

Average fidelity between random quantum states

Karol Życzkowski^{1,2,3,*} and Hans-Jürgen Sommers^{4,†}¹*Instytut Fizyki im. Smoluchowskiego, Uniwersytet Jagielloński, ulica Reymonta 4, 30-059 Kraków, Poland*²*Centrum Fizyki Teoretycznej, Polska Akademia Nauk, Aleja Lotników 32/44, 02-668 Warszawa, Poland*³*Perimeter Institute, Waterloo, Ontario, Canada N2L 2Y5*⁴*Fachbereich Physik, Universität Duisburg-Essen, Campus Essen, 45117 Essen, Germany*

(Received 11 May 2004; published 15 March 2005)

We analyze mean fidelity between random density matrices of size N , generated with respect to various probability measures in the space of mixed quantum states: the Hilbert-Schmidt measure, the Bures (statistical) measure, the measure induced by the partial trace, and the natural measure on the space of pure states. In certain cases explicit probability distributions for the fidelity are derived. The results obtained may be used to gauge the quality of quantum-information-processing schemes.

DOI: 10.1103/PhysRevA.71.032313

PACS number(s): 03.67.Mn, 03.65.Ta, 03.65.Ud

I. INTRODUCTION

Modern applications of quantum theory renewed interest in the characterization of the set of mixed quantum states. It is often necessary to quantify how a certain mixed state may be approximated by another one. For this purpose one may use various distances defined in the space of mixed quantum states, e.g., the trace distance, the Hilbert-Schmidt (HS) distance, and the Bures distance [1]. The last distance is a function of *fidelity* [2], and may be considered as a generalization of the overlap between pure states [3]. Fidelity between a pair of mixed states is equal to unity if and only if they do coincide. Optimal fidelity between the input and the output states is used to characterize the quality of a cloning algorithm [4,5].

In various quantum problems one computes the mean fidelity, averaging over a certain ensemble of states. Analyzing the dynamics of quantum chaotic systems one studies the fidelity between a given initial state and its image under the action of the quantum map [6]. To extract global information on the entire system one averages this quantity over the natural, Fubini-Study (FS) measure on the space of initial pure states. The mean fidelity between two images of a random pure state obtained by the action of a certain unitary operation and a certain irreversible, contracting superoperator \mathcal{E} was found by Bowdery *et al.* [7] for qubits and by Nielsen [8] for the more general case of N -dimensional states. Another expression for the average gate fidelity was recently derived by Bagan *et al.* [9], in which the nontrivial term was shown to be proportional to the mean value of the Hilbert-Schmidt scalar product $\langle \text{Tr} \gamma_i \mathcal{E}(\gamma_i) \rangle_i$ of the $SU(N)$ generators γ_i and their images $\mathcal{E}(\gamma_i)$, averaged over all of them, $i=1, \dots, N^2-1$.

In this work we study a complementary problem and analyze the mean fidelity $\langle F \rangle$ between two independent, random states. This problem may be interesting from a practical point of view: The average fidelity may serve as a reference value

for analyzing the mean (maximal and minimal) fidelity achieved in a certain protocol of quantum cloning. For instance, if the measured (computed) fidelity between a certain pair of one-qubit mixed states only slightly exceeds the average value, one should not conclude that these states are more correlated than two generic, random mixed states.

In this way we are in a position to propose a general tool for measuring the quality of a given theoretical scheme of quantum-information processing or its experimental realization. Let \bar{F} denote the mean fidelity between the state obtained in an analyzed cloning protocol and the target state. Then the quality of the protocol may be gauged by the dimensionless coefficient $\alpha = [\bar{F} - \langle F \rangle] / \sqrt{\langle F^2 \rangle - \langle F \rangle^2}$, where $\langle F \rangle$ denotes the average over an appropriate ensemble of random density matrices.

We are also interested in the probability distribution $P(F)$. Two averaging schemes should be distinguished. In the symmetric case, both states are drawn at random according to the same measure (e.g., both pure states or both mixed states generated with respect to the same probability distribution). In the nonsymmetric case, both probability distributions are different: in particular, we study the mean fidelity between a random pure state and a random mixed state, generated with respect to a specified measure.

Let us emphasize here that there exists no single, naturally distinguished probability measure in the set of mixed quantum states [10–12]. Guessing a mixed state of size N at random, we might use additional information, if available. For instance, knowing that the mixed state has arisen by partial tracing over a K -dimensional environment, the induced measure [11] should be used. In particular, if the size K of the environment and the size N of the system are equal, then the measure induced by the partial trace coincides with the Hilbert-Schmidt measure. Without any information concerning the random state whatsoever, it will be legitimate to make use of the Bures measure, related to the Jeffrey prior, statistical distance and the distinguishability.

The paper is organized as follows. In Sec. II we review the basic properties of fidelity, while in Sec. III we introduce the necessary measures in the set of mixed quantum states of size N . The mean fidelity between pure and mixed states is

*Email address: karol@cft.edu.pl

†Email address: sommers@theo-phys.uni-essen.de

analyzed in Sec. IV. The main results of this work are presented in Sec. V, in which we compute the mean fidelity, averaged over two independent random mixed states, generated with respect to an arbitrary induced measure, labeled by the size K of the environment. The probability distribution for fidelity between a random pure state and a random mixed state distributed according to the Bures measure is computed in Appendix B while the derivation of the generating functions for the moments of the root fidelity for two mixed states of arbitrary N generated independently according to an induced measure is given in Appendix A.

II. FIDELITY

Let \mathcal{M}_N denote the set of all mixed quantum states of size N . It contains all Hermitian, semipositive definite matrices of size N , which are trace normalized,

$$\text{Tr}\rho = 1. \tag{2.1}$$

We are going to consider two distances in this set: the *Hilbert-Schmidt distance*

$$D_{\text{HS}}(\rho_1, \rho_2) = \sqrt{\text{Tr}[(\rho_1 - \rho_2)^2]} \tag{2.2}$$

and the *Bures distance* [1,3]

$$[D_B(\rho_1, \rho_2)]^2 = 2 - 2 \text{Tr} \sqrt{\sqrt{\rho_1} \rho_2 \sqrt{\rho_1}} = 2 - 2 \sqrt{F(\rho_1, \rho_2)}, \tag{2.3}$$

respectively.

The Bures distance is distinguished by several remarkable properties: for pure states it agrees with the natural, Fubini-Study distance, while in the space of diagonal density matrices it induces the statistical (Fisher) distance [13]. The Bures distance is a function of *fidelity* [2]:¹

$$F(\rho_1, \rho_2) := [\text{Tr} \sqrt{\sqrt{\rho_1} \rho_2 \sqrt{\rho_1}}]^2. \tag{2.4}$$

This quantity is sometimes called the *Uhlmann transition probability* [3], since for a pair of pure states it reduces to the squared overlap, $F = \text{Tr} \rho_1 \rho_2 = |\langle \psi_1 | \psi_2 \rangle|^2$.

Fidelity enjoys several important properties [2]: it is a symmetric, non-negative, continuous, concave function of both states, unitarily invariant, equal to unity if and only if both states do coincide. Therefore it becomes an important tool to characterize the closeness of any two mixed states, often used in modern applications of quantum mechanics (see, e.g., [14]). The only disadvantage consists in computing it explicitly: to find the fidelity one needs to diagonalize the density matrices, but more importantly, the fidelity stays as a function of the eigenvectors.

Apart from the fidelity F , we will also use the square root fidelity \sqrt{F} . This quantity also satisfies several appealing properties [14] and in certain cases its probability distribution is easier to compute than $P(F)$. Furthermore the quantity $\arccos[\sqrt{F(\sigma, \rho)}]$ has a clear geometric interpretation as the *Bures angle* in the space of mixed states equipped with the

Bures metric. It is equal to the geodesic Riemannian distance between the two mixed states [15,16], and in the case of pure states it coincides with the Fubini-Study distance.

Computation of fidelity is much simpler for $N=2$. To derive an explicit formula for fidelity we use the first steps of the calculation of the Bures distance presented by Hübner [17]. Any 2×2 matrix A obeys the characteristic equation

$$A^2 - A \text{Tr} A + \mathbb{1} \det A = 0. \tag{2.5}$$

Taking the trace we obtain

$$(\text{Tr} A)^2 = \text{Tr} A^2 + 2 \det A. \tag{2.6}$$

Let us now set $A = \sqrt{\sqrt{\rho_1} \rho_2 \sqrt{\rho_1}}$, so that $\text{Tr} A^2 = \text{Tr} \rho_1 \rho_2$ and $\det A = \sqrt{\det \rho_1 \det \rho_2}$. Let (p_1, p_2) denote the spectrum of a state ρ . Hence $1 = (p_1 + p_2)^2 = \text{Tr} \rho^2 + 2 \det \rho$ and $2 \det \rho = 1 - \text{Tr} \rho^2$. Substituting this into Eq. (2.6) we obtain

$$F(\rho_1, \rho_2) = (\text{Tr} A)^2 = \text{Tr} \rho_1 \rho_2 + \sqrt{(1 - \text{Tr} \rho_1^2)(1 - \text{Tr} \rho_2^2)}. \tag{2.7}$$

III. MEASURES IN THE SPACE OF MIXED QUANTUM STATES

Random quantum states may be generated according to different measures, and it is hardly possible to distinguish the unique probability measure in the set of density matrices. Usually one considers product measures, which may be factorized [10,11],

$$d\mu_x = d\nu_x(\lambda_1, \lambda_2, \dots, \lambda_N) \times dh. \tag{3.1}$$

The second factor dh , determining the distribution of the eigenvectors of the density matrix, is the unique, unitarily invariant Haar measure on $U(N)$, while the first factor depends only on the eigenvalues λ_i of ρ and may be chosen by an arbitrary probability distribution $d\nu_x = P_x(\vec{\lambda}) d^N \lambda$. The joint probability distribution is defined on the $(N-1)$ -dimensional simplex Δ_{N-1} , which contains all vectors of non-negative entries summing to unity.

The Hilbert-Schmidt measure, induced by the Hilbert-Schmidt metric, is defined by the following joint probability distribution [10,11]:

$$P_{\text{HS}}^{(N)}(\vec{\lambda}) = \frac{\Gamma(N^2) \delta\left(\sum_{j=1}^N \lambda_j - 1\right)}{\prod_{j=0}^{N-1} \Gamma(N-j) \Gamma(N-j+1)} \prod_{i < j}^N (\lambda_i - \lambda_j)^2. \tag{3.2}$$

The Bures metric leads to the Bures measure in the simplex of eigenvalues,

¹Although this was the original definition of Jozsa, some authors use this name for \sqrt{F} .

$$P_B^{(N)}(\vec{\lambda}) = \frac{2^{N^2-N}\Gamma(N^2/2)}{\pi^{N/2}\Gamma(1)\cdots\Gamma(N+1)} \frac{\delta\left(\sum_{j=1}^N \lambda_j - 1\right)}{\sqrt{\lambda_1\lambda_2\cdots\lambda_N}} \prod_{i<j} \frac{(\lambda_i - \lambda_j)^2}{\lambda_i + \lambda_j}. \quad (3.3)$$

This probability distribution was derived by Hall [10], while the normalization constants were found in [18] for $N=3,4,5$ and in [19] for an arbitrary N .

It is also instructive to consider a family of measures in the space of mixed states of size N induced by the Haar measure on the unitary group $U(NK)$. The integer parameter K , used to label the measure $\mu_{N,K}$, represents the size of an ancilla. A mixed state of size N may be obtained by tracing a certain random pure state $|\Phi\rangle$ of size NK over the K -dimensional ancilla, $\rho = T_K(|\Phi\rangle\langle\Phi|)$. Representing the pure state $|\Phi\rangle$ in an arbitrary product basis $|i,j\rangle = |i\rangle \otimes |j\rangle$ where $i=1, \dots, N$ and $j=1, \dots, K$, we obtain $|\Phi\rangle = \sum_{ij} \Phi_{ij} |i,j\rangle$. The rectangular matrix of coefficients Φ_{ij} of size $N \times K$ allows us to write the reduced state as $\rho = \Phi\Phi^\dagger$. If the matrices Φ are random, the matrices ρ constructed in such a way are called *Wishart matrices*. The probability distribution of eigenvalues of ρ reads [11,20–22]

$$P_{\mu_{N,K}}(\vec{\lambda}) = \frac{\Gamma(KN)\delta\left(\sum_{j=1}^N \lambda_j - 1\right)}{N-1} \prod_i \lambda_i^{K-N} \prod_{i<j} (\lambda_i - \lambda_j)^2 \prod_{j=0}^{K-1} \Gamma(K-j)\Gamma(N-j+1) \quad (3.4)$$

and for $K=N$ reduces to the Hilbert-Schmidt measure (3.2). In the above equation the inequality $K \geq N$ is assumed and this case is called the Wishart case. If this is not the case, (the so-called anti-Wishart case [23,24]) induced measures with $K < N$ are singular, since they are supported by the subspace of states of submaximal rank K which belongs to the boundary of \mathcal{M}_N . In particular, the measure $\mu_{N,1}$ is just the natural Fubini-Study measure on the space of pure states in \mathcal{H}_N , since the partial trace over a one-dimensional ancilla does not change the pure state.

Interestingly, in the one-qubit case, for $K=3/2$, the induced measure (3.4) reduces to the Bures measure (3.3),

$$P_B^{(2)}(\vec{\lambda}) = P_{\mu_{2,3/2}}(\vec{\lambda}). \quad (3.5)$$

Although such a coincidence occurs for a noninteger value of the dimensionality of the environment, and seems not to have any physical meaning, it will help us to obtain some results for the Bures measure by analytical continuation in K . Unfortunately this trick works only in the $N=2$ case, for which $\lambda_1 + \lambda_2 = 1$, so the denominator under the product in the distribution (3.3) is trivially equal to unity.

We are going to study the mean fidelity $\langle F \rangle$ with respect to different measures. Let $\langle F \rangle_\mu$ denote the homogeneous case, in which both arguments of the fidelity are random mixed states, distributed independently with respect to the same probability measure μ . In a more general case we may average over two different measures and such averages will

be denoted by $\langle F \rangle_{\mu_1}^{\mu_2}$. Since fidelity is symmetric $F(\rho_1, \rho_2) = F(\rho_2, \rho_1)$, we have $\langle F \rangle_{\mu_1}^{\mu_2} = \langle F \rangle_{\mu_2}^{\mu_1}$.

An analogous notation will also be used to label probability distributions for fidelity: $P_\mu(F)$ denotes the distribution for the symmetric case, in contrast to $P_{\mu_1}^{\mu_2}(F)$, in which both states are averaged over different measures. To simplify notation, instead of writing $\mu_{N,K}$ as a label denoting a certain induced measure, we shall use the labels N, K .

IV. MEAN FIDELITY: NONSYMMETRIC AVERAGING

A. One state pure, one arbitrary

Computation of fidelity between two states simplifies considerably, if one of the states is pure, $\rho_1 = |\psi_1\rangle\langle\psi_1|$,

$$F(|\psi_1\rangle\langle\psi_1|, \rho_2) = \text{Tr}|\psi_1\rangle\langle\psi_1|\rho_2. \quad (4.1)$$

Working in the basis that contains $|\psi_1\rangle$ we see that fidelity is equal to the matrix element $\rho_{11} := \langle\psi_1|\rho_2|\psi_1\rangle$. We are going to analyze the case in which the random pure state $|\psi_1\rangle$ is generated according to the natural, Fubini-Study measure on the space of pure states. For any mixed state represented in a random basis all components have, on average, the same magnitude; hence

$$\langle F \rangle_{\text{FS}} = \langle F \rangle_{N,1} = \frac{1}{N}. \quad (4.2)$$

If the second random state is also pure, $\rho_2 = |\phi\rangle\langle\phi|$, then the fidelity is equal to the overlap between the two states, $F = |\langle\psi|\phi\rangle|^2$. Assuming both states to be generated independently according to the same FS measure we infer that fidelity is equal to the squared component of a random vector in a random basis. The probability distribution for this quantity

$$P_{N,1}(F) = (N-1)(1-F)^{N-2} \quad (4.3)$$

was derived in [25] while analyzing eigenvectors of a random unitary matrix pertaining to a circular unitary ensemble (CUE) and distributed according to the Haar measure on $U(N)$. Note that this result holds also in the case if one of the pure states (say the second one) is fixed, $P(\rho_2) = \delta(\rho_2 - |\psi_*\rangle\langle\psi_*|)$.

Let us now consider a nonsymmetric averaging: one state $\rho_1 = |\psi_1\rangle\langle\psi_1|$ is pure and is distributed according to the FS measure, while the other one ρ_2 is distributed according to the measure $\mu_{N,K}$ in the space of mixed states. Hence the latter state may be obtained by tracing a certain random pure state $|\Phi\rangle$ of size NK over the K -dimensional ancilla. The fidelity between them, $F(|\psi_1\rangle\langle\psi_1|, \rho_2)$, is given by the sum of K terms, $F = \rho_{11} = \sum_{i=1}^K |c_i|^2$ where c_i , $i=1, \dots, KN$, denote the components of the pure state $|\Phi\rangle$. In our previous work we have analyzed M -dimensional truncations of complex random vectors of dimensionality L and unit length. The length t of the truncated vector was shown to be distributed according to $P(t) \sim t^{2M-1}(1-t^2)^{L-M-1}$ [26]. In the case considered the fidelity is just equal to the squared length, $F = t^2$, the initial length of the vector $L = KN$, and the length of the truncation M is equal to K . Hence changing variables and finding

the normalization constants in terms of the Euler Γ function we arrive at the probability distribution

$$P_{N,K}^{N,1}(F) = \frac{\Gamma(KN)}{\Gamma(K)\Gamma[K(N-1)]} F^{K-1}(1-F)^{K(N-1)-1} \quad (4.4)$$

describing the fidelity F between a random pure state of size N and a random mixed state generated according to the measure $\mu_{N,K}$. In the special case $K=1$ the second state is also pure, and the above formula reduces to (4.3). In the case $K=N$ the mixed state is distributed according to the Hilbert-Schmidt measure, and the probability distribution reads

$$P_{N,HS}(F) = \frac{\Gamma(N^2)}{\Gamma(N)\Gamma[N^2-N]} F^{N-1}(1-F)^{N(N-1)-1}. \quad (4.5)$$

For completeness, let us formulate an analogous result following from studying truncations of real random vectors [26],

$$P_{N,K}^{N,1,R}(F) = \frac{\Gamma(KN/2)}{\Gamma(K/2)\Gamma[K(N-1)/2]} F^{K/2-1}(1-F)^{K(N-1)/2-1}. \quad (4.6)$$

This distribution characterizes fidelity F between a *real* random pure state of size N and a *real* random mixed state generated according to the induced measure.

Let us examine in some detail the special case of $N=2$. If F denotes the fidelity between ρ_2 and $|\psi_1\rangle\langle\psi_1|$ then the fidelity of the same mixed state ρ_2 with respect to any pure state orthogonal to $|\psi_1\rangle$ is equal to $1-F$. Since we average over the entire Bloch sphere of pure states, the probability distribution will be a symmetric function of F and $(1-F)$. This is indeed the case and for $N=2$ the distribution (4.4) reduces to $P_{2,K}^{2,1} \sim F^{K-1}(1-F)^{K-1}$. In particular, for the HS measure ($K=2$) and the Bures measure ($K=3/2$), one obtains

$$P_{2,HS} = 6F(1-F) \text{ and } P_{2,B} = \frac{8}{\pi}\sqrt{F(1-F)}, \quad (4.7)$$

respectively. Equation (4.6) implies analogous results for the rebits,

$$P_{2,HS}^R = 1 \text{ and } P_{2,B}^R = 1. \quad (4.8)$$

Note that for rebits $P_{2,HS}^R$ and $P_{2,B}^R$ coincide, while $K=3/2$ has no direct physical meaning in this case.

In the general case of an arbitrary N it is also possible to analyze the fidelity between a random pure state and a random mixed state, distributed according to the Bures measure. The probability distribution, in a sense complementary to Eq. (4.5),

$$P_{N,B}(F) = \frac{\Gamma(N^2/2)\Gamma(2N-1)}{\Gamma(N)[\Gamma(N-1/2)]^2\Gamma(N^2/2-N)} F^{N-1} \times \int_F^1 \frac{(x-F)^{N^2/2-N-1}(1-x)^{N-3/2} dx}{x^{N^2/2-N+1/2}} \quad (4.9)$$

is derived in Appendix B (to understand the method, it is more helpful first to read Sec. V D and Appendix A). In the case $N=2$ the integral diverges. However this divergence is

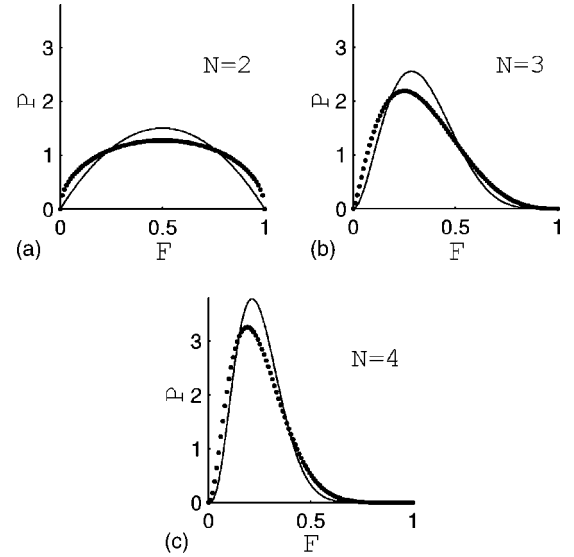


FIG. 1. Probability distribution of fidelity between a random pure state and a random mixed state distributed according to the Hilbert-Schmidt measure, Eq. (4.5), solid line, and the Bures measure, Eq. (4.9), bold dotted line, for $N=(a)$ 2, (b) 3, and (c) 4.

compensated by the last factor $\Gamma(0)$ in the denominator, so it is not too difficult (by partial integration of the first factor under the integral) to show that Eq. (4.9) reduces in this case to the second formula of Eq. (4.7). A comparison of distributions of fidelity between a pure state and a mixed state generated according to the HS measure and the Bures measure is presented in Fig. 1. Observe that the distributions for the Bures measure are broader since the HS measure is more concentrated in the vicinity of the maximally mixed state.

B. One state maximally mixed, one arbitrary

Let us now analyze another special case, if one state is maximally mixed, $\rho_1 = \rho_* := \mathbb{1}/N$. Hence the fidelity with respect to any state $\rho_2 = \rho$ reduces to

$$F(\rho_*, \rho) = \frac{1}{N} (\text{Tr} \sqrt{\rho})^2. \quad (4.10)$$

It is then convenient to study the mean root fidelity

$$\sqrt{F(\rho_*, \rho)} = \frac{1}{\sqrt{N}} \text{Tr} \rho^{1/2}, \quad (4.11)$$

which may be written as a function of the generalized Rényi entropy of order one-half.

Let us now assume that the random state ρ is distributed according to the Hilbert-Schmidt (3.2) or Bures (3.3) measure. Average moments for these ensembles of random density matrices were analyzed in [11,12], in which we derived asymptotic formulas

$$\langle \text{Tr} \rho^q \rangle_{HS} = N^{1-q} \frac{\Gamma(1+2q)}{\Gamma(1+q)\Gamma(2+q)} \left[1 + O\left(\frac{1}{N}\right) \right] \quad (4.12)$$

for the HS measure and

$$\langle \text{Tr} \rho^q \rangle_B = N^{1-q} 2^q \frac{\Gamma[(3q+1)/2]}{\Gamma[(1+q)/2]\Gamma(2+q)} \left[1 + O\left(\frac{1}{N}\right) \right] \quad (4.13)$$

for the Bures measure. Substituting $q=1/2$ we find asymptotic results for the fidelity of a random mixed state with respect to the maximally mixed state

$$\langle \sqrt{F(\rho_*, \rho)} \rangle_{\text{HS}} = \frac{8}{3\pi} \approx 0.843 \quad (4.14)$$

for the HS measure and

$$\langle \sqrt{F(\rho_*, \rho)} \rangle_B = \frac{\sqrt{2}\Gamma(5/4)}{\Gamma(3/4)\Gamma(5/2)} \approx 0.787 \quad (4.15)$$

for the Bures measure. Observe that both results, valid in the limit $N \rightarrow \infty$, converge asymptotically to some nontrivial constants, independent of N . Comparison of the Bures and the Hilbert-Schmidt measures reveals that the former favors states of a larger purity [11], hence the mean value with respect to the Bures measure (4.15) is smaller than the analogous result (4.14) for the HS measure.

V. MEAN FIDELITY: SYMMETRIC AVERAGING

We are going to analyze the symmetric problem of computing average fidelity between two random states, *both* of which are generated according to the same probability distribution covering the entire set of mixed states.

A. Case $N=2$, average values

For $N=2$ the problem simplifies considerably since the explicit formula (2.7) may be used. The expectation value $\langle \text{Tr} \rho_1 \rho_2 \rangle = 1/2$ if ρ_1 and ρ_2 are independent random mixed states generated with respect to any product measure (3.1). To show this let us write both states in the Pauli matrix representation

$$\rho = \frac{1}{2} + \vec{\tau} \cdot \vec{\lambda}. \quad (5.1)$$

The vector of the normalized Pauli matrices, $\vec{\lambda} = \vec{\sigma}/\sqrt{2}$, together with the rescaled identity matrix $1/\sqrt{2}$, form an orthonormal basis in the set of 2×2 complex matrices in the sense of the Hilbert-Schmidt scalar product $\langle A|B \rangle = \text{Tr} A^\dagger B$. Expanding in this basis the scalar product

$$\text{Tr} \rho_1 \rho_2 = \frac{1}{2} + \vec{\tau}_1 \cdot \vec{\tau}_2 \quad (5.2)$$

we see that due to symmetry of the distribution of the orientation of the Bloch vector $\vec{\tau}$ the second term does not contribute to the average $\langle \text{Tr} \rho_1 \rho_2 \rangle$. For any $N=2$ mixed state one has $\text{Tr} \rho^2 = 1/2 - r^2$ where $r = |\vec{\tau}|$ denotes the length of the Bloch vector and $r \in [0, 1/\sqrt{2}]$. Thus the fidelity may be expressed by [17] [see Eq. (2.7)]

$$F(\rho_1, \rho_2) = \vec{\tau}_1 \cdot \vec{\tau}_2 + \frac{1}{2} + \sqrt{\frac{1}{2} - r_1^2} \sqrt{\frac{1}{2} - r_2^2}, \quad (5.3)$$

so to compute the mean fidelity averaged over *both* random mixed states distributed according to a given measure in the space of mixed states it is sufficient to find the expected value of the following function of the radius $t = \sqrt{\frac{1}{2} - r^2}$, averaged with respect to an appropriate measure. The Hilbert-Schmidt measure covers the entire Bloch ball uniformly, so $P_{\text{HS}}(r) = 6\sqrt{2}r^2$ [10] and it is straightforward to find the average $\langle t \rangle_{\text{HS}}$, which leads to

$$\langle F \rangle_{\text{HS}} = \frac{1}{2} + \langle t \rangle_{\text{HS}}^2 = \frac{1}{2} + \frac{9}{512} \pi^2 \approx 0.6735. \quad (5.4)$$

In the same way we may evaluate the mean fidelity $\langle F \rangle_{\mu_{2,K}}$ with respect to the induced measures obtained by the partial trace of pure states of the $2K$ -dimensional Hilbert space with an arbitrary natural K . The probability distribution for eigenvalues, given explicitly in [11], implies the following radial distribution:

$$P_K(r) = \frac{2^{K+3/2} \Gamma\left(K - \frac{1}{2}\right)}{\sqrt{\pi} \Gamma(K-1)} \left(\frac{1}{2} - r^2\right)^{K-2} r^2. \quad (5.5)$$

The expectation values of t may be readily expressed by the Euler Gamma function and allow us to compute the average fidelity. For instance, in the case of the $K=3$ induced measure we obtain

$$\langle F \rangle_{2,3} = \frac{1}{2} + \left(\frac{15}{128} \sqrt{2} \pi\right)^2 \approx 0.7711, \quad (5.6)$$

while the general result for any $K \geq 2$ reads

$$\langle F \rangle_{2,K} = \frac{1}{2} + \frac{1}{2} \left(\frac{\Gamma\left(K + \frac{1}{2}\right) \Gamma\left(K - \frac{1}{2}\right)}{\Gamma(K+1) \Gamma(K-1)} \right)^2 \quad (5.7)$$

and for $K=2$ reduces to Eq. (5.4). In the limit of an infinitely large ancilla, $K \rightarrow \infty$, the double quotient of the Γ functions tends to unity, so $\lim_{K \rightarrow \infty} \langle F \rangle_{2,K} = 1$. This result is rather intuitive, since in this limit all random states tend to be close to the maximally mixed state ρ_* .

In the case of the Bures measure, the states of larger purity (larger radius r) are preferred and $P_B(r) = (8/\pi) r^2 / \sqrt{\frac{1}{2} - r^2}$ [10,11]. Note that the expression (5.5) includes the above case of the Bures metric by analytic continuation: $K \rightarrow 3/2$. Computing the mean value $\langle t \rangle_B$ we arrive at the result

$$\langle F \rangle_B = \frac{1}{2} + \langle t \rangle_B^2 = \frac{1}{2} + \frac{8}{9\pi^2} \approx 0.590, \quad (5.8)$$

which was independently obtained by Bagan *et al.* [27] and is a particular case of (5.7) with $K=3/2$.

It is worth emphasizing that for any product measure in the space of qubits the average fidelity is not smaller than $1/2$. The equality occurs for the Fubini-Study measure $\langle F \rangle_{\text{FS}} = 1/2$, since this measure is concentrated exclusively on the pure states, $P_{\text{FS}}(r) = \delta(r-R)$, so that the last term in Eq. (5.3) vanishes. Here R stands for the Hilbert-Schmidt radius of the Bloch ball, $R = \sqrt{2}/2$.

B. Case $N=2$, probability distribution

In order to calculate the probability distribution $P_{2,K}(F)$ we are going to use Eq. (5.3) and integrate out the angle ϑ between \vec{r}_1 and \vec{r}_2 and the radii $r_i \in [0, R]$,

$$P_{2,K}(F) = \frac{1}{2} \int_0^R dr_1 \int_0^R dr_2 \int_0^\pi \sin \vartheta d\vartheta P_K(r_1) P_K(r_2) \times \delta \left[F - r_1 r_2 \cos \vartheta - \frac{1}{2} - \sqrt{\frac{1}{2} - r_1^2} \sqrt{\frac{1}{2} - r_2^2} \right]. \quad (5.9)$$

The radial distribution $P_K(r)$ for the measure induced by tracing over K -dimensional environment is given in Eq. (5.5).

One first integrates out the angle ϑ . Using the property of the step function $\theta(x-F) - \theta(y-F) = \theta((x-F)(F-y))$ for $x > y$ and performing a partial integration one finds

$$P_{2,K}(F) = C(K) [F(1-F)]^{2(K-1)} \times \int_0^1 \frac{dx}{x} \left(x + \frac{1}{x} + 2(1-2F) \right)^{2(1-K)} \quad (5.10)$$

with

$$C(K) = 2(K-1) \left(\frac{\Gamma(2K)}{\Gamma(K)^2} \right)^2. \quad (5.11)$$

We see that the expression is analytic in K . For $K \rightarrow 1$ we obtain $P_{2,1}(F) = 1 = \text{const}$. The last integral can be done for an integer $2(K-1)$ and we obtain

$$P_{2,K}(F) = C(K) \left(\frac{F(1-F)}{4} \right)^{2(K-1)} \frac{1}{(2K-3)!} \left(\frac{d}{dF} \right)^{2K-3} \times \frac{\arccos(1-2F)}{\sqrt{F(1-F)}}. \quad (5.12)$$

Interestingly the simplest case is obtained for the Bures metric

$$P_{2,B}(F) = P_{2,3/2}(F) = \frac{16}{\pi^2} \sqrt{F(1-F)} \arccos(1-2F), \quad (5.13)$$

while for the Hilbert-Schmidt metric ($K=2$) we obtain

$$P_{2,2}(F) = \frac{9}{2} F(1-F) - \frac{9}{4} \sqrt{F(1-F)} (1-2F) \arccos(1-2F). \quad (5.14)$$

These probability distributions are presented in Fig. 2 together with exemplary numerical results. The behavior for $K \rightarrow \infty$ may be obtained by a saddle-point calculation, which we start from the form

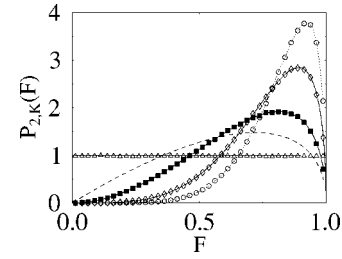


FIG. 2. Probability distribution of fidelity for random one-qubit states generated according to the induced measures $\mu_{2,K}$ where $K = 1$ (Δ), 2 (\square), 3 (\diamond), and 4 (\circ). Flat distribution represents averaging over pure states, while full symbols refer to the Hilbert-Schmidt measure, $K=N=2$. Solid lines represent Eqs. (4.3) and (5.10), while dashed line denotes the case $K=3/2$ corresponding to the Bures distribution (5.13).

$$P_{2,K}(F) = C(K) [F(1-F)]^{2(K-1)} \times \frac{1}{2} \int_0^\infty \frac{dx}{x} \left[x + \frac{1}{x} + 2(1-2F) \right]^{2(1-K)} \quad (5.15)$$

using the symmetry of the integral with respect to the inversion $x \rightarrow 1/x$. We find as asymptotic form for $K \rightarrow \infty$

$$P_{2,K}(F) = \frac{\Gamma(2K+1/2)}{\Gamma(3/2)\Gamma(2K-1)} F^{2(K-1)} \sqrt{1-F} \left[1 + O\left(\frac{1}{K}\right) \right]. \quad (5.16)$$

As expected, for large dimensionality K this distribution tends to a δ function located at $\langle F \rangle$, which in the limit $K \rightarrow \infty$ tends to unity according to Eq. (5.7).

C. General case, $N \geq 3$, average values

In the general case one has to use the general formula for fidelity Eq. (2.4), not as convenient for analytical computations as Eq. (2.7) valid for $N=2$. Before describing the analytical results let us compare the problem for an arbitrary N with the symmetric case, in which the averaging in both arguments is performed over the set of pure states. For any nonsingular measure covering the entire set of mixed states, the mean value will be larger than $1/N$, since the mean distance between random mixed states is smaller than the mean distance between random pure states.

This statement concerns in particular all induced measures $\mu_{N,K}$ analyzed for a fixed system size N . Since the mean purity decreases with the size K of the ancilla, $\langle \text{Tr} \rho^2 \rangle = (N+K)/(NK+1)$ [11], one may infer that $\langle F \rangle_{N,K} > \langle F \rangle_{N,L}$ if $K > L$. In the analogy to the simplest case $N=2$ one may thus expect that for any N the mean fidelity tends to unity, $\lim_{K \rightarrow \infty} \langle F \rangle_{N,K} = 1$.

Veracity of this reasoning may be checked by analysis of the following general results, derived in Appendix A for an arbitrary induced measure $\mu_{N,K}$. We are going to study the moments of the root fidelity $\langle \sqrt{F} \rangle_{N,K}$, so the second moment gives the average fidelity. Let us denote $n = K - N \geq 0$ and introduce constants

$$G(m) = \left(\frac{\Gamma(KN)}{\Gamma(KN+m/2)} \right)^2. \quad (5.17)$$

Defining an auxiliary matrix of size N

$$(X_n)_{k,l} := \Gamma(n+k+l-1)\Gamma(n+l) \text{ for } k, l = 1, 2, \dots, N. \quad (5.18)$$

the rather complicated averages may be written down in a concise way,

$$\langle \sqrt{F} \rangle_{N,K} = G(1) \text{Tr}[X_n^{-1} X_{n+1/2}] \quad (5.19)$$

and

$$\langle F \rangle_{N,K} = G(2) \{ \text{Tr}(X_n^{-1} X_{n+1}) + [\text{Tr}(X_n^{-1} X_{n+1/2})]^2 - \text{Tr}[(X_n^{-1} X_{n+1/2})^2] \}. \quad (5.20)$$

The above formula is one of the main results of this paper. For $N=2$ one needs to work with matrices X_n of size 2. Computing the necessary traces one shows that Eq. (5.20) simplifies to formula (5.7), while Eq. (5.19) allows us to write down an explicit formula

$$\langle \sqrt{F} \rangle_{2,K} = \left(\frac{\Gamma(2K)}{\Gamma(2K + \frac{1}{2})} \right)^2 \left[\frac{3}{2} \left(\frac{\Gamma(K + \frac{1}{2})}{\Gamma(K)} \right)^2 + \frac{1}{2} \left(\frac{\Gamma(K - \frac{1}{2})}{\Gamma(K-1)} \right)^2 \right]. \quad (5.21)$$

For large K this average tends to unity. This result was derived for $K \geq N$, and it is ill defined, e.g., for $K=1$. Interestingly, by an analytical continuation $K \rightarrow 1$ one obtains the correct result for averaging over the space of pure states, $\langle \sqrt{F} \rangle_{2,1} = 2/3$, in agreement with the trivial integral $\int_0^1 \sqrt{F} dF$ following from the uniform distribution (4.3) with $N=2$. For the Bures measure we have $\langle \sqrt{F} \rangle_{2,3/2} = 2^7 13 / (3^2 5^2 \pi^2) \approx 0.7493$, while the average for the HS measure ($K=2$) is larger, $\langle \sqrt{F} \rangle_{2,2} = 2^5 31 / (5^2 7^2) \approx 0.8098$.

Analogous results obtained for $N=3$ from Eqs. (5.19) and (5.20) read

$$\langle \sqrt{F} \rangle_{3,K} = \left(\frac{\Gamma(3K)}{\Gamma(3K + \frac{1}{2})} \right)^2 \left[\frac{3}{8} \left(\frac{\Gamma(K - \frac{3}{2})}{\Gamma(K-2)} \right)^2 + \frac{3}{4} \left(\frac{\Gamma(K - \frac{1}{2})}{\Gamma(K-1)} \right)^2 + \frac{15}{8} \left(\frac{\Gamma(K + \frac{1}{2})}{\Gamma(K)} \right)^2 \right] \quad (5.22)$$

and

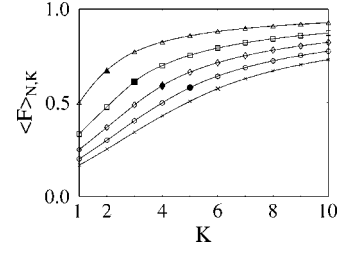


FIG. 3. Mean fidelity averaged over both states distributed according to the induced measure $\mu_{N,K}$, as a function of the size K of the ancilla for $N=2$ (Δ), 3 (\square), 4 (\diamond), 5 (\circ), and 6 (\times). Solid lines denote analytical results, Eqs. (5.7) and (5.20). Full symbols represent averaging over the Hilbert-Schmidt measure, $K=N$.

$$\langle F \rangle_{3,K} = \frac{1}{3} + \frac{1}{K^2} \left[\left(\frac{\Gamma(K - \frac{1}{2})}{\Gamma(K-1)} \right)^2 \left[\frac{5}{12} \left(\frac{\Gamma(K + \frac{1}{2})}{\Gamma(K)} \right)^2 + \frac{1}{12} \left(\frac{\Gamma(K - \frac{3}{2})}{\Gamma(K-2)} \right)^2 \right] + \frac{1}{6} \left(\frac{\Gamma(K + \frac{1}{2})\Gamma(K - \frac{3}{2})}{\Gamma(K)\Gamma(K-2)} \right)^2 \right]. \quad (5.23)$$

In the limit $K \rightarrow \infty$ both results tend to unity, e.g., $\langle F \rangle_{3,K} \rightarrow \frac{1}{3} + \frac{5}{12} + \frac{1}{12} + \frac{1}{6} = 1$. As in the case $N=2$, the above formulas hold for $K \geq N$, but by analytical continuation for $K \rightarrow 1$ one obtains correct results for averaging over the space of pure states $\langle \sqrt{F} \rangle_{3,1} = 8/15$ and $\langle F \rangle_{3,1} = 1/3$. Also results in the limit $K \rightarrow 2$, $\langle F \rangle_{3,2} = 1/3 + 15(\pi/32)^2 \approx 0.4779$ agree with the data obtained numerically by averaging over the manifold of the mixed states with rank $K=2$. Numerical results obtained from a sample of 10^6 random states, presented in Fig. 3, confer with predictions obtained by means of the general formula (5.20). Interestingly, the mean fidelity for the HS measure, $K=N$, decreases with the system size N .

D. General case, $N \geq 3$, probability distributions

Figure 4 presents the distributions of fidelity $P_{N,K}(F)$, averaged symmetrically over both states distributed according to the induced measures $\mu_{N,K}$ for $N=2, 3$, and 4. Analytical

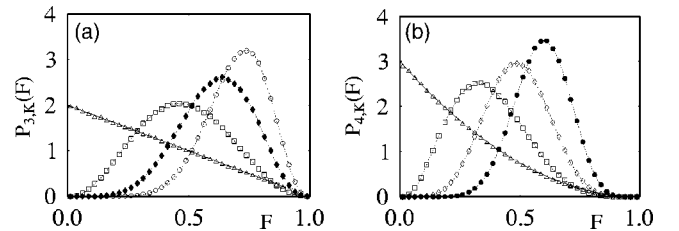


FIG. 4. Probability distribution of fidelity while averaging symmetrically over both states distributed according to induced measures $\mu_{N,K}$. The size of the system equals $N=(a)$ 3 and (b) 4 and while the size K of the ancilla is coded by symbols: $K=1$ (Δ), 2 (\square), 3 (\diamond), and 4 (\circ). Full symbols represent averaging over Hilbert-Schmidt measure, $K=N$. Solid line for $K=1$ denotes Eq. (4.3), dotted lines are plotted to guide the eye.

results (4.3) available for pure states ($K=1$) are marked by solid lines. In general, the larger size K of the ancilla, the more the distribution is shifted toward higher values of F , since both states get closer to the maximally mixed state. For large size of the ancilla the distributions become concentrated at the mean value $\langle F \rangle_{N,K}$ which tends to unity in the limit $K \rightarrow \infty$.

Obtaining explicitly analytical results for the probability distribution $P_{N,K}(F)$ in the general case of arbitrary N and K seems not to be simple. However, we may obtain required information concerning these distributions by studying the sequence of higher moments of the root fidelity. Knowing all moments $\langle (\sqrt{F})^m \rangle_{N,K}$ for $m=2,4,\dots$ we may in principle extract the desired distribution $P_{N,K}(F)$. To compute such moments for $K \geq N$ we construct a generating function

$$Z(\lambda) = \det \left[\sum_{m=0}^{\infty} \frac{(-\lambda)^m}{m!} \Gamma\left(\frac{m}{2} + k + l + K - N - 1\right) \times \Gamma\left(\frac{m}{2} + l + K - N\right) \right] \quad (5.24)$$

which we obtain by replacing the fixed trace ensembles for ρ_1 and ρ_2 by Laguerre ensembles and integrating out eigenvectors of $\sqrt{\rho_1} \rho_2 \sqrt{\rho_1}$ with the help of the Itzykson-Zuber integral. The determinant concerns an $N \times N$ matrix with indices $k, l=1, \dots, N$. To obtain the mean values of $(\sqrt{F})^m$ one needs to multiply the expansion coefficients of $Z(\lambda)$ by constants $G(m)$ defined in Eq. (5.17):

$$\langle (\sqrt{F})^m \rangle_{N,K} = G(m) (-d/d\lambda)^m Z(\lambda) / Z(0) |_{\lambda=0}. \quad (5.25)$$

For any fixed N the moments are analytic in K , so one may try to use the analytic extension for the cases $K < N$. Alternatively, we may treat this case separately, investigating another generating function

$$Z_K(\lambda) = \det \left\{ \sum_{m=0}^{\infty} \frac{(-\lambda)^m}{m!} \left[\Gamma\left(\frac{m}{2} + k + N - K\right) \right]^2 \times \frac{\Gamma(m/2 + k + l - 1)}{\Gamma(m/2 + k + l + N - 2K)} \right\} \quad (5.26)$$

with determinant of a $K \times K$ matrix with indices $k, l=1, \dots, K$. This formula holds for $N \geq 2K$, but may be extended analytically in N beyond this restriction. It is obtained by reducing $\sqrt{\rho_1} \rho_2 \sqrt{\rho_1}$ by unitary rotations to the spaces of nonzero eigenvalues with dimension $K \leq N$ using the symmetry properties of the fidelity and again integrating out all unitary rotations with the help of the Itzykson-Zuber integral (here applied twice).

To show an application of this approach let us expand the generating function Z_K up to the second order in λ . Fixing $K=2$ we obtain the averages for variable N

$$\langle \sqrt{F} \rangle_{N,2} = \frac{\sqrt{\pi}}{16} (22N - 13) \left(\frac{\Gamma(2N)}{\Gamma\left(2N + \frac{1}{2}\right)} \right)^2 \frac{\Gamma\left(N - \frac{1}{2}\right)}{\Gamma(N)} \quad (5.27)$$

and

$$\langle F \rangle_{N,2} = \frac{1}{N} \left[1 + \frac{3\pi}{16} \frac{\Gamma\left(N - \frac{1}{2}\right) \Gamma\left(N + \frac{1}{2}\right)}{\Gamma(N-1) \Gamma(N+1)} \right]. \quad (5.28)$$

These formulas are valid for arbitrary N , and for $N=2,3$ are consistent with Eqs. (5.21)–(5.23). In a similar way one may proceed with $K=3,4,\dots$. Furthermore, expanding the generating function to the m th order one could calculate the expectation values of $(\sqrt{F})^m$ and obtain further information concerning the probability distribution $P_{N,K}(F)$. There are analogous formulas for the moments $\langle (\sqrt{F})^m \rangle_{N,K}$ to Eqs. (5.19) and (5.20) in terms of traces involving $K \times K$ matrices.

To give an explicit expression for the distribution of fidelity $P_{N,K}(F) = W(\sqrt{F}) / 2\sqrt{F}$ we start from the fixed trace ensemble with traces $t_1 = \text{Tr} \rho_1$, $t_2 = \text{Tr} \rho_2$, $t_3 = \text{Tr}(\sqrt{\rho_1} \rho_2 \sqrt{\rho_1})^{1/2}$. We take the Laplace transform with respect to t_1, t_2, t_3 , calculate it, and then apply the inverse Laplace transform at $t_1 = 1, t_2 = 1$, and $t_3 = \sqrt{F}$. What we obtain is a threefold contour integral

$$W(\sqrt{F}) = C \int \frac{ds_1 e^{s_1}}{2\pi i s_1^{KN}} \int \frac{ds_2 e^{s_2}}{2\pi i s_2^{KN}} \int \frac{ds_3 e^{\sqrt{F}s_3}}{2\pi i} Z\left(\frac{s_3}{\sqrt{s_1 s_2}}\right) \quad (5.29)$$

with $C = \Gamma(K^2 N^2) / Z(0)$. It is easy to see that this equation is equivalent to Eq. (5.25). All three contours go along the whole imaginary axis with a small positive real part. We need the analytic properties of the function $Z(x)$ which can be seen from the form

$$Z(x) = \det \left(2 \int_0^{\infty} dy \frac{y^{k-2} \Gamma[k-1+2(K-N+l)]}{(y+1/y+x)^{k-1+2(K-N+l)}} \right). \quad (5.30)$$

$Z(x)$ has a cut along the real axis for $x \leq -2$ and behaves asymptotically for $x \rightarrow \infty$ like $(\ln x)^N / x^{2KN}$, which is not easy to see, but can be derived from the explicit form for $Z(x)$,

$$Z(x) = \det[(d/dx)^{2(K-N+l-1)+k} H_k(x) \ln(x/2 + \sqrt{x^2/4 - 1})] \quad (5.31)$$

with

$$H_k(x) = -[(x/2 + \sqrt{x^2/4 - 1})^{k-1} + (x/2 - \sqrt{x^2/4 - 1})^{k-1}] / \sqrt{x^2/4 - 1}. \quad (5.32)$$

For later use we need also for $x > 2$ (in the following $\epsilon > 0$)

$$\lim_{\epsilon \rightarrow 0} [Z(-x - i\epsilon)] = \det[(d/dx)^{2(K-N+l-1)+k} H_k(x) \ln(x/2 + \sqrt{x^2/4 - 1}) + i\pi(d/dx)^{2(K-N+l-1)+k} H_k(x)]. \quad (5.33)$$

Using appropriate contour deformations and partial integrations we are able to perform the s_1 and s_2 integrations, arriving at

$$W(\sqrt{F}) = \frac{\Gamma(K^2 N^2)}{Z(0)\pi^2} \lim_{\epsilon \rightarrow 0} \left(\int_2^\infty dx B(x) \text{Im}[Z(-x - i\epsilon)] \right) \quad (5.34)$$

with

$$B(x) = F^{KN-1} \int_2^{2/\sqrt{F}} \frac{dy}{\sqrt{1 - Fy^2/4}} \frac{\theta(x-y)(x-y)^{2KN-3}}{(2KN-3)!}. \quad (5.35)$$

Finally for numerical convenience we may use the following integral representations for $x > 2$: $Z(x) = \det(A_1)$ and $\lim_{\epsilon \rightarrow 0} [Z(-x - i\epsilon)] = \det(A_1 - iA_2)$ with

$$A_1 = 4 \int_0^\infty \frac{du \cosh[(k-1)u] \Gamma(k-1+2(K-N+l))}{[2 \cosh(u) + x]^{k-1+2(K-N+l)}} \quad (5.36)$$

and

$$A_2 = 4 \int_0^\pi \frac{du \cos[(k-1)u] \Gamma(k-1+2(K-N+l))}{[2 \cos(u) + x]^{k-1+2(K-N+l)}}, \quad (5.37)$$

where $k, l = 1, \dots, N$, so A_1 and A_2 are square matrices of size N .

VI. CONCLUDING REMARKS

In this work we have posed and solved the problem of computing the average fidelity between two random quantum states. As easy to predict, the results depend heavily on the probability measure according to which the quantum states are generated. We have concentrated on two cases we consider to be the most important: the Bures measure μ_B , used to guess a random state of size N in lack of any other information, and the induced measure $\mu_{N,K}$, applied if it is known that the mixed state is obtained by a partial trace over a K -dimensional environment. The latter case reduces to the Hilbert-Schmidt measure if $K=N$.

In general, one has to distinguish the case of symmetric averaging, in which both states are generated according to the same measure, and the asymmetric case, e.g., the problem of computing the mean fidelity between a pure random state and a mixed random state.

In particular we have obtained explicit results for symmetric averaging over the induced measures $\mu_{N,K}$, which have a simple physical interpretation. The mean value $\langle F \rangle_{N,K}$ corresponds to the case of picking at random pure states in

$(N \times K)$ -dimensional Hilbert space and then studying the fidelity between two mixed states obtained by partial tracing over the K -dimensional environment.

In certain cases we have derived the probability distribution for fidelity $P(F)$ which may be used to formulate statistical statements that evaluate quantitatively certain quantum operations and quantum protocols. For instance, the universal protocol of quantum cloning of an N -dimensional pure state gives the fidelity $F_u = (N+3)/(2N+2)$ [28]. Making use of the distribution (4.3) we see that the probability p_N that a randomly taken N -dimensional pure state will give a better fidelity than that obtained by the cloning procedure is equal to

$$p_N = \int_{F_u}^1 P_{N,1}(F) dF = \frac{1}{2^{N-1}} \left(\frac{N-1}{N+1} \right)^{N-1}. \quad (6.1)$$

For $N=2$ there exists a considerable probability $p_2 = 1/6$ that picking at random a pure state of a qubit provides results better than the cloning protocol. However, for larger system sizes the probability p_N decreases exponentially with N , which means that the relative strength of the cloning procedure with respect to the ‘‘random choice’’ strategy increases with the size of the system.

ACKNOWLEDGMENTS

We thank D. Savin for useful discussions and I. Bengtsson, R. Muoz-Tapia, and A. Uhlmann for helpful correspondence. This work was supported by Sonderforschungsbereich/Transregio 12 der Deutschen Forschungsgemeinschaft and Grant No. PBZ-MIN-008/P03 of the Polish Committee for Scientific Research.

APPENDIX A: GENERATING FUNCTIONS FOR MOMENTS

1. Induced measures: Wishart case, $K \geq N$

In this appendix we present a brief derivation of the generating functions for moments of the square-root fidelity which hold for an arbitrary induced measure $\mu_{N,K}$. In the first subsection we consider the case $K \geq N$. Then the distribution of square-root fidelity is given by

$$W(\sqrt{F}) \propto \int D\rho_1 \int D\rho_2 \det(\rho_1 \rho_2)^{K-N} \times \delta(1 - \text{Tr}\rho_1) \delta(1 - \text{Tr}\rho_2) \delta(\sqrt{F} - \text{Tr}(\sqrt{\rho_1} \rho_2 \sqrt{\rho_1})^{1/2}), \quad (A1)$$

where $D\rho_1$ and $D\rho_2$ are the matrix volume elements and we have to integrate over positive matrices ρ_1 and ρ_2 . Since $\text{Tr}[(\sqrt{\rho_1} \rho_2 \sqrt{\rho_1})^{1/2}]$ is a homogeneous function of both ρ_1 and ρ_2 of degree $1/2$, moments can equivalently be obtained from the generating function

$$Z(\lambda) \propto \int D\rho_1 \int D\rho_2 \det(\rho_1 \rho_2)^{K-N} e^{-\text{Tr}\rho_1} e^{-\text{Tr}\rho_2} \times e^{-\lambda \text{Tr}[(\sqrt{\rho_1} \rho_2 \sqrt{\rho_1})^{1/2}]} \quad (A2)$$

following Eq. (5.25). We make a transformation ρ_2

$\rightarrow \rho_1^{-1/2} \rho_2 \rho_1^{-1/2}$ and taking into account the Jacobian we obtain

$$Z(\lambda) \propto \int D\rho_1 \int D\rho_2 \det(\rho_1)^{-N} \det(\rho_2)^{K-N} e^{-\text{Tr}\rho_1} e^{-\text{Tr}\rho_2/\rho_1} \times e^{-\lambda \text{Tr}(\rho_2)^{1/2}}. \quad (\text{A3})$$

Note that the difficult square roots have disappeared and we can use the Itzykson-Zuber integral to integrate out the eigenvectors of ρ_2 in the expression $e^{-\text{Tr}\rho_2/\rho_1}$. As result we obtain

$$Z(\lambda) \propto \int_0^\infty \frac{dx_1}{x_1} \dots \frac{dx_N}{x_N} \int dy_1 \dots dy_N (y_1 \dots y_N)^{K-N} e^{-(x_1 + \dots + x_N)} \times e^{-\lambda(\sqrt{y_1} + \dots + \sqrt{y_N})} \det(e^{-y_k/x_l}) \prod_{k<l} (x_k - x_l)(y_k - y_l) \quad (\text{A4})$$

where x_1, \dots, x_N are the eigenvalues of ρ_1 and y_1, \dots, y_N are the eigenvalues of ρ_2 . Using the properties of the Vandermonde determinant we reduce this expression to a single determinant and arrive at Eq. (5.30).

2. Induced measures: Anti-Wishart case, $K < N$

In this case the matrices ρ_1 and ρ_2 are of rank K and they can be obtained by a unitary transformation of the form

$$U = \begin{pmatrix} \sqrt{1 - XX^\dagger} & -X \\ X^\dagger & \sqrt{1 - X^\dagger X} \end{pmatrix}$$

to block diagonal form. If U is drawn from the CUE it can be shown that the corresponding measure DX is flat, where X is a complex $K \times (N-K)$ matrix with the restriction $XX^\dagger \leq 1$. Calling the nonzero blocks again ρ_1 and ρ_2 , now $K \times K$ matrices, we may write the generating function for moments as

$$Z_K(\lambda) \propto \int D\rho_1 \int D\rho_2 \int_{XX^\dagger \leq 1} DX \det(\rho_1 \rho_2)^{N-K} e^{-\text{Tr}\rho_1} e^{-\text{Tr}\rho_2} \times e^{-\lambda \text{Tr}[(\sqrt{\rho_1} \sqrt{1 - XX^\dagger} \rho_2 \sqrt{1 - XX^\dagger} \sqrt{\rho_1})^{1/2}]}. \quad (\text{A5})$$

In a first step we make the transformation $\rho_2 \rightarrow (1 - XX^\dagger)^{-1/2} \rho_2 (1 - XX^\dagger)^{-1/2}$, arriving at

$$Z_K(\lambda) \propto \int D\rho_1 \int D\rho_2 \int_{XX^\dagger \leq 1} DX \frac{\det(\rho_1 \rho_2)^{N-K}}{\det(1 - XX^\dagger)^N} e^{-\text{Tr}\rho_1} \times e^{-\text{Tr}\rho_2/(1 - XX^\dagger)} e^{-\lambda \text{Tr}[(\sqrt{\rho_1} \rho_2 \sqrt{\rho_1})^{1/2}]}. \quad (\text{A6})$$

Then we use the symmetry $\text{Tr}[(\sqrt{\rho_1} \rho_2 \sqrt{\rho_1})^{1/2}] = \text{Tr}[(\sqrt{\rho_2} \rho_1 \sqrt{\rho_2})^{1/2}]$ and make the transformation $\rho_1 \rightarrow \rho_2^{-1/2} \rho_1 \rho_2^{-1/2}$, leading to

$$Z_K(\lambda) \propto \int D\rho_1 \int D\rho_2 \int_{XX^\dagger \leq 1} DX \frac{\det(\rho_1)^{N-K}}{\det(\rho_2)^K \det(1 - XX^\dagger)^N} \times e^{-\text{Tr}\rho_1/\rho_2} e^{-\text{Tr}\rho_2/(1 - XX^\dagger)} e^{-\lambda \text{Tr}\sqrt{\rho_1}}. \quad (\text{A7})$$

Now we see that the matrix $W = XX^\dagger$ is again of the Wishart type and is positive definite for $K \leq (N-K)$. Let us focus on

this case; then the distribution of W is proportional to $\det(W^{N-2K})$ and we may reduce the integral to the eigenvalues x_1, \dots, x_K of ρ_1 , y_1, \dots, y_K of ρ_2 , and z_1, \dots, z_K of W using twice the Itzykson-Zuber integral. The resulting expression contains in the integrand the Vandermonde determinants of x_1, \dots, x_K and of z_1, \dots, z_K and can therefore again be reduced to a single determinant which is given by

$$Z_K(\lambda) = \det \left\{ 2 \int_0^\infty dx \int_0^\infty \frac{dy}{y} \int_0^1 dz \frac{x^{N-K+k-1} z^{N-2K}}{(1-z)^{N-K-l+1}} \times \exp \left[-\sqrt{\frac{x}{1-z}} \left(y + \frac{1}{y} \right) \right] e^{-\lambda \sqrt{x}} \right\}. \quad (\text{A8})$$

Expanding the threefold integral in powers of λ , one arrives at Eq. (5.26).

APPENDIX B: DERIVATION OF THE DISTRIBUTION (4.9)

To derive the distribution $P(F)$ for the fidelity between a random pure state and a random mixed state distributed according to the Bures measure (3.3) consider

$$P(F) \propto \int_{\rho>0} D\rho \int_{A=A^\dagger} DA \delta(1 - \text{Tr}\rho A^2) \delta(1 - \text{Tr}\rho) \times \delta(F - \text{Tr}\rho|\psi\rangle\langle\psi|), \quad (\text{B1})$$

where we introduced an auxiliary Hermitian matrix A to generate the distribution (3.3) and the last two δ functions correspond to the constraints (2.1) and (4.1). The δ functions may be written as inverse Laplace transforms along the imaginary axis shifted slightly to the right and then the integration over the positive definite $N \times N$ matrix ρ can be done, arriving at

$$P(F) \propto \int \frac{ds_1 e^{s_1}}{2\pi i} \int \frac{ds_2 e^{s_2}}{2\pi i} \int \frac{ds_3 e^{F s_3}}{2\pi i} \times \int DA \det(s_1 A^2 + s_2 + s_3 |\psi\rangle\langle\psi|)^{-N}. \quad (\text{B2})$$

After a suitable rescaling of the matrix A , we can do the s_1 and s_3 integrations and obtain

$$P(F) \propto \int \frac{DA}{\det(1 + A^2)^N} \int_{-i\infty+\epsilon}^{+i\infty+\epsilon} \frac{ds e^s}{2\pi i s^{N/2-2-N}} \times [\langle\psi|(1 + A^2)^{-1}|\psi\rangle]^{-N} F^{N-1} \exp\left(-\frac{sF}{\langle\psi|(1 + A^2)^{-1}|\psi\rangle}\right). \quad (\text{B3})$$

Now it is possible to show that with the correspondence $U = (1 + iA)/(1 - iA)$ the measure $DA/\det(1 + A^2)^N$ is equivalent to the invariant measure on the group of unitary $N \times N$ matrices U . Since only $\langle\psi|(1 + A^2)^{-1}|\psi\rangle = \langle\psi|(2 + U + U^\dagger)/4|\psi\rangle$ occurs, the integration over A can be reduced to a one-dimensional one and after integrating over s in the complex plane and restoring the normalization we end up with formula (4.9).

- [1] D. J. C. Bures, *Trans. Am. Math. Soc.* **135**, 199 (1969).
- [2] R. Jozsa, *J. Mod. Opt.* **41**, 2315 (1994).
- [3] A. Uhlmann, *Rep. Math. Phys.* **9**, 273 (1976).
- [4] V. Bužek and M. Hillery, *Phys. Rev. A* **54**, 1844 (1996).
- [5] N. J. Cerf, *Phys. Rev. Lett.* **84**, 4497 (2000).
- [6] T. Prosen, *Phys. Rev. E* **65**, 036208 (2002).
- [7] M. D. Bowdrey, D. K. L. Oi, A. J. Short, K. Banaszek, and J. A. Jones, *Phys. Lett. A* **294**, 258 (2002).
- [8] M. A. Nielsen, *Phys. Lett. A* **303**, 249 (2002).
- [9] E. Bagan, M. Baig, and R. Muñoz-Tapia, *Phys. Rev. A* **67**, 014303 (2003).
- [10] M. J. Hall, *Phys. Lett. A* **242**, 123 (1998).
- [11] K. Życzkowski and H.-J. Sommers, *J. Phys. A* **34**, 7111 (2001).
- [12] H.-J. Sommers and K. Życzkowski, *J. Phys. A* **37**, 8457 (2004).
- [13] D. Petz and C. Sudár, *J. Math. Phys.* **37**, 2662 (1996).
- [14] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, U.K., 2000).
- [15] A. Uhlmann, *Phys. Lett. A* **161**, 329 (1992).
- [16] A. Uhlmann, *Rep. Math. Phys.* **36**, 461 (1995).
- [17] M. Hübner, *Phys. Lett. A* **163**, 239 (1992).
- [18] P. B. Slater, *J. Phys. A* **32**, 8231 (1999).
- [19] H.-J. Sommers and K. Życzkowski, *J. Phys. A* **36**, 10083 (2003).
- [20] E. Lubkin, *J. Math. Phys.* **19**, 1028 (1978).
- [21] S. Lloyd and H. Pagels, *Ann. Phys. (N.Y.)* **188**, 186 (1988).
- [22] D. Page, *Phys. Rev. Lett.* **71**, 1291 (1993).
- [23] Y.-K. Yu and Y.-C. Zhang, *Physica A* **312**, 1 (2002).
- [24] R. A. Janik and M. A. Nowak, *J. Phys. A* **36**, 3629 (2003).
- [25] M. Kuś, J. Mostowski, and F. Haake, *J. Phys. A* **21**, L1073 (1988).
- [26] K. Życzkowski and H.-J. Sommers, *J. Phys. A* **33**, 2045 (2000).
- [27] E. Bagan, M. Baig, R. Muñoz-Taipa, and A. Rodriguez, *Phys. Rev. A* **69**, 010304 (2004).
- [28] R. Werner, *Phys. Rev. A* **58**, 1827 (1998).