Testing integrability with a single bit of quantum information

David Poulin,[1,2] Raymond Laflamme,[1,2] G. J. Milburn,[3] and Juan Pablo Paz[4,5]
[1]*Perimeter Institute for Theoretical Physics, 35 King Street N., Waterloo, Ontario, Canada N2J 2W9*
[2]*Institute for Quantum Computing, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1*
[3]*Centre for Quantum Computer Technology, School of Physical Science, The University of Queensland, Queensland 4072, Australia*
[4]*Departamento de Física "J.J. Giambiagi," FCEN, UBA, Pabell on 1, Ciudad Universitaria, 1428 Buenos Aires, Argentina*
[5]*Theory Division, MS B213, Los Alamos National Laboratory, Los Alamos, New Mexico 87545, USA*
(Received 11 March 2003; published 1 August 2003)

We show that deterministic quantum computing with a single bit can determine whether the classical limit of a quantum system is chaotic or integrable using $O(N)$ physical resources, where N is the dimension of the Hilbert space of the system under study. This is a square-root improvement over all known classical procedures. Our study relies strictly on the random matrix conjecture. We also present numerical results for the nonlinear kicked top.

DOI: 10.1103/PhysRevA.68.022302 PACS number(s): 03.67.Lx, 05.45.Mt

I. OVERVIEW

After an initial success in solving mathematical problems (see Ref. [1] for an overview), a large fraction of the researches in the field of quantum information processing has shifted to its original motivation: the simulation of quantum systems [2]. It is now well established [3–5] that evolution produced by certain classes of Hamiltonians can be simulated efficiently on a universal quantum processor. However, extracting useful information from the physical simulation is a problem whose complexity has been underestimated. Indeed, the ability to simulate the dynamics of a system does not grant one with the ability to evaluate efficiently all physical quantities of interest. These quantities (e.g., spectral properties) are usually measured experimentally on a (exponentially) large number of physical systems—macroscopic samples. A direct quantum simulation, on the other hand, can only reproduce the statistical output of a single quantum system which yields drastically less information than what is learned from costly classical simulations. Thus, it is not clear at this point whether quantum simulators can always outperform their classical analogs.

Some of these spectral properties play a central role in the study of quantized chaotic systems. One particular question of interest is whether the classical limit of a quantum system exhibits regular or chaotic motion. It has become widely accepted (see Refs. [6,7], and references therein) that the answer to this question lies in some spectral properties of the system, which can be reproduced by those of canonical random matrices with the appropriate symmetries. Given a description of the Hamiltonian of the system, the best-known algorithms evaluating these ''signatures of chaos'' require classical computing resources which grow at least as fast as N^2, the square of the dimension of the Hilbert space of the system under study. Indeed, a close inspection of these algorithms shows that they require either matrix multiplication, diagonalization, or evaluation of a determinant [6]. Since such a growth is intractable on any conventional computer (remember that N grows exponentially with the size of the physical system), it is quite natural to try to tackle this problem with a quantum computer. In recent years, this interest has led to a demonstration that the standard model of quantum computation can simulate efficiently the dynamics of a few quantized chaotic models [8–10]; unfortunately, none of these proposals indicate how to circumvent the measurement problem mentioned above.

A recent work by Emerson *et al.* [11] proposes to study statistical properties of the system's eigenvectors relative to a perturbation as a signature of chaos. They also provide an efficient procedure to measure these statistics using the standard model of quantum computation. Their motivation for this work was to show that quantum processors can be used to test the validity of signatures of chaos. Indeed, it is not clearly established that this signature is universal, perturbation independent, and, most importantly, that the decay time does not scale with the size of the system.

Here, we concentrate on a different model (presumably weaker): deterministic quantum computation with a single pseudopure bit (DQC1) which was introduced in Ref. [12]. In this setting, the initial state of the $K+1$ qubits computer is

$$\rho = \left\{ \frac{1-\epsilon}{2}\mathbb{1} + \epsilon|0\rangle\langle 0| \right\} \otimes \frac{1}{2^K}\mathbb{1},$$

where $0<\epsilon\leqslant 1$ is a constant. Note that, from a computational complexity point of view, this is equivalent to a model where the state of the first qubit is pure, while the other ones are completely random; we shall therefore assume that $\epsilon = 1$ in the remaining part of the paper. The final answer is given by a finite accuracy evaluation of the average value of σ_z on the first qubit. As for the dynamics, we assume that we are provided with the ability to excercise coherent control over one and two qubits at a time. This model is of particular interest, since it is weaker than the computational model offered by liquid-state nuclear magnetic resonance (NMR) quantum computing [13]. Such a computing device, we shall show, can test for integrability using $O(N)$ physical resources, given that the dynamics of the system of interest is efficiently simulatable on the standard model of quantum computation without ancillary pure qubits [or, more precisely, with no more than $O(\log_2 K)$ ancillary pure qubits].

In order to do so, we must first relate the theory underlying the spectral property at the center of our study; this is done in Sec. II. We then show how it can be evaluated with $O(N)$ physical resources in the DQC1 model. In Sec. IV, we present numerical results for canonical random matrices as well as for a physical map, the nonlinear kicked top. Finally, we conclude with a summary of our results and a discussion on possible extensions.

II. LEVEL DISTRIBUTION

In the theory of quantum chaos, a key role is played by the statistics of eigenvalues [6,7]. In the case of systems with a periodically time-varying Hamiltonian, the central dynamical object is the Floquet operator $\hat{F}=\tilde{T}[\exp\{-i\int_0^T H(t)dt\}]$, which maps the state from one time to a time exactly one modulation period T later, $\tilde{T}$ being the time-ordering operator. The eigenvalues of $\hat{F}$ lie on the unit circle and may be parametrized in terms of eigenphases, or quasienergies, as $\hat{F}|\phi_j\rangle=e^{-i\phi_j}|\phi_j\rangle$.

The random matrix conjecture asserts that the statistics of eigenvalues of chaotic systems (dynamical systems and maps) are typically well modeled by the statistics of the eigenvalues of random matrices (Hermitian Hamiltonians and unitary Floquet operators) with appropriate symmetries [6,7]. While many important mathematical results underpin the conjecture, a rigorous proof is lacking and support rests on a very large accumulation of numerical results.

An integrable system, by definition, possesses as many symmetries—constant of motion—as degrees of freedom. One can thus write the system's Hamiltonian as the direct sum of independent Hamiltonians acting on smaller subspaces; one for each value of the constants of motion. Some spectral properties of these Hamiltonians can thus be reproduced by those of matrices that are the direct sum of independent random Hermitian operators. The distribution characterizing the entire spectrum is therefore given by the superposition of many independent spectra; as a consequence, the correlations between levels vanish. Thus, one might expect that the nearest-neighbor level spacing distribution (LSD) follow a Poisson law $\text{prob}(\phi_{j+1}-\phi_j=S)=P(S)\sim e^{-\Gamma S}$, a straightforward consequence of their statistical independence. This is indeed observed experimentally, numerically, and most importantly can be derived formally [14].

On the other hand, chaotic systems possess no or just a few symmetries. It can be shown [6] that the LSD—keping aside systematic degeneracy following the symmetries—obeys a power law $P(S)\sim S^{\beta}e^{-\alpha S^2}$. The parameter β characterizes the symmetries of the system; it is equal to 1 when the system possesses a time-reversal symmetry and some geometric invariance, 2 when it has no symmetries, and 4 when it has a time-reversal symmetry with Kramer's degeneracy. Similarly, we will refer to the Poisson ensemble—the characteristic ensemble of integrable systems—as $\beta=0$.

The exact form of the LSD is not relevant to us; we shall capitalize on the crucial distinct behavior of $P(S\to 0)$ for chaotic and regular systems. In the former case, $P(S)$ reaches a minimum at $S=0$: the levels tend to repel each other. In the latter case, $P(S)$ is maximal at $S=0$, a consequence of the levels statistical independence called clustering.

With these considerations, one can predict the behavior of the ensemble-average form factors

$$T_n=|\text{Tr}\{\hat{F}^n\}|^2=\left|\sum_{j=1}^{N} e^{-in\phi_j}\right|^2, \tag{1}$$

from which most spectral properties can be extracted. For regular systems, $\text{Tr}\{\hat{F}\}=\Sigma_j e^{-i\phi_j}$ behaves like the end point of a random walk in the complex plane: each step having unit length and uncorrelated random orientation ϕ_j. After N steps, the average distance from the origin is expected to be $\sqrt{N}$ so we should find $\overline{T_1}=N$. For times $n>1$, the analysis is identical; if the angles $\{\phi_j\}$ are statistically independent, so are $\{\phi_j^{(n)}=n\phi_j \text{mod}(2\pi)\}$, n taking positive integer values. We conclude that the ensemble-average form factors of integrable systems should be time independent and equal to N.

For chaotic systems, more elaborate calculations are required for the ensemble-average form factors. They can be found in Ref. [6]; here, we shall simply provide an approximate result for $0<n<N$ (accuracy of the order of 10^{-2}) known as the Wigner surmises:

$$\overline{T_n}=\begin{cases} 2n-n\displaystyle\sum_{m=1}^{n}\frac{1}{m+(N+1)/2} & \text{for } \beta=1 \\ n & \text{for } \beta=2 \\ n+\dfrac{n}{2}\displaystyle\sum_{m=1}^{n}\frac{1}{N+1/2-m} & \text{for } \beta=4. \end{cases} \tag{2}$$

Although simple arguments could not indicate the exact behavior of these form factors, we could guess their general form: they are initially very small $\overline{T_1}\ll N$, and, as n grows, they reach the same value as the Poisson ensemble. Here, $\text{Tr}\{\hat{F}\}$ is analogous to an *anticorrelated* random walk in the complex plane composed of N unit steps. As a consequence of level repulsion, each steps tend to be oriented in different directions; the probability of finding two steps oriented within an angle ϵ decreases as $\epsilon^{\beta+1}$. Thus, the distance from the origin after N of these anticorrelated steps should definitely be smaller than $\sqrt{N}$, which is the expected value for uncorrelated steps. As n grows, the phases $n\phi_j \text{mod}(2\pi)$ get wrapped around the unit circle; the effect is analogous to superposing n independent spectral distributions, blurring out the correlations. When $n\sim N$, one should thus expect a behavior similar to the Poisson ensemble.

It should be noted that the few symmetries of a chaotic system may slightly affect the predictions of Eq. (2). The average $\overline{T_n}$ was evaluated for fixed values of the constant of motion. In what follows, we shall often neglect this point for the sake of simplicity. Nevertheless, as long as the number of invariant subspaces is small ($\ll\sqrt{N}$), this omission will not affect our conclusions. For example, if a chaotic system possesses a symmetry, which breaks its Hilbert space into k

equal invariant subspaces, the small-n behavior $\overline{T_n} \simeq n$ will be transformed into $\overline{T_n} \simeq k^2 n \ll N$, which is all that interests us. One can circumvent this issue when some exact symmetries of the system are known: it suffices to simulate the dynamics of the system within an invariant subspace.

In the light of this analysis, it may seem that form factors constitute a powerful tool to distinguish between classically regular and chaotic systems. In particular, T_n should clearly identify each regime for small values of n. Nevertheless, the form factor T_n of a fixed Floquet operator $\hat{F}$ will generally fluctuate about the ensemble average $\overline{T_n}$. Thus, we seek a signature of an *ensemble property* on a *single element* drawn from this ensemble.

The solution is to use a version of the ergodic theorem. If we normalize out the explicit time dependence of the form factors, an average over a time interval Δn reproduces the effect of an ensemble average. More precisely, one can show [6] that

$$\langle T_n / \overline{T_n} \rangle = \frac{1}{\Delta n} \sum_{n'=n-\Delta n/2}^{n+\Delta n/2} T_{n'} / \overline{T_{n'}} \tag{3}$$

converges to 1 with a variance σ^2 bounded by $1/\Delta n$. For large N, we can thus use the first $\Delta n \ll N$ form factors to determine whether the Floquet operator belongs to a polynomial or a Poisson ensemble. Since the values of $\overline{T_n}$—hence the matrix ensemble—are needed to compute Eq. (3), we shall proceed by hypothesis testing: for which choice of $\overline{T_n}$ ($\overline{T_n} = N$ regular, $\overline{T_n} \simeq n$ chaotic) does Eq. (3) converge to 1? In other words, we need to determine which of the two variables

$$t_0 = \frac{1}{\Delta n} \sum_{n=1}^{\Delta n} \frac{T_n}{N} \quad \text{or} \quad t_1 = \frac{1}{\Delta n} \sum_{n=1}^{\Delta n} \frac{T_n}{n} \tag{4}$$

is most probably drawn from a distribution centered at 1 with $1/\sqrt{\Delta n}$ standard deviation. If we restrict our attention to a regime where $\Delta n \ll N$, both hypotheses cannot have high probabilities simultaneously [17]. On the other hand, when the probabilities of both hypothesis are low, the test is inconclusive. Nevertheless, remember that the presence of symmetries in a chaotic system shifts the value of the distribution by a factor k^2, where k is the number of invariant subspaces. For $k^2 \ll N$, this should be clearly distinguishable from the value of a regular system. This should not be seen as a limitation but a feature of our approach allowing one to estimate k, the number of invariant subspaces.

Applying this test to a particular dynamical system would require one to compute the spectrum of the Floquet operator. If one was to try and simulate a dynamical map on a quantum computer with K qubits, a direct computation would require determining all $N = 2^K$ eigenvalues. In the following section we will construct a quantum circuit that would enable the form factors themselves to be extracted with $O(N)$ physical resources, thus allowing a direct test of nonintegrability that circumvented the need to explicitly compute all eigenvalues.

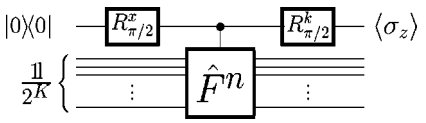

FIG. 1. Quantum circuit evaluating the trace of $\hat{F}^n$. The gates R^k_θ are rotation in the Bloch sphere by an angle θ around axis $k = x$ or y. When k is set to x, we get the real part of the trace, while $k = y$ yields the imaginary part.

III. QUANTUM ALGORITHM

The DQC1 algorithm evaluating the form factor is based on the idea reported in Ref. [15] of using a quantum computer as a spectrometer. The circuit is shown at Fig. 1 where $K = \lceil \log_2 N \rceil$. By hypothesis, we are able to efficiently simulate the dynamics of the system under study so the gate $\hat{F}^n$ only requires a polynomial (in n and K) number of elementary gates to be constructed. Here, it is not $\hat{F}^n$ we wish to implement but a coherently controlled version of it, i.e., a linear gate acting on $K+1$ qubits which applies $\hat{F}^n$ to the last K qubits when the first qubit is in state $|1\rangle$ and does not do anything when it is in state $|0\rangle$. Given the circuit for $\hat{F}^n$, standard techniques can be used to construct a controlled version of it at polynomial cost [16].

It should also be emphasized that the K qubits on which the Floquet operator is applied generate a Hilbert space of dimension 2^K which might be larger than the simulated system's Hilbert space. Thus, when applying $\hat{F}$ to those qubits, one really applies $\hat{F} \oplus U$, where ideally U is the identity operator on $2^K - N$ states; it can be any other unitary operator as long as its trace can be evaluated. The effect of these extra dimensions will be to add a contribution $\mathrm{Tr}\{U\}/N$ to the output signal which should be systematically subtracted as we shall henceforth assume.

The output of this computation will be the real and imaginary parts of $(\mathrm{Tr}\{\hat{F}^n\})/2^K$ when the last rotation is made about axis $k = x$ and $k = y$, respectively. Thus, our task is to distinguish between a signal whose amplitude is of the order of $1/N$ (chaotic dynamics) and one of the order of $1/\sqrt{N}$ (regular dynamics) which can be a chieved using $O(N)$ physical resources. In the special case of NMR quantum computing, one can, for example, increase the size of the sample by a factor N as the size of the system increases, or simply repeat the procedure N times and sum up the outputs. We thus get a quadratic advantage over all known classical algorithms.

IV. NUMERICAL RESULTS

A. Random matrices

Before applying our general proposal to a physical model, we give a numerical example illustrating the main results used from random matrix theory: the ergodic theorem of Eq. (4). In order to estimate the average and variance of t_0 and t_1 in a given universal matrix ensemble, we draw many random matrices $U^{(k)}$ from the ensemble and numerically evaluate each quantity. As an example, we have generated 50 random

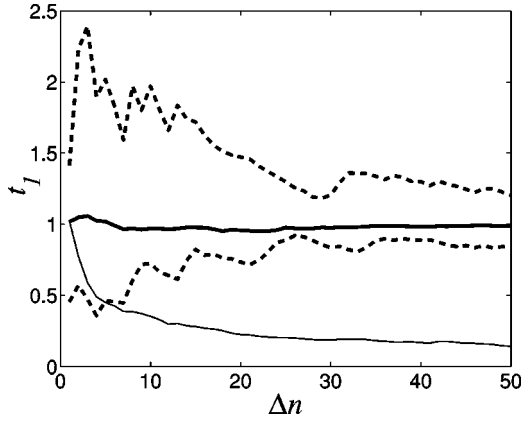

FIG. 2. The two dashed lines show t_1 as a function of Δn [Eq. (4)] for two random unitary matrices drawn from the ensemble $\beta=2$. The heavy full line is the value of t_1 averaged over 50 such random matrices, while the light line shows its variance, which drops as $1/\sqrt{\Delta n}$ as expected.

matrices from the $\beta=2$ ensemble—the set of unitary matrices with no symmetries. This is illustrated in Fig. 2, where the matrices are of size 600×600. For each random matrix $U^{(k)}$ drawn from this ensemble, we can compute $t_1(U^{(k)})$ as functions of Δn. Two such curves (dashed) are plotted on Fig. 2. By applying this procedure to many samples (here 50), we can estimate the average of t_1 and its fluctuations. We have computed

$$\langle t_1\rangle=\frac{1}{50}\sum_{k=1}^{50} t_1(U^{(k)}),\quad \langle (t_1)^2\rangle=\frac{1}{50}\sum_{k=1}^{50}[t_1(U^{(k)})]^2; \tag{5}$$

the average $\langle t_1\rangle$ and mean deviation $\sigma=\sqrt{\langle (t_1)^2\rangle-\langle t_1\rangle^2}$ are also plotted in Fig. 2 (heavy and light full lines, respectively): as expected, t_1 converges to 1 as $1/\sqrt{\Delta n}$. The same procedure can be applied to t_0; nevertheless, since t_1 does converge to 1 in this ensemble, t_0 obviously does not since it differs by a factor of roughly $N/\Delta n\simeq20$ for the range of Δn we have studied. Of course, this difference would vanish when Δn approaches N, since the form factor of any universal ensemble converge to those of the Poisson ensemble (see Sec. II); this is why we must restrict our study to $\Delta n\ll N$. The same conclusions can be reached for the other ensembles characterizing chaotic systems, i.e., $\beta=1$, 2, and 4.

Similarly, had the matrices $U^{(k)}$ been drawn from the $\beta=0$ ensemble—the set of matrices characterizing regular systems—we would have observed t_0 converging to 1 as $1/\sqrt{\Delta n}$, while t_1, smaller by a factor of roughly $\Delta n/N$, would roughly vanish. From these considerations, the hypothesis test "t_0 converges to 1" versus "t_1 converges to 1" allows us to discriminate between random matrices drawn from $\beta=0$ and those drawn from one of the $\beta=1$, 2, or 3, with a probability of error decreasing as $1/\sqrt{\Delta n}$. Thus, as long as the random matrix conjecture holds, it should also allow one to discriminate between regular and chaotic motion.

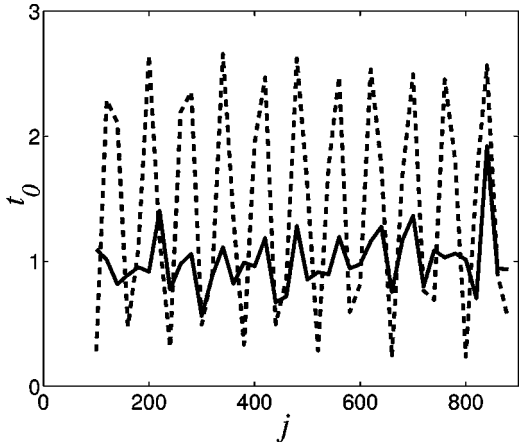

FIG. 3. Value of t_0 [Eq. (4)] of the kicked top in a regular regime $\mathbf{p}_r=(0,0,1,0,0,10)$ as in Ref. [6] for different values of j. Dashed curve: $\Delta n=1$ so it is simply $\mathrm{Tr}\{\hat{F}\}/N$. Full curve: To decrease the fluctuation, we have used ergodic averaging over the first $\Delta n=30$ normalized form factors $\mathrm{Tr}\{\hat{F}^n\}/N$, $n=1,2,\ldots,30$.

B. Kicked top

We now focus our attention on a physical model of great interest for its good agreement with random matrix theory: the nonlinear kicked top. We write the Floquet operator in its most general form following Haake [6], $\hat{F}=U_zU_yU_x$ with

$$U_k=\exp\left\{-i\frac{\tau_kJ_k^2}{2j+1}-i\alpha_kJ_k\right\}, \tag{6}$$

where J_k, $k=x$, y, and z, are the canonical angular-momentum operators. We conveniently define a parameter vector $\mathbf{p}=(\alpha_x,\alpha_y,\alpha_z,\tau_x,\tau_y,\tau_z)$. Some authors use a restricted form of this Floquet operator where only τ_z and α_y are nonzero. Since $[\hat{F},\mathbf{J}^2]=0$, the value of the angular momentum j—which appears in Eq. (6)—is conserved. The dimension of the Hilbert space is simply given by $N=2j+1$.

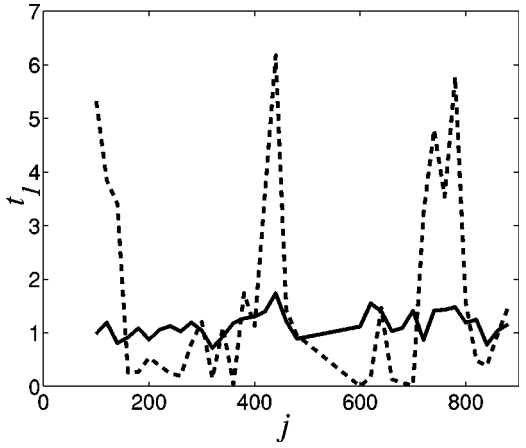

FIG. 4. Value of t_1 [Eq. (4)] of the kicked top in a chaotic regime $\mathbf{p}_c=(1.1,1,1,4,0,10)$ as in Ref. [6] for different values of j. Dashed curve: $\Delta n=1$ so it is simply $\mathrm{Tr}\{\hat{F}\}$. Full curve: To decrease the fluctuation, we have used ergodic averaging over the first $\Delta n=30$ normalized form factors $\mathrm{Tr}\{\hat{F}^n\}/n$, $n=1,2,\ldots,30$.

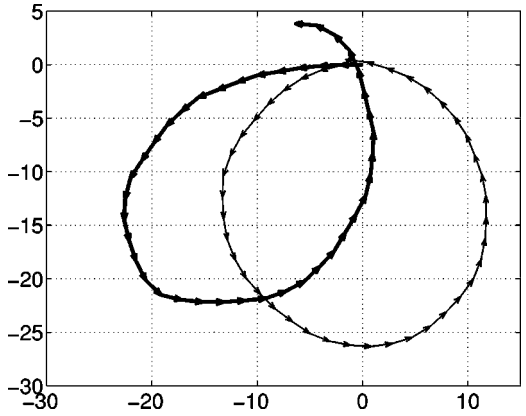

FIG. 5. Vectorial representation of eigenphases: $\Sigma_j(\cos\phi_j, \sin\phi_j)$, where the ϕ_j have been ordered in an increasing order. The α and τ parameters of the Floquet operator [Eq. (6)] are tuned so the system is in a regular regime (heavy vectors) and a chaotic regime (light vectors) as in Figs. 3 and 4. The value of j is 20 so each curve contains 41 vectors.

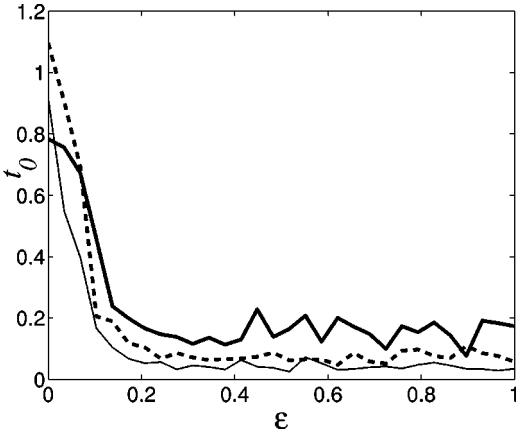

FIG. 6. Value of t_0 [Eq. (4)] with $\Delta n = 30$ for different system size: Full heavy line, $j = 50$; dashed line, $j = 100$; and light full line, $j = 200$.

By adequately choosing the parameters **p**, the kicked top can be either in a regular or in a chaotic regime; see Ref. [6] for more details. Thus, we can evaluate t_0 and t_1 of Eq. (4) in both regimes and verify that they indeed allow one to discriminate between them. This is presented in Figs. 3 and 4 for different values of the total angular momentum j. In Fig. 3, the system is in a regular regime; we have only plotted t_0 since t_1 is larger by a factor proportional to j so clearly does not converge to 1. Similarly, only the value of t_1 is exhibited in Fig. 4. Notice that while ergodic averaging decreases the fluctuations, it is not essential to discriminate between regular and chaotic regimes. Indeed, the scale of fluctuation is extremely small compared to j, which is the factor by which t_0 and t_1 differ.

The analogy with a random walk in the plane can also be illustrated graphically. In Fig. 5 we have plotted the sum of the eigenvalues vectorially. The apparent structure of the vectors is purely artificial, the eigenphases were ordered in an increasing order (the sum of vectors is obviously a commutative operation); we have chosen this ordering to facilitate the presentation.

The effect of LSD are striking in Fig. 5. The light vectors (chaotic regime) are arranged in an almost perfect circle; eigenphases tend to be equally separated. On the other hand, the heavy vectors (regular regime) are quite often aligned in an almost straight line; a manifestation of level clustering. As a consequence, the heavy vectors end up further apart from the origin than do the light vectors; on an average, these distances differ by a factor $\sqrt{N}$.

Finally, we can use the form factor to study the transition between regular and chaotic motions. To do so, we let the parameter vector continuously vary from its regular value to its chaotic value: $\mathbf{p} = (1-\epsilon)\mathbf{p}_r + \epsilon\,\mathbf{p}_c$ (see captions of Figs. 3 and 4). For $\epsilon = 0$, the expected value of t_0 is 1. As ϵ increases, the system enters a chaotic regime; when chaos has fully developed, t_0 should vanish as $1/N$. This is indeed observed in Fig. 6, where we have plotted t_0 as a function of ϵ for different system sizes. Moreover, the results indicate that the transition to chaos becomes more sensible as the size of the system increases.

V. CONCLUSION

We have shown that, using a single bit of quantum information, we can test whether the spectrum of a unitary matrix obeys a Poisson or a polynomial law. Under the random matrix conjecture, this can be used to determine whether the system has a regular or chaotic behavior in its classical limit. The idea relies on estimating the averaged form factor using the ergodic theorem which roughly states that a time average can reproduce an ensemble average. The form factors in a regular and chaotic regimes differ by a factor of $\sqrt{N}$ and the output signal of our computation decreases as $1/N$: the required physical resources thus scale as N. This is a quadratic improvement over all known classical algorithms. We are presently investigating a different signature of quantum chaos which might not suffer from this signal loss, and hence, could offer an exponential speedup.

This result provides an insight into the nature of the potential computational speedup offered by quantum mechanics. In particular, it provides a strong argument towards the computational power of mixed state quantum computing.

ACKNOWLEDGMENTS

We thank Harold Ollivier for stimulating discussions and careful reading of this manuscript and Howard Wiseman for pointing out an error in an earlier version of this work. D.P. was financially supported by Canada's NSERC and R.L. by NSERC and CIAR. This work was partially funded by NSA.

[1] M.A. Nielsen and I.L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
[2] R.P. Feynman, Int. J. Theor. Phys. **21**, 467 (1982).
[3] S. Lloyd, Science **273**, 1073 (1996).
[4] G. Ortiz, J.E. Gubernatis, E. Knill, and R. Laflamme, Phys. Rev. A **64**, 22 319 (2001).
[5] R. Somma, G. Ortiz, J.E. Gubernatis, E. Knill, and R. Laflamme, Phys. Rev. A **65**, 42 323 (2002).
[6] F. Haake, *Quantum Signatures of Chaos* (Springer-Verlag, Berlin, 2001).
[7] H.-J. Stöckmann, *Quantum Chaos an Introduction* (Cambridge University Press, Cambridge, 1999).
[8] R. Schack, Phys. Rev. A **57**, 1634 (1998).
[9] B. Georgeot and D.L. Shepelyansky, Phys. Rev. Lett. **86**, 2890 (2001).
[10] G. Benenti, G. Casati, S. Montangero, and D.L. Shepelyansky, Phys. Rev. Lett. **87**, 227901 (2001).
[11] J. Emerson, Y.S. Weinstein, S. Lloyd, and D.G. Cory, Phys. Rev. Lett. **89**, 284102 (2002).
[12] E. Knill and R. Laflamme, Phys. Rev. Lett. **81**, 5672 (1998).
[13] D.G. Cory *et al.*, Fortschr. Phys. **48**, 875 (2000).
[14] M.V. Berry and M. Tabor, Proc. R. Soc. London, Ser. A **356**, 375 (1977).
[15] C. Miquel, J.P. Paz, M. Saraceno, E. Knill, R. Laflamme, and C. Negrevergne, Nature (London) **418**, 59 (2002).
[16] A. Barenco, C.H. Bennett, R. Cleve, D.P. DiVincenzo, N. Margolus, P.W. Shor, T. Sleator, J.A. Smolin, and H. Weinfurter, Phys. Rev. A **52**, 3457 (1995).
[17] It is important to note that Δn need not increase with N; in fact, it is quite the opposite. The probability of error scales like the overlap of two Gaussian distributions of width $\sigma = 1/\Delta n$ and centered about points μ_1 and $\mu_2 \simeq N\mu_1$: clearly, this overlap decreases with N.