Entanglement Generation of Nearly Random Operators

Yaakov S. Weinstein* and C. Stephen Hellberg†

Center for Computational Materials Science, Naval Research Laboratory, Washington, D.C. 20375, USA

(Received 21 December 2004; published 12 July 2005)

We study the entanglement generation of operators whose statistical properties approach those of random matrices but are restricted in some way. These include interpolating ensemble matrices, where the interval of the independent random parameters are restricted, pseudorandom operators, where there are far fewer random parameters than required for random matrices, and quantum chaotic evolution. Restricting randomness in different ways allows us to probe connections between entanglement and randomness. We comment on which properties affect entanglement generation and discuss ways of efficiently producing random states on a quantum computer.

DOI: 10.1103/PhysRevLett.95.030501 PACS numbers: 03.67.Mn, 03.67.Lx, 05.45.Mt

Highly entangled, random quantum states play a central role in many aspects of quantum information processing (QIP). Protocols enabled by random quantum states include superdense coding [1], remote state preparation [2], data hiding schemes [3], and single spin measurement [4]. Random states are produced from computational basis states by applying random unitary operators. However, the implementation of operators randomly drawn from the circular unitary ensemble (CUE), the space of all unitaries, is inefficient.

Independent of its usefulness in QIP, entanglement is a uniquely quantum phenomenon. Entanglement is a conjectured signature of quantum chaos [5–9] and plays an important role in studies of decoherence [10] and measurement. Understanding entanglement allows us to better exploit it as a QIP resource and provides insight into the working of quantum mechanics.

In this Letter we study the entanglement production of operator classes that approach, but do not properly cover, CUE. The purpose of this is twofold. First, it allows us to explore the relationship between randomness and entanglement and investigate which statistical properties of randomness lead to entanglement production. Second, some of the operators explored here may be implemented efficiently on a quantum computer. Thus, this study is an exercise of how best to produce highly entangled random states.

The first class of operators we explore are ensembles of random matrices which interpolate between integrable and CUE [11]. These operators require the same number of random parameters as CUE but the parameters are drawn from restricted intervals. The second class is pseudorandom (PR) operators [12–14], possibly efficient substitutes for random operators in QIP protocols. These operators fall far short of the requisite number of random parameters when compared to CUE operators. The third class is quantum analogs of classically chaotic systems. These operators are the most restricted in terms of random parameters but are known to exhibit certain statistical properties of random matrices [15] and can be efficiently implemented on a quantum computer.

As a practical measure of multipartite entanglement, we use the average bipartite entanglement between each qubit and the rest of the system [16,17],

$$Q(|\psi\rangle) = \frac{4}{n}\sum_{j=1}^{n} D(|\tilde{u}_j\rangle, |\tilde{v}_j\rangle) = 2 - \frac{2}{n}\sum_{j=1}^{n} \mathrm{Tr}[\rho_j^2], \quad (1)$$

where $|\psi\rangle = |0\rangle_j \otimes |\tilde{u}_j\rangle + |1\rangle_j \otimes |\tilde{v}_j\rangle$, $D(|\tilde{u}_j\rangle, |\tilde{v}_j\rangle)$ is the norm squared of the wedge product between $|\tilde{u}_j\rangle$ and $|\tilde{v}_j\rangle$, and ρ_j is the reduced density matrix of qubit j. We apply matrices from the above classes to computational basis states and the average entanglement produced as a function of time (number of iterations), $\langle Q(t)\rangle$, is compared to the CUE average entanglement $\langle Q\rangle_{\mathrm{CUE}} = (N-2)/(N+1)$ [18], where N is the Hilbert space dimension. Other entanglement measures, specifically the concurrence between the two most significant qubits and linear entropy between the two $N/2$ dimensional subspaces, exhibit behavior similar to Q for the operators explored here.

The statistical properties we examine are the level or number variance, the randomness of the eigenvectors, and the matrix element distribution. The number variance measures a two-point eigenvalue correlation function which, for many dynamical systems, is known to deviate from CUE at long range due to short periodic orbits [19]. Thus, the number variance provides insight into entanglement generation as a function of time since periodic orbits will cause deviations from CUE. In the limit of large N, the CUE number variance is [20] $\Sigma^2_{\mathrm{CUE}}(L) = \frac{1}{\pi^2}(\ln(2\pi L) + 1 + \gamma)$, where $\gamma \simeq 0.577$ is the Euler constant.

A lower bound for the asymptotic bipartite entanglement production with respect to time, S_{asy}, is the bipartite entanglement of the systems' eigenvectors, S_{eig}, minus one [21]. This result can be extended to Q since it is an average of bipartite entanglements, $Q_{\mathrm{asy}} \geq 2Q_{\mathrm{eig}} - 1$. Let c_k^l denote the kth component of the lth system eigenvector. The distribution of amplitudes, $\eta = |c_k^l|^2$, for CUE eigenvec-

tors in the limit $N \to \infty$ and after rescaling to unit mean is $P_{\mathrm{CUE}}(y) = e^{-y}$, where $y = N\eta$ [22].

When applying an operator to a computational basis state the resulting state is a column of the applied operator. Repeated applications are simply powers of the column. Thus, an operator's matrix elements, the resulting state elements, play a central role in the amount of entanglement generated. This is seen by writing the average Q over all states in terms of $|c_i|^2$, the state element amplitudes

$$\langle Q\rangle = 4\Big(\sum_{m=1}^{N/2}\sum_{n=(N/2)+1}^{N}\langle|c_m|^2|c_n|^2\rangle - \sum_{q=1}^{N/2}\langle|c_q|^2|c_{q+(N/2)}|^2\rangle\Big). \quad (2)$$

CUE matrices can be generated by multiplying eigenvectors of a Gaussian unitary ensemble (GUE) Hermitian matrix by random phases and using the resulting vectors as matrix columns [23]. Since the eigenvector distribution of CUE and GUE are the same [15], and multiplication by a phase does not change the amplitude of the elements, $P_{\mathrm{CUE}}(x)$, the distribution of the rescaled amplitude of CUE matrix elements x, is equal to $P_{\mathrm{CUE}}(y)$. The closeness of an operator's matrix element amplitude distribution to that of CUE indicates of how much entanglement the operator can generate.

The interpolating ensembles are a one-parameter interpolation between diagonal matrices with uniform, independently distributed elements, and CUE [11]. They are constructed based on the Hurwitz parameterization of CUE matrices. The CUE construction starts with elementary unitary transformations, $E^{(i,j)}(\phi, \psi, \chi)$, with nonzero elements [23,24]

$$\begin{aligned} E^{(i,j)}_{kk} &= 1, \qquad k = 1,\ldots,N, \qquad k \neq i,j,\\ E^{(i,j)}_{ii} &= e^{i\psi}\cos\phi, \qquad E^{(i,j)}_{ij} = e^{i\chi}\sin\phi, \\ E^{(i,j)}_{ji} &= -e^{-i\chi}\sin\phi, \qquad E^{(i,j)}_{jj} = e^{-i\psi}\cos\phi, \end{aligned} \quad (3)$$

which are used to form $N-1$ composite rotations

$$\begin{aligned} E_1 &= E^{(N-1,N)}(\phi_{01}, \psi_{01}, \chi_1),\\ E_2 &= E^{(N-2,N-1)}(\phi_{12}, \psi_{12}, 0)E^{(N-1,N)}(\phi_{02}, \psi_{02}, \chi_2)\ldots,\\ E_{N-1} &= E^{(1,2)}(\phi_{N-2,N-1}, \psi_{N-2,N-1}, 0)\\ &\quad\times E^{(2,3)}(\phi_{N-3,N-1}, \psi_{N-3,N-1}, 0)\\ &\quad\times \ldots E^{(N-1,N)}(\phi_{0,N-1}, \psi_{0,N-1}, \chi_{N-1}), \end{aligned} \quad (4)$$

and, finally, $U_{\mathrm{CUE}} = e^{i\alpha}E_1E_2\ldots E_{N-1}$. Angles ψ, χ, and α are drawn uniformly from the intervals

$$0 \le \psi_{rs} \le 2\pi, \quad 0 \le \chi_s \le 2\pi, \quad 0 \le \alpha \le 2\pi, \quad (5)$$

and $\phi_{rs} = \sin^{-1}(\xi_{rs}^{1/(2r+2)})$, with ξ_{rs} drawn uniformly from 0 to 1. The 2×2 block $E^{(i,j)}_{m,n}$ with $m, n = i, j$ and $r = 0$ is a random SU(2) rotation with respect to the Haar measure. Interpolating ensemble construction is the same with the angles drawn from constricted intervals

$$0 \le \psi_{rs} \le 2\pi\delta, \qquad 0 \le \chi_s \le 2\pi\delta, \qquad 0 \le \alpha \le 2\pi\delta, \quad (6)$$

with $\phi_{rs} = \sin^{-1}(\delta\xi_{rs}^{1/(2r+2)})$ and ξ_{rs} drawn from 0 to 1. The whole is multiplied by a diagonal matrix of random phases drawn uniformly from 0 to 2π. The parameter δ ranges from 0 to 1 and provides a smooth transition of certain statistical properties between the diagonal circular Poisson ensemble and CUE [11].

For our purposes the interpolating ensembles have the same number of random parameters as CUE matrices, drawn, however, from restricted intervals. We stress that δ restricts all N^2 independent variables, such that even ensembles of the highest δ used here cover only an extremely small fraction of CUE space. Figure 1 shows the difference between $\langle Q\rangle_\delta$, and $\langle Q\rangle_{\mathrm{CUE}}$ as a function of time and δ. For $\delta \gtrsim 0.96$, $\langle Q\rangle_\delta$ approaches $\langle Q\rangle_{\mathrm{CUE}}$ as an exponential whose rate decreases with decreasing δ. For $\delta \lesssim 0.5$, the approach is a power law. For constant δ, $\langle Q\rangle_\delta$ approaches its asymptotic value faster for lower N while the difference between the asymptotic value and $\langle Q\rangle_{\mathrm{CUE}}$ increases for lower N.

The next class of operators we investigate is PR operators [12–14], potentially efficient replacements of CUE operators for QIP. To implement a PR operator apply m iterations of the n qubit gate: random SU(2) rotation, Eqs. (3) and (5), to each qubit, and evolve the system via all nearest neighbor couplings [12]. The coupling operator is $U_{nnc} = e^{i(\pi/4)\sum_{j=1}^{n-1}\sigma_z^j\otimes\sigma_z^{j+1}}$, where σ_z^j is the jth qubit z-direction Pauli spin operator. The random rotations are

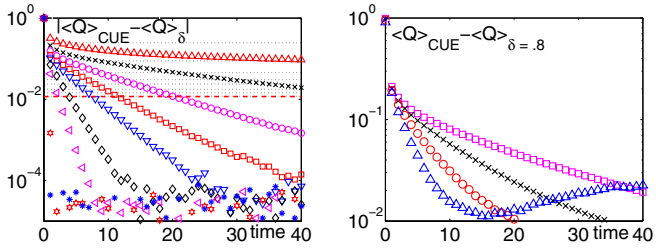

FIG. 1 (color online). Absolute value of difference between the CUE average entanglement, $\langle Q\rangle_{\mathrm{CUE}}$ and the average Q for interpolating ensemble operators, $\langle Q\rangle_\delta$, applied t times to each computational basis state. (left) $N = 256$, $\langle Q\rangle_{\mathrm{CUE}} = 0.9883$ and $\delta = 0.5$ ($\triangle$), 0.8 ($\times$), 0.9 ($\bigcirc$), 0.94 ($\square$), 0.96 ($\triangledown$), 0.98 ($\diamond$), 0.99 (left-triangles), 0.999 (six-pointed stars), and 0.9999 ($*$). The dotted lines show Q_{asy} determined by the eigenvectors of each set of operators. The dashed line shows the lower bound for CUE eigenvectors. (right) $N = 256$ ($\square$), 128 ($\times$), 64 ($\bigcirc$), and 32 ($\triangle$). As N decreases the difference between $\langle Q\rangle_\delta$ and $\langle Q\rangle_{\mathrm{CUE}}$ as a function of time goes from power law to exponential (for $\delta = 0.8$), and the exponential rate increases. This is due to the increased randomness of the matrix elements.

different for each qubit and each iteration. After the mth iteration, a final set of random rotations is applied.

The total number of random parameters used to create a PR operator is $3n(m+1)+1$ where n is the number of qubits. This is compared to $2^{2n}=N^2$ random parameters needed for a CUE matrix. Unless m is exponential in n these operators cannot cover CUE simply because there are too few random parameters.

The absolute value of the difference between $\langle Q\rangle_{\mathrm{CUE}}$ and $\langle Q\rangle_m$ for $n=8$ PR operators as a function of time is shown in Fig. 2. As with the interpolating ensemble operators, $\langle Q\rangle_m$ approaches $\langle Q\rangle_{\mathrm{CUE}}$ as a power law, for low values of m, less coverage of CUE, and as an exponential for greater m. There are a number of interesting features in this plot. First, for values of m where $\langle Q(t)\rangle_m$ approaches $\langle Q\rangle_{\mathrm{CUE}}$ exponentially, the average entanglement fluctuates around $\langle Q\rangle_{\mathrm{CUE}}$ after the exponential saturates (Fig. 2 plots absolute value). $\langle Q\rangle_{40}$ converges immediately into these fluctuations so increasing m beyond 40 will not increase entanglement generation. Also, for operators exhibiting exponential convergence, an operator with $m=m_1$ at time t_1 has approximately the same $\langle Q\rangle$ as an operator with $m_2=\alpha m_1$ at time $t_2=t_1/\alpha$. For example, $\langle Q(t=1)\rangle_{m=24}$ is about equal to $\langle Q(t=3)\rangle_{m=8}$. This is not the case for operators that exhibit nonexponential decay. To create states with $\langle Q\rangle\simeq\langle Q\rangle_{\mathrm{CUE}}$ one can apply an $m=40$ operator once or an $m=8$ operator 5 times. These procedures take the same amount of time, but the $m=8$ operator requires fewer random parameters. Thus, the number of independent variables needed to create entanglement $\simeq\langle Q\rangle_{\mathrm{CUE}}$ in a reasonable time is the number required for the lowest m that gives exponential convergence (for $n=8$ this is approximately $m=8$). Unlike the interpolating ensemble matrices, the behavior of Q as a function of time barely changes with N.

The above shows that one can create states with CUE levels of multipartite entanglement though only a small portion of CUE is covered. An $m=8$ PR operator, for example, has only $193/256^2=0.3\%$ of the random parameters needed for CUE operators but can generate CUE levels of entanglement by iterating the operator 5–6 times.

The interpolating ensemble operators and PR operators lead to similar average entanglement generation behavior as a function of time. For both, the entanglement approaches $\langle Q\rangle_{\mathrm{CUE}}$ as a power law and, as the operators cover more of CUE, an exponential. *A priori*, there is no reason that different restrictions on CUE should give rise to similar average entanglement behavior, especially since the distributions of Q after one iteration are very different for the two types of operators (not shown).

In light of these results, Fig. 3 shows how various statistical properties relate to entanglement production with the aim to explain why the entanglement generation approaches $\langle Q\rangle_{\mathrm{CUE}}$ as a power law or exponential, and why $\langle Q\rangle_\delta$ is dependent on N while $\langle Q\rangle_{\mathrm{PR}}$ is not.

Based on our numerical investigations, the number variance determines the approach of $\langle Q\rangle$ to $\langle Q\rangle_{\mathrm{CUE}}$. For the interpolating ensembles with $\delta<0.9$ and low m PR operators the number variance diverges almost immediately from $\Sigma^2_{\mathrm{CUE}}(L)$. For values of δ and m where $\langle Q\rangle$ approaches $\langle Q\rangle_{\mathrm{CUE}}$ exponentially as a function of time, $\Sigma^2_\delta(L)$ follows CUE faithfully even for large L. In other words, operators for which $\langle Q\rangle$ approaches $\langle Q\rangle_{\mathrm{CUE}}$ as a power law do not follow $\Sigma^2_{\mathrm{CUE}}(L)$, while those that approach $\langle Q\rangle_{\mathrm{CUE}}$ as an exponential follow $\Sigma^2_{\mathrm{CUE}}(L)$ up to long range correlations, corresponding to short time.

As expressed in Eq. (2), the matrix element distribution (Fig. 3) is key in determining entanglement generation. The matrix element distribution approaches the CUE distribution at a rate similar to that of the one iteration entanglement distribution, $P(Q)$ (not shown). This rate of convergence is slower than that of other explored statistics. Second, the matrix element distributions explains the be-

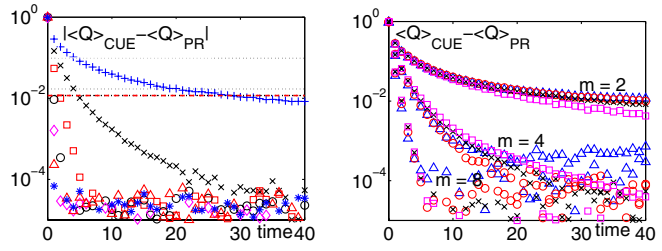

FIG. 2 (color online). Absolute value of difference between $\langle Q\rangle_{\mathrm{CUE}}$ and $\langle Q(t)\rangle_m$. (left) $n=8$ qubits, $m=2$ (+), 4 ($\times$), 8 ($\square$), 16 ($\bigcirc$), 24 ($\diamond$), 32 ($\triangle$), and 40 ($*$). Each average is taken over 100 operators applied to all $N=256$ computational basis states. The dotted lines show Q_{asy} as determined from the eigenvectors. Note that the lower bound for $m\geq 16$ operators is higher than the lower bound of random eigenvectors. (right) The same for $n=9$ ($\square$), 8 ($\times$), 7 ($\bigcirc$), and 6 ($\triangle$). The entanglement production compared to CUE changes only slightly as a function of n.

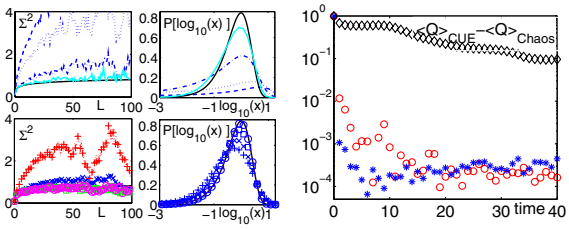

FIG. 3 (color online). (left) Number variance (left) and matrix element distribution (right), for interpolating ensemble (top) and PR operators (bottom). Shown are statistics for interpolating ensembles with $\delta=0.1$ (dashed line), 0.5 (dotted line), 0.9 (chained line), and 0.98 (light solid line). For the PR operators statistics are shown for $m=2$ (+), 4 ($\times$), 8 ($\square$), and 16 ($\bigcirc$). As m and δ are increased the statistical properties approach CUE (solid line). The rate of approach for the matrix element distribution is slower than other statistics. (right) Absolute value of difference between $\langle Q\rangle_{\mathrm{CUE}}$ and $\langle Q(t)\rangle$ of the quantum baker's map ($\diamond$) and sawtooth map for noninteger kick strength $0<k_{\mathrm{saw}}<5$ ($\bigcirc$), and Harper's map for $1\leq\gamma_H\leq 6$ ($*$).

havior of the entanglement generation as a function of N. For the interpolating ensemble operators, the eigenvector and eigenvalue statistics are practically unchanged with N [11]. The matrix element distribution, however, is strongly dependent on N as is the entanglement generation. For $\delta = 0.9$ operators, the matrix element distribution is fully random for $N = 8$ but deviates as N increases. For the PR operators the eigenvector and eigenvalue statistics depend only slightly on N, as with the matrix element distribution. The entanglement generation is also essentially unchanged.

The final class of operators we explore are quantum chaotic operators. While a full analysis is beyond the scope of this Letter we discuss them in comparison to the other operators. Figure 3 shows entanglement generation as a function of time for the quantum baker's map [25] and ensembles of chaotic sawtooth [26] and Harper maps [27]. The convergence to $\langle Q \rangle_{\mathrm{CUE}}$ is between exponential and Gaussian but the asymptotic value is lower than the other operators. The chaotic maps require on order n^2 [25] or n^3 [26] gates. The PR operators require $n - 1$ coupling terms and n rotations per iteration, approximately $2mn$ gates per operator. These are comparable as long as m is less than quadratic in n. However, unlike the quantum chaotic operators, the coupling terms at every iteration of the PR algorithm can be applied simultaneously. The PR operators thus require only $2m + 1$ gates which appears to be less than that required of chaotic operators.

In conclusion, we have studied the entanglement generation of interpolating ensemble, PR, and quantum chaotic operators as a function of time. These operators restrict the full space of CUE in different ways and the effect of these restrictions can be seen in the entanglement generation. The statistical properties which influence the entanglement generation include the number variance, which effects the entanglement generation as a function of time, and the matrix element distribution, which determines other aspects of the entanglement. Finally, we note that the PR operators may be efficiently implemented on a quantum computer and provide a way to create highly entangled, random states.

The authors thank K. Zyczkowski for clarifying interpolating ensemble generation, J. Emerson for helpful discussions, and acknowledge support from the DARPA QuIST (MIPR 02 N699-00) program. Y. S. W. acknowledges support of the National Research Council through the Naval Research Laboratory. Computations were performed at the ASC DoD Major Shared Resource Center.

*To whom all correspondence should be addressed.
Present address: Quantum Information Science Group, MITRE, Eatontown, NJ, 07724, USA.
Electronic address: weinstein@mitre.org

†Electronic address: hellberg@dave.nrl.navy.mil

[1] A. Harrow, P. Hayden, and D. Leung, Phys. Rev. Lett. **92**, 187901 (2004).
[2] C. H. Bennett, P. Hayden, D. Leung, P. Shor, and A. Winter, IEEE Trans. Inf. Theory **51**, 56 (2005).
[3] P. Hayden, D. Leung, P. Shor, and A. Winter, Commun. Math. Phys. **250**, 371 (2004).
[4] P. Cappellaro, J. Emerson, N. Boulant, C. Ramanathan, S. Lloyd, and D. G. Cory, Phys. Rev. Lett. **94**, 020502 (2005).
[5] A. Lakshminarayan, Phys. Rev. E **64**, 036207 (2001); J. N. Bandyopadhyay and A. Lakshminarayan, Phys. Rev. Lett. **89**, 060402 (2002).
[6] K. Furuya, M. C. Nemes, and G. Q. Pellegrino, Phys. Rev. Lett. **80**, 5524 (1998).
[7] P. A. Miller and S. Sarkar, Phys. Rev. E **60**, 1542 (1999).
[8] X. Wang, S. Ghose, B. C. Sanders, and B. Hu, Phys. Rev. E **70**, 016217 (2004).
[9] A. Tanaka, H. Fujisaki, and T. Miyadera, Phys. Rev. E **66**, 045201(R) (2002); H. Fujisaki, T. Miyadera, and A. Tanaka, Phys. Rev. E **67**, 066201 (2003).
[10] W. H. Zurek, Phys. Rev. D **26**, 1862 (1982).
[11] K. Zyczkowski and M. Kus, Phys. Rev. E **53**, 319 (1996).
[12] J. Emerson, Y. S. Weinstein, M. Saraceno, S. Lloyd, and D. G. Cory, Science **302**, 2098 (2003).
[13] Y. S. Weinstein and C. S. Hellberg, Phys. Rev. A **69**, 062301 (2004).
[14] Y. S. Weinstein and C. S. Hellberg, Phys. Rev. A **71**, 014303 (2005).
[15] F. Haake, *Quantum Signatures of Chaos* (Springer, New York, 1991).
[16] D. A. Meyer and N. R. Wallach, J. Math. Phys. (N.Y.) **43**, 4273 (2002).
[17] G. K. Brennen, Quantum Inf. Comput. **3**, 619 (2003).
[18] A. Scott and C. Caves, J. Phys. A **36**, 9553 (2003).
[19] R. Aurich and F. Steiner, Physica D (Amsterdam) **82**, 266 (1995).
[20] M. L. Mehta, *Random Matrices* (Academic, New York, 1991).
[21] R. Demkowicz-Dobrzanski and M. Kus, Phys. Rev. E **70**, 066216 (2004).
[22] F. Haake and K. Zyczkowski, Phys. Rev. A **42**, R1013 (1990).
[23] K. Zyczkowski and M. Kus, J. Phys. A **27**, 4235 (1994); M. Pozniak, K. Zyczkowski, and M. Kus, J. Phys. A **31**, 1059 (1998).
[24] Because of misprints contained in the referenced papers [11,23] we explicitly present the algorithm actually used in those works.
[25] N. L. Balazs and A. Voros, Ann. Phys. (N.Y.) **190**, 1 (1989); R. Schack, Phys. Rev. A **57**, 1634 (1998).
[26] A. Lakshminarayan and N. L. Balzs, Chaos Solitons Fractals **5**, 1169 (1995); G. Benenti, G. Casati, S. Montangero, and D. L. Shepelyansky, Phys. Rev. Lett. **87**, 227901 (2001).
[27] P. Leboeuf, J. Kurchan, M. Feingold, and D. P. Arovas, Phys. Rev. Lett. **65**, 3076 (1990); P. Bianucci, J. P. Paz, and M. Saraceno, Phys. Rev. E **65**, 046226 (2002); B. Levi and B. Georgeot, Phys. Rev. E **70**, 056218 (2004).