Quantum Information and Computation, Vol. 9, No. 9&10 (2009) 0773-0777


# EXACT UNIVERSALITY FROM ANY ENTANGLING GATE WITHOUT INVERSES

ARAM W. HARROW
*Department of Mathematics, University of Bristol, Bristol, U.K.*
*a.harrow@bris.ac.uk*

Received June 14, 2008
Revised March 11, 2009

This note proves that arbitrary local gates together with any entangling bipartite gate $V$ are universal. Previously this was known only when access to both $V$ and $V^\dagger$ was given, or when approximate universality was demanded.

*Communicated by*: S Braunstein & M Mosca

A common situation in quantum computing is that we can apply only a limited set $S \subset \mathcal{U}_d$ of unitary gates to some $d$-dimensional system. The first question we want to ask in this situation is whether gates from $S$ can (approximately) generate any gate in $\mathcal{PU}_d = \mathcal{U}_d/\mathcal{Z}(\mathcal{U}_d)$ (the set of all $d \times d$ unitary matrices up to an overall phase). When this is possible, we say that $S$ is (approximately) universal. See [1,3,6,9,12] for original work on this subject, or Sect 4.5 of [11] or Chapter 8 of [10] for reviews.

Formally, $S$ is universal (for $\mathcal{PU}_d$) if, for all $W \in \mathcal{PU}_d$, there exists $U_1, \ldots, U_k \in S$ such that

$$W = U_k U_{k-1} \cdots U_2 U_1, \tag{1}$$

whereas $U$ is approximately universal (for $\mathcal{PU}_d$) if, for all $W \in \mathcal{PU}_d$ and all $\epsilon > 0$, there exists $U_1, \ldots, U_k \in S$ such that

$$d(W, U_k U_{k-1} \cdots U_2 U_1) < \epsilon. \tag{2}$$

Here $d(\cdot, \cdot)$ can be any metric, but for concreteness we will take it to be the $\mathcal{PU}_d$ analogue of operator distance:

$$d(U, V) := 1 - \inf_{|\psi\rangle \neq 0} \frac{|\langle\psi|U^\dagger V|\psi\rangle|}{\langle\psi|\psi\rangle}. \tag{3}$$

Similar definitions could also be made for $\mathcal{U}_d$, other groups, or even semigroups.

A natural way to understand universality is in terms of the group generated by $S$, which we denote $\langle S\rangle$, and define to be the smallest subgroup of $\mathcal{PU}_d$ that contains $S$. An alternate and more constructive definition is that $\langle S\rangle$ consists of all products of a finite number of elements of $S$ or their inverses. When $S$ contains its own inverses (i.e. $S = S^{-1} := \{x : x^{-1} \in S\}$) then $\langle S\rangle$ provides a concise way to understand universality: $S$ is universal iff $\langle S\rangle = \mathcal{PU}_d$ and $S$ is approximately universal iff $\langle S\rangle$ is dense in $\mathcal{PU}_d$.

But what if $S$ does not contain its own inverses? The equivalence between approximate universality and $\langle S\rangle$ being dense in $\mathcal{PU}_d$ still holds. One direction remains trivial: if $S$ is approximately universal then $\langle S\rangle$ is dense in $\mathcal{PU}_d$. The easiest way to prove the converse is with simultaneous Diophantine approximation, which implies that for any $U \in \mathcal{PU}_d$ and for any $\epsilon > 0$, there exists $n \geq 0$ such that $d(U^n, U^{-1}) \leq \epsilon$. The proof is due to Dirichlet, and for completeness we include it here. We prove the claim for $U \in \mathcal{U}_d$, and the $\mathcal{PU}_d$ result will follow from the fact that ignoring a global phase can only decrease distance. Let the eigenvalues of $U$ be $(e^{2\pi i\alpha_1}, \ldots, e^{2\pi i\alpha_d})$ for some $\alpha \in (\mathbb{R}/\mathbb{Z})^d$. Here $(\mathbb{R}/\mathbb{Z})^d$ is the $d$-dimensional torus, which can be obtained by gluing together opposite faces of the hypercube $[0,1]^d$. Under the $L_\infty$-norm, a ball of radius $\epsilon/2$ will have volume $\epsilon^d$. Thus, if $n \geq 1/\epsilon^d$ then the set $\{0, \alpha, 2\alpha, \ldots, (n-1)\alpha\}$ will have two distinct points, $n_1\alpha$ and $n_2\alpha$, with $\|n_1\alpha - n_2\alpha\|_\infty \leq \epsilon$. If $n' = |n_2 - n_1|$ then $0 < n' < n$ and $\|n'\alpha\|_\infty \leq \epsilon$. This implies that $\|U^{n'-1} - U^{-1}\|_\infty \leq |1 - e^{i\epsilon}| = 2\sin\epsilon/2 \leq \epsilon$, thus completing the proof.

For any $W \in \mathcal{PU}_d$ and $\epsilon > 0$, the fact that $\langle S\rangle$ is dense in $\mathcal{PU}_d$ means that there exists an $\frac{\epsilon}{2}$-approximation to $W$ of the form $U_1^{\pm 1} \ldots U_k^{\pm 1}$, with each $U_i \in S$. Now we replace each $U_i^{-1}$ term with $U_i^{n_i}$ for $n_i$ satisfying $\|U_i^{n_i} - U_i^{-1}\| \leq \epsilon/2k$. By the triangle inequality this yields an $\epsilon$-approximation to $W$ out of a finite sequence of unitaries from $S$.

The case of exact universality is more difficult, and is the subject of the current note. Again if $S$ is universal then $\langle S\rangle = \mathcal{PU}_d$, and again we would like to argue that the converse holds. Unfortunately this statement is not known to be true, and there may well be counter-examples along the lines of the Banach-Tarski paradox. However in the special case where $S$ contains a non-trivial one-parameter subgroup then we can prove that universality with inverses implies universality without inverses. In fact we prove something a little stronger: not only can any element of $\mathcal{PU}_d$ be written as a finite product of elements from $S$, but there is a uniform upper bound on the length of these products. If we define $S^L$ to be the set of products of $L$ elements from $S$, then we can prove

**Theorem 1:**

(a) Suppose $S \subset \mathcal{PU}_d$, $\langle S\rangle = \mathcal{PU}_d$ and there exists a Hermitian matrix $H$ such that $H$ is not proportional to the identity and $e^{iHt} \in S$ for all $t \in \mathbb{R}$. Then $S$ is exactly universal for $\mathcal{PU}_d$. In fact there exists an integer $L$ such that $S^L = \mathcal{PU}_d$.

(b) Suppose $S \subset \mathcal{U}_d$, $\langle S\rangle = \mathcal{U}_d$ and there exists a Hermitian matrix $H$ such that $H$ has nonzero trace, $H$ is not proportional to the identity and $e^{iHt} \in S$ for all $t \in \mathbb{R}$. Then $S$ is exactly universal for $\mathcal{U}_d$, and there exists $L$ such that $S^L = \mathcal{U}_d$.

The main interest of this theorem is in its application to the setting of a bipartite quantum system where local unitaries are free and nonlocal operations are restricted. Say that $d = d_A d_B$ and that $S = \mathcal{U}_{d_A} \times \mathcal{U}_{d_B} \cup \{V\}$, where $\mathcal{U}_{d_A} \times \mathcal{U}_{d_B}$ is embedded in $\mathcal{U}_{d_A d_B}$ according to $(U_A, U_B) \to U_A \otimes U_B$ and $V$ is some arbitrary unitary in $\mathcal{U}_{d_A d_B}$. In other words, we can perform $V$ as well as arbitrary local unitaries, meaning unitaries of the form $U_A \otimes U_B$. Say that $V$ is *imprimitive* if there exists $|\varphi_A\rangle \in \mathbb{C}^{d_A}, |\varphi_B\rangle \in \mathbb{C}^{d_B}$ such that $V(|\varphi_A\rangle \otimes |\varphi_B\rangle)$ is entangled. Equivalently $V$ is imprimitive if it cannot be written as $U_A \otimes U_B$ for any $U_A \in \mathcal{U}_{d_A}, U_B \in \mathcal{U}_{d_B}$, nor, if $d_A = d_B$, as SWAP $\cdot\, (U_A \otimes U_B)$. Then [1] proved that $\langle S\rangle = \mathcal{PU}_d$ if and only $V$ is imprimitive. It was claimed in [1] that in fact $S$ was exactly universal when $V$ is imprimitive, but their proof assumed that $V^\dagger \in S$. Theorem 1 then fills in the missing step in the proof of [1], and together with the fact that local unitaries contain at least one nontrivial one-parameter subgroup and the results of [1], we obtain

**Corollary 2:** If $S = \mathcal{U}_{d_A} \times \mathcal{U}_{d_B} \cup \{V\}$ and $V$ is imprimitive then $S$ is exactly universal for $\mathcal{U}_{d_A d_B}$. In fact, there exists an integer $L$ such that $S^L = \mathcal{U}_{d_A d_B}$.

This corollary is used in [8] to prove that unitary gates have the same communication capacities with or without the requirement that clean protocols be used. Exact universality there is used to show that a protocol (possibly inefficient) exists for exact communication using a fixed bipartite unitary gates supplemented by arbitrary local operations. Now we turn to the proof of Theorem 1.

**Proof:** We start with an overview of the proof (which is similar in strategy to the proof of [12]), and then discuss the details of each step. Let $G$ denote the group we are working with, which could be either $\mathcal{PU}_d$ or $\mathcal{U}_d$, and let $m = d^2 - 1$ if $G = \mathcal{PU}_d$ or $m = d^2$ if $G = \mathcal{U}_d$. Note that $G$ is an $m$-dimensional real manifold[5, 7].

(1) We will define a smooth (i.e. infinitely differentiable) map $f$ from $\mathbb{R}^m$ to $G$. It will have the property that $df_0$ (its derivative at the point 0) is non-singular.

(2) We will construct a map $\tilde{f} : \mathbb{R}^m \to G$ such that $d\tilde{f}_0$ is non-singular and there exists an integer $\ell$ such that $\tilde{f}(x) \in S^\ell$ for all $x \in \mathbb{R}^m$.

(3) We will construct an open neighborhood $N$ of the identity matrix $I \in G$ such that $N \subset S^{\ell+\ell'}$ for some integer $\ell'$.

(4) We will show that $G = N^n$ for some integer $n$, and thus that $G = S^{n(\ell+\ell')}$.

*Step 1:* For some $U_1, \ldots, U_m \in G$ to be determined later, we define

$$f(x) = U_1 e^{iHx_1} U_1^\dagger U_2 e^{iHx_2} U_2^\dagger \cdots U_m e^{iHx_m} U_m^\dagger, \tag{4}$$

where $H$ is the Hermitian matrix satisfying $\{e^{iHt} : t \in \mathbb{R}\} \subset S$. The partial derivatives at $x = 0$ are given by

$$\frac{\partial f}{\partial x_j}(0) = iU_j H U_j^\dagger. \tag{5}$$

We would like to choose $U_1, \ldots, U_m$ so that the $U_j H U_j^\dagger$ are linearly independent. Consider first the $G = \mathcal{PU}_d$ case. Then the space of Hermitian traceless matrices (which we call $\mathfrak{su}_d$) is a $d^2 - 1$-dimensional irrep of $G$, so the span of $\{UHU^\dagger : U \in G\}$ is equal to all of $\mathfrak{su}_d$. Thus, there exists a basis of $m = d^2 - 1$ matrices of the form $U_j H U_j^\dagger$.

When $G = \mathcal{U}_d$, the tangent space is instead the set of Hermitian matrices $\mathfrak{u}_d$, which decomposes into irreps as $\mathfrak{u}_d = \mathfrak{su}_d \oplus \mathbb{R}I$. Since $H$ is neither traceless nor proportional to $I$, it has nonzero overlap with both irreps. Again we would like to show that the span of $\{UHU^\dagger : U \in G\}$ (which we denote by $\mathfrak{h}$) is equal to $\mathfrak{u}_d$. First, we use the fact that $\mathcal{U}_d$ acts transitively on matrices of fixed spectrum. Averaging over all $d!$ diagonal matrices isospectral to $H$ we find that $(\operatorname{tr} H)I/d$ (which we have assumed is nonzero) is in $\mathfrak{h}$. Second, we replace

$H$ with $H - (\operatorname{tr} H)I/d$ (which is in $\mathfrak{h}$ and $\mathfrak{su}_d$) and use the result for $\mathcal{PU}_d$ to show that the span of $\mathfrak{su}_d \subset \mathfrak{h}$. Thus $\mathfrak{h}$ equals all of $\mathfrak{u}_d$. Since $\mathfrak{h}$ was spanned by matrices of the form $UHU^\dagger$, this means we can choose a set of $d^2$ linearly independent matrices $U_1HU_1^\dagger, \ldots, U_mHU_m^\dagger$ to form a basis for $\mathfrak{h} = \mathfrak{u}_d$.

In either case, $df_0$ has $m$ linearly independent columns of length $m$, and thus is non-singular. Denote the smallest singular value of $df_0$ by $\sigma_{\min}(df_0)$.

*Step 2:* Since $\langle S \rangle = G$, $S$ is approximately universal and so we can approximate $U_j$ and $U_j^\dagger$ with products of elements of $S$, which we call $\widetilde{U_j}$ and $\widetilde{U_j^\dagger}$ respectively. Demand that each approximation be accurate to within a parameter $\epsilon$ which we will choose later. We then define $\tilde{f}$ as follows:

$$\tilde{f}(x) := \widetilde{U_1} e^{iHx_1} \widetilde{U_1^\dagger} \widetilde{U_2} e^{iHx_2} \widetilde{U_2^\dagger} \cdots \widetilde{U_m} e^{iHx_m} \widetilde{U_m^\dagger}. \tag{6}$$

An explicit calculation of $df_0$ and $d\tilde{f}_0$ shows that each matrix element of $df_0^\dagger df_0 - d\tilde{f}_0^\dagger d\tilde{f}_0$ has absolute value at most $2m\epsilon \operatorname{tr} H^2$. Thus $\sigma_{\min}(d\tilde{f}_0) \geq \sigma_{\min}(df_0) - 2m^2\epsilon \operatorname{tr} H^2$ which is strictly positive if we choose $\epsilon = m^2 \operatorname{tr} H^2/4$. In this way, we can guarantee that $d\tilde{f}_0$ is non-singular.

Additionally, each $e^{iHx_j} \in S$ and each $\widetilde{U_j}$ and $\widetilde{U_j^\dagger}$ is a product of a finite number of elements from $S$, so there exists $\ell$ such that $\tilde{f}(x) \in S^\ell$ for all $x \in \mathbb{R}^m$.

*Step 3:* According to the inverse function theorem (see e.g. [7]), $\tilde{f}$ is a local diffeomorphism at 0. This means that there exists a neighborhood $X$ of 0 such that $\tilde{f}(X)$ is a neighborhood of $\tilde{f}(0)$ and $\tilde{f} : X \to \tilde{f}(X)$ is a diffeomorphism (one-to-one, onto, smooth and such that $\tilde{f}^{-1}$ is also smooth). Let $B_\delta(U) := \{V : d(U,V) < \delta\}$ denote the open ball of radius $\delta$ around $U$. Since $\tilde{f}(X)$ is a neighborhood of $\tilde{f}(0)$, there exists $\delta > 0$ such that $B_{2\delta}(\tilde{f}(0)) \subset \tilde{f}(X)$. Now we again use the approximate universality of $S$ to construct a $\delta$-approximation to $\tilde{f}(0)^{-1}$, which we call $V$. Then $V \cdot \tilde{f}(X)$ contains $B_\delta(I) =: N$. Additionally, if $V \in S^{\ell'}$ then $N \subset V \cdot \tilde{f}(X) \subset S^{\ell+\ell'}$.

*Step 4:* If $n > \pi/2\sin^{-1}(\delta/2)$ then $B_\delta(I)^n = G$. This is because $G = \{e^{iH} : \|H\|_\infty \leq \pi\}$ (optionally modulo overall phase) and $B_\delta(I) = \{e^{iH} : \|H\|_\infty \leq 2\sin^{-1}(\delta/2)\}$. Thus $G = S^{n(\ell+\ell')}$ $\square$.

We conclude with some open questions. First, it would be nice to know the exact conditions on $S$ for which $\langle S \rangle = G$ implies exact universality. One easy extension of the above Theorem (proof omitted) is to assume only that $S$ contains $\{U_1 e^{iHt} U_2 : t_1 \leq t \leq t_2\}$ for some $t_1 \leq t_2 \in \mathbb{R}$ and $U_1, U_2 \in \mathcal{U}_d$. A perhaps more important question is that of efficiency. If $S$ is approximately universal and contains its own inverses, then the Solovay-Kitaev theorem[2, 10] states that any gate can approximated to an accuracy $\epsilon$ by $S^\ell$ for $\ell = \operatorname{poly}\log(1/\epsilon)$. But if $S$ does not contain its own inverses, the best bound known on $\ell$ is the trivial $\operatorname{poly}(1/\epsilon)$ bound from Dirichlet's theorem. This is the more operationally relevant question, since in any practical application there will always be a small but nonzero approximation error. Finally, the gap between universality with and without inverses also appears in Trotter-Suzuki approximations[13] and their applications to the theory of composite pulses[14]. Here is known that access to inverses improves the efficiency of constructions[15], but the full extent of this advantage is unknown in general.

## Acknowledgments

My funding is from the U.S. Army Research Office under grant W9111NF-05-1-0294, the European Commission under Marie Curie grants ASTQIT (FP6-022194) and QAP (IST-2005-15848), and the U.K. Engineering and Physical Science Research Council through "QIP IRC."

## References

[1] J.-L. Brylinski and R. Brylinski, *Universal quantum gates*, Mathematics of Quantum Computation, 2002. arXiv:quant-ph/0108062.

[2] C. M. Dawson and M. A. Nielsen, *The Solovay-Kitaev algorithm*, Quantum Inf. Comput. **6** (2006), no. 1, 81–95. arXiv:quant-ph/0505030.

[3] D. Deutsch, A. Barenco, and A. Ekert, *Universality in Quantum Computation*, 1995. arXiv:quant-ph/9505018.

[4] J.P.G. Lejeune Dirichlet, *Werke, vol I* (L. Kronecker, ed.), Reimer, Berlin, 1889.

[5] O. Ya Viro and D. B. Fuchs, *Topology II: Homotopy and Homology : Classical Manifolds* (S. P. Novikov and V. A. Rokhlin, eds.), Springer, 2004.

[6] M. Freedman, A. Kitaev, and J. Lurie, *Diameters of Homogeneous Spaces*, 2002. arXiv:quant-ph/0209113.

[7] V. Guillemin and A. Pollack, *Differential Topology*, Prentice Hall, 1974.

[8] A.W. Harrow and P.W. Shor, *Time reversal and exchange symmetries of unitary gate capacities*, 2005. arXiv:quant-ph/0511219.

[9] S. L. Lloyd, *Almost any quantum logic gate is universal*, Phys. Rev. Lett. **75** (1995), no. 2, 346–349.

[10] A. Yu. Kitaev, A. H. Shen, and M. N. Vyalyi, *Classical and Quantum Computation*, Graduate Studies in Mathematics, vol. 47, AMS, 2002.

[11] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, New York, 2000.

[12] N. Weaver, *On the universality of almost every quantum logic gate*, J. Math. Phys. **41** (2000), no. 1, 240–243.

[13] M. Suzuki, *General theory of higher-order decomposition of exponential operators and symplectic integrators*, Phys. Lett. A **165** (1992), 387–395.

[14] K. R. Brown and A. W. Harrow and I. L. Chuang, *Arbitrarily accurate composite pulses*, Phys. Rev. A **70** (2004). arXiv:quant-ph/0407022.

[15] S. Blanes and F. Casas, *On the necessity of negative coefficients for operator splitting schemes of order higher than two*, Appl. Num. Math. **54** (2005), 23–37.