Statistical Distinguishability between Unitary Operations

A. Acín*

Departament d'Estructura i Constituents de la Matèria, Universitat de Barcelona, Diagonal 647, E-08028 Barcelona, Spain

(Received 7 March 2001; published 4 October 2001)

The problem of distinguishing two unitary transformations, or quantum gates, is analyzed and a function reflecting their statistical distinguishability is found. Given two unitary operations, U_1 and U_2, it is proved that there always exists a finite number N such that $U_1^{\otimes N}$ and $U_2^{\otimes N}$ are perfectly distinguishable, although they were not in the single-copy case. This result can be extended to any finite set of unitary transformations. Finally, a fidelity for one-qubit gates, which satisfies many useful properties from the point of view of quantum information theory, is presented.

DOI: 10.1103/PhysRevLett.87.177901 PACS numbers: 03.67.–a, 03.65.Ta

Quantum nonorthogonality is one of the basic features of quantum mechanics. The deep implications of nonorthogonality can be reflected by the study of the following simple scenario: Consider the case in which one has to determine an unknown state chosen from a set of two quantum alternatives which are not orthogonal. It is well known that a complete determination is not possible unless you are provided with an infinite number of copies of the unknown state. Starting from this simple situation, some measures have been defined trying to quantify the degree of orthogonality, or distinguishability, between quantum states, either for pure [1] or mixed [2] states. A geometrical structure for the set of quantum states emerges from these measures: the closer the two states, the less distinguishable they are.

Not very much is known about how to extend some of these concepts to the case of unitary operations, although many results were found in [3]. In this Letter, after reviewing some of the existing ideas for quantum states, we look for the measurement maximizing the statistical distinguishability between two unitary transformations. From this result, as it happens for states, one can define a fidelitylike function based on statistical distinguishability which measures the *orthogonality* between unitary transformation (or quantum gates). Remarkably, and contrary to what happens in the case of quantum states, it is proved that, given two unitary matrices $U_1, U_2 \in \mathrm{SU}(d)$, it is always possible to find a finite number N such that $U_1^{\otimes N}$ and $U_2^{\otimes N}$ are perfectly distinguishable, although they were not for $N = 1$. The case of SU(2) is studied with detail due to its simplicity and importance in quantum information theory. But first, let us review some known results about distinguishability between classical probability distributions, and how they are translated into the quantum domain.

A generic probability distribution of M elements is given by a vector, $\vec{p} = (p_1, \ldots, p_M)$, with positive components satisfying $\sum_i p_i = 1$. The $M - 1$ hyperplane generated by these points is called M simplex and corresponds to the space of probability distributions of M elements. There is a privileged metric in it, the Fisher metric, which reads

$$ds^2 = \sum_i \frac{dp_i^2}{p_i}. \tag{1}$$

It induces a geodesic distance between two probability distributions, $\vec{p}$ and $\vec{q}$,

$$d(\vec{p}, \vec{q}) = \arccos\left(\sum_i \sqrt{p_i q_i}\right) \equiv \arccos\sqrt{F}, \tag{2}$$

which can be thought of as a measure of the statistical distinguishability between two probability distributions [4]. The square of the term inside the brackets is the overlap or fidelity, F, between $\vec{p}$ and $\vec{q}$. The Fisher metric is then a measure of distinguishability between two neighboring probability distributions and indeed it is the only metric in the space of probability distributions which is monotone under stochastic matrices [5] (a very natural property any measure of distinguishability should satisfy). Moreover, any generalized relative entropy of the form $H_g(\vec{p}, \vec{q}) = \sum_i p_i g(p_i/q_i)$, where g is a convex function on $(0, \infty)$ with $g(1) = 0$, and, in particular, the Kullback information entropy [6], $H_{\log}$, leads to the Fisher metric [7].

In [1,2] the classical statistical distinguishability was extended to the quantum domain, for pure and mixed states. Consider the case in which one has to distinguish an unknown given state, chosen from a set of two quantum states, ρ_1 and ρ_2, belonging to an arbitrary Hilbert space. A measurement will be performed over the system in order to obtain some information about it. The most general measurement in quantum mechanics corresponds to a resolution of the identity by means of positive operators, the so-called positive operator valued measure (POVM),

$$\sum_{i=1}^{r} M_i = 1, \tag{3}$$

with r arbitrary and $M_i \geq 0$. The POVM maps a quantum state, ρ, into a probability distribution of r elements,

$$p_i = \mathrm{tr}(M_i \rho). \tag{4}$$

The problem of distinguishing the two quantum states is now translated into discriminating between the two

probability distributions, $\vec{p}_1, \vec{p}_2$, associated to the quantum states through (4). A distance between states is then defined, using (2) by looking for the measurement apparatus that maximizes the statistical distinguishability between the resulting probability distributions,

$$d(\rho_1, \rho_2) \equiv \max_{M_i} \arccos\left(\sum_i \sqrt{\mathrm{tr}(M_i \rho_1)\mathrm{tr}(M_i \rho_2)}\right), \quad (5)$$

which is equivalent to minimize the term inside the brackets, i.e., the fidelity or overlap,

$$\sqrt{F(\rho_1, \rho_2)} \equiv \min_{M_i} \sum_i \sqrt{\mathrm{tr}(M_i \rho_1)\mathrm{tr}(M_i \rho_2)}\,. \quad (6)$$

For the case of one-dimensional projectors, $\rho = |\psi\rangle\langle\psi|$, Wootters [1] proved that (6) gives

$$F(\psi_1, \psi_2) = |\langle\psi_1|\psi_2\rangle|^2, \quad (7)$$

while for mixed states it was shown in [2,8] that the solution of (6) leads to

$$\sqrt{F(\rho_1, \rho_2)} = \mathrm{tr}\left(\sqrt{\sqrt{\rho_1}\,\rho_2\sqrt{\rho_1}}\right). \quad (8)$$

Both quantities are a measure of the statistical distinguishability between quantum states [it is easy to prove that (8) gives (7) when restricted to pure states]. It is remarkable that the fidelity obtained for pure states is equal to the usual overlap, while for the case of mixed states (8) is equal to Uhlmann's fidelity [9], although in principle there was no argument for this coincidence.

Furthermore, the corresponding distance, $d = \arccos\sqrt{F}$, induces a metric tensor in the space of states based on statistical distinguishability. For pure states, one finds the Fubini-Study metric [10], which is the only metric in the space of Hilbert space rays (pure states without the global phase) invariant under the action of unitary transformations, while for mixed states the statistical distance leads to the Bures metric [11]. A connection between quantum geometry and statistical distinguishability seems to appear (see also [12]).

Our aim is to extend these ideas to the case of one-qubit gates or SU(2) transformations, looking for a measure of the statistical distinguishability between two unitary matrices, $U_1, U_2 \in \mathrm{SU}(2)$. After introducing some notation, the strategy that maximizes the statistical distinguishability between two SU(2) transformations is presented. From this result, one obtains a measure of their distinguishability, which can be thought of as a fidelity for one-qubit gates.

A generic unitary transformation $U \in \mathrm{SU}(2)$ can be parametrized as

$$U = \cos\alpha + i \sin\alpha \hat{n}(\theta, \phi) \cdot \vec{\sigma} = e^{i\alpha \hat{n}(\theta,\phi)\cdot\vec{\sigma}}, \quad (9)$$

where θ, ϕ, and α are the standard polar angles of S^3 [13]. Its spectral decompositions will be denoted by

$$U = e^{i\alpha}|u\rangle\langle u| + e^{-i\alpha}|u^\perp\rangle\langle u^\perp|, \quad (10)$$

$|u\rangle$ and $|u^\perp\rangle$ being the eigenvectors of $\hat{n}(\theta, \phi) \cdot \vec{\sigma}$ with eigenvalues ± 1.

Given two unitary matrices, $U_1, U_2 \in \mathrm{SU}(2)$, we explore whether it is possible to obtain a fidelity function measuring their statistical distinguishability. The most general strategy is considered [3,14]: The unitary matrices are applied on one of the qubits of an entangled two-qubit state, $|\psi\rangle \in C^2 \otimes C^2$, and we want to find the measurement that maximizes the distinguishability between the states $U_i \otimes 1|\psi\rangle, i = 1, 2$. The existing results for pure states [15] can be used, and from (7) a fidelity for one-qubit gates is defined as

$$F(U_1, U_2) \equiv \min_{|\psi\rangle} |\langle\psi|\,(U_1^\dagger \otimes 1)\,(U_2 \otimes 1)\,|\psi\rangle|^2. \quad (11)$$

Since the unitary operations act on the first qubit, the expression to be minimized is, with $\rho_A \equiv \mathrm{tr}_B(|\psi\rangle\langle\psi|)$,

$$\min_{\rho_A} |\mathrm{tr}(\rho_A U)|^2 = \min_{\vec{s}} \tfrac{1}{2}|\mathrm{tr}[(1 + \vec{s} \cdot \vec{\sigma})U]|^2, \quad (12)$$

where $\vec{s}$ is the Bloch vector of ρ_A and $U \equiv U_1^\dagger U_2$ is again a unitary matrix. Using the parametrization of (9), the quantity to be minimized is equal to $\cos^2\alpha + (\hat{n} \cdot \vec{s})^2 \sin^2\alpha$. The maximal distinguishability, or minimum overlap, is obtained when $|\psi\rangle$ is a maximally entangled state, $s \equiv |\vec{s}| = 0$, or $\hat{n}$ and $\vec{s}$ are orthogonal, and the fidelity for one-qubit gates reads

$$F(U_1, U_2) = \frac{|\mathrm{tr}(U_1^\dagger U_2)|^2}{4}\,. \quad (13)$$

Note that this expression is equal to the known trace inner product in the space of square matrices and $\mathrm{tr}(U)$ is the group character.

The spectral decomposition (10) allows for an alternative derivation of the result which is going to be quite fruitful for its generalization. In fact, writing (12) in the basis where U is diagonal, we have

$$\min_{\rho_{uu}} |\rho_{uu} e^{i\alpha} + (1 - \rho_{uu}) e^{-i\alpha}|^2 = \cos^2\alpha = \frac{|\mathrm{tr}U|^2}{4}\,, \quad (14)$$

where $\rho_{uu} \equiv \langle u|\rho_A|u\rangle$. All the pure states $|\psi\rangle$ such that $\rho_{uu} = 1/2$ are optimal for distinguishing two unitary operations satisfying $U_1^\dagger U_2 = U$. In particular, it is always possible to find an optimal state, depending on U, which is not entangled, while the maximally entangled state is optimal independently of the two gates to be distinguished.

The fidelity (13) has been also proposed in [14] and the maximally entangled state of two qubits seems to be the state that best captures the information about one-qubit gates in a single run: It is indeed optimal for the problem of estimating an unknown gate [14] and, as it has been proven here, for discriminating between two possible SU(2) operations.

Consider the case in which one has to distinguish an unknown one-qubit gate chosen from a set of two alternatives, $U_1, U_2 \in \mathrm{SU}(2)$, but now N copies of the unknown gate are provided (i.e., it is possible to run the gate N times in parallel). This means that the best strategy maximizing

the distinguishability between $U_1^{\otimes N}$ and $U_2^{\otimes N}$ should be obtained. It can be proved that, contrary to what happens for quantum states, there always exists a finite number N such that $U_1^{\otimes N}$ and $U_2^{\otimes N}$ are perfectly distinguishable although this was not the case for $N = 1$.

Take as above $U = U_1^\dagger U_2$, with spectral decomposition given by (10), with $0 \le \alpha \le \pi/2$ (when $\pi/2 \le \alpha \le \pi$ the same reasoning can be applied). The eigenvalues of $U^{\otimes N}$ are $\{e^{\pm iN\alpha}, e^{\pm i(N-2)\alpha}, \ldots, e^{\pm i(N \bmod 2)\alpha}\}$, where $(N \bmod 2)$ is equal to 1 (0) for odd (even) N, with eigenvectors given by the corresponding tensor products of $|u\rangle$ and $|u^\perp\rangle$. The determination of the state $|\Psi\rangle \in C^{2^N} \otimes C^{2^N}$, of the composite system AB, minimizing $|\langle\Psi|U^{\otimes N} \otimes 1|\Psi\rangle|$ will provide us with a measure of the distinguishability between the N copies of the two SU(2) operations. Denoting by u_i^N and $|u_i^N\rangle$ the eigenvalues and eigenvectors of $U^{\otimes N}$ and by $\varrho \equiv \mathrm{tr}_B(|\Psi\rangle\langle\Psi|)$, this quantity can be shown to be equal to [see (14)]

$$|\langle\Psi|U^{\otimes N} \otimes 1|\Psi\rangle|^2 = \left| \sum_i \lambda_i u_i^N \right|^2, \tag{15}$$

where $\lambda_i \equiv \langle u_i^N|\varrho|u_i^N\rangle$ are positive numbers satisfying $\sum_i \lambda_i = 1$. This implies that the optimization of the distinguishability is equivalent to minimize the convex sum of the eigenvalues of $U^{\otimes N}$, which are complex numbers distributed over the circle $|z| = 1$ (see also [3]). It is now easy to prove that this expression gives zero, i.e., perfect distinguishability, when $N\alpha \ge \pi/2$. Indeed, take the first integer number, $N_{\min}$, satisfying this condition,

$$N_{\min} = \left[\frac{\pi}{2\alpha} \right]. \tag{16}$$

In this case the separable state $|\Psi\rangle \equiv |\Psi^s\rangle \otimes |0\rangle$, where

$$|\Psi^s\rangle = \sqrt{q}\,(|u_{+N}\rangle + |u_{-N}\rangle) + \sqrt{\tfrac{1}{2} - q}\,(|u_+\rangle + |u_-\rangle), \tag{17}$$

$u_{\pm N}$ and $u_\pm$ are the eigenvectors with eigenvalues $e^{\pm iN_{\min}\alpha}$ and $e^{\pm i(N_{\min} \bmod 2)\alpha}$, and

$$q = \frac{\cos[(N_{\min} \bmod 2)\alpha]}{2\{\cos[(N_{\min} \bmod 2)\alpha] - \cos(N_{\min}\alpha)\}} \tag{18}$$

allows for a perfect discrimination between the $N_{\min}$ copies of the two unitary matrices; i.e., the states $|\Psi_i^s\rangle \equiv U_i^{\otimes N_{\min}}|\Psi^s\rangle$ are orthogonal. Of course, a very similar procedure can be applied when $N > N_{\min}$. The minimal number of copies of the unknown gate, $N(U_1, U_2)$, needed for perfect distinguishability is then given by (16), that is, the first integer N such that the minimal arclength in the circle $|z| = 1$ including all the eigenvalues of $U^{\otimes N}$ is greater than π. Note that this is always possible with a finite number of copies, unless $U = 1$, i.e., $U_1 = U_2$.

The measure of the distinguishability induces, as in the case of quantum states, a distance in the space of one-qubit unitary operations. Given $U_1, U_2 \in \mathrm{SU}(2)$, the distance based on their statistical distinguishability is

$$d(U_1, U_2) = \arccos\left(\frac{|\mathrm{tr}(U_1^\dagger U_2)|}{2} \right), \tag{19}$$

with $0 \le d \le \pi/2$. Using this formula, the minimal number of copies for perfect distinguishability is the first integer satisfying

$$N(U_1, U_2)d(U_1, U_2) \ge \frac{\pi}{2}, \tag{20}$$

the closer the two gates are, the larger the number N is.

One may consider a U-independent strategy, where the unknown unitary is applied on N copies of the maximally entangled state (which has been proven to be optimal for the single-copy case). The fidelity is now equal to $\cos^{2N}\alpha$, and for large N it goes similar to a Gaussian with variance $1/\sqrt{2N}$. In this case, we are able to distinguish, almost with certainty, unitaries that differ by an angle $\alpha \gtrsim N^{-1/2}$, while our U-dependent strategy gives perfect discrimination up to $\alpha \gtrsim N^{-1}$ (20).

From (19), a Riemannian metric in SU(2) is found:

$$ds_U^2 = \tfrac{1}{2}\mathrm{tr}(dU dU^\dagger). \tag{21}$$

This is the Cartan-Killing metric form on the SU(2) group manifold, and it has a nice geometric interpretation. A generic SU(2) matrix can be parametrized by two complex numbers, $\beta = \beta_1 + i\beta_2$ and $\gamma = \gamma_1 + i\gamma_2$,

$$U = \begin{pmatrix} \beta & \gamma \\ -\gamma^* & \beta^* \end{pmatrix}, \tag{22}$$

with $\beta_1^2 + \beta_2^2 + \gamma_1^2 + \gamma_2^2 = 1$. Thus, any unitary operation can be thought of as a point in a three-sphere. It is easy to see that the Euclidean metric on this three-sphere is equal to (21), and the volume element given by the square root of the determinant of the metric tensor is equal to the Haar measure [13], as it was expected.

Finally, we explore the extension of these ideas to the case of arbitrary dimension; i.e., we look for a fidelity function reflecting the statistical distinguishability between two unitary transformations $U_1, U_2 \in \mathrm{SU}(d)$. As above, the most general strategy consists of taking a bipartite pure state, now $|\psi\rangle \in C^d \otimes C^d$, and applying the unknown transformation, chosen from a set of two alternatives, over one of the subsystems. The pure state minimizing the overlap $|\langle\psi|\,(U_1^\dagger U_2) \otimes 1|\psi\rangle|$ will provide us with a measure of the statistical distinguishability between the two unitary operations. Taking the spectral decomposition of $U = U_1^\dagger U_2$, $\{|u_i\rangle, u_i\}$, and $\rho_A \equiv \mathrm{tr}_B(|\psi\rangle\langle\psi|)$, the statistical distinguishability between the two SU(d) transformations is

$$\min \left| \sum_i \lambda_i u_i \right|^2, \tag{23}$$

where $\lambda_i \equiv \langle u_i|\rho_A|u_i\rangle$. The eigenvalues of U are complex numbers of modulus equal to one. Defining by 2δ the

minimal arclength in the circle $|z| = 1$ such that all the u_i are included in it, it is not difficult to see, generalizing the result of SU(2), that (23) is equal to zero when $\delta \geq \pi/2$; i.e., one is able to distinguish the two unitary transformations. When $\delta < \pi/2$, the best strategy consists of taking the two eigenvalues whose phases are maximally separated on the unit circle [3]. The found fidelity, based on statistical distinguishability, is

$$F(U_1, U_2) = \cos^2 d(U_1, U_2), \tag{24}$$

where $d(U_1, U_2) = \min(\delta, \pi/2)$. Again, the maximal distinguishability can be obtained with an unentangled state. Note that, for SU(2), since there are only two eigenvalues, this formula gives (13) and the state $|\psi\rangle$ can be chosen equal to a maximally entangled state of two qubits, independently of the two unitary matrices. In the general case, SU(d), the results are not as simple and the optimal state depends on the two unitary operations.

Let us mention that again it is always possible to find a finite number N such that $U_1^{\otimes N}$ and $U_2^{\otimes N}$ are perfectly distinguishable, although this was not the case for $N = 1$. The formula for this number is the same as (20), and it is consistent with the found measure of statistical distance.

In this work, we have studied the problem of distinguishing unitary operations starting from the simplest scenario: An unknown unitary operations is chosen from a set of two alternatives, $U_1, U_2 \in \mathrm{SU}(d)$. Previous results for quantum states have been used and a measure of the statistical distinguishability between U_1 and U_2 has been found. Contrary to what happens for quantum states, there always exists a finite number N such that N copies of the unknown gate are enough for its complete determination, although this was not possible when $N = 1$. As we have shown, the closer the two gates are, the larger the number N. Indeed, we can generalize this result to the case in which the unknown gate belongs to a finite set of k unitary transformations. By performing $k - 1$ tests as described above, each test allows to discard one of the alternatives, so a perfect discrimination is possible after a finite number of gate runs. The pair of gates that are more distant should be chosen in each test, in order to minimize the number of runs.

For the particular case of SU(2), the found measure of statistical distinguishability (13) has a nice geometrical interpretation and has been also proposed as a good measure of the similarity between gates from the point of view of estimation of an unknown unitary operation [14]. Indeed, it is also interesting to define a new measure between unitary operations reflecting, instead of their statistical distinguishability, the overlap resulting from their application; i.e., it compares their ability on average to make quantum states orthogonal. The expression for this quantity will be

$$\bar{F}(U_1, U_2) = \int d\psi \, |\langle\psi|U_1^\dagger U_2|\psi\rangle|^2, \tag{25}$$

which for the case of SU(2) leads to

$$\bar{F}(U_1, U_2) = \tfrac{1}{3} + \tfrac{2}{3} F(U_1, U_2). \tag{26}$$

In view of all these results, we propose expression (13) as a fidelity for one-qubit gates, since it captures the notion of statistical distinguishability between two SU(2) transformations in several ways and it has a nice geometrical interpretation. We hope this function will be useful in any context where a figure of merits for one-qubit gates is required.

The author thanks E. Jané, J. I. Latorre, D. Leung, L. Masanes, and G. Vidal for many useful comments. Financial support from Spanish MEC and ESF-QIT is also acknowledged.

*Email address: acin@ecm.ub.es

[1] W. K. Wootters, Phys. Rev. D **23**, 357 (1981).
[2] S. L. Braunstein and C. M. Caves, Phys. Rev. Lett. **72**, 3439 (1994).
[3] A. M. Childs, J. Preskill, and J. Renes, J. Mod. Opt. **47**, 155 (2000).
[4] For an extended review of many of these concepts, see R. E. Kass, Stat. Sci. **4**, 188 (1989).
[5] N. N. Cencov, *Statistical Decision Rules and Optimal Inferences,* Translations of Mathematical Monographs (AMS, Providence, 1982), Vol. 53; L. L. Campbell, Proc. Am. Math. Soc. **98**, 135 (1986).
[6] S. Kullback, *Information Theory and Statistics* (Wiley, New York, 1959).
[7] A. Lesniewski and M. B. Ruskai, J. Math. Phys. **40**, 5702 (1999).
[8] C. A. Fuchs, Ph.D. thesis, University of New Mexico, 1995, quant-ph/9601020.
[9] A. Uhlmann, Rep. Math. Phys. **9**, 273 (1976); see also R. Josza, J. Mod. Opt. **41**, 2315 (1994).
[10] J. Anandan, Found. Phys. **21**, 1265 (1991).
[11] D. J. C. Bures, Trans. Am. Math. Soc. **135**, 199 (1969).
[12] A. Fujiwara and H. Nagaoka, Phys. Lett. A **201**, 119 (1995); D. C. Brody and L. P. Hughston, Phys. Rev. Lett. **77**, 2851 (1996).
[13] J. F. Cornwell, *Group Theory in Physics* (Academic, London, 1984), pp. 44–91.
[14] A. Acín, E. Jané, and G. Vidal, quant-ph/0012015.
[15] It is easy to prove that no gain in the distinguishability is obtained using mixed states instead of pure states.