# Pseudorandom circuits from Clifford-plus-$T$ gates

Yaakov S. Weinstein
*Quantum Information Science Group, MITRE, 200 Forrestal Road, Princeton, New Jersey 08540, USA*
(Received 25 July 2013; published 2 December 2013)

We explore the implementation of pseudorandom single-qubit rotations and multiqubit pseudorandom circuits constructed only from Clifford gates and the $T$ gate, a phase rotation of $\pi/4$. Such a gate set would be appropriate for computations performed in a fault tolerant setting. For single-qubit rotations the distribution of parameters found for unitaries constructed from Clifford plus $T$ quickly approaches that of random rotations and requires significantly fewer gates than the construction of arbitrary single-qubit rotations. For Clifford-plus-$T$ pseudorandom circuits we find an exponential convergence to a random matrix element distribution and a Gaussian convergence to the higher-order moments of the matrix element distribution. In addition, the nearest-neighbor eigenangle statistics distribution almost immediately converges to that of random unitary matrices. All of these convergence rates are found to be insensitive to the number of qubits.

DOI: 10.1103/PhysRevA.88.062303 PACS number(s): 03.67.Lx, 03.67.Mn, 03.67.Bg

Quantum information can be protected against errors by properly encoding it into suitable quantum error correction codes [1]. Manipulating the information while it remains encoded can be done if all manipulations, such as quantum gates and the like, respect the symmetries of the code. The framework which allows the implementation of a universal set of gates on the encoded information in such a way that the quantum information does not leave the encoded space is known as quantum fault tolerance (QFT) [2–5]. Within a QFT setting many quantum error correction codes, such as the Calderbank-Shor-Steane (CSS) codes [6,7], utilize a universal gate set consisting of Clifford gates, gates that map Pauli matrices to Pauli matrices, plus the $T$ gate, a single-qubit $\pi/4$ phase rotation. Clifford gates can be implemented bitwise, while the $T$ gate is implemented with the utilization of appropriate ancilla qubits.

The universality of the gate set Clifford plus $T$, meaning the ability to implement any quantum operation using only gates from this set, does not by itself provide a prescription of how to use these gates to implement quantum protocols. A major difficulty in such a prescription is the implementation of arbitrary single-qubit rotations. Initial work on this problem was done in [8,9] and more recent investigations have resulted in techniques with markedly improved efficiencies with respect to the number of necessary gates needed to achieve a prescribed gate accuracy $\epsilon$ [10–16]. In this paper we are interested not in implementing any specific gate, but in implementing random single-qubit gates and random unitary operations with an arbitrary number of qubits with gates that are appropriate for QFT. Thus, it is necessary to design algorithms that can implement random unitary operators using only Clifford and $T$ gates.

Random unitary operators and quantum states play an important role in many quantum information protocols. Random states saturate the classical communication capacity of a noisy quantum channel [17], and are used for superdense coding of quantum states [18], and data hiding schemes [19]. Random quantum states can also be used for randomized benchmarking of quantum processes in the presence of noise [20]. Random unitaries themselves are useful for remote state preparation [21] and noise characterization [22–24].

The above protocols require random unitary operators drawn uniformly from the Haar measure of the circular unitary ensemble (CUE). However, the number of quantum gates necessary to implement CUE random unitaries on a quantum computer grows exponentially with the number of qubits [22,25]. A possible substitute for CUE random matrices is the pseudorandom (PR) unitaries introduced in [22]. PR unitaries have statistical moments that approximate those of CUE matrices.

An efficient means of implementing PR unitaries is via PR circuits [22,26–29]. PR circuits consist of an iterated set of one- and two-qubit gates having certain degrees of freedom which are chosen at random. As an example, each iteration of the standard PR circuit introduced in [22] consists of a random rotation on each single qubit followed by controlled-phase (CZ) gates between all nearest neighbors. The three Euler angles that determine the single-qubit rotations serve as the degrees of freedom for the PR circuit. They are chosen randomly and independently for each rotation. As more iterations are applied (using different single-qubit gates for each qubit and at each time step) the statistical properties of the total unitary operator implemented compare more favorably to the statistical properties of random unitaries.

Subsequent studies of PR circuits have focused on the convergence of such algorithms to different statistical properties of random unitaries [30,31]. Reference [32] specifically demonstrates that such circuits can efficiently implement unitaries whose statistical moments up to order $k$ approximate that of the Haar measure, within any prescribed accuracy $\epsilon$, for arbitrary $k$. Additional work has been done on the choice of two-qubit gates [27], the choice of single-qubit gates [29], some aspects of the topology of the qubits [27,28,33], and the ability of such unitaries to efficiently construct states of generic entanglement [26]. PR circuits have also been formulated for cluster-state quantum computation [29,34].

Unlike previous work, here we restrict our gate set to those appropriate when operating within a QFT framework. We do not assume the ability to perform arbitrary single-qubit rotations but instead limit our gate set to those that will keep quantum information within the quantum error correction encoding. Thus, we will attempt to construct random rotations

 

and PR unitaries utilizing only single-qubit Clifford gates, the $T$ gate, and the CZ gate.

We first explore the construction of random single-qubit rotations using only the Clifford gates Hadamard $H$ and phase $S$, and the $T$ gate given by

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \quad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}. \tag{1}$$

We note that the phase gate is equivalent to implementing the $T$ gate twice in a row, $S = T^2$. Nevertheless, we identify it separately because it can be implemented bitwise at much less of a cost in time and ancilla qubits than even a single implementation of a $T$ gate. One possible construction protocol would be to randomly apply one of these three gates at every time step $t$. However, we reject this suggestion as there are too many combinations of gates that would be extraneous: $T^2 = S$ and $H^2 = \mathbb{1}$. Instead we look to the gate sequences commonly found in prescriptions of arbitrary rotation using only gates from the set Clifford plus $T$ [10,15,16]. We choose the sequences $HT$ and $SHT$ and apply one or the other at every time step to construct our single-qubit rotations. We equally weigh every one of the $2^t$ possible rotations for every time step up to $t = 25$ and compare the statistics of these unitaries with those of random single-qubit rotations.

Random single-qubit rotations are unitaries drawn uniformly with respect to the Haar measure of SU(2) and are completely parametrized by the Euler angles $\psi$, $\chi$, and $\phi$, as follows:

$$U_1 = \begin{pmatrix} e^{i\psi}\cos\phi & e^{i\chi}\sin\phi \\ -e^{-i\chi}\sin\phi & e^{-i\psi}\cos\phi \end{pmatrix}, \tag{2}$$

where $\psi$ and $\chi$ are drawn independently and uniformly from between 0 and $2\pi$, and $\phi = \sin^{-1}\sqrt{\xi}$ where $\xi$ is drawn uniformly from between 0 and 1.

To compare the Clifford-plus-$T$-gate constructed unitaries with single-qubit random unitaries we extract from each of the $2^t$ constructed unitaries the paramaters $\psi$, $\chi$, and $\xi$ which are then sorted into equally spaced bins (our simulations are only slightly dependent on the number of bins). The normalized distributions of these parameters, $\tilde{P}(\alpha)$ for $\alpha = \psi, \chi, \xi$, are compared to the appropriate distributions for random unitaries, $P(\alpha)$. The difference between these distributions is then calculated as $D(\alpha) = \sum |\tilde{P}(\alpha) - P(\alpha)|^2$ where the sum is taken over all bins.

Figure 1 plots each $D(\alpha)$ as a function of time step. As shown, $D(\alpha)$ decreases at an exponential rate $e^{-\kappa t}$ where a least-squares fit for the decay constant $\kappa$ gives 0.63, 0.60, and 0.66 for $D(\chi)$, $D(\psi)$, and $D(\xi)$ respectively. These results demonstrate that the distribution of single-qubit rotations based on Clifford-plus-$T$ gates quickly approaches that of random unitaries, justifying our initial choice of gate to sequences to be applied. We note that the average number of time steps to achieve $D(\alpha) < 10^{-5}$ is 20 which translates into 20 $T$ gates and an average total of 50 single-qubit gates. This number is significantly below the number of single-qubit gates needed to construct an arbitrary single-qubit rotation to the same accuracy [15,16].

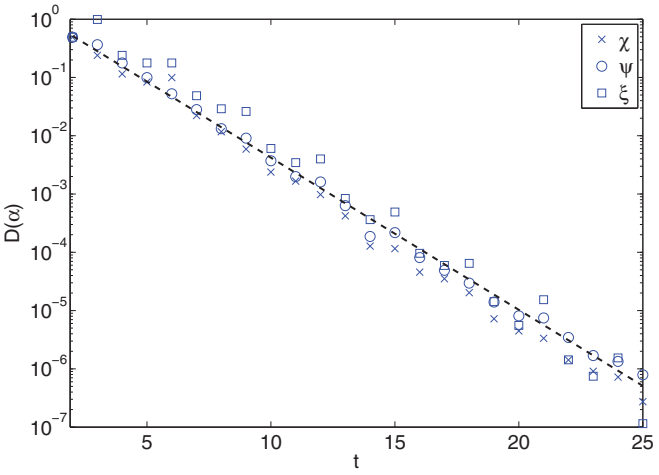


FIG. 1. (Color online) Difference $D(\alpha)$ between the distributions of $\xi$ (×), $\psi$ (○), and $\chi$ (□) for random single-qubit unitary matrices and those constructed from Clifford-plus-$T$ gates as a function of time step $t$. The least-squares fit to $D(\psi)$ (dotted line) is given by $\exp(0.54–0.60t)$. Least-squares fitting to $D(\chi)$ and $D(\xi)$ gives similar coefficients.

Based on the above, a straightforward way to implement PR circuits on multiple qubits using only gates from Clifford plus $T$ is to simply replace the single-qubit unitaries drawn from SU(2) of the standard PR circuit [22] with a sequence of $HT$ and $SHT$ gates that would implement a PR single-qubit unitary. The convergence to CUE statistics would be similar to the standard case at an increased cost in number of gates applied equal to the number of gates used to implement the PR single-qubit rotation (depending on the desired accuracy) times the number of qubits.

For the sake of increased efficiency, however, we would like to explore the possibility of applying only one iteration of the sequence $HT$ or $SHT$ on each of the qubits in place of the random single-qubit rotations of the standard PR circuit. Thus, a time step $t$ of the Clifford-plus-$T$ gate PR circuit on a line of $n$ qubits would involve applying to each qubit either the single-qubit gates $HT$ or the gates $SHT$ (each with a probability of 0.5), followed by CZ gates between all nearest neighbors.

To determine the randomness of the PR unitaries constructed in this way we compare a number of statistical properties of the constructed unitaries to those of CUE matrices. We start with the matrix element distribution and its higher-order moments. For CUE matrices, random matrix theory provides the following distribution [35]:

$$P(l) = \frac{N-1}{N} e^l \left(1 - \frac{e^l}{N}\right)^{N-2}, \tag{3}$$

where $N = 2^n$ is the Hilbert space dimension and $l$ is a function of the matrix elements $U_{ij}$ given by $l = \ln(N|U_{ij}|^2)$. We compare this distribution to that of the PR unitaries from Clifford-plus-$T$ gates by constructing a sample number $r$ of PR unitaries and binning the $rN^2$ $l$ values into equally spaced bins. The distance between the normalized distributions is, as

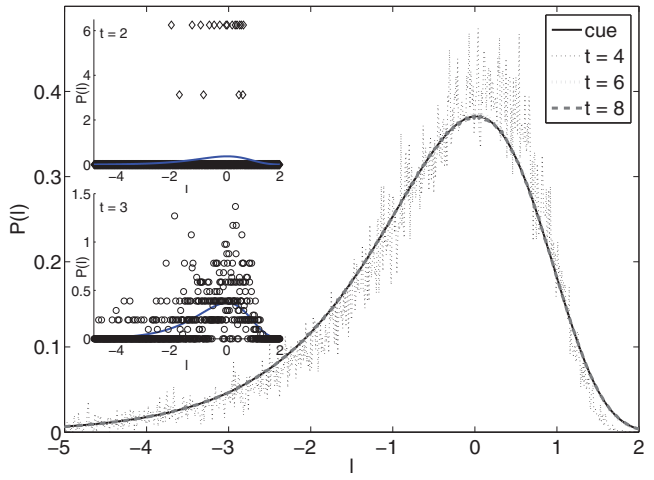


FIG. 2. (Color online) Matrix element distribution $\tilde{P}(l)$ for $n = 6$ PR circuits from Clifford-plus-$T$ gates at different time steps. For $t = 2$ (top left inset) and $t = 3$ (bottom left inset) the distribution is simply a series of large spikes. For higher $t$ (main figure) the spikes merge into a continuous distribution and collapse into the CUE random matrix element distribution.

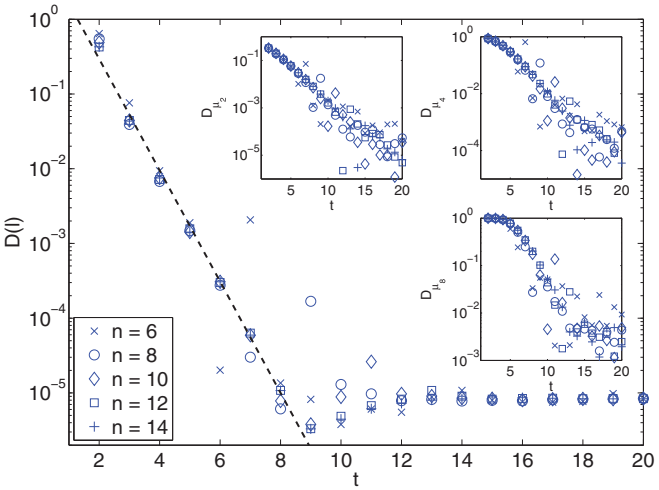


FIG. 3. (Color online) Difference $D(l)$ between the distributions for CUE random matrices and those constructed via PR circuits from Clifford-plus-$T$ gates for $n = 6$ ($\times$), 8 ($\circ$), 10 ($\diamond$), 12 ($\square$), and 14 ($+$) qubits. The least-squares fit to the 12-qubit case (dotted line) is given by $\exp(2.21–1.71t)$. The insets show the deviation from the random matrix derived moments of the matrix element distribution as a function of time step for moments $k = 2$ (top left), 4 (top right), and 8 (bottom). Note that the convergence to the moments is not exponential but Gaussian.

above, given by

$$D(l) = \sum |\tilde{P}(l) - P(l)|^2, \tag{4}$$

where the sum is taken over all bins. This is done for $n = 6$, 8, 10, 12, and 14 qubits using $r = 10\,000$ for the cases $n = 6$ and 8, $r = 1000$ for $n = 10$, $r = 50$ for $n = 12$, and $r = 5$ for $n = 14$.

The convergence of the matrix element distribution for the Clifford-plus-$T$-gate constructed unitaries to that of CUE is shown in Fig. 2 for the case of $n = 6$. Of note is the behavior of the approach. Initially the matrix elements are confined to very specific magnitudes such that the distribution is simply a series of large spikes. As $t$ increases the spikes shrink and increase in number before joining together to collapse into the desired distribution. This behavior should be contrasted, for example, with that demonstrated in [36] where for low $t$ the distribution is heavily weighted towards higher magnitude elements before spreading out and filling up the lower magnitude parts of the distribution.

The complete results are shown in Fig. 3 and demonstrate the ability to construct PR unitaries from the Clifford-plus-$T$ gates. As the number of time steps increase $\tilde{P}(l)$ converges to $P(l)$ at an exponential rate marred only by an overshoot at $t = n$ followed by a spike at $t = n + 1$. The magnitude of this overshoot and spike decreases with increasing number of qubits. In addition, the rate of convergence is independent of the number of qubits and the decay constant is $\kappa \simeq 1.71$ (this will depend somewhat on the level of binning). We note that the lack of sensitivity to qubit number is due to the PR circuit prescribing that two-qubit gates are applied between all nearest neighbors at every time step. PR circuits that apply only one two-qubit gate at a time, such as [36], converge at a rate that is strongly dependent on the number of qubits.

To explore further the accuracy with which the PR unitaries built from Clifford-plus-$T$ gates resemble random unitaries we look at higher-order moments of the matrix element distributions $\tilde{P}(l)$. Moments of distribution of matrix elements were analyzed in the context of PR unitaries in Ref. [36]. Here we are especially interested in whether the evolution of these moments will depend on the number of qubits. The $k$th moment of the matrix element distribution $\mu_k$ is defined as $N^k \langle |U_{i,j}|^{2k} \rangle$. For CUE matrices the moments are given by [36]

$$\mu_k = \frac{k! N^k (N-1)!}{(N+k-1)!}. \tag{5}$$

We look at the deviation from the random matrix derived moments via

$$D_{\mu_k} = \frac{|\mu_k - \tilde{\mu}_k|}{\mu_k}, \tag{6}$$

where $\tilde{\mu_k}$ is the calculated matrix element distribution moment for the unitaries constructed from the set of gates Clifford plus $T$. The results for moments $k = 2$, 4, and 8 are shown in the insets of Fig. 3. First, we see that, as with the difference in distributions, the results are basically independent of the number of qubits except for the same overshoot and recovery phenomenon discussed above at time steps $t = n$ and $n + 1$. In contrast to the difference in distributions however, the rate of convergence to the CUE is not exponential but a Gaussian with the exact behavior depending on $k$: the higher the moment the slower the initial convergence.

We now look at the nearest-neighbor eigenangle separation distribution for our constructed unitaries and compare them to the same distribution for CUE matrices. For CUE matrices the distribution of nearest-neighbor eigenangle separation is given

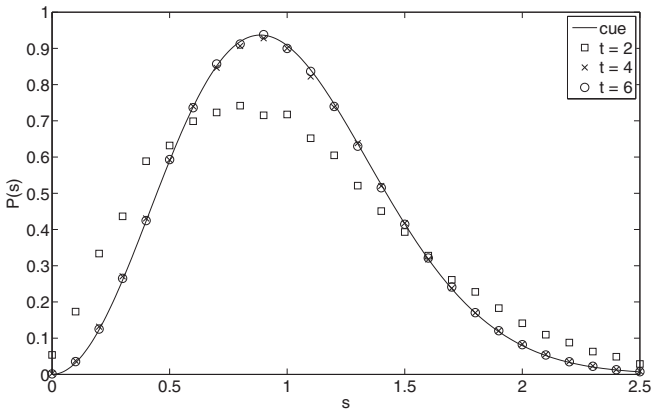


FIG. 4. Distribution of nearest-neighbor eigenangle difference distribution for Clifford-plus-$T$-gate PR circuits with 2 (□), 4 (×), and 6 (○) iterations, compared to the same distribution for CUE matrices (solid line). As the number of iterations increases, the eigenangle difference distribution quickly approaches that of CUE matrices.

by [37]

$$P(s) = \frac{32s^2}{\pi^2} e^{4s^2/\pi}, \tag{7}$$

where $s$ is the difference between two ordered eigenangles. Figure 4 shows the almost immediate convergence of the nearest-neighbor eigenangle difference distribution of PR unitaries to $P(s)$. While the results shown are for six qubits, very similar statistical distributions were found for 8, 10, 12, and 14 qubits. In addition, the distribution of eigenvector elements for circuits with all the above numbers of qubits was determined and compared to that of CUE. The convergence was again almost immediate and similar to the convergence of the nearest-neighbor eigenangle difference distribution.

In conclusion, we have demonstrated the construction of random single-qubit unitaries by stringing together sequences of the gates $HT$ and $SHT$. We have shown that the statistical distributions of the Euler angles from the set of unitaries quickly approach that of random SU(2) matrices. We then extended the exploration to more qubits, devising pseudorandom circuits utilizing only Clifford gates and the $T$ gate. The matrix elements from the unitaries thus constructed quickly approach the distribution of CUE matrix elements with little sensitivity to the number of qubits.

This exploration provides a useful algorithm to construct random states and unitaries within the quantum fault tolerant framework. Future work will focus on the accuracy and robustness of the algorithm when subject to errors. In that case (noisy) gates will be implemented on logical qubits that allow quantum error correction to be explicitly implemented.

Y.S.W. thanks S. Pappas for constructive conversations and G. Gilbert for comments. Support was provided by the MITRE Technology Program under MTP Grant No. 07MSR205.

[1] M. Nielsen and I. Chuang, *Quantum Information and Computation* (Cambridge University Press, Cambridge, England, 2000).
[2] J. Preskill, Proc. R. Soc. London, Ser. A **454**, 385 (1998).
[3] P. W. Shor, *Proceedings of the the 35th Annual Symposium on Fundamentals of Computer Science* (IEEE, Los Alamitos, CA, 1996).
[4] D. Gottesman, Phys. Rev. A **57**, 127 (1998).
[5] P. Aliferis, D. Gottesman, and J. Preskill, Quantum Inf. Comput. **6**, 97 (2006); A. M. Steane, Phys. Rev. Lett. **77**, 793 (1996).
[6] P. W. Shor, Phys. Rev. A **52**, R2493 (1995).
[7] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996).
[8] A. Y. Kitaev, Russ. Math. Surv. **52**, 1191 (1997); A. Y. Kitaev, A. H. Shen, and M. N. Vyalyi, *Classical and Quantum Computation*, Graduate Studies in Mathematics No. 47 (American Mathematical Society, Providence, 2002).
[9] C. M. Dawson and M. A. Nielsen, Quantum Inf. Comput. **6**, 81 (2006).
[10] A. Bocharov and K. M. Svore, Phys. Rev. Lett. **109**, 190501 (2012).
[11] V. Kliuchnikov, D. Maslov, and M. Mosca, Quantum Inf. Comput. **13**, 607 (2013).
[12] T. T. Pham, R. Van Meter, and C. Horsman, Phys. Rev. A **87**, 052332 (2013).
[13] G. Duclos-Ciani and K. M. Svore, Phys. Rev. A **88**, 042325 (2013).
[14] V. Kliuchnikov, D. Maslov, and M. Mosca, Phys. Rev. Lett. **110**, 190502 (2013).
[15] P. Selinger, arXiv:1212.6253.
[16] V. Kliuchnikov, D. Maslov, and M. Mosca, arXiv:1212.6964.
[17] S. Lloyd, Phys. Rev. A **55**, 1613 (1997).
[18] A. Harrow, P. Hayden, and D. Leung, Phys. Rev. Lett. **92**, 187901 (2004).
[19] P. Hayden, D. Leung, P. Shor, and A. Winter, Commun. Math. Phys. **250**, 371 (2004).
[20] E. Magesan, J. M. Gambetta, and J. Emerson, Phys. Rev. Lett. **106**, 180504 (2011); Phys. Rev. A **85**, 042311 (2012).
[21] C. H. Bennett, P. Hayden, D. Leung, P. Shor, and A. Winter, IEEE Trans. Inform. Theor. **51**, 56 (2005).
[22] J. Emerson, Y. S. Weinstein, M. Saraceno, S. Lloyd, and D. G. Cory, Science **302**, 2098 (2003).
[23] J. Emerson, M. Silva, O. Moussa, C. Ryan, M. Laforest, J. Baugh, D. G. Cory, and R. Laflamme, Science **317**, 1893 (2007).
[24] B. Levi, C. C. Lopez, J. Emerson, and D. G. Cory, Phys. Rev. A **75**, 022314 (2007).
[25] M. Pozniak, K. Zyczkowski, and M. Kus, J. Phys. A **31**, 1059 (1998).
[26] R. Oliveira, O. C. O. Dahlsten, and M. B. Plenio, Phys. Rev. Lett. **98**, 130502 (2007); O. C. O. Dahlsten, R. Oliveira, and M. B. Plenio, J. Phys. A **40**, 8081 (2007).
[27] M. Znidaric, Phys. Rev. A **76**, 012318 (2007).
[28] Y. Most, Y. Shimoni, and O. Biham, Phys. Rev. A **76**, 022328 (2007).
[29] W. G. Brown, Y. S. Weinstein, and L. Viola, Phys. Rev. A **77**, 040303(R) (2008).
[30] J. Emerson, E. Livine, and S. Lloyd, Phys. Rev. A **72**, 060302(R) (2005).

[31] Y. S. Weinstein and C. S. Hellberg, Phys. Rev. Lett. **95**, 030501 (2005).
[32] W. G. Brown and L. Viola, Phys. Rev. Lett. **104**, 250501 (2010).
[33] Y. S. Weinstein, W. G. Brown, and L. Viola, Phys. Rev. A **78**, 052332 (2008).
[34] A. D. K. Plato, O. C. Dahlsten, and M. B. Plenio, Phys. Rev. A **78**, 042332 (2008).
[35] F. Haake, *Quantum Signatures of Chaos*, 2nd ed. (Springer, Berlin, Heidelberg, 2000).
[36] L. Arnaud and D. Braun, Phys. Rev. A **78**, 062329 (2008).
[37] M. L. Mehta, *Random Matrices* (Academic, New York, 1991).