AIP | Journal of Mathematical Physics

On the universality of almost every quantum logic gate

Nik Weaver

Citation: Journal of Mathematical Physics **41**, 240 (2000); doi: 10.1063/1.533131
View online: http://dx.doi.org/10.1063/1.533131
View Table of Contents: http://scitation.aip.org/content/aip/journal/jmp/41/1?ver=pdfcov
Published by the AIP Publishing

Articles you may be interested in
Effect of laser pulse shaping parameters on the fidelity of quantum logic gates
J. Chem. Phys. **137**, 104306 (2012); 10.1063/1.4747703

The operations of quantum logic gates with pure and mixed initial states
J. Chem. Phys. **134**, 134103 (2011); 10.1063/1.3571597

Quantum Hall Fabry–Pérot interferometer: Logic gate responses
J. Appl. Phys. **108**, 033710 (2010); 10.1063/1.3457357

Comment on “On the universality of almost every quantum logic gate” [J. Math. Phys. 41, 240 (2000)]
J. Math. Phys. **41**, 3300 (2000); 10.1063/1.533308

Nuclear magnetic resonance quantum logic gates using quadrupolar nuclei
J. Chem. Phys. **112**, 6963 (2000); 10.1063/1.481293

This article is copyrighted as indicated in the article. Reuse of AIP content is subject to the terms at: http://scitation.aip.org/termsconditions. Downloaded to IP: 144.82.180.134 On: Tue, 18 Nov 2014 13:37:27

On the universality of almost every quantum logic gate

Nik Weaver[a]
Mathematics Department, Washington University, St. Louis, Missouri 63130

(Received 14 June 1999; accepted for publication 6 October 1999)

Lloyd [Phys. Rev. Lett. **75**, 346 (1995)] showed that almost every quantum logic gate is universal in the sense that it can be used to approximate any unitary transformation. The argument relied on a more general fact whose proof was not given in detail. We give a complete proof of this more general fact. © *2000 American Institute of Physics.* [S0022-2488(00)02201-5]

In Ref. 1 Lloyd announced the following result. Let A and B be Hermitian matrices of dimension at least 2 and let $\mathcal{L}$ be the Lie algebra they generate though commutation—that is, $\mathcal{L}$ is the real linear span of the matrices

$$A,B,i[A,B],[A,[A,B]],\ldots;$$

then for any $L\in\mathcal{L}$, the unitary matrix $U=e^{iL}$ can be expressed in the form

$$U=e^{iAt_1}e^{iBt_2}e^{iAt_3}e^{iBt_4}\cdots. \qquad (*)$$

This implies that almost every A and B are universal in the sense that any unitary matrix U can be realized by the expression (*).

Informally, one thinks of A as the intrinsic Hamiltonian of a quantum system and takes B to be a different Hamiltonian resulting from some external influence which can be applied at will. By turning B on and off for successive time intervals of various lengths, one can achieve any time evolution of the form (*), and the claim is that for almost every A and B this suffices to produce any desired unitary evolution. It follows that almost any quantum logic gate with two inputs is universal. This verifies a conjecture of Deutsch[2] and generalizes a result of Deutsch, Barenco, and Ekert.[3]

The proof was only sketched in Ref. 1, and actually the claim is not exactly true. The problem involves the use of negative values for t_j, clearly a practical impossibility, first explicitly in the expression

$$(e^{-iB\sqrt{t/n}}e^{-iA\sqrt{t/n}}e^{-iB\sqrt{t/n}}e^{iA\sqrt{t/n}})^n$$

and then implicitly in the assertion that the unitaries given by (*) form a manifold. However, this problem is irrelevant to the main issue of universality of quantum logic gates, since, as Lloyd notes later in his paper, e^{iAt} can be approximated with arbitrary accuracy by the powers of some fixed e^{iAt_A}. This is true for both positive and negative values of t, so the difficulty does not invalidate the main line of argument.

Nonetheless, this objection is genuine, as the following example shows. Let A and B be the 2×2 matrices,

$$A=\begin{pmatrix} a & 0\\ 0 & b\end{pmatrix},\quad B=\begin{pmatrix} 0 & 0\\ 0 & 0\end{pmatrix}$$

[a]Electronic mail: nweaver@math.wustl.edu

 © 2000 American Institute of Physics

This article is copyrighted as indicated in the article. Reuse of AIP content is subject to the terms at: http://scitation.aip.org/termsconditions. Downloaded to IP: 144.82.180.134 On: Tue, 18 Nov 2014 13:37:27

(a,b real). Then any expression of the form $(*)$ with non-negative t_j can be simplified to e^{iAt} for some $t \geqslant 0$. But if a/b is irrational, then $U = e^{-iA}$ cannot be expressed in such a form. For then we would have

$$e^{-iA} = e^{iAt},$$

hence

$$\begin{pmatrix} e^{-ia} & 0 \\ 0 & e^{-ib} \end{pmatrix} = \begin{pmatrix} e^{iat} & 0 \\ 0 & e^{ibt} \end{pmatrix}$$

and

$$e^{i(at+a)} = 1 = e^{i(bt+b)},$$

so that $at+a$ and $bt+b$ are both integer multiples of 2π. Since $t \neq -1$ this implies that $a/b = (at+a)/(bt+b)$ is rational.

In the previous example the operator e^{-iA} can be *approximated* by e^{iAt} for positive values of t. Indeed, in general if A is a Hermitian matrix of any finite dimension then given any $s > 0$ we may find $t > s$ such that λt is approximately an integer multiple of 2π, simultaneously for every eigenvalue λ of A. Then e^{iAt} approximates the identity matrix, so $e^{iA(t-s)}$ approximates e^{-iAs}. This is essentially the same as the observation following Eq. (3) in Ref. 1.

Thus, the reasoning in Ref. 1 does imply that for every $L \in \mathcal{L}$ the unitary matrix e^{iL} can be approximated by operators of the form $(*)$. This does not settle the question of exact representation of unitary matrices. However, the approximate result can be used to prove an exact result.

We review the argument that verifies this approximate result, which states: *Let A and B be $n \times n$ Hermitian matrices $(n \geqslant 2)$ and let $\mathcal{L}$ be the Lie algebra they generate through commutation; then for any $L \in \mathcal{L}$, the unitary matrix $U = e^{iL}$ can be approximated by finite products of the form $(*)$, with each t_j positive*. The proof proceeds on the complexity of L. If $L = A$ or $L = B$ the conclusion is immediate. For $L = i[A,B]$ we have

$$\lim_{k \to \infty} (e^{iA/\sqrt{k}} e^{iB/\sqrt{k}} e^{-iA/\sqrt{k}} e^{-iB/\sqrt{k}})^k = e^{iL}.$$

Thus e^{iL} can be approximated by finite products of the form $(*)$, if the t_j are allowed to take negative values. But as we previously noted, the negative exponents $e^{-iA/\sqrt{k}}$ and $e^{-iB/\sqrt{k}}$ can be approximated by positive exponents; so in fact e^{iL} can be approximated by finite products of the form $(*)$ with positive t_j. The conclusion can be inductively extended to more complex commutators.

Using this approximate result, we can now prove the desired theorem: *For almost all Hermitian $n \times n$ matrices A and B $(n \geqslant 2)$, every unitary $n \times n$ matrix can be exactly represented in the form $(*)$ with each $t_j \geqslant 0$.*

Observe first that it will suffice to consider only unitary matrices which are close to the identity matrix I, because any unitary matrix is a power of one close to the identity. That is, if $U = e^{iL}$ then $U = (e^{iL/k})^k$, so we need only to represent $e^{iL/k}$ in the form $(*)$ for large k.

Indeed, it will suffice to represent all unitaries close to *any* given unitary U_0. For any unitary close to I may be expressed as a power of U_0 times a unitary close to U_0. In other words, if we can represent every V within some neighborhood of U_0 then in particular we can represent U_0 itself, and hence also anything of the form $U_0^k V$. Choosing a power of U_0 which is sufficiently close to U_0^{-1}, this left multiplication by U_0^k will take the neighborhood of U_0 onto a neighborhood of I.

Let $\mathcal{L}$ be the Lie algebra generated by A and B through commutation. As noted in Ref. 1, for almost every A and B this algebra contains every Hermitian matrix. Therefore we assume this is the case.

This article is copyrighted as indicated in the article. Reuse of AIP content is subject to the terms at: http://scitation.aip.org/termsconditions. Downloaded to IP: 144.82.180.134 On: Tue, 18 Nov 2014 13:37:27

Find unitaries $V_1,\ldots,V_{n^2}$ such that $\{V_1AV_1^{-1},\ldots,V_{n^2}AV_{n^2}^{-1}\}$ span the real vector space of all $n\times n$ Hermitian matrices. This can be done provided $\mathrm{tr}(A)\neq 0$ and A is not a scalar multiple of I, and such matrices A constitute a set of full measure; to avoid interrupting the main line of argument we postpone verification of this claim to the end of the proof. We may also take $V_1=I$. Now by the approximate representation result, find unitaries $U_1,\ldots,U_{n^2-1}$ each in the form (*) with positive t_j, such that U_j approximates $e^{-iA}V_j^{-1}V_{j+1}$. Then let $U_{n^2}=e^{-iA}$ and $U_0=e^{iA}U_1e^{iA}U_2\ldots e^{iA}U_{n^2}$.

Let M be the manifold of all $n\times n$ unitary matrices and consider the map $\Phi:\mathbf{R}^{n^2}\to M$ defined by

$$\Phi(s_1,\ldots,s_{n^2})=e^{iAs_1}U_1e^{iAs_2}U_2\cdots e^{iAs_{n^2}}U_{n^2}.$$

If the s_j are all positive then $\Phi(s_1,\ldots,s_{n^2})$ is evidently representable in the form (*) with positive t_j. We will show that Φ maps neighborhoods of the point (1, 1,...,1) onto neighborhoods of U_0, and this will complete the proof.

By the implicit function theorem (see, e.g., Ref. 4), this will follow if we can show that the Jacobian of Φ at (1, 1,...,1) is nonzero. Equivalently we may consider the map Φ_0 defined by $\Phi_0(s_1,\ldots,s_{n^2})=\Phi(s_1,\ldots,s_{n^2})\cdot U_0^{-1}$.

A simple calculation shows that

$$\left.\frac{\partial\Phi}{\partial s_j}\right|_{s_1=\cdots=s_{n^2}=1}=ie^{iA}U_1\cdots e^{iA}U_{j-1}Ae^{iA}U_j\cdots e^{iA}U_{n^2}$$

and therefore

$$\left.\frac{\partial\Phi_0}{\partial s_j}\right|_{s_1=\cdots=s_{n^2}=1}=ie^{iA}U_1\cdots e^{iA}U_{j-1}AU_{j-1}^{-1}e^{-iA}\cdots U_1^{-1}e^{-iA}.$$

By the definition of the U_j's, this simplifies to

$$\left.\frac{\partial\Phi_0}{\partial s_j}\right|_{s_1=\cdots=s_{n^2}=1}\approx iV_jAV_j^{-1},$$

which shows that partial derivatives of Φ_0 at the origin span the space of skew-Hermitian matrices, by our original choice of the V_j's. Thus its Jacobian is nonzero at the the point (1, 1,...,1), as desired.

This completes the proof, modulo the claim that if $\mathrm{tr}(A)\neq 0$ and A is not a scalar multiple of I then the matrices VAV^{-1}, as V ranges over all unitaries, span the real vector space of Hermitian matrices. To verify this we use the fact that $\langle A,B\rangle=\mathrm{tr}(AB)$ defines an inner product which makes the Hermitian matrices into a real Hilbert space. Thus if the matrices VAV^{-1} do not span this space then there must be a Hermitian matrix B such that $\mathrm{tr}(VAV^{-1}B)=0$ for every unitary V. Taking V so that B and VAV^{-1} are simultaneously diagonalizable, we find that $\Sigma a_ib_i=0$ where a_i are the eigenvalues of A—in any order—and b_i are the eigenvalues of B. Since A is not a scalar multiple of I, the a_i are not all identical, and since $\mathrm{tr}(A)\neq 0$ neither are the b_i. Thus there must exist indices i_0 and i_1 such that $a_{i_0}\neq a_{i_1}$ and $b_{i_0}\neq b_{i_1}$, and this implies that $(a_{i_0}-a_{i_1})(b_{i_0}-b_{i_1})\neq 0$, hence

$$a_{i_0}b_{i_0}+a_{i_1}b_{i_1}\neq a_{i_0}b_{i_1}+a_{i_1}b_{i_0}.$$

Therefore we cannot also have $\Sigma a_ib_i=0$ for the rearrangement of the a_i which switches a_{i_0} and a_{i_1}. This contradiction shows that the matrices VAV^{-1} must span the space of Hermitian matrices.

This article is copyrighted as indicated in the article. Reuse of AIP content is subject to the terms at: http://scitation.aip.org/termsconditions. Downloaded to IP: 144.82.180.134 On: Tue, 18 Nov 2014 13:37:27

An interesting feature of this solution is that one cannot achieve or even approximate unitary matrices close to the identity in arbitrarily short times. Because of the restriction to positive t_j, in short times one can only reach unitaries which are, so to speak, ''on one side'' of the identity. A more full explanation of this phenomenon in control-theoretic terms will be given elsewhere.

ACKNOWLEDGMENTS

I wish to thank Vwani Roychowdhury for directing me to Ref. 1 and encouraging this project, and Seth Lloyd for correcting my understanding of Ref. 1.

[1] S. Lloyd, Phys. Rev. Lett. **75**, 346 (1995).
[2] D. Deutsch, Proc. R. Soc. London, Ser. A **425**, 73 (1989).
[3] D. Deutsch, A. Barenco, and A. Ekert, Proc. R. Soc. London, Ser. A **449**, 669 (1995).
[4] J. E. Marsden, *Elementary Classical Analysis* (Freeman, New York, 1974).

This article is copyrighted as indicated in the article. Reuse of AIP content is subject to the terms at: http://scitation.aip.org/termsconditions. Downloaded to IP: 144.82.180.134 On: Tue, 18 Nov 2014 13:37:27