Science
AAAS

Pseudo-Random Unitary Operators for Quantum Information Processing

Joseph Emerson, *et al.*

Science **302**, 2098 (2003);
DOI: 10.1126/science.1090790

Pseudo-Random Unitary Operators for Quantum Information Processing

Joseph Emerson,[1]*†‡ Yaakov S. Weinstein,[1]*
Marcos Saraceno,[3] Seth Lloyd,[2]
David G. Cory[1]

In close analogy to the fundamental role of random numbers in classical information theory, random operators are a basic component of quantum information theory. Unfortunately, the implementation of random unitary operators on a quantum processor is exponentially hard. Here we introduce a method for generating pseudo-random unitary operators that can reproduce those statistical properties of random unitary operators most relevant to quantum information tasks. This method requires exponentially fewer resources, and hence enables the practical application of random unitary operators in quantum communication and information processing protocols. Using a nuclear magnetic resonance quantum processor, we were able to realize pseudo-random unitary operators that reproduce the expected random distribution of matrix elements.

Random numbers are a fundamental component of classical information theory, with practical applications including stochastic estimation, system identification, and cryptographic protocols. For example, in the important case of Monte Carlo simulation, sequences of random numbers permit an unbiased statistical estimation of quantities that are impractical to evaluate by exact methods. It is now clear that quantum theory provides a more general framework for information theory, one that offers important advantages over classical methods of computation and communication [for an introduction, see (*1*)]. In the quantum information paradigm, the basic elements are quantum state vectors [describing the possible states of the quantum bits (qubits)] and unitary operators (describing the desired transformations); information is encoded in a quantum state, and the computational algorithm, or communication protocol, is implemented via a sequence of unitary operators acting on that quantum state.

Quantum analogs of random numbers (i.e., random unitary operators and random quantum states) provide an equally useful and fundamental component to this emerging theory of quantum information. In the case of quantum communication, random quantum states are known to saturate the classical communication capacity of a noisy quantum channel (*2*). Moreover, sets of randomizing unitary operators enable the superdense coding of arbitrary quantum states (*3*) and lead to a decrease in the classical communication cost (in bits) for remote state preparation (*4*). Random unitary operators also allow the construction of more efficient data-hiding schemes and provide a means to reduce the key length required for the (approximate) encryption of quantum states (*5*). In the case of quantum processing, random unitary operators enable methods for characterizing the coherent control over large quantum devices serving as prototype quantum computers.

Identification of the dominant noise sources for a quantum device is an essential first step toward the realization of fault-tolerant quantum computation on that device. Unfortunately, a complete characterization of the noise via process tomography cannot be carried out for a large quantum processor because the number of experiments (and the amount of data) grows exponentially with the number of qubits (*6*). Moreover, the distribution and strength of these noise operators will generally depend on the target transformation. However, when the target transformation is a random unitary operator, key measurable signatures of noise and decoherence—such as the rate of fidelity decay (*7*) and the rate of purity loss (*8*)—become independent of the target transformation and depend only on the intrinsic properties of the noise (*9–11*). As a result, the implementation of random unitary operators on a quantum processor enables stochastic methods for estimating unwanted noise sources on prototype quantum processors.

Random unitary operators and quantum states must be defined with respect to a relevant measure. For the set of unitary transformations acting on states of n_q qubits (complex vectors with dimension $N = 2^{n_q}$), the appropriate measure is the Haar measure on the group $U(N)$. This is the unique measure that remains invariant under arbitrary unitary transformations. The random ensemble of $N \times N$ unitary matrices drawn uniformly from this measure is known as the circular unitary ensemble (CUE) (*12*). Because each (pure) quantum state can be obtained by applying a unitary operator to some fixed fiducial state, the Haar measure also defines a natural measure for random quantum states.

The applications noted above motivate the usefulness of implementing uniformly distributed random unitary operators on a quantum processor. However, any circuit implementing an exact parameterization of the CUE will require exponential resources. A unitary operator drawn from the Haar measure on $U(N)$ is conveniently parameterized via the Hurwitz decomposition [see (*13*)]. This decomposition can be reexpressed as a quantum circuit requiring on the order of $n_q^2 2^{2n_q}$ elementary (1- and 2-qubit) gates and 2^{2n_q} independent random "input" parameters. So this direct approach requires both quantum and classical resources that grow exponentially with the number of qubits.

The exponential resources required for an exact circuit motivate the question of whether it is possible to construct an efficient circuit generating pseudo-random unitary operators that share some of the "coarse" statistical features of the Haar measure—in particular, those features that are most relevant to quantum processing applications. A positive answer to this question is indicated from the discovery of efficient gate decompositions for quantum chaos models (*14–16*), which are known to exhibit some of the universal statistical features of the random matrix ensembles (*17, 18*). However, for these quantum chaos models, the correspondence with the random matrix ensembles is limited by the requirement of a fixed classical limit. Indeed, although the number of independent matrix elements of a unitary operator grows as N^2, for these models the number of independent "input" parameters remains constant. As a result, observables of interest, such as the fidelity decay (*7*), entropy growth rate (*19*), and entangling power (*20*), have been shown to exhibit features that reflect the underlying classical structures rather than the universal random matrix predictions. To overcome these biases, it is convenient to discard the requirement of a fixed classical limit and to devise a quantum circuit that fully exploits the resources that are readily available in a universal quantum processor.

We consider a circuit comprising m iterations of a two-step gate acting on n_q

[1]Department of Nuclear Engineering, [2]Department of Mechanical Engineering, Massachusetts Institute of Technology, Cambridge, MA 02139, USA. [3]Unidad de Actividad Fisica, Tandar, Comisión Nacional de Energía Atómica, 1429, Buenos Aires, Argentina.

*These authors contributed equally to this work.
†Present address: Perimeter Institute for Theoretical Physics, 35 King Street N., Waterloo, Ontario N2J 2W9, Canada.
‡To whom correspondence should be addressed. E-mail: jemerson@perimeterinstitute.ca

qubits. The first step consists of rotating each qubit by independent unitary operators drawn from the Haar measure on $U(2)$. This first step requires $3n_q$ independent variables that are drawn randomly at each iteration. The second step consists of simultaneous two-body interactions of the form

$$U = \exp\left[i(\pi/4) \sum_{j=1}^{n_q - 1} \sigma_z^j \otimes \sigma_z^{j+1} \right] \quad (1)$$

where σ_z^j is the usual Pauli operator of the jth qubit, and the coupling angle is fixed at $\pi/4$ to maximize the entanglement produced by the two-body interactions. Because we imagine a simple one-dimensional array of qubits and a spatially local coupling interaction, we have limited our basic gates to include only nearest-neighbor couplings.

Our construction induces a measure over the set of circuits of length m. For finite m, the distribution of unitary operators generated by the random circuit is biased with respect to the uniform (Haar) measure on $U(N)$. In this sense the random circuits generate "pseudo-random" unitary operators. For $m > m_c = O(n_q^3 2^{2n_q})$, this distribution, although biased, does enjoy nonvanishing support over all elements of the group $U(N)$ (*21*). Moreover, we expect that the measure over the composed circuits converges exponentially to the uniform measure with increasing m.

To see this, consider a sequence of successive random circuits of the same length, each of which is drawn from some distribution f. Combining these random circuits gives rise to a distribution described by the group convolution $f * f * f \ldots * f * f$ (*22*). In the case of a finite group, this stochastic process may be expressed as a matrix. Because the basic gate is universal, for a sufficiently large sequence the matrix has only positive entries and hence, by the Frobenius-Perron theorem, has a single nondegenerate eigenvalue (=1) whose eigenvector corresponds to the uniform measure. Consequently, under repeated application of the circuit, the distribution converges exponentially to the uniform measure over the group. To make this argument rigorous in the case of a continuous compact group requires the use of Fourier analysis, in analogy to the usual proof of the central limit theorem. It is worth stressing that this argument indicates that any universal gate set generates the uniform measure asymptotically, no matter how biased the method with which the gates are drawn from the universal set.

We now turn to the question of whether the measure over random circuits with length m growing no faster than polynomially with n_q can mimic a practical subset of statistical features associated with the Haar measure. We are in particular interested in properties of unitary operators and states that are relevant to quantum information tasks, and so we first consider the distribution of entanglement produced by the circuit. Specifically, we consider the entanglement of the states obtained by applying the random circuit to the computational basis states. As a practical measure of entanglement for multipartite systems, we first consider the average bipartite entanglement between each qubit and the rest of the system,

$$Q = 2 - (2/n_q) \sum_{i=1}^{n_q} \mathrm{Tr}[\rho_i^2] \quad (2)$$

(*23, 24*), where ρ_i is the reduced density operator of the ith qubit. One has $0 \leq Q \leq 1$, with $Q = 0$ for completely factorable states and $Q = 1$ for the generalized Bell states. The distribution of Q produced by a set of random circuits, as a function of increasing m, is shown in Fig. 1 for an 8-qubit system. For $m = 40$ the distribution becomes indistinguishable (on the scale of the figure) from the distribution produced by CUE maps. It is useful to note that the exact CUE average,

$$\langle Q \rangle = \frac{(N-2)}{(N+1)} \approx 1 - (3/N) + O(N^{-2}) \quad (3)$$

approaches the maximum value of Q exponentially as a function of n_q. Moreover, the standard deviation decreases exponentially with increasing n_q (*20*). Thus, in the limit of large n_q, almost all random (and pseudo-random) states have $Q \approx \langle Q \rangle \approx Q_{\max}$.

To check the efficiency with which the random circuits can mimic the uniform distribution, we have measured the rate at which the average Q for the random circuits approaches the CUE average. For fixed n_q (inset, Fig. 1), the rate is exponential with increasing m, which is consistent with the Frobenius-Perron argument above. As n_q increases, the exponential rate rapidly approaches a nonvanishing asymptotic rate; this indicates that, at worst, resources growing as a polynomial of n_q are required to converge to the CUE average. The average bipartite entanglement produced by the random circuits for factor spaces of 1, 2, 3, and 4 qubits exhibits the same rate of exponential convergence to the CUE average (fig. S1).

An important elementary feature of random unitary operators is the distribution of the matrix elements. This distribution also plays a key practical role in the approximate randomization of states (*3–5*). Moreover, this is a random matrix feature that one-body quantum chaos models typically fail to exhibit as a result of the constraints on the matrix elements imposed by the requirement of a fixed classical limit. The squared modulus, η, of the matrix

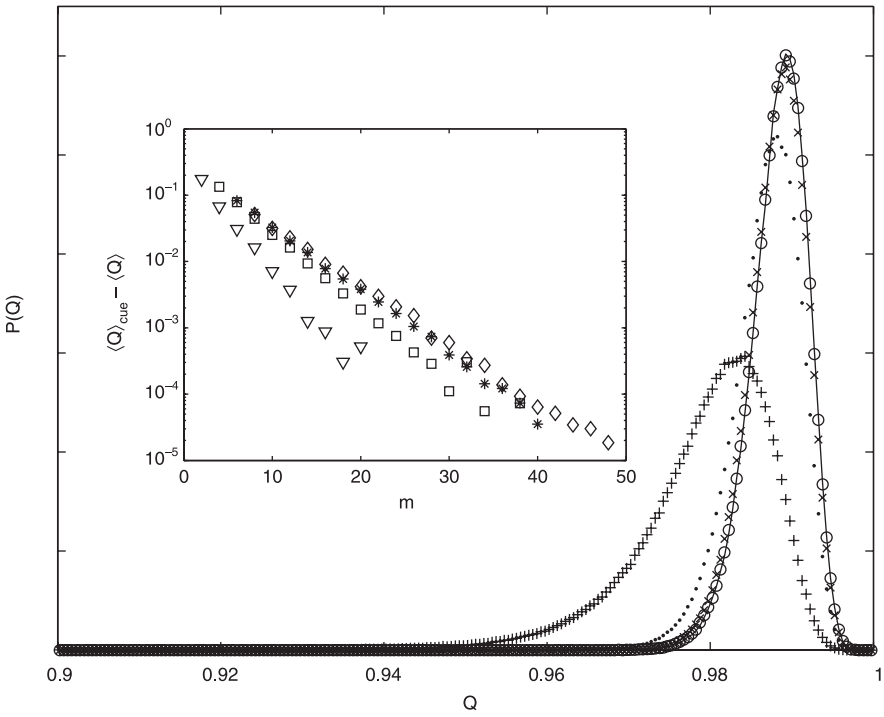

Fig. 1. Distribution of Q for the columns of the pseudo-random unitary operators with $m = 16$ (+), 24 (●), 32 (×), and 40 (○). As m increases, the distribution of Q approaches that for the uniform distribution (solid line). (**Inset**) The difference between the average Q for the random circuits and for the uniform distribution decreases exponentially with increasing m for $n_q = 4$ (▽), 6 (□), 8 (*), and 10 (◇).

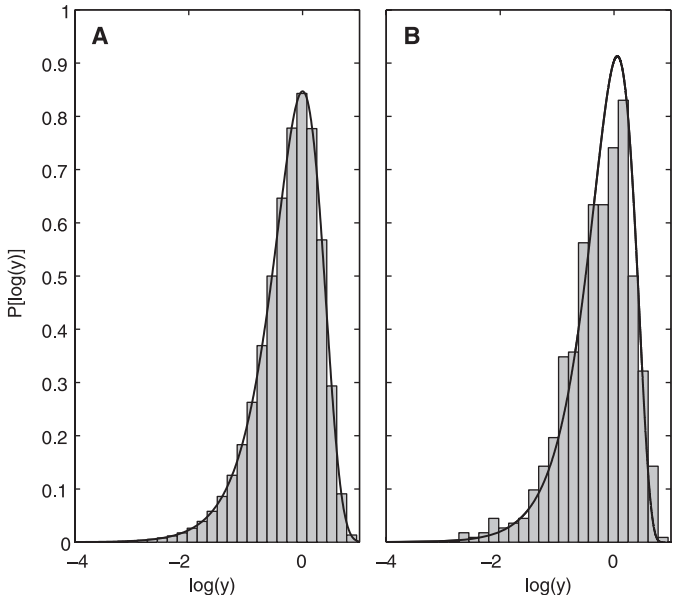

Fig. 2. (**A**) Numerical distribution of matrix elements for 100 random circuits on 8 qubits after $m = 32$ iterations compared to the prediction for uniformly random matrices (Eq. 4 with $N = 256$). (**B**) Experimental histogram of output state components obtained from applying a set of 10 random circuits on 3 qubits to each of the pseudo-pure computational basis states. The data are compared to the prediction for uniformly random pure states (Eq. 4 with $N = 8$).

elements for unitary operators drawn from the uniform measure is distributed according to

$$P_{\mathrm{CUE}}(y) = (N-1)[1-(y/N)]^{N-2} \quad (4)$$

(*13, 18*), where $y = N\eta$. In Fig. 2 we provide the distribution of matrix elements of the random circuits, determined numerically (for $m = 32$ and $n_q = 8$), which shows excellent agreement with the CUE distribution. Moreover, the rate at which the random circuit distribution approaches the exact curve is exponential. In fig. S2, we demonstrate an exponentially decreasing difference between the standard deviations of both distributions as m increases. We have also numerically checked other elementary properties of the random circuits, such as the eigenphase fluctuations and the distribution of eigenvector components, and found similar results. The latter feature has particular relevance to quantum processing because it is the randomness of the circuit eigenvectors that enables unbiased estimation of unknown noise sources (*9*).

The practical design of the two-step gate permits the implementation of several gate iterations with high fidelity using currently available nuclear magnetic resonance (NMR) techniques. We experimentally realized 10 independent random circuits on the three carbon-13 spins of an alanine sample (*25, 26*). Each circuit comprised seven iterations of a slightly weaker two-step gate: Each single-qubit rotation was composed of a sequence of random rotations about the x, y, and z axes, and only one 2-qubit coupling was active per iteration. Each random circuit was applied to each of the eight pseudo-pure (*27, 28*) computational basis states. Because of decoherence errors, the final states, measured by state tomography (*6*), were no longer pseudo-pure. A pure state $|\psi\rangle$ was obtained from each measured state ρ by finding the eigenvector of ρ with the largest eigenvalue. This eigenvector maximizes the fidelity $F = \langle\psi|\rho|\psi\rangle$, the average value of which was 0.78 for the 80 measured states. Because of the limited number of qubits, the most statistically significant test of the experimental data is a comparison of the purified state components with the distribution expected for exact random states (Eq. 4 with $N = 8$) (Fig. 2). The agreement is good ($\chi^2_\nu \approx 1.7$) given the limited statistics, and is comparable to the agreement obtained theoretically using the same number of random circuits ($\chi^2_\nu \approx 1.6$).

These experimental results demonstrate that the practical realization of pseudo-random operators is possible with very few gate iterations. In analogy with the widespread relevance of pseudo-random numbers in classical information theory, we anticipate that these pseudo-random operators will find broad application in quantum information protocols.

References and Notes

1. M. Nielsen, I. Chuang, *Quantum Computation and Quantum Information* (Cambridge Univ. Press, Cambridge, 2001).
2. S. Lloyd, *Phys. Rev. A* **55**, 1613 (1997).
3. A. Harrow, P. Hayden, D. Leung, available at http://arxiv.org/abs/quant-ph/0307221.
4. C. H. Bennett, P. Hayden, D. Leung, P. W. Shor, A. Winter, available at http://arxiv.org/abs/quant-ph/0307100.
5. P. Hayden, D. Leung, P. W. Shor, A. Winter, available at http://arxiv.org/abs/quant-ph/0307104.
6. I. L. Chuang, M. A. Nielson, *J. Mod. Opt.* **44**, 2455 (1997).
7. Ph. Jacquod, P. G. Silvestrov, C. W. J. Beenakker, *Phys. Rev. E* **64**, 055203 (2001).
8. F. M. Cucchietti, D. A. R. Dalvit, J. P. Paz, W. H. Zurek, available at http://arxiv.org/abs/quant-ph/0306142.
9. J. Emerson, Y. S. Weinstein, S. Lloyd, D. G. Cory, *Phys. Rev. Lett.* **89**, 284102 (2002).
10. R. Alicki, A. Lozinski, P. Pakonski, K. Zyczkowski, available at http://arxiv.org/abs/quant-ph/0309194.
11. Broadly speaking, a single complex system in a large Hilbert space will exhibit, with extremely high probability, universal statistical features that are characteristic of the random matrix ensemble. Indeed, this universality feature has led to the successful application of the random matrix ensembles to characterize a variety of complex quantum systems such as heavy nuclei (*29*), quantum chaos models (*18*), and disordered mesoscopic devices (*30*).
12. M. L. Mehta, *Random Matrices* (Academic Press, New York, 1991).
13. M. Pozniak, K. Zyczkowski, M. Kus, *J. Phys. A* **31**, 1059 (1998).
14. R. Schack, *Phys. Rev. A* **57**, 1634 (1998).
15. B. Georgeot, D. L. Shepelyansky, *Phys. Rev. Lett.* **86**, 2890 (2001).
16. G. Benenti, G. Casati, S. Montangero, D. L. Shepelyansky, *Phys. Rev. Lett.* **87**, 227901 (2001).
17. O. Bohigas, M. J. Giannoni, C. Schmit, *Phys. Rev. Lett.* **52**, 1 (1984).
18. F. Haake, *Quantum Signatures of Chaos* (Springer, New York, 1991).
19. P. Bianucci, J. P. Paz, M. Saraceno, *Phys. Rev. E* **65**, 046226 (2002).
20. A. J. Scott, C. M. Caves, *J. Phys. A* **36**, 9553 (2003).
21. This parameterized gate is therefore universal for quantum computation. Specifically, there exists a multiple $m_c = O(n_q^3 N^2)$ and some choice of input parameters for which a circuit composed of m_c gates corresponds to any element of $U(N)$. The additional power on n_q relative to the standard universal set follows from the fact that we have only allowed nearest-neighbor couplings in the parameterized basic gate.
22. S. Sternberg, *Group Theory and Physics* (Cambridge Univ. Press, Cambridge, 1994).
23. D. A. Meyer, N. R. Wallach, *J. Math. Phys.* **43**, 4273 (2002).
24. G. K. Brennen, *Quantum Inform. Comput.* **3**, 619 (2003).
25. The resonant frequency of carbon-13 on a 300-MHz spectrometer is approximately 75.468 MHz, with frequency differences of 9456.5 Hz between spins 1 and 2, 2594.3 Hz between 2 and 3, and 12050.8 Hz between 1 and 3. The J-couple constants between the three spins are $J_{12} = 54.2$ Hz, $J_{23} = 35.1$ Hz, and $J_{13} = -1.2$ Hz. T_1 relaxation times for the three carbon spins in alanine are all longer than 1.5 s; the T_2 relaxation times are longer than 400 ms. The average attenuated correlation (*31*) for the 80 output states is 0.68.
26. L. Viola *et al.*, *Science* **293**, 2059 (2001).
27. D. G. Cory, A. F. Fahmy, T. F. Havel, *Proc. Natl. Acad. Sci. U.S.A.* **94**, 1634 (1997).
28. N. A. Gershenfeld, I. L. Chuang, *Science* **275**, 350 (1997).
29. C. E. Porter, *Statistical Theory of Spectra: Fluctuations* (Academic Press, New York, 1965).
30. C. W. J. Beenakker, *Rev. Mod. Phys.* **69**, 731 (1997).
31. E. M. Fortunato *et al.*, *J. Chem. Phys.* **116**, 7599 (2002).

32. We thank K. Zyczkowski, T. F. Havel, J. P. Paz, P. Zanardi, D. Leung, and J. Goldstone for helpful discussions. Supported by the NSF, Army Research Office, Defense Advanced Research Projects Agency, Agencia Nacional de Promoción Científica y Tecnológica (Argentina), and Cambridge-MIT Institute.

Supporting Online Material

www.sciencemag.org/cgi/content/full/302/5653/2098/DC1

Figs. S1 and S2

25 August 2003; accepted 11 November 2003