PHYSICAL REVIEW E **74**, 035203(R) (2006)

Quantum chaos in the spectrum of operators used in Shor's algorithm

Krishnendu Maity and Arul Lakshminarayan*
Department of Physics, Indian Institute of Technology Madras, Chennai, 600036, India
(Received 16 April 2006; published 15 September 2006)

We provide compelling evidence for the presence of quantum chaos in the unitary part of the operator usually employed in Shor's factoring algorithm. In particular we analyze the spectrum of this part after proper desymmetrization and show that the fluctuations of the eigenangles as well as the distribution of the eigenvector components follow the circular unitary ensemble of random matrices, of relevance to quantized chaotic systems that violate time-reversal symmetry. However, as the algorithm tracks the evolution of a single state, it is possible to employ other operators; in particular, it is possible that the generic quantum chaos found above becomes of a nongeneric kind such as is found in the quantum cat maps and in toy models of the quantum baker's map.

DOI: 10.1103/PhysRevE.74.035203 PACS number(s): 05.45.Mt, 03.67.Lx

The signatures of classical chaos in the quantum domain have been of continuing interest for many years now and have impacted various areas of physics [1–3]. The recent developments in quantum information theory and quantum computation have also prompted studies that delve into the effects of chaos on quantum computers [4] and on entanglement [5], a key resource in such processes. There have also been studies that seek efficient implementation of quantum chaotic models on quantum computers [6], as well as, to the best of our knowledge, one study that seeks to see if there is intrinsic chaos in some quantum algorithms [7]. Such algorithms are typically unitary evolutions, generated ultimately by Hamiltonian evolutions, followed by measurements. The previous study [7] focused on the quantum Fourier transform and Grover's search algorithm, and several tests of quantum chaos were used. The evidence for quantum chaos was not unequivocal due to extreme degeneracies and other unusual features. Besides, the quantum Fourier transform viewed as Weyl quantization quantizes a 90° rotation of phase space and should therefore not be expected to have properties typical of quantum chaos. For any value of dimensionality of the transform, its fourth power is unity.

On the other hand, that Shor's factoring algorithm [8] is a candidate for quantum chaos has been indicated by earlier works of one of the authors [9]. This is due the fact that the order-finding algorithm, at the heart of Shor's algorithm, has a key component, the modular exponentiation operator, which is essentially a shift permutation operator S. This shift permutation operator has been shown to be metrically close to the quantum baker's map [10], quantization of a paradigm of classical chaos—namely, the double-sided left shift [11]. Operators closely allied with the shift operator may also be thought of as quantizing a multivalued [12] or a random map [13]. Viewed as a Weyl quantization, its action on phase-space-coherent states produces stretching and folding [9], its overall periodicity making it akin to the quantum cat map [14]. The quantum cat map quantizes another classically fully chaotic system: the cat map [15]. However, its quantum propagator is exactly periodic, with a periodicity that plays the role of the order in Shor's algorithm. We have also previously shown how to construct the quantum baker's map using the shift operator and suitable projectors [9].

In this Rapid Communication we examine Shor's algorithm as a whole and show that its unitary part has properties that one would normally ascribe to systems that are classically chaotic and for which time-reversal symmetry is broken. The order-finding part of the algorithm [8] is quantum mechanical and involves two registers containing n_1 and n_2 qubits, respectively. We call the corresponding Hilbert spaces $\mathcal{H}^1$ and $\mathcal{H}^2$. The standard product basis in the space $\mathcal{H}^1 \otimes \mathcal{H}^2$ is denoted as $|j\rangle|k\rangle$, $0 \le j \le 2^{n_1}-1$ and $0 \le k \le 2^{n_2}-1$. Shor's algorithm proceeds by using the following operator:

$$U = (F^{-1} \otimes \mathrm{I}) U_x (H \otimes \mathrm{I}). \tag{1}$$

Here F^{-1} is the inverse discrete Fourier transform and H is the Hadamard matrix, which act only on the first register, while U_x is the entangling part defined by its action on a basis vector $|j\rangle|k\rangle$ as

$$U_x|j\rangle|k\rangle = |j\rangle|x^j k \bmod N\rangle \equiv |j\rangle S^j|k\rangle, \quad 0 \le k \le N-1. \tag{2}$$

If $k \ge N$, then $U_x|j\rangle|k\rangle = |j\rangle|k\rangle$. This defines the shift operator S as $S|k\rangle = |xk \bmod N\rangle$ for $0 \le k \le N-1$ and $S|k\rangle = |k\rangle$ otherwise. Here N is the integer we wish to factor and x is an integer that is coprime to it.

For our study below we will take $x=2$ and N to be an odd integer so that we are guaranteed that an integer r exists such that $2^r = 1 \bmod N$, where r is the order we are seeking. Thus U acts nontrivially in a $(2^{n_1}N)$-dimensional subspace of the full Hilbert space $\mathcal{H}^1 \otimes \mathcal{H}^2$. Now Shor's algorithm proceeds by taking a particular initial state $|0\rangle|1\rangle$, acting on this with U and measuring the first register, followed by classical steps intended to find the order r, from which using standard number theory it may be possible to find a factor of N if it exists. We will analyze the *entire* spectrum of U considered as an operator of dimension $2^{n_1} N$.

*Electronic address: arul@physics.iitm.ac.in

We note that as the order-finding algorithm needs to consider only action on the initial state $|0\rangle \otimes |1\rangle$, U is not the only operator that achieves the necessary result. For instance the first operation of a Hadamard gate on the qubits of the first register may be replaced by a Fourier transform, since acting on $|0\rangle$ this also produces an equal superposition of all standard basis states: $H|0\rangle = F|0\rangle$. In this case the overall unitary part of the algorithm would be

$$\tilde{U} = (F^{-1} \otimes \mathrm{I}) U_x (F \otimes \mathrm{I}). \tag{3}$$

The eigenvalues of $\tilde{U}$ are thus the same as that of U_x. The central operation is the modular exponentiation, and the quantum chaos in this can be made "generic" or not, depending on the choice of unitary operators such as U or $\tilde{U}$ above. The experimental realizations of the Shor algorithm and order-finding algorithms [16] that have been carried out so far use the Hadamard gates on the first register, and the operator U is of relevance herein. We will return to consider $\tilde{U}$ later, but for now consider the standard operator U.

We first notice that

$$[U, \mathrm{I} \otimes S] = 0. \tag{4}$$

We can label the eigenstates of U with eigenvalues of S, which are like good quantum numbers. The spectrum of S is thus of interest. As $S^r = \mathrm{I}_N$, we have

$$S|s_j\rangle = e^{i\theta_j}|s_j\rangle, \quad 0 \le j \le N-1, \tag{5}$$

where θ_j, the eigenangle, is of the form $2\pi k/r$ and $0 \le k \le r-1$. The eigenstates of U can be chosen to be $|\phi_l\rangle|s_j\rangle$, unentangled states of the two registers. We show this as follows. Let $H|\phi_l\rangle = \Sigma_m a_m |m\rangle$ and $|s_j\rangle = \Sigma_k b_k |k\rangle$. Then

$$\begin{aligned} U_2(H \otimes \mathrm{I})|\phi_l\rangle|s_j\rangle &= U_2 \sum_{m,k} a_m b_k |m\rangle|k\rangle = \sum_{m,k} a_m b_k |m\rangle S^m |k\rangle \\ &= \sum_m a_m e^{im\theta_j} |m\rangle|s_j\rangle \\ &= \sum_m e^{im\theta_j} |m\rangle\langle m|H|\phi_l\rangle|s_j\rangle \\ &= (\Lambda_j H \otimes \mathrm{I})|\phi_l\rangle|s_j\rangle, \end{aligned} \tag{6}$$

where $\Lambda_j = \Sigma_m e^{im\theta_j}|m\rangle\langle m|$ is a diagonal operator on the first register whose entries are powers of the eigenvalues of S. Hence $U|\phi_l\rangle|s_j\rangle = (F^{-1}\Lambda_j H|\phi_l\rangle)|s_j\rangle$. Therefore $|\phi_l\rangle|s_j\rangle$ will be an eigenstate of U with eigenvalue λ_{jl} if

$$F^{-1}\Lambda_j H|\phi_l\rangle = \lambda_{jl}|\phi_l\rangle, \quad 0 \le l \le 2^{n_1} - 1. \tag{7}$$

Thus we have split or block-diagonalized the full $(2^{n_1}N)$-dimensional matrix diagonalization problem to that for N matrices of dimensions 2^{n_1} each. There is also a dependence of the eigenstates $|\phi_l\rangle$ on the eigenangle θ_j, but we suppress this.

The operators $F^{-1}\Lambda_j H$, for $0 \le j \le N-1$, are unitary operators whose eigenvalues are that of the unitary part of Shor's algorithm. When $\theta_j = 0$, the relevant operator is simply $F^{-1}H$. This "Fourier transform of the Hadamard transform" was studied recently as a model of eigenstates of quantum chaos [17]. It was demonstrated that columns of this matrix could be multifractals in the $N \to \infty$ limit with peaks connected to the periodic and homoclinic orbits of the doubling map $x \mapsto 2x \bmod 1$. These are of relevance to the spectrum of the quantum baker's map. It is thus of interest that a generalized construction arises in the spectral problem of Shor's algorithm.

On using the matrix elements of F^{-1} and the Hadamard matrix it is possible to write the matrix elements

$$(F^{-1}\Lambda_j H)_{kl} = \frac{1}{2^{n_2}} \prod_{m=0}^{n_1-1} [1 + (-1)^{b_m} e^{-2\pi i k 2^{m-n_1}} e^{i\theta_j 2^m}], \tag{8}$$

where $l = \Sigma_{m=0}^{n_1-1} b_m 2^m$ is the binary representation of l. When $\theta_j = 0$ and $l = 2^{n_1} - 1$ corresponding the case $b_m = 1$ for all m, this is the Fourier transform of the Thue-Morse sequence [18], well known to be a multifractal in the large-n_1 limit [19]. Thus the matrix elements of $F^{-1}\Lambda_j H$ while having a simple form that is efficient to compute are in fact quite complex objects. We now demonstrate that their spectrum has characteristics of that of a random matrix.

We illustrate this with a case $n_1 = 10$ and $N = 29$. We diagonalize $F^{-1}\Lambda_j H$ for five different values of θ_j—namely, $-20\pi/28$, 0, $4\pi/28$, $6\pi/28$, and $14\pi/28$, choosing these to be a mixture of generic and special eigenangles of S. The eigenvectors of S can also be written, for example, as

$$|s_j\rangle = \frac{1}{\sqrt{r}} \sum_{n=0}^{r-1} \exp\left(\frac{-2\pi i j n}{r}\right) |2^n \bmod N\rangle, \tag{9}$$

where $0 \le j \le r-1$ are eigenvectors corresponding to eigenvalues $e^{2\pi i j/r}$. In general this is not the complete set, but others can be found based on subgroups generated by other "seeds," where the seed is the integer i_0 and the group it generates is the set of integers $2^k i_0 \bmod N$ for various k. For instance, in the case $N = 29$, the above set generates $r = 28$ eigenstates of S with the seed 1. The remaining state is a stand-alone one with the seed 0 and is the state $|0\rangle$ itself, with an eigenvalue 1. Thus apart from the double degeneracy of this eigenvalue the other 27 eigenvalues are nondegenerate. However, this depends on the order r—for example, if $N = 31$ and $r = 5$, the spectrum of S is highly degenerate. In these cases there are other symmetries like a bit flip that arise [20], but we will not elaborate on these as they are inessential to the central purpose of this Rapid Communication.

It is, however, pertinent to point out that eigenvectors such as in Eq. (9) are completely delocalized, in fact have modulus unity for almost all components, and the phase would seem random. Thus these are simple examples of states that are ergodic in accordance with Shnirelman's theorem [21] about a measure of states that tend to be ergodic in the classical limit for quantized ergodic systems. The classical limit in this case would be over integers N that are such that their order (with respect to 2) is $N-1$.

Returning to the central issue, we find the nearest-neighbor spacings (NNS's) of eigenangles for the five chosen cases, thus making an ensemble with statistical significance. The NNS's are calculated for the normalized spacings $\Delta\alpha_{jl} 2^{n_1}/2\pi$ such that the mean spacing is unity, where

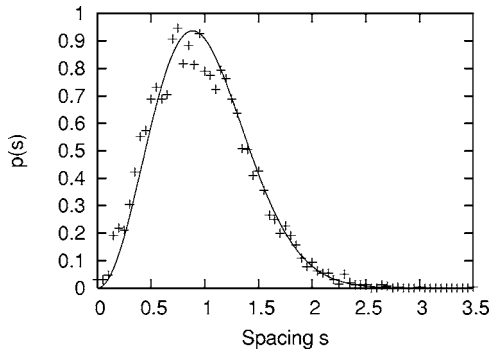

FIG. 1. The nearest-neighbor spacing distribution of eigenangles from an ensemble consisting of 5115 level spacings for the case when the first register has 10 qubits and the number to be factored is 29. The smooth curve shows the circular unitary ensemble (CUE) distribution of random matrix theory.

$\lambda_{jl}=e^{i\alpha_{jl}}$ and $\Delta\alpha_{jl}$ refers to spacings between nearest neighbors. In Fig. 1 we show how the NNS's are distributed along with the curve expected for the circular unitary ensemble (CUE), which consists of the unitary group U(n) of $n\times n$ unitary matrices endowed with its Haar measure [22]. The good agreement with the CUE distribution [22] (which coincides with the Wigner surmise for the Gaussian ensembles for large dimensionality)

$$p(s)=\frac{32s^2}{\pi^2}e^{-4s^2/\pi} \tag{10}$$

indicates the applicability of random matrix theory (RMT) to the spectral fluctuations of the unitary part of Shor's algorithm. It is generally accepted that while there are exceptions, random matrix fluctuations are quantum signatures of classical chaos [3]. In this case the classical limit may be considered to be the large-N (or n_1) limit, which is in fact the regime where Shor's factoring algorithm will ever be usefully implemented.

The eigenfunctions are also of interest, and in Fig. 2 is shown a typical eigenstate of $F^{-1}\Lambda_j H$ in the standard basis for the first of the five values of θ_j stated above. Almost all of the eigenfunctions have this very random appearance and

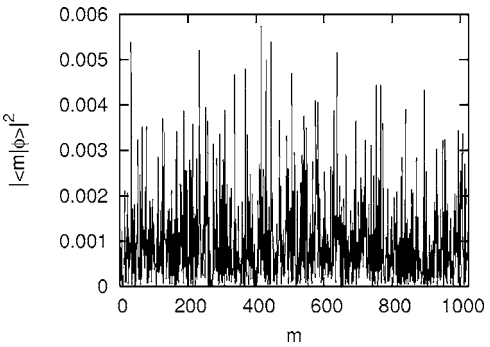

FIG. 2. The intensities of a typical eigenstate of the operator $F^{-1}\Lambda_j H$ for the same case as in Fig. 1. The complete eigenstate of the unitary part of Shor's algorithm is a tensor product of such states with eigenstates of the shift permutation operator.

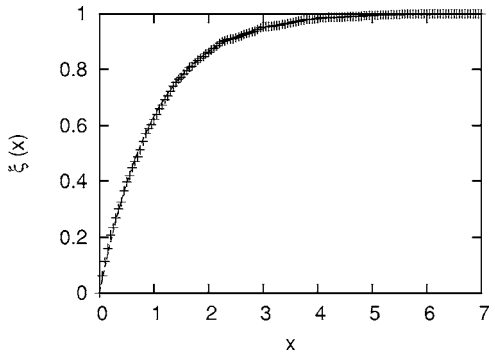

FIG. 3. The cumulative distribution $\xi(x)$ of the intensities of the eigenstate shown in Fig. 2, these being normalized so that the mean is unity. Shown as a smooth curve is the random matrix theory expectation $1-e^{-x}$.

an analysis of the distribution of its normalized intensities $x=2^{n_1}|\langle m|\phi\rangle|^2$ fits with that expected from random matrix theory. These normalized intensities with unit mean are distributed in an exponential manner e^{-x}. In Fig. 3 we show the cumulative distribution $\xi(x)$ of x and compare it to that expected from random matrix theory—namely, $1-e^{-x}$ [3]—and again find a good fit. Data not shown here confirm both the NNS and eigenvector component statistics for a variety of other parameter values and states, the results shown being typical. Of course the complete eigenstate of the unitary part of Shor's algorithm is a tensor product of such eigenstates of random appearance with eigenstates of the form in Eq. (9), which have phase complexity but in modulus are almost equidistributed.

Thus there is compelling evidence that the operator U used in standard implementations of Shor's algorithm has quantum chaos in it, of the type expected of systems that do not have time-reversal symmetry. The genesis of this is from two sources: One is the modular exponentiation operator, which as we have noted earlier is closely allied to models of quantum chaos such as the quantum baker's map [9]. The other is from a combination of the Fourier and Hadamard transforms. Thus the spectral properties of $F^{-1}H$ by itself may be interesting. It may be also noted that this is the operator relevant to the subspace $\theta_j=0$, which also includes the subspace left out due to the modular exponentiation part acting as identity on it [of dimension $(2^{n_2}-N)2^{n_1}$]. This last combination may be made irrelevant to Shor's algorithm by making use of $\tilde{U}$ instead of U. The operator $\tilde{U}$ is exactly periodic, as both F and U_x are. Its spectrum is highly degenerate and the same as the shift operator. The eigenvalues are thus equally spaced on the unit circle, reminiscent of the quantum cat maps. The use of H instead of F (U instead of $\tilde{U}$) seems to lift this nongeneric spectrum into a more generic one. There could be other operators that also accomplish order finding with different initial states, but the core of the algorithm, the modular exponentiation, will introduce quantum chaos into the system.

There could be implications of the RMT fluctuations found on the practical functioning of the algorithm. In particular quantum chaotic systems have been found to have hypersensitivity to perturbations of the Hamiltonian or noise

[24,23]. It is possible that in some way the state used in Shor's algorithm as the initial state is "protected" from this, but it remains to be seen whether this is indeed the case. For this, an analysis that concentrates on the time evolution rather than stationary states will be of relevance. In particular it is of interest to investigate whether U and $\tilde{U}$ are qualitatively different in their response to perturbations and more generally whether use of the Fourier transform to produce equal superpositions out of $|0\rangle$ instead of the Hadamard gate is more robust. Work is ongoing in these directions [25].

A.L. wishes to thank Dr. Arvind for discussions.

[1] M. V. Berry, Proc. R. Soc. London, Ser. A **413**, 183 (1987).
[2] *Chaos and Quantum Physics, 1991 Les Houches Lectures II*, edited by M.-J. Giannoni, A. Voros, and J. Zinn-Justin (North-Holland, Amsterdam, 1991).
[3] F. Haake, *Quantum Signatures of Chaos* (Springer, Berlin, 1991).
[4] B. Georgeot and D. L. Shepelyansky, Phys. Rev. E **62**, 6366 (2000).
[5] A. Lakshminarayan, Phys. Rev. E **64**, 036207 (2001).
[6] B. Georgeot and D. L. Shepelyansky, Phys. Rev. Lett. **86**, 2890 (2001).
[7] D. Braun, Phys. Rev. A **65**, 042317 (2002).
[8] P. W. Shor, SIAM J. Comput. **26**, 1484 (1997); M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).
[9] Arul Lakshminarayan, J. Phys. A **38**, L597 (2005).
[10] N. L. Balazs and A. Voros, Ann. Phys. (N.Y.) **190**, 1 (1989).
[11] A. J. Lichtenberg and M. A. Lieberman, *Regular and Chaotic Dynamics* (Springer, New York, 1992).
[12] S. Nonnenmacher and M. Zworski, J. Phys. A **38**, 10683 (2005).
[13] M. Tracy Mark and A. J. Scott, J. Phys. A **35**, 8341 (2002).
[14] J. H. Hannay and M. V. Berry, Physica D **1**, 267 (1980); J. P. Keating, Nonlinearity **4**, 309 (1991).
[15] V. I. Arnold and A. Avez, *Ergodic Problems of Classical Mechanics* (Benjamin, New York, 1968).
[16] L. K. M. Vandersypen *et al.*, Phys. Rev. Lett. **85**, 5452 (2000); Nature (London) **414**, 883 (2001).
[17] N. Meenakshisundaram and Arul Lakshminarayan, in *Proceedings of the National Conference on Nonlinear Systems and Dynamics*, edited by M. Lakshmanan and R. Sahadevan (Allied Publishers, Chennai, India, 2006).
[18] J. P. Allouche and J. Shallit, Sequences and their Applications, *Proceedings of the 1998 SETA Conference*, edited by C. Ding, T. Helleseth, and H. Niederreiter (Springer, Berlin, 1999); *Automatic Sequences: Theory, Applications and Generalizations* (Cambridge University Press, Cambridge, England, 2003).
[19] C. Godreche and J. M. Luck, J. Phys. A **23**, 3769 (1999); M. A. Zaks, A. S. Pikovsky, and J. Kurths, *ibid.* **32**, 1523 (1999).
[20] N. Meenakshisundaram and Arul Lakshminarayan, J. Phys. A **39**, 11205 (2006).
[21] A. Schnirelman, Usp. Mat. Nauk **29**, 181 (1974).
[22] M. L. Mehta, *Random Matrices*, 3rd ed. (Academic Press, New York, 1991).
[23] A. Peres, in *Quantum Chaos*, edited by H. A. Cerdeira, R. Ramaswamy, M. C. Gutzwiller, and G. Casati (World Scientific, Singapore, 1991).
[24] R. Schack, G. M. D'Ariano, and C. M. Caves, Phys. Rev. E **50**, 972 (1994); R. Schack and C. M. Caves, *ibid.* **53**, 3257 (1996).
[25] N. Meenakshisundaram and Arul Lakshminarayan (unpublished).