All maximally entangling unitary operators

Scott M. Cohen

Phys. Rev. A **84**, 052308 — Published 7 November 2011

DOI: 10.1103/PhysRevA.84.052308

All maximally entangling unitaries

Scott M. Cohen[1,2*]
[1] *Department of Physics, Duquesne University, Pittsburgh, Pennsylvania 15282*
[2] *Department of Physics, Carnegie-Mellon University, Pittsburgh, Pennsylvania 15213*

We characterize all maximally entangling bipartite unitary operators, acting on systems A, B of arbitrary finite dimensions $d_A \leq d_B$, when ancillary systems are available to both parties. Several useful and interesting consequences of this characterization are discussed, including an understanding of why the entangling and disentangling capacities of a given (maximally entangling) unitary can differ and a proof that these capacities must be equal when $d_A = d_B$.

PACS numbers: 03.67.Ac

I. INTRODUCTION

A key question in quantum information theory is to understand the communication capabilities of quantum channels, wherein information is encoded in a quantum system which is then sent through the channel, which will generally introduce noise into the state of the transmitted system. A noisy quantum channel can be modeled as a unitary interaction between the system and its environment, and it is common to assume that the environment starts out in a fixed pure state. One can, however, imagine a more general scenario, where the system and environment are allowed to have a completely arbitrary initial state. Then, we are considering the action of a unitary gate between two systems, and by varying their initial state, we can seek to maximize the amount of information communicated between the corresponding parties, where this communication may be in the form of classical information, quantum information, or both. In the case of quantum information, there is a close relationship to the amount of entanglement that can be produced by the given unitary interaction, and this is the question of interest to us here: What is the capacity of a bipartite unitary gate to generate entanglement [1]?

We consider a unitary $\mathcal{U}$ acting on systems A and B held by Alice and Bob, respectively, system A described by Hilbert space $\mathcal{H}_A$ and B by $\mathcal{H}_B$, these Hilbert spaces having dimensions $d_A \leq d_B$. Alice and Bob are allowed the use of ancillary systems, a held by Alice ($\mathcal{H}_a$) and b held by Bob ($\mathcal{H}_b$). It is well known that the use of ancillary systems increases the capacity of a unitary to generate entanglement [2, 3]. If the input state on $AaBb$ is $|\Psi_{in}\rangle$ and the output is then $|\Psi_{out}\rangle = I_a \otimes I_b \otimes \mathcal{U}|\Psi_{in}\rangle$, with $I_{a(b)}$ the identity operator on $a(b)$, the capacity to generate entanglement is defined as

$$\mathcal{E}(\mathcal{U}) = \sup_{|\Psi_{in}\rangle} \left(E(\Psi_{out}) - E(\Psi_{in}) \right), \tag{1}$$

where $E(\Psi)$ measures the entanglement of $|\Psi\rangle$. The maximum possible value of $\mathcal{E}(\mathcal{U})$ is $2 \log d_A$, since any $\mathcal{U}$ can be simulated by LOCC using this amount of entanglement as a resource (the state of Alice's system can then be teleported to Bob and back) and LOCC cannot increase entanglement [4]. In this paper, we will only be interested in those $\mathcal{U}$ that are maximally entangling, that is, those that can increase entanglement by $2 \log d_A$ ebits with some choice of $|\Psi_{in}\rangle$.

In general, it is not known how large the ancilla need be to maximize the generation of entanglement for a given $\mathcal{U}$, a significant barrier to understanding the entangling capacity of unitary interactions. However, in the case that $\mathcal{U}$ is maximally entangling, it has been shown that one can restrict consideration to $d_a = d_A$ and $d_b = d_B$ [5]. There it was also shown that in this case, one may use an initial state that is product,

$$|\Psi_{in}\rangle_{AaBb} = |\Phi\rangle_{Aa} \otimes |\Psi\rangle_{Bb}, \tag{2}$$

with $|\Phi\rangle_{Aa} = \sum_{k=1}^{d_A} |k\rangle_a |k\rangle_A / \sqrt{d_A}$ a maximally entangled state. In the next section, we use these results to characterize all maximally entangling unitaries for any dimensions d_A, d_B. Then, in section III, we deduce

[*] Electronic address: cohensm@duq.edu

several consequences of this characterization. Note that two separate examples appear in this section, one being the general case of two-qubit unitaries (see consequence 3) and the other being the example from [5] of a unitary which has unequal entangling and disentangling capacities (see consequence 6). Finally, in section IV, we summarize what has been accomplished.

II. CHARACTERIZATION OF MAXIMALLY ENTANGLING UNITARIES

Our goal is to establish a characterization of maximally entangling bipartite unitaries. To that end, we will find it convenient to expand $\mathcal{U}$, assumed to be unitary and maximally entangling, in terms of a finite group G, elements $f, g \in G$, group multiplication represented by fg. Thus, we have

$$\mathcal{U} = \sum_{f \in G} \Gamma(f) \otimes W(f), \tag{3}$$

where $W(f)$ act on $\mathcal{H}_B$, $\{\Gamma(f)\}$ are a set of unitary matrices acting on $\mathcal{H}_A$ and representing group G up to phases, which means that the product of two of the Γ matrices is another Γ multiplied by a phase factor: $\Gamma(f)\Gamma(g) = \mu(f,g)\Gamma(fg)$, with $|\mu(f,g)| = 1 \; \forall f,g$ [6].

We know that such an expansion is always possible, since there exist groups of order $|G| = d_A^2$ that have representations forming a complete basis of the space of $d_A \times d_A$ matrices, and then any operator acting on $\mathcal{H}_A \otimes \mathcal{H}_B$ (not just our unitary $\mathcal{U}$) can be written in the form of (3) (see [9] for further discussion and extensive application of this type of expansion); the generalized Pauli operators provide one such complete basis. However, for many unitaries, smaller groups are certainly possible, so we need to address the question of how to choose G. In [9], we used this type of expansion of bipartite unitaries to develop protocols for implementing $\mathcal{U}$ using local operations and classical communication (LOCC) with prior shared entanglement as a resource. For a given $\mathcal{U}$ and any G with which such an expansion of $\mathcal{U}$ is possible, we showed how to deterministically simulate $\mathcal{U}$ by LOCC with a resource state having entanglement equal to $\log|G|$. Since LOCC cannot increase the entanglement, we see that $\log|G|$ must be at least as large as the amount of entanglement that $\mathcal{U}$ can generate. This means that for the maximally entangling unitaries we are considering here, which have the ability to generate $2\log d_A$ ebits, we need a group of order $|G| \geq d_A^2$.

Writing the (to this point unknown) initial state on Bb as

$$|\Psi\rangle_{Bb} = \sum_{m,n=1}^{d_B} M_{mn}|n\rangle_b|m\rangle_B, \tag{4}$$

the action of $\mathcal{U}$ on the input state $|\Psi_{in}\rangle$ of (2) yields

$$\begin{aligned}
|\Psi_{out}\rangle &= \sum_{f \in G}[I_a \otimes \Gamma(f)]|\Phi\rangle_{Aa} \otimes [I_b \otimes W(f)]|\Psi\rangle_{Bb} \\
&= \frac{1}{\sqrt{d_A}}\sum_{j,k=1}^{d_A}|k\rangle_a|j\rangle_A \sum_{f \in G}[\Gamma(f)]_{jk} \sum_{m,n=1}^{d_B} M_{mn}|n\rangle_b W(f)|m\rangle_B \\
&= \frac{1}{d_A}\sum_{j,k=1}^{d_A}|k\rangle_a|j\rangle_A \otimes |b_{jk}\rangle,
\end{aligned} \tag{5}$$

where $[\Gamma(f)]_{jk}$ is the jk matrix element of $\Gamma(f)$, this basis chosen for convenience to be that which completely reduces the $\Gamma(f)$ matrices into irreducible representations (the finest block-diagonal form of these matrices). We have defined

$$|b_{jk}\rangle = \sqrt{d_A}\sum_{f \in G}[\Gamma(f)]_{jk}\sum_{m,n=1}^{d_B} M_{mn}|n\rangle_b W(f)|m\rangle_B. \tag{6}$$

Assuming that $|\Psi_{in}\rangle$ is an optimal input, achieving the maximal entanglement generation of $2\log d_A$ ebits, we see immediately from (5) that the states $|b_{jk}\rangle$ must form an orthonormal set, $\delta_{jj'}\delta_{kk'} = \langle b_{j'k'}|b_{jk}\rangle$. This implies, first of all, that for each fixed j,k, $\exists f$ such that $[\Gamma(f)]_{jk} \neq 0$. Recalling that we have chosen the j,k

basis to be that which completely decomposes matrices $\Gamma(f)$ into irreducible representations, we see that these matrices are themselves an irreducible representation for G of dimension d_A. Therefore, the choice of G is restricted to one which has an irreducible representation of this dimension. Since the sum of the squared dimensions of all irreducible representations of G is equal to $|G|$, we here have another (related) way of seeing that $|G| \geq d_A^2$. As mentioned previously, we can always choose a representation by the generalized Pauli matrices, for which $|G| = d_A^2$, and we will assume this choice has been made throughout the remainder of this paper [8].

It is shown in appendix A that as a consequence of Schur's orthogonality relations for group representations [7, 10], the orthonormality condition on states $|b_{jk}\rangle$ is equivalent to a corresponding orthonormality condition on operators $W(f)$,

$$\mathrm{Tr}\left[W(f)MM^\dagger W(g)^\dagger\right] = \frac{1}{d_A^2}\delta(f,g),\ \forall f,g \in G, \tag{7}$$

where $\delta(f,g) = 1$ when $f = g$, and otherwise is equal to zero. Thus we have our main result:

Theorem 1. *The bipartite unitary $\mathcal{U}$ is maximally entangling iff there exists a positive semi-definite 'metric' $MM^\dagger$ such that (7) is satisfied $\forall f,g \in G$, where operators $W(f)$ are obtained from an expansion of $\mathcal{U}$ as in (3), with the $\Gamma(f)$ taken to be the generalized Pauli operators. The operator M defines an optimal input state on systems bB through (4).*

In the next section, we discuss consequences of this result.

III. CONSEQUENCES OF THEOREM 1

Consequence 1. *Method to check if $\mathcal{U}$ is maximally entangling.*

Given bipartite unitary $\mathcal{U}$, theorem 1 provides a method of determining whether or not $\mathcal{U}$ is maximally entangling. One need only expand $\mathcal{U}$ in terms of the generalized Pauli operators, identify the set of operators $\{W(f)\}$, and then check to see if there exists a positive semi-definite operator to play the role of $MM^\dagger$ such that (7) is satisfied. One way to do this is to form all products, $W(g)^\dagger W(f),\ f \neq g$, reshape each into a column vector (such as by stacking individual columns of each product one on top of the other) and collect all these columns into a matrix. The nullspace of this matrix corresponds (by reshaping vectors in this nullspace back into matrices) to the space of all operators orthogonal to the $W(g)^\dagger W(f),\ f \neq g$, as is required to satisfy (7). One then needs to search, perhaps numerically, for positive operators in this nullspace. This is relatively easy to do, at least for small enough nullspaces. Note that if operators $W(f)$ are mutually orthogonal and normalized properly (according to (7)), then the nullspace will obviously contain I_B, and $\mathcal{U}$ is immediately seen to be maximally entangling. In general, however, we are not aware of an easy way to determine when a subspace (our nullspace, here) contains at least one positive operator.

Consequence 2. *Design of maximally entangling unitaries.*

Theorem 1 also allows one to design unitaries that are maximally entangling. This amounts to choosing operator M and a set of d_A^2 linearly independent operators $W(f)$ that satisfy (7). In addition, there is also the necessity that the chosen set of $W(f)$ are such that $\mathcal{U}$ is unitary. When the dimensions are not too large, it is straightforward and reasonably fast to numerically generate a maximally entangling unitary in this way (for $d_A = 4,\ d_B = 8$ it takes less than 10 minutes on my laptop). Note that since $d_A \leq d_B$ it is always possible to choose d_A^2 mutually orthogonal $W(f)$, in which case M unitary (input state on Bb maximally entangled) will satisfy (7) as long as the $W(f)$ are also chosen to be suitably normalized. Actually, when $d_A < d_B$, there exist mutually orthogonal sets of $W(f)$ that are not full rank, in which case M need not be full rank, either. Then, it would be sufficient (though certainly not necessary) that there exist a projector (identified as $MM^\dagger$) satisfying $W(f)MM^\dagger = W(f),\ \forall f$. Nonetheless, one also has to be sure that the chosen (orthogonal) $W(f)$ yield unitary $\mathcal{U}$ via (3), so we are still left with a non-trivial task in designing maximally entangling unitaries.

Consequence 3. *Characterizing maximally entangling interaction Hamiltonians for two-qubit systems.*

A characterization of two-qubit maximally entangling Hamiltonians H has been given in [11]. Using the well-known result [2] that up to local unitaries, every two-qubit unitary may be written as $\mathcal{U} = e^{-iH}$ (the usual factor $t/\hbar$ is here absorbed into the definition of H for notational convenience) with

$$H = \sum_{j=x,y,z} \alpha_j \sigma_j \otimes \sigma_j, \tag{8}$$

they showed that for $\mathcal{U}$ to be maximally entangling, it must be that $\cos^2 \alpha_x = 1/2 = \cos^2 \alpha_y$, with the value of α_z being unconstrained (permutations of $\{x, y, z\}$ are also allowed, of course). In appendix B, we provide an alternative proof of this result based on (7). This means there is a continuum of maximally entangling two-qubit unitaries ranging from the double CNOT ($\alpha_z = 0$) to the SWAP ($\cos^2 \alpha_z = 1/2$).

Consequence 4. *Operators $W(f)$ must form a linearly independent set.*

This is easily proven, as is shown at the end of appendix A. Notice also that by theorem 4 of [9] and for whatever group G and representation Γ are chosen for the expansion of maximally entangling $\mathcal{U}$, the number of linearly independent operators in the collection $\{\Gamma(f)\}$ is d_A^2, because only the single d_A-dimensional irreducible representation appears in these matrices. This is consistent with the fact that the Schmidt rank of $\mathcal{U}$ must be at least as large as the ratio of the Schmidt rank of the output state to that of the input state. That is, since our input state has Schmidt rank of one and the output state has Schmidt rank of d_A^2, $\mathcal{U}$ must have Schmidt rank of d_A^2 as well.

Consequence 5. *Input state on Bb is uniquely determined up to local unitaries when $d_A = d_B$, and must be a maximally entangled state.*

This was proven in [5]; we provide an alternative proof based on (7) in appendix A.

Consequence 6. *Why the entangling and disentangling powers can be unequal.*

It is now easy to see for a maximally entangling unitary how the entangling and disentangling powers can be unequal [5]. Recall that the disentangling power of $\mathcal{U}$ is just the entangling power of $\mathcal{U}^\dagger$. Therefore for the disentangling power, we must replace the set $\{W(f)\}$ by $\{W(f)^\dagger\}$ in (7). Then, for $\mathcal{U}$ to be maximally disentangling, we require the existence of an $M'M'^\dagger$ orthogonal to the set of operators $\{W(g)W(f)^\dagger\}$, $\forall f \neq g \in G$, whereas for maximally entangling, the orthogonality requirement applies to the generally different set, $\{W(g)^\dagger W(f)\}$, $\forall f \neq g \in G$. In addition, there is the normalization condition for $f = g$, and this again applies to a generally different set of operators in the two cases. As an example, [5] provided the original demonstration that the entangling and disentangling powers can be unequal by constructing a specific maximally entangling $\mathcal{U}$ and then showing that $\mathcal{U}^\dagger$ has strictly less than the maximum entangling power. We have calculated the $W(f)$ for their $\mathcal{U}$ and find that it is easy to satisfy (7) with these $W(f)$ (set $MM^\dagger = [|1\rangle_B\langle 1| + |3\rangle_B\langle 3|]/2$), but find (numerically) that it is not possible to do so when the set $\{W(f)\}$ is replaced by $\{W(f)^\dagger\}$ (one choice that almost works is to set $M'M'^\dagger = c_0|1\rangle_B\langle 1| + c(|2\rangle_B\langle 2| + |3\rangle_B\langle 3|)$, which satisfies orthogonality, but the normalizations cannot all be the same no matter how c_0, c are chosen).

Consequence 7. *Entangling and disentangling powers are equal for maximally entangling unitaries on $d \times d$ systems.*

It was shown in [12] that the entangling and disentangling powers of any $\mathcal{U}$ are equal when $d_A = 2 = d_B$. We can now extend this result to arbitrary dimensions $d_A = d_B$ when restricting to maximally entangling unitaries. From consequence 5, we have that $MM^\dagger$ must be proportional to I_B. Therefore, a replacement $\{W(f)\} \to \{W(f)^\dagger\}$ makes no difference whatsoever in (7), from which this claim follows immediately. That is, when $d_A = d_B$ and $\mathcal{U}$ is maximally entangling, then $\mathcal{U}^\dagger$ is also maximally entangling.

Consequence 8. *If d_B is large enough compared to d_A, it can be that no ancillary system is needed on Bob's side.*

We here provide a construction of operators $W(f)$ corresponding to $\mathcal{U}$ for which system b is not needed. This requires only that the first columns of the different $W(f)$ operators are mutually orthogonal and have norm equal to $1/d_A$ (the remaining part of each $W(f)$ is unconstrained apart from the requirement that $\mathcal{U}$ is unitary). Then we have that the matrix element $\langle 1|W(g)^\dagger W(f)|1\rangle = \delta(f, g)/d_A^2$. Choosing $MM^\dagger = |1\rangle_B\langle 1|$ shows that (7) is satisfied $\forall f, g$. This choice of $MM^\dagger$ corresponds to a product state across B/b, so system b

never plays a role and may be discarded. Recalling that there are d_A^2 different $W(f)$ operators, the mutual orthogonality of their first columns is possible only when the length d_B of those columns is at least d_A^2. Hence, this construction is only possible when $d_B \geq d_A^2$. Then there is a d_A^2-dimensional subspace of $\mathcal{H}_B$ that becomes maximally entangled with systems Aa, the remaining space not being involved in the process. Thus, it is almost as if system B has the ancillary system already embedded within itself, which is most clearly understood when $d_B = d_A^2 = d_A \times d_A$. In this case, B can be thought of as itself consisting of two d_A-dimensional systems, one of which plays the role of ancillary b.

IV. CONCLUSIONS

We have given a characterization of all maximally entangling bipartite unitaries for any dimensions $d_A \leq d_B$. This allows one to check if a given unitary is maximally entangling, to construct maximally entangling unitaries, and to determine optimal input states that achieve the maximal generation of entanglement. It also provides an understanding of why the entangling and disentangling capacities can differ, as well as a proof that this can only happen when $d_B > d_A$. We also saw that for $d_B \geq d_A^2$, it is possible that no ancillary system is needed on Bob's side. Finally, we have given an alternative method of characterizing maximally entangling Hamiltonians for two-qubit systems [11]. An interesting open question is to determine what Hamiltonians can be maximally entangling in higher-dimensional systems.

V. ACKNOWLEDGMENTS

This work has been supported in part by the National Science Foundation through Grant PHY-0757251, as well as by a grant from the Research Corporation.

Appendix A: Proof of theorem 1

Here we show that orthonormality of the states $|b_{jk}\rangle$ defined in (6) is equivalent to condition (7) on operators $W(f)$, which appear in an expansion of $\mathcal{U}$ of the form (3) with $|G| = d_A^2$. From (6), we have

$$\begin{aligned}\langle b_{j'k'}|b_{jk}\rangle &= d_A \sum_{f,g\in G} [\Gamma(g)]^*_{j'k'} [\Gamma(f)]_{jk} \sum_{m,n=1}^{d_B} \sum_{m',n'=1}^{d_B} M^*_{m'n'} M_{mn} \langle n'|n\rangle \langle m'|W(g)^\dagger W(f)|m\rangle \\ &= d_A \sum_{f,g\in G} [\Gamma(g)]^*_{j'k'} [\Gamma(f)]_{jk} \sum_{m',m=1}^{d_B} \left[MM^\dagger\right]_{mm'} \langle m'|W(g)^\dagger W(f)|m\rangle \\ &= d_A \sum_{f,g\in G} [\Gamma(g)]^*_{j'k'} [\Gamma(f)]_{jk} \operatorname{Tr}\left[MM^\dagger W(g)^\dagger W(f)\right]. \end{aligned} \tag{A1}$$

First notice that if $\operatorname{Tr}\left[W(f)MM^\dagger W(g)^\dagger\right] = \delta(f,g)/d_A^2$, the right-hand side of this equation becomes $\sum_f [\Gamma(f)]^*_{j'k'} [\Gamma(f)]_{jk}/d_A$. However, considering the d_A^2 vectors $\vec{\gamma}_{jk}$, $j,k = 1,\ldots,d_A$, whose components (labeled by $f \in G$) are given by

$$(\vec{\gamma}_{jk})_f = \frac{1}{\sqrt{d_A}} [\Gamma(f)]_{jk}\,, \tag{A2}$$

then by Schur's orthogonality relations for irreducible representations [10] and the fact that the $\Gamma(f)$ representation is irreducible, these vectors form a complete orthonormal basis for the d_A^2-dimensional space in which they lie (recall that $|G| = d_A^2$ is the dimension of these vectors). That is,

$$\sum_f [\Gamma(f)]^*_{j'k'} [\Gamma(f)]_{jk}/d_A = \delta_{jj'}\delta_{kk'}, \tag{A3}$$

which yields one of the implications we sought to prove.

To prove the converse, define $d_A^2 \times d_A^2$ matrix $\mathcal{O}$, with matrix elements labeled by $f, g \in G$ given by

$$[\mathcal{O}]_{gf} = \mathrm{Tr}\left[W(f) M M^\dagger W(g)^\dagger\right]. \tag{A4}$$

Then if $\langle b_{j'k'} | b_{jk} \rangle = \delta_{jj'}\delta_{kk'}$, (A1) can be written as

$$\frac{1}{d_A^2}\delta_{jj'}\delta_{kk'} = \vec{\gamma}^\dagger_{j'k'} \cdot \mathcal{O} \cdot \vec{\gamma}_{jk}. \tag{A5}$$

By (A5), $\mathcal{O} \cdot \vec{\gamma}_{jk}$ is orthogonal to every vector in the complete basis of the $\vec{\gamma}$-vectors except for one, that being $\vec{\gamma}_{jk}$. Therefore, $\forall j, k$, $\mathcal{O} \cdot \vec{\gamma}_{jk}$ is proportional to $\vec{\gamma}_{jk}$, and the proportionality constant is equal to $1/d_A^2$, independent of j, k, again by (A5). Thus, we have that $\mathcal{O} = I/d_A^2$, where I is the $d_A^2 \times d_A^2$ identity matrix. Finally, recalling the definition of $\mathcal{O}$ in (A4), we have

$$\frac{1}{d_A^2}\delta(f, g) = \mathrm{Tr}\left[W(f) M M^\dagger W(g)^\dagger\right], \tag{A6}$$

which completes the proof. ■

A necessary condition for (A6) to be satisfied is that the collection of $|G| = d_A^2$ operators $W(f)$ are linearly independent. This is easily seen by contradiction, so assume they are linearly dependent. Then,

$$0 = \sum_{f \in G} c(f) W(f), \tag{A7}$$

for some coefficients $c(f)$ not all equal to 0. Multiply this expression by $MM^\dagger W(g)^\dagger$ for each fixed $g \in G$ and then take the trace to obtain from (A6) that

$$0 = \sum_{f \in G} c(f)\mathrm{Tr}\left[W(f) M M^\dagger W(g)^\dagger\right] = \frac{c(g)}{d_A^2}, \tag{A8}$$

assuming (A6). This says that $c(g) = 0 \ \forall g \in G$, which contradicts the assumption of linear dependence and proves the claim.

We now give an alternate proof (see also [5]) that $\rho = MM^\dagger$ is uniquely determined when $\mathcal{U}$ is maximally entangling and $d_A = d_B$. Indeed, by contradiction, assume both ρ and ρ' serve our purpose. Then from (A6),

$$0 = \mathrm{Tr}\left[W(f)(\rho - \rho')W(g)^\dagger\right] \ \ \forall f, g \in G, \tag{A9}$$

which must hold even when $f = g$. This says that for each $f, g \in G$, $W(f)(\rho - \rho')$ is orthogonal to $W(g)$. However, as we have just seen, the $d_A^2 = d_B^2$ operators $W(g)$ are linearly independent, hence span the entire space $\mathcal{B}(\mathcal{H}_B)$ of operators acting on $\mathcal{H}_B$. Therefore, it must be that

$$W(f)(\rho - \rho') = 0 \tag{A10}$$

for every $f \in G$. Now, choose coefficients $e(f)$ such that $I_B = \sum_f e(f) W(f)$, which can always be done since $W(f)$ are a basis of $\mathcal{B}(\mathcal{H}_B)$. Multiplying (A10) by $e(f)$ and summing over f we obtain $0 = \rho - \rho'$, proving the claim.

Appendix B: Two-qubit maximally entangling Hamiltonians

Using (8) gives $\mathcal{U} = e^{-iH} = \sum_f k_f \sigma_f \otimes \sigma_f$ with $f = e, x, y, z$ labeling the group element (e is the identity element). From this we identify $W_f = k_f \sigma_f$ ($\sigma_e = I$, the two-by-two identity matrix) , where

$$\begin{aligned}
k_e &= c_x c_y c_z - i s_x s_y s_z, \\
k_x &= c_x s_y s_z - i s_x c_y c_z, \\
k_y &= s_x c_y s_z - i c_x s_y c_z, \\
k_z &= s_x s_y c_z - i c_x c_y s_z,
\end{aligned} \tag{B1}$$

and we've used the abbreviations $c_f = \cos\alpha_f$ and $s_f = \sin\alpha_f$. Applying the condition (7) with $MM^\dagger = I/2$ (because $d_A = d_B$), the orthogonality conditions ($f \neq g$) are automatically satisfied because the Pauli operators are themselves mutually orthogonal. Therefore, we only need to worry about normalizations ($f = g$ in (7)), which give

$$\begin{aligned} c_x^2c_y^2c_z^2 + s_x^2s_y^2s_z^2 &= 1/4, \\ c_x^2s_y^2s_z^2 + s_x^2c_y^2c_z^2 &= 1/4, \\ s_x^2c_y^2s_z^2 + c_x^2s_y^2c_z^2 &= 1/4, \\ s_x^2s_y^2c_z^2 + c_x^2c_y^2s_z^2 &= 1/4. \end{aligned} \tag{B2}$$

It not too difficult to show that these lead to the necessary and sufficient condition that two of the α's must have squared cosines equal to 1/2, the third α being unconstrained, which is what we set out to prove.

[1] C. H. Bennett, A. W. Harrow, D. W. Leung, and J. A. Smolin, IEEE Trans. Inf. Theory **49**, 1895 (2003).

[2] J. I. Cirac, W. Dür, B. Kraus, and M. Lewenstein, Phys. Rev. Lett. **86**, 544 (2001).

[3] B. Kraus and J. I. Cirac, Phys. Rev. A **63**, 062309 (2001).

[4] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. A **53**, 2046 (1996).

[5] N. Linden, J. A. Smolin, and A. Winter, Phys. Rev. Lett. **103**, 030501 (2009).

[6] The quantities $\mu(f,g)$ constitute what is known as a factor system [7], but this notion is not crucial to understanding our results. When $\mu(f,g) = 1\ \forall f,g$, we have an ordinary representation of the group; otherwise it is known as a projective representation.

[7] S. K. Kim, *Group Theoretical Methods and Applications to Molecules and Crystals* (Cambridge University Press, Cambridge, 1999).

[8] With this choice of representation by the generalized Pauli matrices, we have a projective irreducible representation, and for the given set of phase factors, $\mu(f,g)$, this is the *only* irreducible representation for G. It is often convenient to define the $\Gamma(f)$ such that $\mu(e,g) = \mu(g,e) = \mu(g,g^{-1}) = 1,\ \forall g \in G$. One possibility is to use $\Gamma(f) = \Gamma(m,n) = e^{i\theta_{mn}}X^mZ^n$, with $\theta_{mn} = \pi[mn \pmod{d_A}]/d_A$.

[9] L. Yu, R. B. Griffiths, and S. M. Cohen, Phys. Rev. A **81**, 062315 (2010).

[10] I. V. Schensted, *A Course on the Application of Group Theory to Quantum Mechanics* (NEO Press, Peaks Island, Maine, 1976).

[11] H. Bao-Lin and D. Yao-Min, Commun. Theor. Phys. (Beijing, China) **47**, 1029 (2007).

[12] D. W. Berry and B. C. Sanders, Phys. Rev. A **67**, 040302(R) (2003).