Diagonal unitary entangling gates and contradiagonal quantum states

Arul Lakshminarayan*
Department of Physics, Indian Institute of Technology Madras, Chennai 600036, India

Zbigniew Puchała†
Institute of Theoretical and Applied Informatics, Polish Academy of Sciences, Bałtycka 5, 44-100 Gliwice, Poland and Institute of Physics, Jagiellonian University, ul. Reymonta 4, 30-059 Kraków, Poland

Karol Życzkowski‡
Institute of Physics, Jagiellonian University, ul. Reymonta 4, 30-059 Kraków, Poland and Center for Theoretical Physics, Polish Academy of Sciences, Warsaw, Poland

(Dated: July 4, 2014)

Nonlocal properties of an ensemble of diagonal random unitary matrices of order N^2 are investigated. The average Schmidt strength of such a bipartite diagonal quantum gate is shown to scale as $\log N$, in contrast to the $\log N^2$ behavior characteristic to random unitary gates. Entangling power of a diagonal gate U is related to the von Neumann entropy of an auxiliary quantum state $\rho = AA^\dagger/N^2$, where the square matrix A is obtained by reshaping the vector of diagonal elements of U of length N^2 into a square matrix of order N. This fact provides a motivation to study the ensemble of non-hermitian unimodular matrices A, with all entries of the same modulus and random phases and the ensemble of quantum states ρ, such that all their diagonal entries are equal to $1/N$. Such a state is contradiagonal with respect to the computational basis, in sense that among all unitary equivalent states it maximizes the entropy copied to the environment due to the coarse graining process. The first four moments of the squared singular values of the unimodular ensemble are derived, based on which we conjecture a connection to a recently studied combinatorial object called the "Borel triangle". This allows us to find exactly the mean von Neumann entropy for random phase density matrices and the average entanglement for the corresponding ensemble of bipartite pure states.

I. INTRODUCTION

Entanglement has been at the focus of recent researches in quantum information – for a review see [1], as it enables a range of uniquely quantum tasks such as teleportation, quite apart from being a singular nonclassical phenomenon and therefore of fundamental interest. It is well appreciated now that many particle pure states are typically highly entangled [2–5], and share entanglement in a manner that is almost wholly of a multipartite nature. Here typicality refers to ensembles of pure states selected according to the uniform (Haar) measure. If two distinct subsystems of a pure state are such that together they make up the entire system in a typical pure state, then the two subsystems will be largely entangled. In early works, Page and others [3, 6] had found the average entanglement, which in this case is simply the mean von Neumann entropy of the reduced state, and showed that it is nearly the maximum possible.

More recent studies have explored the distribution of entanglement in such complete bipartite partitions of random states [7]. If the two subsystems do not comprise the entire systems, for example two particles in a three particle state, the average entanglement depends on the dimensionality of the subsystems. Roughly speaking if the complementary space of the subsystems (say A and B) is smaller, the density matrices ρ_A and ρ_B will be typically negative under partial transpose and therefore A and B are entangled [8].

Ways to generate entangled states from initially unentangled ones via unitary operators is of natural interest, and in the context of quantum computation implies the construction of appropriate gates. Investigations of entangling power of a unitary quantum gate were initiated by Zanardi and co-workers [9, 10], while some measures of non–locality were analyzed in [11–16]. A typical quantum gate acting on a composed system consisting of two N–level systems can be represented by a random unitary matrix of order N^2. Nonlocal properties of such random gates were investigated in [17].

In this work we shall analyze a simpler ensemble of diagonal unitary random matrices and will characterize nonlocality of the corresponding quantum gates. It is also naturally related to an ensemble of pure bipartite states in N^2 dimensional space whose components in some fixed basis are of the form $e^{i\phi_j}/N^2$, and ϕ_i are uniformly distributed random numbers. Such an ensemble has been recently studied as phase-random states [18], and in fact connections to diagonal quantum circuits has been pointed out [19]. Part of the motivation for the study of diagonal quantum gates is that many Hamil-

* arul@physics.iitm.ac.in
† z.puchala@iitis.pl
‡ karol@tatry.if.uj.edu.pl

tonians have the structure that the basis in which the interaction is diagonal can be chosen to be unentangled. Time evolution is then governed by unitary operators whose entangling parts are diagonal. Recently studies of measurement-based quantum computation has also used diagonal unitary gates and shown that it can still remain superior to classical computation [20, 21].

Also explicitly, unitary operators such as $(U_A \otimes U_B)U_{AB}$ occur in the study of coupled systems including kicked quantum tops – see the book of Haake [22]. The coupling could be of the form $J_A^z J_B^z$, where $J_z^{A,B}$ are spin operators. Thus the nonlocal part of the evolution is diagonal again. It is found numerically that the eigenstates of such operators as well as the time evolution engendered by repeated applications of such operators can create large entanglement well approximated by that of random states [23]. However such operators have much fewer number of possible independent elements than Haar distributed unitaries on $\mathcal{H}^N \otimes \mathcal{H}^N$. Thus it is of interest to study the origin of such large entanglement.

Furthermore, we are going to study the related ensemble of "unimodular random matrices", comprising complex matrices whose all entries have the same modulus and randomly chosen phases. Such matrices arise from reshaping a pure phase random state as defined in [18]. Note that the usage of the term 'unimodular' concerns all the entries of a matrix, so such a matrix is *not* unimodular in the sense of being integer matrices with determinants ± 1.

Although the unimodular ensemble differs from the Ginibre ensemble of complex, non-hermitian matrices, with independent, normally distributed elements, it displays the same asymptotic behavior of the level density, which covers uniformly the unit disk. On the other hand the squared singular values of unimodular matrices coincide with eigenvalues of certain specific quantum states of size N, the diagonal entries which are equal to $1/N$. As the notion of an "antidiagonal matrix" has entirely different meaning, the density matrices with all diagonal elements equal will be called *contradiagonal*. Observe that reduced density matrices of random phase pure states are thus contradiagonal. We investigate properties of such an ensemble of quantum states and discuss the contradiagonalization procedure, which brings any hermitian matrix to such a basis, that all their diagonal elements do coincide.

One may expect that random contradiagonal states correspond to the large entanglement of the pure bipartite states and we show that indeed these states have larger von Neumann entropy than those sampled according to the Ginibre ensemble. The unimodular ensemble, while having no obvious invariance properties, seems to also have remarkable underlying mathematical structure. For example, the average of the moments of the matrices in the ensemble are connected to polynomials with combinatorial interpretations. We evaluate the first four moments and use this to conjecture an exact expression for *all* of them. We numerically show that this is more than likely to be correct. Analytical continuation of the moments to non-integer powers allows us to evaluate the average von Neumann entropy for this ensemble which appears to be *exact* for all dimensions.

This paper is organized as follows. In Section II the ensemble of diagonal unitary gates is introduced, while in Section III the related ensemble of unimodular matrices is analyzed. Low order moments are calculated analytically, and a natural conjecture is made for exact expressions for all moments. Numerical evidence is presented for this. Nonlocality and entangling powers of random unitary gates is studied in Sec. IV. An exact expression based on a continuation of moments is presented for the average Schmidt strength of diagonal unitaries, or equivalently of the von Neumann entropy of the random phase states. Procedure of contra-diagonalization of a hermitian matrix, which makes all diagonal elements equal, is introduced in Sec. V. In this section we study in particular the cognate ensemble of random contradiagonal states and show their particular properties concerning the transfer of quantum information. The paper is concluded in Sec VI, and an Appendix reviewing the operator Schmidt decomposition and entangling entropy.

II. DIAGONAL BIPARTITE QUANTUM GATES

Consider a diagonal unitary matrix U of order N^2. Each entry is assumed to be random, so that $U_{\mu\nu} = \delta_{\mu\nu} \exp(i\phi_\nu)$, where ϕ_ν are independent random phases distributed uniformly in $[0, 2\pi)$. Such a matrix represents a diagonal unitary gate acting on a bipartite quantum system, a state in $\mathcal{H}^N \otimes \mathcal{H}^N$.

Any matrix U acting on the composed Hilbert space $\mathcal{H}_N \otimes \mathcal{H}_N$, can be represented in its operator Schmidt form,

$$U = \sum_{k=1}^{K} \sqrt{\Lambda_k}\, B'_k \otimes B''_k, \tag{1}$$

where the Schmidt rank $K \leq N^2$. Note that the matrices B'_k and B''_k of order N in general are non unitary.

It can be shown [24] that the Schmidt coefficients Λ_k, $k = 1, \ldots, K$, can be obtained as squared singular values of the reshuffled matrix U^R. This fact is briefly recalled in Appendix A, where the notation is explained. A generic diagonal matrix of size four, after reshuffling forms a non-hermitian matrix of rank two,

$$U = \begin{bmatrix} U_{11} & 0 & 0 & 0 \\ 0 & U_{22} & 0 & 0 \\ 0 & 0 & U_{33} & 0 \\ 0 & 0 & 0 & U_{44} \end{bmatrix}, \quad U^R = \begin{bmatrix} U_{11} & 0 & 0 & U_{22} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ U_{33} & 0 & 0 & U_{44} \end{bmatrix}. \tag{2}$$

For a diagonal matrix U of order N^2 the reshuffled matrix U^R contains $N(N-1)$ columns and rows with all entries equal to zero. Hence the non-zero singular values

of U^R are equal to the singular values of a square matrix A of size N, obtained by reshaping the diagonal of the unitary gate, $A_{jk} = \exp(i\phi_\nu)$, where $\nu = (j-1)N + k$. As all entries of A are unimodular and have a random phase, this construction defines an ensemble of random unimodular matrices.

III. RANDOM UNIMODULAR MATRICES

Consider a complex square matrix A of size N from the *unimodular ensemble*, so that a) all entries have the same modulus, $|A_{jk}| = 1$, and b) the phases are drawn independently from a uniform distribution,

$$A_{jk} = \exp(i\phi), \quad P(\phi) = \frac{1}{2\pi}, \quad \text{for} \quad \phi \in [0, 2\pi). \quad (3)$$

Such a random matrix A could be called a *pre–Hadamard* as all entries have the same modulus, so choosing an appropriate set of phases it may become unitary, and thus belong to the class of complex Hadamard matrices [25]. In our model all phases are random and non-correlated, so a typical matrix from this ensemble exhibits effects of strong non-unitarity. The ensemble of unimodular matrices A with all independent, well–behaved, identically distributed entries is of the Wigner type. Thus this non-hermitian ensemble or random matrices satisfies asymptotically the circular law of Girko [26].

As shown in Fig. 1 already for $N = 100$ the spectral density for the unimodular ensemble is close to uniform in the unit disk. Furthermore, the distribution of rescaled squared singular values, $x = \mathrm{eig}(AA^\dagger)/N$, is asymptotically described by the Marchenko–Pastur (MP) distribution $P_{MP}(x) = \frac{1}{\pi}\sqrt{1/x - 1/4}$ for $x \in [0, 4]$, characteristic to the Ginibre ensemble. The moments of this distribution are given by the Catalan numbers, while its entropy reads $-\int_0^4 x \log x P_{MP}(x) dx = -1/2$. As $x = N\lambda$, where λ denotes the eigenvalue of a normalized density matrix

$$\rho = AA^\dagger/N^2 \quad (4)$$

satisfying $\mathrm{Tr}\rho = 1$, the average entropy of spectrum of ρ behaves asymptotically as $\log N - 1/2$. Note that this behavior is characteristic to random quantum states distributed uniformly with respect to the Hilbert–Schmidt measure [27] in the entire set of quantum states of a given dimension.

Although for large N statistical properties of the unimodular ensemble coincide with those of complex Ginibre ensemble, deviations are visible for small matrix size. To visualize these effects we studied the moments of the distribution of squared singular values $M_m = \int x^m P(x) dx$. Fig. 2 shows a comparison of the moments M_2, M_3 and M_4 for random matrices of the unimodular ensemble and the Hilbert–Schmidt ensemble of order N. In the later case analytical predictions for the moments are known as the traces of the random states ρ_N of size N distributed

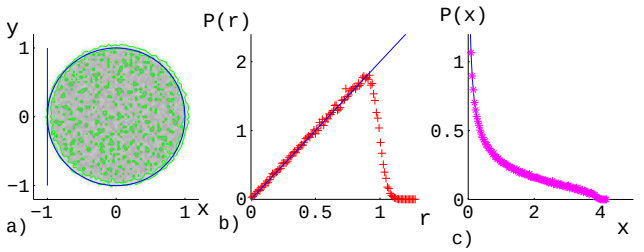

FIG. 1. Properties of random unimodular matrices of order $N = 100$ are close to those of the complex Ginibre ensemble: a) the spectrum of $A/\sqrt{N}$ in the complex plane satisfies the circular law of Girko; b) the radial density $P(r)$ of the complex eigenvalues grows linearly in the center of the unit disk; and c) the distribution of squared singular values $P(x)$ is described by the Marchenko–Pastur distribution.

according to the Hilbert–Schmidt measure read [2, 27],

$$\langle \mathrm{Tr}\rho_N^2 \rangle_{HS} = \frac{2N}{N^2+1}, \quad \langle \mathrm{Tr}\rho_N^3 \rangle_{HS} = \frac{5N^2+1}{(N^2+1)(N^2+2)}, \quad (5)$$

and due to rescaling of the variable x one has $M_m = N^{m-1}\mathrm{Tr}\rho^m$. Numerical data, such as that presented in Fig. (2), show that for a given N the moments for the unimodular ensemble are smaller, so the corresponding distribution are narrower, even though for large N both distributions tend to the limiting Marchenko–Pastur distribution.

Note that the averages moments for the distribution of squared singular values for random Ginibre matrices of a given size N, derived recently in [28], coincide with the predictions (5) for the HS ensemble only in the asymptotic case $N \to \infty$. In the former ensemble the constraint concerns the average trace $\langle \mathrm{Tr}GG^\dagger \rangle$, while in the latter each random matrix has a fixed trace, $\mathrm{Tr}\rho = 1$, so that this difference asymptotically vanishes.

A. Lower order moments and a conjecture for all orders

The lower order moments of the unimodular ensemble can be exactly evaluated and compared to the above case. In fact we will calculate exactly moments till the fourth and conjecture an exact formula for any moment. The density matrix elements are

$$\rho_{\alpha_1\alpha_2} = \frac{1}{N^2}\sum_{l_1=1}^{N} \exp[i(\phi_{\alpha_1 l_1} - \phi_{\alpha_2 l_1})]. \quad (6)$$

1. *The second moment* $\langle \mathrm{Tr}\rho_N^2 \rangle_{UE}$

The second moment while being the simplest, also serves as a measure of purity of a given quantum mixed

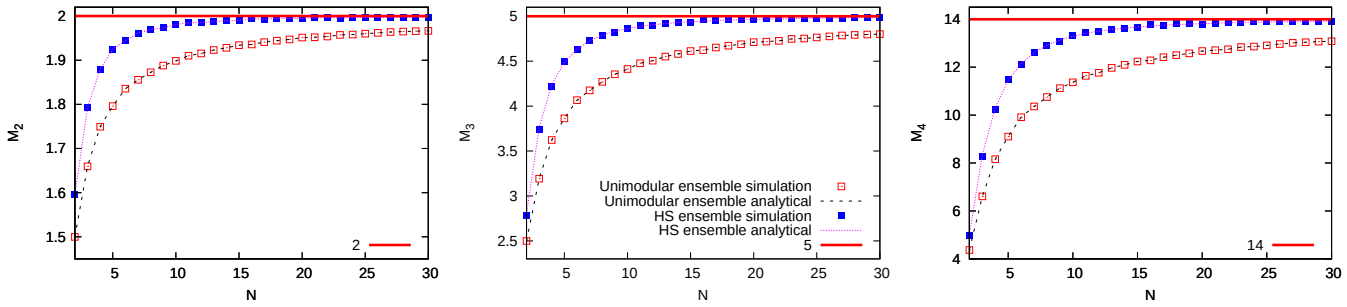

FIG. 2. Moments of the distribution of squared singular values $P(x)$ for unimodular ensemble and the Hilbert–Schmidt measure as a function of the matrix size N: from left to right are shown the second moments M_2, third moments M_3, and fourth moments M_4 respectively. Horizontal lines at $M_2 = C_2 = 2$ and $M_3 = C_3 = 5$ and $M_4 = C_4 = 14$ denote the Catalan numbers, which give the corresponding moments of the MP distribution and determine the the asymptotic behavior of both moments. Solid lines represent predictions (5) for the Hilbert-Schmidt measure, while the dashed lines the predictions for the unimodular ensemble.

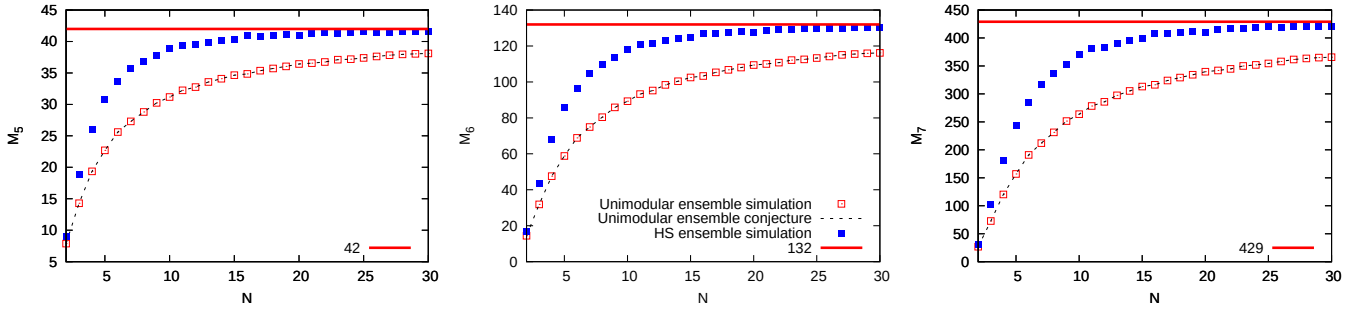

FIG. 3. The fifth, sixth and seventh moments, M_5, M_6, and M_7 of the distribution of squared singular values $P(x)$ for the unimodular ensemble as a function of the matrix size N. the points are from numerical simulation based on a million realizations while the curves are from the formula in Eq. (15). The horizontal lines are at $C_5 = 42$, $C_6 = 132$ and $C_7 = 429$, further Catalan numbers and the asymptotic value of the scaled moments.

state. We have

$$\mathrm{Tr}\rho^2 = \frac{1}{N^4}\sum_{\alpha_1\alpha_2}\sum_{l_1l_2}\exp[i(\phi_{\alpha_1 l_1} - \phi_{\alpha_1 l_2} + \phi_{\alpha_2 l_2} - \phi_{\alpha_2 l_1})]. \tag{7}$$

On averaging over the uniform phases the only terms that would survive are those cases for which the phase vanishes. This happens if $\alpha_1 = \alpha_2$ for arbitrary l_1 and l_2. Thus this case contributes

$$\frac{1}{N^4}\sum_{\alpha_1}\sum_{l_1l_2} 1 = \frac{N^3}{N^4} = \frac{1}{N}. \tag{8}$$

Indeed this is the "diagonal" contribution. The phase also vanishes if $\alpha_1 \neq \alpha_2$, but $l_1 = l_2$. This "off-diagonal" contribution is

$$\frac{1}{N^4}\sum_{\alpha_1\neq\alpha_2}\sum_{l_1} 1 = \frac{1}{N^4}N(N-1)N = \frac{N-1}{N^2}. \tag{9}$$

As these exhaust the exclusive possibilities, the average second moment for the level density of related to the unimodular ensemble reads

$$\langle \mathrm{Tr}\rho_N^2\rangle_{UE} = \frac{2N-1}{N^2}. \tag{10}$$

Equivalently $M_2 = (2N-1)/N$, which indeed tends to 2 for large N. Also note that $\langle \mathrm{Tr}\rho^2\rangle_{HS} - \langle \mathrm{Tr}\rho^2\rangle_{UE} = (N-1)^2/[N^2(N^2+1)] > 0$, indicating that the density matrices constructed from the unimodular ensemble are on average more mixed than those from the Ginibre ensemble.

2. *The third moment* $\langle \mathrm{Tr}\rho_N^3\rangle_{UE}$

The third moment is obtained by considering all those cases when

$$\phi_{\alpha_1 l_1} - \phi_{\alpha_1 l_2} + \phi_{\alpha_2 l_2} - \phi_{\alpha_2 l_3} + \phi_{\alpha_3 l_3} - \phi_{\alpha_3 l_1}$$

vanishes for arbitrary sets of phases, where α_i and l_i take values in $1, \cdots, N$. The indexes are ordered in such a way that a bijection to a standard counting problem becomes possible. Starting from the first pair, the sign is reversed while the second index is new in the second pair. The third pair is obtained by again reversing the sign of the second but now the first index becomes new, and so on. Finally when there are 6 pairs, the last index is the same as that of the first pair. It is clear that this generalizes to the moment of order k, where there are $2k$ such pairs.

At this level a bijection to several standard problems in counting that involve the Catalan numbers C_k [29] is possible. For example that of matching 3 pairs of parentheses: $()()(), (())(), ()(()), ((())), (()())$ is relevant to the third moment, each parenthesis represents the pair of indexes at the corresponding place. The matched pair of parentheses imply that the pair of indexes are equal. The first possibility and its translation in terms of indexes is: $()()()$: $\alpha_1 l_1 = \alpha_1 l_2$, $\alpha_2 l_2 = \alpha_2 l_3$, $\alpha_3 l_3 = \alpha_3 l_1$, or $l_1 = l_2 = l_3$. The second $(())()$: $\alpha_1 l_1 = \alpha_2 l_3$, $\alpha_1 l_2 = \alpha_2 l_2$, $\alpha_3 l_3 = \alpha_3 l_1$, or $\alpha_1 = \alpha_2$, $l_1 = l_3$. Similarly $()(())$: $\alpha_2 = \alpha_3$, $l_1 = l_2$, $((()))$: $\alpha_1 = \alpha_3$, $l_2 = l_3$, $(()())$: $\alpha_1 = \alpha_2 = \alpha_3$. The unconstrained indexes can take arbitrary values between 1 and N. Another bijection is between the indexes and points that are joined by noncrossing semicircles. Thus the contributions from $()()()$ and $(()())$ are respectively

$$\sum_{l_1} \sum_{\alpha_1,\alpha_2,\alpha_3} 1 = N^4, \sum_{\alpha_1} \sum_{l_1,l_2,l_3}{}' 1 = N^4 - N^2.$$

The last sum is restricted in the sense that it does not include the case $l_1 = l_2 = l_3$ that is already included in the first count. The other three cases contribute equally

$$\sum_{\alpha_1 \neq \alpha_3} \sum_{l_1 \neq l_2} 1 = N^2(1-N)^2,$$

where the distinct indexes are always unequal; if they are equal it will reduce to a term considered in the first two cases. Thus putting them all together we get

$$\langle \mathrm{Tr}\rho^3 \rangle_{UE} = \frac{1}{N^4}(5N^2 - 6N + 2), \tag{11}$$

and $M_3 = N^2 \langle \mathrm{Tr}\ \rho_N^3 \rangle = (5 - 6/N + 2/N^2)$.

The k–th moment $\langle \mathrm{Tr}\rho^k \rangle$ is of the form $P_k(N)/N^{2(k-1)}$, where $P_k(N)$ is a degree $k-1$ polynomial in N whose leading term's coefficient is $C_k = \frac{1}{k+1}\binom{2k}{k}$, the k–th Catalan number. Thus it follows that the moments $M_k = N^{k-1}\langle \mathrm{Tr}\rho^k \rangle$ tend to C_k and hence the asymptotic density is described by the universal Marchenko-Pastur distribution. Writing explicit expressions for the moments M_k for the unimodular ensemble we are in position to quantify the deviations from the asymptotic universal MP distribution.

3. *The fourth moment* $\langle \mathrm{Tr}\rho_N^4 \rangle_{UE}$

We will now evaluate explicitly the fourth moment that presents some challenges and then *conjecture* an *exact* expression for $P_k(N)$. There are 14 different parenthesizations for the $k = 4$ case with 8 pairs of indexes involved. There are 3 "contractions" in each case. For instance the contractions corresponding to $()(())()$ are $l_1 = l_2$, $\alpha_2 = \alpha_3$, $l_4 = l_1$. Thus there are $8 - 3 = 5$ sums that are unconstrained from each of the 14 parenthesizations and hence the leading term in $N^8\langle \mathrm{Tr}\rho_N^4 \rangle$ is $14N^5$. Generalizing, to the k–th moment, the number of contractions is $k-1$. This is seen by writing the alternating indexes as actual products and sums while respecting their distinctness and requiring $\sum_{i=1}^{k} \alpha_i(l_i - l_{i+1}) = 0$ with $l_{k+1} = l_1$. Setting say $\alpha_n l_n = \alpha_m l_{m+1}$ for some n and m reduces the number of terms by 1. Due to periodic boundary conditions, the number of contractions that will set the whole sum to 0 is $k-1$. Thus it follows that in general the leading term in $N^{2k}\langle \mathrm{Tr}\rho^k \rangle$ is $C_k N^{2k-(k-1)} = C_k N^{k+1}$.

Overcounting however lowers the value of $N^8\langle \mathrm{Tr}\rho_N^4 \rangle$ from $14N^5$, and in general from $C_k N^{k+1}$. Sticking to the $k = 4$ case, the combined contributions from $()()()()$ and $(()()())$ which either contract all l_i or all α_i respectively is $2N^5 - N^2$, N^2 being the double count of all α_i being the same and all l_i being the same. The other 12 contributions involve sums such as

$$\sum_{\alpha_1=\alpha_2} \sum_{\alpha_3=\alpha_4\neq\alpha_1} \sum_{l_1=l_3} \sum_{l_2,l_4}{}' 1 = (N^2-1)(N-1)N^2,$$

where the restricted sum eliminates the cases when $l_2 = l_4 = l_1 = l_3$, which has already been considered. While this case corresponds to the parenthesization $(())(())$, the other 11 have sums over 5 indexes with similar restrictions.

Thus these contribute $12N^2(N-1)(N^2-1)$, however there still remains some overcounting to be accounted for. For example the above case includes instances when $l_2 = l_1 = l_3$ but $\neq l_4$ which is also possible when the contracted indexes are $\alpha_2 = \alpha_4$, and $l_1 = l_2 = l_3$ and corresponds to the paranthesization $()()(())$. Exhaustive enumeration of these terms that originate from contracting 4 indexes reveals that there are 16 such terms each of which gives

$$\sum_{\alpha_1=\alpha_2} \sum_{\alpha_3=\alpha_4\neq\alpha_1} \sum_{l_1=l_2=l_3} \sum_{l_4\neq l_1} 1 = N^2(N-1)^2.$$

There is no further overcounting as the cases with > 4 contractions have already been properly included. Finally in total the contribution is $2N^5 - N^2 + 12(N^2-1)(N-1)N^2 - 16N^2(N-1)^2 = 14N^5 - 28N^4 + 20N^3 - 5N^2$ and we get

$$\langle \mathrm{Tr}\ \rho_N^4 \rangle_{UE} = \frac{1}{N^6}(14N^3 - 28N^2 + 20N - 5). \tag{12}$$

4. *A conjecture for all moments* $\langle \mathrm{Tr}\rho_N^n \rangle_{UE}$

The complexity of the counting problem is naturally increasing. However having found the polynomials $P_2(N) = 2N - 1$, $P_3(N) = 5N^2 - 6N + 2$ and $P_4(N) = 14N^3 - 28N^2 + 20N^3 - 5$ exactly, the following are evident: they have alternating signs, satisfy $P_k(1) = 1$, and the constants (coefficients of N^0) have the absolute value 1, 2 and 5 which are themselves Catalan numbers. That $P_k(1) = 1$ follows simply as for $N = 1$, there is a only a single pure phase $e^{i\phi}$ and the "density matrix" is simply $e^{i\phi}e^{-i\phi} = 1$.

Based on the triangle of coefficients $\{1,\{2,1\},\{5,6,2\},\{14,28,20,5\}\}$ a search in the On-line Encyclopedia of Integer Sequences [30] (OEIS) returns two sequences A062991 and A234950. In the first of which is the signed version (that we encounter), it arises as generalizations of Pascal's triangles via Riordan arrays [31]. In the second the unsigned version, which the authors call *Borel's triangle* [32] and make connections to new counting problems in commutative algebra and discrete geometry. Going beyond what we have above, the first seven rows of the unsigned triangle reads:

$$\begin{array}{ccccccc}
1 & & & & & & \\
2 & 1 & & & & & \\
5 & 6 & 2 & & & & \\
14 & 28 & 20 & 5 & & & \\
42 & 120 & 135 & 70 & 14 & & \\
132 & 495 & 770 & 616 & 252 & 42 & \\
429 & 2002 & 4004 & 4368 & 2730 & 924 & 132 \\
\ldots & & & & & &
\end{array}$$

The left and rightmost entries are Catalan numbers. The entry $f_{n,k}$ ($n \geq 0$, $k \geq 0$) of the Borel triangle is

$$f_{n,k} = \sum_{s=0}^{n} \binom{s}{k} C_{n,s} \tag{13}$$

where $C_{n,s}$ is *Catalan's triangle*:

$$\begin{array}{ccccc}
1 & & & & \\
1 & 1 & & & \\
1 & 2 & 2 & & \\
1 & 3 & 5 & 5 & \\
1 & 4 & 9 & 14 & 14 \\
\ldots & & & &
\end{array}$$

which satisfies the recursion $C_{n,k} = C_{n-1,k} + C_{n,k-1}$, that is the entries are sums of the one to the left and the one above. The first column of all 1 is the "boundary condition" $C_{n,0} = 1$. Explicit formula for $C_{n,k}$ and $f_{n,k}$ are available [31]:

$$C_{n,k} = \frac{(n+k)!(n-k+1)}{k!(n+1)!},$$

$$f_{n,k} = \frac{1}{n+1}\binom{2n+2}{n-k}\binom{n+k}{k}.$$

It is then natural to *conjecture* that for $n \geq 1$ the average moments of the level density of the random matrices of size N are

$$\langle \mathrm{Tr}\rho_N^n \rangle_{UE} = \frac{1}{N^{2(n-1)}} \sum_{k=0}^{n-1} (-1)^k f_{n-1,k}\, N^{n-k-1}. \tag{14}$$

The smallest unproven case is $n = 5$, which can be simply read off from Borel's triangle:

$$\langle \mathrm{Tr}\rho^5 \rangle_{UE} = \frac{1}{N^8}(42N^4 - 120N^3 + 135N^2 - 70N + 14). \tag{15}$$

Fig. 3 displays the numerical calculations of moment $M_5 = N^4\langle \mathrm{Tr}\rho^5 \rangle$, as well as M_6 and M_7 from a million random realizations of the ensemble and shows how well this conjecture fares. There seems to be no room for doubting the correctness of the conjecture.

A calculation of the first few cumulants from the moments M_n of the scaled variables $N\lambda$ results in (apart from $\kappa_1 = 1$)

$$\begin{aligned}
\kappa_2 &= \frac{1}{N}(N-1), \\
\kappa_3 &= \frac{1}{N^2}(N-1)(N-2), \\
\kappa_4 &= -\frac{1}{N^3}(N-1)(4N-5), \\
\kappa_5 &= -\frac{1}{N^4}(N-1)(N-2)(4N^2+2N-7).
\end{aligned} \tag{16}$$

As $N \to \infty$ these tend to $\{1,1,1,0,-4,\ldots\}$, the initial cumulants corresponding to the moments being the Catalan numbers $\{1,2,5,14,42,\cdots\}$.

The moments of the unimodular ensemble themselves also seem to have combinatorial significance. For example the moments for $N = 3$ are such that $3^{(n-1)}M_n(N = 3)$ is the integer sequence $\{1,5,29,181,1181,\cdots\}$. If we include an additional 1 corresponding to M_0, this sequence is found as a column in the entry A183134 of the OEIS. Indeed the other columns of the square array of this entry are similarly the moments for different values of N, $N = 1,2,\cdots$. This prompts the additional conjecture that the $N^{2(n-1)}\mathrm{Tr}(\rho_N^n)$ is the same as the number of N-alphabet words of length $2n$ beginning with the first character of the alphabet by repeatedly inserting doublets into the initially empty word, as this is the counting problem that is stated in the OEIS entries (see also [33]). For example in the case of $n = 2$ and $N = 2$, the alphabet set is binary $\{ab,\}$. Doublets are repeated alphabets. Thus inserting two doublets (for $n = 2$) one gets *aaaa*, *aabb*, *abba* as the three possibilities that start with *a*. This coincides with $2N-1$ that we derived above.

Having explored the moments of the unimodular ensemble we now turn to one of our central motivations, finding the entangling power of diagonal unitaries.

IV. ENTROPY OF THE UNIMODULAR ENSEMBLE AND NONLOCALITY OF RANDOM DIAGONAL GATES,

By construction, the average entropy of squared singular values of random unimodular matrices A is equal to the average entropy of entanglement for the corresponding unitary gates $U = A^R$. As squared singular values of A are asymptotically described by the Marchenko–Pastur distribution, making use of the Page formula [3] we infer that the mean entropy of entanglement (A4) of a random diagonal gate behaves as

$$\langle S(U) \rangle_{\mathrm{diag}} \;=\; \langle S(\rho = AA^\dagger/N^2) \rangle_{UE} \;\approx\; \log N - 1/2. \tag{17}$$

This result forms approximately a half of the entropy of generic Haar random unitary matrices [17]

$$\langle S(U)\rangle_{\rm Haar} \;\approx\; 2\log N - 1/2. \tag{18}$$

Based on the discussion of moments in the previous section, and taking them to be exact allows us to find what appears to be an exact expression for the average entropy of entanglement, which can be interpreted as entanglement in a random ensemble of states $\langle S(\rho)\rangle_{UE}$ where ρ is defined in Eq. (4) or the average entanglement of diagonal unitary gates via Eq. (A4). Using the view of state entanglement, from the last section, the expression in Eq. (14) can be used to write the n^{th} moment as

$$\langle {\rm Tr}\rho_N^n\rangle_{UE} = \frac{1}{nN^{n-1}}\binom{2n}{n-1}\,{}_2F_1(n,1-n;2+n;1/N). \tag{19}$$

Using this we can continue the moments to noninteger powers, so that we have $\sum_i \lambda_i^x$ for x real. Observing that the average entropy $\langle S(\rho)\rangle_{UE}$ is the limit of $(1-\sum_i \lambda_i^x)/(x-1)$ as $x\to 1^+$, we have that

$$\langle S(\rho)\rangle_{UE} = -df(x)/dx|_{x=1} \tag{20}$$

where $f(x) = \langle {\rm Tr}\rho_N^x\rangle =$

$$\frac{1}{N^{x-1}}\frac{\Gamma(2x+1)}{\Gamma(x+1)\Gamma(x+2)}\,{}_2F_1(x,1-x;2+x;1/N). \tag{21}$$

While it is not evident that such a continuation be exact, that it is indeed very likely to be so is illustrated in Fig. (4), where the moments are plotted for $1\le x\le 2$ for small values of N. This gives us confidence that the entropy found from such a procedure is also *exact*.

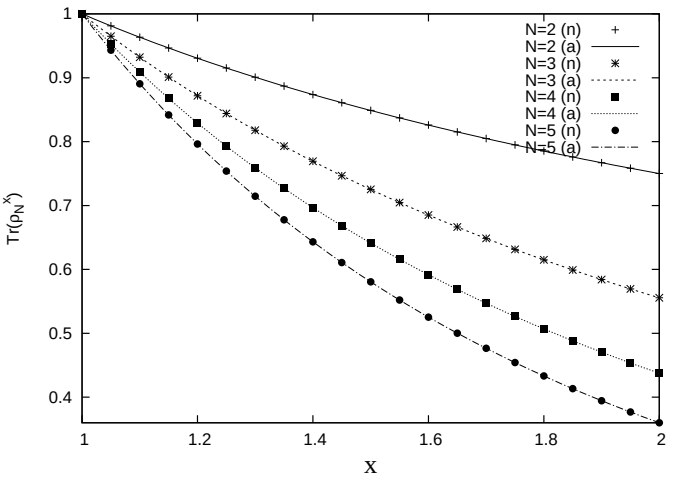

FIG. 4. The moments for non-integer powers between 1 and 2 are plotted for the unimodular ensemble, and $N = 2, 3, 4$. The points are obtained by numerical simulation using 10^6 realizations from the ensemble, while the lines are those from the analytical expression in Eq. (21).

To evaluate $-f'(1)$ one needs to evaluate the derivatives of gamma functions and the hypergeometric function with respect to their parameters. Using that $\Gamma'(z) = \Gamma(z)\psi_0(z)$, where $\psi_0(z)$ is the digamma function we get that

$$-\frac{d}{dx}\frac{1}{N^{x-1}}\frac{\Gamma(2x+1)}{\Gamma(x+1)\Gamma(x+2)}|_{x=1} = \log N - \frac{1}{2}, \tag{22}$$

where the origin of $1/2$ is due to the fact that $\psi_0(3) - \psi_0(2) = 1/2$. The derivative of the hypergeometric function can be evaluated using its definition as an infinite series. We have to compute

$$\frac{d}{dx}\sum_{m=0}^{\infty}\frac{(x)_m(1-x)_m}{(x+2)_m}\frac{1}{m!N^m}, \tag{23}$$

for which we need the derivatives of the Pochhammer symbols which are defined as $(a)_n = a(a+1)\cdots(a+n-1)$. Due to the fact that we need to evaluate the derivative at $x=1$ (and $(0)_m = 0$ for $m>1$, while $(0)_0 = 1$), we only need that $d(1-x)_m/dx|_{x=1} = -(m-1)!$ which is easy to see from the definition of the symbol. Putting these together we get that

$$\begin{aligned} &-\frac{d}{dx}\,{}_2F_1(x,1-x,x+2;1/N)|_{x=1} = \\ &\sum_{m=1}^{\infty}\frac{2}{m(m+1)(m+2)}\frac{1}{N^m} = \\ &\frac{3}{2} - N - (N-1)^2\log(1-\frac{1}{N}). \end{aligned} \tag{24}$$

The last equality is obtained as the infinite sum can be evaluated by elementary means, integrating thrice the identity $1/(1-x) = 1 + x + x^2 + \cdots$. and thus finally the average entropy is the sum of the results in Eqs. (22) and 24:

$$\langle S(\rho)\rangle_{UE} = \log N - (N-1) - (N-1)^2\log\left(\frac{N-1}{N}\right). \tag{25}$$

Numerical results presented in Fig. (5) provide further arguments that the above expressions for the average entropy are exact for any dimension. The differences between the formula and numerical simulations are shown to be smaller than $1/\sqrt{N_S}$, where N_S denotes the size of the numerical sample. For large N it is easy to see that this approaches $\log N - 1/2$ with the neglected terms being of order $1/N$, in agreement with what is expected from the Marchenko-Pastur distribution and from the Page formula [3] for the HS ensemble. For instance, if $N=2$, the exact density of the eigenvalues in $[0,1]$ reads $1/(\pi\sqrt{y(1-y)})$, as discussed in the next section. Hence the average entropy is

$$\int_0^1 \frac{-2y\log y}{\pi\sqrt{y(1-y)}} = \log 4 - 1, \tag{26}$$

which agrees with Eq. (25). We may compare this with the exact entropy from the HS ensemble, which is

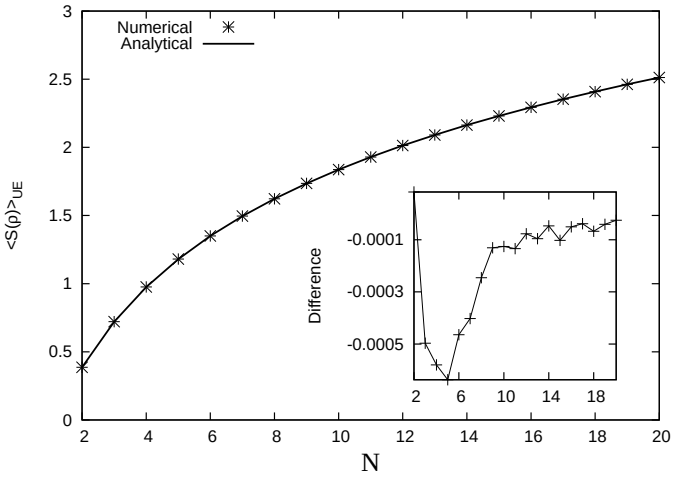

FIG. 5. The average entropy or entanglement in the unimodular ensemble is plotted against various dimensionalities. The points are obtained by a numerical simulation using 10^6 realizations, while the smooth line is from the analytical formula in Eq. (25). The essentially exact nature of the expression is illustrated in the inset where the difference between the numerical and analytical is shown to be consistent with statistical fluctuations from a million realizations.

$\langle S(\rho)\rangle_{HS} = \sum_{k=N+1}^{N^2} 1/k - (N-1)/(2N)$ [3]. For example for $N = 2$ this gives $1/3$ which is smaller than that for the UE ensemble that is $\log 4 - 1 \approx 0.39$. Although the difference decreases with the matrix size, the relation $\langle S(\rho)\rangle_{HS} < \langle S(\rho)\rangle_{UE}$ holds true, which indicates again the enhanced average entanglement in the unimodular ensemble.

Another measure of nonlocality of gates is the so-called *entangling power* based on the ability of operators to create subsystem mixed states from originally unentangled pure bipartite states. If $|\psi_1\rangle \otimes |\psi_2\rangle$ is an unentangled state in $\mathcal{H}_N \otimes \mathcal{H}_N$, and U is an unitary operator on this space, its entangling power as defined by Zanardi, Zalka and Faoro [9] is

$$e_p(U) = \overline{E(U|\psi_1\rangle \otimes |\psi_2\rangle)}^{\psi_1,\psi_2}, \tag{27}$$

the average being over all product states. Any entanglement measure can be used for E, the one that was used in [9] being the simplest useful one, the linear entropy: $E(|\psi\rangle) = 1 - \mathrm{Tr}_1\mu^2$, where $\mu \equiv \mathrm{Tr}_2|\psi\rangle\langle\psi|$ is the reduced density matrix of the subsystem labeled by 1.

The case of interest in the present work is one where the matrix U is diagonal and hence the following is obtained:

$$\langle\alpha|\langle l|U|\psi_1\rangle|\psi_2\rangle = e^{i\phi_{\alpha l}}\langle\alpha|\psi_1\rangle\langle l|\psi_2\rangle, \tag{28}$$

where we have used $\langle\alpha l|U|\beta m\rangle = e^{i\phi_{\alpha l}}\delta_{\alpha\beta}\delta_{lm}$. The reduced density matrix is

$$\mu_{\alpha_1\alpha_2} = \sum_l e^{i(\phi_{\alpha_1 l} - \phi_{\alpha_2 l})}\langle\alpha_1|\psi_1\rangle\langle l|\psi_2\rangle\langle\psi_1|\alpha_2\rangle\langle\psi_2|l\rangle, \tag{29}$$

and therefore

$$\mathrm{Tr}\mu^2 = \sum_{\alpha_1,\alpha_2,l_1,l_2} e^{i(\phi_{\alpha_1 l_1} - \phi_{\alpha_1 l_2} + \phi_{\alpha_2 l_2} - \phi_{\alpha_2 l_1})} \times|\langle\alpha_1|\psi_1\rangle|^2|\langle l_1|\psi_2\rangle|^2|\langle\alpha_2|\psi_1\rangle|^2|\langle l_2|\psi_2\rangle|^2. \tag{30}$$

Averaging over the states $|\psi_{1,2}\rangle$ can be done assuming that they are random vectors distributed uniformly according to the invariant Haar measure. Further assuming the general case of complex random states [34], the following are the average of the products of two intensity components:

$$\overline{|\langle\alpha_1|\psi_1\rangle|^2|\langle\alpha_2|\psi_1\rangle|^2} = \frac{\delta_{\alpha_1\alpha_2} + 1}{N(N+1)}. \tag{31}$$

Using this, it follows that

$$\overline{\mathrm{Tr}\mu^2} = \frac{N^2 + 2N^3 + N^4\mathrm{Tr}(\rho^2)}{N^2(N+1)^2}. \tag{32}$$

The connection to $\mathrm{Tr}\rho^2$ of the last section follows from Eq. (7). Thus the entangling power of diagonal unitaries $e_p(U) = 1 - \overline{\mathrm{Tr}\mu^2}$ is directly related to the second moment of the squared singular values of the reshaped matrix. The average entangling power, now averaged over all phases in the diagonal unitary gates is

$$\langle e_p(U)\rangle_{diag} = 1 - \frac{N^2 + 2N^3 + N^2(2N-1)}{N^2(N+1)^2} = \left(\frac{N-1}{N+1}\right)^2, \tag{33}$$

where the result $\langle\mathrm{Tr}\rho^2\rangle_{UE} = (2N-1)/N^2$ has been used from the previous section. This can be compared with the average entangling power of unitary gates [9]: $\langle e_p(U)\rangle = (N-1)^2/(N^2+1)$, which is only marginally larger. The entropies of full unitaries were almost twice as large as the diagonal ones. At the level of the purity however one still sees the difference in that $\langle\overline{\mathrm{Tr}\mu^2}\rangle = 4N/(N-1)^2 \approx 4/N$ is double that of the reduced density matrix of typical random states in $\mathcal{H}_N \otimes \mathcal{H}_N$, which reads $2/N$ [2].

V. CONTRADIAGONAL HERMITIAN MATRICES

Any ensemble of random matrices, allows one to generate an ensemble of quantum states [35]. Taking a random matrix A, one writes $\sigma = AA^\dagger/\mathrm{Tr}AA^\dagger$ to get a random density matrix: a hermitian, positive operator normalized by the trace condition $\mathrm{Tr}\sigma = 1$. In the case of unimodular random matrices (3) one has $\mathrm{Tr}AA^\dagger = N^2$, hence $\sigma = AA^\dagger/N^2$.

Observe that by construction of the unimodular matrix A the corresponding positive Wishart matrix $AA^\dagger$ has all diagonal elements *equal*. Thus the diagonal elements of the corresponding random density matrix ρ read $\rho_{ii} = 1/N$, where $i = 1, \ldots, N$. In other words, the state ρ is represented in such a particular basis $\{|1\rangle, |2\rangle, \ldots, |N\rangle\}$ that the expectation values among each of the basis states

are equal. Thus the entropy of an orthogonal measurement in this basis is maximal and equal to $\log N$. We show below that such a basis is dual to the basis in which a given state is diagonal, in sense that the norm of all the off-diagonal elements is maximal. Thus any density matrix $\sigma = AA^\dagger/N^2$ constructed out of a random unimodular matrix A has all diagonal elements equal and therefore will be called *contradiagonal*.

A. Procedure of contra–diagonalization of a matrix

Let H be a Hermitian matrix of order N and let $G = VHV^\dagger$ be a unitarily similar matrix, as $VV^\dagger = V^\dagger V = \mathbb{I}_N$. All matrices from this orbit share the same spectrum and posses the same trace, $\mathrm{Tr}G = \mathrm{Tr}H =: t$. For any fixed H we are going to analyze the sum of the squared moduli of off-diagonal elements of G and define a function $f(V) = \sum_{i\neq j} |G_{ij}|^2$. Let us denote by D any hermitian matrix $VHV^\dagger$ for which the function f becomes minimal,

$$D = U_{min} H U_{min}^\dagger \ : f(U_{min}) = \min_{V\in U(N)} \sum_{i\neq j} |(VHV^\dagger)_{ij}|^2. \tag{34}$$

In a similar way let A represent a hermitian matrix $VHV^\dagger$ for which the function f becomes maximal,

$$A = U_{max} H U_{max}^\dagger \ : f(U_{max}) = \max_{V\in U(N)} \sum_{i\neq j} |(VHV^\dagger)_{ij}|^2. \tag{35}$$

It is clear that the minimum $f(U_{min}) = 0$ is achieved for a matrix $U = U_{min}$ consisting of eigenvectors of H, so D is a diagonal matrix of eigenvalues of H or any other matrix similar with respect to permutations $D' = PDP^T$. As the standard procedure to find $D = UHU^\dagger$ is called diagonalization, the transformation of H by U_{max}, leading to the maximum in (35), will be called *contra–diagonalization*. For any given hermitian H we shall show below how to find its contra–diagonalizing matrix $U_{\max}$.

It is well known [50] that any matrix can be unitarily transformed to a form, in which all the diagonal entries are equal. As the trace of a Hermitian matrix H is unitarily invariant this constant reads $H_{jj} = \mathrm{Tr}H/N$ for $j = 1, \ldots, N$.

Let F denote a complex Hadamard matrix [25] of order N, so that F is unitary and the moduli of all its entries are equal, $|F_{jk}| = 1/\sqrt{N}$. As a typical example let us mention the *Fourier matrix* of size N with entries $(F_N)_{jk} = \exp(ijk\pi/N)/\sqrt{N}$ for $j, k = 0, \ldots, N-1$. Two complex Hadamard matrices are called equivalent, written $H_2 \sim H_1$, if they are equivalent up to enphasing and permutations, $H_2 = P_1 E_2 H_1 E_2 P_2$. Here E_1 and E_2 denote diagonal unitary matrices while P_1 and P_2 represent permutation matrices of order N. For $N = 2, 3$ and $N = 5$ all complex Hadamard matrices are equivalent to the Fourier matrices F_2, F_3 and F_5 respectively, see [25].

In order to compare spectra of hermitian matrices it is convenient to use the notion of majorization. Consider vectors of size N ordered decreasingly, $x_1 \geq x_2 \geq \ldots x_N$. A vector y is said to *majorize* [36] vector x, written $x \prec y$, if partial sums satisfy following inequalities $\sum_{i=1}^m x_i \leq \sum_{i=1}^m y_i$ for $m = 1, \ldots, N-1$ and additionally $\sum_{i=1}^N x_i = \sum_{i=1}^N y_i$. A function $f : \mathbb{R}^N \to R$ is said to be Schur convex when $x \prec y$ implies $f(x) \leq f(y)$.

Now we can formulate the following result.

Proposition 1 *Let H be a Hermitian matrix of order N and let V be unitary. Then*

a) the maximum in (35) is obtained for $U_{\max} = FU_{min}$ where U_{min} denotes the matrix of eigenvectors of H and F is a complex Hadamard matrix,

b) the matrix $A = U_{max} H U_{max}^\dagger$ obtained in this way is contradiagonal, $A_{jj} = \mathrm{Tr}H/N$ for $j = 1, \ldots, N$,

c) the maximum reads $f_{max}(V) = \mathrm{Tr}H^2 - (\mathrm{Tr}H)^2/N$.

Proof of Proposition 1.

First to show item b) we consider first diagonal matrix $H = D$ and take an arbitrary complex Hadamard matrix F and find that $A = FDF^\dagger$ is contradiagonal, as all its diagonal elements are equal,

$$(FDF^\dagger)_{ii} = \sum_{kl} F_{ik} D_{kl} (F^\dagger)_{li} = \sum_k F_{ik} D_{kk} \overline{F_{ik}} = \sum_k |F_{ik}|^2 D_{kk} = \frac{1}{N} \mathrm{Tr}D. \tag{36}$$

Consider now any hermitian matrix H and denote by U the matrix of its eigenvectors. Thus taking a unitary matrix $U_{\max} = FU_{min}$ we see that the transformed matrix

$$A = U_{max} H U_{max}^\dagger = FU_{min} H U_{min}^\dagger F^\dagger \tag{37}$$

is contradiagonal, as all its diagonal elements are equal, as stated in item b).

To prove item a) we note, that the sum in (35) is maximized, if and only if the sum

$$\sum_i |(VHV^\dagger)_{ii}|^2 \tag{38}$$

is minimized, since the vector of diagonal elements majorizes the constant vector of the same sum, and the sum of squares is a Schur-convex function we obtain the result.

The last item c) is obtained from the definition of the function f by computing the trace of H^2 and subtracting the sum of squared elements at the diagonal.

A generalization of this procedure allowing to find a basis in which Hermitian matrix with spectrum y has diagonal $x \prec y$ is presented in Appendix B.

Proposition 2 *Consider a family of unitarily similar hermitian matrices*

$$G = VDV^\dagger, \tag{39}$$

where D is a given diagonal matrix, then the maximal Hilbert-Schmidt distance between the orbit of the unitarily similar matrices to diagonal matrix D optimized with respect to all permutation matrices is given by

$$\max_{V\in U(N)}\min_{P\in Perm}\|D-PVDV^\dagger P^T\|^2_{\rm HS}=2\left({\rm Tr}D^2-\frac{({\rm Tr}D)^2}{N}\right), \tag{40}$$

and for the optimal matrix $V_{\rm opt}$ one can take any complex Hadamard matrix F.

Consider an arbitrary hermitian matrix H, such that $H=UDU^\dagger$, so its diagonalization corresponds to transforming the basis by the matrix U consisting of eigenvectors. The above lemma explains why representing it in the basis $W=FU^\dagger$ can be called contra–diagonalization, as the matrix $A=WHW^\dagger$ has all diagonal elements equal and is as far from the diagonal matrix as possible.

Proof of Proposition 2. To prove the lemma we write

$$\begin{aligned}&\max_{V\in U(N)}\min_{P\in Perm}\|D-PVDV^\dagger P^T\|^2_{\rm HS}=\\&\max_{V\in U(N)}\min_{P\in Perm}2{\rm Tr}D^2-2{\rm Tr}DPVDV^\dagger P^T.\end{aligned} \tag{41}$$

Next we note, that

$$\max_{P\in Perm}{\rm Tr}DPVDV^\dagger P^T=\max_{P\in Perm}\langle d|Pq^{(V)}\rangle, \tag{42}$$

where d is a diagonal of matrix D and $q^{(V)}$ is a diagonal of matrix $VDV^\dagger$. It is easy to see that one obtain the maximum value if the vectors are ordered in the same way, i.e.

$$\max_{P\in Perm}\langle d|Pq^{(V)}\rangle=\langle d^\downarrow|(q^{(V)})^\downarrow\rangle. \tag{43}$$

To perform minimization over the set of unitary matrices $V\in U(N)$ we note that the minimum value for the above inner product is achieved, if vector q is minimal in the majorization partial order,

$$\min_{V\in U(N)}\langle d^\downarrow|(q^{(V)})^\downarrow\rangle\le\frac{\sum d_i}{N}\sum d_i=\frac{({\rm Tr}D)^2}{N}. \tag{44}$$

The above minimum can be achieved if the unitary matrix V is complex Hadamard for instance the Fourier matrix F_N.

To summarize the proof we write

$$\begin{aligned}&\max_{V\in U(N)}\min_{P\in Perm}\|D-PVDV^\dagger P^T\|^2_{\rm HS}\\&\qquad=2\left({\rm Tr}D^2-\frac{1}{N}({\rm Tr}D)^2\right),\end{aligned} \tag{45}$$

and every complex Hadamard matrix V gives the maximum and in this case one can take any permutation matrix P. □

B. Contradiagonal density matrices

The statements on contra-diagonalization introduced above for arbitrary hermitian (or normal) matrices can be now used for a positive definite density matrices $\rho^\dagger=\rho\ge 0$ normalized as ${\rm Tr}\rho=1$. Thus a quantum state σ of size N will be called *contradiagonal* if $\sigma_{ii}=1/N$ for $i=1,\ldots,N$.

Spectral density for the ensemble of contradiagonal states obtained form a random unimodular matrix A by Eq. (4) is shown Fig. 6 for $N=2,3,4$. For $N=2$ a random contradiagonal density matrix takes the form $\sigma=\frac{1}{2}\begin{bmatrix}1 & z\\ \bar z & 1\end{bmatrix}$, where $z=e^{i\psi_1}+e^{i\psi_2}$ and the phases ψ_1 and ψ_2 are random. Thus the rescaled eigenvalues of σ are distributed according to the arcsin law, $P_{\rm As}(x)=1/\pi\sqrt{x(2-x)}$ for $x\in(0,2)$, as shown in Fig. 6.

Note oscillations of the level density $P(x)$ present for $N\ge 3$. Observe that the conjectures above yield all the moments for any value of the matrix size N. It is then a classic moment problem to find the corresponding density. Curiously, there exists densities that have the exact same moments on different intervals and are found in [35] as a sequence of densities that converges to the MP distribution. We were however unable to solve this moment problem, to find the actual oscillatory one that is found for the unimodular ensemble. While the appearance of multiple densities with the same moments is known in the literature [38], this seems to be a curious case as the densities have support in $(0,1]$. The fact that the densities diverge at the origin makes the current moment problem not belong to the class of Haussdorf moment problems that treat compact intervals and absolutely continuous densities [38].

The Schur–Horn theorem states [37] that for any density matrix ρ its diagonal is majorized by the spectrum, ${\rm diag}(\rho)\prec{\rm eig}(\rho)$. The uniform vector $x_*=\{1/N,\ldots,1/N\}$ is majorized by any other probability vector. This observation implies the following fact

Proposition 3 *Let σ denotes a contradiagonal state of order N, so that $\sigma_{ii}=1/N$, and let U be a unitary matrix of order N. Then the following majorization relation holds*

$${\rm diag}(\sigma)\ \prec\ {\rm diag}(U\sigma U^\dagger)\ \prec\ {\rm eig}(\sigma). \tag{46}$$

The above result provides an additional argument in favor of usage of the notion of a contra–diagonal form of a matrix, as σ is distinguished by the majorization order (46) and is opposite to the diagonal form of a density matrix.

Let ρ denote an arbitrary density matrix, $U_{\rm min}$ the matrix of its eigenvectors and $U_{\rm max}=FU_{\rm min}$ the matrix defining the bases in which the state is contradiagonal. Then the entropy of the projective measurement of ρ with respect to the basis $U_{\rm max}$ is maximal and equal

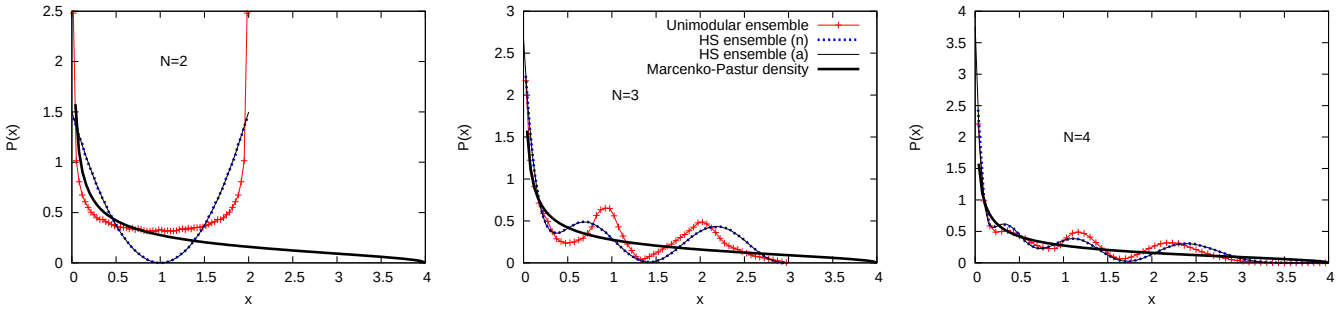

FIG. 6. Distribution of squared singular values $P(x)$ for random unimodular matrices of order a) $N = 2$, b) $N = 3$ and c) $N = 4$ (crosses). The case $N = 2$ is described by the arcsin distribution supported in $[0, 2]$, while the asymptotic behavior corresponds to the MP distribution represented by solid lines. The corresponding density of random states distributed according to the Hilbert-Schmidt measure is marked with dots for comparison, while the exact expressions are also plotted.

to $\ln N$. Note that this basis is hence dual to the eigenbasis of ρ for which the entropy of the projective measurement is minimal and equals to the von Neumann entropy $S(\rho)$. As each projective measurement induces the decoherence to the system and copies the information on the eigenstates of the density matrix to the environment, the information copied in the case of the measurement in the contra-diagonal basis is the largest and reads $\ln N - S(\rho)$. In other words, performing a coarse–graining map, $\rho \to \rho' = \mathrm{diag}(\rho)$ on any pure state $\rho = |\psi\rangle\langle\psi|$, the exchange entropy [39] is the largest if the state is represented in the contra-diagonal basis.

Consider, for instance, a single–qubit pure state written its eigenbasis as $H = \mathrm{diag}(1, 0)$. Making use of the real Hadamard matrix F_2 and putting it into Eq. (37) one gets the contradiagonal state σ where

$$F_2 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad \text{and} \quad \sigma = \frac{1}{2} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}. \tag{47}$$

Choosing a complex Hadamard matrix F_2' enphased with an arbitrary complex phase $e^{\imath\phi}$ we obtain a more general contradiagonal state σ' with

$$F_2' = \frac{1}{\sqrt{2}} \begin{bmatrix} e^{i\phi} & e^{i\phi} \\ 1 & -1 \end{bmatrix}, \quad \sigma' = \frac{1}{2} \begin{bmatrix} 1 & e^{i\phi} \\ e^{-i\phi} & 1 \end{bmatrix}. \tag{48}$$

In higher dimensions, a density matrix $|\psi\rangle\langle\psi|$ corresponding to a pure state of size N with spectrum $\mathrm{diag}(1, 0, \ldots, 0)$ transformed as in (37) by the Fourier matrix F_N leads to a flat contradiagonal state σ with all elements equal, $\sigma_{ij} = 1/N$. Multiplying F_N from left and right by two arbitrary diagonal unitary matrices one obtains an enphased, complex Hadamard F_N' [25], which leads to a more general form of a complex Hermitian contradiagonal state σ' with all elements of the same modulus, $|\sigma'_{ij}| = 1/N$, and all diagonal elements equal, $\sigma'_{jj} = 1/N$.

As stated in Proposition 1 the sum of squared moduli of the off diagonal elements is maximal if and only if the matrix is in its contra–diagonal form. The above is equivalent to the fact, that the sum of squared diagonal elements is minimal. On the other hand, since the geometric mean is a Schur concave function, the product of diagonal elements of a semi positive matrix H is maximal if H is contradiagonal. This fact was used in the analysis of an entanglement measure called *collectibility* [40].

VI. CONCLUDING REMARKS

In this work we showed that a generic random diagonal gate acting on a symmetric bipartite system is strongly non-local and is amazingly efficient in generating quantum entanglement. Its average Schmidt strength [14] is on average smaller than this characteristic of a Haar random unitary gate by the factor of two, while the mean entangling powers [9] for both ensembles are only marginally different.

Investigation of the ensemble of diagonal unitary gates of size N^2 leads to the unimodular ensemble of matrices of order N with all entries of the same modulus and independent random phases. We computed first moments of the distribution of the squared singular values of these matrices and showed that it asymptotically converges to the universal Marchenko-Pastur form. The moments have remarkable connections to combinatorial structures that have been recently studied. This allowed us to find the mean entanglement, or von Neumann entropy exactly for the ensemble of unimodular matrices. However, for a finite N we reported the differences with respect to the Hilbert-Schmidt ensemble, which produces, on average, less mixed states.

Squared singular values of a matrix from the unimodular ensemble after a suitable normalization coincide with the spectrum of a density matrix σ of order N, such that all their diagonal elements are equal. This form of a matrix is called contradiagonal, as it is shown to be opposite to the diagonal form of a matrix concerning the majorization order, the norm of the off-diagonal elements and the entropy of the projective measurement performed on a mixed state in such a basis.

In general, for any Hermitian matrix H of order N

we have shown how to find a unitary matrix $U_{\max}$ which brings it to the contra–diagonal form, $H' = U_{\max} H U_{\max}^\dagger$ such that $H'_{jj} = \mathrm{Tr}H/N$. This method based on diagonalization and complex Hadamard matrices [25] can be easily applied for any mixed state ρ to transform it to its contradiagonal form, distinguished form the perspective of quantum information processing.

From a mathematical perspective the problem of constructing a Hermitian matrix with a given spectrum and prescribed diagonal entries was studied in [41, 42] and more recently in [43]. Although several general algorithms for this task were analyzed in these papers, the limiting problem of a constant diagonal was not shown to be reducible to the standard diagonalization procedure followed by a unitary transformation with an arbitrary complex Hadamard matrix.

It is a pleasure to thank Sarika Jalan for the invitation to the CNSD, at IIT Indore, where this work has been initiated. We are thankful to Paweł Horodecki for stimulating discussions and fruitful remarks. We acknowledge support by the grants number DEC-2011/02/A/ST1/00119 and DEC-2012/04/S/ST6/00400 (ZP) financed by Polish National Science Center.

Appendix A: Reshuffling and operator entanglement entropy

In this appendix a link between the operator Schmidt decomposition and an the reshuffling of a matrix [24] is reviewed.

Consider a given unitary matrix U of size $N^2 \times N^2$. It belongs to the composite Hilbert–Schmidt space $\mathcal{H}_{HS} \otimes \mathcal{H}_{HS}$. Let us write down its representation in a product basis in the space of matrices,

$$U = \sum_{m=1}^{N^2} \sum_{n=1}^{N^2} C_{mn} B_m \otimes B_n, \tag{A1}$$

where $C_{mn} = \mathrm{Tr}((B_m \otimes B_n)^\dagger U)$.

The complex matrix C of order $N^2 \times N^2$ need not be Hermitian nor normal. The usual Schmidt decomposition hold for this vector space and therefore the Schmidt decomposition of U given in Eq.(1) consists of K terms entering with the weights $\sqrt{\Lambda_k}$ equal to the singular values of C.

It will be convenient to work with the product bases in the HS space of matrices, generated by the identity matrix, of size $N^2 \times N^2$. Each of the N^2 basis matrices B_n of size $N \times N$ has only a single non vanishing element equal to unity. Let's denote $B_k = B^{m\mu} = |m\rangle\langle\mu|$, where $k = N(m-1) + \mu$.

For this choice of the basis the matrix of the coefficients C in Eq. (A1) takes a particularly simple form,

$$C_{\substack{m\mu \\ n\nu}} = \mathrm{Tr}(B^{m\mu} \otimes B^{n\nu}) U = U_{\substack{mn \\ \mu\nu}}. \tag{A2}$$

Note that both matrices U and C consist of the same entries, ordered in a different way. This particular reordering of a matrix, called *reshuffling* [24], will be denoted as $U^R := C$. In general the notion of reshuffling is well defined if a matrix X acts on a composite Hilbert space, $\mathcal{H}_M \otimes \mathcal{H}_N$. The symbol U^R has a unique meaning if a concrete decomposition of the total dimension, $L = MN$, is specified. Similar reorderings of matrices were considered by Hill et al. [44, 45] while investigating CP maps and also in [46–48] to analyze separability of mixed quantum states and in [49] to generate local unitary invariants. This operation in these latter contexts is also referred to as *realignment*.

To get a better feeling of the transformation of reshuffling observe that reshaping each row of an arbitrary matrix X of length N^2 into a submatrix of size N and placing it according to the lexicographical order block after block produces the reshuffled matrix X^R as defined in (A2). Let us illustrate this procedure for the simplest case $N = 2$, in which any row of the matrix X is reshaped into a 2×2 matrix

$$C_{kj} = X^R_{kj} := \left[\begin{array}{cc|cc} \mathbf{X_{11}} & \mathbf{X_{12}} & X_{21} & X_{22} \\ X_{13} & X_{14} & \mathbf{X_{23}} & \mathbf{X_{24}} \\ \hline \mathbf{X_{31}} & \mathbf{X_{32}} & X_{41} & X_{42} \\ X_{33} & X_{34} & \mathbf{X_{43}} & \mathbf{X_{44}} \end{array}\right]. \tag{A3}$$

It is easy to see that $(X^R)^R = X$. In general, N^3 elements of X do not change their position during the operation of reshuffling, these are typeset in bold in Eq. (A3). the other $N^4 - N^3$ elements do. It is worth to emphasize that if a matrix X is Hermitian the reshuffled matrix X^R needs not to be Hermitian.

The Schmidt coefficients of U are thus equal to squared singular values Λ_i of the reshuffled matrix, U^R, equal to the eigenvalues of a positive matrix $H = (U^R)^\dagger U^R$. The gate U is local if and only if the rank K of H is equal to one, so that the matrix can be factorized into a product form, $U = U_A \otimes U_B$.

The squared Hilbert-Schmidt norm of any unitary matrix of order N^2 is $||U||^2 = N^2$, which implies that $\sum_{k=1}^{N^2} \Lambda_k = N^2$. To characterize nonlocality of a gate U one can then use the normalized vector $\vec{\lambda}$ of the squared singular values, $\lambda_k := \Lambda_k / N^2$, which may be interpreted as a probability vector of length N^2.

In general, the vector of the Schmidt coefficients of an unitary matrix U acting on a composite $N \times N$ system conveys information concerning the non-local properties of U. To characterize quantitatively the distribution of $\vec{\lambda}$ one uses the Shannon entropy,

$$S(U) := S(\vec{\lambda}) = -\sum_{k=1}^{N^2} \lambda_k \ln(\lambda_k) \tag{A4}$$

called in this context *entropy of entanglement* of U [10], (or *Schmidt strength* [14]), and the generalized, Rényi

entropies

$$S_q(U) := S_q(\vec{\lambda}) = -\frac{1}{1-q}\ln\Big[\sum_{k=1}^{N^2}(\lambda_k)^q\Big], \qquad \text{(A5)}$$

which tend to S in the limit $q \to 1$. The entropy S_0, sometimes called *Hartley entropy*, is equal to $\ln K$, where K denotes the number of positive coefficients λ_i, and is called *Schmidt rank* (or Schmidt number). The second order Rényi entropy S_2 is closely related to the linear entropy $E(U) = 1 - \exp(-S_2)$ used by Zanardi in [10].

The generalized entropies S_q are equal to zero if and only if the gate U has a product structure, so it can be obtained by performing local gates. The upper bound, $S_q^{\max} = 2\log N$ is achieved e.g. for the Fourier unitary matrix of size N^2 defined by

$$F_{kl}^{(N^2)} \;:=\; \frac{1}{N}\exp\big(i2\pi kl/N^2\big)\ . \qquad \text{(A6)}$$

To show this fact it is sufficient to notice that the reshuffled matrix F^R remains unitary, so all its singular values are equal to unity, hence the Schmidt vector contains N^2 equal components and is maximally mixed.

Appendix B: Hermitian matrices with prescribed spectrum

We begin with a fact, known as a Horn lemma [37]

Lemma 4 *Assume that $x \prec y$ then there exist an orthostochastic matrix $\mathcal{O}$ such, that $x = \mathcal{O}y$.*

The matrix $\mathcal{O}$ is said to be orthostochastic, if there exist an orthogonal matrix W, such that $\mathcal{O}_{ij} = W_{ij}^2$.

The above lemma in the case of bistochastic matrix instead of orthostochastic is well known [50], and sometimes used in a definition of majorization.

The Horn lemma allows us to formulate a simple lemma, which is a generalization of Proposition 1(b).

Lemma 5 *Let H be a Hermitian matrix with spectrum y and let $x \prec y$, then there exist a unitary matrix V, such that the diagonal of $VHV^\dagger$ is given by x.*

To prove it we assume, without loss of generality, that H is in its diagonal form with vector y on diagonal, and let $\mathcal{O}$ be an orthostochastic matrix such that $x = \mathcal{O}y$. By W we denote an orthogonal matrix such that $\mathcal{O}_{ij} = W_{ij}^2$. Now we write

$$(WHW^T)_{ii} = \sum_k W_{ik}H_{kk}W_{ik} = \sum_k \mathcal{O}_{ik}y_k = x_i. \quad \text{(B1)}$$

In other words the unitary matrix V which describes the unitary transformation can be represented as a product of a unitary matrix W appearing in the Horn lemma and the matrix $U^\dagger$ containing eigenvectors of H. In particular if x is flat, i.e. all x_i are equal, the matrix W present in the Horn lemma can be taken as a complex Hadamard matrix and item (b) in Proposition 1 is recovered.

This allows us to obtain an alternative solution to the problem of constructing Hermitian matrices with prescribed spectrum, studied in [41–43].

[1] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009).
[2] E. Lubkin, J. Math. Phys. **19**, 1028 (1978).
[3] D. Page, Phys. Rev. Lett. **71**, 1291 (1993).
[4] K. Życzkowski and H.-J. Sommers, Induced measures in the space of mixed quantum states, J. Phys. A: Math. Theory **34**, 7111 (2001).
[5] P. Hayden, D. W. Leung, and A. Winter, Commun. Math. Phys. **265**, 95 (2006).
[6] S. Sen, Phys. Rev. Lett. **77**, 1 (1996).
[7] C. Nadal, S.N. Majumdar, and M. Vergassola, J. Stat. Phys. **142**, 403 (2011).
[8] U. T. Bhosale, S. Tomsovic and A. Lakshminarayan, Phys. Rev. A **85**, 062331 (2012).
[9] P. Zanardi, C. Zalka and L. Faoro, On the entangling power of quantum evolutions, Phys. Rev. A **62**, 030301(R) (2000).
[10] P. Zanardi, Entanglement of quantum evolution, Phys. Rev. A**63**, 040304(R), (2001).
[11] K. Hammerer, G. Vidal and J.I. Cirac, Characterization of non-local gates, Phys. Rev. A **66**, 062321 (2002).
[12] J. Zhang, J. Vala, K.B. Whaley and S. Sastry, A geometric theory of non-local two-qubit operations, Phys. Rev. A **67**, 042313 (2003).
[13] X. Wang, B. C. Sanders, and D. W. Berry, Entangling power and operator entanglement in qudit systems, Phys. Rev. A **67**, 042323 (2003).
[14] M. A. Nielsen, C. M. Dawson, J. L. Dodd, A. Gilchrist, D. Mortimer, T. J. Osborne, M. J. Bremner, A. W. Harrow and A. Hines, Quantum dynamics as physical resource, Phys. Rev. A **67**, 052301 (2003).
[15] A. J. Scott, Multipartite entanglement, quantum-error-correcting codes, and entangling power of quantum evolutions, Phys. Rev. A **69**, 052330 (2004).
[16] S. Balakrishnan, R. Sankaranarayanan, Characterizing the geometrical edges of nonlocal two-qubit gates, Phys. Rev. A **79**, 052339 (2009).
[17] M. Musz, M. Kuś, and K. Życzkowski, Unitary quantum gates, perfect entanglers and unistochastic maps, Phys. Rev. A **87**, 022111 (2013).
[18] Y. Nakata, P. S. Turner, and M. Murao, Phase-random states: Ensembles of states with fixed amplitudes and uniformly distributed phases in a fixed basis, Phys. Rev. A **86**, 012301 (2012).
[19] Y. Nakata, M. Koashi, and M. Murao, Generating a state t-design by diagonal quantum circuits, New Journal of Physics **16**, 053043 (2014).

[20] M. J. Bremner, R. Jozsa, and D. J. Shepherd, Proc. R. Soc. A **465** 459 (2011).

[21] M. J. Hoban, J. J. Wallman, H. Anwar, N. Usher, R. Raussendorf, and D. E. Browne, Phys. Rev. Lett. **112**, 140505 (2014).

[22] F. Haake, *Quantum Signatures of Chaos*, 3rd. ed., Springer, Berlin, 2010.

[23] J. N. Bandyopadhyay and A. Lakshminarayan, Phys. Rev. Lett. **89**, 060402 (2002).

[24] K. Życzkowski and I. Bengtsson, On duality between quantum states and quantum maps, Open Syst. Inf. Dyn. **11**, 3-42 (2004).

[25] W. Tadej and K. Życzkowski, A concise guide to complex Hadamard matrices, Open Syst. Inf. Dyn. 13, 133-177 (2006).

[26] T. Tao, V. Vu, Random matrices: Universality of local eigenvalue statistics, Acta Mathematica **206**, 127, (2011).

[27] H.–J. Sommers and K. Życzkowski, Statistical properties of random density matrices, J. Phys. A: Math. Theory. **37** 8457-8466 (2004).

[28] G. Akemann, M. Kieburg and L. Wei, Singular value correlation functions for products of Wishart random matrices, J. Phys. A: Math. Theory. **46**, 275205 (2013).

[29] T. Koshy, *Catalan Numbers with Applications*, Oxford University Press, New York, 2008.

[30] N. J. A. Sloane, On-line Encyclopedia of Integer Sequences, http://www.research.att.com/∼njas/sequences (2013).

[31] P. Barry, A note on a family of generalized Pascal matrices defined by Riordan arrays, J. Integer Seq. **16**, Article 13.5.4, (2013).

[32] C. Francisco, J. Mermin, and Jay Schweig, https://www.math.okstate.edu/∼jayjs/ppt.pdf, (2013).

[33] Christian Kassel, and Christophe Reutenauer, Algebraicity of the zeta function associated to a matrix over a free group algebra, arXiv:1303.3481v5 [math.CO].

[34] T. A. Brody, J. Flores, J. B. French, P. A. Mello, A. Pandey, and S. S. M. Wong, Rev. Mod. Phys. **53**, 385 (1981).

[35] K. Życzkowski, K. A. Penson, I. Nechita, B. Collins, Generating random density matrices, J. Math. Phys. **52**, 062201(20) (2011).

[36] A. W. Marshall and O. Olkin, *Inequalities: Theory of Majorization and Its Applications* New York: Academic, 1979.

[37] I. Bengtsson and K. Życzkowski, *Geometry of Quantum States. An introduction to quantum entanglement* (Cambridge University Press, Cambridge, 2006).

[38] T. W. Korner, *Fourier Analysis* (Cambridge University Press, Cambridge, 1988).

[39] B. Schumacher, Sending entanglement through noisy quantum channels, Phys. Rev. A **54**, 2614–2628 (1996).

[40] Ł. Rudnicki, Z. Puchała, P. Horodecki, K. Życzkowski, Collectibility for mixed quantum states, *Phy. Rev. A*, 86, (6), 062329, (2012).

[41] M. T. Chu, Constructing a Hermitian matrix from its diagonal entries and eigenvalues, SIAM J. Matrix Anal. Appl. **16**, 207217 (1995).

[42] I.S. Dhillon, R. W. Heath Jr. M. A. Sustik and J.A. Tropp, Generalized finite algorithms for constructing hermitian matrices with prescribed spectrum, SIAM J. Matrix Anal. 27, 6171 (2005).

[43] M. Fickus, D.G. Mixon, M.J. Poteet, N. Strawn, Constructing all self-adjoint matrices with prescribed spectrum and diagonal, Adv. Comput. Math. **39**, 585-609 (2013).

[44] C. J. Oxenrider and R. D. Hill, On the matrix reordering Γ and Ψ, Linear Alg. Appl. **69**, 205 (1985).

[45] D. A. Yopp and R. D. Hill, On completely copositive and decomposable linear transformations, Linear Alg. Appl. **312**, 1 (2000).

[46] O. Rudolph, On the cross norm criterion for separability, J. Phys. A: Math. Theory. **36**, 5825 (2003).

[47] K. Chen and L.-A. Wu, A matrix realignment method for recognizing entanglement, Quant. Inf. Comp. **3**, 193 (2003).

[48] M. Horodecki, P. Horodecki, and R. Horodecki, Characterization of separable states: Linear contractions, and permutattion criteria, Open Systems Inform. Dynamics **13**, 103 (2004).

[49] U. T. Bhosale, K. V. Shuddhodan, and A. Lakshminarayan, Phys. Rev. A **87**, 052311 (2013).

[50] R. A. Horn, C. R. Johnson, *Topics in Matrix Analysis* Cambridge University Press, New York (1991).