

The principle of majorization: application to random quantum circuits

Raúl O. Vallejos* and Fernando de Melo†

Centro Brasileiro de Pesquisas Físicas (CBPF), Rua Dr. Xavier Sigaud 150, 22290-180 Rio de Janeiro, Brazil

Gabriel G. Carlo‡

Departamento de Física, Comisión Nacional de Energía Atómica,
Avenida del Libertador 8250, (1429) Buenos Aires, Argentina

(Dated: February 22, 2021)

We test the principle of majorization [J. I. Latorre and M. A. Martín-Delgado, Phys. Rev. A **66**, 022305 (2002)] in random circuits. Three classes of circuits were considered: (i) universal, (ii) classically simulatable, and (iii) neither universal nor classically simulatable. The studied families are: {CNOT, H, T}, {CNOT, H, NOT}, {CNOT, H, S} (Clifford), matchgates, and IQP (instantaneous quantum polynomial-time). We verified that all the families of circuits satisfy on average the principle of decreasing majorization. In most cases the asymptotic state (number of gates $\rightarrow \infty$) behaves like a random vector. However, clear differences appear in the *fluctuations* of the Lorenz curves associated to asymptotic states. The fluctuations of the Lorenz curves discriminate between universal and non-universal classes of random quantum circuits, and they also detect the complexity of some non-universal but not classically efficiently simulatable quantum random circuits. We conclude that majorization can be used as an indicator of complexity of quantum dynamics, as an alternative to, e.g., entanglement spectrum and out-of-time-order correlators (OTOCs).

PACS numbers: 03.67.-a, 03.67.Lx,

I. INTRODUCTION

Majorization is a mathematical concept that allows one to decide whether a probability distribution is more disordered/spread than another. Offering an answer to such a fundamental question, the notion of majorization has found applications in many fields of social and natural sciences [1]. The first known use of the majorization notion dates back to the beginning of the twentieth century, and it is due to the economist Max Otto Lorenz who used it as a measure for wealth concentration [2].

Within physics and information theory, the concept of majorization precedes that of entropy. If a probability distribution associated to a random variable X majorizes the probability distribution of a random variable Y (see definition in Sec. II), then the (Shannon) entropy of Y is bigger than that of X . However, the reverse statement is not necessarily true: if the entropy of Y is bigger than that of X , it is not necessarily the case that X majorizes Y . The majorization relation is thus a finer criteria to compare the spread of probability distributions than the entropy comparison [3]. With that in mind, Ruch and collaborators proposed a stronger version of the second law of thermodynamics, known as the *principle of increasing mixing character* [3–5]: the time development of a statistical ensemble of isolated systems proceeds in such a way that the probability distributions at earlier times majorize those at later times.

As expected, this intuition remains true in the quantum arena, with the majorization concept also playing an important role in quantum and nano thermodynamics (see, e.g., [6–

10]). Within quantum information theory, Nielsen & Vidal's theorem [11] asserts that majorization determines the possible transformations between bipartite entangled states by means of local operations and classical communication. One recent example related to quantum computation: in the context of boson sampling [12], Chin and Huh explained quantitatively that the complexity of the computation relates to the majorization ordering of the input and output particle-distribution vectors [13].

While generic dynamics proceeds in the direction of growing disorder, Orús et al noticed that in many quantum algorithms the opposite is true: in the course of the computation the state of the system is step-by-step majorized, with the final result being maximally ordered [14, 15]. Later on, by carrying a systematic analysis of a variety of quantum algorithms, these authors concluded that fast and efficient algorithms (quantum Fourier transform, Grover's algorithm, the algorithm for the hidden affine function problem, and others) obey a *majorization principle* (MP), i.e., satisfy step-by-step majorization. Supporting this conjecture, they gave examples of some quantum algorithms not showing any computational speed-up which violate the MP [16]. Further evidence supporting the MP came from adiabatic algorithms [17]. Recently step-by-step majorization for the Fourier Transform was observed experimentally in photonic circuits [18]. A detailed analysis of the Grover algorithm can be found in [19].

In recent years random quantum circuits have grown in importance. Besides various applications in quantum information and communication [20–22], random quantum circuits are becoming the test-bed for the so called quantum advantage. Even within the noisy intermediate scale quantum (NISQ) era, when quantum computers are composed of around hundred qubits and are still not amendable to error correction, sampling from random quantum circuits was proved a hard task for classical simulations [23, 24], and as such it is

* vallejos@cbpf.br

† fmelo@cbpf.br

‡ carlo@tandar.cnea.gov.ar

a clear demonstration of quantum advantage. Using random quantum circuits of 53 qubits, such quantum advantage was experimentally reported in Ref. [25].

To determine properties of quantum random circuits that help to characterize their “complexity” is thus an important task. Recently, in a series of articles [26–28], it was established an apparent connection between the entanglement spectrum statistics of the output of a random circuit and its complexity – as defined by the universality of the gate set determining ensemble. More concretely, let \mathcal{G} be a set of quantum gates, and take an ensemble of N qubit quantum circuits formed by uniformly sampling from \mathcal{G} . Initiating the circuit with a random product state, the authors observed that the level spacing statistics for the entanglement spectrum (the Schmidt values of the balanced partition) at the end of the circuit follows the random matrix theory (RMT) prediction if \mathcal{G} forms a universal set of gates, and a Poissonian distribution in the opposite case [27]. The authors go one step further and suggest a connection between the impossibility of returning from a stationary entangled state to a separable state (via a Metropolis like algorithm) and the complexity of the random circuit: universal set of gates would lead to an effectively irreversible entanglement dynamics (when the sequence of gates leading to the stationary state is forgotten).

Another characteristic of complex quantum dynamics is that local information spreads quickly over the whole system. Widely used indicators of this process are the out-of-time ordered correlators (OTOCs): Exponentially fast changes of OTOCs have been taken as a sign of “quantum chaos”, i.e., quantum complexity [29–31].

It is the aim of the present work to analyze the majorization principle in different ensembles of random quantum circuits. Here we show that not only the majorization principle holds (on average) for random circuits, but the fluctuations of cumulant vectors (see below) do seem to correctly identify complex computation. In addition, we show that non-universal but classically non-simulatable quantum circuits might also lead to a RMT entanglement spectrum. Our calculations demonstrate that this intermediate class of circuits can be identified by the majorization criteria.

II. MAJORIZATION & RANDOM CIRCUITS

In the following we define majorization, succinctly describe the various types of quantum random circuits used, and touch upon some related questions.

A. Majorization

Let x and y be real vectors of length N . It is said that x is majorized by y (or y majorizes x), denoted by $x \prec y$, if, for all $k < N$,

$$\sum_{i=1}^k x_i^\downarrow \leq \sum_{i=1}^k y_i^\downarrow, \quad (1)$$

and

$$\sum_{i=1}^N x_i^\downarrow = \sum_{i=1}^N y_i^\downarrow, \quad (2)$$

where x^\downarrow means that the components of x have been arranged in nonincreasing order. The partial sums in the equations above will be called *cumulants*. The k -th cumulant of x will be denoted $F_x(k)$. Here we will always use majorization for comparing probability vectors, i.e., real vectors of non-negative components and normalized to unity: $x_i \geq 0, \forall 1 \leq i \leq N$ and $F(N) = 1$.

A very useful way of visualizing the majorization (partial ordering $x \prec y$ is by plotting the *Lorenz curves* $F_x(k)$ and $F_y(k)$ vs k/N [2]. Then, one has that $x \prec y$ iff the Lorenz curve for y is above the curve for x for all values of k/N . Some examples of Lorenz curves can be seen in Fig. 1. Note that there exist vectors x and y for which neither x majorizes y , nor y majorizes x .

B. The random circuits

We consider unitary quantum circuits with n qubit lines ($n = 8$ in our numerical calculations). The total system dimension, and the dimension of the probability vectors, is thus $N = 2^n$. The system evolution through the quantum circuit is given in unit time steps. Fixed a gate set \mathcal{G} , at each time step a gate from \mathcal{G} is chosen and it is applied to a selected set of qubits. In a quantum *random* circuit the choice of gate to be applied at a given time, and the selection of qubits to which this gate is going to be applied, are both probabilistic – as defined by preset measures. For each step we evaluate the state in the computational basis, the associated probabilities, and the cumulants $F(k)$, $k = 1, \dots, N$. This is repeated for a number N_s of time steps.

We always use completely factorized initial states, i.e., $|\psi\rangle = |\psi_1\rangle \otimes \dots \otimes |\psi_n\rangle$. Each $|\psi_i\rangle$ may be random or a fixed state. In the first case, we chose each factor state independently and uniformly distributed on the Bloch sphere (Haar measure for vectors). Diagonal-gate circuits (IQP) use always $|0\rangle^{\otimes n}$ as input. In some cases we tested both kinds of initial states for a given type of circuit.

Starting from a separable state, the successive application of gates eventually leads to highly entangled states showing statistical properties typical of random vectors. This is clearly true for the universal sets, e.g., $G3$ (see below). Likewise, most families of circuits considered here show a similar behavior. In particular, the Lorenz curves associated to asymptotic (large number of gates) states are very close to those corresponding to random complex vectors. We denote the ensemble of n -qubit states, with the induced Haar measure, as *Haar- n* .

When speaking of classical simulatability of quantum circuits one can distinguish between two main notions: strong (all output probabilities are calculated) or weak (only a sample of the output probability is required). It is said that a simulation by classical means is efficient if it runs in polynomial time

in the input size. The efficiency of a classical simulation may depend on the input type (arbitrary product state or computational basis state), and on how many output lines are measured (single-line or multiline measurement). Other ingredients like intermediate measurements, post-selection, etc., will not be considered. We have given a very compact definition of (efficient) classical simulatability. Thorough definitions may be found in the references: [32–36] (Clifford circuits), [37–39] (IPQ/diagonal circuits), [40–42] (matchgates).

We employed seven classes of circuits: $G1$, $G2$, $G3$, MG , $D2$, $D3$, Dn . They are described in the following three sections.

1. Circuits constructed from a few generators

We considered the three sets used in Ref. [27], i.e., $G1=\{\text{CNOT}, \text{H}, \text{NOT}\}$, $G2=\{\text{CNOT}, \text{H}, \text{S}\}$, and $G3=\{\text{CNOT}, \text{H}, \text{T}\}$, where CNOT is the controlled-NOT gate, H stands for Hadamard, and S and T are $\pi/4$ and $\pi/8$ phase gates, respectively. The set $G3$ is universal and thus approximates the full unitary group $U(N)$ to arbitrary precision. Both sets $G1$ and $G2$ contain only Clifford gates, thus are nonuniversal and classically simulatable (in the setting of the Gottesman-Knill theorem [32, 35]). The circuits constructed from $G2$ generate the Clifford group [32]. The gates in $G1$ generate a subgroup of Clifford, then the simulatability of $G2$ implies the simulatability of $G1$ (in the same settings).

The probability for a gate to be selected at given time is always 1/3 for the four families above. We also choose with equal probability the qubits or pairs of qubits to which a selected gate is applied.

2. Matchgate circuits (MG)

Matchgates are two-qubit gates formed from two one-qubit gates A and B with the same determinant: A acts on the even parity subspace (spanned by $|00\rangle$ and $|11\rangle$) and B acts on the odd parity subspace (spanned by $|01\rangle$ and $|10\rangle$). A and B are randomly chosen according the Haar measure in the unitary group $U(2)$. All pairs of qubits are equiprobable. Circuits of matchgates acting on nearest-neighbor lines only are classically simulatable; however, if the nearest-neighbor restriction is lifted, the resulting circuits are universal for quantum computation [41, 42].

3. Diagonal-gate circuits ($D2$, $D3$, Dn)

These circuits are made up from gates which are diagonal in the computational (Z) basis. The initial state is set to $|0\rangle^{\otimes n}$ and Hadamard gates are placed at the beginning and ending of each line [37]. This class of circuits is also called IQP (instantaneous quantum polynomial-time): As diagonal gates commute, they can be applied simultaneously and thus there is not a natural time ordering of gates for a given circuit.

Diagonal circuits cannot perform universal computation, however, in general, they are not classically simulatable [37, 43].

We shall deal with a particular subclass of diagonal circuits: the r -qubit phase-random circuits [44]. In this case, each gate acts upon r qubits and has the form

$$W_r = \text{diag}\{e^{i\phi_1}, e^{i\phi_2}, \dots, e^{i\phi_{2^r}}\}, \quad (3)$$

with the ϕ 's independent random uniform in $[0, 2\pi)$. The gates are applied on all combinations of r (out of n) qubits, the ordering being random. Here we use only three values for r , namely $r = 2, 3, n$. For $r = 2$ the circuits contain $n(n-1)/2$ gates, while for $r = n$ the circuits consist of only one random gate. So, our diagonal circuits have a well defined number of gates. On the contrary, $G1$, $G2$, $G3$ and MG may have an arbitrary length.

In the case $r = 2$ we also consider the situation of gates acting on nearest-neighbor qubits. Assuming a ring topology, these circuits contain only n gates, and they are classically simulatable [39].

C. Abbreviations

As we are considering various types of circuits, connectivity, and initial states, for the sake of compactness, we shall employ abbreviations to designate the different possibilities. To a triplet {circuit, connectivity, initial state} we shall associate the word $A-B-C$. A stands for the type of circuit: $G1$, $G2$, $G3$, MG , $D2$, $D3$, Dn ; B may equal nn (nearest neighbor), m (random neighbors), or all (all combinations of r qubits –only for diagonal circuits); and C may be rs (random initial state) or 0 ($|0\rangle^{\otimes n}$ as input).

For instance, $MG-mn-rs$, denotes a circuit composed from matchgates acting on arbitrary neighbors, with random initial state. Analogously, $D3-all-0$ denotes a diagonal 3-qubit random phase circuit.

Before proceeding with the numerical calculations, we note that, for our purposes, the various families of circuits to be analyzed can be split into three categories: (i) universal, (ii) classically simulatable, and (iii) neither universal nor classically simulatable. We shall try to correlate the different features in our calculations with these three classes.

III. NUMERICAL CALCULATIONS

We start by giving an example of Lorenz curves for a particular realization of a circuit $G1$ and a random initial state. In Fig. 1(a) we plot a set of Lorenz curves for different times. We see that, as time grows, there is an overall tendency to decreasing majorization. For example, if x_t denotes the probability vector at time t , then we have $x_0 \succ x_{25} \succ x_t$, for $t = 50, 75, 100, \dots$. However, there are cases of increasing majorization (curve swapping, e.g., $x_{125} \prec x_{150}$) as well as cases of no definite majorization order (curve crossing, e.g., x_{75} and x_{100}). We have observed analogous behavior for other

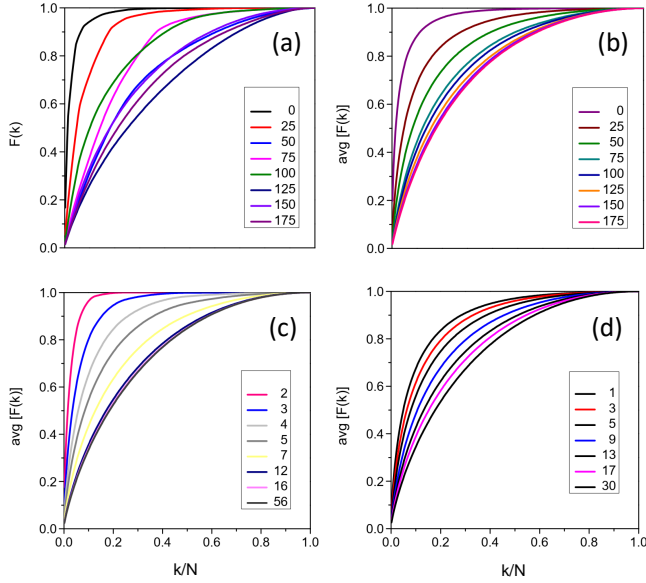


FIG. 1. (a) Lorenz curves for a single realization of a circuit belonging to the family $GI = \{\text{CNOT}, \text{H}, \text{NOT}\}$. The topmost curve corresponds to the initial state. The other curves were calculated after the action of 25/50/75/100/125/150/175 gates (the color scheme for the different numbers of gates is shown in the inset). (b) Lorenz curves for the family GI but now averaged over 500 realizations. The numbers of gates are the same than in (a). (c) Same as (b) but for diagonal $D3\text{-all-}0$ circuits. The curves were calculated after the application of 2/3/4/5/7/12/16/56 gates. (d) Same as (b) but for matchgates $MG\text{-}m\text{-}rs$ circuits. Number of gates are 1/3/5/9/13/17/30. All circuits have 8 qubit lines.

realizations of GI , and also for circuits belonging to other families.

Not surprisingly, crossings and swappings vanish by averaging over realizations and/or initial conditions, and then majorization order appears. This can be clearly seen in Fig. 1 [panels (b)-(d)], where we exhibit Lorenz curves for selected times, but now averaged over 500 circuits/initial states. Results for families $GI\text{-}m\text{-}rs$, $D3\text{-all-}0$, and $MG\text{-}m\text{-}rs$ are qualitatively similar, all showing decreasing majorization as the number of gates is increased.

Though the rate of change of the Lorenz curves depends of the type of circuit, the asymptotic curves are almost identical. From here on, we focus on the asymptotic Lorenz curves – asymptotic meaning large number of gates for circuits GI , $G2$, $G3$, MG or the maximum number of gates for $D2$, $D3$, Dn .

Figure 2 depicts averages of the asymptotic Lorenz curves for all classes of circuits considered. Most curves coincide (within visual resolution) with that corresponding to random vectors of 8 qubits ($Haar\text{-}8$).

We have verified numerically that the Lorenz curves associated with random vectors tend to a limiting curve, $Haar\text{-}\infty$,

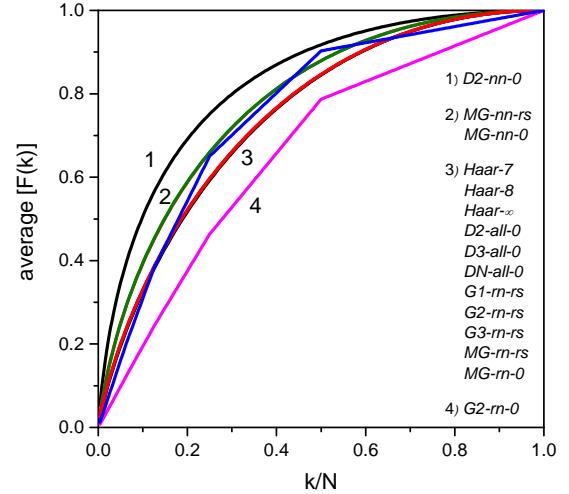


FIG. 2. Average Lorenz curves for asymptotic states generated by various families of random circuits of 8 qubits. For circuits GI , $G2$, $G3$, MG we used 500 gates to ensure convergence. For the diagonal ones, i.e., $D2$, $D3$, Dn , the maximum number of gates was used (see Sec. II B 3). Inset: circuit names ordered to correspond to curve ordering (decreasing majorization), except for $GI\text{-}m\text{-}0$ (broken blue line).

as the dimension increases. In Fig. 2 we see that this limit is reached already for 7 qubits.

Some comments about Fig. 2 are in place. We have also plotted $Haar\text{-}7$ because matchgates preserve the symmetry of the initial state, then, if we start from $|0\rangle^{\otimes n}$, the final states will live in the positive parity subspace. This subspace has dimensionality $2^n/2$, i.e., the final state-vector has $2^n/2$ null components. We discarded these null components, thus considering state-vectors of half the dimension of the initial state. Because of this, results for $MG\text{-}rnd\text{-}0$ and $MG\text{-}nn\text{-}0$ must be compared with $Haar\text{-}7$.

The circuits $D2\text{-}nn\text{-}0$ and $G2\text{-}m\text{-}0$ produce average Lorenz curves which deviate the most from the universal, random vector, behavior (presumably $D2\text{-}nn\text{-}0$ has too few gates for scrambling the initial state). Note that both circuits are classically simulatable under fairly undemanding settings [32, 39]. GI and $G2$ (Clifford) circuits acting on the state $|0\rangle^{\otimes n}$ produce states with highly degenerate amplitudes [34, 45]. Then, the corresponding Lorenz curves are piece-wise linear.

Having seen that average Lorenz curves fail to differentiate universal from nonuniversal families, we decided to look at the *fluctuations* of the Lorenz curves, i.e., the fluctuation of each cumulant $F(k)$ for each class of circuits, averaged over many realizations. The result of this calculation is shown in Fig. 3.

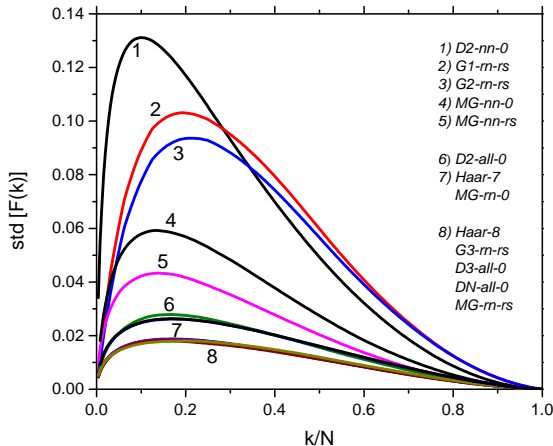


FIG. 3. Fluctuations (standard deviation) of Lorenz curves for asymptotic states generated by various families of random circuits of 8 qubits. For each family we considered 5000 samples of 500 gates, except for diagonal circuits which have fixed lengths. Inset: circuit names. Name ordering corresponds to curve ordering. The families $G1$ - rn -0 and $G2$ - rn -0 show much larger fluctuations; their Lorenz curves are piecewise quadratic (not shown).

Here we observe a larger spread of the Lorenz curves, with a partial removal of the coalescence of Fig. 3: $G1$ and $G2$ (both nonuniversal) have separated off the main group, exhibiting larger fluctuations. The smallest, universal fluctuations correspond to the circuits $G3$ - rn - rs , MG - rn - rs , DN - all -0, $D3$ - all -0 (coincide with $Haar$ -8), and MG - rn -0 (coincides with $Haar$ -7).

The family $D2$ - all -0 stands as a special case because, in spite of showing very small fluctuations does not match the universal prediction for circuits without symmetries, i.e., $Haar$ -8. We return to this point below.

We have verified numerically that the fluctuations corresponding to random vectors decrease as the number of qubits grows (cf. Fig. 3). This raises the questions: What is the associated scaling law? Do the fluctuations of the various families obey different laws? Answering these questions, though a source of potentially valuable information, lays outside of the scope of the present paper.

A. Entanglement spectra

Following [27] we considered a 50-50 bipartition and calculated the spectra of the asymptotic reduced matrices. Let us denote the eigenvalues $\lambda_1, \lambda_2, \dots, \lambda_{N/2}$, in decreasing order. Use the gaps $\epsilon_i = \lambda_{i+1} - \lambda_i$ to form the quotients $r_i = \epsilon_{i+1}/\epsilon_i$. Then construct the histogram $P(r)$ by sampling within each class of circuit. If the distribution of gaps follows a Wigner-Dyson law (characteristic of Gaussian random matrix ensembles [46]), the theoretical prediction for $P(r)$, in the

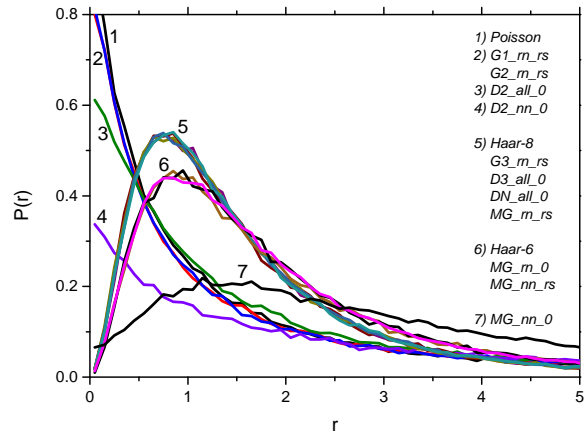


FIG. 4. Entanglement spectra for asymptotic states generated by various families of random circuits. Shown are averages of 5000 circuits of 500 gates. Diagonal circuits have fixed lengths. All circuits have 8 qubits.

limit of large matrices, is [47]

$$P_{\text{WD}}(r) = \frac{1}{Z} \frac{(r+r^2)^\beta}{(1+r+r^2)^{1+3\beta/2}}, \quad (4)$$

where $Z = \frac{8}{27}$ for the Gaussian Orthogonal Ensemble (GOE) with $\beta = 1$, and $Z = \frac{4}{81} \frac{\pi}{\sqrt{3}}$ for the Gaussian Unitary Ensemble (GUE) with $\beta = 2$.

On the other side, if the spectrum is uncorrelated, then the corresponding statistics is Poissonian:

$$P_{\text{Poisson}}(r) = \frac{1}{(1+r)^2}. \quad (5)$$

Given that the circuits considered here do not exhibit time-reversal symmetry, their spectral statistics should follow the predictions of GUE – provided they exhibit complex dynamics. In fact, it was shown in [27] that $P(r)$ for the universal family $G3$ agrees with GUE, i.e., Eq. (4) with $\beta = 2$. On the other side, the families $G1$ and $G2$ showed Poisson-like fluctuations.

Our matrices are not large enough to use the asymptotic expressions above. So, in order to account for finite dimensions effects, we resorted to numerical calculations. In the case of GUE statistics, instead of employing Eq.(4), we used the spectra of reduced density matrices obtained via partial trace of Haar random vectors of n qubits. The results obtained from these spectra will be labeled $Haar$ - n . In the other side, we generated Poissonian spectra simply by choosing $N/2$ levels $\in (0, 1)$ independently and random-uniformly.

We extend the spectral calculations of $P(r)$ in [27] (restricted to $G1$, $G2$ and $G3$) to matchgates and diagonal circuits. In Fig. 4 we show histograms representing $P(r)$ for

all the circuits. We observe that they can essentially be divided into two groups: (a) Poisson-like, i.e., decreasing probability distributions ($G1-rn-rs$, $G2-rn-rs$, $D2-all-0$, $D2-nn-0$), and (b) GUE-like, i.e., peaked histograms. The latter category includes the circuits $G3-rn-rs$, $D3-all-0$, $DN-all-0$, $MG-rn-rs$, which show excellent agreement with the GUE prediction ($Haar-8$), and $MG-rn-0$ which coincides with $Haar-6$ (this was to be expected because $MG-rn-0$ is universal but has parity symmetry [48]).

The spectra corresponding to the families $G1-rn-0$ and $G2-rn-0$ consist of several multiply degenerated levels. Thus, the associated $P(r)$ are singular (nor Poisson- neither GUE-like) and were not plotted.

In the previous sections we have limited ourselves to presenting the results of our calculations, reserving the discussion thereof for the next, concluding section.

IV. DISCUSSION & FINAL REMARKS

The purpose of this paper was to characterize the complexity of quantum random circuits using majorization criteria. The authors of [27] had showed that the entanglement spectrum could be used to distinguish universal from non-universal families of circuits, using as examples the families $G1$, $G2$, $G3$. Here we extended the analysis of [27] in two directions. First, we considered additional families of circuits, i.e., those constructed either from matchgates or diagonal gates.

Second, we inquired about the complexity (according to majorization criteria or entanglement spectrum) of the families that, in spite of being non-universal, cannot be efficiently simulated in a classical computer. We found that some families of diagonal circuits (non-universal) must be classified as complex according to the above mentioned criteria.

After verifying that all circuit families satisfy the principle of decreasing majorization (on average), we focused on the Lorenz curves of the output states. Our results, displayed in Figs. 2, 3, 4, are summarized in Table I. The last two columns exhibit the agreement, for all the circuits, between both complexity indicators considered. Also included in the table are the settings for efficient classical simulatability (fourth column). The third column displays the settings for which a given family is known to be *not* simulatable. Altogether we have considered eight possible settings, corresponding to three binary choices: weak vs strong simulation, single- or multi-line tasks, and the input being either $|0\rangle^{\otimes n}$ or a random product state (the latter information makes part of the circuit name). So, when we state that a family is “always” or “never” simulatable, we mean as far as the eight above-mentioned settings are concerned.

These settings present different degrees of difficulty for efficient classical simulation, ranging from OUT(1)-WEAK (easiest) to OUT(MANY)-STRONG (hardest). Circuit families that are simulatable under the hardest settings are farthest from performing universal quantum computation. Accordingly, these families are expected to deviate most from

the universal behavior described by random matrices/vectors. This correspondence is clearly exemplified by $G2-rn-0$ and $MG-nn-0$, which exhibit the lowest complexity records [both are OUT(MANY)-STRONG simulatable]. In spite of being simulatable under weaker conditions, $MG-nn-rn$ and $D2-nn-0$ also rank as the lowest complex circuits (however, these families might be simulatable in stronger settings [51] [52]).

We have written a clear-cut YES/NO in the last three columns of Table I based on the strict agreement (or not) between our data and the predictions for random outputs. If we descend to the semi-quantitative level, the complexity indicators may become in conflict. For instance, $MG-nn-rs$ [OUT(1)-STRONG simulatable] has indeed a GUE-like spectrum but intermediate-size cumulant fluctuations. On the other side, $D2-all-0$ [OUT(1)-WEAK simulatable] has Poisson-like spectrum, however its fluctuations are close to universal. The case of $MG-nn-0$ [OUT(MANY)-STRONG] is clearer: mildly GUE-like spectrum and large fluctuations. In the previous cases both indicators cooperate to characterize the respective circuit families as not complex.

Some unexpected behaviors, e.g., $MG-nn-rs$ having a spectrum close to GUE, or, $D2-all-0$ having Poisson-like spectrum and small cumulant fluctuations, call for further studies. In particular one should analyze how the cumulant fluctuations decrease as the system size increases. In this respect, it would be very useful to have analytical results for the fluctuations of Lorenz curves in the case of complex random vectors, which seems feasible [53].

We verified that the *fluctuations* of the Lorenz curves qualify as an indicator of complexity, producing essentially the same classification as the entanglement spectrum. Both measures, therefore, not only discriminate between universal and non-universal classes of random quantum circuits, but they also detect the complexity of some non-universal but not classically efficiently simulatable quantum random circuits. It should be noted, however, that the fluctuations of the Lorenz curves are more easily obtained than the entanglement spectrum. The former requires simple evaluation/measurement of the probabilities of the computational basis, while the latter requires full tomography of half the qubits and further diagonalization of the obtained reduced density matrix.

To conclude, we have introduced a criterion based on majorization (fluctuations of Lorenz curves) as an indicator of complexity of quantum computations/dynamics. This indicator is intended to serve as an alternative or complement to the well known entanglement spectrum and OTOCs.

Acknowledgments: We gladly acknowledge fruitful discussions with Andreas Ketterer, Daniel Brod, Eduardo Mucciolo, Ernesto Galvão, Felipe Monteiro, and Tobias Micklitz. We are grateful to E. Mucciolo for providing us with some of the codes used in the numerical calculations. This work is supported by the Brazilian funding agencies CNPq and CAPES, and it is part of the Brazilian National Institute for Quantum Information (INCT-IQ). G.G.C. gratefully acknowledges support from CONICET.

Circuit name	UNIV?	Non classically simulatable?	Classically simulatable?	Ave-H?	Fluc-H?	Spec-RMT?
<i>G3-rn-rs</i>	Yes	Always	Never	Yes	Yes	Yes
<i>G2-rn-rs</i>	No	OUT(MANY) WEAK [35]	OUT(1) STRONG [33]	Yes	No	No
<i>G1-rn-rs</i>	No	(?)	OUT(1) STRONG	Yes	No	No
<i>G2-rn-0</i>	No	Never	OUT(MANY) STRONG [33]	No	No	No
<i>MG-rn-rs</i>	Yes	Always	Never	Yes	Yes	Yes
<i>MG-rn-0</i>	Yes	Always	Never	Yes	Yes	Yes
<i>MG-nn-rs</i>	No	(?)	OUT(1) STRONG [41, 42]	No	No	No*
<i>MG-nn-0</i>	No	Never	OUT(MANY) STRONG [40, 49, 50]	No	No	No
<i>DN-all-0</i>	No	OUT(MANY) WEAK [37]	OUT(1) WEAK [37]	Yes	Yes	Yes
<i>D3-all-0</i>	No	OUT(MANY) WEAK [37]	OUT(1) WEAK [37]	Yes	Yes	Yes
<i>D2-all-0</i>	No	OUT(MANY) WEAK [37]	OUT(1) WEAK [37]	Yes	No**	No
<i>D2-nn-0</i>	No	OUT(MANY) STRONG [39]	OUT(MANY) WEAK [39]	No	No	No

TABLE I. Summary of the results. The first column lists the circuits. The second column says if the circuit family is universal or not. The third and fourth columns inform about the classical simulatability (or not) and the settings of the corresponding proofs. The acronyms STRONG and WEAK refer to the tasks of calculating or sampling from the output probability, respectively (see II B). OUT(1) and OUT(MANY) say whether the task is single- or multi-line. Ave-H: average cumulants of the final states coincide with those of random vectors (Haar measure); Fluc-H: same as before, but for the fluctuations of the cumulants; Spec-RMT: reduced density matrix spectra well described by random matrix theory; (?): No results, to best of our knowledge; No*: RMT-like, coincides with *Haar-6*, but for this non-symmetric case RMT predicts *Haar-8*; No**: Very close to *Haar-6*, however, as before, the prediction of RMT is *Haar-8*.

-
- [1] A. W. Marshall, I. Olkin, and B. C. Arnold, *Inequalities: theory of majorization and its applications*, Vol. 143 (Springer, 1979).
- [2] M. O. Lorenz, Methods of measuring the concentration of wealth, *Publications of the American Statistical Association* **9**, 209 (1905).
- [3] E. Ruch, The diagram lattice as structural principle, *Theoretica Chimica Acta* **38**, 167 (1975).
- [4] E. Ruch and A. Mead, The principle of increasing mixing character and some of its consequences, *Theoretica Chimica Acta* **41**, 95 (1976).
- [5] E. Ruch, R. Schraner, and T. H. Seligman, The mixing distance, *The Journal of Chemical Physics* **69**, 386 (1978).
- [6] M. Horodecki, P. Horodecki, and J. Oppenheim, Reversible transformations from pure to mixed states and the unique measure of information, *Phys. Rev. A* **67**, 062104 (2003).
- [7] A. E. Allahverdyan, R. Balian, and T. M. Nieuwenhuizen, Maximal work extraction from finite quantum systems, *EPL* **67**, 565 (2004).
- [8] M. Horodecki and J. Oppenheim, Fundamental limitations for quantum and nanoscale thermodynamics, *Nature Communications* **4**, 2059 (2013).
- [9] J. M. Renes, Work cost of thermal operations in quantum thermodynamics, *The European Physical Journal Plus* **129**, 153 (2014).
- [10] D. Egloff, O. C. O. Dahlsten, R. Renner, and V. Vedral, A measure of majorization emerging from single-shot statistical mechanics, *New Journal of Physics* **17**, 073001 (2015).
- [11] M. A. Nielsen and G. Vidal, Majorization and the interconversion of bipartite states., *Quantum Information & Computation* **1**, 76 (2001).
- [12] S. Aaronson and A. Arkhipov, The computational complexity of linear optics, in *Proceedings of the forty-third annual ACM symposium on Theory of computing* (ACM, 2011) pp. 333–342.
- [13] S. Chin and J. Huh, Majorization, entropy and computing power of linear optics, preprint arXiv:1710.05551 (2017).
- [14] R. Orús, J. I. Latorre, and M. A. Martín-Delgado, Natural majorization of the quantum fourier transformation in phase-estimation algorithms, *Quantum Information Processing* **1**, 283 (2002).
- [15] J. I. Latorre and M. A. Martín-Delgado, Majorization arrow in quantum-algorithm design, *Phys. Rev. A* **66**, 022305 (2002).
- [16] R. Orús, J. I. Latorre, and M. A. Martín-Delgado, Systematic analysis of majorization in quantum algorithms, *The European Physical Journal D-Atomic, Molecular, Optical and Plasma Physics* **29**, 119 (2004).
- [17] Z. Wei, Z. Ji, and M. Ying, Majorization in quantum adiabatic algorithms, *Phys. Rev. A* **74**, 042320 (2006).
- [18] F. Flamini, N. Viggianiello, T. Giordani, M. Bentivegna, N. Spagnolo, A. Crespi, G. Corrielli, R. Osellame, M. A. Martín-Delgado, and F. Sciarrino, Observation of majorization principle for quantum algorithms via 3-d integrated photonic circuits, preprint arXiv:1608.01141 (2016).
- [19] F. M. García, Majorization in general grover’s algorithms: Efficient vs non-efficient cases, preprint arXiv:1806.04272 (2018).
- [20] P. Hayden, D. Leung, P. W. Shor, and A. Winter, Randomizing quantum states: Constructions and applications, *Communications in Mathematical Physics* **250**, 371 (2004).
- [21] W. Brown and O. Fawzi, Decoupling with random quantum circuits, *Communications in Mathematical Physics* **340**, 867 (2015).
- [22] F. G. Brandao, A. W. Harrow, and M. Horodecki, Local random quantum circuits are approximate polynomial-designs, *Communications in Mathematical Physics* **346**, 397 (2016).
- [23] A. W. Harrow and A. Montanaro, Quantum computational supremacy, *Nature* **549**, 203 (2017).
- [24] A. Bouland, B. Fefferman, C. Nirkhe, and U. Vazirani, On the complexity and verification of quantum random circuit sampling, *Nature Physics* **15**, 159 (2019).
- [25] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. Brandao, D. A. Buell, et al., Quantum supremacy using a programmable superconducting processor, *Nature* **574**, 505 (2019).
- [26] C. Chamon, A. Hamma, and E. R. Mucciolo, Emergent irreversibility and entanglement spectrum statistics, *Phys. Rev. Lett.* **112**, 240501 (2014).
- [27] D. Shaffer, C. Chamon, A. Hamma, and E. R. Mucciolo, Irre-

- versibility and entanglement spectrum statistics in quantum circuits, *Journal of Statistical Mechanics: Theory and Experiment* **2014**, P12007 (2014).
- [28] Z.-C. Yang, A. Hamma, S. M. Giampaolo, E. R. Mucciolo, and C. Chamon, Entanglement complexity in quantum many-body dynamics, thermalization, and localization, *Phys. Rev. B* **96**, 020408 (2017).
- [29] A. I. Larkin and Y. N. Ovchinnikov, Quasiclassical Method in the Theory of Superconductivity, *Soviet Journal of Experimental and Theoretical Physics* **28**, 1200 (1969).
- [30] J. Maldacena, S. H. Shenker, and D. Stanford, A bound on chaos, *Journal of High Energy Physics* **2016**, 1 (2016).
- [31] B. Swingle, Unscrambling the physics of out-of-time-order correlators, *Nature Phys.* **14**, 988 (2018).
- [32] D. Gottesman, The heisenberg representation of quantum computers, preprint arXiv quant-ph/9807006 (1998).
- [33] S. Clark, R. Jozsa, and N. Linden, Generalized clifford groups and simulation of associated quantum circuits, *Quantum Info. Comput.* **8**, 106–126 (2008).
- [34] M. Van Den Nest, Classical simulation of quantum computation, the gottesman-knill theorem, and slightly beyond, *Quantum Info. Comput.* **10**, 258–271 (2010).
- [35] R. Jozsa and M. Van Den Nest, Classical simulation complexity of extended clifford circuits, *Quantum Info. Comput.* **14**, 633–648 (2014).
- [36] D. E. Koh, Further extensions of clifford circuits and their classical simulation complexities, *Quantum Info. Comput.* **17**, 262–282 (2017).
- [37] M. J. Bremner, R. Jozsa, and D. J. Shepherd, Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy, *Proc. R. Soc. A* **467-472**, 459 (2011).
- [38] X. Ni and M. Van Den Nest, Commuting quantum circuits: Efficient classical simulations versus hardness results, *Quantum Info. Comput.* **13**, 54–72 (2013).
- [39] K. Fujii and T. Morimae, Commuting quantum circuits and complexity of ising partition functions, *New Journal of Physics* **19**, 033003 (2017).
- [40] L. Valiant, Quantum circuits that can be simulated classically in polynomial time, *SIAM J. Comput.* **31**, 1229 (2002).
- [41] R. Jozsa and A. Miyake, Matchgates and classical simulation of quantum circuits, *Proc. R. Soc. A* **464**, 3089 (2008).
- [42] D. J. Brod and A. M. Childs, The computational power of matchgates and the xy interaction on arbitrary graphs, *Quantum Info. Comput.* **14**, 901–916 (2014).
- [43] D. Shepherd and M. J. Bremner, Temporally unstructured quantum computation, *Proc. R. Soc. London, Ser. A* **465**, 1413 (2009).
- [44] Y. Nakata and M. Muraio, Diagonal quantum circuits: their computational power and applications, *Eur. Phys. J. Plus* **129**, 152 (2014).
- [45] J. Dehaene and B. De Moor, Clifford group, stabilizer states, and linear and quadratic operations over $\text{gf}(2)$, *Phys. Rev. A* **68**, 042318 (2003).
- [46] M. L. Mehta, *Random Matrices*, 3rd ed. (Academic Press, New York, 2004).
- [47] Y. Y. Atas, E. Bogomolny, O. Giraud, and G. Roux, Distribution of the ratio of consecutive level spacings in random matrix ensembles, *Phys. Rev. Lett.* **110**, 084101 (2013).
- [48] The final states of the circuits $MG-rr-0$ possess parity symmetry. It is easy to show that the corresponding reduced density matrices also are parity-symmetric. Because of this, their entanglement spectra consist of two uncorrelated sequences, each one having a definite parity. Thus, we separated the ensemble of spectra into two symmetry classes, and then calculated two sets of histograms. Both set of histograms are consistent with the GUE distribution. Some considerations apply to $MG-rr-0$. In both cases we considered only the even-symmetry spectra (odd spectra produce statistically identical histograms).
- [49] B. M. Terhal and D. P. DiVincenzo, Classical simulation of noninteracting-fermion quantum circuits, *Phys. Rev. A* **65**, 032325 (2002).
- [50] D. J. Brod, Efficient classical simulation of matchgate circuits with generalized inputs and measurements, *Phys. Rev. A* **93**, 062332 (2016).
- [51] The family $D2-rr-0$ might be *almost* strongly simulatable. Indeed, Fujii and Morimae [39] devised a simulatability proof for IPQ circuits formed by gates of the type $\exp(i\theta Z_j \otimes Z_k)$, with (j, k) denoting nearest-neighbor qubit lines. They name the simulatability class of nearest-neighbor IQP “almost strongly simulatable”, between strongly simulatable (in the exact sense) and weakly simulatable. However, strictly speaking, one can not assert that both $D2-rr-0$ and nearest-neighbor IQP belong to the same simulatability class because $D2-rr-0$ contains nearest-neighbor IQP.
- [52] Matchgates acting on nearest neighbors, having random product states as inputs, are OUT(MANY)-STRONG simulatable on the line (open boundary conditions) [50]. Can this result be extended to the cycle (periodic boundary conditions, as used in the present paper)? Brod presents some geometric arguments in contrary, however, he admits that these may not be definitive: “Curiously, the circuit [...] for periodic boundary conditions corresponds to a geometry where matchgates are universal [...], although it might just use this geometry in a very restricted manner that does not break the simulability” [50].
- [53] Tobias Micklitz and Felipe Monteiro, private communication.