Entangled quantum states generated by Shor's factoring algorithm

Yishai Shimoni, Daniel Shapira, and Ofer Biham
Racah Institute of Physics, The Hebrew University, Jerusalem 91904, Israel
(Received 25 August 2005; published 6 December 2005)

The intermediate quantum states of multiple qubits, generated during the operation of Shor's factoring algorithm are analyzed. Their entanglement is evaluated using the Groverian measure. It is found that the entanglement is generated during the preprocessing stage of the algorithm and remains nearly constant during the quantum Fourier transform stage. The entanglement is found to be correlated with the speedup achieved by the quantum algorithm compared to classical algorithms.

DOI: 10.1103/PhysRevA.72.062308 PACS number(s): 03.67.Lx, 89.70.+c

I. INTRODUCTION

The potential speedup of quantum algorithms is demonstrated by Shor's factoring algorithm, which is exponentially faster than any known classical algorithm [1]. Several other quantum algorithms, which are more efficient than their classical counterparts were introduced [2–5]. Factorization is of special interest due to its role in current methods of cryptography. Although the origin of the speedup offered by quantum algorithms is not fully understood, there are indications that quantum entanglement plays a crucial role [6,7]. In particular, it was shown that quantum algorithms that do not create entanglement can be simulated efficiently on a classical computer [8]. Therefore, it is of interest to quantify the entanglement produced by quantum algorithms and examine its correlation with their efficiency. This requires us to develop entanglement measures for the quantum states of multiple qubits that appear in quantum algorithms. Recently, the Groverian measure of entanglement was introduced and used for the evaluation of entanglement in certain pure quantum states of multiple qubits [9]. Using computer simulations of the evolution of quantum states during the operation of a quantum algorithm, one can obtain the time evolution of the entanglement. Such an analysis was performed for Grover's search algorithm with various initial states and different choices of the marked states [10]. It was shown that Grover's iterations generate highly entangled states in intermediate stages of the quantum search process, even if the initial state and the target state are product states.

In this paper, we analyze the quantum states that are created during the operation of Shor's factoring algorithm. The entanglement in these states is evaluated using the Groverian measure. It is found that the entanglement is generated during the preprocessing stage. When the quantum Fourier transform (QFT) is applied to the resulting states, their entanglement remains unchanged. This feature is unique to periodic quantum states, such as those that result from the preprocessing stage of Shor's algorithm. When other states, such as product states or random states are fed into the QFT, their entanglement does change. Another interesting feature is that the entanglement is found to be correlated with the speedup achieved by the quantum factoring algorithm compared to classical algorithms. This means that the cases where no entanglement is created are those in which classical factoring is efficient.

The paper is organized as follows. In Sec. II, we briefly review Shor's factoring algorithm, the QFT algorithm, and the quantum circuit used to perform it. In Sec. III, we describe the Groverian entanglement measure and the numerical method in which it is calculated. In Sec. IV, we use the Groverian measure to evaluate the entanglement created by Shor's algorithm. The results are discussed in Sec. V and summarized in Sec. VI.

II. SHOR'S FACTORING ALGORITHM

Shor's algorithm factorizes a given nonprime integer N, namely, it finds integers p_1 and p_2, such that their product $p_1 p_2 = N$. The algorithm consists of three parts: (a) preprocessing stage, in which the quantum register is prepared using classical algorithms and quantum parallelism; (b) quantum Fourier transform, which is applied on the output state of the previous stage; (c) measurement of the register and postprocessing using classical algorithms.

A. Preprocessing

Given an integer N to be factorized, choose any integer $y < N$ and find the integer $q = 2^L$ that satisfies

$$N^2 < q \leqslant 2N^2. \tag{1}$$

Prepare a register of L qubits (later referred to as the main register) in the equal superposition state

$$|\eta\rangle = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle. \tag{2}$$

Next, use quantum operations to calculate $y^a \bmod N$ for all the indices, $a = 0, \ldots, q-1$, of the basis states above, and store the results in an auxiliary register, giving rise to the joint state

$$\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle |y^a \bmod N\rangle. \tag{3}$$

This essentially completes the preprocessing stage. However, in order to present the next stage of the algorithm more clearly, it is helpful to measure the auxiliary register in the computational basis. Suppose that the result of the measure-

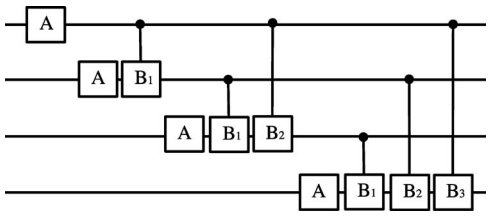

FIG. 1. The circuit of the quantum Fourier transform (QFT) performed on a four-qubit register. The operator A is the Hadamard gate. The operators B_1, B_2, and B_3 are the controlled-phase gates $B_{k,m}$, where $m-k=1$, 2, and 3, respectively.

ment is a state $|z\rangle$, where $z=y^l(\mathrm{mod}\,N)$ and l is the smallest positive integer that gives the value z. The order of y mod N is defined as an integer r that satisfies $y^r=1(\mathrm{mod}\,N)$. The equality

$$y^{jr+l}=y^l(\mathrm{mod}\,N) \tag{4}$$

is thus satisfied for any integer j. From Eq. (4), it follows that the measurement will select from the main register all values of $a=l,l+r,l+2r,\ldots,l+Ar$, where A is the largest integer which is smaller than $(q-1)/r$. The state of the register after the measurement is, therefore,

$$|\phi_l\rangle=\frac{1}{\sqrt{A+1}}\sum_{j=0}^{A}|jr+l\rangle. \tag{5}$$

B. Quantum Fourier Transform

The quantum Fourier transform is given by

$$\sum_{a=0}^{q-1}f(a)|a\rangle\mapsto\sum_{c=0}^{q-1}\tilde{f}(c)|c\rangle, \tag{6}$$

where

$$\tilde{f}(c)=\frac{1}{\sqrt{q}}\sum_{a=0}^{q-1}\exp\left(\frac{2\pi iac}{q}\right)f(a). \tag{7}$$

The quantum circuit of the QFT is shown in Fig. 1. To obtain the transformation in Eq. (6), the L qubits of register $|a\rangle$ in the input (and throughout the quantum circuit) are indexed by $k=1,\ldots,L$, from bottom to top. The output of the circuit is stored in register $|c\rangle$, whose qubits are indexed from top to bottom. We define the operator A_k to be the Hadamard gate applied to qubit k, and the operator $B_{k,m}$ (where $m>k$) to be a controlled phase operator, which applies a phase of $\theta_{k,m}=\pi/2^{m-k}$ only if both qubits k and m are 1. We also define

$$F_k=A_kB_{k,k+1}B_{k,k+2}\ldots B_{k,L}, \tag{8}$$

for $k=1,\ldots,L$, where we follow the standard notation for quantum operators, namely, those on the right-hand side operate first. With these definitions, the sequence of quantum operations that perform the QFT is given by

$$\mathrm{QFT}=F_1F_2\ldots F_L. \tag{9}$$

The number of one-qubit and two-qubit gates required in the quantum circuit which performs QFT is a polynomial in the size of the register.

In the simple case in which r divides q exactly, namely $A+1=q/r$, one obtains

$$\mathrm{QFT}|\phi_l\rangle=\frac{1}{\sqrt{r}}\sum_{j=0}^{r-1}\exp\left(\frac{2\pi ilj}{r}\right)\left|j\frac{q}{r}\right\rangle, \tag{10}$$

where $|\phi_l\rangle$ is defined in Eq. (5). The resulting state is a superposition of all basis states with indices which are products of q/r. If r is not a divisor q, namely, q/r is not an integer, Eq. (10) should be modified such that the large amplitude states are those which correspond to integers adjacent to jq/r, $j=0,1,\ldots,r-1$. Our choice of q in Eq. (1) ensures that, with high probability, the measurement will yield only states whose indices are the nearest integers to jq/r.

C. Measurement and postprocessing

The third part of the algorithm starts with a measurement of the register. It yields an integer approximation c of one of the values jq/r, $j=0,1,\ldots,r-1$. Thus, cr is approximately an integer multiple of q. Here, again, our choice of q in Eq. (1) ensures that in most cases there exists another integer c' which satisfies $|rc-c'q|\leqslant r/2$. As a result

$$\left|\frac{c}{q}-\frac{c'}{r}\right|\leqslant\frac{1}{2q}. \tag{11}$$

Using a continued fraction expansion of c/q, it is possible to efficiently find c' and r. There is only one such approximation which satisfies Eq. (11) for $r<N$. Thus, the correct value of r is obtained. If r is even, we can define $x=y^{r/2}$ which satisfies

$$x^2-1=(x-1)(x+1)=0(\mathrm{mod}\,N). \tag{12}$$

From Eq. (12), we obtain that $x+1(\mathrm{mod}\,N)$ and $x-1(\mathrm{mod}\,N)$ are candidates for having a common divisor with N. Using Euclid's greatest common divisor (GCD) algorithm, this common divisor is found and the factoring process is completed.

III. THE GROVERIAN MEASURE OF ENTANGLEMENT

A. Formal definition

Consider a quantum algorithm, given by the unitary operator U, applied to the equal superposition state $|\eta\rangle$. For a certain class of quantum algorithms, the final, or target state

$$|t\rangle=U|\eta\rangle, \tag{13}$$

is a computational basis state. This state stores the correct result of the calculation, which can be extracted by measurement. Not all quantum algorithms can be expressed in this form, because the final state, before the measurement is done, may be a superposition state. However, in the case of Grover's search algorithm with a single marked state, this description applies [9]. Consider the case in which such an algorithm U is applied to an arbitrary pure state $|\psi\rangle$. The probability of success is defined as the probability that the measurement will still give the state $|t\rangle$. This probability is given by $P_s=|\langle t|\psi\rangle|^2$.

The success probability can be used to evaluate the entanglement of the state $|\psi\rangle$. To this end, before the algorithm U is applied, one applies a local unitary operator U_k on each qubit $k=1,2,\ldots,L$. These operators are chosen such that the success probability of the algorithm will be maximized. The maximal success probability is

$$P_{\max} = \max_{U_1,\ldots,U_L} |\langle t|UU_1 \otimes \cdots \otimes U_L|\psi\rangle|^2. \quad (14)$$

Using Eq. (13), the success probability $P_{\max}$ can be expressed by

$$P_{\max} = \max_{U_1,\ldots,U_L} |\langle \eta|U_1 \otimes \cdots \otimes U_L|\psi\rangle|^2. \quad (15)$$

This can be rewritten as

$$P_{\max} = \max_{|e_1\rangle,\ldots,|e_L\rangle} |\langle e_1 \otimes \cdots \otimes e_L|\psi\rangle|^2, \quad (16)$$

where the $|e_k\rangle$'s are single-qubit states. Equation (16) means that for a given initial state $|\psi\rangle$, the maximal success probability of such algorithm U is equal to the maximal overlap of $|\psi\rangle$ with any product state.

The Groverian measure of entanglement $G(\psi)$ is defined by

$$G(\psi) = \sqrt{1 - P_{\max}}. \quad (17)$$

For the case of pure states, for which $G(\psi)$ is defined, it is closely related to an entanglement measure introduced in Refs. [11–13] and was shown to be an entanglement monotone. The latter measure is defined for both pure and mixed states. It can be interpreted as the distance between the given state and the nearest separable state and expressed in terms of the fidelity of the two states. Based on these results, it was shown [9] that $G(\psi)$ satisfies: (a) $G(\psi) \geqslant 0$, with equality only when $|\psi\rangle$ is a product state; (b) $G(\psi)$ cannot be increased using local operations and classical communication (LOCC). Therefore, $G(\psi)$ is an entanglement monotone for pure states. A related result was obtained in Ref. [14], where it was shown that the evolution of the quantum state during the iteration of Grover's algorithm corresponds to the shortest path in Hilbert space using a suitable metric.

B. Numerical evaluation

Consider a pure quantum state of L qubits

$$|\psi\rangle = \sum_{j=0}^{2^L-1} a_j|j\rangle. \quad (18)$$

In order to find $G(\psi)$, we form a convenient representation of the tensor product states used in Eq. (16). The state of each qubit in the product state is given by

$$|e_k\rangle = e^{i\delta_k}[\cos\theta_k|0\rangle + e^{i\gamma_k}\sin\theta_k|1\rangle]. \quad (19)$$

Let us denote

$$b_j^{(k)} = \begin{cases} \cos\theta_k & \text{if } j_k = 0 \\ e^{i\gamma_k}\sin\theta_k & \text{if } j_k = 1 \end{cases}, \quad (20)$$

where j_k, $k=1,\ldots,L$ is the kth most significant bit in the binary representation of j. The overlap between $|\psi\rangle$ and the product state $|e_1 \otimes \cdots \otimes e_L\rangle$ is given by $f(\psi,\theta_1,\ldots,\theta_L,\gamma_1,\ldots,\gamma_L) = \langle e_1 \otimes \cdots \otimes e_L|\psi\rangle$. It can then be written as

$$f(\psi,\theta_1,\ldots,\theta_L,\gamma_1,\ldots,\gamma_L) = \sum_{j=0}^{2^L-1} b_j^{(1)} b_j^{(2)} \ldots b_j^{(L)} a_j. \quad (21)$$

The phases δ_k only introduce a global phase which can be ignored. The Groverian entanglement measure for the state $|\psi\rangle$ is given by

$$P_{\max} = \max_{\theta_1,\ldots,\theta_L,\gamma_1,\ldots,\gamma_L} |f(\psi,\theta_1,\ldots,\theta_L,\gamma_1,\ldots,\gamma_L)|^2, \quad (22)$$

namely, the dimension of the parameter space in which the maximization is obtained is $2L$. However, the number of terms summed up in the calculation of f increases exponentially with the number of qubits. Therefore, to make the calculation of $G(\psi)$ feasible, one should minimize the number of evaluations of f. The commonly used steepest descent algorithm, requires a large number of evaluations of f and is thus computationally inefficient. Here we accelerate the calculation by performing the maximization analytically and separately for a single pair of θ_k and γ_k. During each maximization step, all the other parameters are held fixed. In the maximization, we have a function of the form

$$f = c_k \cos\theta_k + d_k e^{i\gamma_k}\sin\theta_k, \quad (23)$$

where $a_k = |a_k|e^{i\alpha_k}$ and $b_j = |b_j|e^{i\beta_j}$ depend on the other $2L-2$ parameters. The maximization of $|f|^2$ vs θ_k and γ_k leads to

$$|f|^2 \to |c_k|^2 + |d_k|^2, \quad (24)$$

where

$$\cos\theta_k \to \frac{|c_k|}{\sqrt{|c_k|^2 + |d_k|^2}} \quad (25)$$

and

$$\gamma_k \to \alpha_k - \beta_k. \quad (26)$$

Using this method, the number of evaluations of f is significantly reduced. To find the global maximum, $P_{\max}$ and then $G(\psi)$, we perform several rounds of maximization over all the $2L$ parameters. Trying different initial conditions, we find that the convergence to the global maximum is fast and no other local maxima are detected.

IV. ENTANGLEMENT DURING SHOR'S ALGORITHM

Shor's factoring algorithm includes a preprocessing stage followed by QFT. Here we analyze the quantum states generated in each of these stages and evaluate their entanglement using the Groverian measure.

A. Entanglement generated by the QFT procedure

Here we evaluate the time evolution of the Groverian entanglement during the QFT process, shown in Fig. 1. The Groverian measure is evaluated after each operation of the $B_{k,m}$ operator. The A_k operators are local and do not change

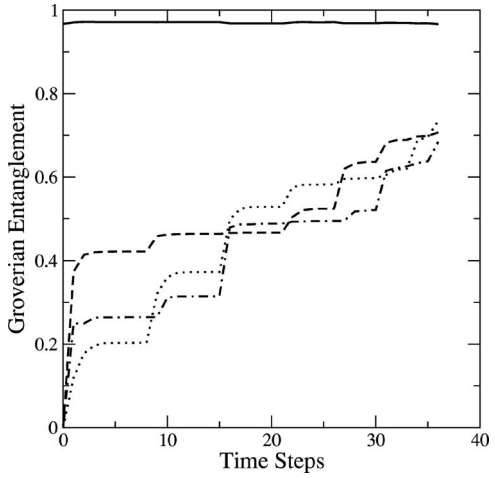

FIG. 2. The Groverian measure of entanglement for states created during the operation of the QFT on three randomly chosen tensor product states (dashed, dotted, and dashed-dotted) as well as on a single random state (solid line). All the states are of nine qubits.

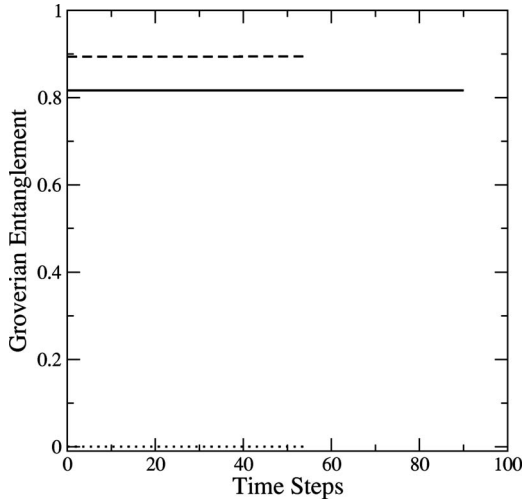

FIG. 3. The Groverian measure of entanglement for states created during the QFT stage of Shor's factoring algorithm. The solid line shows the factorization of $N=91$ using $y=41$. The dotted line (with zero entanglement) shows the factorization of $N=33$ using $y=23$. The dashed line shows the factorization of $N=33$ using $y=4$.

the entanglement. We first perform this analysis for general quantum states and then focus on the specific quantum states that appear in the factoring algorithm.

1. QFT applied on general quantum states

To examine the effect of QFT on the Groverian entanglement, we construct an ensemble of random product states as well as random states of n qubits. The state of each qubit in the random product states is described by Eq. (19), where $0 \leqslant \theta_k < \pi$ and $0 \leqslant \gamma_k < 2\pi$ are chosen randomly. The random states are drawn from an isotropic distribution in the 2^L-dimensional Hilbert space [10]. These states turn out to be highly entangled.

In Fig. 2, we present the time evolution of the Groverian measure during the processing of QFT on three random product states as well as on a random state of nine qubits. For the random product states, one observes that during most time steps, the entanglement remains unchanged. Most of the variation takes place at specific times, common to all the different states. Clearly, the entanglement is generated by the controlled phase operators $B_{k,m}$. The large variations in $G(\psi)$ are found to take place when $|m-k|$ is small, namely when $B_{k,m}$ is applied on pairs of adjacent qubits. The Groverian measure during the operation of QFT on a highly entangled random state is also shown in Fig. 2. It exhibits only small variations with no obvious regularity.

2. QFT within Shor's factoring algorithm

In Fig. 3, we present the time evolution of the Groverian measure during QFT, when it is applied on states obtained from the preprocessing stage of Shor's factoring algorithm. The different lines correspond to the factorization process of different numbers. Surprisingly, for all numbers that we have tested, the entanglement was essentially unchanged throughout the process, as implied by the horizontal lines. This is in contrast to the behavior observed when QFT is applied to general quantum states.

A special property of the states generated by the preprocessing is that they are periodic. This motivated us to examine the time evolution of the Groverian measure during QFT of general periodic states. The state $\Sigma_m |l+mr\rangle$ (up to normalization factor) is a periodic state of L qubits, with period r and shift l. The summation is over all integers m such that $0 \leqslant l+mr \leqslant q-1$, where $q=2^L$. It was found that the Groverian measure essentially does not change during the QFT process of such states and that the changes which do occur vanish exponentially with the number of qubits. The value of the Groverian measure for these states depends almost solely on the odd part of the period r. More precisely, for a periodic state with period $r=2^M d$ (where d is odd), we obtain $P_{\max} \simeq 1/d$. This is easy to explain for states with a period $r=2^M$, which are known to be tensor product states. For these states, $d=1$, thus the correct result of $P_{\max}=1$ is obtained. For general periodic states, we do not have an analytical derivation of the expression for $P_{\max}$.

B. Entanglement in the preprocessing stage

Having found that the QFT stage of Shor's algorithm does not alter the entanglement of states created by the preprocessing stage, it is clear that all the entanglement is produced during preprocessing (see Fig. 4). We have evaluated this entanglement generated during the factoring process of all the integers in the range $3 \leqslant N \leqslant 200$. To factorize an integer N, one has to choose another integer $1 < y < N-1$. In our analysis, we examined all possible choices within this range, and for each of them, we applied the preprocessing stage as described in Sec. II. At the end of the preprocessing stage, we evaluated the Groverian measure of the resulting state of the main register, following a measurement of the auxiliary register. In Fig. 4, we present the Groverian measure for the states obtained after preprocessing vs N for $3 \leqslant N \leqslant 200$.

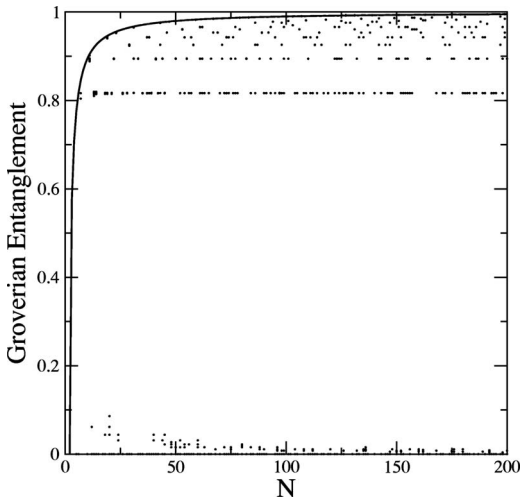

FIG. 4. The Groverian measure of entanglement for the states created by the preprocessing stage of Shor's algorithm. Each dot corresponds to a single choice of $2<N\leqslant 200$ and $1<y<N-1$.

Each dot represents the Groverian measure after preprocessing for the integer N and for a specific choice of $1<y<N-1$. The solid line represents the function $\sqrt{1-1/(2N)}$. We observe that all the dots are below this line, which resembles the upper bound of the Groverian measure, namely that for any state $|\psi\rangle$ of L qubits $G(\psi)\leqslant\sqrt{1-1/2^L}$.

Additionally, there are many values of N and choices of y for which the Groverian measure is $G=0$, namely the factoring process does not involve any entanglement. For these particular choices, it should thus be possible to perform the factoring of N efficiently using a classical algorithm [8]. We find that for some of the pairs of N and y which produce no entanglement, $\mathrm{GCD}(N,y)\neq 1$, thus a divisor of N can be easily found classically. The rest of these pairs are found to satisfy $y^{2^n}=1 \bmod N$, for some integer n, which means that $\mathrm{GCD}(y^{2^{n-1}}+1,N)$ or $\mathrm{GCD}(y^{2^{n-1}}-1,N)$ are divisors of N, which can be easily found by classical algorithms. We thus find that in cases in which no entanglement is produced by the quantum algorithm, it offers no speedup compared to classical algorithms. This is consistent with the assumption that the entanglement generated by a quantum algorithm is correlated with the speedup it provides.

V. DISCUSSION

It is found that the states prepared by the preprocessing stage of Shor's algorithm, like all periodic states, exhibit the property that their Groverian entanglement does not change throughout the QFT stage. One may take the view that the Groverian entanglement somehow represents the amount of quantum information present in a quantum state. This is rather like the von Neumann entropy. Taking this view, our result may seem natural because the information needed to perform the factoring is already present after the preprocessing stage. The QFT only rearranges the information such that it can be extracted by measurement.

It is found that the Groverian measure of the states generated by Shor's algorithm is lower than that of random states, which are almost maximally entangled, with $G(\psi)\simeq\sqrt{1-1/q}$ [10,15]. Yet, the maximal entanglement created by the algorithm exhibits the same functional behavior, where q is replaced by $2N$.

Considering the fact that Shor's algorithm is exponentially faster than its known classical counterparts, it is expected to use all the entanglement available. Thus, our result provides further indication that classical algorithms are unlikely to perform factoring in polynomial time.

Unlike Shor's algorithm, Grover's search algorithm is only polynomially more efficient than its classical counterparts [2,3]. Grover's algorithm also creates entanglement, which is bound by a constant lower than unity [15].

A different approach to the analysis of the entanglement generated by Shor's factoring algorithm was presented in Ref. [16], where the bipartite entaglement between the main register and the auxiliary register was evaluated during both the preprocessing and QFT stages, using the negativity [17,18] as an entanglement measure. It was found that the entanglement is primarily generated during the preprocessing stage, in agreement with our results.

VI. SUMMARY

The quantum states created during the operation of Shor's factoring algorithm have been analyzed and the entanglement in these states was evaluated using the Groverian measure. It was found that the entanglement is generated during the preprocessing stage and remains unchanged during the QFT stage. It was shown that the latter feature is unique to periodic states, such as those obtained from the preprocessing stage, while QFT does affect the entanglement of general quantum states. Another interesting feature is that the entanglement is found to be correlated with the speedup achieved by the quantum algorithm compared to classical algorithms. This means that the cases where no entanglement is created are those in which classical factoring is efficient.

[1] 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.

[2] L. Grover, in *Proceedings of the Twenty-Eighth Annual Symposium on the Theory of Computing* (ACM Press, New York, 1996), p. 212.

[3] L. K. Grover, Phys. Rev. Lett. **79**, 325 (1997).

[4] D. Deutsch and R. Jozsa, Proc. R. Soc. London, Ser. A **439**, 553 (1992).

[5] R. Josza, Proc. R. Soc. London, Ser. A **454**, 323 (1998).

[6] R. Jozsa and N. Linden, Proc. R. Soc. London, Ser. A **459**, 2011 (2003).

[7] G. Vidal, Phys. Rev. Lett. **91**, 147902 (2003).
[8] D. Aharonov and M. Ben-Or, in *Proceedings of the 37th Annual Symposium on the Foundations of Computer Science*, edited by S. Goldwasser (IEEE Computer Society, Los Alamitos, CA, 1996), p. 46.
[9] O. Biham, M. A. Nielsen, and T. J. Osborne, Phys. Rev. A **65**, 062312 (2002).
[10] Y. Shimoni, D. Shapira, and O. Biham, Phys. Rev. A **69**, 062303 (2004).
[11] V. Vedral, M. B. Plenio, M. A. Rippin, and P. L. Knight, Phys. Rev. Lett. **78**, 2275 (1997).
[12] V. Vedral and M. B. Plenio, Phys. Rev. A **57**, 1619 (1998).
[13] V. Vedral, M. B. Plenio, K. Jacobs, and P. L. Knight, Phys. Rev. A **56**, 4452 (1997).
[14] A. Miyake and M. Wadati, Phys. Rev. A **64**, 042317 (2001).
[15] O. Biham, D. Shapira, and Y. Shimoni, Phys. Rev. A **68**, 022326 (2003).
[16] V. M. Kendon and W. J. Munro, e-print quant-ph/0412140 (unpublished).
[17] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).
[18] K. Życzkowski, P. Horodecki, A. Sanpera, and M. Lewenstein, Phys. Rev. A **58**, 883 (1998).