and δ (which characterizes the strength of the coupling to the environment). For $\delta>0$ the maximum of Q is obtained for $m<L$. Thus in the presence of decoherence one should use the AQFT rather than the QFT.

This ''less is more'' result can be easily understood. The AQFT means less gates in the network and because each B gate introduces phase fluctuations the approximate network generates less decoherence as compared to the regular QFT network. By decreasing m we effectively decrease the impact of decoherence. On the other hand, decreasing m implies approximations which reduces the quality factor. This tradeoff between the two phenomena results in the maximum value Q for $m\in[1,L]$.

It is worth pointing out that for $\delta=0$ (no decoherence) Q remains almost constant for those values of m that satisfy the lower bound condition (derived in the Appendix)

$$m>\log_2 L+2, \tag{21}$$

and when $\delta>0$ the optimum m is found near this lower bound. In Fig. 7 we also show how Q decreases rapidly with L in the QFT network (although there is not enough data in the figure to determine if it really decreases exponentially).

Our simulations were performed for ensembles which consisted typically of one to two thousand individual realizations.

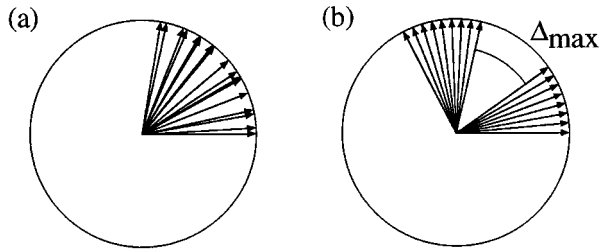


FIG. 9. (a) Argand diagram for the AQFT. Vectors are rotated by an angle $\Delta(jr,c)$. (b) To obtain a closed form for a bound for $\mathrm{Prob}_A(\overline{c})$ we consider the worst case in which half of the phases pick up a factor $\Delta_{\max}$.

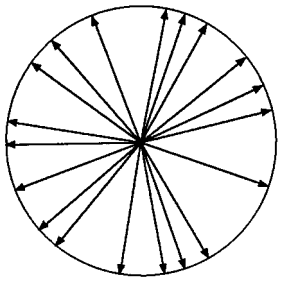


FIG. 10. In the case that the order m of the AQFT is such that $\Delta_{\max} > \pi/2$, the individual phases can get scrambled in such a way that there is no constructive interference effect. The probability $\mathrm{Prob}_A(\overline{c})$ can become vanishingly small and the AQFT of order m is inefficient.

VII. CONCLUSIONS AND COMMENTS

We have analyzed the approximate quantum Fourier transform in the presence of decoherence and found that the approximation does not imply a worse performance. On the contrary, using the periodicity estimation as an example of a computational task, we have shown that for some algorithms the approximation may actually imply a better performance.

Needless to say, there is room for further simplifications of the quantum Fourier transform which may lead to at least partial suppressing of unwelcome effects of decoherence. For example, if the QFT is followed by a bit by bit measurement of the register then the conditional dynamics in the network can be converted to a sequence of conditional bit by bit measurements (cf. [16]). However, one should note that this approach is limited because it cannot be used if the quantum Fourier transform is only an intermediate step in some much more complicated calculation.

In our discussion of decoherence in the QFT network we have not analyzed the various quantum error correcting techniques that have been proposed recently (see e.g., [17–20]). This is simply because quantum encoding and decoding require additional networks which are assumed to be error free. Clearly this is an unrealistic assumption in the context of quantum computation (but a reasonable one in the context of quantum communication over a noisy channel). Any discussion of the performance of the QFT network with error correction must also include the performance of these auxiliary networks (after all encoding and decoding is a quantum computation on its own).

It has been pointed out that any experimental quantum computation requires unpreceedingly high accuracy of control [21]. These requirements obviously limit the efficiency of the quantum computation, but tend to be dependent on the particular implementation of the computation (see e.g., [22]) and thus we have not considered them here.

In this article we have wanted to show that there are cases where quantum networks that are composed of imprecise components can guarantee a ''pretty good performance.'' This topic has also a more general context; it has been shown that reliable classical networks can be assembled from unreliable components [23]. It is an open question whether a similar result holds for quantum networks.

ACKNOWLEDGMENTS

A.B. thanks E. S. Trounz for discussions. A.E. is supported by the Royal Society. A.B. acknowledges the Berrow fund at Lincoln College (Oxford), and K.-A.S. and P.T. acknowledge the Academy of Finland for financial support, and thank A.E. and the rest of the group for kind hospitality during visits to Oxford.

APPENDIX

Consider the quantum state

$$|\Psi\rangle = \frac{1}{\sqrt{\mathcal{N}}} \sum_{a=0}^{2^L-1} f(a)|a\rangle, \tag{A1}$$

where

$$f(a) = \delta_{l,\ a \bmod r}. \tag{A2}$$

Here $f(a)$ is a periodic function with period $r \ll 2^L$ and offset l, which is an arbitrary positive integer smaller than r; see Fig. 3(a). The normalization factor is equal to the number of nonzero values $f(a)$: $\mathcal{N} = [2^L/r]$. Because $r \ll 2^L$ we use from now on $[2^L/r] \simeq 2^L/r$. The state (A1) plays an important role in the Shor quantum factorization algorithm [the algorithm enables us to factorize an integer N by finding r such that $x^r = (1 \bmod N)$ for some x coprime with N — r is estimated from a quantum computation that generates a state of the form (A1)].

Applying QFT to this state we obtain

$$|\tilde{\Psi}\rangle = \sum \tilde{f}(c)|c\rangle, \tag{A3}$$

where

$$\tilde{f}(c) = \frac{\sqrt{r}}{2^L} \sum_{j=0}^{2^{L/r}-1} \exp[2\pi i(jr+l)c/2^L]. \tag{A4}$$

The probability of seeing an integer c is then

$$\mathrm{Prob}(c) = |\tilde{f}(c)|^2 = \frac{r}{2^{2L}} \Big| \sum_{j=0}^{2^{L/r}-1} \exp[2\pi i j(rc \bmod 2^L)/2^L] \Big|^2. \tag{A5}$$

As can be seen from Fig. 3(b) the peaks of the power spectrum of $f(a)$ are centered at integers c, which are the closest approximation to multiplies of $2^L/r$.

Let us now evaluate Prob($\overline{c}$) for $\overline{c}$ being the closest integer to $\lambda 2^L/r$, i.e., $\overline{c}=[\lambda 2^L/r]$. By definition $\overline{c}$ must satisfy

$$-\frac{1}{2}<\overline{c}-\lambda\frac{2^L}{r}<\frac{1}{2}. \tag{A6}$$

We define $\theta_{\overline{c}}=2\pi(r\overline{c} \bmod 2^L)$ so that Prob($\overline{c}$) now involves a geometric series with ratio $\exp(i\theta_{\overline{c}})$. By viewing these terms as vectors on an Argand diagram it is clear that the total distance from the origin decreases as $\theta_{\overline{c}}$ increases. Hence Prob($\overline{c}$)$\geqslant$Prob($\overline{c}$ with largest allowed $\theta_{\overline{c}}$). Let us denote by $\theta_{\max}$ the largest allowed $\theta_{\overline{c}}$. By Eq. (A6), $\theta_{\max}\leqslant\pi r/2^L$ and summing the geometric series with $\theta_{\max}=\pi r/2^L$ (see Fig. 8) we obtain

$$\mathrm{Prob}(\overline{c})\geqslant\frac{r}{2^{2L}}\frac{1}{\sin^2\left(\frac{\pi}{2}\frac{r}{2^L}\right)}\simeq\frac{4}{\pi^2}\frac{1}{r}, \tag{A7}$$

where we have used the fact that $r/2^L$ is small. Since there are r such values $\overline{c}$, the total probability of seeing one of them is

$$\mathrm{Prob}\geqslant 4/\pi^2. \tag{A8}$$

By performing this measurement several times on different states $|\Psi\rangle$ (each one with possibly different l), one gets with high probability values $\overline{c_0}$, $\overline{c_1}$, . . . that are the closest integers to $n_0 2^L/r$, $n_1 2^L/r$, . . . and which allow us to calculate r [cf. inset in Fig. 3(b)].

We estimate now the probability of measuring one of the desired values $\overline{c}$ when the AQFT of order m has been performed instead of the QFT. The difference between the QFT and the AQFT of order m is in the arguments of the exponentials in Eq. (A5). The phase difference for each term in the sum is

$$\Delta(a,c)=\frac{2\pi}{2^L}\left(ac-\sum_{(j,k)\in\mathcal{E}}^{L-1}a_j c_k 2^{j+k}\right), \tag{A9}$$

where

$$\mathcal{E}=\{(j,k)|0\leqslant j,k\leqslant L-1, L-m\leqslant j+k\leqslant L-1\}. \tag{A10}$$

The probability to measure $|\overline{c}\rangle$, where $\overline{c}$ is the closest integer to one of the r values $n2^L/r$, now becomes

$$\mathrm{Prob}_A(c)=\frac{r}{2^{2L}}\left|\sum_{j=0}^{2^L/r-1}\exp[2\pi ij(rc \bmod 2^L)/2^L-i\Delta(jr,c)]\right|^2. \tag{A11}$$

This is the same summation as is involved in the QFT, except that in the case of the AQFT, each vector of the Argand diagram of Fig. 8(a) may be rotated by an angle $\Delta(jr,c)$, as shown in Fig. 9. In the worst case, when $a=c=2^L-1$, i.e., $a_i=c_i=1\ \forall i$, $\Delta(a,c)$ is equal to

$$\Delta_{\max}=\frac{2\pi}{2^m}(L-m-1+2^{m-L}). \tag{A12}$$

However, for any other values of a and c, $0\leqslant\Delta(a,c)<\Delta_{\max}$.

We are interested in the lower bound for the probability so we assume that the vectors in the Argand diagram fill one half of the circle ($\theta_{\max}=\pi r/2^L$) as illustrated in Fig. 8(b). The approximation allows to rotate each vector by the maximum angle $\Delta_{\max}$. The minimum of the probability is obtained when half of the vectors are rotated by $\Delta_{\max}$; see Fig. 9(b). In this case vectors in two areas of size $\Delta_{\max}$ cancel each other, and all we have to do is to calculate geometrical sums of the vectors in the two areas of size $\pi/2-\Delta_{\max}$. In an area of that size there are $(2^L/r)[\frac{1}{2}-(\Delta_{\max}/\pi)]$ vectors, since the total number of vectors is $2^L/r$. Note that because $2^L\gg r$, we can assume that $[2^L/r]\pm 1\simeq 2^L/r$. The square of the geometric sum then becomes

$$\left|\sum_{j=0}^{2^L/r(1/2-\Delta_{\max}/\pi)-1}\exp\left(i\frac{\pi r}{2^L}j\right)\right|^2=\frac{\sin^2\left[\frac{1}{2}\left(\frac{\pi}{2}-\Delta_{\max}\right)\right]}{\sin^2\left(\frac{\pi}{2}\frac{r}{2^L}\right)}. \tag{A13}$$

The two sum vectors in the two areas of size $\pi/2-\Delta_{\max}$ are of equal length and orthogonal to each other, so the square of their sum vector, contributing to the total probability, is twice the value given by (A13). Finally we obtain

$$\mathrm{Prob}_A\geqslant 2\frac{r^2}{2^{2L}}\frac{\sin^2\left[\frac{1}{2}\left(\frac{\pi}{2}-\Delta_{\max}\right)\right]}{\sin^2\left(\frac{\pi}{2}\frac{r}{2^L}\right)}\simeq\frac{8}{\pi^2}\sin^2\left[\frac{1}{2}\left(\frac{\pi}{2}-\Delta_{\max}\right)\right]. \tag{A14}$$

For $\Delta_{\max}=0$ this expression reduces to the result derived for the QFT:

$$\mathrm{Prob}_A \geqslant \frac{8}{\pi^2}\sin^2\left(\frac{\pi}{4}\right) = \frac{4}{\pi^2}, \tag{A15}$$

and for $\Delta_{\max} = \pi/2$ we have $\mathrm{Prob}_A \geqslant 0$. To avoid a zero probability, $\Delta_{\max}$ must always be bounded by

$$\Delta_{\max} = \frac{2\pi}{2^m}(L - m - 1 + 2^{m-L}) < \frac{\pi}{2}, \tag{A16}$$

which for large L implies

$$m > \log_2 L + 2. \tag{A17}$$

Equation (21) gives a lower bound to the order of the AQFT performed on a register of length L, if one wants to have a nonzero probability of success in measuring a value c. Simple geometric considerations also show that $\Delta_{\max} < \pi/2$ is a limit for a non-negligible probability: for $\Delta_{\max} > \pi/2$ the vectors in the Argand diagram can be rotated so that there is no longer any constructive interference; see Fig. 10.

For large L we can write

$$\Delta_{\max} \simeq \frac{2\pi}{2^m}(L - m). \tag{A18}$$

If we use the lower bound for m (21), we obtain

$$\Delta_{\max} \leqslant \frac{\pi}{2}\left(1 - \frac{m}{L}\right), \tag{A19}$$

which allows us to write the probability (A14) in a simple form,

$$\mathrm{Prob}_A \geqslant \frac{8}{\pi^2}\sin^2\left(\frac{\pi}{4}\frac{m}{L}\right). \tag{A20}$$

[1] J. B. J. Fourier, *Théorie Analytique de la Chaleur* (Didot, Paris, 1822); reprinted (Gabay, Sceaux, 1988); translated: *The Analytical Theory of Heat* (Dover, New York, 1955).

[2] J. W. Cooley and J. W. Tukey, Math. Comput. **19**, 297 (1965).

[3] E. O. Brigham, *The Fast Fourier Transform* (Prentice Hall, Englewood Cliffs, 1974).

[4] P. W. Shor, in *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science*, edited by S. Goldwasser (IEEE Computer Society Press, Los Alamitos, CA, 1994), p. 124.

[5] A. Barenco, D. Deutsch, A. Ekert, and R. Jozsa, Phys. Rev. Lett. **74**, 4083 (1995); D. Deutsch, A. Barenco, and A. Ekert, Proc. R. Soc. London Ser. A **449**, 669 (1995); A. Barenco, *ibid.* **449**, 679 (1995).

[6] T. Sleator and H. Weinfurter, Phys. Rev. Lett. **74**, 4087 (1995).

[7] V. Vedral, A. Barenco, and A. Ekert, Phys. Rev. A (to be published).

[8] A. Barenco, *Physics and Quantum Computers*, Contemp. Phys. (to be published); C. Bennett, Phys. Today **48** (10), 24 (1995); D. P. DiVincenzo, Science **270**, 255 (1995); S. Lloyd, Sci. Am. **273** (4), 44 (1995).

[9] D. Coppersmith, IBM Research Report No. RC19642 (1994); D. Deutsch (unpublished).

[10] D. E. Knuth, *The Art of Computer Programming, Volume 2: Seminumerical Algorithms*, 2nd ed. (Addison-Wesley, Reading, MA, 1981).

[11] W. Unruh, Phys. Rev. A **51**, 992 (1995).

[12] G. M. Palma, K.-A. Suominen, and A. Ekert, Proc. R. Soc. London Ser. A **452**, 567 (1996).

[13] W. H. Zurek, Phys. Today **44** (10), 36 (1991).

[14] J. Dalibard, Y. Castin, and K. Mølmer, Phys. Rev. Lett. **68**, 580 (1992); Y. Castin, K. Mølmer, and J. Dalibard, J. Opt. Soc. Am. B **10**, 524 (1993).

[15] J. I. Cirac and P. Zoller, Phys. Rev. Lett. **74**, 4091 (1995).

[16] R. B. Griffiths and C. S. Niu, Report No. quant−ph/9511007 (unpublished).

[17] A. Berthiaume, D. Deutsch, and R. Jozsa, in *Proceedings of Workshop on Physics and Computation — PhysComp94* (IEEE Computer Society Press, Dallas, 1994); A. Barenco, A. Berthiaume, D. Deutsch, A. Ekert, R. Jozsa, and C. Macchiavello (unpublished).

[18] A. R. Calderbank and P. W. Shor, Report No. quant−ph/9512032.

[19] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, Report No. quant−ph/9602019 (unpublished).

[20] A. Steane, Report No. quant-ph/9601029 (unpublished).

[21] R. Landauer, Trans. R. Soc. London Ser. A **353**, 367 (1995).

[22] M. Plenio and P. L. Knight, Phys. Rev. A **53**, 2986 (1996).

[23] U. Feige, P. Raghavan, D. Peleg, and U. Upfal, SIAM J. Comput. **23**, 1001 (1994).