Distinguishing n Hamiltonians on $\mathbb{C}^n$ by a single measurement

D. Janzing* and Th. Beth
Institut für Algorithmen und Kognitive Systeme, Am Fasanengarten 3a, D-76 131 Karlsruhe, Germany
(Received 7 March 2001; published 4 January 2002)

If an experimentalist wants to decide which one of n possible Hamiltonians acting on an n-dimensional Hilbert space is present, he can conjugate the time evolution by an appropriate sequence of known unitary transformations in such a way that the different Hamiltonians result in mutual orthogonal final states. We present a general scheme providing an approximation for such a sequence.

DOI: 10.1103/PhysRevA.65.022303 PACS number(s): 03.67.−a

Controlling simple quantum systems has become a large field of research during the last decade. Experimental and theoretical investigations deal with the preparation of certain quantum states, the implementation of unitary transformations, and the design of measurement procedures for different quantum observables. Whereas the problem of distinguishing quantum *states* by optimal measurements is a large field of research (see, e.g., [1]), discussions about optimal estimation of unknown quantum *evolutions* are comparably rare. In *quantum process tomography* [2–4] either many identical copies of the same system are subjected to the considered evolution or one system is subjected to the same evolution many times with a measurement after each time period. If one is allowed to use only a restricted number N of copies, e.g., $N=1$, the unknown evolution cannot be identified perfectly and one can only try to obtain maximal information about it [5,6]. If the set of possible dynamical evolutions can be restricted by prior knowledge, there can exist schemes to decide which evolution has been applied to the system without any error probability. This has been shown for specific Hamiltonian evolutions in [7]. In [8] it was shown that n possible Hamiltonian evolutions without further restrictions can be distinguished by $n-1$ measurements since each of the measurements distinguishes between two alternatives. In this paper we assume to have only one copy of the system and we want to distinguish the Hamiltonians without coupling it to a large Hilbert space. Furthermore, only one measurement is allowed.

The problem of estimating an unknown Hamiltonian can arise in various contexts: Assume we want to use a single quantum system in order to detect classical fields, e.g., a spin particle as detector for a magnetic field. We expose the test particle to the field for a certain time period and estimate the field strength by measuring the particle's quantum state. Assume the experimentalist is allowed to perform arbitrary unitary transformations on the test particle, expose the particle to the field again, repeat this several times and perform a single measurement at the end. What is the best procedure for estimating the field? If the set of possible values for the field strength is larger than n, a single measurement of the test particle can only allow *estimations* of the field. By basic quantum mechanics, it is well known that a set of *states* is perfectly distinguishable by a single measurement if and only if their density matrices have disjoint support. Led by this simple statement concerning the distinguishability of *states*, we focus on the question of distinguishing between n possible Hamiltonians $\{H_1, \ldots, H_n\}$ of a quantum system on the Hilbert space $\mathcal{H} := \mathbb{C}^n$ and show that they are always perfectly distinguishable provided they do not only differ by an *additive* constant and it is not necessary to have more than one copy of the considered system. We assume that the experimentalist is allowed to prepare the initial state, to perform definite unitary transformations interrupting the unknown natural evolution, and to perform an arbitrary measurement at the end. The assumption about the restricted set of possibilities is more natural than it might seem at first sight. Take the following model of a measurement interaction (compare [9]): on the joint Hilbert space of the measured system and the measurement apparatus, we assume to have the Hamiltonian

$$G := \sum_j P_j \otimes H_j ,$$

where $(P_j)_j$ is the family of spectral projections of the measured observable and H_j are different self-adjoint operators moving the pointer of the measurement apparatus conditioned on the state of the measured system. Assume that we do not have any direct access to the measured system and that we are not able to change the interaction at all. The only way to use the interaction for a measurement procedure consists in initializing the measuring device, waiting (i.e., implementing e^{-iGt}), and interrupting this evolution several times by implementing local unitary transformations on the measurement apparatus in order to get mutual orthogonal pointer states for different Hamiltonians H_j. Our considerations show that this is always possible [if $H_j - \mathrm{tr}(H_j) \neq H_i - \mathrm{tr}(H_i)$ for $i \neq j$] and give a general rule for such a quantum algorithm.

The algorithm consists of quite a large number of steps; since we are working in the Lie algebra instead of the Lie group our scheme requires arbitrarily many unitary transformations (close to the identity) in order to obtain the correct result with arbitrary reliability. We are convinced that there exist much simpler algorithms for particular sets of n Hamiltonians. Whether or not there are general rules requiring only a few steps is unclear. Developing short procedures for the general case might result in computationally hard word problems in the Lie group SU_n, whereas our classical precompu-

*Electronic address: janzing@ira.uka.de

tation consists only in solving linear equations for the price of obtaining only approximative solutions.

First we present an example of n Hamiltonians that can be distinguished easily: Set $H_j := jD$ with $D := \mathrm{diag}(1,2,\ldots,n)$. By waiting for time $t=2\pi/n$, we have implemented the unitary transformations $e^{-ij2\pi D/n}$. Take the initial vector $|\psi\rangle := (1,1,\ldots,1)^T$. Then the states $e^{-ij2\pi D/n}|\psi\rangle$ are orthogonal for different values of j since they are the discrete Fourier transforms of the canonical basis vectors of $\mathbb{C}^n$. In the rest of the paper we show that the general problem can be reduced to this example. For doing so we start by developing some technical tools.

By waiting for time t, we have implemented the transformation e^{-iHt} for the unknown Hamiltonian $H \in \{H_1,\ldots,H_n\}$. We show that there is a procedure simulating e^{iHs} for arbitrary s: Choose a finite subgroup $\mathcal{G}$ of SU_n acting irreducibly on $\mathcal{H}$. Then

$$\sum_{U\in\mathcal{G}} UHU^\dagger$$

is an operator commuting with every $U\in\mathcal{G}$ and is therefore a multiple of the identity operator by Schur's Lemma (this fact is used in decoupling techniques [10,11]). Without loss of generality we assume every H_j to be traceless. Then one has $\Sigma_{U\in\mathcal{G}} UHU^\dagger = 0$ and hence $\Sigma_{U\in\mathcal{G}\setminus\{1\}} UHU^\dagger = -H$. We obtain

$$\lim_{m\to\infty} (\Pi_{U\in\mathcal{G}\setminus\{1\}} Ue^{iHt/m}U^\dagger)^m = e^{-iHt}.$$

Set $G := \{1,U_1,\ldots,U_l\}$. Then for large m we have approximately an implementation of e^{iHt} as follows:

begin

for $k=1$ to m do

for $s=1$ to l do

implement U_s

wait the time t/m

implement $U_s^\dagger$

end.

Note that for a strongly restricted set of Hamiltonians, this method for inverting an unknown evolution has already been used in usual nuclear magnetic resonance [12] spin-echo experiments. The Hamiltonian considered there is the Pauli matrix σ_z multiplied by an unknown factor λ. Conjugating the time evolution by the unitary transformation σ_x simulates the inverse evolution. In contrast to the general scheme explained above, this is a precise implementation of the inverse evolution and not just an approximation. Moreover, a spin-spin interaction, e.g., the so-called dipolar coupling

$$H := \sum_\alpha \sigma_\alpha\otimes\sigma_\alpha - 3\sigma_z\otimes\sigma_z \qquad (1)$$

with $\alpha = x,y,z$ can be inverted as follows (e.g., [15,16]). Choose unitary operators U_x and U_y such that $U_\alpha\sigma_z U_\alpha^\dagger = \sigma_\alpha$ for $\alpha = x,y$. The first term of Eq. (1) is invariant with respect to a rotation $U_\alpha\otimes U_\alpha$. Hence one obtains

$$(U_x\otimes U_x)H(U_x^\dagger\otimes U_x^\dagger) + (U_y\otimes U_y)H(U_y^\dagger\otimes U_y^\dagger) = -H.$$

More general inversion schemes have been considered recently (e.g., [13,14]).

The possibility of implementing e^{-iHt} even for negative t is decisive for using Lie algebraic tools in the sequel: Let $\mathcal{A}$ be the Lie algebra of traceless self-adjoint operators acting on $\mathcal{H}$.

By using the well-known formula

$$\lim_{m\to\infty} (e^{iH/m}e^{iA/m}e^{-iH/m}e^{-iA/m})^{m^2} = e^{-[H,A]},$$

we can design an algorithm simulating the unitary

$$e^{-[H,A]s}$$

for arbitrary $s\in\mathbb{R}, A\in\mathcal{A}$ with an arbitrary small error. In the same way we conclude the following more generally.

Lemma 1. Let $\mathcal{F},\mathcal{G}:\mathcal{A}\to\mathcal{A}$ be arbitrary (not necessarily linear) functions. Assume there exist for every $s\in\mathbb{R}$ procedures for simulating the unitary transformations

$$e^{-i\mathcal{F}(H)s}$$

and

$$e^{-i\mathcal{G}(H)s}$$

with an arbitrary small error for the unknown Hamiltonian $H\in\{H_1,\ldots,H_n\}$. Then there are procedures simulating

$$e^{[\mathcal{G}(H),\mathcal{F}(H)]s}$$

and

$$e^{[\mathcal{F}(H),A]s}$$

for every $A\in\mathcal{A}$ and every $s\in\mathbb{R}$ with an arbitrary small error.

Obviously, for every $A\in\mathcal{A}$ we can find an algorithm performing $i[H,A] =: \mathrm{ad}(H)(A)$. Hence we can find for every $k\in\mathbb{N}$ an algorithm performing $[\mathrm{ad}(H)]^k(A)$. We obtain the following result that can be found in a more general formulation in control theory [18].

Corollary. Let $\mathcal{F}:\mathcal{A}\to\mathcal{A}$ be an arbitrary function. Assume that for every required accuracy and every $s\in\mathbb{R}$ there exists a procedure such that

$$e^{-i\mathcal{F}(H)s}$$

is implemented. Then Lemma 1 provides a scheme for implementing

$$\exp\{-ip[\mathrm{ad}(\mathcal{F}(H))](A)\},$$

where p is an arbitrary real polynomial and $A\in\mathcal{A}$.

Furthermore, we will need the following observation.

Lemma 2. Let $\mathrm{Hom}(\mathcal{A},\mathcal{A})$ be the ring of $\mathbb{R}$ linear maps on the vector space $\mathcal{A}$. Let S be a group of unitaries with the property that the representation

$$\pi: S \to \mathrm{Hom}(\mathcal{A},\mathcal{A})$$

with $\pi(U)(A) := UAU^\dagger$ acts irreducibly on the complexification of $\mathcal{A}$.

Then every map in $\mathcal{L} \in \mathrm{Hom}(\mathcal{A},\mathcal{A})$ can be written as

$$\mathcal{L}(A) = \sum_j c_j U_j A U_j^\dagger$$

with positive numbers c_j.

Proof. The maps $\pi(U)$ are orthogonal maps on the real vector space $\mathcal{A}$. They act irreducibly on $\mathcal{A}$ by assumption. The smallest algebra containing them is the full matrix algebra, since every complex finite-dimensional algebra, which is closed under conjugation, is a direct sum of full matrix algebras [19]. Hence it is possible to write the real map $\mathcal{L}$ as a complex linear combination of products of maps in $\{\pi(U)\}_{U\in S}$. Since π is a group representation, one can rewrite such a sum as linear combinations of maps $\pi(U)$. Each map $\pi(U)$ is real, hence all the coefficients can be chosen to be real too. Furthermore, they can be taken positive due to the inverting scheme explained above because $\pi(S)$ can only act irreducibly on $\mathcal{A}$ if S acts irreducibly on $\mathbb{C}^n$.

The condition of Lemma 2 is satisfied, in particular, for the full special unitary group: The complex space $\mathcal{A}+i\mathcal{A}$ is the simple Lie algebra of the special linear group. Its adjoint representation ad is therefore irreducible [20]. It follows that ad is an irreducible representation of $\mathcal{A}$ on the complex space $\mathcal{A}+i\mathcal{A}$. Since $\mathcal{A}$ is the Lie algebra of the group SU_n, the latter acts irreducibly on $\mathcal{A}+i\mathcal{A}$ too. Finite subgroups satisfying the condition of Lemma 2 are studied in full detail in [17].

A straightforward implication of Lemma 2 is that if an experimentalist is able to implement all the transformations of such a group S, then he can convert any given Hamiltonian into an arbitrary one in the sense of the average Hamiltonian theory: the real Hamiltonian is H, but the system is made to evolve as if it was subjected to the Hamiltonian $\mathcal{L}(H)$. Furthermore, it follows that he can make the system evolve according to $\mathcal{L}(H)$ without knowing H for every linear map $\mathcal{L}$. Note that the sum of the positive coefficients for the maps $\pi(U)$ give the time overhead of simulating $\mathcal{L}(H)$ if H is present.

We conclude the following.

Lemma 3. Let $\mathcal{F}: \mathcal{A} \to \mathcal{A}$ be arbitrary. If there is a scheme implementing $e^{-i\mathcal{F}(H)s}$ for the unknown Hamiltonian $H \in \{H_1, \ldots, H_n\}$ then

$$e^{-i\mathcal{L}(\mathcal{F}(H))s}$$

for arbitrary $\mathcal{L} \in \mathrm{Hom}(\mathcal{A},\mathcal{A})$ can be implemented with an arbitrary small error by

$$[U_1 \exp\{-i\mathcal{F}(H)c_1 s/k\}U_1^\dagger U_2 \times \exp\{-i\mathcal{F}(H)c_2 s/k\}U_2^\dagger \ldots U_m \times \exp\{-i\mathcal{F}(H)c_m s/k\}U_m^\dagger]^k,$$

where U_j are the unitaries and c_j are the coefficients corresponding to $\mathcal{L}$ in the sense of Lemma 2 and k is large enough to keep the error small.

Now we are able to construct our algorithm: Choose an operator $G \in \mathcal{A}$ with exactly two different eigenvalues called α and β. Choose $\mathcal{L} \in \mathrm{Hom}(\mathcal{A},\mathcal{A})$ in such a way that $\mathcal{L}(H_j) = \lambda_j G$ with $\lambda_j > 0$ and $\lambda_i \neq \lambda_j$. This is possible due to basic linear algebra. The map $\mathrm{ad}(G) := i[G,.]$ has the eigenvalues $\pm i(\alpha-\beta)$ and 0. The spectrum of the map $\mathrm{ad}(\lambda_j G)$ is hence given by the values $\pm\lambda_j i(\alpha-\beta)$,0. Choose a real polynomial p such that $p(\pm\lambda_j i[\alpha-\beta]) = \pm j i[\alpha-\beta]$ and $p(0)=0$. Due to the functional calculus for the diagonalizable operator $\mathrm{ad}(G)$ this implies

$$p(\lambda_j[\mathrm{ad}(G)]) = j\,\mathrm{ad}(G).$$

By defining $C := \mathrm{ad}(G)(A)$ for arbitrary $A \in \mathcal{A}\backslash\{0\}$ we obtain

$$p(\mathrm{ad}(\lambda_j G))(A) = jC. \tag{2}$$

Now choose a map $\tilde{\mathcal{L}} \in \mathrm{Hom}(\mathcal{A},\mathcal{A})$ such that

$$\tilde{\mathcal{L}}(C) = D2\pi/n.$$

We obtain $\tilde{\mathcal{L}}(p(\mathrm{ad}(\mathcal{L}(H)))(A)) = jD2\pi/n$.

The classical precomputation for our algorithm can be sketched as follows.

(1) Choose an element $G \in \mathcal{A}$ with a two-valued spectrum and find a linear map $\mathcal{L}$ such that $\mathcal{L}(H_j) = \lambda_j G$ with different values λ_j.

(2) Find a set of unitary transformations $U_1, \ldots, U_l$ and a set of positive numbers c_j such that $\mathcal{L}(B) = \Sigma_j c_j U_j B U_j^\dagger$ for every $B \in \mathcal{A}$. This is possible due to Lemma 2.

(3) Choose a polynomial p such that $p(\pm\lambda_j i(\alpha-\beta)) = \pm j$ and $p(0)=0$, if α,β are the eigenvalues of G.

(4) Choose an arbitrary operator $A \in \mathcal{A}\backslash\{0\}$ and a map $\tilde{\mathcal{L}}$ such that $\tilde{\mathcal{L}}(p(\mathrm{ad}(G))[A]) = D2\pi/n$. Find a set of unitary operators $V_1, \ldots, V_m$ and positive numbers d_j such that $\tilde{\mathcal{L}}(B) = \Sigma_j d_j V_j B V_j^\dagger$.

Now we sketch the required sequence of quantum operations as follows.

(1) Prepare the initial state $|\psi\rangle := (1/\sqrt{n})(1, \ldots, 1)^T$.

(2) Call a subroutine performing the evolution $e^{-ijD2\pi/n}$ if the Hamiltonian H_j is present.

(3) Measure in the basis defined by the discrete Fourier transforms of the canonical basis vectors of $\mathbb{C}^n$. If the result is the jth basis state, then the Hamiltonian H_j is present.

The subroutine called in step (2) is recursively defined: The implementation of

$$e^{-ijD2\pi/n} = \exp[-i\tilde{\mathcal{L}}(p(\mathrm{ad}(L(H_j)))(A))]$$

is based on Lemma 2 by calling a subroutine simulating

$$\exp[-ip(\mathrm{ad}(\mathcal{L}(H_j)))(A)s]$$

for small s several times. The implementation of the latter is based on the corollary to Lemma 2 by calling a subroutine for implementing

$$e^{-i\mathcal{L}(H_j)s}$$

several times (Lemma 3).

We thank P. Wocjan, M. Rötteler, E. Farhi, and A. Childs for useful comments. This work has been supported by grants of the project Q-ACTA of the European Union.

[1] C. Fuchs, e-print quant-ph/9601020.
[2] M. Nielsen and I. Chuang, J. Mod. Opt. **44**, 2455 (1997).
[3] J. Poyatos, I. Cirac, and P. Zoller, Phys. Rev. Lett. **78**, 390 (1997).
[4] A. Childs, I. Chuang, and D. Leung, Phys. Rev. A **64**, 012314 (2001); e-print quant-ph/0012032.
[5] A. Acin, E. Jane, and G. Vidal, e-print quant-ph/0012015.
[6] G. D'Ariano and P. Presti, e-print quant-ph/001207.
[7] E. Farhi and S. Gutmann, Phys. Rev. A **57**, 2403 (1998); e-print quant-ph/9612026.
[8] A. Childs, J. Preskill, and J. Renes, J. Mod. Opt. **47**, 155 (2000); e-print quant-ph/9904021.
[9] A. Kitaev, e-print quant-ph/9511026.
[10] P. Zanardi, Phys. Rev. B **59**, 8170 (1999); e-print quant-ph/9809064.
[11] L. Viola, E. Knill, and S. Lloyd, Phys. Rev. Lett. **82**, 2417 (1999).
[12] S. Slichter, *Principles of Magnetic Resonance* (Springer, New York, 1978).
[13] D. Janzing, P. Wocjan, and T. Beth, e-print quant-ph/0106085.
[14] D. Leung, e-print quant-ph/0107041.
[15] R. Ernst, G. Bodenhausen, and A. Wokaun, *Principles of Nuclear Magnetic Resonance in One and Two Dimensions* (Clarendon Press, Oxford, 1987).
[16] W. Rhim, A. Pines, and J. Waugh, Phys. Rev. Lett. **25**, 218 (1970).
[17] P. Wocjan, M. Rötteler, D. Janzing, and T. Beth, e-print quant-ph/0109063.
[18] G. Heymes and H. Hermes, SIAM J. Control **8**, 450 (1970).
[19] G. Murphy, *C*-Algebras and Operator Theory* (Academic Press, San Diego, 1990).
[20] D. Želobenko, *Compact Lie Groups and their Representations* (American Mathematical Society, Providence, RI, 1973).