Characterization of non-universal two-qubit Hamiltonians

by

Laura Mancinska

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Mathematics
in
Combinatorics and Optimization

Waterloo, Ontario, Canada, 2009

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

It is known that almost all 2-qubit gates are universal for quantum computing (Lloyd 1995; Deutsch, Barenco, Eckert 1995). However, an explicit characterization of non-universal 2-qubit gates is not known. We consider a closely related problem of characterizing the set of non-universal 2-qubit Hamiltonians. We call a 2-qubit Hamiltonian n-universal if, when applied on different pairs of qubits, it can be used to approximate any unitary operation on n qubits. It follows directly from the results of Lloyd and Deutsch, Barenco, Eckert, that almost any 2-qubit Hamiltonian is 2-universal. Our main result is a complete characterization of 2-non-universal 2-qubit Hamiltonians. There are three cases when a 2-qubit Hamiltonian H is not universal: (1) H shares an eigenvector with the gate that swaps two qubits; (2) H acts on the two qubits independently (in any of a certain family of bases); (3) H has zero trace. The last condition rules out the Hamiltonians that generate SU(4)—it can be omitted if the global phase is not important.

A Hamiltonian that is not 2-universal can still be 3-universal. We give a (possibly incomplete) list of 2-qubit Hamiltonians that are not 3-universal. If this list happens to be complete, it actually gives a classification of n-universal 2-qubit Hamiltonians for all $n \geq 3$.

Acknowledgements

I am most grateful to my supervisors Debbie Leung and Andrew Childs who were always ready to listen and discuss the intermediate results. They proposed the problem addressed in this thesis.

I want to thank John Watrous for his comments that helped me to improve the structure of this thesis as well as simplify the proof of Claim 1. Thanks to Debbie for carefully reading through the proof details and pointing out the loopholes in them. I also want to thank Andrew for his suggestions, that helped to improve the style of this thesis.

I am grateful to my family back in Latvia for they continued patience and moral support.

I want to thank my friends Roohen S. Tarighat and Xavier Pérez for sharing their insights on Diophantine approximations as well as encouraging me during the writing process.

Finally, I want to thank Māris Ozols, who was always there to support me. His collaboration was invaluable for reaching the results presented in this thesis.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

It is often useful to understand when a given set of resources is sufficient to perform universal computation. In particular, universal Hamiltonians have many applications in quantum computation.

Suppose we can implement one specific 2-qubit Hamiltonian $H \in \mathfrak{u}(4)$, where $\mathfrak{u}(4)$ denotes the set of all 4×4 Hermitian matrices. Assume that we have n qubits and we can apply H to any ordered pair of them for any amount of time. We say that H is n-universal if it is possible to approximate any unitary evolution $U \in \mathrm{U}(2^n)$ to any desired accuracy by repeatedly applying H to different pairs of qubits.

It is known that almost any 2-qubit Hamiltonian is universal [10, 22], i.e., non-universal 2-qubit Hamiltonians form a measure zero subset of $\mathfrak{u}(4)$. Given a specific $H \in \mathfrak{u}(4)$, it is relatively easy to check if H is n-universal. We just have to check whether the Lie algebra generated by H (when applied on different pairs of qubits) is equal to $\mathfrak{u}(2^n)$, the Lie algebra of $\mathrm{U}(2^n)$ (see Section 3.3).

However, so far there has been no closed-form characterization of the set of non-universal 2-qubit Hamiltonians. In particular, we would like to have a characterization that is capable of answering structural questions about the entire set of Hamiltonians. For example, suppose we can implement Hamiltonians of a certain form. Then we would like to be able to say which of these Hamiltonians are universal.

In this thesis we characterize the set of all 2-non-universal 2-qubit Hamiltonians in a way that would help to answer questions of the form described above. We give a finite list of families of 2-non-universal 2-qubit Hamiltonians such that each family can be easily parametrized and together they cover all 2-non-universal 2-qubit Hamiltonians.

We now explain the structure of the thesis. In Section 2 we provide some background material that is needed in order to better understand the following sections. We start by introducing some notation in Section 2.1.1. Then in Sections 2.1.2 and 2.1.3 we define and briefly discuss normal matrices and Pauli matrices, respectively. We continue by discussing quantum states and evolutions in Sections 2.2.1 and 2.2.2, respectively.

In the next section we formally define the problem to be addressed (Section 3.1), explain the relevant previous results (Section 3.2) and give proofs of some results regarding n-universality (Section 3.3).

The goal of Section 4 is to give a complete characterization of 2-non-universal 2-qubit Hamiltonians. We start by discussing the properties of the gate that swaps the two qubits in Section 4.1. Next, we present examples of non-universal Hamiltonians in Section 4.2. It will turn out that these examples capture the essence of what can make a 2-qubit Hamiltonian non-universal. In Section 4.3 we consider transformations that preserve the 2-universality property of 2-qubit Hamiltonians. Using these transformations we bring a generic 2-qubit Hamiltonian to a specific normal form and give sufficient conditions for a Hamiltonian in this normal form to be non-universal (see Sections 4.5.1 and 4.5.2). To prove that these conditions are also necessary, we give explicit expressions for linear combinations of nested commutators that provide a maximal number of linearly independent Hamiltonians (see Section 4.5.3). Finally, we reach Theorem 7 which gives a complete characterization of 2-non-universal 2-qubit Hamiltonians.

In Section 5 we list the families of 2-qubit Hamiltonians that we know to be 3-non-universal and discuss their relation to families of 2-non-universal 2-qubit Hamiltonians given in Theorem 7.

Chapter 2

Background on quantum computing

The idea of a quantum computer first appeared in the works of Benioff and Feynman around 1980. Benioff showed that quantum systems can simulate a classical reversible Turing machine [3, 4]. Feynman considered the opposite problem and observed that it is very hard to simulate a quantum system using a classical computer [13]. He also observed that in principle quantum systems could be simulated efficiently using a quantum computer.

The first quantum algorithm in which quantum effects were used is due to Deutsch [8]; it was subsequently improved and generalized by Deutsch and Jozsa [11] (see [23] or [19] for a modern treatment of both results). Deutsch's algorithm computes the value of $f(0) \oplus f(1)$ for some unknown function $f : \{0,1\} \to \{0,1\}$ with just one query to f, whereas any deterministic algorithm needs two queries. Similarly, the Deutsch-Jozsa algorithm determines if $f : \{0,1\}^n \to \{0,1\}$ is constant (the value of $f(x)$ does not depend on x) or balanced ($f(x) = 0$ for exactly half of all inputs x, and $f(x) = 1$ for the other half) with a single query to f, whereas any deterministic algorithm requires $2^{n-1}+1$ queries in the worst case. One can see that for this particular problem quantum computer has a tremendous advantage over a deterministic classical computer. However, the quantum over classical advantage becomes negligible if we consider probabilistic classical algorithms, since there is a probabilistic algorithm whose success probability is at least $2/3$ that can solve this problem with just 2 queries [19].

The next breakthrough was Simon's algorithm, which significantly outperforms even a probabilistic classical algorithm [27]. The best known quantum algorithm requires a linear number of queries, whereas any probabilistic classical algorithm requires an exponential number of queries. This work led to one of the most important achievements in quantum computing—Shor's polynomial-time algorithm for factoring, which is exponentially faster than the best known classical algorithm [26].

Another well-known result is Grover's algorithm for searching an unsorted database [15, 14]. It provides only a quadratic speedup over the best classical algorithm, but its importance stems from its wide range of applications.

2.1 Mathematical tools

2.1.1 Notation

We start by introducing notation that will be useful later. In this section we already use the Dirac notation. We refer the reader who is not familiar with it to Section 2.2.1.

Let I_N be the $N \times N$ identity matrix (we often abbreviate I_2 as I). We use $M^\dagger$ to denote the conjugate transpose of a matrix M. We define some commonly used sets:

- $\mathrm{M}_N(\mathbb{C})$ – the set of all $N \times N$ complex matrices.
- $\mathrm{M}_N(\mathbb{R}) \subset \mathrm{M}_N(\mathbb{C})$ – the set of all $N \times N$ real matrices.
- $\mathrm{U}(N) := \left\{U \in \mathrm{M}_N(\mathbb{C}) \mid U^\dagger U = I_N\right\}$ – the *unitary group*.
- $\mathrm{SU}(N) := \{U \in \mathrm{U}(N) \mid \det U = 1\} \subset \mathrm{U}(N)$ – the *special unitary group*.
- $\mathrm{O}(N) := \left\{O \in \mathrm{M}_N(\mathbb{R}) \mid O^\mathsf{T} O = I_N\right\} = \mathrm{M}_N(\mathbb{R}) \cap \mathrm{U}(N)$ – the *orthogonal group*.
- $\mathrm{SO}(N) := \{O \in \mathrm{O}(N) \mid \det O = 1\} \subset \mathrm{O}(N)$ – the *special orthogonal group*.
- $\mathfrak{u}(N) := \left\{H \in \mathrm{M}_N(\mathbb{C}) \mid H = H^\dagger\right\}$ – the *Lie algebra* of $\mathrm{U}(N)$ or the set of all $N \times N$ *Hermitian matrices*.
- S_n – the *symmetric group* or the set of all n-element permutations.
- $\mathcal{S}_n \subset \mathrm{M}_{2^n}(\{0,1\}) \cap \mathrm{O}(2^n)$ – the group of all n-qubit permutation matrices. To every permutation $\pi \in S_n$ we assign the corresponding n-qubit permutation matrix $P_\pi \in \mathcal{S}_n$ that acts in the standard basis as follows:
$$\forall s \in \{0,1\}^n : P_\pi\big(|s_1\rangle\,|s_2\rangle \ldots |s_n\rangle\big) = \left|s_{\pi^{-1}(1)}\right\rangle \left|s_{\pi^{-1}(2)}\right\rangle \ldots \left|s_{\pi^{-1}(n)}\right\rangle. \quad (2.1)$$
- $[n] := \{1, \ldots, n\}$ – the set of natural numbers from 1 to n.

Whenever we need to take a norm of an operator we choose to use the spectral norm. Most of the time, however, it does not matter which norm one chooses to use.

Definition 1. Let $M \in \mathrm{M}_N(\mathbb{C})$. Then the *spectral* or *operator norm* of M is defined as
$$\|M\|_\infty := \max\left\{\|Mv\| : v \in \mathbb{C}^N, \|v\| = 1\right\}$$
where $\|\cdot\|$ is the Euclidean norm.

2.1.2 Normal matrices

In quantum computing we often work with *normal* matrices. In this section we define this class of matrices and list some useful theorems. See [17] or any other standard textbook on matrix analysis for the proofs and more discussion.

Definition 2. We say that a matrix $M \in \mathrm{M}_N(\mathbb{C})$ is *normal* if $MM^\dagger = M^\dagger M$.

We will mainly deal with two special types of normal matrices, namely *Hermitian* matrices and *unitary* matrices.

Definition 3. We say that a matrix $U \in \mathrm{M}_N(\mathbb{C})$ is *unitary* if $UU^\dagger = I_N$.

Definition 4. We say that a matrix $M \in \mathrm{M}_N(\mathbb{C})$ is *Hermitian* if $M = M^\dagger$.

Given an arbitrary matrix $M \in \mathrm{M}_N(\mathbb{C})$, we can find a basis of $\mathbb{C}^N$ in which this matrix is *almost* diagonal. This almost diagonal form is know as the Jordan normal form of M. However, if we consider a normal matrix $A \in \mathrm{M}_N(\mathbb{C})$, then its Jordan form is diagonal. Moreover, it is always possible to choose an *orthonormal* basis of $\mathbb{C}^N$ such that A is diagonal in that basis. That is, we can express A as

$$A = \sum_{i=1}^{N} \lambda_i \left|\psi_i\right\rangle \left\langle\psi_i\right|,$$

where $\{\left|\psi_1\right\rangle, \ldots, \left|\psi_N\right\rangle\} \subset \mathbb{C}^N$ is an orthonormal basis and $\lambda_i \in \mathbb{C}$ for all $i \in [N]$. We call the above expression a *spectral decomposition* of A and $\{\lambda_i\}_{i=1}^N$ the *spectrum* of A.

Suppose $H \in \mathrm{M}_N(\mathbb{C})$ is a Hermitian matrix. Since H is normal, it has a spectral decomposition and we have

$$\sum_{i=1}^{N} \lambda_i \left|\psi_i\right\rangle \left\langle\psi_i\right| = H = H^\dagger = \sum_{i=1}^{N} \lambda_i^* \left|\psi_i\right\rangle \left\langle\psi_i\right|.$$

Since the $\left|\psi_i\right\rangle$ are pairwise orthogonal, we conclude that $\lambda_i = \lambda_i^*$. Thus, the eigenvalues of a Hermitian matrix are real.

Now suppose $U \in \mathrm{M}_N(\mathbb{C})$ is unitary. Since U is normal, it has a spectral decomposition and we have

$$\sum_{i=1}^{N} \left|\psi_i\right\rangle \left\langle\psi_i\right| = I_N = UU^\dagger = \sum_{i,j=1}^{N} \lambda_i\lambda_j^* \left|\psi_i\right\rangle \left\langle\psi_i|\psi_j\right\rangle \left\langle\psi_j\right| = \sum_{i=1}^{N} \left|\lambda_i\right|^2 \left|\psi_i\right\rangle \left\langle\psi_i\right|,$$

where $\sum_{i=1}^{N} \lambda_i \left|\psi_i\right\rangle \left\langle\psi_i\right|$ is a spectral decomposition of U. Since $\left|\psi_i\right\rangle$ are pairwise orthogonal, we conclude that $\left|\lambda_i\right|^2 = 1$. Thus, the eigenvalues of a unitary matrix are of the form $e^{i\varphi}$, where $\varphi \in \mathbb{R}$.

Definition 5. Let $A, B \in \mathrm{M}_N(\mathbb{C})$. Then the *commutator* of A and B, denoted $[A, B]$, is given by

$$[A, B] := AB - BA.$$

We say that A and B *commute* when $[A, B] = 0$.

Definition 6. Let $A, B \in \mathrm{M}_N(\mathbb{C})$. Then the *anticommutator* of A and B, denoted $\{A, B\}$, is given by

$$\{A, B\} := AB + BA.$$

We say that A and B *anticommute* when $\{A, B\} = 0$.

In quantum mechanics observables that have commuting matrix representations correspond to properties that can simultaneously assume definite values. However, we are interested in commutators of normal matrices, because we will investigate Lie algebras generated via commutation. The following theorem gives an equivalent condition for determining whether two *normal* matrices commute. A proof of this theorem can be found in [17].

Theorem 1. Let A and B be normal matrices. Then $[A, B] = 0$ if and only if A and B are simultaneously diagonal in some orthonormal basis.

Suppose we are given a mapping $f : \mathbb{C} \to \mathbb{C}$. Then we can extend the domain and range of this map to normal matrices in the following way:

$$f(A) := \sum_{i=1}^{N} f(\lambda_i) \left|\psi_i\right\rangle \left\langle\psi_i\right|,$$

where $\sum_{i=1}^{N} \lambda_i \left|\psi_i\right\rangle \left\langle\psi_i\right|$ is a spectral decomposition of A.

We will be mostly interested in extending the domain of the exponential map e^{-ix} to the set of Hermitian matrices. If $H \in \mathrm{M}_N(\mathbb{C})$ is Hermitian, then we can think of e^{-iH} in two ways. We can use the spectral decomposition of H and think of e^{-iH} as the matrix obtained by applying e^{-ix} to the eigenvalues of H. Alternatively, we can consider the power series of e^{-ix} and think of e^{-iH} as the matrix given by the following (convergent) infinite sum:

$$I + \frac{-iH}{1!} + \frac{(-iH)^2}{2!} + \frac{(-iH)^3}{3!} + \dots .$$

The two approaches are equivalent. However, sometimes it may be advantageous to use one or the other. We now list some facts that follow directly from one of the above interpretations of e^{-iH}.

Fact 1. Let $H, H_1, H_2 \in \mathfrak{u}(N)$. Then the following statements hold.

- H and e^{-iH} have the same eigenvectors.
- If $[H_1, H_2] = 0$, then $e^{-iH_1}e^{-iH_2} = e^{-i(H_1+H_2)}$. However, this is not true in general.
- For all $U \in \mathrm{U}(N)$, we have $Ue^{-iH}U^\dagger = e^{-iUHU^\dagger}$.

Unitary matrices are related to Hermitian ones via the exponential map. If $H \in \mathrm{M}_N(\mathbb{C})$ is Hermitian, then e^{-iH} is a unitary, since $e^{-iH}(e^{-iH})^\dagger = I_N$. Moreover, any unitary can be obtained in this way. Consider $U \in \mathrm{U}(N)$ with spectral decomposition

$$U = \sum_{i=1}^{N} e^{i\varphi_i} \left|\psi_i\right\rangle \left\langle\psi_i\right| .$$

Then $U = e^{-iH}$ for *exactly* the Hamiltonians of the form

$$H = \sum_{i=1}^{N} (-\varphi_i + 2\pi k_i) \left|\psi_i'\right\rangle \left\langle\psi_i'\right| ,$$

where $k_i \in \mathbb{Z}$ and $\{\left|\psi_i'\right\rangle\}$ is some eigenbasis of U such that $\left|\psi_i'\right\rangle$ corresponds to eigenvalue $e^{i\varphi_i}$ for all $i \in [N]$. Hence, the exponential map takes any Hamiltonian to a unique unitary matrix, whereas the preimage of any unitary matrix contains infinitely many Hamiltonians that all have the same eigenvectors and each of their eigenvalues differ by some multiple of 2π.

2.1.3 Pauli matrices

In this section we briefly discuss the Pauli matrices and list some of their properties. Usually one refers to the following four Hermitian matrices when talking about *Pauli matrices*:

$$I := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad X := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Y := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad Z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} .$$

Note that Pauli matrices form a basis of the real vector space of 2×2 Hermitian matrices. Similarly, $n-$fold tensor products of Pauli matrices form a basis of the real vector space of $2^n \times 2^n$ Hermitian matrices.

Definition 7. The *weight* of $\sigma_1 \otimes \ldots \otimes \sigma_n$, where $\sigma_i \in \{I, X, Y, Z\}$, is the number of times non-identity Pauli matrices appear in the tensor product. For example, the weight of $Y \otimes Y \otimes I \otimes Z$ is 3.

It turns out that

$$\{\alpha\, \sigma_1 \otimes \ldots \otimes \sigma_n : \alpha \in \{\pm 1, \pm i\} \text{ and } \sigma_1, \ldots, \sigma_n \in \{I, X, Y, Z\}\}$$

is a group under matrix multiplication. Also one often finds it useful that all nonidentity Pauli matrices anticommute with each other.

2.2 Quantum states and evolutions

In this section we briefly discuss the allowed states of a quantum computer and how these states evolve. For a more in-depth discussion see [23, 19, 21].

2.2.1 Quantum states

In general, the space of quantum states depends on the particular system considered. However, the state of any closed quantum system can be described as a unit vector in some complex Hilbert space $\mathcal{H}$. The principle of *superposition* says that if a given system can be in states $|\psi_1\rangle, |\psi_2\rangle \in \mathcal{H}$ then any normalized superposition $c_1|\psi_1\rangle + c_2|\psi_2\rangle$ is also a valid state of that system, where $c_1, c_2 \in \mathbb{C}$.

In quantum computing we use the so called *Dirac* or *bra-ket notation*. In this notation, we write the name of a column vector inside a *ket*, e.g., $|\psi\rangle$. We use a *bra* to denote the dual vector, e.g., $\langle\psi|$. If $|\psi\rangle$ is a finite dimensional vector, then its dual vector $\langle\psi|$ is the row vector whose entries are complex conjugates of the corresponding entries of $|\psi\rangle$. Hence, $\langle\psi|\varphi\rangle$ denotes the inner product of $|\psi\rangle$ and $|\varphi\rangle$.

When given a Hilbert space $\mathcal{H}$ with $\dim(\mathcal{H}) = 2^n$, we use the n-bit string binary representation of $k \in \{0, \dots, 2^n - 1\}$ to denote the $(k+1)-$th standard basis vector. For example, if $\mathcal{H} = \mathbb{C}^2$, then

$$|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ and } |1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Similarly, if $\mathcal{H} = \mathbb{C}^4$, then we have

$$|00\rangle := \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad |01\rangle := \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad |10\rangle := \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad |11\rangle := \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

2.2.2 Quantum evolutions

The evolution of a closed quantum system is described by the Schrödinger equation

$$i\frac{\mathrm{d}\,|\psi(t)\rangle}{\mathrm{d}t} = H(t)\,|\psi(t)\rangle\,,$$

where $|\psi(t)\rangle$ is the state of the system at time t and $H(t)$ is a Hermitian matrix known as the system's *Hamiltonian*. In practice we deal with systems that are not closed, i.e., they are interacting with an environment to some extent. However, if the system is sufficiently isolated, we can assume that it is closed and the Schrödinger equation gives a good approximation of its dynamics.

If the system starts out in the state $|\psi(t_1)\rangle$, then by solving the Schrödinger equation we can get its state at time $t_2 \geq t_1$:

$$|\psi(t_2)\rangle = e^{-iH(t_2-t_1)}\,|\psi(t_1)\rangle\,.$$

Recall from Section 2.1.2 that $e^{-iH(t_2-t_1)}$ is a unitary matrix. Therefore, all evolutions of a (closed) quantum system are *unitary*.

Chapter 3

Universality in quantum computing

3.1 The problem

Definition 8. We say that H is an *n-qubit Hamiltonian* if $H \in \mathfrak{u}(2^n)$, i.e., $H \in \mathrm{M}_{2^n}(\mathbb{C})$ and H is Hermitian ($H^\dagger = H$).

In this thesis we mainly deal with 2-qubit Hamiltonians, i.e., 4×4 Hermitian matrices. We often say "a Hamiltonian H", without explicitly mentioning that it is a 2-qubit Hamiltonian.

Definition 9. We say that we can *simulate* a unitary transformation $U \in \mathrm{U}(N)$ using Hamiltonians $H_1, \ldots, H_k \in \mathfrak{u}(N)$, if for all $\varepsilon > 0$ there exist $l \in \mathbb{N}$, $j_1, \ldots, j_l \in [k]$, and $t_1, \ldots, t_l \geq 0$ such that

$$\left\| U - e^{-iH_{j_1}t_1} e^{-iH_{j_2}t_2} \ldots e^{-iH_{j_l}t_l} \right\|_\infty < \varepsilon.$$

Definition 10. We say that an m-qubit Hamiltonian H is *n-universal* where $2 \leq m \leq n$, if we can simulate all unitary transformations in $\mathrm{U}(2^n)$ using Hamiltonians from the set

$$\left\{ P(H \otimes I^{\otimes n-m})P^\dagger \mid P \in \mathcal{S}_n \right\},$$

i.e., by applying H to any ordered subset of m qubits (out of n qubits in total).

Recall from Section 2.1.2 that any evolution of a quantum system is unitary. Therefore, if we are given an n-universal Hamiltonian H, then we can use it to approximate the evolution of an n-qubit system to any desired precision. This justifies the choice of the term "universal".

Universal Hamiltonians and unitary gates have been studied previously [9, 12, 1, 24, 2, 22, 10]. However, there does not seem to be a single commonly accepted definition of universality. Sometimes it is assumed that it is possible to permute the physical qubits and therefore all $P \in \mathcal{S}_n$ can be simulated exactly. However, in our case we only assume the ability to apply the Hamiltonian H to different tuples of qubits, not to permute the qubits themselves. It is also common to allow the use of ancillary qubits that start out, for example, in the $|0\rangle$ state. Sometimes it is required that at the end of the simulation these ancillary qubits need to be returned in the same state as they started out in. In our definition of universality the use of ancillary qubits is not permitted. Also we are not concerned about the time it takes to complete the simulation. We just require the ability to simulate any unitary using H, and accept any simulation as valid even if it takes an unrealistically long time.

In Definition 9 we allowed the use of only non-negative t_{j_i} for simulating unitary U by Hamiltonians $H_1, \ldots, H_k$, since t_{j_i} corresponds to the length of time we evolve according to some Hamiltonian. However, the following claim shows that the restriction $t_{j_i} \geq 0$ in Definition 9 can be relaxed. The essence of the claim is that although we cannot physically evolve our system according to a Hamiltonian H for *negative* time, it turns out that we can approximate the effect by evolving our system according to H for some positive amount of time instead.

Claim 1. Let $H \in \mathfrak{u}(N)$ be a Hamiltonian and $\tau < 0$. Then for all $\varepsilon > 0$ there exists $t \geq 0$ such that $\left\| e^{-iH\tau} - e^{-iHt} \right\|_\infty < \varepsilon$.

Proof. Let $U := e^{-iH}$. Consider the sequence $\mathcal{K} := \{U^i\}_{i=1}^\infty \subset \mathrm{M}_N(\mathbb{C})$. Note that we can think of $\mathrm{M}_N(\mathbb{C})$ as a real vector space of dimension $2N^2$. Since $\mathcal{K}$ is bounded with respect to the spectral norm, by the Bolzano-Weierstrass theorem, $\mathcal{K}$ has a convergent subsequence. It follows that for all $\varepsilon > 0$ and all $n_0 \in \mathbb{N}$ there exist $j, k \in \mathbb{N}$ such that $j - k > n_0$ and $\varepsilon > \left\| U^k - U^j \right\|_\infty = \left\| I_4 - U^{j-k} \right\|_\infty$. Equivalently, for all $\varepsilon > 0$ and all $n_0 \in \mathbb{N}$ there exists $n > n_0$ such that $\varepsilon > \left\| I_4 - U^n \right\|_\infty$. Therefore, given $\tau < 0$, for all $\varepsilon > 0$ there exists $n > |\tau|$ such that

$$\varepsilon > \left\| I_4 - e^{-iHn} \right\|_\infty = \left\| e^{-iH\tau} - e^{-iH(n+\tau)} \right\|_\infty . \tag{3.1}$$

If we take $t := n + \tau > 0$, the claim follows. □

The main goal of this thesis is to characterize the set of 2-qubit 2-universal Hamiltonians. A motivation of this study is that any 2-universal 2-qubit Hamiltonian is also n-universal for all integers $n \geq 2$ (see Corollary 2 below). Note that a 2-qubit Hamiltonian H is 2-universal if we can simulate all unitary transformations in $\mathrm{U}(4)$ using H and THT, where T is the gate that swaps the two qubits and has the following representation in the standard basis

$$T := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} . \tag{3.2}$$

To achieve our goal, we will classify those 2-qubit Hamiltonians that are *not* 2-universal.

3.2 Previous results

We start by discussing some results on universal gate sets for logical boolean functions and proceed with the quantum analogues. It is common to allow the use of ancillary bits or qubits. We proceed to define universality with ancillae.

For all $n \in \mathbb{N}$ let $\mathrm{L}(2^n)$ be the set of matrix representations of n-bit logical boolean functions $f : \{0,1\}^n \to \{0,1\}^n$, i.e.,

$$\mathrm{L}(2^n) := \left\{ M \in \mathrm{M}_{2^n}(\{0,1\}) : \sum_{i=1}^{2^n} M_{i,j} = 1, \forall j \in [2^n] \right\}.$$

Definition 11. We say that a set of logical gates S is *universal with ancillae*, if for all $n \in \mathbb{N}$ and all $\mathcal{L} \in \mathrm{L}(2^n)$ there exist $n_a \in \mathbb{N}$ and a logical circuit $\mathcal{G} \in \mathrm{L}(2^{n+n_a})$ containing gates exclusively from S that simulates $\mathcal{L}$ using ancillae, i.e., there exists $a \in \{0,1\}^{n_a}$ such that for all $\psi \in \{0,1\}^n$ we have

$$(\mathcal{L} |\psi\rangle) \otimes |a\rangle = \mathcal{G}(|\psi\rangle \otimes |a\rangle).$$

Definition 12. We say that a set of unitary gates S is *universal with ancillae*, if for all $n \in \mathbb{N}$, all $\varepsilon > 0$ and all $U \in \mathrm{U}(2^n)$ there exist $n_a \in \mathbb{N}$ and a quantum circuit $\mathcal{G} \in \mathrm{U}(2^{n+n_a})$ containing gates exclusively from S that approximates U with precision ε using ancillae, i.e., there exists $a \in \{0,1\}^{n_a}$ such that for all $|\psi\rangle \in \mathbb{C}^{2^n}$ we have

$$\|(U |\psi\rangle) \otimes |a\rangle - \mathcal{G}(|\psi\rangle \otimes |a\rangle)\| < \varepsilon.$$

Note that in the above definitions we assume the ability to prepare standard basis states. We allow to initialize the ancillary bits to arbitrary standard basis states as opposed to just $|0\rangle$, since some of the gates considered in the coming section (e.g. Toffoli gate and Deutsch's gate) need ancillary bits prepared in basis states other than $|0\rangle$ to achieve universality. However, other reasonable definitions of universality with ancillae are possible different form the ones given above.

In the classical case we are able to implement any logical gate *precisely* using components from a universal gate set. In contrast in the quantum case we only require the ability to *approximate* any unitary to arbitrary precision. This definition is reasonable, since with components from a discrete gate set we cannot hope to implement a continuum of unitary matrices exactly. We are interested in finding *discrete* universal gate sets, since such a set is needed for doing fault-tolerant computing [16].

3.2.1 Universality in classical computing

It is well known that the NAND and FANOUT gates (see Figure 3.1) form a set of logical gates that is universal with ancillae. Since it is often assumed that the ancillary bits and the FANOUT gate are given by default, one often hears that NAND gate is universal for implementing any logical gate.

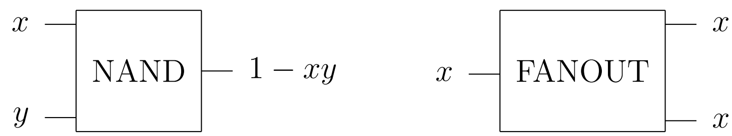

Figure 3.1: NAND and FANOUT gates.

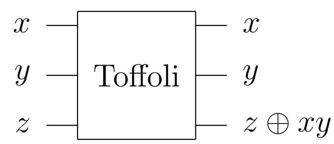

Figure 3.2: Toffoli or the controlled-controlled-NOT gate.

3.2.2 Universal 3-qubit gate

In 1980 Toffoli [28] showed that the *reversible* Toffoli gate (see Figure 3.2) is universal with ancillae for implementing any logical gate. Later on in 1988 Deutsch [9] considered the following family of unitary gates

$$S_Q(\alpha) := I_4 \oplus \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & i\cos\frac{\pi\alpha}{2} & \sin\frac{\pi\alpha}{2} \\ 0 & 0 & \sin\frac{\pi\alpha}{2} & i\cos\frac{\pi\alpha}{2} \end{pmatrix}. \tag{3.3}$$

$S_Q(\alpha)$ is a generalization of the Toffoli gate, since by setting $\alpha = 1$ we obtain the Toffoli gate. Deutsch showed that if α is irrational, then $S_Q(\alpha)$ is universal with ancillae (see Definition 12). At the end of [9] Deutsch conjectures that almost any $2^n \times 2^n$ unitary for $n \geq 3$ is universal in the sense of Definition 12.

3.2.3 Universal gates on at most two qubits

In addition to being useful in fault-tolerant quantum computing, another reason why we are interested in finding universal gate sets is that in order to build a computer we only have to implement a finite number of gates instead of infinitely many. In 1995 DiVincenzo [12] indicated that it might be difficult to implement $S_Q(\alpha)$, since it is a 3-qubit gate and it is hard to build a mechanical device that brings three spins together. However, in the same paper he resolves this difficulty. By building upon Deutsch's result in [9] DiVincenzo shows that for irrational values of ϕ, the set of the following four one- and two-qubit gates is universal with ancillae

$$N := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad V(\phi) := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \cos\phi & \sin\phi \\ 0 & 0 & -\sin\phi & \cos\phi \end{pmatrix}$$

$$X(\phi) := \begin{pmatrix} e^{i\phi} & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad U(\phi) := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \cos\phi & i\sin\phi \\ 0 & 0 & i\sin\phi & \cos\phi \end{pmatrix}. \tag{3.4}$$

Previously, in order to show that a given set of gates is universal, one usually gave circuits for approximating certain classes of unitary gates and used various other ad hoc techniques. However, DiVincenzo noted that the set of unitary transformations that can be approximated using unitary gates from (3.4) is the Lie group corresponding to the Lie algebra generated by the Hamiltonians of those unitary gates. Other authors later on employed this observation to show that almost any 2-qubit gate is universal.

3.2.4 Universal 2-qubit gate

Later in 1995 Barenco [1] improved DiVincenzo's result by showing that a *single* 2-qubit unitary gate can be used to approximate Deutsch's $S_Q(\alpha)$ to any desired precision. Barenco proposed to use the following 2-qubit unitary:

$$A(\phi,\beta,\theta) := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{i\beta}\cos\theta & -ie^{i(\beta-\phi)}\sin\theta \\ 0 & 0 & -ie^{i(\beta+\phi)}\sin\theta & e^{i\beta}\cos\theta \end{pmatrix}, \tag{3.5}$$

where ϕ, β and θ are irrational multiples of π and each other.

3.2.5 Universality of $CNOT$ and 1-qubit gates

It is a well-known fact that any $U \in \mathrm{U}(N)$ can be expressed as a product of elementary unitary gates that act non-trivially on no more than two basis states. These elementary unitary operations are known as *Givens rotations* (e.g., see Cybenko [7]). Cybenko in [7] also gives a quantum circuit for any Givens rotation that contains only one-qubit unitary gates and the controlled-not gates. The original result that one-qubit gates together with the controlled-not gate are universal for implementing any unitary transformation was proved by Barenco et al. in 1995 [2]. There are few points worth noting about this result.

- Using one-qubit unitary gates and the controlled-not gate it is possible to implement all the unitary transformations *exactly* instead of just approximating them. This can be done since we are given the freedom to use a continuum of one-qubit unitary gates.

- Ancillary qubits are *not* needed in order to implement all the unitary transformations. Recall that Deutsch needed ancillae to show the universality of $S_Q(\alpha)$. Since the other universal gate sets discussed above build upon Deutsch's result, they all required ancillae to achieve universality.

- The only 2-qubit gate in this universal gate set, i.e., the controlled-not gate, is classical, meaning that it permutes computational basis states.

Even though the universal gate set proposed in [2] contains a continuum of one-qubit unitary matrices, it is of practical importance, since any $U \in \mathrm{U}(2)$ can be expressed as

$$U = e^{i\phi} e^{-iZt_1} e^{-iYt_2} e^{-iZt_3},$$

where $\phi, t_1, t_2, t_3 \in \mathbb{R}$ and Y, Z are Pauli matrices [23, 2]. Therefore, in order to experimentally implement all one-qubit unitary gates one only needs to be able to evolve the one-qubit system according to Hamiltonians Y and Z for any desired amount of time.

Barenco et al. [2] also investigated how many one-qubit and controlled-not gates are needed to implement Deutsch's $S_Q(\alpha)$ gate and a variety of other two and three-qubit unitary transformations.

In 1997 Kitaev [20] showed that the following set of gates

$$H := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad S^2 := \sqrt{Z} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \tag{3.6}$$

$$CNOT := I_2 \oplus \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad T := I_6 \oplus \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \tag{3.7}$$

consisting of one-qubit unitaries (Hadamard gate and a square root of Pauli Z), the controlled-not gate and the Toffoli gate, is universal for approximating any unitary transformation.

In 1999 Boykin et al. [6] improved the previous result of Kitaev by showing that a set of one- and two-qubit unitaries $\left\{H, \sqrt{S}, CNOT\right\}$ is both universal for approximating any unitary transformation and can be implemented in a *fault-tolerant* way.

3.2.6 Encoded universality

In 2008 Rudolph and Grover [25] considered the following gate:

$$G := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \cos\phi & -\sin\phi \\ 0 & 0 & \sin\phi & \cos\phi \end{pmatrix},$$

where $\phi \in \mathbb{R}$ is some irrational multiple of π. Note that by applying G to different pairs of qubits we cannot implement all unitary transformations, since all matrix entries of G are real. However, it turns out that any computation involving complex amplitudes can be simulated with a computation involving only real ones. The simulation is achieved by introducing an ancillary qubit, whose two orthogonal states are used to encode the real and imaginary parts of the amplitudes. In [25] it is shown that G can be used to approximate any such real simulation. Therefore, we say that G is universal in *encoded* sense. For the most part of this thesis we won't consider encoded universality. However, we get back to it in the last section, where we list the open problems.

3.2.7 Universality of almost any 2-qubit gate

In 1995 both Lloyd [22] and Deutsch et al. [10] independently showed that almost any 2-qubit gate can be used to approximate all 2-qubit unitary evolutions. In other words, the set of non-universal unitary gates form a measure zero subset of the $\mathrm{U}(4)$ group. Therefore, if we pick $U \in \mathrm{U}(4)$ uniformly at random, then U is universal with probability one. It is notable that in order to achieve universality, ancillary qubits are not required. The approaches used in [22] and [10] are similar in many respects. Both of them are not constructive and use the Lie algebra generated through commutation by H and THT, where H is a Hamiltonian corresponding to a generic unitary and T is the gate exchanging the two qubits (see equation (3.2)). Some of the missing details in [22] were later filled in by Weaver [30]. We now review the result presented in [10].

We first outline the proof given by Deutsch et al. in [10] and then continue with discussion of it. Consider a generic $U \in \mathrm{U}(4)$ and let $H \in \mathfrak{u}(4)$ be such that $U = e^{iH}$. Define the *repertoire* of U to be the set of gates that can be approximated by applying U and TUT on two qubits. Since U is generic, the arguments of the eigenvalues of U are irrational multiples of π and each other. Therefore, we can approximate all real powers of U with natural ones. Hence, all gates of the form

$$U^r = e^{iHr}, \quad r \in \mathbb{R} \tag{3.8}$$

are in the repertoire of U. It is possible to argue (see Section 3.3) that if unitary operations e^{iHr} and e^{iTHTr} are in the repertoire of U for all $r \in \mathbb{R}$, then so are all the unitary operations of the form e^{iL} where $L \in \mathcal{L}(H, THT)$ and $\mathcal{L}(H, THT)$ is the Lie algebra generated by H and THT through commutation (see Definition 13). Therefore, U is universal if we can list 16 nested commutators of H and THT that are linearly independent over $\mathbb{R}$.

Now consider the following *commutator scheme* consisting of 16 Hamiltonians:

$$\begin{aligned} H_1 &:= H \\ H_2 &:= TH_1T, \\ H_j &:= i[H_1, H_{j-1}], \quad j \in \{3, \ldots, 14\}, \\ H_{15} &:= i[H_2, H_3], \\ H_{16} &:= i[H_2, H_5]. \end{aligned} \tag{3.9}$$

To show the universality of U it suffices to check that $\{H_1, \ldots, H_{16}\}$ are linearly independent. To check linear independence, we can verify that $\Delta(H) := \det(M) \neq$

0, where M is a real 16×16 matrix whose columns are the vectors corresponding to $H_1, \ldots, H_{16}$, when expressed in some orthonormal basis of $\mathfrak{u}(4)$.

The idea behind the general proof is illustrated by first constructing a one-dimensional affine subspace $\{H(k) : k \in \mathbb{R}\} \subset \mathfrak{u}(4)$, where $H(0) = H$ and $H(k)$ is universal for almost all $k \in \mathbb{R}$. Consider

$$H(k) := H + k(\tilde{H} - H), \tag{3.10}$$

where $\tilde{H}$ is some fixed (universal) Hamiltonian such that[1] $\Delta(\tilde{H}) \neq 0$. For $H(k)$ we compute the parametrized generators $H_j(k)$ using the commutator scheme (3.9) and find the determinant $\Delta(H(k))$. Note that $\Delta(H(k))$ is a polynomial in k of a finite degree (In fact, the degree of $\Delta(H(k))$ is 100). Since $\Delta(H(1)) = \Delta(\tilde{H}) \neq 0$, we conclude that $\Delta(H(k)) \not\equiv 0$. This means that $\Delta(H(k))$ vanishes only at a finite number of different values of k. Thus, if we pick $k \in \mathbb{R}$ uniformly at random, then $e^{-iH(k)}$ is universal with probability one.

The generators in an entire 16-dimensional neighborhood of H can be parametrized by 16 coordinates chosen in the manner similar to (3.10):

$$H(k_1, \ldots, k_{16}) = H + k_1(\tilde{H}^{(1)} - H) + \ldots + k_{16}(\tilde{H}^{(16)} - H), \tag{3.11}$$

where $\tilde{H}^{(1)}, \ldots, \tilde{H}^{(16)}$ are some fixed (universal) Hamiltonians such that $\Delta(\tilde{H}^{(i)}) \neq 0$ for all $i \in [16]$. Again for $H(k_1, \ldots, k_{16})$ we compute the parametrized Hamiltonians $H_j(k_1, \ldots, k_{16})$ according to the commutator scheme (3.9) and find the determinant $\Delta(H(k_1, \ldots, k_{16}))$. Since $\Delta(H(k_1, \ldots, k_{16}))$ is a non-zero polynomial of degree 100 in variables $k_1, \ldots, k_{16}$, it can vanish on at most 15-dimensional variety. Therefore, almost any 2-qubit unitary is universal.

However, some aspects of this proof are unsatisfactory:

1. The goal of [10] is to establish the universality of a generic unitary $U \in \mathrm{U}(4)$. However, in the very beginning of the proof U is replaced by a Hamiltonian H generating U, i.e., satisfying $U = e^{iH}$. Note that one cannot speak about *the* Hamiltonian corresponding to a unitary U (see Section 2.1.2). There are infinitely many Hamiltonians H that satisfy $U = e^{iH}$ for any given U. In fact, even the dimensions of the Lie algebras generated by two Hamiltonians corresponding to the same unitary can differ.

   For example, consider $U := I_4$ and

$$H := \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad H' := \begin{pmatrix} 2\pi & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

   Note that $U = e^{iH} = e^{iH'}$. However,

$$\dim \mathcal{L}\,(H, THT) = 0 \quad \text{while} \quad \dim \mathcal{L}\,(H', TH'T) = 1. \tag{3.12}$$

[1] Note that for an arbitrary universal Hamiltonian H' the determinant $\Delta(H')$ is not necessarily non-zero, since a commutator scheme certifying the universality of H' might differ from the one given in (3.9).

Therefore, one should take extra care to check that for a generic unitary U the Lie algebra $\mathcal{L}(H, THT)$ does not depend on the choice of H satisfying $U = e^{iH}$.

2. Recall the fixed universal Hamiltonian $\tilde{H}$ such that $\Delta(\tilde{H}) \neq 0$ from equation (3.10). In [10] $\tilde{H} := H^A$ is used, where $e^{iH^A} = A(\phi, \beta, \theta)$ and $\phi, \beta, \theta \in \mathbb{R}$ are irrational multiples of π and each other (see equation (3.5)). Recall that Barenco [1] has shown that such $A(\phi, \beta, \theta)$ is universal *with ancillae*. However, ancillary qubits are not allowed in the model used in [10]. Without ancillary qubits A cannot be universal, since both A and TAT have eigenvector $|00\rangle$. Therefore, using A and TAT it is not possible to approximate any $U \in \mathrm{U}(4)$ that does not have $|00\rangle$ as an eigenvector.

   To argue that H^A is universal, in [10] it is claimed that $\Delta(H^A) \neq 0$. The Hamiltonian H^A generating the unitary gate $A(\phi, \beta, \theta)$ is not given explicitly, but let us for instance consider

$$H^A := \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & \beta & -\theta e^{-i\phi} \\ 0 & 0 & -\theta e^{i\phi} & \beta \end{pmatrix}.$$

   Then Hamiltonians $H^A_1, \ldots, H^A_{16} \in \mathfrak{u}(4)$ formed according to the commutator scheme (3.9) are linearly dependent, since they all share eigenvector $|00\rangle$. Therefore, $\Delta(H^A) = 0$, which contradicts the claim made in [10].

3. At the very end of the proof it is claimed that the 16-dimensional neighborhood of H can be parametrized by coordinates chosen in a manner similar to (3.10). However, it is not specified how to do this exactly and equation (3.11) is only our interpretation of how this could be done. Moreover, to employ this approach, 16 linearly independent universal Hamiltonians $\tilde{H}^{(1)}, \ldots, \tilde{H}^{(16)}$ for which $\Delta(\tilde{H}^{(i)}) \neq 0$ for all $i \in [16]$ should be presented. In fact, in [10] not even one such Hamiltonian is explicitly given. Moreover, it is not clear that it is *in principle* possible to find 16 linearly independent universal Hamiltonians for which there exists a *common* commutator scheme that certifies their universality.

In [10] it is also discussed which 2-qubit unitary gates are non-universal and it is conjectured that these are precisely

1. unitary gates that permute states of some orthogonal basis,

2. unitary gates that are tensor products.

In fact, it is not obvious that unitary gates in item (1) are non-universal. Even if U is a permutation matrix in some basis, it does not mean that TUT also permutes the basis vectors of the *same* orthogonal basis. Hence, probably in item (1) the authors of [10] wanted to require that *both* U and TUT permute states of the same orthogonal basis.

In this thesis we answer a slight modification of the above question raised in [10]: we give a complete characterization of the set of non-universal 2-qubit Hamiltonians (instead of 2-qubit unitary gates). In particular, our characterization disproves the conjecture given in [10] (see Theorem 7).

3.3 Proving universality

It is not obvious how to check if a given Hamiltonian is universal according to the above definition, i.e., can be used to simulate any unitary matrix. Thus we would like to have an equivalent but simpler universality condition that is more practical. In other words, we are looking for an efficient algorithm for deciding if a given Hamiltonian is universal.

First, we need to understand which evolutions can be simulated using a given Hamiltonian H. In order to do that, we introduce the notion of a Lie algebra.

Definition 13. We say that $\mathcal{L}(H_1, \ldots, H_k)$ denotes the *Lie algebra generated by Hamiltonians* $H_1, \ldots, H_k$. It is defined inductively by the following three rules:

1. $H_1, \ldots, H_k \in \mathcal{L}(H_1, \ldots, H_k)$,
2. If $A, B \in \mathcal{L}(H_1, \ldots, H_k)$ then $\alpha A + \beta B \in \mathcal{L}(H_1, \ldots, H_k)$ for all $\alpha, \beta \in \mathbb{R}$,
3. If $A, B \in \mathcal{L}(H_1, \ldots, H_k)$ then $i[A, B] = i(AB - BA) \in \mathcal{L}(H_1, \ldots, H_k)$.

One can think of $\mathcal{L}(H_1, \ldots, H_k)$ as a real vector space equipped with a way of combining any two vectors to obtain the third. Note that if A, B are Hermitian, then $i[A, B]$ is also Hermitian, since we have

$$(i[A, B])^\dagger = -i(B^\dagger A^\dagger - A^\dagger B^\dagger) = i[A, B].$$

Therefore, $\mathcal{L}(H_1, \ldots, H_k)$ is a real subspace of Hermitian matrices. It consists of all those Hermitian matrices that can be expressed as finite real linear combinations of nested commutators of Hamiltonians $H_1, \ldots, H_k$.

The following lemma helps us to understand the set of evolutions that we are able to simulate using some given set of Hamiltonians.

Lemma 1. Assume that we can evolve according to Hamiltonians $H_1, \ldots, H_k$ for any desired amount of time. Then we can simulate unitary U if and only if

$$U \in \operatorname{cl}\left\{e^{-iL} : L \in \mathcal{L}(H_1, \ldots, H_k)\right\}, \tag{3.13}$$

where "cl" denotes the closure of a set.[2]

[2]This claim is not true if we omit the closure. For example, consider $H = \left(\begin{smallmatrix} 1 & 0 \\ 0 & \sqrt{2} \end{smallmatrix}\right)$. We can use H to simulate any diagonal 2×2 unitary. However, there are diagonal unitary matrices that are not of the form e^{-iHt} for $t \in \mathbb{R}$. For example, consider $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$.

Proof. First, we show that if we can evolve according to $H_1, \ldots, H_k$, then we can simulate any $U \in \mathrm{cl}\left\{e^{-iL} : L \in \mathcal{L}(H_1, \ldots, H_k)\right\}$. Note that it suffices to show that we can simulate any $U = e^{-iL}$ where $L \in \mathcal{L}(H_1, \ldots, H_k)$. Recall that $\mathcal{L}(H_1, \ldots, H_k)$ was defined in an inductive way, i.e., every $L \in \mathcal{L}(H_1, \ldots, H_k)$ can be obtained from $H_1, \ldots, H_k$ by taking linear combinations and commutators. Thus we consider three cases.

1. We can simulate $U = e^{-iLt}$ for all $t \in \mathbb{R}$ if L is one of $H_1, \ldots, H_k$. Note that simulation for $t < 0$ follows from Claim 1.

2. If we are given simulations of e^{-iAt_1} and e^{-iBt_2} for all $t_1, t_2 \in \mathbb{R}$, then we can simulate $e^{-i(\alpha A + \beta B)}$ for arbitrary $\alpha, \beta \in \mathbb{R}$, since
$$e^{-i(\alpha A+\beta B)} = \lim_{n\to\infty} \left(e^{-i\alpha A/n} e^{-i\beta B/n}\right)^n . \tag{3.14}$$

3. If we are given simulations of e^{-iAt_1} and e^{-iBt_2} for all $t_1, t_2 \in \mathbb{R}$, then we can simulate $e^{-i(i[A,B])t}$ for all $t \in \mathbb{R}$, since
$$e^{-i(i[A,B])t} = e^{[A,B]t} = \lim_{n\to\infty} \left(e^{iA\sqrt{\frac{t}{n}}} e^{-iB\sqrt{\frac{t}{n}}} e^{-iA\sqrt{\frac{t}{n}}} e^{iB\sqrt{\frac{t}{n}}}\right)^n . \tag{3.15}$$

Consult [29] for the proof of (3.14) and (3.15).

Now we proceed to show that, if we can simulate unitary U, then
$$U \in \mathrm{cl}\left\{e^{-iL} : L \in \mathcal{L}(H_1, \ldots, H_k)\right\} .$$

Since we can simulate U (see Definition 9), we can approximate it to any desired precision using expressions of the form
$$e^{-iH_{j_1}t_1} e^{-iH_{j_2}t_2} \ldots e^{-iH_{j_l}t_l} \tag{3.16}$$
for some $l \in \mathbb{N}$, $j_1, \ldots, j_l \in [k]$, and $t_1, \ldots, t_l \geq 0$. Now we will show that all expressions of the above form can be expressed as e^{-iL} for some $L \in \mathcal{L}(H_1, \ldots, H_k)$.

Consider the Baker-Campbell-Hausdorff formula
$$e^{-iAt_1} e^{-iBt_2} = e^{-iH}, \text{ where} \tag{3.17}$$
$$H = At_1 + Bt_2 - \frac{t_1 t_2}{2} i[A,B] + \frac{t_1^2 t_2}{12} i[A, i[A,B]] + \frac{t_1 t_2^2}{12} i[B, i[B,A]] + \ldots . \tag{3.18}$$

See [18] for the proof of Baker-Campbell-Hausdorff formula. Assume $A, B \in \mathcal{L}(H_1, \ldots, H_k)$. In order to claim that $H \in \mathcal{L}(H_1, \ldots, H_k)$, we have to show that it can be expressed as a *finite* real linear combination of nested commutators of $H_1, \ldots, H_k$. Since there is only a finite number of linearly independent nested commutators in expression (3.18), we can rewrite it as a finite real linear combination of these linearly independent nested commutators. Therefore, $H \in \mathcal{L}(H_1, \ldots, H_k)$.

Repeatedly applying the Baker-Campbell-Hausdorff formula to (3.16), we can argue that all expressions of the form (3.16) belong to $\mathcal{L}(H_1, \ldots, H_k)$. This means that there exists a sequence of unitary transformations $\{U_n\}_{n=1}^{\infty}$ such that
$$U = \lim_{n\to\infty} U_n$$

where each $U_i = e^{-iL_i}$ for some $L_i \in \mathcal{L}(H_1, \ldots, H_k)$. Hence,

$$U \in \mathrm{cl}\left\{e^{-iL} : L \in \mathcal{L}(H_1, \ldots, H_k)\right\}. \qquad \square$$

Now we can obtain a simpler and more practical characterization of n-universality than the original one in Definition 10.

Lemma 2. Let $m \leq n$. Then an m-qubit Hamiltonian H is n-universal if

$$\mathcal{L}\left(\left\{P(H \otimes I^{\otimes n-m})P^\dagger : P \in \mathcal{S}_n\right\}\right) = \mathfrak{u}(2^n),$$

where $\mathcal{S}_n$ is the group of matrices that permute n qubits and $\mathfrak{u}(2^n)$ is the set of all $2^n \times 2^n$ Hermitian matrices.

Proof. Let $N := 2^n$ and $\mathcal{L} := \mathcal{L}\left(\left\{P(H \otimes I^{\otimes n-m})P^\dagger : P \in \mathcal{S}_n\right\}\right)$. Since every unitary $U \in \mathrm{U}(N)$ can be expressed as $U = e^{-iL}$ for some $L \in \mathfrak{u}(N) = \mathcal{L}$, then according to Lemma 1 we conclude that it is possible to simulate all of $\mathrm{U}(N)$ by applying H to different ordered subsets of m qubits. Therefore, H is n-universal. $\square$

Corollary 1. A 2-qubit Hamiltonian H is 2-universal if $\mathcal{L}(H, THT) = \mathfrak{u}(4)$, where $\mathfrak{u}(4)$ is the set of all 4×4 Hermitian matrices.

Now we proceed to show that if a Hamiltonian H is n-universal then it is also m-universal for all $m \geq n$. Note that the result is not completely trivial, since the added qubits are not ancillary, i.e., we have to be able to simulate any unitary on *all* of the qubits.

Lemma 3. One can simulate any evolution on n qubits given the ability to evolve according to X, Y, and $X \otimes X$ on any of the qubits.[3]

Proof. For the sake of convenience we omit the tensor product signs in this proof, i.e., we write XX instead of $X \otimes X$.

Recall that any Hermitian matrix can be expressed as a real linear combination of tensor products of Pauli matrices (see Section 2.1.3). Also recall that if we can simulate evolution according to some Hamiltonians then we can also simulate evolution according to any real linear combination of them (see equation (3.14)). Therefore, it suffices to show that the evolution according to any tensor product of Pauli matrices can be simulated.

We also know that given H_1 and H_2 we can approximate evolution according to $i[H_1, H_2]$ (see equation (3.15)). Thus, we can simulate 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 simulate 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. (See Table 3.1 for commutation relations of Pauli matrices).

To show that any evolution on n qubits can be simulated, it is sufficient to show that any tensor product of Pauli matrices can be expressed as a nested commutator

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

	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 3.1: 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.

of weight-2 tensor products of Pauli matrices. This can be done by decomposing a tensor product of Pauli matrices into a sequence of weight-2 tensor products of Pauli matrices so that every two adjacent elements in this sequence anti-commute. □

We now give an example of the above mentioned decomposition of a tensor product of Pauli matrices. Let us Consider a specific tensor product of Pauli matrices, e.g., $XZYXXIZIYZX$ (see Table 3.2). We can break this string down into overlapping sequences of length two: XZ, ZY, YX, XX, ... Then for each adjacent tensor product 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:

$$-\frac{1}{2}i[XXI, IYY] = \frac{1}{2}i[XYI, IXY] = XZY. \tag{3.19}$$

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 the overlapping matrix for each pair of adjacent tensor products 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 3.2.

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 3.2: 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.

Lemma 4. If a Hamiltonian H is n-universal for some $n \geq 2$, then it is also m-universal for all $m \geq n$.

Since H is n-universal for some $n \geq 2$, it can be used to simulate all unitary transformations in $\mathrm{U}(2^m)$ that act non-trivially on no more than two qubits. It is known that any unitary gate on m qubits can be decomposed into gates that act non-trivially only on one or two qubits without the need of ancilla [2, 23]. Therefore, we conclude that H is m-universal.

However, the statement also immediately follows from Lemma 3.

Corollary 2. If a 2-qubit Hamiltonian H is 2-universal, then it is also n-universal for all integers $n \geq 2$.

Chapter 4

Characterization of 2-universal Hamiltonians

In this section we classify 2-qubit Hamiltonians that are *not* 2-universal. Since we will be talking only about 2-universality, we will simply say that a Hamiltonian is universal (instead of "2-universal") or non-universal (instead of "not 2-universal").

4.1 The T gate

The gate that swaps the two qubits is central to our problem of characterizing 2-universal Hamiltonians, since it is the only non-trivial permutation of two qubits. In this section we make a few simple observations revealing some properties of the swap gate that will be relevant to the further discussion. We will use the letter T to refer to the swap gate.

The matrix representation of the T gate is

$$T := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{4.1}$$

It has two eigenspaces, namely

$$E_- := \operatorname{span}_{\mathbb{C}} \{|01\rangle - |10\rangle\} \text{ and } E_+ := \operatorname{span}_{\mathbb{C}} \{|00\rangle, |01\rangle + |10\rangle, |11\rangle\}, \tag{4.2}$$

where E_- corresponds to the eigenvalue -1 and E_+ to the eigenvalue $+1$. We call the normalized vector

$$|s\rangle := \frac{|01\rangle - |10\rangle}{\sqrt{2}} \tag{4.3}$$

that spans E_- the *singlet* state.

Lemma 5. Let N be a normal matrix. The singlet $|s\rangle$ is an eigenvector of N if and only if $[N, T] = 0$.

Proof. Assume $|s\rangle$ is an eigenvector of N. Then $\mathcal{B} = \{|s\rangle, |n_1\rangle, |n_2\rangle, |n_3\rangle\}$ is an orthonormal eigenbasis of N for some orthonormal vectors $\{|n_i\rangle\}_{i=1}^{3} \subset \mathbb{C}^4$. Since $\mathcal{B}$ is orthonormal, $\{|n_i\rangle\}_{i=1}^{3} \in E_-^{\perp} = E_+$. Therefore, $\mathcal{B}$ is also an eigenbasis of T; and both N and T are simultaneously diagonal in this basis. Thus, according to Theorem 1 $[N, T] = 0$.

Conversely, assume $[N, T] = 0$. By Theorem 1 we know that N and T are simultaneously diagonal in some orthonormal basis $\mathcal{B}$. Since $|s\rangle$ spans the one-dimensional eigenspace E_- of T, we know that $e^{i\phi}|s\rangle \in \mathcal{B}$ for some $\phi \in \mathbb{R}$. Thus, $|s\rangle$ is an eigenvector of N. □

Lemma 6. A normal matrix N has a common eigenvector with the T gate if and only if N has an eigenvector orthogonal to $|s\rangle$.

Proof. Assume N shares an eigenvector $|v\rangle$ with the T gate. Then we can assume that either $|v\rangle = |s\rangle$ or $|v\rangle \in E_+$. In the latter case we are done, since every vector in E_+ is orthogonal to $|s\rangle$. In the case when $|v\rangle = |s\rangle$, $E_+ = \mathrm{span}_{\mathbb{C}}(|v\rangle)^{\perp}$ is an invariant subspace for the normal matrix N. Therefore, E_+ contains an eigenvector of N.

The other direction of the statement is obvious. □

Lemma 7. Suppose $U \in \mathrm{U}(4)$ and $[U, T] = 0$. Then the singlet state $|s\rangle$ is an eigenvector of both U and $U^\dagger$.

Proof. Since $[U, T] = 0$, we know that U and T are simultaneously diagonal in some orthonormal basis (see Theorem 1). The singlet $|s\rangle$ must belong to this basis, since it spans the one-dimensional (-1)-eigenspace of the T gate. Therefore, $|s\rangle$ has to be an eigenvector of U as well. Note that U and $U^\dagger$ have the same eigenvectors. Thus, $|s\rangle$ is also an eigenvector of $U^\dagger$. □

4.2 Examples of non-universal Hamiltonians

In this section we will consider three families of non-universal Hamiltonians. Later on we will see that these three families capture the essence of what makes a Hamiltonian non-universal.

- *Consider a local Hamiltonian $H = H_1 \otimes I + I \otimes H_2$.* Note that we end up acting independently on both qubits no matter whether we evolve our system according to H or THT, since

  $$THT = I \otimes H_1 + H_2 \otimes I.$$

  Therefore, any sequence of evolutions according to H and THT will result in action that is independent on both qubits and we will not be able to simulate entangling operations.

- *Consider a Hamiltonian H that shares an eigenvector v with the gate that swaps two qubits, T.* In this case any sequence of evolutions according to H and THT will leave the vector v unchanged. Therefore, we will not be able to simulate unitary transformations that act non-trivially on this vector.

- *Consider a traceless Hamiltonian H.* Since the trace is basis independent, also $\mathrm{Tr}(THT) = 0$. Now note that by exponentiating a traceless Hamiltonian we get a unitary with determinant one. Any sequence of evolutions according to H and THT corresponds to a product of unitary matrices from the special unitary group. This shows that using a traceless Hamiltonian we will not be able to simulate anything outside the special unitary group. Even though traceless Hamiltonians are not universal according to the Definition 10, for many applications it suffices to simulate only special unitary group.

We summarize the observations made above in the following lemma.

Lemma 8. A two-qubit Hamiltonian H is non-universal if any of the following conditions holds:

1. H is a local Hamiltonian, i.e., $H = H_1 \otimes I + I \otimes H_2$, for some 1-qubit Hamiltonians H_1, H_2,

2. H shares an eigenvector with the T gate,

3. $\mathrm{Tr}(H) = 0$.

The converse of the above lemma is not true. However, in the following sections we will generalize the first condition (see Lemma 10). Then we will be able to show that the converse of the generalized lemma holds as well, i.e., if a Hamiltonian does not fall in any of the three categories then it is universal.

4.3 Transformations preserving universality

In this section we look for unitary transformations that conjugate all universal two-qubit Hamiltonians to universal ones and all non-universal two-qubit Hamiltonians to non-universal ones. We say that such transformations *preserve the universality*.

Let us recall when two matrices are said to be similar.

Definition 14. Matrices A and B are said to be *similar* if there exists an invertible matrix P such that $B = PAP^{-1}$.

Now we are ready to introduce the notion of T-similarity.

Definition 15. Matrices A and B are said to be *T-similar* if there exists a unitary matrix P such that $B = PAP^{\dagger}$ and $[P, T] = 0$.

Note that in the case of T-similarity we require the transformation P ensuring the similarity to be unitary instead of just invertible.

Theorem 2. Let A, B be T-similar 2-qubit Hamiltonians. Then A is universal if and only if B is.

Proof. Assume 2-qubit Hamiltonians A and B are T-similar. So there is $P \in \mathrm{U}(4)$ such that $B = PAP^\dagger$ and $[P, T] = 0$. Suppose A is universal. We want to show that B is also universal. We have to show that using B we can simulate every $U \in \mathrm{U}(4)$ with any desired precision. Pick arbitrary $U \in \mathrm{U}(4)$ and precision $\varepsilon > 0$. Since A is universal, we can simulate $P^\dagger U P \in \mathrm{U}(4)$ with precision ε, i.e., there exists $n \in \mathbb{N}$ and $t_1, \ldots, t_n \geq 0$ such that

$$\left\| P^\dagger U P - e^{-iAt_1} e^{-iTATt_2} e^{-iAt_3} \ldots e^{-iTATt_n} \right\|_\infty < \varepsilon. \tag{4.4}$$

Since $TP = PT$, we have

$$\begin{aligned} & e^{-iBt_1} e^{-iTBTt_2} e^{-iBt_3} \ldots e^{-iTBTt_n} \\ &= e^{-iPAP^\dagger t_1} e^{-iTPAP^\dagger Tt_2} e^{-iPAP^\dagger t_3} \ldots e^{-iTPAP^\dagger Tt_n} \\ &= e^{-iPAP^\dagger t_1} e^{-iPTATP^\dagger t_2} e^{-iPAP^\dagger t_3} \ldots e^{-iPTATP^\dagger t_n} \\ &= Pe^{-iAt_1} P^\dagger P e^{-iTATt_2} P^\dagger P e^{-iAt_3} P^\dagger \ldots P e^{-iTATt_n} P^\dagger \\ &= Pe^{-iAt_1} e^{-iTATt_2} e^{-iAt_3} \ldots e^{-iTATt_n} P^\dagger. \end{aligned} \tag{4.5}$$

By combining (4.4) with (4.5) and noting that the spectral norm of an operator is invariant under unitary conjugation, we get

$$\begin{aligned} & \left\| U - e^{-iBt_1} e^{-iTBTt_2} e^{-iBt_3} \ldots e^{-iTBTt_n} \right\|_\infty \\ &= \left\| U - Pe^{-iAt_1} e^{-iTATt_2} e^{-iAt_3} \ldots e^{-iTATt_n} P^\dagger \right\|_\infty \\ &= \left\| P^\dagger U P - e^{-iAt_1} e^{-iTATt_2} e^{-iAt_3} \ldots e^{-iTATt_n} \right\|_\infty < \varepsilon. \end{aligned}$$

Hence, $e^{-iBt_1} e^{-iTBTt_2} e^{-iBt_3} \ldots e^{-iTBTt_n}$ is the desired simulation of U with precision ε. We conclude that B is universal and the theorem follows. $\square$

Now with our new tool in hand we can return to Lemma 8 and try to generalize it using Theorem 2. We can conjugate all three classes of Hamiltonians in Lemma 8 by unitary transformations commuting with the T gate and see if we get any new non-universal Hamiltonians.

Let us first consider the local Hamiltonians (condition 1 in Lemma 8). It turns out that by conjugating local Hamiltonians with unitary transformations that commute with T it is possible to obtain non-universal Hamiltonians that are not mentioned in Lemma 8. For example, consider the following local Hamiltonian H and unitary U which commutes with T:

$$H := \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \otimes I + I \otimes \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad U := \begin{pmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{1}{\sqrt{2}} \end{pmatrix}$$

By conjugating the local Hamiltonian H by unitary U, we obtain a non-universal Hamiltonian that is not local:

$$UHU^\dagger = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} = I \otimes I + \frac{1}{2}(X \otimes X - Y \otimes Y)$$

Thus, we conclude that local Hamiltonians are not closed under conjugation by unitary transformations that commute with the T gate.

We will see that the other two families of non-universal Hamiltonians mentioned in conditions 2 and 3 of Lemma 8 are closed under conjugation by unitary transformations that commute with the T gate. It is very easy to see this in the case of traceless Hamiltonians (condition 3). Since the trace is basis independent, traceless Hamiltonians are closed under conjugation. In the following lemma we prove that also the set of Hamiltonians satisfying condition 2 is closed under conjugation by unitary transformations that commute with T.

Lemma 9. The set of two-qubit Hamiltonians sharing an eigenvector with the T gate is closed under conjugation with unitary transformations that commute with T.

Proof. Let U satisfy $[U, T] = 0$ and let $|v\rangle$ be the eigenvector shared by H and the T gate, i.e., $H|v\rangle = \lambda_H |v\rangle$ and $T|v\rangle = \lambda_T |v\rangle$ for some λ_H, λ_T. We will show that $U|v\rangle$ is an eigenvector shared by the T gate and $UHU^\dagger$. First, note that $UHU^\dagger(U|v\rangle) = UH|v\rangle = \lambda_H U|v\rangle$. We also have $T(U|v\rangle) = UT|v\rangle = \lambda_T U|v\rangle$. Thus, $U|v\rangle$ is an eigenvector shared by the T gate and $UHU^\dagger$. □

Note that in the proof we did not make use of the fact that the T gate is the unitary that swaps two qubits. Therefore, the above lemma holds for an arbitrary matrix T.

The following lemma is a generalization of Lemma 8. It follows directly from the discussion above and Lemma 9.

Lemma 10. A two-qubit Hamiltonian H is non-universal if any of the following conditions holds:

1. H is T-similar to a local Hamiltonian,

2. H shares an eigenvector with the T gate,

3. $\mathrm{Tr}(H) = 0$.

Imagine that we want to determine if a given Hamiltonian is not universal. The best we could do at this point would be to check whether it falls into any of the families that are listed as non-universal in Lemma 10. However, it is not straightforward how to check if a given Hamiltonian is T-similar to a local Hamiltonian (condition 1). Thus, in the next section we introduce a new notion that will turn out to be useful in checking condition 1 in the above lemma.

4.4 Patterns

In this section we introduce the notion of a *pattern* of a Hamiltonian. Patterns will enable us to efficiently check whether a given Hamiltonian is T-similar to a local one (condition 1 in Lemma 10), which is the main goal of this section.

We first define a pattern of a Hamiltonian. Then in Section 4.4.1 we formalize the notion of a pattern for Hamiltonians with repeated eigenvalues and characterize the patterns of such Hamiltonians. In section 4.4.2 we show that Hamiltonians have the same pattern if and only if they are T-similar (see Theorem 3). Finally, in Section 4.4.3 we characterize the set of Hamiltonians that are T-similar to the local ones in terms of their patterns (see Theorem 4). This characterization allows us to efficiently check whether a given Hamiltonian is T-similar to a local one. In Section 4.4.3 we also give one more characterization of the set of Hamiltonians that are T-similar to the local ones (see Theorem 5).

Definition 16. Assume that a two-qubit Hamiltonian H has eigenvalues λ_i with corresponding orthonormal eigenvectors $|\psi_i\rangle$. Then we define a *pattern* of H to be

$$\begin{Bmatrix} \lambda_1 & \lambda_2 & \lambda_3 & \lambda_4 \\ s_1 & s_2 & s_3 & s_4 \end{Bmatrix}, \tag{4.6}$$

where $s_i := |\langle s|\psi_i\rangle|^2$ and $|s\rangle$ is the singlet state as given in (4.3). Note that a pattern is defined up to a permutation of the columns.

One could wonder why we use the state $|s\rangle$ for calculating the overlaps. Recall that the T gate has only two eigenspaces, E_+ and E_- (4.2), and E_- is spanned by $|s\rangle$. Therefore, the overlap with the singlet state completely determines the overlap with the (+1)-eigenspace E_+.

4.4.1 Patterns of degenerate Hamiltonians

Definition 17. We say that a Hamiltonian H is *degenerate* if it has a degenerate (i.e., repeated) eigenvalue. We say that H is *non-degenerate* if it does not have repeated eigenvlaues.

Note that the pattern is unique up to permutation of columns for non-degenerate Hamiltonians. It is not so for degenerate ones. This is because one can choose any orthonormal eigenbasis of the subspace corresponding to the degenerate eigenvalue. This choice affects the corresponding overlaps with the singlet state.

It turns out that for the purpose of characterizing universal Hamiltonians, we could restrict our attention only to non-degenerate Hamiltonians, since the following Lemma says that all degenerate Hamiltonians are non-universal.

Lemma 11. If a 2-qubit Hamiltonian H has a degenerate eigenvalue, then it is not universal.

Proof. Assume H has a degenerate eigenvalue. Then the eigenspace E corresponding to the degenerate eigenvalue has dimension at least two. Recall that the T gate has a 3-dimensional $(+1)$-eigenspace E_+. Now note that the intersection $E \cap E_+$ is at least 1-dimensional, since $E, E_+ \subseteq \mathbb{C}^4$ and $\dim(E) \geq 2$, $\dim(E_+) = 3$. Any nonzero $|v\rangle \in E \cap E_+$ is a common eigenvector of H and the T gate. By Lemma 8 we conclude that H is non-universal. $\square$

Due to the above lemma we could restrict attention to non-degenerate Hamiltonians and avoid dealing with patterns that are not well-defined. However, we will take a more general approach and prove all theorems for general (possibly degenerate) Hamiltonians. If H is degenerate, every symbol of the form (4.6) that fulfills the requirements posed in Definition 16 is considered to be a pattern of H.

We proceed to characterize the different patterns of the same (degenerate) Hamiltonian. The following lemma shows that for degenerate Hamiltonians, patterns are defined up to a way we choose to split up the sum of the overlaps corresponding to the degenerate eigenvalue.

Lemma 12. Let H be a degenerate Hamiltonian with a degenerate eigenvalue λ_1. Let E be the k-dimensional eigenspace corresponding to the degenerate eigenvalue λ_1, where $2 \leq k \leq 4$. Then (up to a permutation of columns) H has all patterns of the form

$$\begin{Bmatrix} \lambda_1 & \lambda_2 & \lambda_3 & \lambda_4 \\ s_1 & s_2 & s_3 & s_4 \end{Bmatrix}, \tag{4.7}$$

where $\lambda_1 = \lambda_2 = \ldots = \lambda_k$, $s_1 + s_2 + \ldots + s_k = \|\Pi_E |s\rangle\|^2$, and Π_E is the projection onto the eigenspace E.

Proof. Let $s_1, \ldots, s_k$ be given. Pick an arbitrary orthonormal basis $\{|e_1\rangle, \ldots, |e_k\rangle\}$ of E. Let U be any unitary transformation that sends $\Pi_E |s\rangle$ to $\sqrt{s_1}\,|e_1\rangle + \sqrt{s_2}\,|e_2\rangle + \ldots + \sqrt{s_k}\,|e_k\rangle$ and acts trivially on $E^\perp$. Since $\langle e_i| (I - \Pi_E) |s\rangle = 0$ and

$$\begin{aligned} U|s\rangle &= U(I - \Pi_E)|s\rangle + U(\Pi_E|s\rangle) && (4.8)\\ &= (I - \Pi_E)|s\rangle + (\sqrt{s_1}\,|e_1\rangle + \sqrt{s_2}\,|e_2\rangle + \ldots + \sqrt{s_k}\,|e_k\rangle), && (4.9) \end{aligned}$$

we have

$$\left|\langle s| U^\dagger |e_i\rangle\right|^2 = \left|(U|s\rangle)^\dagger |e_i\rangle\right|^2 = s_i. \tag{4.10}$$

This tells us that $\left\{U^\dagger |e_1\rangle, U^\dagger |e_2\rangle, \ldots, U^\dagger |e_k\rangle\right\}$ is an orthonormal basis of E that gives rise to the pattern of the desired form (4.7). $\square$

Corollary 3. Suppose degenerate Hamiltonians H_1 and H_2 both have a common pattern p. Then all patterns of H_1 are also patterns of H_2 and vice versa.

4.4.2 T-similarity and patterns

In this section we characterize T-similar Hamiltonians in terms of their patterns. This characterization will help to prove a theorem that gives an efficiently checkable necessary and sufficient condition for a given Hamiltonian to be T-similar to a local one.

Definition 18. We say that Hamiltonians H_1 and H_2 have the *same pattern* if H_1 and H_2 share some common pattern[1].

Theorem 3. Hamiltonians H_1 and H_2 are T-similar if and only if they have the same pattern.

Proof. Assume H_1 and H_2 are T-similar, i.e., $H_2 = UH_1U^\dagger$ for some $U \in \mathrm{U}(4)$ such that $[U,T]=0$. We want to show that H_1 and $UH_1U^\dagger$ have the same pattern. Since $[U,T]=0$, by Lemma 7 we know that $|s\rangle$ is an eigenvector of $U^\dagger$. Let $|v\rangle$ be an eigenvector of H_1. Then $U|v\rangle$ is the corresponding eigenvector of $UH_1U^\dagger$. Now we have $|\langle s|(U|v\rangle)| = \left|(U^\dagger|s\rangle)^\dagger|v\rangle\right| = |\langle s|v\rangle|$, i.e., the corresponding eigenvectors of H_1 and $UH_1U^\dagger$ have the same overlaps with the singlet state. Since conjugation does not change the eigenvalues, we have shown that the patterns of H_1 and $H_2 = UH_1U^\dagger$ are the same.

Conversely, assume that H_1 and H_2 have a pattern p. Let φ_j be the eigenvalues of H_1 and H_2, and let $|v_j\rangle$, $|w_j\rangle$ be the corresponding eigenvectors that give rise to the pattern p. Let $r_j := |\langle s|v_j\rangle| = |\langle s|w_j\rangle|$. We can express the singlet state $|s\rangle$ in the eigenbases of H_1 and H_2 as follows:

$$|s\rangle = \sum_{j=1}^{4} r_j e^{i\alpha_j}|v_j\rangle, \tag{4.11}$$

$$|s\rangle = \sum_{j=1}^{4} r_j e^{i\beta_j}|w_j\rangle, \tag{4.12}$$

where $\alpha_j, \beta_j \in \mathbb{R}$. Now let

$$U := \sum_{j=1}^{4} e^{i(\beta_j-\alpha_j)}|w_j\rangle\langle v_j|. \tag{4.13}$$

We claim that (a) $UH_1U^\dagger = H_2$, (b) $|\langle s|U|s\rangle| = 1$.

(a) By expressing U as in (4.13) and recalling that $|v_j\rangle$ and $|w_j\rangle$ are the eigenvectors of H_1 and H_2, respectively, we get

$$\begin{aligned} UH_1U^\dagger &= \sum_{j=1}^{4} e^{i(\beta_j-\alpha_j)}|w_j\rangle\langle v_j| \sum_{k=1}^{4}\varphi_k|v_k\rangle\langle v_k| \sum_{l=1}^{4} e^{-i(\beta_l-\alpha_l)}|v_l\rangle\langle w_l| \\ &= \sum_{k=1}^{4} e^{i(\beta_k-\alpha_k)}\varphi_k e^{-i(\beta_k-\alpha_k)}|w_k\rangle\langle w_k| \\ &= \sum_{k=1}^{4}\varphi_k|w_k\rangle\langle w_k| = H_2. \end{aligned}$$

[1] According to Corollary 3, in such a case every pattern of H_1 is also a pattern of H_2 and vice versa.

(b) By expressing $\langle s|$ as in (4.12), $|s\rangle$ as in (4.11) and U as in (4.13), we get

$$\begin{aligned}\langle s| U |s\rangle &= \sum_{j=1}^{4} r_j e^{-i\beta_j} \langle w_j| \sum_{k=1}^{4} e^{i(\beta_k-\alpha_k)} |w_k\rangle \langle v_k| \sum_{l=1}^{4} r_l e^{i\alpha_l} |v_l\rangle \\ &= \sum_{k=1}^{4} r_k e^{-i\beta_k} e^{i(\beta_k-\alpha_k)} r_k e^{i\alpha_k} = \sum_{k=1}^{4} r_k^2 = 1.\end{aligned}$$

Part (a) tells us that H_1 and H_2 are similar via U. From (b) it follows that $|s\rangle$ is an eigenvector of U. Thus, according to Lemma 5, U commutes with T. Hence, H_1 and H_2 are T-similar. □

4.4.3 Patterns of local Hamiltonians

We are now ready to prove the main theorem of this section, which will allow us to check easily whether a given Hamiltonian is T-similar to a local one. Thus, we will be able to efficiently determine whether a given Hamiltonian falls into any of three families of non-universal Hamiltonians listed in Lemma 10.

Theorem 4. A two-qubit Hamiltonian H is T-similar to a local Hamiltonian if and only if it has a pattern of the form

$$\begin{Bmatrix} \lambda_{11} & \lambda_{12} & \lambda_{21} & \lambda_{22} \\ s & t & t & s \end{Bmatrix}, \text{ where } \lambda_{11} + \lambda_{22} = \lambda_{12} + \lambda_{21}. \tag{4.14}$$

Proof. Assume H is T-similar to some local Hamiltonian $H' = H_1 \otimes I + I \otimes H_2$. According to Theorem 3, H and H' have the same pattern. Thus, in order to show that H has a pattern of the form (4.14), it suffices to prove that H' has the required pattern.

First, let us diagonalize H_1 and H_2:

$$H_1 = \alpha_1 |v_1\rangle \langle v_1| + \alpha_2 |v_2\rangle \langle v_2|, \quad H_2 = \beta_1 |w_1\rangle \langle w_1| + \beta_2 |w_2\rangle \langle w_2|. \tag{4.15}$$

Let the first eigenvectors of H_1 and H_2 be

$$|v_1\rangle = \begin{pmatrix} a \\ b \end{pmatrix}, \quad |w_1\rangle = \begin{pmatrix} c \\ d \end{pmatrix}. \tag{4.16}$$

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

$$|v_2\rangle = \begin{pmatrix} -b^* \\ a^* \end{pmatrix}, \quad |w_2\rangle = \begin{pmatrix} -d^* \\ c^* \end{pmatrix}. \tag{4.17}$$

Then

$$|v_1\rangle \otimes |w_1\rangle, \quad |v_1\rangle \otimes |w_2\rangle, \quad |v_2\rangle \otimes |w_1\rangle, \quad |v_2\rangle \otimes |w_2\rangle \tag{4.18}$$

are eigenvectors of H'. If we calculate the overlaps with $|s\rangle$, we get

$$|\langle s|v_1, w_1\rangle|^2 = \tfrac{1}{2}\,|ad - bc|^2 =: s, \tag{4.19}$$
$$|\langle s|v_1, w_2\rangle|^2 = \tfrac{1}{2}\,|ac^* + bd^*|^2 =: t, \tag{4.20}$$
$$|\langle s|v_2, w_1\rangle|^2 = \tfrac{1}{2}\,|-a^*c - b^*d|^2 = \tfrac{1}{2}\,|ac^* + bd^*|^2 = t, \tag{4.21}$$
$$|\langle s|v_2, w_2\rangle|^2 = \tfrac{1}{2}\,|a^*d^* - b^*c^*|^2 = \tfrac{1}{2}\,|ad - bc|^2 = s. \tag{4.22}$$

The eigenvalues corresponding to vectors in (4.18) are

$$\lambda_{11} = \alpha_1 + \beta_1, \quad \lambda_{12} = \alpha_1 + \beta_2, \quad \lambda_{21} = \alpha_2 + \beta_1, \quad \lambda_{22} = \alpha_2 + \beta_2 \tag{4.23}$$

and they satisfy $\lambda_{11} + \lambda_{22} = \lambda_{12} + \lambda_{21}$. So we conclude that H' has a pattern of the form (4.14).

Now let us prove the other direction. We want to show that for any H that has a pattern of the form (4.14) we can find a local Hamiltonian H' such that H and H' are T-similar. By Theorem 3 we know that if H and H' have the same pattern, then they are T-similar. Therefore, it suffices to show that we can construct a local Hamiltonian $H' = H_1 \otimes I + I \otimes H_2$ with any given pattern of the form (4.14).

As before, we use α_i and $|v_i\rangle$ to refer to corresponding eigenvalues and eigenvectors of H_1. Similarly, we use β_i and $|w_i\rangle$ for H_2. First, given λ_{ij} from (4.14), we choose the eigenvalues of H_1 and H_2 as follows: $\alpha_1 = 0$, $\alpha_2 = \lambda_{21} - \lambda_{11}$, $\beta_1 = \lambda_{11}$, and $\beta_2 = \lambda_{12}$. Note that after this choice the eigenvalues of H' are

$$\alpha_1 + \beta_1 = \lambda_{11}, \quad \alpha_1 + \beta_2 = \lambda_{12}, \quad \alpha_2 + \beta_1 = \lambda_{21}, \quad \alpha_2 + \beta_2 = \lambda_{22}, \tag{4.24}$$

where the last equality holds since $\lambda_{11}+\lambda_{22} = \lambda_{12}+\lambda_{21}$. Then we have to choose the corresponding eigenvectors of H_1 and H_2 so that they have the required overlaps. It suffices to make the right choice just for $|v_1\rangle$ and $|w_1\rangle$, since they completely determine the overlaps. 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 $|v_1\rangle = \left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right)$ and $|w_1\rangle = \left(\begin{smallmatrix} c \\ d \end{smallmatrix}\right)$ is θ, then $ad - bc = \sin\theta$ (pseudo-scalar product) and $ac + bd = \cos\theta$ (scalar product). Thus, the overlaps (4.19) and (4.20) become $\frac{1}{2}\sin^2\theta = s$ and $\frac{1}{2}\cos^2\theta = t$, respectively (recall that $2s + 2t = 1$). So we can take any two real unit vectors having angle

$$\theta = \arcsin\sqrt{2s}. \tag{4.25}$$

□

We now give yet another characterization of the set of Hamiltonians that are T-similar to the local ones.

Definition 19. We say that H is an *antisymmetric Hamiltonian* if $H = H^\dagger$ (H is Hermitian) and $H^T = -H$ (H is antisymmetric).

If H is an antisymmetric Hamiltonian, then $H^* = -H$. This means that all entries of H are purely imaginary. In fact, two-qubit antisymmetric Hamiltonians correspond exactly to real linear combinations of Pauli basis elements containing exactly one Y, i.e., $\mathrm{span}_{\mathbb{R}}\{I \otimes Y, X \otimes Y, Z \otimes Y, Y \otimes I, Y \otimes X, Y \otimes Z\}$.

Note that if H is an antisymmetric Hamiltonian, then e^{-iHt} and e^{-iTHTt} are real matrices for all $t \geq 0$. This can easily be seen by considering the Taylor expansion of e^x. Also note that $\det(e^{-iHt}) = e^{-i\,\mathrm{Tr}(H)t} = 1$. Therefore, we can simulate only some subset of $\mathrm{SO}(4)$ using H, so H is clearly non-universal. Moreover, even $rI+H$ is non-universal for all $r \in \mathbb{R}$. This is because $e^{-i(rI+H)t} = e^{-irt}e^{-iHt}$ and so every unitary that can be simulated is of the form $e^{i\varphi}O$, where $O \in \mathrm{SO}(4)$ and $\varphi \in \mathbb{R}$. Now by Theorem 2 we conclude that all Hamiltonians that are T-similar to $rI+H$ are non-universal as well.

However, it turns out that we don't need to add any new family of non-universal Hamiltonians to the list in Lemma 10. The following theorem tells us that the above family of non-universal Hamiltonians coincides with the family of Hamiltonians T-similar to some local Hamiltonian (the first item in Lemma 10).

Theorem 5. Let H be a two-qubit Hamiltonian. Then the following are equivalent:

(1) H is T-similar to a local Hamiltonian,

(2) H has pattern of the form (4.14), and

(3) H is T-similar to $rI+A$ for some $r \in \mathbb{R}$ and some antisymmetric Hamiltonian A.

Proof. From Theorem 4 we know that (1) and (2) are equivalent. We will show that (2) and (3) are equivalent.

Assume (2) holds. Theorem 3 tells us that T-similar matrices have the same overlaps with $|s\rangle$. Therefore, it suffices to show that given a pattern

$$p = \begin{Bmatrix} \lambda_{11} & \lambda_{12} & \lambda_{21} & \lambda_{22} \\ s & \frac{1-2s}{2} & \frac{1-2s}{2} & s \end{Bmatrix}, \text{ with } \lambda_{11} + \lambda_{22} = \lambda_{12} + \lambda_{21} \tag{4.26}$$

it is possible to choose $r \in \mathbb{R}$ and an antisymmetric Hamiltonian A so that $rI + A$ has pattern p. First, take $r := \frac{1}{2}(\lambda_{11} + \lambda_{22})$. Now let

$$A' := \begin{pmatrix} \varphi_1 & 0 \\ 0 & \varphi_2 \end{pmatrix} \otimes \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}. \tag{4.27}$$

where $\varphi_1 := \lambda_{11} - r$ and $\varphi_2 := \lambda_{12} - r$. The eigenvalues of A' are $\varphi_1, \varphi_2, -\varphi_2, -\varphi_1$ with the corresponding eigenvectors

$$\begin{aligned} |v'_{11}\rangle &:= \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}, \quad |v'_{12}\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}, \\ |v'_{21}\rangle &:= \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix}, \quad |v'_{22}\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix}. \end{aligned} \tag{4.28}$$

Note that the eigenvalues of $rI + A'$ are $\lambda_{11}, \lambda_{12}, \lambda_{21}, \lambda_{22}$ with corresponding eigenvectors $|v'_{ij}\rangle$ as in (4.28). So the matrix $rI + A'$ has the correct eigenvalues but not necessarily the correct overlaps. Thus, we conjugate $rI + A'$ with an orthogonal matrix

$$O := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta & 0 \\ 0 & \sin\theta & \cos\theta & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{4.29}$$

to get a matrix A with eigenvectors that give rise to the desired overlaps. Consider the following eigenbasis of $A := O(rI + A')O^\dagger$:

$$\begin{aligned} |v_{11}\rangle &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i\cos\theta \\ i\sin\theta \\ 0 \end{pmatrix}, |v_{12}\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ -\sin\theta \\ \cos\theta \\ i \end{pmatrix}, \\ |v_{21}\rangle &= \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ -\sin\theta \\ \cos\theta \\ -i \end{pmatrix}, |v_{22}\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i\cos\theta \\ -i\sin\theta \\ 0 \end{pmatrix}, \end{aligned} \tag{4.30}$$

where $|v_{ij}\rangle = O\left|v'_{ij}\right\rangle$ corresponds to the eigenvalue λ_{ij}. The overlaps of these eigenvectors are

$$|\langle s|v_{11}\rangle|^2 = |\langle s|v_{22}\rangle|^2 = \frac{1}{4}(\cos\theta - \sin\theta)^2 = \frac{1-\sin(2\theta)}{4} \tag{4.31}$$

$$|\langle s|v_{21}\rangle|^2 = |\langle s|v_{21}\rangle|^2 = \frac{1}{4}(\cos\theta + \sin\theta)^2 = \frac{1+\sin(2\theta)}{4}. \tag{4.32}$$

Therefore, if we choose $\theta := \frac{1}{2}\arcsin(1-4s)$, we get overlap s in (4.31) and $\frac{1-2s}{2}$ in (4.32). So we have constructed a matrix $A = O(rI + A')O^\dagger = rI + OA'O^\dagger$ that has pattern p. Note that $OA'O^\dagger$ is indeed an antisymmetric Hamiltonian, since $(OA'O^\dagger)^\dagger = OA'O^\dagger$ and $(OA'O^\dagger)^* = -OA'O^\dagger$ as A' is an antisymmetric Hamiltonian and O is an orthogonal matrix.

We proceed to show the other direction. Assume (3) holds. Again, due to Theorem 3, it suffices to show that $rI+A$ has a pattern of the form (4.14). Assume A has an eigenvector $|v\rangle$ with eigenvalue λ. Since A is an antisymmetric Hamiltonian,

$$A\,|v^*\rangle = -(A\,|v\rangle)^* = -(\lambda\,|v\rangle)^* = -\lambda\,|v^*\rangle\,,$$

where $|v^*\rangle$ is obtained from $|v\rangle$ by taking the complex conjugate of each of its components. So A also has an eigenvector $|v^*\rangle$ with eigenvalue $-\lambda$.

We consider two cases, when A has only non-zero eigenvalues and when it has 0 as an eigenvalue.

- Assume A has only non-zero eigenvalues. Then $rI+A$ has eigenvalues $r+\lambda_1$, $r-\lambda_1$, $r+\lambda_2, r-\lambda_2$ with corresponding eigenvectors $|v_1\rangle, |v_1^*\rangle, |v_2\rangle, |v_2^*\rangle$. Since the singlet is a real vector, we have $|\langle s|v_i\rangle|^2 = |\langle s|v_i^*\rangle|^2$. So $rI+A$ has a pattern

$$p = \begin{Bmatrix} r+\lambda_1 & r+\lambda_2 & r-\lambda_2 & r-\lambda_1 \\ s & \frac{1-2s}{2} & \frac{1-2s}{2} & s \end{Bmatrix}, \tag{4.33}$$

where $s := |\langle s|v_1\rangle|^2$. Note that $(r+\lambda_1)+(r-\lambda_1) = 2r = (r+\lambda_2)+(r-\lambda_2)$. Therefore, p is of the desired form (4.14).

- Assume A has eigenvalue 0. If $A = 0$, then $rI + A = rI$. Since all eigenvalues of rI are the same, according to Lemma 12, we can choose an eigenbasis of rI to obtain any desired overlaps. For instance, $rI + A$ has a pattern

$$p = \begin{Bmatrix} r & r & r & r \\ \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} \end{Bmatrix}, \tag{4.34}$$

  which is of the form (4.14).

  Now assume $A \neq 0$. Then A has non-zero eigenvalues $\pm\lambda$ with corresponding eigenvectors $|v\rangle$ and $|v^*\rangle$. Thus, the eigenvalue 0 has multiplicity 2. Accordingly, $rI + A$ has eigenvalues $r \pm \lambda$ with corresponding eigenvectors $|v\rangle$ and $|v^*\rangle$ and eigenvalue r with multiplicity 2. According to Lemma 12, we can choose two orthonormal eigenvectors in the r-eigenspace so that they have the same overlaps with $|s\rangle$. Therefore, $rI + A$ has a pattern

$$p = \begin{Bmatrix} r+\lambda & r & r & r-\lambda \\ s & \frac{1-2s}{2} & \frac{1-2s}{2} & s \end{Bmatrix}, \tag{4.35}$$

  where $s := |\langle s|v\rangle|^2 = |\langle s|v^*\rangle|^2$. It remains to note that the pattern p is of the desired form (4.14).

$\square$

4.5 Proving the converse

In this section we show that the list of non-universal families of Hamiltonians in Lemma 10 is in fact complete. That is, we prove that any two-qubit Hamiltonian that does not fall in any of the three categories in Lemma 10 is universal.

In this section we often work in a basis where the T gate is diagonal and the singlet state is the first basis vector. There are infinitely many choices for the other three basis vectors. It does not matter which choice we make as long as we fix it. We make a particular choice and call this basis the *T-basis*. We use $\tilde{T}$ and $|\tilde{s}\rangle$ to denote the T gate and the singlet state in the T-basis, i.e.,

$$\tilde{T} := \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \text{ and } |\tilde{s}\rangle := \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}. \tag{4.36}$$

We use U_T to denote the unitary implementing the basis change from the standard basis to the T-basis. In particular, $\tilde{T} = U_T T U_T^\dagger$ and $|\tilde{s}\rangle = U_T |s\rangle$.

4.5.1 Tridiagonal form

We start by introducing a normal form for 2-qubit Hamiltonians.

Definition 20. We say that a 2-qubit Hamiltonian Ξ is in the *tridiagonal form* if it is of the form

$$\begin{pmatrix} a & b & 0 & 0 \\ b & c & d & 0 \\ 0 & d & e & f \\ 0 & 0 & f & g \end{pmatrix}, \tag{4.37}$$

where $a, b, c, d, e, f, g \in \mathbb{R}$ and $b, d, f \geq 0$. In the case when either of b, d is 0, we additionally require that

- if $b = 0$, then $d = f = 0$ and $c \geq e \geq g$,
- if $d = 0$, then $f = 0$ and $e \geq g$.

Note that a tridiagonal Hamiltonian Ξ is of one of the following types:

$$\underset{\text{Type 1}}{\begin{pmatrix} * & + & 0 & 0 \\ + & * & + & 0 \\ 0 & + & * & + \\ 0 & 0 & + & * \end{pmatrix}} \quad \underset{\text{Type 2}}{\begin{pmatrix} * & + & 0 & 0 \\ + & * & + & 0 \\ 0 & + & * & 0 \\ 0 & 0 & 0 & * \end{pmatrix}} \quad \underset{\text{Type 3}}{\begin{pmatrix} * & + & 0 & 0 \\ + & * & 0 & 0 \\ 0 & 0 & *_1 & 0 \\ 0 & 0 & 0 & *_2 \end{pmatrix}} \quad \underset{\text{Type 4}}{\begin{pmatrix} * & 0 & 0 & 0 \\ 0 & *_1 & 0 & 0 \\ 0 & 0 & *_2 & 0 \\ 0 & 0 & 0 & *_3 \end{pmatrix}}$$

where $*_1 \geq *_2 \geq *_3$ and "+" stands for a positive entry and "$*$" for any real entry.

When given a 2-qubit Hamiltonian Ξ in the tridiagonal form, we will often use letters a, b, c, d, e, f, g to refer to its entries as indicated in equation (4.37).

Definition 21. Let H be a 2-qubit Hamiltonian given in the standard basis. We say that Ξ *is the tridiagonal form of* H if the following two requirements are met:

1. Ξ is in the tridiagonal form,
2. H and $U_T^\dagger \Xi U_T$ are T-similar,

where U_T implements the basis change from the standard basis to the T-basis.

If H is a 2-qubit Hamiltonian in the standard basis, then its tridiagonal form Ξ is in fact the same Hamiltonian expressed in some basis that diagonalizes the T gate. The following Lemma says that it is always possible to find a basis in which both the T gate is diagonal and the Hamiltonian H is tridiagonal. This basis depends on the Hamiltonian we are considering. However, $|s\rangle$ will always be the first basis vector in this basis, independently on the Hamiltonian considered. Hence, in this basis $|s\rangle$ and the T gate will assume the form of $|\tilde{s}\rangle$ and $\tilde{T}$, respectively.

Lemma 13. Every 2-qubit Hamiltonian H has a unique tridiagonal form Ξ.

Proof. We start by showing that for every H there *exists* a tridiagonal form Ξ. Note that condition 2 in Definition 21 is equivalent to saying that $U_T H U_T^\dagger$ is T-similar to Ξ. Now we are working in the T-basis. Therefore, matrices A and B are considered to be T-similar if $B = UAU^\dagger$, where $[U, \tilde{T}] = 0$. We let $\tilde{H} := U_T H U_T^\dagger$ and proceed to show how to tridiagonalize $\tilde{H}$ by conjugating it with matrices that commute with $\tilde{T}$. These are exactly block matrices of the form $\mathrm{U}(1) \oplus \mathrm{U}(3)$. However, we will only use matrices of the form

$$\begin{pmatrix} 1 & 0 \\ 0 & \mathrm{U}(3) \end{pmatrix}. \tag{4.38}$$

Let the first column of $\tilde{H}$ 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 (4.38), such that the first column of $\tilde{H}_1 := P_1 \tilde{H} P_1^\dagger$ is $(h_1, b, 0, 0)^T$, where $b \geq 0$. Next, we consider the matrices of the form

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \mathrm{U}(2) \end{pmatrix}. \tag{4.39}$$

Again, let the second column of $\tilde{H}_1$ 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 (4.39), such that the second column of $\tilde{H}_2 := P_2 \tilde{H}_1 P_2^\dagger$ is $(h_1, h_2, d, 0)^T$, where $d \geq 0$. Note that the first column of $\tilde{H}_2$ remains the same as for $\tilde{H}_1$. Finally, we can find P_3 of the form

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \mathrm{U}(1) \end{pmatrix}, \tag{4.40}$$

such that the last entry f of the third column of $\tilde{H}_3 := P_3 \tilde{H}_2 P_3^\dagger$ is real and non-negative. Since H_3 is Hermitian, its diagonal entries are real. Hence, it is of the form (4.37). If none of b and d is zero, we are done. If $b = 0$, we diagonalize the lower right 3×3 block of $\tilde{H}_3$ by conjugating with unitary transformations of the form $1 \oplus \mathrm{U}(3)$. Similarly, if $d = 0$ we diagonalize the lower right 2×2 block. Note that we have obtained a tridiagonal form Ξ of H.

We proceed to show the uniqueness of the tridiagonal form Ξ. Any tridiagonal form of H can be obtained by conjugating $\tilde{H}$ with unitary transformations of the form $\mathrm{U}(1) \oplus \mathrm{U}(3)$. Thus, if Ξ_1 and Ξ_2 are two tridiagonal forms of H, then $\Xi_2 = U \Xi_1 U^\dagger$, where $U \in \mathrm{U}(1) \oplus \mathrm{U}(3)$.

Assume Ξ_1 is of type 1. Since the first column of Ξ_2 has to be of the form $(a, b, 0, 0)^T$ for some $a, b \in \mathbb{R}$, $b > 0$, the unitary U has to be of the form $e^{i\varphi} I_2 \oplus \mathrm{U}(2)$ for some $\varphi \in \mathbb{R}$. Similarly, by looking at the second and third column of Ξ_2, we conclude that $U = e^{i\varphi} I_4$. Thus, we have $\Xi_2 = (e^{i\varphi} I_4) \Xi_1 (e^{-i\varphi} I_4) = \Xi_1$.

Assume Ξ_1 is of type 2. Adopting similar reasoning as in the previous case we conclude that $U = e^{i\varphi_1} I_3 \oplus e^{i\varphi_2}$ for some $\varphi_1, \varphi_2 \in \mathbb{R}$. Thus, we have $\Xi_2 = (e^{i\varphi_1} I_3 \oplus e^{i\varphi_2}) \Xi_1 (e^{-i\varphi_1} I_3 \oplus e^{-i\varphi_2}) = \Xi_1$

Assume Ξ_1 is of type 3. Again, we can argue that U is of the form $e^{i\varphi} I_2 \oplus \mathrm{U}(2)$. Note that by conjugating Ξ_1 of type 3 by unitary of the form $e^{i\varphi} I_2 \oplus \mathrm{U}(2)$, we can only change the lower right 2×2 block of Ξ_1. Thus, Ξ_2 is also of type 3 and its lower right 2×2 block has to be diagonal with sorted diagonal entries. Since diagonalization of the matrix is unique up to arrangement of eigenvalues, we conclude that $\Xi_1 = \Xi_2$.

Using similar reasoning as above we can argue that $\Xi_1 = \Xi_2$ for the case when Ξ_1 is of type 4. This shows that the tridiagonal form of a Hamiltonian is unique. $\square$

Claim 2. *T-similar 2-qubit Hamiltonians have the same tridiagonal form.*

Proof. Let H_1 and H_2 be T-similar 2-qubit Hamiltonians and Ξ be the tridiagonal form of H_1. We want to show that Ξ is also the tridiagonal form of H_2. We do this by checking the two conditions in the Definition 21. Since Ξ is the tridiagonal form of H_1, the first condition is satisfied. Since H_1 is T-similar to both H_2 and $U_T^\dagger \Xi U_T$, it follows that H_2 and $U_T^\dagger \Xi U_T$ are also T-similar. Thus, condition 2 is also satisfied and Ξ is also the tridiagonal form of H_2. $\square$

4.5.2 Tridiagonal forms of non-universal Hamiltonians

In this section we investigate the structure of the tridiagonal forms of the three families of non-universal Hamiltonians from Lemma 10. It will turn out that it is very easy to tell if a Hamiltonian falls in any of these three families by just considering its tridiagonal form. It is trivial to recognize traceless Hamiltonians from their tridiagonal form, since the trace is basis-independent. The next two Lemmas deal with Hamiltonians from the other two families of non-universal Hamiltonians.

Lemma 14. *Let H be a 2-qubit Hamiltonian given in the standard basis and let Ξ be its tridiagonal form. Then H has a common eigenvector with the T gate if and only if Ξ has $b = 0$ or $d = 0$ or $f = 0$ (see equation (4.37)).*

Proof. Due to Lemma 6, it suffices to show that H has an eigenvector orthogonal to $|s\rangle$ if and only if $b = 0$ or $d = 0$ or $f = 0$ for Ξ. Note that Ξ is the same Hamiltonian H expressed in some basis where the T gate is diagonal and $|s\rangle$ is the first basis vector. Thus, H has an eigenvector orthogonal to $|s\rangle$ if and only if Ξ has an eigenvector orthogonal to $|\tilde{s}\rangle$. So it suffices to show that Ξ has an eigenvector orthogonal to $|\tilde{s}\rangle$ if and only if $b = 0$ or $d = 0$ or $f = 0$.

If $b = 0$ or $d = 0$ or $f = 0$, then Ξ has an invariant subspace orthogonal to the singlet $|\tilde{s}\rangle$. This subspace has dimension 3 or 2 or 1, respectively. Since every invariant subspace contains at least one eigenvector, we conclude that Ξ has an eigenvector orthogonal to $|\tilde{s}\rangle$.

These conditions are also necessary. Assume Ξ has an eigenvector $|v\rangle$ that is orthogonal to $|\tilde{s}\rangle$. Note that $|v\rangle = (0, v_2, v_3, v_4)^T$ for some $v_2, v_3, v_4 \in \mathbb{C}$, not all zero. Since $|v\rangle$ is an eigenvector of Ξ, we have $\Xi\,|v\rangle = r\,|v\rangle$ for some $r \in \mathbb{R}$, or equivalently,

$$\begin{pmatrix} bv_2 \\ cv_2 + dv_3 \\ dv_2 + ev_3 + fv_4 \\ fv_3 + gv_4 \end{pmatrix} = \begin{pmatrix} 0 \\ rv_2 \\ rv_3 \\ rv_4 \end{pmatrix},$$

where a, b, c, d, e, f, g are entries of Ξ as given in (4.37). We see that $bv_2 = 0$. Now either $b = 0$ (one of our conditions) or $v_2 = 0$. If $b \neq 0$, then $v_2 = 0$ and therefore $cv_2 + dv_3 = rv_2$ is equivalent to $dv_3 = 0$. So either $d = 0$ or $v_3 = 0$. If $d \neq 0$, we repeat the same argument and note that $|v\rangle \neq 0$ to show that $f = 0$. $\square$

Lemma 15. Let H be a 2-qubit Hamiltonian given in the standard basis and let Ξ be its tridiagonal form. Assume H does not share an eigenvector with T. Then H is T-similar to a local Hamiltonian if and only if Ξ has $a = c = e = g$ (see equation (4.37)).

Proof. Assume $a = c = e = g$. In order to show that H is T-similar to a local Hamiltonian, we calculate its pattern and check that it is of the form (4.14). Since the eigenvalues and the inner products are basis-independent, Ξ and H have the same pattern, where we use $|\tilde{s}\rangle$ for calculating overlaps for the pattern of Ξ. Therefore, it suffices to show that Ξ has a pattern of the form (4.14).

We proceed to calculate a pattern of Ξ. A straightforward calculation shows that Ξ has the following eigenvalues and overlaps with $|\tilde{s}\rangle$:

$$\lambda = a \pm_1 \sqrt{\frac{b^2 + d^2 + f^2 \pm_2 z}{2}}, \quad s = \frac{z \pm_2 (b^2 - d^2 - f^2)}{4z}, \tag{4.41}$$

where the subscripts indicate which overlap corresponds to which eigenvalue and z is given by

$$z := \sqrt{b^4 + d^4 + f^4 + 2(b^2d^2 + d^2f^2 - b^2f^2)}. \tag{4.42}$$

Eigenvalues with opposite first sign and the same second sign sum to $2a$ and have the same overlaps. Therefore, the pattern of Ξ is of the form (4.14). By Theorem 5, we conclude that H is T-similar to a local Hamiltonian.

Conversely, assume that H is T-similar to a local Hamiltonian. First, we show that H is T-similar to some H' that can be expressed as

$$H' = (\alpha_1 I + x_1 X + z_1 Z) \otimes I + I \otimes (z_2 Z) \tag{4.43}$$

for some $\alpha_1, x_1, z_1, z_2 \in \mathbb{R}$. Next, we show that H' has tridiagonal form with $a = c = e = g$. Since by Claim 2 we know that T-similar Hamiltonians have the same tridiagonal form, this proves that the tridiagonal form Ξ of H has $a = c = e = g$.

We proceed to show that H is T-similar to some H' of the form (4.43). It suffices to show that there exists $U \in \mathrm{SU}(2)$ such that $H' = (U \otimes U)H(U \otimes U)^\dagger$, since $[U \otimes U, T] = 0$ for all $U \in \mathrm{SU}(2)$. Since T-similarity is an equivalence relation, we can assume that H is a local Hamiltonian. A local 2-qubit Hamiltonian H is of the form

$$H = H_1 \otimes I + I \otimes H_2, \tag{4.44}$$

where H_1 and H_2 are 1-qubit Hamiltonians.

We can write any 1-qubit Hamiltonian K as

$$K = \varphi I + r(xX + yY + zZ), \tag{4.45}$$

where X, Y, Z are Pauli matrices, (x, y, z) is a unit vector in $\mathbb{R}^3$, and $\varphi, r \in \mathbb{R}$. Conjugation of K by a unitary transformation from SU(2) corresponds to an orthogonal transformation of (x, y, z). Moreover, any orthogonal transformation on $\mathbb{R}^3$ can be achieved in this way.

By conjugating H from (4.44) with some $U \otimes U$ where $U \in \mathrm{SU}(2)$, we can simplify H so that H_2 has no X and Y components. However, there is still some freedom left—we can conjugate H with $U \otimes U$, where $UZU^\dagger = Z$. In this way we can get rid of the Y component of H_1, without affecting H_2. Without loss of generality we can assume that H_2 is traceless. This shows that H is T-similar to H' of the form (4.43) as required.

Now we proceed to show that the tridiagonal form Ξ of H' has $a = c = e = g$. Consider the following unitary transformation:

$$U_T := \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 1 & -1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & -1 \end{pmatrix}. \tag{4.46}$$

Note that U_T implements a basis change form standard basis to a T-basis, since it maps $|s\rangle$ to $|00\rangle$. If we conjugate H' from (4.43) with U_T, we get

$$\tilde{H} := U_T H' U_T^\dagger = \alpha_1 (I \otimes I) + x_1 (Y \otimes Y) + z_1 (I \otimes X) - z_2 (Z \otimes X). \tag{4.47}$$

In matrix form $\tilde{H}$ looks as follows:

$$\tilde{H} = \begin{pmatrix} \alpha_1 & z_1 - z_2 & 0 & -x_1 \\ z_1 - z_2 & \alpha_1 & x_1 & 0 \\ 0 & x_1 & \alpha_1 & z_1 + z_2 \\ -x_1 & 0 & z_1 + z_2 & \alpha_1 \end{pmatrix}. \tag{4.48}$$

Since H does not share an eigenvector with T, we can argue that $x_1 \neq 0$ by Lemma 14. Observe that $\tilde{H}$ is almost tridiagonal. We apply one more T-similarity transformation Q to bring $\tilde{H}$ to the tridiagonal form. We can do this due to Claim 2. Since we are now working in a T-basis, note that Q must commute with $\tilde{T}$. We choose Q as follows:

$$Q := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{z_1 - z_2}{l} & 0 & \frac{x_1}{l} \\ 0 & 0 & 1 & 0 \\ 0 & \frac{-x_1}{l} & 0 & \frac{z_1 - z_2}{l} \end{pmatrix}, \tag{4.49}$$

where $l = \sqrt{x_1^2 + (z_1 - z_2)^2} > 0$. Then we have

$$\Xi = Q^\dagger \tilde{H} Q = \begin{pmatrix} \alpha_1 & l & 0 & 0 \\ l & \alpha_1 & \frac{-2x_1 z_2}{l} & 0 \\ 0 & \frac{-2x_1 z_2}{l} & \alpha_1 & \frac{x_1^2 + z_1^2 - z_2^2}{l} \\ 0 & 0 & \frac{x_1^2 + z_1^2 - z_2^2}{l} & \alpha_1 \end{pmatrix}. \tag{4.50}$$

Depending on the values of x_1, z_1, and z_2 we may have to conjugate Ξ by a diagonal matrix with diagonal entries ± 1 to make the entries above and below the main diagonal non-negative. Note that this is a T-similarity transformation that does not change the diagonal entries. None of the entries $\Xi_{2,1}$, $\Xi_{3,2}$, $\Xi_{4,3}$ is 0, since H does not share an eigenvector with T. Therefore, Ξ is the tridiagonal form of H and it has equal diagonal entries. $\square$

Now we can restate the sufficient conditions for non-universality in Lemma 10 in terms of the parameters in the tridiagonal form of the Hamiltonian. We will show shortly that if the tridiagonal form of the Hamiltonian does not fall in any of the three categories mentioned in the corollary below, then H is universal.

Corollary 4. Let H be a 2-qubit Hamiltonian and Ξ be its tridiagonal form. Then H is non-universal if any of the following holds

1. Ξ has $b = 0$ or $d = 0$ or $f = 0$,

2. Ξ has $a = c = e = g$,

3. Ξ has $a + c + e + g = 0$,

where a, b, c, d, e, f, g denote the entries of Ξ as given in (4.37).

Due to Lemmas 14 and 15, the set of non-universal Hamiltonians described in the above corollary coincides with the set of non-universal Hamiltonians described in Lemma 10.

4.5.3 Universality certificate for tridiagonal Hamiltonians

In this section we finally prove the converse of Lemma 10, i.e., that if a 2-qubit Hamiltonian is not traceless, does not share an eigenvector with the T gate and is not T-similar to a local one, then it is universal. This result together with Lemma 10 gives us a complete characterization of non-universal 2-qubit Hamiltonians (see Theorem 7), which was the goal of this thesis.

Theorem 6. Let H be a 2-qubit Hamiltonian and let Ξ be its tridiagonal form. Then H is universal if Ξ does not satisfy any of the following conditions.

1. Ξ has $b = 0$ or $d = 0$ or $f = 0$,

2. Ξ has $a = c = e = g$,

3. $\mathrm{Tr}(\Xi) = 0$,

where a, b, c, d, e, f, g denote the entries of Ξ as given in (4.37).

Proof. By Corollary 1 we know that if $\mathcal{L}\,(H, THT) = \mathfrak{u}(4)$ then H is universal. Also note that $\mathcal{L}\,(H, THT) = \mathcal{L}(\Xi, \tilde{T}\Xi\tilde{T})$. Therefore, it suffices to show that $\mathcal{L}(\Xi, \tilde{T}\Xi\tilde{T})$ is the full Lie algebra of U(4). To show this, it is enough to choose a specific basis for 16×16 Hermitian matrices and express them in terms of linear combinations and commutators $i[\cdot, \cdot]$ starting from Ξ and $\tilde{T}\Xi\tilde{T}$.

Let $E_{k,l} := |k\rangle\langle l|$ and let us define a basis for traceless Hermitian matrices as follows:

$$X_{k,l} = E_{k,l} + E_{l,k}, \qquad (1 \le k < l \le 4) \tag{4.51}$$

$$Y_{k,l} = -iE_{k,l} + iE_{l,k}, \qquad (1 \le k < l \le 4) \tag{4.52}$$

$$Z_k = E_{k,k} - E_{k+1,k+1}. \qquad (1 \le k \le 3) \tag{4.53}$$

These 15 matrices together with any Hermitian matrix that has non-zero trace is a basis for the real vector space of 4×4 Hermitian matrices. We will give expressions for these basis vectors in terms of linear combinations of nested commutators of Ξ and $T\Xi T$. One can check them by doing a straightforward calculation.

Since the tridiagonal form Ξ does not satisfy condition 2 we can take linear combinations with coefficients $1/b$, $1/d$, and $1/f$. Let

$$A = \frac{1}{2b} i[\Xi, \tilde{T}\Xi\tilde{T}]. \tag{4.54}$$

One can show that the first three basis elements can be obtained as follows:

$$X_{1,2} = \frac{1}{2b}(\Xi - \tilde{T}\Xi\tilde{T}), \tag{4.55}$$

$$Y_{1,3} = \frac{1}{3d}(i[i[X_{1,2}, A], X_{1,2}] - 4A), \tag{4.56}$$

$$X_{2,3} = i[X_{1,2}, Y_{1,3}]. \tag{4.57}$$

Next, define

$$B = \frac{1}{2}(\Xi + \tilde{T}\Xi\tilde{T}). \tag{4.58}$$

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

$$Y_{1,2} = \begin{cases} \dfrac{1}{a-c}(dY_{1,3} + A) & \text{if } a \neq c, \\ \dfrac{1}{c-e} i[Y_{1,3}, i[B, X_{2,3}]] & \text{if } c \neq e, \\ \dfrac{1}{a-g}\dfrac{1}{f^2} i[i[X_{2,3}, B], i[B, i[Y_{1,3}, B]]] & \text{otherwise } (a = c = e \neq g). \end{cases} \tag{4.59}$$

Since Ξ does not satisfy condition (3), at least one of these cases is guaranteed to hold. We obtain the next two basis elements as follows:

$$X_{1,3} = i[Y_{1,2}, X_{2,3}], \tag{4.60}$$

$$X_{1,4} = \frac{1}{f}((c-e)X_{1,3} + i[A, X_{2,3}] + i[Y_{1,3}, B]). \tag{4.61}$$

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

$$X_{2,4} = i[X_{1,4}, Y_{1,2}], \tag{4.62}$$
$$X_{3,4} = i[X_{1,4}, Y_{1,3}], \tag{4.63}$$
$$Y_{1,4} = i[X_{2,4}, X_{1,2}], \tag{4.64}$$
$$Y_{2,3} = i[X_{1,3}, X_{1,2}], \tag{4.65}$$
$$Y_{2,4} = i[X_{1,4}, X_{1,2}], \tag{4.66}$$
$$Y_{3,4} = i[X_{1,4}, X_{1,3}]. \tag{4.67}$$

Finally, we add three diagonal matrices with zero trace:

$$Z_1 = \frac{1}{2} i[Y_{1,2}, X_{1,2}], \tag{4.68}$$
$$Z_2 = \frac{1}{2} i[Y_{2,3}, X_{2,3}], \tag{4.69}$$
$$Z_3 = \frac{1}{2} i[Y_{3,4}, X_{3,4}]. \tag{4.70}$$

At this point we can generate the Lie algebra of SU(4). If condition (3) does not hold ($\mathrm{Tr}\,\Xi \neq 0$), we can generate the whole $\mathfrak{u}(4)$ by including Ξ. $\square$

As a direct consequence of Theorem 6, Corollary 4 and Lemmas 14 and 15 we get the following theorem which gives a complete characterization of universal 2-qubit Hamiltonians.

Theorem 7. A two-qubit Hamiltonian H is 2-universal if and only if it does not satisfy any of the following conditions

1. H is T-similar to a local Hamiltonian,
2. H shares an eigenvector with T, the gate that swaps two qubits,
3. $\mathrm{Tr}(H) = 0$.

Recall that in order to check the first condition we only have to compute a pattern and see whether it is of the form (4.14) (see Theorem 4). Also it is not hard to check the last two conditions.

Chapter 5

3-non-universal Hamiltonians

Having understood 2-universality we would like to understand $n-$universality for $n > 2$. In this section we concentrate on $3-$universality. It turns out that there indeed are 2-non-universal 2-qubit Hamiltonians that are 3-universal. A complete characterization of 3-universal 2-qubit Hamiltonians is not yet known. In this section we list families of Hamiltonians which we know to be 3-non-universal and discuss their relation to the families of 2-non-universal Hamiltonians.

In Section 4.3 we introduced T-similarity transformations and proved that these transformations preserve 2-universality of a 2-qubit Hamiltonian. Now as a corollary we state a generalization of Theorem 2. We do not give the proof, since it is very similar to the that of Theorem 2.

Corollary 5. Let H be an m-qubit Hamiltonian and $H' := U(H \otimes I^{\otimes n-m})U^\dagger$, where $m \leq n$ and $U \in \mathrm{U}(2^n)$ is such that $[P, U] = 0$ for all $P \in \mathcal{S}_n$. Then H is n-universal if and only if H' is.

Moreover, if H' is a tensor product containing identity matrices and H'' is obtained from H' by removing those identity matrices, then H' is n-universal if and only if H'' is. For example, if $H' = H_1 \otimes I^{\otimes 3} \otimes H_2 \otimes I$, then H' is n-universal if and only if $H'' = H_1 \otimes H_2$ is.

We now list some families of 2-qubit Hamiltonians which we know to be 3-non-universal.

Lemma 16. A 2-qubit Hamiltonian H is 3-non-universal if any of the following conditions holds:

1. H is a local Hamiltonian, i.e., $H = H_1 \otimes I + I \otimes H_2$ for some 1-qubit Hamiltonians H_1, H_2,
2. H has an eigenvector of the form $|a\rangle|a\rangle$ for some $|a\rangle \in \mathbb{C}^2$,
3. $\mathrm{Tr}(H) = 0$,
4. $H = rI_4 + (U \otimes U)A(U \otimes U)^\dagger$ for some $r \in \mathbb{R}$, $U \in \mathrm{U}(2)$ and some antisymmetric Hamiltonian $A \in \mathfrak{u}(4)$ (see Definition 19),

5. $[H, U \otimes U] = 0$ for some $U \in \mathrm{U}(2)$ that has distinct eigenvalues.

Proof. 1. If H is a local Hamiltonian, then so is $P(H \otimes I)P^\dagger$ for all $P \in \mathcal{S}_3$. Therefore, by evolving different pairs of qubits according to H, we will be able to approximate only unitary transformations of the form $U_1 \otimes U_2 \otimes U_3$, where $U_1, U_2, U_3 \in \mathrm{U}(2)$. Thus, H is 3-non-universal.

2. If H has an eigenvector of the form $|a\rangle|a\rangle$, then $P(H \otimes I)P^\dagger$ has an eigenvector $|a\rangle|a\rangle|a\rangle$ for all $P \in \mathcal{S}_3$. Therefore, using H we cannot approximate those $U \in \mathrm{U}(8)$ that do not have this eigenvector. Thus, H is 3-non-universal.

3. If H is traceless, then we cannot approximate unitary transformations that have determinant other than 1. Thus, H is 3-non-universal.

4. Consider an antisymmetric Hamiltonian $A \in \mathfrak{u}(4)$. By evolving different pairs of qubits according to A, we can approximate only matrices from special orthogonal group. Therefore, A is 3-non-universal and

$$\dim\left(\mathcal{L}\left(\left\{P(A \otimes I)P^\dagger, P \in \mathcal{S}_3\right\}\right)\right) \leq \dim(\mathrm{SO}(2^3)) = 28.$$

Since for all $U \in \mathrm{U}(2)$ and all $P \in \mathcal{S}_3$ we have $[U^{\otimes 3}, P] = 0$, by Corollary 5 we conclude that all Hamiltonians of the form $(U \otimes U)A(U \otimes U)^\dagger$ are not 3-universal. Moreover, as $U^{\otimes 3}$ commutes with all qubit permutations, we have

$$\mathcal{L}\left(\left\{PU^{\otimes 3}(A \otimes I)(U^\dagger)^{\otimes 3}P^\dagger, P \in \mathcal{S}_3\right\}\right) = U^{\otimes 3}\mathcal{L}\left(\left\{P(A \otimes I)P^\dagger, P \in \mathcal{S}_3\right\}\right)(U^\dagger)^{\otimes 3},$$

which still has dimension at most 28. If we add rI_4 to $(U \otimes U)A(U \otimes U)^\dagger$, the dimension of the Lie algebra can increase by at most 1, since I_8 commutes with all other elements of the Lie algebra. Thus, the dimension can be at most 29. Hence, $H = rI_4 + (U \otimes U)A(U \otimes U)^\dagger$ is 3-non-universal.

5. If $[H, U \otimes U] = 0$ for some $U \in \mathrm{U}(2)$, then also $[P(H \otimes I)P^\dagger, U^{\otimes 3}] = 0$ for all $P \in \mathcal{S}_3$. Therefore, using H we can only approximate those $V \in \mathrm{U}(8)$ that commute with $U^{\otimes 3}$. Thus, H is 3-non-universal.

□

It is easy to see that the 3-non-universal Hamiltonians given in the list of Lemma 16 are in fact n-non-universal for all $n \geq 3$. Therefore, if we could show that this list is complete, then we would have a complete characterization of n-universal 2-qubit Hamiltonians.

Recall that a 3-non-universal 2-qubit Hamiltonian H is also 2-non-universal (see Lemma 4). Therefore, the 2-qubit Hamiltonians described in Lemma 16 form a subset of the 2-non-universal Hamiltonians described in Theorem 7. In fact, numerical experiments suggest that almost any 2-qubit Hamiltonian that is T-similar to a local Hamiltonian (one of the families of 2-non-universal Hamiltonians in Theorem 7)

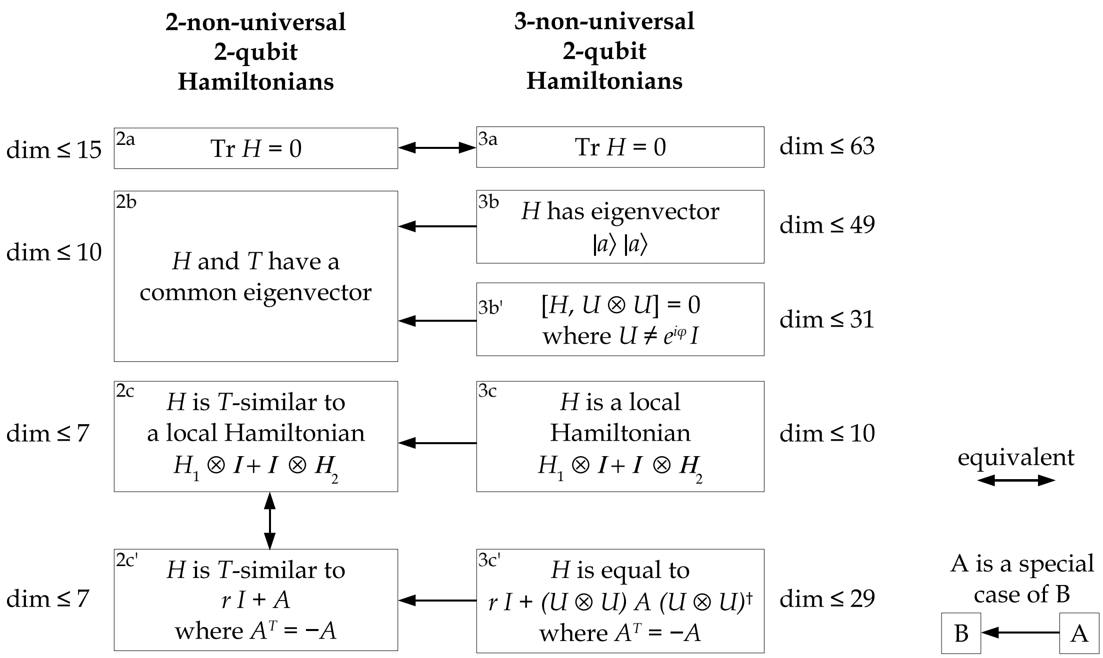

Figure 5.1: Relations between the families of 2-non-universal and 3-non-universal Hamiltonians. On the side of the boxes we indicate the maximum possible dimension of the Lie algebra corresponding to that type of Hamiltonian.

is 3-universal. The same holds true for 2-qubit Hamiltonians sharing an eigenvector with the T gate (another family of 2-non-universal Hamiltonians in Theorem 7).

It turns out that for each of the families of 3-non-universal Hamiltonians $\mathcal{F}_3$ in Lemma 16 we can choose a family of 2-non-universal Hamiltonians $\mathcal{F}_2$ from Theorem 7 so that $\mathcal{F}_3 \subset \mathcal{F}_2$ (see Figure 5.1).

We proceed to justify the relations indicated in Figure 5.1. Equivalence of boxes 2a and 3a is obvious. So is the fact that box 3c is a special case of 2c. Box 3c' is a special case of 2c' since $U \otimes U$ is a special type of T-similarity transformation, as $[U \otimes U, T] = 0$ for all $U \in \mathrm{U}(2)$. Equivalence of boxes 2c and 2c' is shown in Theorem 5. Box 3b is a special case of 2b since $|a\rangle|a\rangle$ is an eigenvector of the T gate for all $|a\rangle \in \mathbb{C}^2$.

It remains to show that box 3b' is a special case of 2b. Let λ_1, λ_2 be the distinct eigenvalues of U and let E_U be the two-dimensional eigenspace corresponding to the eigenvalue $\det(U) = \lambda_1\lambda_2$. By Theorem 1, we know that $U \otimes U$ and H are simultaneously diagonal in some orthonormal basis $\mathcal{B}$. Two of the vectors from $\mathcal{B}$ belong to $E_U^\perp$. Let $|\psi\rangle$ be one of them. Since $U \otimes U\,|s\rangle = \det(U)\,|s\rangle$, the singlet state $|s\rangle \in E_U$. Thus, we have $\langle\psi|s\rangle = 0$ and therefore $|\psi\rangle$ belongs to the 3-dimensional $(+1)$-eigenspace of the T gate. Hence, $|\psi\rangle$ is an eigenvector shared by H and T.

It might seem that box 3b' is a special case of 3b. However, this is not the case. Suppose $[H, Z \otimes Z]$=0. Consider

$$\mathcal{B} := \left\{ \frac{|00\rangle + |11\rangle}{\sqrt{2}}, \frac{|00\rangle - |11\rangle}{\sqrt{2}}, |01\rangle, |10\rangle \right\}$$

which is an eigenbasis of $Z \otimes Z$ that does not contain any vector of the form $|a\rangle|a\rangle$. Therefore, all Hamiltonians H that have eigenbasis $\mathcal{B}$ and non-degenerate eigenvalues are in box 3b' but not in box 3b.

Similarly, it is possible to choose H that has eigenvector $|a\rangle\,|a\rangle$ but does not commute with $U \otimes U$ for any $U \in \mathrm{U}(2)$. Also, neither of the boxes 3c and 3c' is contained in the other.

Chapter 6

Conclusions and open problems

The main result of this thesis is a complete characterization of 2-universal 2-qubit Hamiltonians, as summarized in the following theorem.

Theorem 7. A 2-qubit Hamiltonian H is 2-universal if and only if it does not satisfy any of the following conditions:

1. H is T-similar to a local Hamiltonian,
2. H shares an eigenvector with T, the gate that swaps two qubits,
3. $\mathrm{Tr}(H) = 0$.

Numerical results suggest that almost any 2-qubit Hamiltonian H of type (1) and (2) above is 3-universal. We do not know a complete characterization of 3-universal 2-qubit Hamiltonians, but we know some sufficient conditions for a 2-qubit Hamiltonian to be 3-non-universal (see Lemma 16). Since these conditions are sufficient also for n-non-universality for all $n \geq 3$, completeness of this list would imply a characterization of n-universal 2-qubit Hamiltonians for all $n \geq 2$. We are currently working on this problem.

There are several modifications of the problem addressed in this thesis that could also be studied in the future:

1. Which 2-qubit Hamiltonians are universal with ancillae (see Section 3.2 and Definition 12 for the definition of universality with ancillae for gates)? One can also consider a scenario in which the number of the allowed ancillary qubits is restricted.
2. Which 2-qubit Hamiltonians give us encoded universality, e.g., generate $\mathrm{O}(4)$? Universal quantum computation can be performed with a restricted repertoire of gates. For example, real gates are enough [25, 5], since $\mathrm{O}(2 \cdot 2^n)$ contains $\mathrm{U}(2^n)$. Thus we say that H is *n-universal in encoded sense*, if there exists $k \in \mathbb{N}$ such that the Lie algebra generated by H on $n+k$ qubits $\mathcal{L}_n \subseteq \mathfrak{u}(2^{n+k})$ contains $\mathfrak{u}(2^n)$ as a subalgebra. However, it is not even clear how one could check this for a *particular* Hamiltonian.

3. Which 2-non-universal 2-qubit Hamiltonians are n-universal, i.e., become universal on $n \geq 3$ qubits? Is there $n_0 \in \mathbb{N}$ such that n_0-non-universality implies n-non-universality for all $n \geq n_0$? In particular, is $n_0 = 3$?

References

[1] Adriano Barenco. A universal two-bit gate for quantum computation. *Proceedings of the Royal Society of London A, Mathematical and Physical Sciences*, 449(1937):679–683, 1995.

[2] Adriano Barenco, Charles H. Bennett, Richard Cleve, David P. DiVincenzo, Norman H. Margolus, Peter W. Shor, Tycho Sleator, John A. Smolin, and Harald Weinfurter. Elementary gates for quantum computation. *Physical Review A*, 52(5):3457–3467, 1995.

[3] Paul A. Benioff. Quantum mechanical Hamiltonian models of Turing machines. *Journal of Statistical Physics*, 29(3):515–546, 1982.

[4] Paul A. Benioff. Quantum mechanical models of Turing machines that dissipate no energy. *Physical Review Letters*, 48(23):1581–1585, June 1982.

[5] Ethan Bernstein and Umesh Vazirani. Quantum complexity theory. In *STOC '93: Proceedings of the twenty-fifth annual ACM symposium on Theory of computing*, pages 11–20, New York, NY, USA, 1993. ACM.

[6] P. Oscar Boykin, Tal Mor, Matthew Pulver, Vwani Roychowdhury, and Farrokh Vatan. On universal and fault-tolerant quantum computing. In *FOCS '99: 40th Annual Symposium on Foundations of Computer Science*, pages 486–494. Society Press, 1999.

[7] George Cybenko. Reducing quantum computations to elementary unitary operations. *Computing in Science and Engineering*, 3(2):27–32, 2001.

[8] David Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London A, Mathematical and Physical Sciences*, 400(1818):97–117, 1985.

[9] David Deutsch. Quantum computational networks. *Proceedings of the Royal Society of London A, Mathematical and Physical Sciences*, 425(1868):73–90, 1989.

[10] David Deutsch, Adriano Barenco, and Artur Ekert. Universality in quantum computation. *Proceedings of the Royal Society of London A, Mathematical and Physical Sciences*, 449(1937):669–677, 1995.

[11] David Deutsch and Richard Jozsa. Rapid solution of problems by quantum computation. *Proceedings of the Royal Society of London A, Mathematical and Physical Sciences*, 439(1907):553–558, 1992.

[12] David P. Divincenzo. Two-bit gates are universal for quantum computation. *Physical Review A*, 51:1015–1022, February 1995.

[13] Richard P. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21:467–488, June 1982.

[14] Lov K. Grover. A fast quantum mechanical algorithm for database search. In *STOC '96: Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, pages 212–219, New York, NY, USA, 1996. ACM.

[15] Lov K. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Physical Review Letters*, 79(2):325–328, July 1997.

[16] Aram W. Harrow, Benjamin Recht, and Isaac L. Chuang. Efficient discrete approximations of quantum gates. *Journal of Mathematical Physics*, 43(9):4445–4451, 2002.

[17] Roger A. Horn and Charles R. Johnson. *Topics in matrix analysis*. Cambridge University Press, 1991.

[18] Nathan Jacobson. *Lie Algebras*. Interscience Publishers, 1962.

[19] Phillip Kaye, Raymond Laflamme, and Michele Mosca. *An Introduction to Quantum Computing*. Oxford University Press, Inc., 2007.

[20] Alexei Yu Kitaev. Quantum computations: algorithms and error correction. *Russian Mathematical Surveys*, 52(6):1191–1249, 1997.

[21] Alexei Yu Kitaev, Alexander Shen, and Mikhail N. Vyalyi. *Classical and Quantum Computation*. American Mathematical Society, 2002.

[22] Seth Lloyd. Almost any quantum logic gate is universal. *Physical Review Letters*, 75(2):346–349, July 1995.

[23] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, October 2000.

[24] Michael Reck, Anton Zeilinger, Herbert J. Bernstein, and Philip Bertani. Experimental realization of any discrete unitary operator. *Physical Review Letters*, 73:58–61, July 1994.

[25] Terry Rudolph and Lov K. Grover. A 2 rebit gate universal for quantum computing. *ArXiv Quantum Physics e-prints*, October 2002.

[26] Peter W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *FOCS '94: 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, November 1994.

[27] Daniel R. Simon. On the power of quantum computation. In *FOCS '94: 35th Annual Symposium on Foundations of Computer Science*, pages 116–123, November 1994.

[28] Tommaso Toffoli. Reversible computing. In *Proceedings of the 7th Colloquium on Automata, Languages and Programming*, pages 632–644, London, UK, 1980. Springer-Verlag.

[29] Veeravalli S. Varadarajan. *Lie Groups, Lie Algebras, and Their Representations*. Springer-Verlag, 1984.

[30] Nik Weaver. On the universality of almost every quantum logic gate. *Journal of Mathematical Physics*, 41(1):240–243, 2000.