PAPER • OPEN ACCESS

Cutoff phenomenon and entropic uncertainty for random quantum circuits

To cite this article: Sangchul Oh and Sabre Kais 2023 *Electron. Struct.* **5** 035004

View the article online for updates and enhancements.

Electronic Structure

Cutoff phenomenon and entropic uncertainty for random quantum circuits

Sangchul Oh[1,2] and Sabre Kais[1,*]

1   Department of Chemistry, Department of Physics and Astronomy, and Purdue Quantum Science and Engineering Institute, Purdue University, West Lafayette, IN, United States of America
2   School of Physics and Applied Physics, Southern Illinois University, Carbondale, IL 62901, United States of America
*   Author to whom any correspondence should be addressed.

E-mail: kais@purdue.edu

Abstract

How fast a state of a system converges to a stationary state is one of the fundamental questions in science. Some Markov chains and random walks on finite groups are known to exhibit the non-asymptotic convergence to a stationary distribution, called the cutoff phenomenon. Here, we examine how quickly a random quantum circuit could transform a quantum state to a Haar-measure random quantum state. We find that random quantum states, as stationary states of random walks on a unitary group, are invariant under the quantum Fourier transform (QFT). Thus the entropic uncertainty of random quantum states has balanced Shannon entropies for the computational basis and the QFT basis. By calculating the Shannon entropy for random quantum states and the Wasserstein distances for the eigenvalues of random quantum circuits, we show that the cutoff phenomenon occurs for the random quantum circuit. It is also demonstrated that the Dyson-Brownian motion for the eigenvalues of a random unitary matrix as a continuous random walk exhibits the cutoff phenomenon. The results here imply that random quantum states could be generated with shallow random circuits.

1. Introduction

How many shuffles are enough to ensure that a deck of 52 cards is mixed randomly? The answer is $\frac{3}{2}\log_2 52$, approximately 8.55, for the riffle shuffling case, as shown by Aldous and Diaconis [1] and by Bayer and Diaconis [2]. Fewer than this number are not enough to mix the deck of cards and more do not significantly improve the randomness. This non-asymptotic convergence to a steady or equilibrium state is called the cutoff phenomenon [3] and has been discovered in various fields. Some finite Markov chains exhibit the cutoff phenomenon. These include the Ehrenfest urn model as a simplified diffusion model [4], random walks on a hypercube [5], some Metropolis algorithms [3], Glauber dynamics of Ising models [6], and certain quantum Markov chains [7].

The card shuffling problem is considered a random walk on the symmetric group S_{52}. The cutoff phenomenon occurs also for random walks on a compact Lie group. Rosenthal [8] considered that random walk on the special orthogonal group SO(N) given by repeated rotations by a fixed angle through randomly chosen planes. Rosenthal showed that the random walk on SO(N), after $1/(2(1-\cos\theta))N\log N + cN$ rotations with a fixed angle θ and a constant c, converges rapidly to the Haar measure in total variation distance. Porod [9, 10] showed that random walks on O(N), U(N), and Sp(N) given by random reflections converge to Haar measure in the total variation distances and the cutoff phenomena occurs at $\frac{1}{2}N\log N$ steps.

Random circuit sampling is a task to sample bit-strings from a probability distribution defined by random quantum circuits, and considered a good candidate to demonstrate quantum advantage with noisy-intermediate scale quantum computers. In 2019, it was implemented on the Sycamore processor with 53 qubits [11] and recently on the Zuchongzhi processor with 56 and 60 qubits [12, 13]. In both quantum computations, the random circuit was implemented by applying repeatedly, up to 20 and 24 cycles, randomly-chosen single qubit gates and the two-qubit gate acting on the nearest neighbor qubits. The

number of cycles plays the same role as the number of times a deck of cards is shuffled or the number of random rotations on Lie groups. So it is natural to ask the same questions which have been answered for the card shuffling problem. How many depths of random quantum circuits, i.e. the number of cycles, are needed to obtain a Haar-measure random unitary operator or to transform an initial quantum state into a pure random quantum state? Does the cutoff phenomenon occur? What is going on in a system after a steady state has been reached? Is there any tool to measure the closeness to a steady state in addition to the total variance distance? In this paper, we present partial answers to these questions using the random circuit implemented on the Sycamore processor and a time-dependent random Hamiltonian model. The former is considered a discrete random walk on a unitary group and the latter a continuous random walk called the Dyson-Brownian motion for eigenvalues of a unitary operator. A pure random quantum state at the steady state will be analyzed with the Shannon entropy. Instead of the total variation distance $||\mu_k - \mu_{\mathrm{Haar}}||_{\mathrm{TV}}$ between the probability distribution μ_k at the kth time step and the Haar measure distribution μ_{Haar}, we employ the Wasserstein distance for the distribution of eigenvalues of a unitary operator.

The paper is organized as follows. In section 2, we will discuss the cutoff phenomenon for random quantum circuits by calculating the Shannon entropy and the Wasserstein distance. We show that the Shannon entropy of a random quantum state is invariant under the quantum Fourier transform (QFT). We discuss the entropic uncertainty relation of random quantum states for the computational basis and the QFT basis. In section 3, we investigate the cutoff phenomenon of the Dyson-Brownian motion generated by a time-dependent random Hamiltonian. Finally, in section 4, we will summarize the result and present the discussion.

2. Cutoff phenomenon for random quantum circuits

Let us begin with the introduction to the random quantum sampling implemented on the Sycamore quantum processor and on the Zuchongzhi quantum processor [11, 12]. The task is to sample bit-strings $x = a_1 a_2 \cdots a_n \in \{0, 1\}^n$ from the probability $p(x) = |\langle x| U |0\rangle^{\otimes n}|^2$ given by a random quantum circuit U acting on n qubits where $|0\rangle^{\otimes n} = |0_1 \cdots 0_n\rangle$ is the initial state and $|x\rangle \equiv |a_1 a_2 \cdots a_n\rangle$ is a computational basis. The random quantum circuit U implemented on both the Sycamore and Zuchongzhi processors is given by repeatedly applying random unitary operators U_k and finally the single-qubit gates S before the measurement

$$U = S U_m \cdots U_2 U_1, \tag{1}$$

where each random quantum circuit U_k is composed of single-qubit gates S chosen randomly from the set $\{\sqrt{X}, \sqrt{Y}, \sqrt{W}\}$ on all qubits and two-qubit gates on the pair of qubits selected in the sequence of the coupler activation patterns of a two-dimensional array of qubits. Millions of bit-strings were sampled from the Sycamore and Zuchongzhi processors. The distributions of bit strings obtained from these noisy quantum processors are deviated from the ideal distribution. Oh and Kais [14–16] investigated this deviation using the random matrix theory and the Wasserstein distances.

Equation (1) is considered random walks or random rotations on a unitary group. If the number of cycles k is large, $U^{(k)} \equiv U_k \cdots U_1$ would approach a random unitary operator U_{Haar} sampled from the Haar probability measure on a unitary group $\mathrm{U}(2^n)$. Typically, the convergence to a stationary state is measured by the total variation distance $||\nu^{*(k)} - \mu_{\mathrm{Haar}}||_{\mathrm{TV}}$ where $\nu^{*(k)}$ is the distribution of the random walk at step k and μ_{Haar} is the Haar measure [8–10]. For the Sycamore processor, the sub-linear convergence, the depth proportional to $\sqrt{n}$, was claimed by calculating the average entropy of random quantum states [17]. Emerson *et al* [18] studied a pseudo-random circuit given by repeated applications of n single-qubit random gates sampled from the Haar measure on $\mathrm{U}(2)$ and simultaneous two-qubit interactions. Moreover, Emerson *et al* employed the measure of entanglement for a multipartite system as the measure of the convergence. It was shown that this random quantum circuit converges to the Haar measure if the circuit depth m is larger than $m_c \equiv \mathcal{O}(n^3 N^2)$ with $N = 2^n$. This is larger than the cutoff step $k_c \equiv \frac{1}{2} N \ln N = \mathcal{O}(nN)$ for random rotations or random reflections on Lie groups shown by Rosenthal [8] and Porod [9, 10].

Different measures have been used to quantify the convergence to the Haar measure distribution, and give rise to the different cutoff steps. Here, we employ the Shannon entropy for quantum states and the Wasserstein distance between the eigenvalue distribution of a random unitary operator sampled from the Haar measure and those of random quantum circuits. Random unitary matrices drawn from the Haar measure on a unitary group are called the circular unitary ensemble. The properties of random quantum states and the eigenvalue distribution of the circular unitary ensemble are well known from the random matrix theory [19].

Let us first investigate how close a quantum state at the kth step, $|\psi^{(k)}\rangle = R^{(k)} |0\rangle = U_k \cdots U_1 |0\rangle$, is to a random quantum state, a stationary state of random walks on a unitary group. An immediate question is

what a pure random quantum state is and how to generate it. A random pure state can be generated in several ways, that is, there are several ways of drawing a random unitary operator from the Haar measure [20–22]. A random unitary operator could be sampled from the Haar measure through the Euler angle method or the QR decomposition of a complex Gaussian random matrix. Basically, a random quantum state $|\psi\rangle = \sum_{i=0}^{N-1} a_i |i\rangle$ can be viewed as a random vector on the $(2N-1)$ sphere and expansion coefficients $a_i = x_i + iy_i$ are drawn from the normal distributions, i.e. $x_i, y_i \sim \mathcal{N}(0,1)$. The distribution $P = \{p_1, p_2, \ldots, p_{N-1}\}$ of probabilities $p_i = |a_i|^2$ of a random quantum state obeys the χ^2 distribution with 2 degree of freedom [19]

$$\Pr(p) = (N-1)(1-p)^{N-2}. \tag{2}$$

The χ^2 distribution for P of p_i of random quantum states makes it possible to calculate the average Shannon entropy. The Shannon entropy for the probability distribution $P = \{p_1, p_2, \ldots, p_{N-1}\}$ is

$$H(P) = H(|\psi\rangle) = -\sum_{i=0}^{N-1} p_i \ln p_i, \tag{3}$$

where $\sum_i p_i = 1$ and $p_i = |a_i|^2$. The Shannon entropy $H(|\psi\rangle)$ for a quantum state measures the amount of uncertainty or the concentration of $P = (p_0, \ldots, p_{N-1})$. The average Shannon entropy over random quantum states can be calculated with equations (2) and (3) and is given by

$$\langle H(|\psi\rangle)\rangle = \ln N - 1 + \gamma, \tag{4}$$

where $\gamma \approx 0.5772$ is the Euler constant and $\langle \cdots \rangle$ is the average over random quantum states. So the Shannon entropy of a quantum state could be used as a measure of convergence of random walks on a unitary group.

Note that the Shannon entropy $H(|\psi\rangle)$ is defined with respect to a specific basis set $\{|i\rangle\}$. If the same quantum state is expanded in terms of another basis set $\{|k\rangle\}$, $|\psi\rangle = \sum_{k=0}^{N-1} b_k |k\rangle$, its Shannon entropy $H(|\psi\rangle)$ will change. For two orthonormal basis sets, $\{|i\rangle\}$ and $\{|k\rangle\}$, the entropic uncertainty relation [24–29] is written as
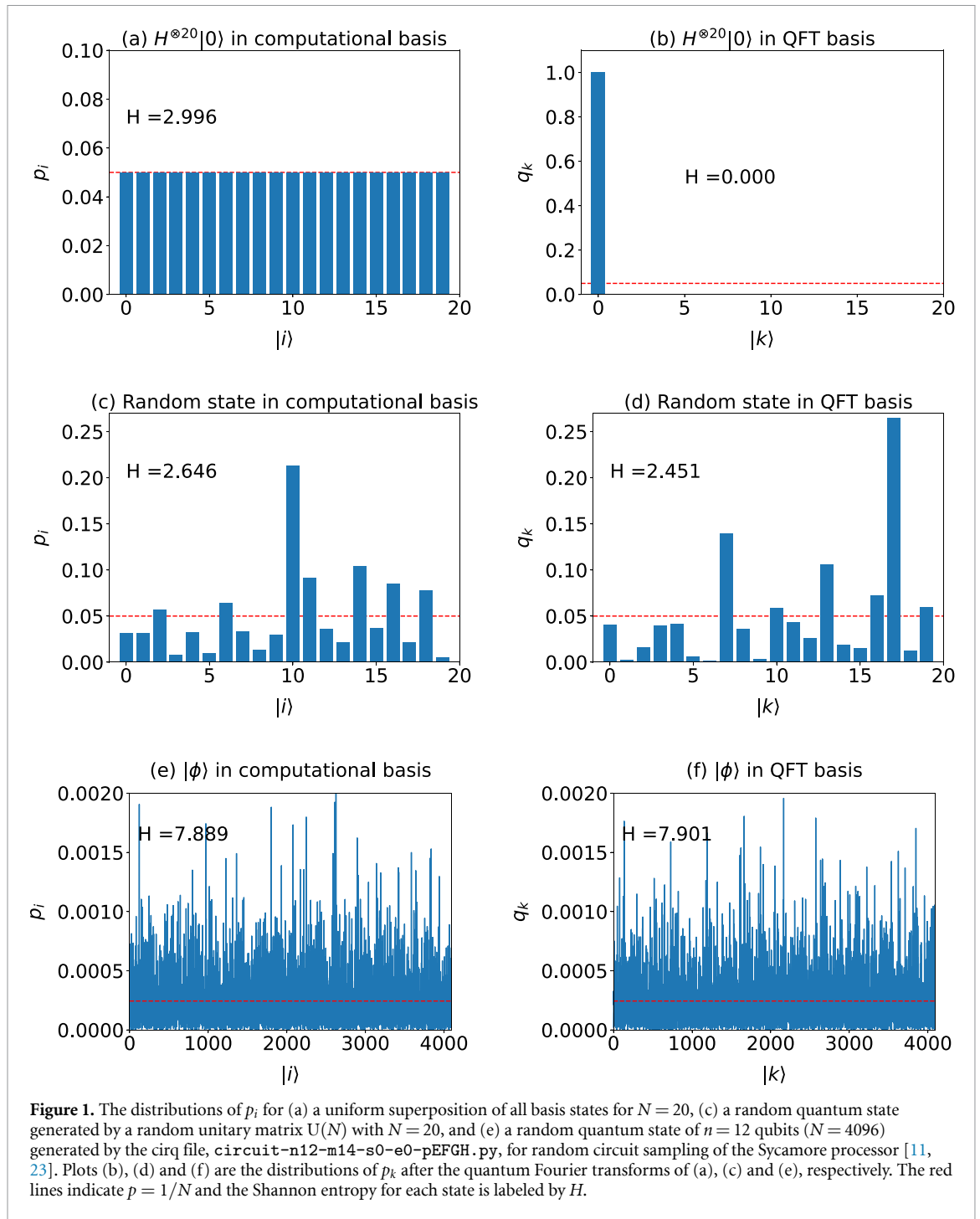
$$H(P) + H(Q) \geqslant -2\ln c \tag{5}$$

where $c = \max|\langle i|k\rangle|$, $P = (p_0, \ldots, p_{N-1})$ with $p_i = |a_i|^2$, and $Q = (q_0, \ldots, q_{N-1})$ with $q_k = |b_k|^2$. We consider the computational basis and the quantum Fourier transformed basis, which are mutually unbiased. The QFT is the discrete Fourier transform of the amplitude vector $(x_0, x_1, \ldots, x_{N-1})$ to another amplitude vector $(y_0, y_1, \ldots, y_{N-1})$, defined by

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{i2\pi \frac{jk}{N}} x_j. \tag{6}$$
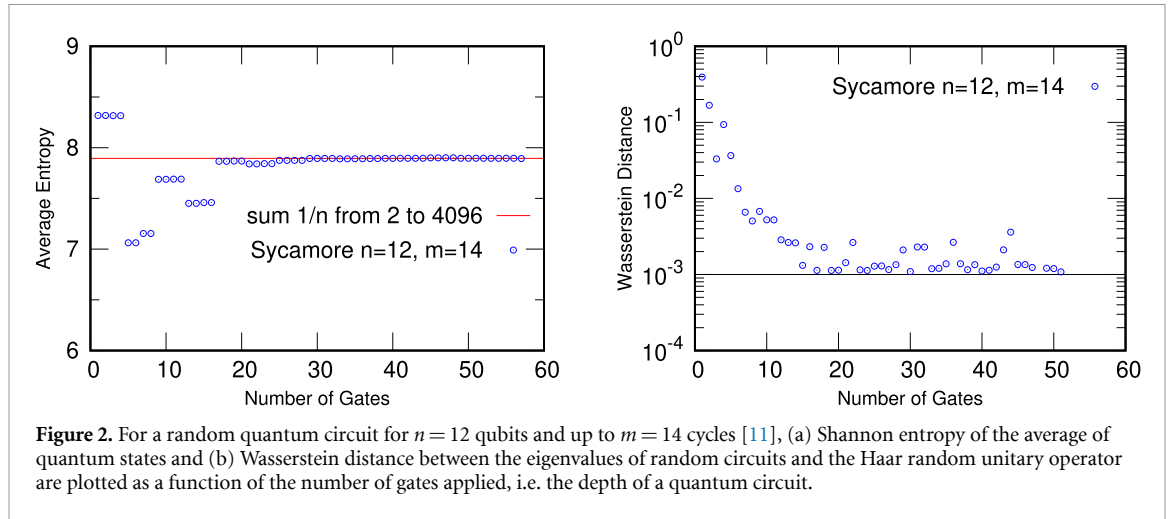
The QFT acting on $|\psi_P\rangle$ is written as

$$|\psi_P\rangle = \sum_{i=0}^{N-1} x_i |i\rangle \quad \longrightarrow \quad |\psi_Q\rangle = \sum_{k=0}^{N-1} y_k |k\rangle. \tag{7}$$

Figure 1 illustrates the distributions of probabilities p_i for two kinds of quantum states in the computational basis and probabilities q_k in the QFT basis. First, consider a uniform superposition of all possible basis states in the computational basis that is given by $|\psi\rangle = \frac{1}{\sqrt{N}}(|0\rangle + |1\rangle + \cdots + |N-1\rangle)$. As shown in figure 1(a), its p_i is distributed uniformly, $p_i = 1/N$ with $i = 0, 1, \ldots, N-1$ and its Shannon entropy has the maximum value, $H(P) = \ln(N)$. The equally-likely distribution among N possible states implies the largest randomness, and the greatest entropy [30]. However, $|\psi\rangle$ in the QFT basis set is localized at one site, so its entropy $H(Q)$ is zero, as depicted in figure 1(d). The entropic uncertainty is given by $H(P) + H(Q) = \ln(N)$. Next, consider a random quantum state $|\phi\rangle = U_{\text{Haar}}|0\rangle$. Figure 1(b) plots the distribution of p_i of a random quantum state where U_{Haar} is generated by the QR decomposition of an $N \times N$ complex Gaussian random matrix. The entropy of a random quantum state is approximately given by $H(P) = \ln N - 1 + \gamma \approx 2.573$ for $N = 20$. Figure 1(e) plots the distribution of q_k in the QFT basis. Interestingly, *the entropy $H(P)$ of a random quantum state in the computational basis is almost equal to its entropy $H(Q)$ in its QFT basis.* We observe that the average entropy for all random quantum states in the computational basis, generated by a random circuit U, is equal to that in the QFT basis. A random quantum state may have the balanced entropic uncertainty, $H(P) = H(Q) = \ln N - 1 + \gamma$. It is analogous to a coherent

Figure 1. The distributions of p_i for (a) a uniform superposition of all basis states for $N = 20$, (c) a random quantum state generated by a random unitary matrix U(N) with $N = 20$, and (e) a random quantum state of $n = 12$ qubits ($N = 4096$) generated by the cirq file, `circuit-n12-m14-s0-e0-pEFGH.py`, for random circuit sampling of the Sycamore processor [11, 23]. Plots (b), (d) and (f) are the distributions of p_k after the quantum Fourier transforms of (a), (c) and (e), respectively. The red lines indicate $p = 1/N$ and the Shannon entropy for each state is labeled by H.

state in the sense that the latter has balanced or symmetric minimum uncertainty: $\Delta x = \Delta p$. It may be interesting to understand why a random quantum state is invariant under the QFT. Figure 1(c) depicts the distribution of p_i for a random quantum state generated by a random quantum circuit implemented on the Sycamore processor for $n = 12$ and the cycles $m = 14$ [23]. Figure 1(f) plots the distribution of q_k in the QFT basis. One can see that the Shannon entropy of a random quantum state in the computational basis is almost same as that of its QFT state. Note that the random circuit here is implemented on a classical computer without any noise. The Shannon entropy in figure 1(e) is close to the theoretical value,
$H = \ln N - 1 + \gamma \approx 7.8949$. However, the Sycamore processor is noisy so the Shannon entropy of the probabilities constructed with bit-strings of the Sycamore processor for $n = 12$ and $m = 14$ is $H \approx 8.217$ and close to $\ln(4096) \approx 8.31$ [31]. A quantum state evolved by a random circuit on the Sycamore processor is close to that of a mixed state.

Since a random quantum state is characterized by its Shannon entropy, $H(P) \approx \ln N - (1 - \gamma)$, the Shannon entropy $H(|\psi^{(k)}\rangle)$ of a quantum state $|\psi^{(k)}\rangle = U_k \dots U_1 |0\rangle$ at the kth step of random walks could

Figure 2. For a random quantum circuit for $n = 12$ qubits and up to $m = 14$ cycles [11], (a) Shannon entropy of the average of quantum states and (b) Wasserstein distance between the eigenvalues of random circuits and the Haar random unitary operator are plotted as a function of the number of gates applied, i.e. the depth of a quantum circuit.

be used as a convergence measure to see whether the cutoff phenomenon happens. The sub-linear convergence proportional to $\sqrt{n}$ was claimed by calculating the average entropy of quantum states [17]. As shown in figure 2(a), the Shannon entropy of a quantum state converges to $\ln N - (1 - \gamma)$ as the number of gates increases and remains there. An interesting question is what happens to a quantum state after the Shannon entropy converges.

The eigenvalue distribution for random unitary operators drawn from the Haar measure is well known [21], so the distance between the eigenvalue distributions could be used to measure the convergence of a random walk. We consider the Wasserstein distance defined by

$$W_p(P, Q) = \left(\inf_{J \in J(P,Q)} \int ||x - y||^p \, dJ(x, y) \right)^{1/p}, \tag{8}$$

where $\mathcal{J}(P, Q)$ denotes all joint distributions $J(P, Q)$. If P and Q are the empirical distributions of a data set $\{x_1, \ldots, x_n\}$ and $\{y_1, \ldots, y_n\}$ respectively, then the Wasserstein distance is given by the distance between order statistics

$$W_p(P, Q) = \left(\sum_{i=1}^{n} ||x_{(i)} - y_{(i)}||^p \right)^{1/p}, \tag{9}$$

where $x_{(i)}$ is the ith order statistic of a samples, i.e. its ith smallest value. Figure 2(b) plots the Wasserstein distance of order 1 between the eigenvalue distribution of the circular unitary ensemble and that of a random quantum circuit as a function of the number of quantum gates applied. The calculation of the Wasserstein distance supports the cutoff phenomenon for random quantum circuits as the Shannon entropy does.

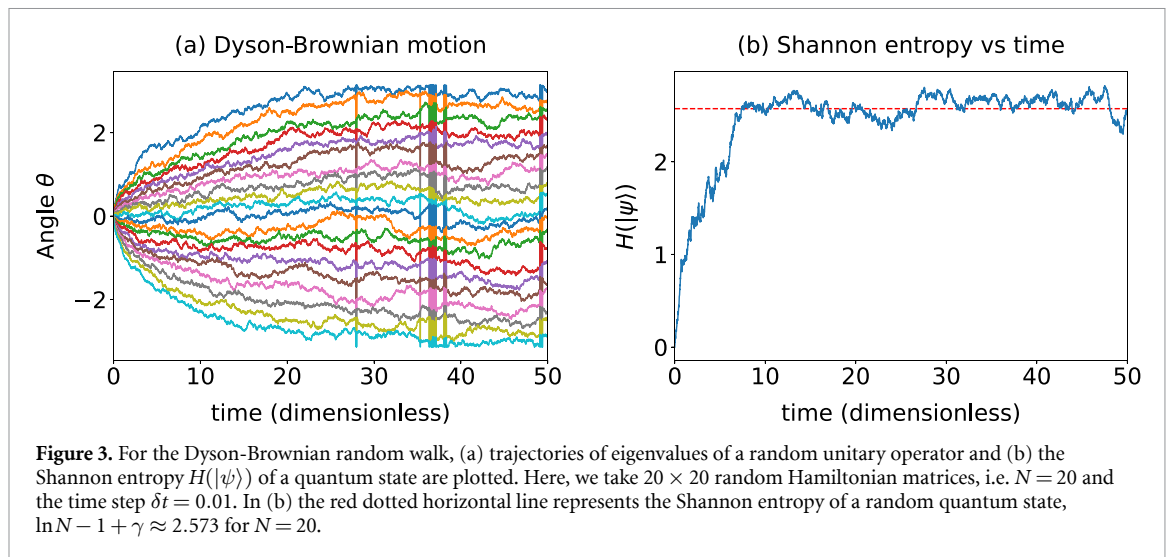## 3. Dyson-Brownian motions on a unitary group

In section 2, the random walk on the unitary group is implemented by applying the sequence of random quantum circuits, $\{U_1, U_2, \ldots\}$. A random quantum state after the kth step is $|\psi\rangle = U_k \ldots U_1 |0\rangle$. This may be considered as a discrete process. In this section, we consider a continuous random walk given by a time-dependent random Hamiltonian to see how quickly a quantum state converges to a random quantum state. The time evolution operator at $t + \delta t$ is given by

$$U(t + \delta t) = e^{i \frac{\delta t}{\hbar} H(t)} U(t) \tag{10}$$

$$\approx \left[1 + i \frac{\delta t}{\hbar} H(t) - \frac{1}{2} \left(\frac{\delta t}{\hbar} \right)^2 H^2(t) \right] U(t), \tag{11}$$

where $U(0) = I$. The time dependent random Hamiltonian $H(t)$ at time t is obtained as follows. We draw a complex random matrix A whose real and imaginary parts of a matrix element A_{ij} are sampled independently from the normal distribution $\mathcal{N}(0, \sigma^2/2N)$ with the variance $\sigma^2/2N$. The Hermitian property of the Hamiltonian H is fulfilled by summing A and its conjugate transpose $A^\dagger$, $H = \frac{1}{2}(A + A^\dagger)$. H is the elements of the Gaussian orthogonal ensemble.

The trajectories of eigenvalues of a random unitary operator U are known as the Dyson-Brownian motions and do not overlap with others. Eigenvalues repel each other. We simulate the time evolution with a

Figure 3. For the Dyson-Brownian random walk, (a) trajectories of eigenvalues of a random unitary operator and (b) the Shannon entropy $H(|\psi\rangle)$ of a quantum state are plotted. Here, we take 20×20 random Hamiltonian matrices, i.e. $N = 20$ and the time step $\delta t = 0.01$. In (b) the red dotted horizontal line represents the Shannon entropy of a random quantum state, $\ln N - 1 + \gamma \approx 2.573$ for $N = 20$.

time-dependent random Hamiltonian for $N = 20$ and $\sigma = 1$ so $\sigma^2/2N = 1/2N$. For simplicity, we take $\hbar = 1$. We set the time step $\delta t = 0.01$. The eigenvalues of $U(t)$ from equation (11) are obtained by diagonalizing it and their trajectories as a function of time are plotted in figure 3(a). The time-evolution of the Shannon entropy of a quantum state $|\psi(t)\rangle = U(t)|0\rangle$ is shown in figure 3(b). We observe the non-asymptotic convergence to $\ln N - 1 + \gamma \approx 2.573$ for $N = 20$. It is interesting to see the eigenvalues and the Shannon entropy fluctuate after arriving at the steady state. Particularly, the fluctuation in the Shannon entropy in figure 3(b) is in contrast to no fluctuation in the Shannon entropy for a finite random walk of a random quantum circuit, shown in figure 2(a).

4. Summary

In this paper, we examined some properties of random quantum states generated by discrete and continuous random walks on a unitary group. It is found that the Shannon entropy of a random quantum state generated by random quantum circuits is invariant under the QFT in the sense that the Shannon entropy does not change before and after applying the QFT. The entropic uncertainty relation of a random quantum state for the computational basis and the QFT basis is balanced, i.e. $H(P) = H(Q)$. This may remind us of the coherent state with the balanced minimum uncertainty relation, $\delta x = \delta p$. While it is not clear why the Shannon entropy of a random quantum state is invariant under the QFT, it may be due to the invariance of Haar measure. Also, we showed that the cutoff phenomenon for a random quantum circuit occurs by calculating the Shannon entropy and the Wasserstein distance for the eigenvalue distributions. It is a open question whether the cutoff of random walks on a unitary group scales with the number of qubits n as sub-linear $\mathcal{O}(\sqrt{n})$ or $\mathcal{O}(n2^n)$ while the numerical calculations here seem to support the sub-linear scaling of the cutoff.

In addition to the demonstration of quantum advantage, random quantum circuits may be applicable to solving interesting problems, for example, in randomized linear algebra. The set of random quantum states $|\psi_i\rangle = U_{\text{Haar}}|i\rangle$ with $i = 0, 1, \ldots, 2^n - 1$ form the orthonormal basis set. The trace of a matrix A could be calculated using $\text{Tr}(A) \approx \frac{1}{M}\sum_{i=1}^{M}\langle\psi_i|A|\psi_i\rangle$ where $|\psi_i\rangle$ is a random quantum state [31].

Data availability statement

All data that support the findings of this study are included within the article (and any supplementary files).

ORCID iD

Sabre Kais ⓘ https://orcid.org/0000-0003-0574-5346

References

[1] Aldous D and Diaconis P 1986 *Am. Math. Mon.* **93** 333–48
[2] Bayer D and Diaconis P 1992 *Ann. Appl. Probab.* **2** 294–313
[3] Diaconis P 1996 *Proc. Natl Acad. Sci.* **93** 1659–64
[4] Ehrenfest P and Ehrenfest-Afanassjewa T 1907 *Über zwei bekannte Einwände gegen das Boltzmannsche H-Theorem* (Hirzel)
[5] Diaconis P, Graham R L and Morrison J A 1990 *Random Struct. Algorithms* **1** 51–72
[6] Lubetzky E and Sly A 2013 *Invent. Math.* **191** 719–55
[7] Kastoryano M J, Reeb D and Wolf M M 2012 *J. Phys. A: Math. Theor.* **45** 075307
[8] Rosenthal J S 1994 *Ann. Probab.* **22** 398–423
[9] Porod U 1996 *Ann. Probab.* **24** 74–96
[10] Porod U 1996 *Probab. Theory Relat. Fields* **104** 181–209
[11] Arute F *et al* 2019 *Nature* **574** 505–10
[12] Wu Y *et al* 2021 *Phys. Rev. Lett.* **127** 180501
[13] Zhu Q *et al* 2022 *Sci. Bull.* **67** 240–5
[14] Oh S and Kais S 2022 *J. Phys. Chem. Lett.* **13** 7469–75
[15] Oh S and Kais S 2022 *Phys. Rev.* A **106** 032433
[16] Oh S and Kais S 2023 *Phys. Rev.* A **107** 022610
[17] Boixo S, Isakov S V, Smelyanskiy V N, Babbush R, Ding N, Jiang Z, Bremner M J, Martinis J M and Neven H 2018 *Nat. Phys.* **14** 595–600
[18] Emerson J, Weinstein Y S, Saraceno M, Lloyd S and Cory D G 2003 *Science* **302** 2098–100
[19] Haake F, Gnutzmann S and Kuś M 2010 *Quantum Signatures of Chaos* (Springer)
[20] Mezzadri F 2007 *Notice of Am. Math. Soc.* **54** 592–604
[21] Meckes E S 2019 *The Random Matrix Theory of the Classical Compact Groups Cambridge Tracts in Mathematics* (Cambridge University Press)
[22] Ozols M 2009 Unpublished essay on http://home.lu.lv/sd20008
[23] Martinis *et al* 2022 Quantum supremacy using a programmable superconducting processor *Dryad, Dataset* https://doi.org/10.5061/dryad.k6t1rj8
[24] Deutsch D 1983 *Phys. Rev. Lett.* **50** 631–3
[25] Kraus K 1987 *Phys. Rev.* D **35** 3070–5
[26] Maassen H and Uffink J B M 1988 *Phys. Rev. Lett.* **60** 1103–6
[27] Coles P J, Berta M, Tomamichel M and Wehner S 2017 *Rev. Mod. Phys.* **89** 015002
[28] Ming F, Wang D, Fan X G, Shi W N, Ye L and Chen J L 2020 *Phys. Rev.* A **102** 012206
[29] Xie B F, Ming F, Wang D, Ye L and Chen J L 2021 *Phys. Rev.* A **104** 062204
[30] Ambegaokar V and Clerk A A 1999 *Am. J. Phys.* **67** 1068–73
[31] Oh S and Kais S Estimating trace of a matrix with random quantum states (in preparation)