Exponential Speedup with a Single Bit of Quantum Information: Measuring the Average Fidelity Decay

David Poulin,[1] Robin Blume-Kohout,[2] Raymond Laflamme,[1] and Harold Ollivier[3]
[1]*Institute for Quantum Computing, University of Waterloo, Ontario, Canada N2L 3G1 and Perimeter Institute for Theoretical Physics, 35 King Street N., Waterloo, Ontario, Canada N2J 2W9*
[2]*Theoretical Division, LANL, MS-B213, Los Alamos, New Mexico 87545, USA*
[3]*INRIA - Projet Codes, BP 105, F-78153 Le Chesnay, France*
(Received 6 October 2003; published 30 April 2004)

We present an efficient quantum algorithm to measure the average fidelity decay of a quantum map under perturbation using a single bit of quantum information. Our algorithm scales only as the complexity of the map under investigation. Thus for those maps admitting an efficient gate decomposition, it provides an exponential speedup over known classical procedures. Fidelity decay is important in the study of complex dynamical systems, where it is conjectured to be a signature of eigenvector statistics. Our result also illustrates the role of chaos in the process of decoherence.

DOI: 10.1103/PhysRevLett.92.177906 PACS numbers: 03.67.Lx, 03.65.Yz, 05.45.Mt

A physical experiment consists of evolving a system from its initial state and performing a measurement. It is by now well appreciated that quantum computers can be used to simulate the evolution of certain quantum systems efficiently [1]. The time evolution operator $U(t', t)$ of a N-dimensional quantum system can always be approximated by a product of elementary "gates" of a $K \approx \log_2 N$ -qubit quantum computer. Moreover, for a wide class of Hamiltonians, the number of gates L required in this decomposition grows only *polynomially* with K and $|t' - t|$: such a simulation is called *efficient*. This is in contrast with classical simulations which typically require computation time growing as the dimension of the Hilbert space of the system, i.e., *exponentially* with K. However, evolution is only one ingredient of a physical experiment. A quantum simulation should also incorporate state initialization and readout, which are generally nontrivial, e.g., there are indications that preparing the ground state of a generic Hamiltonian requires an exponential number of gates [2]. In this Letter, we present a quantum circuit to evaluate a dynamical quantity—namely the average fidelity decay—which circumvents the need to prepare a complex initial state, requires a very simple measurement, and uses a single bit of quantum information.

Fidelity decay (FD) was initially proposed as a signature of quantum chaos by Peres [3] and has since been extensively investigated [4,5]. It measures the rate at which identical initial states diverge when subjected to slightly different dynamics. The discrete time evolution of a closed quantum system can be specified by a unitary operator U, where $\rho(\tau_n) = U^n \rho_0 (U^\dagger)^n$. To examine FD, we construct a slightly perturbed map U_p, where $U_p = UP$ with $P = \exp\{-i\delta V\}$ for some small δ and a Hermitian matrix V. It is conjectured that the overlap (or fidelity)

$$F_n(\psi) = |\langle\psi|(U^n)^\dagger U_p^n|\psi\rangle|^2 \tag{1}$$

between initially identical states ψ undergoing slightly different *evolutions*, U and U_p, should decay differently (as a function of the discrete time n) for regular and chaotic dynamics [3]. While the behavior of these decay rates is not fully understood, some of its general features are now widely accepted. In particular, chaotic maps exhibit a universal response to perturbations: the decay rate is governed *only* by the strength $|V^2|\delta^2$ of the perturbation. This is because FD is an indicator of the relative randomness of the perturbation V in the eigenbasis of the quantum map U [6]. On the other hand, the decay rate of the regular system depends on the details of V, so, in particular, it can be much slower under simple perturbations. Hence, FD provides a powerful diagnostic of chaotic behavior, but calculating it is computationally hard classically. Furthermore, because $F_n(\psi)$ generally shows large fluctuations over time, it is in practice necessary to average $F_n(\psi)$ over a random set of initial states ψ to determine its decay rate, thus increasing the numerical burden.

Since fully controllable and scalable quantum computers are still quite a ways in the future, algorithms which can be performed on a less-ambitious quantum information processor (QIP) are of great interest. A QIP is a quantum device which may fail to satisfy one or more of DiVincenzo's five criteria, but can nonetheless carry out interesting computations [7]. Of particular interest to us is deterministic quantum computation with a single bit (DQC1) [8], a model of quantum information processing which is believed to be less powerful than universal quantum computation and which is naturally implemented by a high-temperature NMR QIP [9]. In this model, universal control over all qubits is still assumed, but state preparation and readout are limited. The initial state of the $(K + 1)$-qubit register is

$$\left(\frac{1-\gamma}{2}\mathbb{1} + \gamma|0\rangle\langle 0|\right) \otimes \frac{\mathbb{1}}{2^K}, \tag{2}$$

i.e., the first qubit (called the probe qubit for reasons which will become clear) is in a pseudopure state, whereas the other K qubits are in the maximally mixed state. Furthermore, the result of the computation is obtained as the noisy expectation value of σ_z on the probe qubit. The variance of σ_z is determined by (i) the polarization γ of Eq. (2) and (ii) the "inherent noise" of the measuring process. The value of γ in high-temperature NMR is independent of the size of the register because only a single qubit needs to be in a pseudopure state. The inherent noise receives contribution from both electronic noise and statistical fluctuations due to the finite sample size. Hence, $\langle\sigma_z\rangle$ can be estimated to within arbitrary ϵ with a probability of error at most p by repeating the computation $O[\log(1/p)/\epsilon^2]$ times [10].

Efficient gate decompositions for some quantized chaotic systems have been known for some time [11] and have recently been incorporated into efficient quantum simulations [6,12,13]. In Ref. [12], an efficient quantum circuit is constructed to evaluate the coarse-grained local density of states — the average profile of the eigenstates of U over the eigenbasis of U_p — which is believed to be a valid indicator of chaos and is formally related to FD via Fourier transform [5]. In Ref. [6], an efficient procedure to estimate the FD using the standard model of quantum computation is presented. Finally, in Ref. [13], a DQC1 circuit is presented to estimate the form factors $t_n = |\mathrm{Tr}\{U^n\}|^2$ of a unitary map U which, under the random matrix conjecture (see [14] and references therein), is a good signature of quantum chaos. The proposed algorithm offers only a quadratic speedup, but since entanglement is very limited in DQC1 [15], this result raises doubt about the common belief that massive entanglement is responsible for quantum-computational speedup [16].

Drawing upon this previous work, we will now construct an efficient DQC1 algorithm to evaluate the average FD associated with any pair of unitary operators U and U_p, provided they can be implemented efficiently, e.g., as those of Ref. [11]. We begin by proving a crucial identity required to implement the efficient algorithm.

Let $f(\psi)$ be a complex-valued function on the space of pure states of a N-dimensional quantum system. We denote its average by $\overline{f(\psi)} = \int f(\psi)d\psi$, where $d\psi$ is the uniform measure induced by the Haar measure, such that $\int d\psi = 1$. For sake of compactness let $\langle\psi|A|\psi\rangle = \langle A\rangle_\psi$.

Theorem: Let $A, B, C, \ldots$ be ℓ linear operators on a N-dimensional Hilbert space. Then

$$\overline{\langle A\rangle_\psi\langle B\rangle_\psi\langle C\rangle_\psi\cdots} = \frac{\mathrm{Tr}\{(A\otimes B\otimes C\cdots)P_S^{(\ell)}\}}{\binom{N+\ell-1}{\ell}}, \quad (3)$$

where $P_S^{(\ell)}$ is the projector on the symmetric subspace of ℓ systems; see Ref. [17] for details on $P_S^{(\ell)}$.

Proof: First, note that

$$\langle A\rangle_\psi\langle B\rangle_\psi\langle C\rangle_\psi\cdots = \mathrm{Tr}\{|\psi\rangle\langle\psi|^{\otimes\ell}(A\otimes B\otimes C\cdots)\}.$$

Therefore, the average over the pure states ψ yields

$$\mathrm{Tr}\{\overline{|\psi\rangle\langle\psi|^{\otimes\ell}}(A\otimes B\otimes C\cdots)\}.$$

Since $\overline{|\psi\rangle\langle\psi|^{\otimes\ell}}$ annihilates any state which is antisymmetric under the interchange of two of the ℓ systems, and is by construction symmetric under such interchange, it must be proportional to the projector $P_S^{(\ell)}$ onto the symmetric subspace. To establish the theorem it is sufficient to find the proportionality factor λ between these two quantities. Letting $A = B = C = \cdots = \mathbb{1}$, we get $1 = \mathrm{Tr}\{\overline{|\psi\rangle\langle\psi|^{\otimes\ell}}\} = \lambda\mathrm{Tr}\{P_S^{(\ell)}\} = \lambda\binom{N+\ell-1}{\ell}$ (see Ref. [17]), which completes the proof. □

A useful corollary to this theorem for any specific ℓ can be obtained by expanding $P_S^{(\ell)}$ in Eq. (3). In the case $\ell = 2$, it reads

$$\begin{aligned}\overline{\langle A\rangle_\psi\langle B\rangle_\psi} &= \sum_{ijmn}\frac{2A_{ij}B_{mn}(P_S^{(2)})_{ji,nm}}{N^2+N}\\ &= \sum_{ijmn}\frac{A_{ij}B_{mn}(\delta_{ij}\delta_{mn}+\delta_{in}\delta_{mj})}{N^2+N}\\ &= \frac{\mathrm{Tr}\{A\}\mathrm{Tr}\{B\}+\mathrm{Tr}\{AB\}}{N^2+N}. \end{aligned}\quad (4)$$

Similar expressions can be derived for $\ell > 2$, which involves the properly normalized sum of all combinations of traces of products and products of traces.

To arrive at our algorithm, it is sufficient to write the average fidelity as $\overline{F_n(\psi)} = \overline{\langle(U^n)^\dagger U_p^n\rangle_\psi\langle(U_p^n)^\dagger U^n\rangle_\psi}$ and apply the identity from Eq. (4) to obtain

$$\overline{F_n(\psi)} = \frac{|\mathrm{Tr}\{(U^n)^\dagger U_p^n\}|^2+N}{N^2+N}. \quad (5)$$

The specific form of our theorem with $\ell = 2$, unitary A, and $B = A^\dagger$ has been used previously [18,24,25], but our proof simplifies the presentation. An efficient DQC1 algorithm to evaluate the trace of any unitary operator [here, $(U^n)^\dagger U_p^n$], provided that it admits an efficient gate decomposition, was presented in Ref. [19]. If the perturbed map takes the form $U_p = UP$ for some

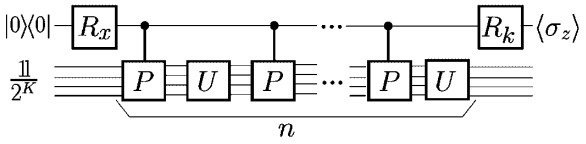

FIG. 1. Quantum circuit evaluating the average fidelity $\overline{F_n(\psi)}$ between the perturbed and unperturbed maps U and $U_p = UP$. The gates R_k are $\pi/2$ rotation in the Bloch sphere around axis $k = x$ or y. When k is set to x, we get the real part of $\mathrm{Tr}\{(U^n)^\dagger U_p^n\}/N$ while $k = y$ yields the imaginary part. The unitary operator P is applied conditionally: when the probe qubit is in state $|1\rangle$, the unitary P is applied to the lower register while no transformation is performed when the state of the probe qubit is $|0\rangle$.

unitary operator P (e.g., $P = \exp\{-i\delta V\}$ as above), the circuit can be further simplified into the one illustrated in Fig. 1.

We now analyze the complexity of our algorithm. We assume that U and U_p admit ϵ-accurate gate decompositions whose sizes grow as $L(K, \epsilon) \in \mathrm{poly}(K, 1/\epsilon)$. This implies that the controlled version of these gates also scales as $L(K, \epsilon)$ [20]. We see from Eq. (5) that the variance of $\overline{F_n(\psi)}$ is at most twice the variance of $\mathrm{Tr}\{(U^n)^\dagger U_p^n\}/N$. Therefore, the overall algorithm — estimating $\overline{F_n(\psi)}$ to within ϵ, with error probability at most p — requires resources growing as $L(K, \epsilon)n \times \log(1/p)/\epsilon^2$, so it is efficient. (The range in n over which the decay is studied should be independent of the system's size.) This algorithm thus provides an *exponential* speedup over all known classical procedures and uses a *single* bit of quantum information. Furthermore, it eliminates any cost of averaging the fidelity over a random set of initial states, as this averaging is done directly.

In order to implement certain unitary maps on K qubits efficiently, it is necessary to introduce a number K_a of ancillary qubits (a "quantum work pad") in the fiducial state $|\psi_0\rangle$. Ancillary qubits in pseudopure states can be used in the DQC1 setting. As a first step of the computation, part of the polarization of the probe qubit of Eq. (2) can be transferred to ancillas initially in maximally mixed states. Thus, as long as the size K_a of the work pad is at most polylogarithmic in K, the algorithm remains efficient.

Perhaps the most surprising feature of the quantum algorithm as it is presented in Fig. 1 is that the probe never gets entangled with the system throughout the computation. To show this, consider a generalized version of the circuit of Fig. 1 where the P's and the U's are free to differ at each iteration, i.e., at step j, we apply P_j conditionally on the probe qubit, followed by U_j. This generalization is necessary since the controlled P gate will in general be decomposed as a sequence of elementary controlled and regular gates [20]. Initially, the probe qubit is in state $\alpha|0\rangle + \beta|1\rangle$. After k steps, the state of the QIP is

$$\rho_k = \frac{1}{N}\{|\alpha|^2|0\rangle\langle 0| \otimes \mathbb{1} + \alpha\beta^*|0\rangle\langle 1| \otimes S^\dagger + \alpha^*\beta|1\rangle\langle 0| \otimes S + |\beta|^2|1\rangle\langle 1| \otimes \mathbb{1}\}, \quad (6)$$

where $S = U_k P_k \cdots U_2 P_2 U_1 P_1 U_1^\dagger U_2^\dagger \cdots U_k^\dagger$. Decomposing this state in the eigenbasis of the unitary matrix $S|\phi_j\rangle = e^{is_j}|\phi_j\rangle$, we get

$$\rho_k = \frac{1}{N}\sum_j |\alpha_j\rangle\langle\alpha_j| \otimes |\phi_j\rangle\langle\phi_j|, \quad (7)$$

where $|\alpha_j\rangle = \alpha|0\rangle + \beta e^{is_j}|1\rangle$; the state is separable. Its separability supports the point of view that the power of quantum computing derives not from the special features of *quantum states* — such as entanglement — but rather from fundamentally *quantum operations* [21].

Our algorithm also illustrates the relation between the decoherence rate and the dynamical properties of the environment [22]. Consider the probe qubit of Fig. 1 as a quantum system interacting with a complex environment consisting of K two-level systems. After a "time" n, the state of the system is given by tracing out the K environmental qubits from Eq. (6). The diagonal elements of the reduced density matrix $|\alpha|^2$ and $|\beta|^2$ are left intact while the off-diagonal elements $\alpha\beta^*$ and $\alpha^*\beta$ are decreased by a factor $|\mathrm{Tr}\{S\}|$ which is roughly equal to $\sqrt{\overline{F_n(\psi)}}$. Thus, in the presence of a chaotic environment, the system will unavoidably decohere at a rate governed solely by the strength of the coupling. On the other hand, given a simple coupling to a regular environment, the system can maintain its coherence over a long period of time. This analogy also provides a very simple example of decoherence without entanglement [23].

On the circuit of Fig. 1, only the perturbation gates P are conditioned on the state of the probe qubit. This suggests a dual interpretation of the algorithm as quantum circuit and quantum probe. On the one hand, U could be a known unitary transformation which is being simulated on the lower K-qubit register over which we have universal control. Then, the gate U would simply be decomposed as a sequence of elementary gates as prescribed in Ref. [11] for example. On the other hand, the lower register could be a real quantum system undergoing its natural evolution U which might not even be known. Then, the probe qubit should really be regarded as a probe which is initialized in a quantum superposition, used to conditionally *kick* the system, and finally measured to extract information about the system under study. In this case, it is not necessary to have universal control over the lower register (the quantum system); we must simply be able to apply a conditional small unitary transformation to it.

Finally, Eq. (5) provides a useful numerical tool that can be used to compute the *exact* average fidelity instead of estimating it by averaging over a finite random sample of initial states. In Ref. [6], FD was illustrated on the quantum kicked top map $U_{\mathrm{QKT}} = \exp\{-i\pi J_y/2\} \times \exp\{-ikJ_z^2/j\}$ acting on the $N = 2j + 1$ dimensional Hilbert space of angular momentum operator $\vec{J}$. The chosen perturbation operator was $P = \prod_{j=1}^K \times \exp\{-i\delta\sigma_z^j/2\}$, a collective rotation of all K qubits of the QIP by an angle δ. The decay rate (governed by the Fermi golden rule in this regime) is $|V^2|\delta^2 = 2.50\delta^2$ for this perturbation [6]. $\overline{F_n(\psi)}$ was estimated in both chaotic ($k = 12$) and regular ($k = 1$) regimes of the kicked top by averaging over 50 initial states. We reproduce these results in Fig. 2 and compare them with the exact average Eq. (5) and theoretical prediction $e^{-|V^2|\delta^2 n}$. The random sample is in good agreement

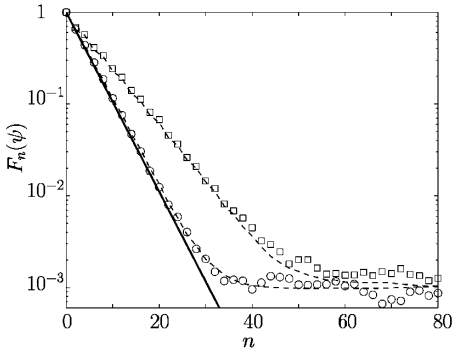

FIG. 2. Fidelity decay $F_n(\psi)$ averaged over 50 initial computational basis states for U_{QKT} in a regular regime ($k = 1$, squares) and chaotic regime ($k = 12$, circles). The dashed lines represent the exact average Eq. (5) and the full line shows the exponential decay at the Fermi golden rule rate $|V^2|\delta^2$.

with the exact average except that the former shows fluctuations. Furthermore, the decay in the chaotic regime is in excellent agreement with the Fermi golden rule, while in the regular regime it is considerably slower.

We have presented an efficient quantum algorithm which computes the average FD of a quantum map under perturbation using a single bit of quantum information. The quantum circuit for this algorithm establishes a link between decoherence by a chaotic environment and FD. Using a special case of our theorem, we numerically evaluated the exact average FD for the quantum kicked top and found good agreement with previous estimations using random samples. Although we have mainly motivated our algorithm for the study of quantum chaos, we believe that it has many other applications such as characterizing noisy quantum channels and computing correlation functions for many-body systems. We have also shown that our algorithm can be viewed as a special experiment where a quantum probe is initialized in a superposition and used to conditionally kick the system under study. This type of *quantum information science by-product* might open the horizon to new types of experimental measurements where a small QIP is used to extract information from the quantum system under study. Finally, the effective speedup despite the limited presence of entanglement — in particular the complete absence of entanglement between the quantum probe and the mixed register — is a step forward in our understanding of quantum-computational speedup.

We thank J. Emerson, G. Milburn, J. P. Paz, and W. H. Zurek for helpful discussions. We also acknowledge the Benasque Center for Science where this work was initiated. This work was supported in part by NSERC, ARDA, CIAR, ACI sécurité informatique, and by the Department of Energy, under Contract No. W-7405-ENG-36.

[1] S. Lloyd, Science **273**, 1073 (1996); C. Zalka, Proc. R. Soc. London, Ser. A **454**, 313 (1998).
[2] W. van Dam, M. Mosca, and U. Vazirani, in *Proceedings of the 42nd Annual Symposium on the Foundations of Computer Science* (IEEE, New York, 2001), p. 279.
[3] A. Peres, Phys. Rev. A **30**, 1610 (1984).
[4] R. A. Jalabert and H. M. Pastawski, Phys. Rev. Lett. **86**, 2490 (2001); F. Cucchietti, C. H. Lewenkopf, E. R. Mucciolo, H. Pastawski, and R. O. Vallejos, arXiv: nlin.CD/0111051, 2001; G. Benenti and G. Casati, quant-ph/0112060; T. Prosen and M. Znidaric, J. Phys. A **35**, 1455 (2002).
[5] P. Jacquod, P. G. Silvestrov, and C. W. J. Beenakker, Phys. Rev. E **64**, 55203 (2001).
[6] J. Emerson, Y. S. Weinstein, S. Lloyd, and D. G. Cory, Phys. Rev. Lett. **89**, 284102 (2002).
[7] R. Blume-Kohout, C. M. Caves, and I. H. Deutsch, Found. Phys. **32**, 1641 (2002)
[8] E. Knill and R. Laflamme, Phys. Rev. Lett. **81**, 5672 (1998).
[9] D. G. Cory *et al.*, Fortschr. Phys. **48**, 875 (2000).
[10] P. J. Huber, *Robust Statistics* (Wiley, New York, 1981).
[11] R. Schack, Phys. Rev. A **57**, 1634 (1998); B. Georgeot and D. L. Shepelyansky, Phys. Rev. Lett. **86**, 2890 (2001); G. Benenti, G. Casati, S. Montangero, and D. L. Shepelyansky, Phys. Rev. Lett. **87**, 227901 (2001).
[12] J. Emerson, S. Lloyd, D. Poulin, and D. Cory, quant-ph/0308164.
[13] D. Poulin, R. Laflamme, G. J. Milburn, and J. P. Paz, Phys. Rev. A **68**, 022302 (2003).
[14] F. Haake, *Quantum Signatures of Chaos* (Springer-Verlag, Berlin, 2001).
[15] K. Zyczkowski, P. Horodecki, A. Sanpera, and M. Lewenstein, Phys. Rev. A **58**, 883 (1998); S. L. Braunstein, C. M. Caves, R. Jozsa, N. Linden, S. Popescu, and R. Schack, Phys. Rev. Lett. **83**, 1054 (1999).
[16] A. Ekert and R. Jozsa, Philos. Trans. R. Soc. London, Ser. A **356**, 1769 (1998); R. Jozsa, in *The Geometric Universe*, edited by S. Huggett, L. Mason, K. P. Tod, S. T. Tsou, and N. Woodhouse (Oxford University Press, New York, 1998).
[17] A. Barenco, A. Berthiaume, D. Deutsch, A. Ekert, R. Jozsa, and C. Macchiavello, SIAM J. Comput. **26**, 1541 (1997).
[18] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. A **60**, 1888 (1999).
[19] C. Miquel, J. P. Paz, M. Saraceno, E. Knill, R. Laflamme, and C. Negrevergne, Nature (London) **418**, 59 (2002).
[20] 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).
[21] R. Schack and C. M. Caves, Phys. Rev. A **60**, 4354 (1999); R. Laflamme, D. G. Cory, C. Negrevergne, and L. Viola, Quant. Info. Comp. **2**, 166 (2001); D. Poulin, Phys. Rev. A **65**, 042319 (2002).
[22] R. Blume-Kohout and W. H. Zurek, quant-ph/0212153.
[23] J. Eisert and M. B. Plenio, Phys. Rev. Lett. **89**, 137902 (2002).
[24] H. Barnum, quant-ph/0205155.
[25] A. Ashikmin, A. Barg, E. Knill, and S. Litsyn, IEEE Trans. Inf. Theory, **46**, 778 (2000).