Research notes on universality v2.4

Andrew Childs, Debbie Leung,
Laura Mancinska, and Maris Ozols

February 17, 2009

Contents

1 Introduction

1.1 The T gate

Throughout the paper T will denote the gate that swaps two qubits:

$$T := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{1}$$

The eigenvalues of T are ± 1. The $(+1)$-eigenspace of T is spanned by[1]

$$\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}. \tag{2}$$

The (-1)-eigenspace of T is spanned by the *singlet state*

$$|s\rangle := \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix}. \tag{3}$$

Sometimes it will be more convenient to work in a basis where T is diagonal. We will use the following diagonal form:

$$\tilde{T} := \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{4}$$

Then the corresponding singlet state is

$$|\tilde{s}\rangle := \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}. \tag{5}$$

1.2 Definition of universality

Definition. The *set generated by* $U \in \mathrm{U}(4)$ consists of all finite products of U and TUT.

Definition. The *set generated by Hamiltonian* H consists of all finite products of $U(t) := e^{-iHt}$ and $TU(t)T$, where any $t \geq 0$ can be used for each $U(t)$.[2]

[1] Here we could use the Bell basis as well.

[2] We might sometimes drop the minus sign and define $U(t)$ as e^{iHt} instead.

Claim. For each $t < 0$ there exists $t' > 0$, such that $U(t) = U(t')$. Therefore we can drop the restriction $t \geq 0$ in the previous definition.

Lemma 1. The set generated by Hamiltonian H is a group.

Proof. We can generated the identity, since $U(0) = I$. We can also get the inverse of any element, since $U(t)^{-1} = U(-t)$. □

Lemma 2. The group generated by U is closed under conjugation by T.

Proof. Let $U_0 = U$ and $U_1 = TUT$. If we can generate a matrix V, then $V = \prod_{i=1}^{n} U_{x_i}$ for some $x \in \{0,1\}^n$. Then $TVT = \prod_{i=1}^{n} TU_{x_i}T = \prod_{i=1}^{n} U_{\bar{x}_i}$ corresponds to $\bar{x}$ – the bitwise negation of x. □

Hence we are interested only in the subgroups of U(4) that are closed under conjugation by T. Note that the Lie algebra of such subgroup is also closed under conjugation by T.

Definition. We say that $U \in \mathrm{U}(4)$ is *universal*, if it generates a set that is dense in U(4). In other words, U and TUT can be used to approximate any unitary $V \in \mathrm{U}(4)$ to any desired accuracy. The *universality of Hamiltonian* H, is defined similarly.

2 T-similarity

2.1 Basic properties of the T gate

Let H be a Hamiltonian.

Lemma 3. The following statements are equivalent:

(1) H commutes with T,

(2) there is an orthonormal basis, such that both H and T are diagonal,

(3) $|s\rangle$ is an eigenvector of H,

(4) H is of the form

$$\begin{pmatrix} x_1 & x_7 + ix_8 & x_7 + ix_8 & x_5 + ix_6 \\ x_7 - ix_8 & x_2 & x_4 & x_9 + ix_{10} \\ x_7 - ix_8 & x_4 & x_2 & x_9 + ix_{10} \\ x_5 - ix_6 & x_9 - ix_{10} & x_9 - ix_{10} & x_3 \end{pmatrix} \tag{6}$$

for some $x_1, \ldots, x_{10} \in \mathbb{R}$.

Lemma 4. The following statements are equivalent:

(1) U and T have a common non-trivial invariant subspace,

(2) U and T have a common eigenvector,

(3) U has an eigenvector orthogonal to $|s\rangle$.

Lemma 5. $E \subseteq \mathbb{C}^n$ is an invariant subspace of $M \in \mathbb{C}^{n\times n}$ if and only if $E = \operatorname{span}\{|v_1\rangle, \ldots, |v_k\rangle\}$, where $|v_1\rangle, \ldots, |v_k\rangle \in \mathbb{C}^n$ are eigenvectors of M and $k = \dim E$.

2.2 T-similarity and the pattern

Observe that all unitary matrices that commute with T form a group. Let us denote this group by $\mathcal{C}$:

$$\mathcal{C} := \{U \in \mathrm{U}(4) | UT = TU\}. \tag{7}$$

Definition. Matrices A and B are called *T-similar*, if there is $P \in \mathcal{C}$, such that $B = PAP^\dagger$. We will also say that two sets of matrices are *T-similar* if one set can be obtained from other by conjugating all elements with some fixed $P \in \mathcal{C}$.

Observe that T-similarity is an equivalence relation and it partitions the set U(4) into equivalence classes.

The notion of T-similarity is central to our problem, since T-similar matrices generate the same subgroup, up to a change of basis.

Claim. If U and V are T-similar, then they generate T-similar subgroups.

Definition. Assume $M \in \mathrm{U}(4)$ has non-degenerate eigenvalues λ_i with corresponding eigenvectors $|\psi_i\rangle$. We call $s_i = |\langle s|\psi_i\rangle|^2$ the *overlap* of $|\psi_i\rangle$ with $|s\rangle$. We define the *pattern* of M to be

$$\begin{Bmatrix} \lambda_1 & \lambda_2 & \lambda_3 & \lambda_4 \\ s_1 & s_2 & s_3 & s_4 \end{Bmatrix}. \tag{8}$$

We will use patterns only of the matrices that do not have degenerate eigenvalues. In such case the pattern is well defined (up to permutations of columns). Note that $s_1 + s_2 + s_3 + s_4 = 1$.

Theorem 1. Assume U and V does not have degenerate eigenvalues. Then U and V are T-similar if and only if they have the same patterns. [old version]

(T1) U and V have the same eigenvalues,

(T2) the eigenvectors of U and V corresponding to the same eigenvalue have equal absolute values of the inner product with $|s\rangle$.

Proof. It is clear that conditions (T1) and (T2) are necessary. We will show that they are also sufficient.

Assume (T1) and (T2) hold. There exists $P \in \mathrm{U}(4)$ such that $PUP^\dagger = V$, since U and V have the same eigenvalues. Let $e^{i\varphi_i}$ be the eigenvalues of U and V

and $|u_i\rangle$ and $|v_i\rangle$ be the corresponding eigenvectors. Let $r_i := |\langle s|u_i\rangle| = |\langle s|v_i\rangle|$. We can express the singlet state $|s\rangle$ in the eigenbasis of U:

$$|s\rangle = \sum_i r_i e^{i\alpha_i} |u_i\rangle . \tag{9}$$

Since $P|u_i\rangle$ is an eigenvector of V, we have $|\langle s| P |u_i\rangle| = r_i$ and

$$\langle s| P |u_i\rangle = r_i e^{i\beta_i} \tag{10}$$

for some phase β_i. Define

$$P' := P \sum_i e^{-i(\alpha_i+\beta_i)} |u_i\rangle \langle u_i| . \tag{11}$$

We claim that (a) $P'UP'^{\dagger} = V$, (b) $|\langle s| P' |s\rangle| = 1$.

(a) We have:

$$P'UP'^{\dagger} = \left(P \sum_i e^{-i(\alpha_i+\beta_i)} |u_i\rangle \langle u_i| \right) \left(\sum_j e^{i\varphi_j} |u_j\rangle \langle u_j| \right) \tag{12}$$

$$\left(\sum_k e^{i(\alpha_k+\beta_k)} |u_k\rangle \langle u_k| P^{\dagger} \right) \tag{13}$$

$$= P \left(\sum_{i,j,k} e^{-i(\alpha_i+\beta_i)+i\varphi_j+i(\alpha_k+\beta_k)} |u_i\rangle \underbrace{\langle u_i|u_j\rangle \langle u_j|u_k\rangle}_{\delta_{i,j,k}} \langle u_k| \right) P^{\dagger} \tag{14}$$

$$= P \left(\sum_i e^{i\varphi_i} |u_i\rangle \langle u_i| \right) P^{\dagger} = PUP^{\dagger} = V. \tag{15}$$

(b) We have:

$$\langle s| P' |s\rangle = \sum_i e^{i\alpha_i} r_i \langle s| P' |u_i\rangle \tag{16}$$

$$= \sum_i e^{i\alpha_i} r_i \langle s| P \sum_j e^{-i(\alpha_j+\beta_j)} |u_j\rangle \langle u_j|u_i\rangle \tag{17}$$

$$= \sum_i e^{i\alpha_i} r_i \langle s| P e^{-i(\alpha_i+\beta_i)} |u_i\rangle = \sum_i e^{-i\beta_i} r_i \langle s| P |u_i\rangle . \tag{18}$$

By applying (10) we get

$$\langle s| P' |s\rangle = \sum_i r_i^2 = 1. \tag{19}$$

Part (a) tells us that U and V are similar via P'. From (b) it follows that $|s\rangle$ is an eigenvector of P'. Thus according to Lemma 3, P' commutes with T. Hence, U and V are T-similar. □

Theorem 2. *U is T-similar to a tensor product if and only if its pattern is:*

$$\begin{Bmatrix} \lambda_{11} & \lambda_{12} & \lambda_{21} & \lambda_{22} \\ s & t & t & s \end{Bmatrix}, \text{ where } \lambda_{11}\lambda_{22} = \lambda_{12}\lambda_{21}. \tag{20}$$

Proof. Let us first prove that the above condition is necessary for U to be T-similar to a tensor product. We know that U is T-similar to some $U' = V \otimes W$. It is sufficient to prove that U' has the required pattern, since according to Theorem 1 the patterns for U and U' are the same.

First, let us diagonalize V and W:

$$V = \alpha_1 |v_1\rangle \langle v_1| + \alpha_2 |v_2\rangle \langle v_2|, \quad W = \beta_1 |w_1\rangle \langle w_1| + \beta_2 |w_2\rangle \langle w_2|. \tag{21}$$

Let the first eigenvectors of V and W be

$$|v_1\rangle = \begin{pmatrix} a \\ b \end{pmatrix}, \quad |w_1\rangle = \begin{pmatrix} c \\ d \end{pmatrix}. \tag{22}$$

Since we can disregard the global phase, we may assume that

$$|v_2\rangle = \begin{pmatrix} -b^* \\ a^* \end{pmatrix}, \quad |w_2\rangle = \begin{pmatrix} -d^* \\ c^* \end{pmatrix}. \tag{23}$$

Then

$$|v_1\rangle \otimes |w_1\rangle, \quad |v_1\rangle \otimes |w_2\rangle, \quad |v_2\rangle \otimes |w_1\rangle, \quad |v_2\rangle \otimes |w_2\rangle. \tag{24}$$

are the eigenvectors of U. If we calculate the overlaps with $|s\rangle$ we get:

$$|\langle s|v_1, w_1\rangle|^2 = \tfrac{1}{2} |ad - bc|^2 =: s, \tag{25}$$

$$|\langle s|v_1, w_2\rangle|^2 = \tfrac{1}{2} |ac^* + bd^*|^2 =: t, \tag{26}$$

$$|\langle s|v_2, w_1\rangle|^2 = \tfrac{1}{2} |-a^*c - b^*d|^2 = \tfrac{1}{2} |ac^* + bd^*|^2 = t, \tag{27}$$

$$|\langle s|v_2, w_2\rangle|^2 = \tfrac{1}{2} |a^*d^* - b^*c^*|^2 = \tfrac{1}{2} |ad - bc|^2 = s. \tag{28}$$

The eigenvalues corresponding to vectors in (24) are

$$\lambda_{11} = \alpha_1\beta_1, \quad \lambda_{12} = \alpha_1\beta_2, \quad \lambda_{21} = \alpha_2\beta_1, \quad \lambda_{22} = \alpha_2\beta_2 \tag{29}$$

and they satisfy $\lambda_{11}\lambda_{22} = \lambda_{12}\lambda_{21}$.

Now let us prove that this condition is also sufficient, i.e., for any U with the pattern of the form (20) we can find a tensor product $U' \in \mathrm{SU}(4)$ such that U and U' are T-similar. It suffices to show that we can construct a tensor product $U' \in \mathrm{SU}(4)$ with any given pattern of the form (20).

First we choose the eigenvalues as follows: $\alpha_1 = 1$, $\beta_1 = \lambda_{11}$, $\beta_2 = \lambda_{12}$, and $\alpha_2 = \lambda_{21}/\lambda_{11}$. Then we have to choose the corresponding eigenvectors so that they have the required overlaps. It suffices to make the right choice just for $|v_1\rangle$ and $|w_1\rangle$. In fact, it is always possible to choose $|v_1\rangle, |w_1\rangle \in \mathbb{R}^2$. If the angle between real unit vectors $\binom{a}{b}$ and $\binom{c}{d}$ is θ, then $ad - bc = \sin\theta$ (pseudo-scalar product) and $ac + bd = \cos\theta$ (scalar product). Thus (25) and (26) become $\frac{1}{2}\sin^2\theta = s$ and $\frac{1}{2}\cos^2\theta = t$ respectively (recall that $2s + 2t = 1$). Thus we can take any two real unit vectors having angle

$$\theta = \arcsin\sqrt{2s}. \tag{30}$$

□

Theorem 3. Let $U \in \mathrm{U}(4)$. The following are equivalent:

(1) U is T-similar to a tensor product,

(2) U has pattern given in equation (20),

(3) U is T-similar to $e^{i\varphi}O$ for some $\varphi \in \mathbb{R}$ and $O \in \mathrm{SO}(4)$.

Proof. From Theorem 2 we know that (1) and (2) are equivalent. It remains to show that (2) and (3) are equivalent. One can check that $e^{i\varphi}O$ has pattern of the form (20). This is the case, since it has paired eigenvalues and the right overlaps. Then one must show that for each pattern (20) one can construct a corresponding matrix $e^{i\varphi}O$. □ [to do...]

Theorem 4. If U is universal, then so is $e^{i\varphi}U$ for any $\varphi \in \mathbb{R}$.

Proof. Ask Debbie :) □ [to do...]

Theorem 5 (Construction 1)**.** There is a 7-parameter set of real symmetric matrices such that each Hamiltonian is T-similar to some matrix from this set.

Proof. It is sufficient to construct a 7-parameter set that contains matrices with all possible patterns. Let us work in the basis where T is diagonal – see equation (4). Then the singlet state is $|\tilde{s}\rangle = (1, 0, 0, 0)^T$ according to equation (5). Let the eigenvalues of our Hamiltonian be $\varphi_1, \varphi_2, \varphi_3, \varphi_4 \in \mathbb{R}$ and the corresponding eigenvectors be

$$\begin{pmatrix} \cos\alpha \\ \sin\alpha \\ 0 \\ 0 \end{pmatrix} \begin{pmatrix} \sin\alpha\cos\beta \\ -\cos\alpha\cos\beta \\ \sin\beta \\ 0 \end{pmatrix} \begin{pmatrix} \sin\alpha\sin\beta\cos\gamma \\ -\cos\alpha\sin\beta\cos\gamma \\ -\cos\beta\cos\gamma \\ \sin\gamma \end{pmatrix} \begin{pmatrix} \sin\alpha\sin\beta\sin\gamma \\ -\cos\alpha\sin\beta\sin\gamma \\ -\cos\beta\sin\gamma \\ -\cos\gamma \end{pmatrix} \tag{31}$$

where all angles are in $[0, \frac{\pi}{2}]$. These vectors clearly form an orthonormal basis. They have the following inner products with $|\tilde{s}\rangle$:

$$\begin{pmatrix} \cos\alpha \\ \sin\alpha\cos\beta \\ \sin\alpha\sin\beta\cos\gamma \\ \sin\alpha\sin\beta\sin\gamma \end{pmatrix}. \tag{32}$$

One can think of it as a unit vector in $\mathbb{R}^4_+$ – the non-negative orthant of $\mathbb{R}^4$. In fact, any unit vector in $\mathbb{R}^4_+$ can be obtained in this way by choosing appropriate angles. Hence by squaring all components of (32) we can obtain any probability distribution over 4 elements and thus any overlaps. Hence, by an appropriate choice of eigenvalues $\{\varphi_1, \varphi_2, \varphi_3, \varphi_4\}$ and angles $\{\alpha, \beta, \gamma\}$ we can get any pattern. □

2.3 Tridiagonal form

Theorem 6 (Construction 2)**.** Any Hamiltonian H is T-similar to a real symmetric *tridiagonal* matrix

$$\begin{pmatrix} a & b & 0 & 0 \\ b & c & d & 0 \\ 0 & d & e & f \\ 0 & 0 & f & g \end{pmatrix}, \tag{33}$$

where $a, b, c, d, e, f, g \in \mathbb{R}$ and $b, d, f \geq 0$.

Proof. Let us again work in the basis where T is diagonal (denoted by $\tilde{T}$). Then all matrices that commute with $\tilde{T}$ are block matrices of the form $\mathrm{U}(1) \oplus \mathrm{U}(3)$. We will use only the matrices that look as follows:

$$\begin{pmatrix} 1 & 0 \\ 0 & \mathrm{U}(3) \end{pmatrix}. \tag{34}$$

[This is probably called Jacobi or Householder method.]

Let the first column of H be $(h_1, h_2, h_3, h_4)^T$, where $\left\|(h_2, h_3, h_4)^T\right\| = b$. Then we can find P_1 in the form (34), such that the first column of $H_1 := P_1 H P_1^\dagger$ is $(h_1, b, 0, 0)^T$, where $b \geq 0$. Next, we consider the matrices of the form

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \mathrm{U}(2) \end{pmatrix}. \tag{35}$$

Again, let the second column of H_1 be $(h_1, h_2, h_3, h_4)^T$, where $\left\|(h_3, h_4)^T\right\| = d$. Then there is P_2 in the form (35), such that the second column of $H_2 := P_2 H_1 P_2^\dagger$ is $(h_1, h_2, d, 0)^T$, where $d \geq 0$. Note that the first column of H_2 remains the same as for H_1. Finally, we can find P_3 of the form

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \mathrm{U}(1) \end{pmatrix}, \tag{36}$$

such that the last entry f of the third column of $H_3 := P_3 H_2 P_3^\dagger$ is real and non-negative. Since H_3 is Hermitian, its diagonal entries are real. Hence it is of the form (33). □

Theorem 7. Hamiltonian in the tridiagonal form (33) has an eigenvector orthogonal to the singlet $|\tilde{s}\rangle$ if and only if $b = 0$ or $d = 0$ or $f = 0$.

Proof. If $b = 0$ or $d = 0$ or $f = 0$, then the Hamiltonian has an invariant subspace orthogonal to the singlet $|\tilde{s}\rangle$. It has dimension 3 or 2 or 1, respectively.

These conditions are also necessary. If $|v\rangle$ is an eigenvector of Hamiltonian H orthogonal to singlet $|\tilde{s}\rangle$, then $|v\rangle = (0, v_2, v_3, v_4)^T$. Let $|w\rangle := H|v\rangle$, then $|w\rangle = (0, w_2, w_3, w_4)^T$. Thus either $b = 0$ (one of our conditions) or $v_2 = 0$. If $b \neq 0$, then $v_2 = 0$ and we consider w_2. Since it must be zero, either $d = 0$ or $v_3 = 0$. If $d \neq 0$, we repeat the same argument and show that $f = 0$. □

Theorem 8. Hamiltonian in the tridiagonal form (33) corresponds to a unitary that is T-similar to a tensor product if and only if $a = c = e = g$.

Proof. Let us first show that these conditions are sufficient. If they hold, the Hamiltonian has the following eigenvalues and overlaps:

$$\lambda = a \pm_1 \sqrt{\frac{b^2 + d^2 + f^2 \pm_2 z}{2}}, \quad s = \frac{z \pm_2 (b^2 - d^2 - f^2)}{4z}. \tag{37}$$

Here subscripts indicate the correspondence between the signs and

$$z = \sqrt{b^4 + d^4 + f^4 + 2(b^2 d^2 + d^2 f^2 - b^2 f^2)}. \tag{38}$$

Eigenvalues with opposite first sign sum to $2a$ and the corresponding overlaps are equal. Therefore the unitary operation associated with this Hamiltonian will satisfy the conditions of Theorem 2 and hence is T-similar to a tensor product.

Let us show that these conditions are also necessary. It is enough to consider unitaries that are tensor products. Note that we need 4 real parameters to specify any 2×2 Hermitian matrix, since it can be written as a real linear combination of

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{39}$$

where σ_i are Pauli matrices. Note also that a 2-qubit unitary that is a tensor product has a Hamiltonian of the following form:

$$H = H_1 \otimes I + I \otimes H_2, \tag{40}$$

where H_1 and H_2 are 1-qubit Hamiltonians. We need 8 real parameters to specify a matrix of the form (40). However, we can use symmetry to reduce it to 4 real parameters.

First, observe that there is no need to specify the global phase for both qubits, since if unitary is a tensor product, the global phases of both qubits factor out. Hence we specify the global phase just for the first qubit. We can write any 1-qubit Hamiltonian in the following form:

$$\frac{\varphi}{2} I + \frac{\theta}{2}(x\sigma_x + y\sigma_y + z\sigma_z), \tag{41}$$

where σ_i are Pauli matrices, (x, y, z) is a unit vector in $\mathbb{R}^3$, and $\varphi, \theta \in \mathbb{R}$. It corresponds to a rotation about axis (x, y, z) by angle θ and global phase φ. [How is the global phase defined?]

We can change the basis of both qubits with the same local unitary, so that the second qubit is rotated around z axis. Thus we need just one parameter for the second qubit – the angle of rotation. However, there is still some freedom left – we can change the basis for both qubits by conjugating with a unitary that rotates around z axis. This does not affect the second qubit, but we can change the axis of rotation for the first qubit so that it has no y component. Thus we have reduced our Hamiltonian (40) to one with just 4 parameters:

$$H = (\alpha_1 I + x_1\sigma_x + z_1\sigma_z) \otimes I + I \otimes (z_2\sigma_z) \tag{42}$$

Recall that the (-1)-eigenspace of T is spaned by the singlet state $|s\rangle$ defined in equation (3) and the $(+1)$-eigenspace of T is spaned by three vectors defined in (2). However, since the $(+1)$-eigenspace is 3-dimensional, there are many ways how T can be diagonalized to obtain $\tilde{T}$. We can choose a different basis for the $(+1)$-eigenspace and diagonalize T by conjugating with the following matrix:

$$P := \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 \end{pmatrix}. \tag{43}$$

If we conjugate our Hamiltonian (42) with $P^\dagger$, we get:

$$H' = P^\dagger H P = \alpha_1(I \otimes I) + x_1(\sigma_y \otimes \sigma_y) + z_1(I \otimes \sigma_x) - z_2(\sigma_z \otimes \sigma_x). \tag{44}$$

In matrix form H' looks as follows:

$$H' = \begin{pmatrix} \alpha_1 & z_1 - z_2 & 0 & -x_1 \\ z_1 - z_2 & \alpha_1 & x_1 & 0 \\ 0 & x_1 & \alpha_1 & z_1 + z_2 \\ -x_1 & 0 & z_1 + z_2 & \alpha_1 \end{pmatrix}. \tag{45}$$

Observe that H' is almost tridiagonal, therefore it is sufficient to do just one more conjugation. As in the proof of Theorem 6, we can find Q that commutes with $\tilde{T}$, such that $Q^\dagger H' Q$ is tridiagonal. We choose Q as follows:

$$Q := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{z_1 - z_2}{l} & 0 & \frac{x_1}{l} \\ 0 & 0 & 1 & 0 \\ 0 & \frac{-x_1}{l} & 0 & \frac{z_1 - z_2}{l} \end{pmatrix}, \tag{46}$$

where $l = \sqrt{x_1^2 + (z_1 - z_2)^2}$. Then we have

$$H'' = Q^\dagger H' Q = \begin{pmatrix} \alpha_1 & l & 0 & 0 \\ l & \alpha_1 & \frac{-2x_1 z_2}{l} & 0 \\ 0 & \frac{-2x_1 z_2}{l} & \alpha_1 & \frac{x_1^2 + z_1^2 - z_2^2}{l} \\ 0 & 0 & \frac{x_1^2 + z_1^2 - z_2^2}{l} & \alpha_1 \end{pmatrix}. \tag{47}$$

Depending on the values of x_1, z_1, and z_2 we may have to multiply the third or the fourth row and column of H'' by -1 to get the entries above and below the main diagonal non-negative. In any case, the diagonal entries does not change. Hence any Hamiltonian of the form (40) is T-similar to one whose diagonal entries are all equal (in our case they are equal to α_1). □

3 Universality conditions

3.1 Sufficient conditions for non-universality

Theorem 9. A Hamiltonian H is not universal if any of the following holds:

(N1) $\operatorname{Tr} H = 0$ ($\dim \leq 15$),

(N2) H and T have a common eigenvector ($\dim \leq 10$),

(N3) H is T-similar to $H' = H_1 \otimes I + I \otimes H_2$ (H' acts on both qubits independently) for some 1-qubit Hamiltonians H_1 and H_2 ($\dim \leq 7$).

Proof. According to Theorem 6 it is enough to consider only Hamiltonians in the tridiagonal form (33). For such Hamiltonians these conditions read:

(N1) $a + c + e + g = 0$,

(N2) $b = 0$ or $d = 0$ or $f = 0$,

(N3) $a = c = e = g$.

If condition (N1) holds, we cannot generate the whole U(4). If we do not care about the global phase then we can ignore this condition. Conditions (N2) and (N3) for tridiagonal Hamiltonians come from Theorems 7 and 8 respectively.

It is clear that these conditions are sufficient for non-universality. □ Explain in more detail.

3.2 The "not so ugly" commutator scheme

Theorem 10. H is universal if it does not satisfy any of conditions (N1-N3).

Proof. We will show that the Lie algebra generated by H and THT is the full Lie algebra of U(4). To show this, it is enough to choose a specific basis of 16 linearly independent (over $\mathbb{R}$) Hermitian matrices and express each of these matrices in terms of linear combinations and commutators $i[\cdot,\cdot]$ of H and THT.

Let $E_{k,l}$ denote a matrix whose only non-zero entry is 1 at position (k,l). Let us define a basis of all traceless Hermitian matrices as follows:

$$X_{k,l} = E_{k,l} + E_{l,k}, \qquad (1 \leq k < l \leq 4) \tag{48}$$

$$Y_{k,l} = -iE_{k,l} + iE_{l,k}, \qquad (1 \leq k < l \leq 4) \tag{49}$$

$$Z_k = E_{k,k} - E_{k+1,k+1}. \qquad (1 \leq k \leq 3) \tag{50}$$

These 15 matrices together with any Hermitian matrix that has non-zero trace span the space of all 4×4 Hermitian matrices.

Since the Hamiltonian H does not satisfy condition (N2) we can take linear combinations with coefficients $1/b$, $1/d$, and $1/f$. Let

$$A = \frac{1}{2b} i[H, THT]. \tag{51}$$

The first three basis elements can be obtained as follows:

$$X_{1,2} = \frac{1}{2b}(H - THT), \tag{52}$$

$$Y_{1,3} = \frac{1}{3d}(i[i[X_{1,2}, A], X_{1,2}] - 4A), \tag{53}$$

$$X_{2,3} = i[X_{1,2}, Y_{1,3}]. \tag{54}$$

Next, define

$$B = \frac{1}{2}(H + THT). \tag{55}$$

To obtain $Y_{1,2}$, we have to consider three cases:

$$Y_{1,2} = \begin{cases} \dfrac{1}{a-c}(dY_{1,3} + A) & \text{if } a \neq c, \\ \dfrac{1}{c-e} i[Y_{1,3}, i[B, X_{2,3}]] & \text{if } c \neq e, \\ \dfrac{1}{a-g}\dfrac{1}{f^2} i[i[X_{2,3}, B], i[B, i[Y_{1,3}, B]]] & \text{otherwise } (a = c = e \neq g). \end{cases} \tag{56}$$

Since H does not satisfy (N3), at least one of these cases is guaranteed to hold. Next two basis elements we obtain as follows:

$$X_{1,3} = i[Y_{1,2}, X_{2,3}], \tag{57}$$

$$X_{1,4} = \frac{1}{f}((c-e)X_{1,3} + i[A, X_{2,3}] + i[Y_{1,3}, B]). \tag{58}$$

The remaining basis elements can be obtained just by taking commutators of the elements we already have:

$$X_{2,4} = i[X_{1,4}, Y_{1,2}], \tag{59}$$

$$X_{3,4} = i[X_{1,4}, Y_{1,3}], \tag{60}$$

$$Y_{1,4} = i[X_{2,4}, X_{1,2}], \tag{61}$$

$$Y_{2,3} = i[X_{1,3}, X_{1,2}], \tag{62}$$

$$Y_{2,4} = i[X_{1,4}, X_{1,2}], \tag{63}$$

$$Y_{3,4} = i[X_{1,4}, X_{1,3}]. \tag{64}$$

Finally, we add three diagonal matrices with zero trace:

$$Z_1 = \frac{1}{2} i[Y_{1,2}, X_{1,2}], \tag{65}$$

$$Z_2 = \frac{1}{2} i[Y_{2,3}, X_{2,3}], \tag{66}$$

$$Z_3 = \frac{1}{2} i[Y_{3,4}, X_{3,4}]. \tag{67}$$

At this point we can generate the Lie algebra of SU(4). If (N3) does not hold ($\operatorname{Tr} H \neq 0$), we can generate the Lie algebra of the whole U(4) by adding

$$Z_4 = H - bX_{1,2} - dX_{2,3} - fX_{3,4}. \tag{68}$$

□

4 Universality for 3 qubits

4.1 Universality conditions

Theorem 11. The following 2-qubit Hamiltonians are not universal for 3 qubits:

(N1) Hamiltonian with zero trace (dim ≤ 63),

(N2) Hamiltonian with an eigenvector of the form $|a\rangle \otimes |a\rangle$ (dim ≤ 49),

(N3) Hamiltonian that acts on both qubits independently ($H_1 \otimes I + I \otimes H_2$) (dim ≤ 10),

(N4) Hamiltonian corresponding to an orthogonal matrix (anti-symmetric matrix times i) conjugated by $U \otimes U$ for some $U \in \mathrm{U}(2)$ and multiplied by a global phase $e^{i\varphi}$ (dim ≤ 28),

(N5) Hamiltonian (conjugated by $U \otimes U$) has central symmetry (dim ≤ 31).

We conjecture that this list is not complete.

4.1.1 Central symmetry

[NEW]

Consider a 2-qubit Hamiltonian H with the following eigenvectors:

$$\begin{pmatrix} \alpha \\ \beta \\ \beta \\ \alpha \end{pmatrix}, \begin{pmatrix} \beta^* \\ -\alpha^* \\ -\alpha^* \\ \beta^* \end{pmatrix}, \begin{pmatrix} \gamma \\ \delta \\ -\delta \\ -\gamma \end{pmatrix}, \begin{pmatrix} \delta^* \\ -\gamma^* \\ \gamma^* \\ -\delta^* \end{pmatrix}, \tag{69}$$

where $\alpha, \beta, \gamma, \delta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = |\gamma|^2 + |\delta|^2 = 1/2$. Consider the basis

$$\begin{array}{cccc} |000\rangle + |111\rangle, & |100\rangle + |011\rangle, & |010\rangle + |101\rangle, & |001\rangle + |110\rangle, \\ |000\rangle - |111\rangle, & |100\rangle - |011\rangle, & |010\rangle - |101\rangle, & |001\rangle - |110\rangle. \end{array} \tag{70}$$

Claim. $H \otimes I$ has block structure $\left(\begin{smallmatrix} H_1 & 0 \\ 0 & H_2 \end{smallmatrix}\right)$ in basis (70), where H_1 and H_2 are traceless 2-qubit Hamiltonians.

Proof. Let $H = \sum_{i=1}^{4} \lambda_i \Pi_i$ be the spectral decomposition of H, where $\Pi_i = |\psi_i\rangle\langle\psi_i|$ and $|\psi_i\rangle$ are given by (69). Note that the matrix elements of Π_i have *central symmetry*, i.e.,

$$\forall s,t \in \{0,1\}^2 : \langle s|\,\Pi_i\,|t\rangle = \langle \bar{s}|\,\Pi_i\,|\bar{t}\rangle\,, \tag{71}$$

where $\bar{s}$ denotes the bitwise negation of the binary string s. For example,

$$\Pi_4 = \begin{pmatrix} |\delta|^2 & -\gamma\delta^* & \gamma\delta^* & -|\delta|^2 \\ -\gamma^*\delta & |\gamma|^2 & -|\gamma|^2 & \gamma^*\delta \\ \gamma^*\delta & -|\gamma|^2 & |\gamma|^2 & -\gamma^*\delta \\ -|\delta|^2 & \gamma\delta^* & -\gamma\delta^* & |\delta|^2 \end{pmatrix} \tag{72}$$

and $\langle 01|\,\Pi_4\,|00\rangle = \langle 10|\,\Pi_4\,|11\rangle = -\gamma^*\delta$. Since H is a linear combination of Π_i, the matrix elements of H also have central symmetry. An equivalent way of saying that H has two 4×4 blocks in basis (70) is:

$$\forall s,t \in \{0,1\}^2 : \big(\langle s| + \langle \bar{s}|\big)H\big(|t\rangle - |\bar{t}\rangle\big) = 0. \tag{73}$$

If we expand this, we get

$$\langle s|\,H\,|t\rangle - \langle \bar{s}|\,H\,|\bar{t}\rangle + \langle \bar{s}|\,H\,|t\rangle - \langle s|\,H\,|\bar{t}\rangle\,. \tag{74}$$

Since H has central symmetry, it satisfies (71), thus the above expression is clearly zero. □

Claim. If a 2-qubit Hamiltonian H has eigenvectors of the form (69), then $H \otimes I$ is not universal for 3 qubits.

Proof. It is sufficient to show that all 3-qubit permutation matrices also have two 4×4 blocks in basis (70). Let P be a 3×3 permutation matrix. Note that the corresponding 8×8 qubit permutation matrix in basis (70) has form

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & P & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & P \end{pmatrix}. \tag{75}$$

This matrix consists of two 4×4 blocks $\left(\begin{smallmatrix} 1 & 0 \\ 0 & P \end{smallmatrix}\right)$. Hence our Hamiltonian cannot be universal, since its Lie algebra has block structure in basis (70). The maximal possible dimension of this Lie algebra is 31 (including the global phase). □

Lemma 6. The following are equivalent:

(1) H has eigenvectors of the form (69),

(2) H has central symmetry,

(3) H commutes with XX,

(4) H is a real linear combination of

$$II \quad \begin{matrix} XX \\ YY \\ ZZ \end{matrix} \quad \begin{matrix} XI \\ IX \end{matrix} \quad \begin{matrix} YZ \\ ZY \end{matrix} \tag{76}$$

(5) H is of the form

$$\begin{pmatrix} a & e+if & g+ih & c \\ e-if & b & d & g-ih \\ g-ih & d & b & e-if \\ c & g+ih & e+if & a \end{pmatrix}. \tag{77}$$

Claim. The set of all 2-qubit Hamiltonians with central symmetry is not closed under conjugation by $U \otimes U$, where $U \in \mathrm{U}(2)$.

Proof. Consider $|\psi\rangle := |+\rangle |+\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$. Clearly

$$|\psi\rangle \langle\psi| = \frac{1}{4} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix} \tag{78}$$

has central symmetry. Let $|\psi'\rangle := (H \otimes H)|\psi\rangle = |00\rangle$, where $H = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$ is the Hadamard matrix. Note that

$$|\psi'\rangle \langle\psi'| = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \tag{79}$$

does not have central symmetry. □

Claim. Let H be a 2-qubit Hamiltonian. The following are equivalent:

- $(U \otimes U)H(U \otimes U)^\dagger$ has central symmetry for some $U \in \mathrm{U}(2)$,
- $[H, (UXU^\dagger) \otimes (UXU^\dagger)] = 0$ for some $U \in \mathrm{U}(2)$,
- $[H, U \otimes U] = 0$ for some $U \in \mathrm{U}(2)$, $U \neq I$ (without loss of generality we can assume that U has eigenvalues $\{1, -1\}$).

4.1.2 Block structure

[NEW]

Consider the following two blocks:

$$\begin{cases} a|000\rangle+b|111\rangle, \\ c|100\rangle+d|011\rangle, \\ c|010\rangle+d|101\rangle, \\ c|001\rangle+d|110\rangle, \end{cases} \quad \begin{cases} -b^*|000\rangle+a^*|111\rangle, \\ -d^*|100\rangle+c^*|011\rangle, \\ -d^*|010\rangle+c^*|101\rangle, \\ -d^*|001\rangle+c^*|110\rangle. \end{cases} \tag{80}$$

For any choice of $a, b, c, d \in \mathbb{C}$ such that $|a|^2 + |b|^2 = |c|^2 + |d|^2 = 1$, they form an orthonormal basis of $\mathbb{C}^8$. This basis is a generalization of (70), since all qubit permutations in this basis have block structure given in (75).

4.1.3 Conjugation by $U \otimes U$

All conditions are relatively easily checkable, except the last one, because we have the freedom to conjugate by $U \otimes U$ for some $U \in \mathrm{U}(2)$. Note that the Hamiltonian corresponding to an orthogonal matrix has only pure imaginary entries. Thus in the Pauli expansion it has only terms with exactly one Y factor. If we allow also any global phase, then we can have also the term $I \otimes I$. General such Hamiltonian is shown in Table 1.

	I	X	Y	Z
I	★		★	
X			★	
Y	★	★		★
Z			★	

Table 1: Hamiltonian corresponding to an orthogonal matrix.

Observe that there are several linear subspaces that are invariant under conjugation by $U \otimes U$:

$$\text{global phase: } \{II \qquad \text{1st qubit: } \begin{cases} XI \\ YI \\ ZI \end{cases} \qquad \text{2nd qubit: } \begin{cases} IX \\ IY \\ IZ \end{cases} \tag{81}$$

$$\text{symmetric: } \begin{cases} XX \\ YY \\ ZZ \\ XY+YX \\ YZ+ZY \\ ZX+XZ \end{cases} \qquad \text{anti-symmetric: } \begin{cases} XY-YX \\ YZ-ZY \\ ZX-XZ \end{cases} \tag{82}$$

Also note that [to do...]

	I	X	Y	Z
I				
X				
Y				
Z				

Table 2:

Dimension	Permutations	Hamiltonian
1	$\mathcal{P}_1$	$\mathcal{H}_1$
2	$\mathcal{P}_1 \oplus \mathcal{P}_1$ $\mathcal{P}_2$	$\mathcal{H}_1 \oplus \mathcal{H}_1$ $\mathcal{H}_2$
3	$\mathcal{P}_1 \oplus \mathcal{P}_1 \oplus \mathcal{P}_1$ $\mathcal{P}_1 \oplus \mathcal{P}_2$	$\mathcal{H}_1 \oplus \mathcal{H}_1 \oplus \mathcal{H}_1$ $\mathcal{H}_1 \oplus \mathcal{H}_2$
4	$\mathcal{P}_1 \oplus \mathcal{P}_1 \oplus \mathcal{P}_1 \oplus \mathcal{P}_1$ $\mathcal{P}_1 \oplus \mathcal{P}_1 \oplus \mathcal{P}_2$ $\mathcal{P}_2 \oplus \mathcal{P}_2$	$\mathcal{H}_1 \oplus \mathcal{H}_1 \oplus \mathcal{H}_1 \oplus \mathcal{H}_1$ $\mathcal{H}_1 \oplus \mathcal{H}_1 \oplus \mathcal{H}_2$ $\mathcal{H}_2 \oplus \mathcal{H}_2$

Table 3: Different types of invariant subspaces for 3-qubit permutations and Hamiltonians of the form $H \otimes I$, where H acts on 2 qubits.

4.2 Invariant subspaces for 3 qubits

[NEW]

Consider the Schur basis for 3 qubits:

$$|u_1\rangle = |100\rangle - |010\rangle\,, \tag{83}$$
$$|u_2\rangle = |100\rangle + |010\rangle - 2\,|001\rangle\,, \tag{84}$$

$$|v_1\rangle = |011\rangle - |101\rangle\,, \tag{85}$$
$$|v_2\rangle = |011\rangle + |101\rangle - 2\,|110\rangle\,, \tag{86}$$

$$|s_0\rangle = |000\rangle\,, \tag{87}$$
$$|s_1\rangle = |100\rangle + |010\rangle + |001\rangle\,, \tag{88}$$
$$|s_2\rangle = |011\rangle + |101\rangle + |110\rangle\,, \tag{89}$$
$$|s_3\rangle = |111\rangle\,. \tag{90}$$

Note that

$$\mathrm{span}_{\mathbb{C}}\left\{|u_1\rangle\,, |u_2\rangle\right\} = \mathrm{span}_{\mathbb{C}}\left\{|100\rangle - |010\rangle\,, |010\rangle - |001\rangle\,, |001\rangle - |100\rangle\right\}, \tag{91}$$
$$\mathrm{span}_{\mathbb{C}}\left\{|v_1\rangle\,, |v_2\rangle\right\} = \mathrm{span}_{\mathbb{C}}\left\{|011\rangle - |101\rangle\,, |101\rangle - |110\rangle\,, |110\rangle - |011\rangle\right\}. \tag{92}$$

So the subspaces $\mathrm{span}_{\mathbb{C}}\left\{|u_1\rangle\,, |u_2\rangle\right\}$ and $\mathrm{span}_{\mathbb{C}}\left\{|v_1\rangle\,, |v_2\rangle\right\}$ are invariant under 3-qubit permutations. In fact, note that all 3-qubit permutations in the (normalized) Schur basis are of the form $(I_2 \otimes U) \oplus I_4$ for some unitary $U \in \mathrm{U}(2)$.

In particular:

$$(12)(3) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad (123) = \frac{1}{2}\begin{pmatrix} -1 & -\sqrt{3} \\ \sqrt{3} & -1 \end{pmatrix}. \tag{93}$$

Since the transposition $(12)(3)$ and rotation (123) generate S_3, one can use (93) to compute the corresponding matrices for all permutations.

Claim. If $\forall i \in \{1,2,3,4\} : \langle s_i|\psi\rangle = 0$, then $|\psi\rangle = ac\,|u_1\rangle$ ... [to do...]

Definition. Let $\dim_{\mathcal{S}_3}|\psi\rangle := \operatorname{rank}_{\mathbb{C}}\{P\,|\psi\rangle : P \in \mathcal{S}_3\}$ be the dimension of the smallest subspace that contains the orbit of $|\psi\rangle$ under the action of 3-qubit permutations $\mathcal{S}_3$.

4.2.1 Dimension 1

Lemma 7. Let $|\psi\rangle \in \mathbb{C}^8$. The following are equivalent:

- $\dim_{\mathcal{S}_3}|\psi\rangle = 1$,
- $|\psi\rangle$ is *fixed* by all 3-qubit permutations, i.e., $\forall P \in \mathcal{S}_3 : P\,|\psi\rangle = |\psi\rangle$,
- $|\psi\rangle = (x,y,y,z,y,z,z,t)^{\mathsf{T}}$ for some $x,y,z,t \in \mathbb{C}$,
- $|\psi\rangle \in \operatorname{span}_{\mathbb{C}}\{|s_0\rangle, |s_1\rangle, |s_2\rangle, |s_3\rangle\}$,
- $|\psi\rangle \in \operatorname{span}_{\mathbb{C}}\{|000\rangle, |111\rangle, |+++\rangle, |---\rangle\}$,
- $|\psi\rangle \in \operatorname{span}_{\mathbb{C}}\left\{|\varphi\rangle\,|\varphi\rangle\,|\varphi\rangle : |\varphi\rangle \in \mathbb{C}^2\right\}$.

Lemma 8. If the eigenvalues of a 2-qubit Hamiltonian H are *not* degenerate and $|\psi\rangle \in \mathbb{C}^8$ is an eigenvector of $H \otimes I$, then $|\psi\rangle = |\psi'\rangle\,|\varphi\rangle$ for some $|\psi'\rangle \in \mathbb{C}^4$ and $|\varphi\rangle \in \mathbb{C}^2$.

Theorem 12. Let H be a 2-qubit Hamiltonian with *non*-degenerate eigenvalues and $|\psi\rangle \in \mathbb{C}^8$ be an eigenvector of $H \otimes I$. Then $\dim_{\mathcal{S}_3}|\psi\rangle = 1$ if and only if $|\psi\rangle = |\varphi\rangle\,|\varphi\rangle\,|\varphi\rangle$ for some $|\varphi\rangle \in \mathbb{C}^2$.

4.2.2 Dimension 2

Claim. Let $|\psi\rangle = |a\rangle + |s\rangle$, where $|s\rangle \in \operatorname{span}_{\mathbb{C}}\{|s_0\rangle, |s_1\rangle, |s_2\rangle, |s_3\rangle\}$ and $|a\rangle$ is orthogonal to $|s\rangle$, and both $|a\rangle$ and $|s\rangle$ are non-zero. Then $\dim_{\mathcal{S}_3}|\psi\rangle \geq 3$.

Proof. We know that $\dim_{\mathcal{S}_3}|s\rangle = 1$. Since $|a\rangle$ is orthogonal to $|s\rangle$, we have $\dim_{\mathcal{S}_3}|a\rangle \geq 2$. Thus we can choose two linearly independent non-zero vectors $|a_1\rangle, |a_2\rangle \in \operatorname{span}_{\mathbb{C}}\{P\,|a\rangle : P \in \mathcal{S}_3\}$. Moreover, we can choose them so that $\langle a_1|a_2\rangle = -\langle s|s\rangle$. Note that both $|a_1\rangle + |s\rangle$ and $|a_2\rangle + |s\rangle$ are non-zero and in $\operatorname{span}_{\mathbb{C}}\{P\,|\psi\rangle : P \in \mathcal{S}_3\}$. Moreover, since both $|a_1\rangle$ and $|a_2\rangle$ are orthogonal to $|s\rangle$, we have $\big(\langle a_1| + \langle s|\big)\big(|a_2\rangle + |s\rangle\big) = \langle a_1|a_2\rangle + \langle s|s\rangle = 0$. Thus $\dim_{\mathcal{S}_3}|\psi\rangle \geq 2$. To show that $\dim_{\mathcal{S}_3}|\psi\rangle \geq 3$, notice that

$$\big(|a_1\rangle + |s\rangle\big) - \big(|a_2\rangle + |s\rangle\big) = |a_1\rangle - |a_2\rangle \in \operatorname{span}_{\mathbb{C}}\{P\,|\psi\rangle : P \in \mathcal{S}_3\}, \tag{94}$$

since $\mathrm{span}_{\mathbb{C}}\{P|\psi\rangle : P \in \mathcal{S}_3\}$ is a linear subspace. Moreover, $|a_1\rangle - |a_2\rangle$ is non-zero and linearly independent from $|a_1\rangle + |s\rangle$ and $|a_2\rangle + |s\rangle$, since it has no component along the direction of $|s\rangle$ (recall that $|s\rangle$ is non-zero). □

4.3 Possible generalizations of T-similarity

At first we thought that the notion of T-similarity cannot be generalized for 3 qubits because of the following lemma.

Lemma 9. Let $P_i \in \mathrm{U}(8)$ be the permutation matrices that permute the three qubits they act on. Then the only $U \in \mathrm{U}(4)$ such that $[U \otimes I, P_i] = 0$ for all P_i is $U = e^{i\varphi} I$, where $\varphi \in \mathbb{R}$.

Proof. By inspection of the Hamiltonian corresponding to U. □

However, we can define it differently (take some $V \in \mathrm{U}(2)$ instead of I).

Lemma 10. Let $U \in \mathrm{U}(4)$. Then H and $UHU^\dagger$ have the same universality property if there exists $V \in \mathrm{U}(2)$ such that $[U \otimes V, P_i] = 0$ for all P_i.

Such matrices U can be characterized as follows.

Lemma 11. Let $V \in \mathrm{U}(2)$ be such that $[U \otimes V, P_i] = 0$ for all P_i. Then $U = V \otimes V \otimes V$.

Proof. By inspection of the Hamiltonian corresponding to U. □

This gives us some classes of equivalent Hamiltonians. We have to see if we can generalize the T-similarity even more. For example.

Lemma 12. Let $U \in \mathrm{U}(8)$, $[U, P_i] = 0$ for all P_i and $U(H \otimes I)U^\dagger = H' \otimes I$ for some Hamiltonian H'. Then H and H' have the same universality property.

We have to examine if $V \otimes V \otimes V$ are the only unitaries U that can be used here.

4.4 Unitary transformations that preserve universality

In this section $\mathcal{S}_n$ will denote the set of all n-qubit permutation matrices.

4.4.1 Centralizer of $\mathcal{S}_n$

Lemma 13. If U is a unitary such that $\forall P \in \mathcal{S}_n : UP = PU$, then the Hamiltonians H and $UHU^\dagger$ are either both universal or non-universal. The set of all unitaries having this property is called the *centralizer* of $\mathcal{S}_n$ and is denoted by $Z(\mathcal{S}_n)$.

In 3-qubit case $Z(\mathcal{S}_n)$ is a 20-parameter subgroup of U(8) isomorphic to $\mathrm{U}(4) \oplus (I \otimes \mathrm{U}(2))$. One way to show this is to consider the Hamiltonians corresponding to unitaries in the centralizer. The corresponding condition for Hamiltonians reads: $\forall P \in \mathcal{S}_n : H = PHP^\dagger$ (it is enough to check this only for the generators of $\mathcal{S}_n$). If we consider a basis of 64 linearly independent (over $\mathbb{R}$) Hermitian matrices (that span all 3-qubit Hamiltonians), this condition is just a system of two linear equations. The solution of this system corresponds to a subspace of all Hermitian matrices. One can find a basis of this subspace such that all Hamiltonians in this subspace are in a block-diagonal form $H_4 \oplus H_2 \oplus H_2$ corresponding to $\mathrm{U}(4) \oplus (I \otimes \mathrm{U}(2))$.

Another way to show this is to consider the invariant subspaces of qubit permutation matrices [1]. Each of the following vectors[3] is invariant under all permutations of qubits:

$$|s_1\rangle = |000\rangle\,, \tag{95}$$
$$|s_2\rangle = |100\rangle + |010\rangle + |001\rangle\,, \tag{96}$$
$$|s_3\rangle = |011\rangle + |101\rangle + |110\rangle\,, \tag{97}$$
$$|s_4\rangle = |111\rangle\,. \tag{98}$$

Qubit permutations act trivially on the subspace $\mathcal{S} = \mathrm{span}\,\{|s_1\rangle\,, \ldots, |s_4\rangle\}$. Notice that this is the largest such subspace, i.e., if all qubit permutations act trivially on some $|\psi\rangle$ then $|\psi\rangle \in \mathcal{S}$ (to see this, express $|\psi\rangle$ in standard basis and consider the terms with equal Hamming weights; by exchanging adjacent qubits it can be shown that terms with the same Hamming weight must have equal coefficients). Hence if we want $U \in \mathrm{U}(8)$ to commute with all permutation matrices, it can act arbitrarily in the subspace $\mathcal{S}$ but must leave it invariant.

Now let us restrict our attention to the orthogonal complement $\mathcal{T} = \mathcal{S}^\perp$. Consider a 2-dimensional subspace of $\mathcal{T}$ spanned by the following vectors:

$$|t_1\rangle = |100\rangle - |010\rangle\,, \tag{99}$$
$$|t_2\rangle = |011\rangle - |101\rangle\,. \tag{100}$$

These vectors are mutually orthogonal and also orthogonal to $\mathcal{S}$. Assume that $\mathcal{T}_1 = \mathrm{span}\,\{|t_1\rangle\,, |t_2\rangle\}$ is an invariant subspace for our unitary $U \in \mathrm{U}(8)$. Let $\tilde{U} \in \mathrm{U}(2)$ be its restriction to the subspace $\mathcal{T}_1$. Let $\mathcal{T}_2 = \mathcal{T}_1^\perp$ be the orthogonal complement of $\mathcal{T}_1$ in $\mathcal{T}$. Then it turns out that U must act in the same way (as $\tilde{U}$) on $\mathcal{T}_2$.

Since U must commute with all qubit permutation matrices, it must act as $\tilde{U}$ in the following subspaces (obtained from $\{|t_1\rangle\,, |t_2\rangle\}$ by a cyclic permutation of qubits):

$$|t_1'\rangle = |010\rangle - |001\rangle\,, \qquad |t_1''\rangle = |001\rangle - |100\rangle\,,$$
$$|t_2'\rangle = |101\rangle - |110\rangle\,, \qquad |t_2''\rangle = |110\rangle - |011\rangle\,.$$

[3] For convenience we will use non-normalized vectors in this section.

By linearity U must act as $\tilde{U}$ also in:

$$\left|t_1^{\perp}\right\rangle = |t_1'\rangle - |t_1''\rangle = |100\rangle + |010\rangle - 2\,|001\rangle\,, \tag{101}$$

$$\left|t_2^{\perp}\right\rangle = |t_2'\rangle - |t_2''\rangle = |011\rangle + |101\rangle - 2\,|110\rangle\,. \tag{102}$$

Hence U acts as $\tilde{U}$ also in $\mathcal{T}_2$, since $\mathcal{T}_2 = \operatorname{span}\left\{\left|t_1^{\perp}\right\rangle, \left|t_2^{\perp}\right\rangle\right\}$.

It remains to be shown that U can act arbitrarily in $\mathcal{T}_1$ (i.e., we can take any $\tilde{U} \in \mathrm{U}(2)$). To show this, we must verify that U preserve inner products. [to do...]

4.4.2 Normalizer of $\mathcal{S}_n$

Lemma 14. If U is a unitary such that $\forall P \in \mathcal{S}_n, \exists Q \in \mathcal{S}_n : UP = QU$, then the Hamiltonians H and $UHU^\dagger$ are either both universal or non-universal.

The set of all such unitaries is called the *normalizer* of $\mathcal{S}_n$ and is denoted by $N(\mathcal{S}_n)$. For three qubits it can be shown that $N(\mathcal{S}_3)$ consists of exactly those unitaries U that are of the form $U = PC$, where $P \in \mathcal{S}_3$ and $C \in Z(\mathcal{S}_3)$.

4.4.3 "Monsterizer" of $\mathcal{S}_n$

Lemma 15. If U and V are unitaries such that $\forall P \in \mathcal{S}_n, \exists Q \in \mathcal{S}_n : UP = QV$, then the Hamiltonians H and $UHU^\dagger$ are either both universal or non-universal.

4.5 Pauli basis [NEW]

Every Hamiltonian on n qubits (i.e., $2^n \times 2^n$ Hermitian matrix) can be expressed as a real linear combination of tensor products of Pauli matrices I, X, Y, Z defined in euqation (39), i.e., they form a basis of all $2^n \times 2^n$ Hermitian matrices. The good thing about Pauli matrices is that they provide a basis that is compatible with the tensor product, i.e., the Pauli basis of a composite system is obtained by taking the tensor product of the elements of the Pauli bases of the subsystems. The number of non-identity Pauli matrices in the tensor product we call the *weight*.

4.5.1 From 2 to 3 qubits [NEW]

For convenience in this section we will omit the tensor product sign (XX stands for $X \otimes X$).

Lemma 16. One can attain any evolution on n qubits given the ability to evolve according to X, Y, and XX on any of the qubits.[4]

Proof. It is enough to show that the evolution according to any tensor product of Pauli matrices can be attained, because any Hermitian matrix can be expressed as a real linear combination of them. We also know that given H_1 and H_2 we

[4] The choice of these particular Hamiltonians is arbitrary – we just need two Pauli matrices of weight 1 and one Pauli matrix of weight 2.

can evolve according to $i[H_1, H_2]$ (the commutators of Pauli matrices are listed in Table 4). Thus we can attain arbitrary evolution on any single qubit, since we are given X and Y, and we can obtain $Z = \frac{1}{2}i[Y, X]$. Similarly, we can attain any 2-qubit evolution using XX and the single qubit Hamiltonians, e.g., $XY = \frac{1}{2}i[XX, IZ]$, $ZY = \frac{1}{2}i[YI, XY]$, etc.

	I	X	Y	Z
I	0	0	0	0
X	0	0	$-2Z$	$2Y$
Y	0	$2Z$	0	$-2X$
Z	0	$-2Y$	$2X$	0

Table 4: Commutators $i[R, C] = i(RC - CR)$ of Pauli matrices. R is a label of a row and C is a label of a column.

To show that any evolution on n qubits can be attained, it is sufficient to show that any tensor product of Pauli matrices can be expressed as nested commutators of Pauli matrices that act non-trivially on at most two qubits. We will show this by decomposing a tensor product of Pauli matrices into a sequence of Pauli matrices of weight 2 so that each pair of adjacent sequences anti-commute.

Let us illustrate this with an example – consider a specific tensor product of Pauli matrices, e.g., $XZYXXIZIYZX$ (see Table 5). We can break this string down into overlapping sequences of length two: XZ, ZY, YX, XX, ... Then for each adjacent pair of sequences we modify the overlapping Pauli matrix in different ways. For example, if we take the first two sequences (XZ and ZY), the overlapping matrix is Z. We can change it to X in the first sequence and to Y in the second sequence (or vice versa), and obtain either XX and YY, or XY and XY. In both cases we get the same commutator (up to a constant), when these matrices act on appropriate qubits:

$$-\frac{1}{2}i[XXI, IYY] = \frac{1}{2}i[XYI, IXY] = XZY. \tag{103}$$

Note that this value coincides with the beginning of the string corresponding to the Hamiltonian we want to simulate. If we repeat this process and modify each pair of adjacent overlapping sequences according to the rule specified above, the nested commutator of them will be equal (up to a constant factor) to our Hamiltonian. This is illustrated in Table 5.

□

Theorem 13. If a 2-qubit Hamiltonian H is universal for 2 qubits, then it is universal for n qubits.

It is well known that an analogous statement is true for unitary matrices – it follows from the fact that any unitary on n qubits can be decomposed into gates that act non-trivially only on one or two qubits without the need of ancilla [2, 3]. This implies that it is true also for Hamiltonians. However, it immediately follows from our Lemma 16.

X	Z	Y	X	X	I	Z	I	Y	Z	X
X	Y									
	X	X								
		Z	Z							
			Y	Z						
				Y		Y				
						X		X		
								Z	Y	
									X	X

Table 5: An example of expressing a tensor product of Pauli matrices as a nested commutator of Pauli matrices that act non-trivially on at most two qubits.

Proof. Since H is universal for two qubits, we can simulate X and Y on any qubit and XX on any pair of qubits. Thus according to Lemma 16 we can simulate any Hamiltonian on n qubits. □

5 Schur basis for Hamiltonians

[NEW]

5.1 Decomposition of a 3-qubit Hamiltonian

[NEW]

Let us use the following notation:

$$T_{12} \text{ – the gate that swaps qubits 1 and 2,} \tag{104}$$

$$T_{23} \text{ – the gate that swaps qubits 2 and 3.} \tag{105}$$

Note that any permutation of three qubits can be built out of T_{12} and T_{23}. Moreover, since $T_{12}^2 = T_{23}^2 = I$, we can do this by alternating between T_{12} and T_{23} as shown in Table 6. Note that $T_{23}P_5 = I$.

Definition	Permutation	Type
$P_0 := I$	123	rotation
$P_1 := T_{12}P_0$	213	transposition
$P_2 := T_{23}P_1$	231	rotation
$P_3 := T_{12}P_2$	321	transposition
$P_4 := T_{23}P_3$	312	rotation
$P_5 := T_{12}P_4$	132	transposition

Table 6: $\mathcal{S}_3$ obtained by alternating between T_{12} and T_{23}.

Given a 3-qubit Hamiltonian H, let us consider sums of the following form:

$$H_\chi := \sum_{i=0}^{5} \chi(i) P_i H P_i^\dagger, \tag{106}$$

where $\chi : \{0, \ldots, 5\} \to \mathbb{R}$. Clearly, H_χ can be simulated by H, since it is just a real linear combination of "H applied in different ways". In particular, let

$$S := \frac{1}{6} H_{\chi_S}, \quad A := \frac{1}{6} H_{\chi_A}, \quad R := \frac{1}{3} H_{\chi_R}, \tag{107}$$

where χ_S, χ_A, and χ_R are given in Table 7.

Character	0	1	2	3	4	5
χ_S	1	1	1	1	1	1
χ_A	1	−1	1	−1	1	−1
χ_R	2	0	−1	0	−1	0

Table 7: Characters of irreducible representations of S_3.

Note that

$$H = S + A + R. \tag{108}$$

Let us call the corresponding subspaces $\mathcal{S}$, $\mathcal{A}$, and $\mathcal{R}$. The following commutation relations hold:

$$i[\mathcal{S},\mathcal{S}] \subseteq \mathcal{S}, \tag{109}$$
$$i[\mathcal{S},\mathcal{A}] \subseteq \mathcal{A}, \tag{110}$$
$$i[\mathcal{A},\mathcal{A}] \subseteq \mathcal{S}, \tag{111}$$
$$i[\mathcal{A},\mathcal{R}] \subseteq \mathcal{R}, \tag{112}$$
$$i[\mathcal{S},\mathcal{R}] \subseteq \mathcal{R}. \tag{113}$$

Moreover,

$$\mathcal{A} \cdot \mathcal{A} \subseteq \mathcal{S}, \tag{114}$$
$$\mathcal{S} \cdot \mathcal{S} \subseteq \mathcal{S}. \tag{115}$$

5.2 Schur basis using Pauli matrices

[NEW]

5.2.1 Different view of conjugation

[NEW]

Let us illustrate how conjugation can be viewed as a linear map in some larger space. For this purpose let us define a mapping

$$\mathrm{vec}(|b\rangle\langle a|) := |b\rangle|a\rangle \tag{116}$$

that turns any matrix into a vector [4]. If A, B, and X are arbitrary square matrices of the same size, then

$$\mathrm{vec}(AXB^{\mathsf{T}}) = (A \otimes B)\,\mathrm{vec}(X). \tag{117}$$

In particular, let H be any n-qubit Hamiltonian and $P \in \mathcal{S}_n$ be any n-qubit permutation matrix. Since $P = P^*$, we have

$$\mathrm{vec}(PHP^\dagger) = (P \otimes P)\,\mathrm{vec}(H), \tag{118}$$

In other words, instead of conjugating H by P, we can act with $P \otimes P$ on vectorized from of H. Note that

$$\{P \otimes P \mid P \in \mathcal{S}_n\} \tag{119}$$

is a representation of S_n. We would like to decompose it into irreducible representations (or decompose the action of $P \otimes P$ into invariant subspaces).

5.2.2 Pauli vector

[NEW]

For the purpose of decomposing the representation (119) into irreducible ones, let us use another way how to turn a matrix into a vector. Note that n-qubit Hamiltonians form a real linear space of dimension 2^n. A convenient choice of

basis for this space is the set of all n-fold tensor products of Pauli matrices. Thus we can write any n-qubit Hamiltonian in the form

$$H = \sum_{\sigma_1,\sigma_2,\ldots,\sigma_n \in \{I,X,Y,Z\}} \alpha_{\sigma_1,\sigma_2,\ldots,\sigma_n} \sigma_1 \otimes \sigma_2 \otimes \ldots \otimes \sigma_n. \tag{120}$$

Hence, the set of all n-qubit Hamiltonians is isomorphic to

$$\operatorname{span}_{\mathbb{R}} \left\{ |\sigma_1 \sigma_2 \cdots \sigma_n\rangle \mid \sigma_i \in \{I, X, Y, Z\} \right\}, \tag{121}$$

where strings of Pauli matrices are used to label the basis states. To find the component $\alpha_{\sigma_1,\sigma_2,\ldots,\sigma_n}$ of H along $|\sigma_1\sigma_2 \cdots \sigma_n\rangle$, we compute

$$\alpha_{\sigma_1,\sigma_2,\ldots,\sigma_n} = \frac{1}{2^n} \operatorname{Tr}(H \cdot \sigma_1 \otimes \sigma_2 \otimes \ldots \otimes \sigma_n). \tag{122}$$

Now we can restate the problem of breaking (119) into irreducible representations in other words: we would like to find the Schur basis for $\left(\mathbb{R}^{\{I,X,Y,Z\}}\right)^{\otimes n}$.

6 Case studies for 3 qubits

[NEW]

Next few subsequent sections contain some examples of Hamiltonians that are not universal for 3 qubits, but are not in our list. In all cases you should think of the Hamiltonian as a generic real linear combination of the two matrices mentioned in the title of the corresponding section. More generally, you can even think of the Hamiltonian as a generic real linear combination of *all* basis elements of the Lie algebra, not just the generators. Examples are sorted according to the dimension of the Lie algebra.

Each section begins with a table that shows how the dimension of the Lie algebra increases as we allow more qubits (we do *not* count the global phase). Note that 4^n is the dimension of the whole Lie algebra on n qubits. Then we provide a list of matrices whose permutations form a basis of the Lie algebra (for 3 or possibly more qubits).

Finally, if we happen to know the (block) structure of the Lie algebra on 3 qubits, we describe it at the end of the section.

6.1 Dimension 15

6.1.1 XX, YY

n	2	3	4	5	6
dim	2	15	60	255	1020
4^n	16	64	256	1024	4096

$$n=3 \quad \left\{ \begin{array}{lll} XXI & & \\ YYI & XYZ & \\ ZZI & & \end{array} \right. \tag{123}$$

$$n=4 \quad \left\{ \begin{array}{lll} XXII & XXYY & \\ YYII & XXZZ & XYZI \\ ZZII & YYZZ & \end{array} \right. \tag{124}$$

$$n=5 \quad \left\{ \begin{array}{llll} XXIII & XXYYI & XXXXI & XYZXX \\ YYIII & XXZZI & YYYYI & XYZYY \quad XYZII \\ ZZIII & YYZZI & ZZZZI & XYZZZ \end{array} \right. \tag{125}$$

Lie algebra on 3 qubits has block structure $\left(\begin{smallmatrix} H & 0 \\ 0 & H \end{smallmatrix}\right)$ in basis

$$\begin{array}{llll} |000\rangle, & |011\rangle, & |101\rangle, & |110\rangle, \\ |111\rangle, & |100\rangle, & |010\rangle, & |001\rangle. \end{array} \tag{126}$$

This Lie algebra is a subalgebra of (141) that has 30 dimensions. We can obtain (141) by adding a new generator YZ.

6.1.2 $XX, YZ + ZY$

n	2	3	4	5	6
dim	2	15	60	255	....
4^n	16	64	256	1024	4096

Lie algebra consists of all permutations of

$$XXI, \tag{127}$$
$$(YZ + ZY)I,\ (YZ - ZY)X, \tag{128}$$
$$(YY + ZZ)I,\ (YY - ZZ)X. \tag{129}$$

It has block structure $\left(\begin{smallmatrix} H & 0 \\ 0 & H \end{smallmatrix}\right)$ in basis

$$\begin{gathered} |000\rangle + |111\rangle, \quad |011\rangle + |100\rangle, \quad |101\rangle + |010\rangle, \quad |110\rangle + |001\rangle, \\ -(|000\rangle - |111\rangle) + (|011\rangle - |100\rangle) + (|101\rangle - |010\rangle) + (|110\rangle - |001\rangle), \\ +(|000\rangle - |111\rangle) - (|011\rangle - |100\rangle) + (|101\rangle - |010\rangle) + (|110\rangle - |001\rangle), \\ +(|000\rangle - |111\rangle) + (|011\rangle - |100\rangle) - (|101\rangle - |010\rangle) + (|110\rangle - |001\rangle), \\ +(|000\rangle - |111\rangle) + (|011\rangle - |100\rangle) + (|101\rangle - |010\rangle) - (|110\rangle - |001\rangle). \end{gathered} \tag{130}$$

This Lie algebra is also a subalgebra of (141) that has 30 dimensions. We can obtain (141) by adding a new generator YZ.

6.1.3 $XI, YZ + ZY$

n	2	3	4	5	6
dim	4	15	64	255	....
4^n	16	64	256	1024	4096

Lie algebra consists of all permutations of

$$XII, \tag{131}$$
$$(YZ + ZY)I,\ (YZ - ZY)X, \tag{132}$$
$$(YY + ZZ)X,\ (YY - ZZ)I. \tag{133}$$

Lie algebra on 3 qubits has block structure $\left(\begin{smallmatrix} H & 0 \\ 0 & -H^{\intercal} \end{smallmatrix}\right)$ in basis (130), where H is Hermitian.

This Lie algebra is also a subalgebra of (141) that has 30 dimensions. We can obtain (141) by adding a new generator YZ.

6.2 Dimension 17

6.2.1 $XX, YZ - ZY$

n	2	3	4	5	6
dim	2	17	66	247	....
4^n	16	64	256	1024	4096

Lie algebra consists of all permutations of

$$XXI, \tag{134}$$
$$(YZ - ZY)I,\ (YZ - ZY)X, \tag{135}$$
$$(YY + ZZ)I,\ (YY + ZZ)X, \tag{136}$$
$$(XI - IX)I. \tag{137}$$

If we add one more generator XI, we get Lie algebra with 18 dimensions. However, if we add YZ instead, we get Lie algebra with 30 dimensions that is equal to (141).

6.3 Dimension 28

6.3.1 XI, XY

n	2	3	4	5	6
dim	6	28	120	496	....
4^n	16	64	256	1024	4096

$$n = 3 \quad \left\{ \begin{array}{lll} IIX & XYI & \\ YYX & XIZ & XXX \\ ZZX & XYZ & \end{array} \right. \tag{138}$$

Lie algebra on 3 qubits has block structure $\left(\begin{smallmatrix} iA & B \\ B^\intercal & iA' \end{smallmatrix}\right)$ in basis (126), where A, B, A' are real, A and A' are antisymmetric (A and A' determine each other).

It turns out that this Lie algebra is in our list. Consider the basis of the Lie algebra generated by XI and XY on two qubits:

$$XI,\ IX,\ XY,\ YX,\ XZ,\ ZX. \tag{139}$$

If we rotate both qubits by $\pi/2$ around z axis, we get

$$YI,\ IY,\ YX,\ XY,\ YZ,\ ZY. \tag{140}$$

This is the Lie algebra of the orthogonal group.

6.4 Dimension 30

6.4.1 XI, YZ

n	2	3	4	5	6
dim	6	30	126	510	....
4^n	16	64	256	1024	4096

$$n=3 \quad \left\{ \begin{array}{cccc} XXI & & III & \\ YYI & XYZ & YYX & IYZ \\ ZZI & & ZZX & \end{array} \right. \tag{141}$$

Lie algebra on 3 qubits has block structure $\left(\begin{smallmatrix} H_1 & 0 \\ 0 & H_2 \end{smallmatrix}\right)$ in basis (130) for some traceless Hamiltonians H_1 and H_2.

6.4.2 $XI + IX, YZ$

n	2	3	4	5	6
dim	4	30	126	510	....
4^n	16	64	256	1024	4096

$$n=3 \quad \left\{ \begin{array}{cccc} XXI & & (XI+IX)I & \\ YYI & XYZ & YYX & IYZ \\ ZZI & & ZZX & \end{array} \right. \tag{142}$$

Lie algebra on 3 qubits has block structure $\left(\begin{smallmatrix} H_1 & 0 \\ 0 & H_2 \end{smallmatrix}\right)$ in basis (130) for some traceless Hamiltonians H_1 and H_2.

It turns out that Lie algebras (141) and (142) are the same. If we compare the basis vectors, we see that the only difference is the following: (141) contains all permutations of XII, but (142) contains all permutations of $(XI + IX)I$. To see that they span the same subspace, observe that

$$(XII + IXI) - (IXI + IIX) + (IIX + XII) = 2XII. \tag{143}$$

A generalization of this Lie algebra is discussed in Sect. 4.1.1.

A Case study (C-NC-U gate)

In this section we consider a specific type of 2-qubit Hamiltonians. We give a necessary and sufficient condition for a Hamiltonian of this type to be universal.

A.1 The Hamiltonian

Consider the following 1-qubit Hamiltonian:

$$H_0 = \begin{pmatrix} \alpha & \theta \\ \theta & \alpha \end{pmatrix}. \tag{144}$$

It has eigenvalues $\alpha \pm \theta$. The corresponding unitary matrix[5] is $U_0 = e^{iH_0}$:

$$U_0 = e^{i\alpha} \begin{pmatrix} \cos\theta & i\sin\theta \\ i\sin\theta & \cos\theta \end{pmatrix}. \tag{145}$$

Now consider the product of controlled-U_0 and NOT-controlled-U_0 (with different parameters α and θ). The corresponding Hamiltonian is:

$$H = \begin{pmatrix} \alpha_1 & \theta_1 & 0 & 0 \\ \theta_1 & \alpha_1 & 0 & 0 \\ 0 & 0 & \alpha_2 & \theta_2 \\ 0 & 0 & \theta_2 & \alpha_2 \end{pmatrix}. \tag{146}$$

It has eigenvalues

$$\begin{aligned} \varphi_1 &= \alpha_1 + \theta_1, \quad \varphi_2 = \alpha_1 - \theta_1, \\ \varphi_3 &= \alpha_2 + \theta_2, \quad \varphi_4 = \alpha_2 - \theta_2, \end{aligned} \tag{147}$$

and eigenvectors

$$\begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} 1 \\ -1 \\ 0 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}, \quad \begin{pmatrix} 0 \\ 0 \\ 1 \\ -1 \end{pmatrix}. \tag{148}$$

The corresponding unitary matrix is $U = e^{iH}$, where

$$U = \begin{pmatrix} e^{i\alpha_1}\cos\theta_1 & ie^{i\alpha_1}\sin\theta_1 & 0 & 0 \\ ie^{i\alpha_1}\sin\theta_1 & e^{i\alpha_1}\cos\theta_1 & 0 & 0 \\ 0 & 0 & e^{i\alpha_2}\cos\theta_2 & ie^{i\alpha_2}\sin\theta_2 \\ 0 & 0 & ie^{i\alpha_2}\sin\theta_2 & e^{i\alpha_2}\cos\theta_2 \end{pmatrix}. \tag{149}$$

A.2 The big determinant

If we apply the commutator scheme given in Table 8 to H, we obtain 16 Hamiltonians $H_1, H_2, \ldots, H_{16}$. Each of them is a 4×4 Hermitian matrix and hence can be specified using 16 real parameters. Thus we can identify each Hamiltonian H_i with a vector $h_i \in \mathbb{R}^{16}$. Therefore the set $\{H_1, H_2, \ldots, H_{16}\}$ is linearly

[5] Sorry for not putting the minus sign, i.e., $U_0 = e^{-iH_0}$.

Level	Commutators
0	$H_1 = H$ $H_2 = THT$
1	$H_3 = i[H_1, H_2]$
2	$H_4 = i[H_1, H_3]$ $H_5 = i[H_2, H_3]$
3	$H_6 = i[H_1, H_4]$ $H_7 = i[H_1, H_5]$
4	$H_8 = i[H_1, H_6]$ $H_9 = i[H_1, H_7]$ $H_{10} = i[H_2, H_6]$
5	$H_{11} = i[H_1, H_8]$ $H_{12} = i[H_1, H_9]$
6	$H_{13} = i[H_1, H_{11}]$ $H_{14} = i[H_1, H_{12}]$
7	$H_{15} = i[H_1, H_{13}]$
8	$H_{16} = i[H_1, H_{15}]$

Table 8: Commutator scheme for Hamiltonian (146).

independent over $\mathbb{R}$ if and only if the set $\{h_1, h_2, \ldots, h_{16}\}$ is linearly independent over $\mathbb{R}$.

We can create a 16×16 matrix M using vectors h_i as columns. The determinant of M is:

$$144506880(\alpha_1+\alpha_2)\theta_1^8(\alpha_1+\theta_1-\alpha_2-\theta_2)^8(\alpha_1+\theta_1-\alpha_2+\theta_2)^8 \\ (\alpha_1-\theta_1-\alpha_2-\theta_2)^8(\alpha_1-\theta_1-\alpha_2+\theta_2)^8\theta_2^8(\alpha_1-\alpha_2)^9(\theta_1+\theta_2)^9(\theta_1-\theta_2)^9 \tag{150}$$

If we ignore the constant factor and rewrite (150) in terms of the eigenvalues (147) of H, we get:

$$(\varphi_1+\varphi_2+\varphi_3+\varphi_4)(\varphi_1-\varphi_2)^8(\varphi_1-\varphi_3)^8(\varphi_1-\varphi_4)^8(\varphi_2-\varphi_3)^8(\varphi_2-\varphi_4)^8(\varphi_3-\varphi_4)^8 \\ (\varphi_1+\varphi_2-\varphi_3-\varphi_4)^9(\varphi_1-\varphi_2+\varphi_3-\varphi_4)^9(\varphi_1-\varphi_2-\varphi_3+\varphi_4)^9 \tag{151}$$

A.3 Universality conditions

If we want all H_i to be linearly independent, the value of (151) should not be zero. Thus the following three types of conditions must be satisfied:

(C1) $\varphi_1 + \varphi_2 + \varphi_3 + \varphi_4 \neq 0$.

(C2) $\varphi_1 \neq \varphi_2$, $\varphi_1 \neq \varphi_3$, $\varphi_1 \neq \varphi_4$, $\varphi_2 \neq \varphi_3$, $\varphi_2 \neq \varphi_4$, $\varphi_3 \neq \varphi_4$.

(C3) $\varphi_1 + \varphi_2 \neq \varphi_3 + \varphi_4$, $\varphi_1 + \varphi_3 \neq \varphi_2 + \varphi_4$, $\varphi_1 + \varphi_4 \neq \varphi_2 + \varphi_3$.

More concisely:

(C1) $\operatorname{Tr} H \neq 0$.

(C2) H has distinct eigenvalues.

(C3) The eigenvalues of H are not *paired*.

If the above three conditions hold, then H is universal, since the determinant (151) is not zero. Thus this set of conditions is *sufficient* for universality of H.

A.4 Necessity of conditions

In this section we will show that H is not universal if it violates any of the above three conditions. In other words, the above conditions are *necessary* for universality of H.

A.4.1 Zero trace

Cannot get global phase. Necessary for any Hamiltonian.

A.4.2 Degenerate eigenvalues

This condition is also necessary for any Hamiltonian.

Lemma 17. If H has a degenerate eigenvalue, then H is not universal.

Proof. Let E^+ be the 3-dimensional $(+1)$-eigenspace of T and $\{|t_1\rangle, |t_2\rangle, |t_3\rangle\}$ be its basis. To show that H is not universal, it suffices to prove that it has an eigenvector lying in E^+. Since H has a degenerate eigenvalue, we can find two orthogonal vectors $|b_1\rangle$ and $|b_2\rangle$ with the same eigenvalue. If $|b_1\rangle \notin E^+$, then $\{|t_1\rangle, |t_2\rangle, |t_3\rangle, |b_1\rangle\}$ is a basis of $\mathbb{C}^4$ and we can write:

$$|b_2\rangle = \gamma_1 |t_1\rangle + \gamma_2 |t_2\rangle + \gamma_3 |t_3\rangle + \gamma_4 |b_1\rangle .$$

Since $\langle b_1|b_2\rangle = 0$, $\gamma_4 = 0$ and $|b_2\rangle \in E^+$. □

A.4.3 Paired eigenvalues

Since all eigenvectors (148) of H have overlap $\frac{1}{2}$ with the singlet state $|s\rangle$, and the eigenvalues are paired, according to Theorem 2 the unitary corresponding to H is T-similar to a tensor product. Hence H is not universal.

There are three possible pairings. We will consider these three cases in the increasing order of difficulty and prove that in each case the corresponding unitary matrix is not universal. [old version]

(C3.1) Pairing $\varphi_1 + \varphi_4 = \varphi_2 + \varphi_3$ or $\theta_1 = \theta_2$. Let us denote $\theta = \theta_1 = \theta_2$. The unitary matrix (149) corresponding to this Hamiltonian is [old version]

$$\begin{pmatrix} e^{i\alpha_1} & 0 \\ 0 & e^{i\alpha_2} \end{pmatrix} \otimes \begin{pmatrix} \cos\theta & i\sin\theta \\ i\sin\theta & \cos\theta \end{pmatrix} . \tag{152}$$

It is clearly not universal, since it is a tensor product.

(C3.2) Pairing $\varphi_1+\varphi_2=\varphi_3+\varphi_4$ or $\alpha_1=\alpha_2$. Let us denote $\alpha=\alpha_1=\alpha_2$. The unitary matrix (149) becomes [old version]

$$e^{i\alpha}\begin{pmatrix}\cos\theta_1 & i\sin\theta_1 & 0 & 0\\ i\sin\theta_1 & \cos\theta_1 & 0 & 0\\ 0 & 0 & \cos\theta_2 & i\sin\theta_2\\ 0 & 0 & i\sin\theta_2 & \cos\theta_2\end{pmatrix}. \tag{153}$$

This matrix is not T-similar to (152), since in general (153) and (152) have different eigenvalues. However, (153) is T-similar to some other tensor product. This can be shown by conjugating it with

$$P=\frac{1}{2}\begin{pmatrix}1 & 1 & 1 & -1\\ 1 & 1 & -1 & 1\\ 1 & -1 & 1 & 1\\ 1 & -1 & -1 & -1\end{pmatrix}. \tag{154}$$

Then we obtain

$$e^{i\alpha}\begin{pmatrix}e^{i\frac{\theta_1+\theta_2}{2}} & 0\\ 0 & e^{i\frac{\theta_1+\theta_2}{2}}\end{pmatrix}\otimes\begin{pmatrix}\cos\frac{\theta_1-\theta_2}{2} & i\sin\frac{\theta_1-\theta_2}{2}\\ i\sin\frac{\theta_1-\theta_2}{2} & \cos\frac{\theta_1-\theta_2}{2}\end{pmatrix}. \tag{155}$$

If we ignore the global phase, the matrix (153) is of the following form: [obsolete]

$$\begin{pmatrix}r_1 & 0 & 0 & r_2\\ 0 & r_3 & r_4 & 0\\ 0 & r_5 & r_6 & 0\\ r_7 & 0 & 0 & r_8\end{pmatrix}+i\begin{pmatrix}0 & c_1 & c_2 & 0\\ c_3 & 0 & 0 & c_4\\ c_5 & 0 & 0 & c_6\\ 0 & c_7 & c_8 & 0\end{pmatrix} \tag{156}$$

for some real constants r_i and c_j. Notice that this form is preserved when a matrix is conjugated by T. Moreover, the product of two such matrices is also of the same form. This is because (156) has two types of rows and columns. If we multiply a row and a column of the same type then the obtained matrix entry is a real number, otherwise it is a purely imaginary number. One can check that the real and purely imaginary entries will be at the same places. Thus the matrices that we can generate will also be of the same form. Hence H is not universal.

(C3.3) Pairing $\varphi_1+\varphi_3=\varphi_2+\varphi_4$ or $\theta_1=-\theta_2$. Denote $\theta=\theta_1=-\theta_2$. Now (149) becomes [old version]

$$\begin{pmatrix}e^{i\alpha_1}\cos\theta & ie^{i\alpha_1}\sin\theta & 0 & 0\\ ie^{i\alpha_1}\sin\theta & e^{i\alpha_1}\cos\theta & 0 & 0\\ 0 & 0 & e^{i\alpha_2}\cos\theta & -ie^{i\alpha_2}\sin\theta\\ 0 & 0 & -ie^{i\alpha_2}\sin\theta & e^{i\alpha_2}\cos\theta\end{pmatrix}. \tag{157}$$

This matrix is not universal, since it is T-similar to (152). One can obtain (152) by conjugating (157) with

$$P = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}. \tag{158}$$

[obsolete] Observe that if we take the absolute value of all entries, the obtained matrix can be expressed in the following form:

$$a \begin{pmatrix} 1&0&0&0 \\ 0&1&0&0 \\ 0&0&1&0 \\ 0&0&0&1 \end{pmatrix} + b \begin{pmatrix} 0&0&0&1 \\ 0&0&1&0 \\ 0&1&0&0 \\ 1&0&0&0 \end{pmatrix} + c \begin{pmatrix} 0&1&0&0 \\ 1&0&0&0 \\ 0&0&0&1 \\ 0&0&1&0 \end{pmatrix} + d \begin{pmatrix} 0&0&1&0 \\ 0&0&0&1 \\ 1&0&0&0 \\ 0&1&0&0 \end{pmatrix} \tag{159}$$

for some non-negative real values of a, b, c, and d (in the case of matrix (157) we have $a = |\cos\theta|$, $c = |\sin\theta|$, and $b = d = 0$). Note that this form is preserved under conjugation by T. Let us call this property *absolute value property*. In fact, the matrix (157) has another property. Choose one of the four blocks in (159). The four entries of (157) corresponding to ones in this block are related in the following way: the product of diametrically opposite (with respect to the center of the matrix) entries multiply to the same number. For example, for the first block it reads: $u_{11}u_{44} = u_{22}u_{33}$. For the last block it reads: $u_{13}u_{42} = u_{31}u_{24}$. This property is also preserved under conjugation of T. Let us call it *four pairings property*. For some reason both (this and the previous property) is preserved under matrix multiplication. Therefore H is not universal.

B U-similarity

In this appendix we will generalize the notions of pattern and T-similarity.

To measure how close two vectors (or 1-dimensional subspaces) $|v\rangle$ and $|w\rangle$ are, we can use the following quantity:

$$d(v,w) = |\langle v|w\rangle|^2 = \mathrm{Tr}(|v\rangle\langle v|\,|w\rangle\langle w|). \tag{160}$$

Similarly we can measure the distance between two bases $\mathcal{V} = \{|v_1\rangle, \ldots, |v_m\rangle\}$ and $\mathcal{W} = \{|w_1\rangle, \ldots, |w_n\rangle\}$ with dimensions m and n respectively as follows:

$$d(\mathcal{V},\mathcal{W}) = \sum_{i=1}^{m}\sum_{j=1}^{n} d(v_i,w_j) = \sum_{i=1}^{m}\sum_{j=1}^{n} |\langle v_i|w_j\rangle|^2 = \mathrm{Tr}(\Pi^{\mathcal{V}}\Pi^{\mathcal{W}}), \tag{161}$$

where $\Pi^{\mathcal{V}} = \sum_{i=1}^{m} |v_i\rangle\langle v_i|$ and $\Pi^{\mathcal{W}} = \sum_{j=1}^{n} |w_j\rangle\langle w_j|$ are projectors to the subspaces $\mathcal{V}$ and $\mathcal{W}$ respectively.

Theorem 14 (U-similarity conditions)**.** Let $U, V, W \in \mathrm{U}(d)$. Let $\{\lambda_1, \ldots, \lambda_L\}$, $\{\mu_1, \ldots, \mu_M\}$, and $\{\nu_1, \ldots, \nu_N\}$ be distinct eigenvalues of U, V, and W respectively and let $\{\Pi_1^{\mathcal{U}}, \ldots, \Pi_L^{\mathcal{U}}\}$, $\{\Pi_1^{\mathcal{V}}, \ldots, \Pi_M^{\mathcal{V}}\}$, and $\{\Pi_1^{\mathcal{W}}, \ldots, \Pi_N^{\mathcal{W}}\}$ be the

projectors to the corresponding eigenspaces whose dimensions are $\dim \mathcal{U}_i = l_i$, $\dim \mathcal{V}_i = m_i$, and $\dim \mathcal{W}_i = n_i$. V and W are U-similar if and only if $M = N$ and both conditions hold

$$\mu_j = \nu_j \text{ and } m_j = n_j \tag{162}$$

$$\mathrm{Tr}(\Pi_i^{\mathcal{U}} \Pi_j^{\mathcal{V}}) = \mathrm{Tr}(\Pi_i^{\mathcal{U}} \Pi_j^{\mathcal{W}}), \tag{163}$$

where $i \in \{1, \ldots, L\}$ and $j \in \{1, \ldots, N\}$.

Proof. Let us prove that these conditions are necessary. Let $W = PVP^\dagger$ for some $P \in \mathrm{U}(d)$ such that $[P, U] = 0$. Clearly V and W have the same eigenvalues with the same multiplicities, hence the first condition is necessary. Note that $\Pi_j^{\mathcal{W}} = P \Pi_j^{\mathcal{V}} P^\dagger$ and $[\Pi_i^{\mathcal{U}}, P] = 0$, thus

$$\mathrm{Tr}(\Pi_i^{\mathcal{U}} \Pi_j^{\mathcal{W}}) = \mathrm{Tr}(\Pi_i^{\mathcal{U}} P \Pi_j^{\mathcal{V}} P^\dagger) = \mathrm{Tr}(P \Pi_i^{\mathcal{U}} \Pi_j^{\mathcal{V}} P^\dagger) = \mathrm{Tr}(\Pi_i^{\mathcal{U}} \Pi_j^{\mathcal{V}}), \tag{164}$$

where the cyclical property of trace was used. □ [Other direction?]

C Some simple lemmas

Lemma 18. Let U and V be similar matrices and P be a unitary such that $V = PUP^\dagger$. Let Q be a unitary. Then $V = QUQ^\dagger$ if and only if $Q = PC$ for some unitary C that commutes with U.

Proof. First, let us verify that we can take any Q of the specified form. If $Q = PC$ and $[C, U] = 0$, then $QUQ^\dagger = PCUC^\dagger P^\dagger = PUCC^\dagger P^\dagger = PUP^\dagger = V$.

Assume $V = QUQ^\dagger$. Then $QUQ^\dagger = PUP^\dagger$ and $(P^\dagger Q)U = U(P^\dagger Q)$. Therefore, $[U, P^\dagger Q] = 0$. If we let $C = P^\dagger Q$, then we have $PC = P(P^\dagger Q) = Q$. □

Lemma 19. Let $\mathcal{S}_n \subset S_{2^n}$ be the set of all qubit permutation matrices. Assume $\mathcal{S}_n$ is genrated by k independent generators $P_1, \ldots, P_k$, i.e., $\mathcal{S}_n = \langle P_1, \ldots, P_k \rangle$. Then the following statements are equivalent:

1. $[A, P_i] = 0$ for all i,
2. $[A, P] = 0$ for all $P \in \mathcal{S}_n$,
3. $[A, P^\dagger] = 0$ for all $P \in \mathcal{S}_n$,
4. $[A^\dagger, P] = 0$ for all $P \in \mathcal{S}_n$,
5. $[A^\dagger, P^\dagger] = 0$ for all $P \in \mathcal{S}_n$.

Proof. Clearly 1, 2, and 5 are equivalent. Clearly 3 and 4 are equivalent. Since $\left\{P^\dagger | P \in \mathcal{S}_n\right\} = \mathcal{S}_n$, 2 and 3 are also equivalent. □

D Lie groups and Lie algebras

D.1 O(2)

[This is based on "Finite Reflection Groups" by L.C.Grove and C.T.Benson.]

D.1.1 Rotation

A counter-clockwise rotation $R(\alpha) \in \mathrm{O}(2)$ by angle α is given by:

$$R(\alpha) := \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}. \tag{165}$$

We have:

$$\begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \begin{pmatrix} 1 \\ i \end{pmatrix} = \begin{pmatrix} \cos\alpha - i\sin\alpha \\ \sin\alpha + i\cos\alpha \end{pmatrix} = e^{-i\alpha} \begin{pmatrix} 1 \\ i \end{pmatrix} \tag{166}$$

and

$$\begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \begin{pmatrix} 1 \\ -i \end{pmatrix} = \begin{pmatrix} \cos\alpha + i\sin\alpha \\ \sin\alpha - i\cos\alpha \end{pmatrix} = e^{i\alpha} \begin{pmatrix} 1 \\ -i \end{pmatrix}. \tag{167}$$

Thus

$$R(\alpha) = U \cdot \exp\left[-i \begin{pmatrix} \alpha & 0 \\ 0 & -\alpha \end{pmatrix}\right] \cdot U^\dagger, \tag{168}$$

where

$$U := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}. \tag{169}$$

One possible choice of a Hamiltonian $H_R(\alpha)$ corresponding to $R(\alpha)$ is

$$H_R(\alpha) := U \cdot \begin{pmatrix} \alpha & 0 \\ 0 & -\alpha \end{pmatrix} \cdot U^\dagger = \alpha \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}. \tag{170}$$

So we have

$$R(\alpha) = \exp\left[-iH_R(\alpha)\right]. \tag{171}$$

D.1.2 Reflection

A reflection $S(\alpha) \in \mathrm{O}(2)$ is given by:

$$S(\alpha) := \begin{pmatrix} \cos\alpha & \sin\alpha \\ \sin\alpha & -\cos\alpha \end{pmatrix}. \tag{172}$$

We have:

$$\begin{pmatrix} \cos\alpha & \sin\alpha \\ \sin\alpha & -\cos\alpha \end{pmatrix} \begin{pmatrix} \cos\frac{\alpha}{2} \\ \sin\frac{\alpha}{2} \end{pmatrix} = \begin{pmatrix} \cos\alpha\cos\frac{\alpha}{2} + \sin\alpha\sin\frac{\alpha}{2} \\ \sin\alpha\cos\frac{\alpha}{2} - \cos\alpha\sin\frac{\alpha}{2} \end{pmatrix} \tag{173}$$

$$= \begin{pmatrix} \cos(\alpha - \frac{\alpha}{2}) \\ \sin(\alpha - \frac{\alpha}{2}) \end{pmatrix} = \begin{pmatrix} \cos\frac{\alpha}{2} \\ \sin\frac{\alpha}{2} \end{pmatrix} \tag{174}$$

and

$$\begin{pmatrix} \cos\alpha & \sin\alpha \\ \sin\alpha & -\cos\alpha \end{pmatrix} \begin{pmatrix} -\sin\frac{\alpha}{2} \\ \cos\frac{\alpha}{2} \end{pmatrix} = \begin{pmatrix} -\cos\alpha\sin\frac{\alpha}{2} + \sin\alpha\cos\frac{\alpha}{2} \\ -\sin\alpha\sin\frac{\alpha}{2} - \cos\alpha\cos\frac{\alpha}{2} \end{pmatrix} \tag{175}$$

$$= \begin{pmatrix} \sin(\alpha - \frac{\alpha}{2}) \\ -\cos(\alpha - \frac{\alpha}{2}) \end{pmatrix} = -\begin{pmatrix} -\sin\frac{\alpha}{2} \\ \cos\frac{\alpha}{2} \end{pmatrix}. \tag{176}$$

Thus

$$S(\alpha) = V(\alpha) \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot V(\alpha)^\dagger, \tag{177}$$

where

$$V(\alpha) := \begin{pmatrix} \cos\frac{\alpha}{2} & \sin\frac{\alpha}{2} \\ \sin\frac{\alpha}{2} & -\cos\frac{\alpha}{2} \end{pmatrix}. \tag{178}$$

One possible choice of a Hamiltonian $H_S(\alpha)$ corresponding to $S(\alpha)$ is

$$H_S(\alpha) := V(\alpha) \cdot \begin{pmatrix} 0 & 0 \\ 0 & -\pi \end{pmatrix} \cdot V(\alpha)^\dagger = \frac{\pi}{2} \begin{pmatrix} \cos\alpha - 1 & \sin\alpha \\ \sin\alpha & -\cos\alpha - 1 \end{pmatrix}. \tag{179}$$

So we have

$$S(\alpha) = \exp\left[-iH_S(\alpha)\right]. \tag{180}$$

Note that equation (179) can be rewritten as follows:

$$H_S(\alpha) = \frac{\pi}{2}\big(S(\alpha) - I\big), \tag{181}$$

where $S(\alpha)^2 = I$. Hence

$$\left(\frac{1}{2}\big(S(\alpha) - I\big)\right)^2 = \frac{1}{4}\big(S(\alpha)^2 - 2S(\alpha)I + I^2\big) = -\frac{1}{2}\big(S(\alpha) - I\big). \tag{182}$$

D.2 $\mathrm{O}(n)$

[Rossmann W., Lie Groups - An Introduction Through Linear Groups (Oxford, 2002)]

Lemma 20 (*Eigenvalues for* $\mathrm{O}(n)$)**.** The only possible eigenvalues of $O \in \mathrm{O}(n)$ are: $+1$, -1, and $\left\{e^{i\varphi}, e^{-i\varphi}\right\}$ where $0 < \varphi < \pi$. Moreover, if $O \in \mathrm{SO}(n)$, then the number of eigenvalues -1 is even.

Proof. Since $O \in U(n)$, all eigenvalues have absolute value 1. The characteristic polynomial of O has real coefficients, thus for each root $e^{i\varphi}$ there must also be a complex conjugate root $e^{-i\varphi}$. Finally, $\det O$ is the product of all eigenvalues and is equal to 1 only when the multiplicity of the eigenvalue -1 is even. □

Lemma 21 (*Eigenvectors for* $\mathrm{O}(n)$)**.** For every $O \in \mathrm{O}(n)$ one can find an orthonormal basis of eigenvectors such that: (a) real eigenvalues have real eigenvectors and (b) complex conjugate pairs of eigenvalues have complex conjugate pairs of eigenvectors.

Proof. Let $\lambda = \pm 1$ be a real eigenvalue and $|v\rangle$ be the corresponding eigenvector ($O|v\rangle = \lambda|v\rangle$). Since O and λ are real, we have $O|v\rangle^* = \lambda|v\rangle^*$. Let

$$\begin{aligned} |v_1\rangle &:= |v\rangle + |v\rangle^*, \\ |v_2\rangle &:= \frac{1}{i}(|v\rangle - |v\rangle^*). \end{aligned} \tag{183}$$

Note that both $|v_1\rangle$ and $|v_2\rangle$ are real and $\mathrm{span}_{\mathbb{C}}\left\{|v\rangle, |v\rangle^*\right\} = \mathrm{span}_{\mathbb{C}}\left\{|v_1\rangle, |v_2\rangle\right\}$. Thus both $|v_1\rangle$ and $|v_2\rangle$ are real eigenvectors corresponding to eigenvalue λ. It might happen that $|v_1\rangle$ and $|v_2\rangle$ are linearly dependent over $\mathbb{R}$, but in any case we get at least one real eigenvector corresponding to λ.

If $\lambda = e^{i\varphi} \notin \mathbb{R}$ is a complex eigenvalue and $|v\rangle$ is the corresponding eigenvector, then by taking the complex conjugate we get $O|v\rangle^* = e^{-i\varphi}|v\rangle^*$. □

Theorem 15 (*Block-diagonal form for* $\mathrm{O}(n)$)**.** For every $O \in \mathrm{O}(n)$ there exists $Q \in \mathrm{O}(n)$ such that QOQ^{T} is a block-diagonal matrix with the following kind of blocks: 1, -1, and $R(\alpha)$ defined in equation (165) with $0 < \alpha < \pi$.

Proof. We proceed by induction on n. The base cases are $n = 1$ and $n = 2$. If $n = 1$, we are done, since $O = \pm 1$. For $n = 2$ we have to consider two subcases. If $\det O = 1$, then $O \in \left\{R(\alpha), \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)\right\}$ (see Sect. D.1.1) and it already has the required block structure. If $\det O = -1$, then $O = S(\alpha)$ defined in equation (172) where $0 \leq \alpha < 2\pi$ (see Sect. D.1.2). So we can use $Q = V(\alpha) \in \mathrm{O}(2)$ defined in equation (178) to diagonalize O. We obtain $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ that has the required block structure.

We assume that the claim holds for all $n < k$ for some k and want to prove that it also holds for $n = k$. Let λ be any eigenvalue of O. If $\lambda \in \mathbb{R}$, then $\lambda = \pm 1$ and according to Lemma 21 we can find at least one real eigenvector $|v\rangle$ corresponding to λ. We let O' be the restriction of O to the (real) orthogonal complement of $|v\rangle$ and apply the induction on O'. If $\lambda = e^{i\varphi} \notin \mathbb{R}$ and $|v\rangle$ is the corresponding (complex) eigenvector, then we can define real vectors $|v_1\rangle$ and $|v_2\rangle$ as in equation (183) in Lemma 21. They are not eigenvectors of O anymore. However, the two-dimensional subspace $V = \mathrm{span}_{\mathbb{R}}\left\{|v_1\rangle, |v_2\rangle\right\}$ is invariant under O. Moreover, the restriction of O to V has eigenvalues $\left\{e^{i\varphi}, e^{-i\varphi}\right\}$, thus it is a rotation $R(\varphi)$ by angle φ (see Sect. D.1.1). To conclude the proof, we consider the restriction O' of O to the (real) orthogonal complement of V and apply the induction on O'. □

References

[1] Harrow A.W., Applications of coherent classical communication and the Schur transform to quantum information theory. arXiv:quant-ph/0512255v1.

[2] Barenco A., Bennett C.H., Cleve R., DiVincenzo D.P., Margolus N., Shor P., Sleator T., Smolin J., Weinfurter H., Elementary gates for quantum computation, arXiv:quant-ph/9503016v1.

[3] Nielsen M.A., Chuang I.L., Quantum Computation and Quantum Information, Cambridge University Press, 2000.

[4] Watrous J., Lecture notes, University of Waterloo, 2008.