

Center for Theoretical Physics
Polish Academy of Sciences, Warsaw

Katarzyna Karnas

Universality in quantum computation

Doctoral thesis
field of study PHYSICS
speciality Theoretical Physics

The thesis written under the supervision of
dr hab. Adam Sawicki, prof. CTP PAS

May 2018

Acknowledgments

I would like to express my deepest gratitude to my supervisor Adam Sawicki and my former supervisor and mentor Professor Marek Kuś. This work could not be possible without their support and advice.

Adam Sawicki - for incentive to deal with quantum information theory and number theory, for patience and sense of humor, for revealing the secret how to be successful in science, for being a good supervisor and a good colleague.

Marek Kuś - for introducing me into theoretical physics, for giving me an opportunity to work at the Center for Theoretical Physics despite my engineering education, for many inspiring discussions about everything and for his positive attitude to life.

I acknowledge the support of NCN Grant No. DEC-2015/18/E/ST1/00200.

I would like to thank Professors and my colleagues from the Center for Theoretical Physics, Institute of Physics PAS and Institute of Mathematics PAS for great four years.

I am very grateful to my dear friends from Wrocław, Warsaw and Jerewan for their constant support and encouragement.

Last but not least I would like to thank my family, especially my sisters Karolina and Ewa and my cousin Piotr, without whom I would not be able to finish my work.

Abstract

This thesis is devoted to one of the most important problems in quantum computing, i.e. the universality problem. It reduces to deciding, if a finite set of gates operating on a system of qudits allows to construct an arbitrary operation on the qudits with an arbitrarily small error. This problem has a great practical significance as only a few quantum gates can be realized experimentally quite easily. From a mathematical point of view, universality is a problem of generating an infinite group, like a group of unitary or orthogonal transformations, by a finite number of group elements.

This thesis is a part of a project financed by the National Science Center and devoted to universality, optimality and control in quantum computing DEC-2015/18/E/ST1/00200. The main aim of our study was to formulate an algorithm for deciding universality of an arbitrary set of quantum gates. We required from our algorithm to be easy to apply and return the answer after a finite number of iterations.

Our thesis is organized as follows. In Chapter 1 we present basic concepts from theory of quantum computing. We describe a simple model of a quantum computer and give a mathematically strict definition of universality. In this chapter we also present a detailed structure of this thesis. Chapter 2 includes all the mathematical concepts that are used in this thesis. In Chapters 3 and 4, that are the core of this thesis, we present the results of our study. Chapter 3 includes a method that allows to decide universality for particular sets of one-qubit gates, whereas the approach presented in Chapter 4 can be applied for arbitrary set of quantum gates. The mathematical tools used in both chapters comes from various areas of mathematics, from field theory to representation theory of compact, semisimple Lie groups. Finally, we include in Appendix some results that are outside main thread of this thesis, but which supplement the main results.

Streszczenie

Tematem niniejszej pracy jest jeden z ważniejszych problemów w teorii obliczeń kwantowych, czyli problem uniwersalności bramek kwantowych. Polega on na określeniu, czy ze skończonego zbioru bramek działających na układzie kwantowym można wygenerować dowolną operację unitarną na tym układzie. Problem ten ma ogromne znaczenie praktyczne, jako że tylko niewielka liczba bramek kwantowych może być zrealizowana eksperymentalnie w stosunkowo prosty sposób. Wszystkie pozostałe operacje na układzie muszą być w takim wypadku uzyskane jako złożenie bramek podstawowych. Z drugiej strony, z matematycznego punktu widzenia problem uniwersalności jest problemem generowania nieskończonej grupy ze skończonej, niewielkiej liczby elementów.

Niniejsza rozprawa została zrealizowana w ramach grantu badawczego dotyczącego uniwersalności, optymalności i sterowania w obliczeniach kwantowych, finansowanego przez Narodowe Centrum Nauki DEC-2015/18/E/ST1/00200. Głównym celem badań było opracowanie algorytmu do badania uniwersalności dowolnego zbioru bramek kwantowych. Wymagane było, aby algorytm był łatwy do zaimplementowania i zawsze zwracał wynik po skończonej liczbie iteracji.

Praca składa się z czterech rozdziałów, podsumowania oraz Appendixu. W rozdziale 1 definiujemy podstawowe pojęcia z teorii obliczeń kwantowych, omawiamy zasadę działania komputera kwantowego i podajemy matematyczną definicję uniwersalności. Na końcu tego rozdziału przedstawiamy również szkic całej rozprawy. Rozdział 2 zawiera matematyczne pojęcia i twierdzenia, które wykorzystane zostały w naszej pracy. W następnych dwóch rozdziałach, które stanowią główną część pracy prezentujemy wyniki. Rozdział 3 zawiera dowód uniwersalności dla pewnych szczególnych zbiorów bramek, natomiast w rozdziale 4 przedstawiliśmy podejście, które może być stosowane dla dowolnych zbiorów bramek. Narzędzia użyte w tych dwóch rozdziałach pochodzą z różnych obszarów matematyki, od teorii rozszerzeń ciał po teorię reprezentacji półprostych, zwartych grup i algebr Liego. Na końcu zamieściliśmy Appendix z dodatkowymi wynikami oraz informacjami, które znajdują się poza głównym tematem pracy.

List of publications

Related to the content of this thesis:

1. A. Sawicki, K. Karnas, *Criteria for quantum gates universality*, Physical Review A 95, 062303, 2017
2. A. Sawicki, K. Karnas, *Universality of single qudit gates*, Annales Henri Poincaré 11, 2017
3. K. Karnas, A. Sawicki, *When is a product of finite order qubit gates of infinite order?*, Journal of Physics A: Mathematical and Theoretical 7, 2018

Not related to the content of this thesis:

1. A. Sawicki, M. Oszmaniec, M. Kuś, T. Maciazek, K. Karnas, K. Kowalczyk-Murynka, *Multipartite quantum correlations: symplectic and algebraic geometry approach*, arXiv:1701.03536

Contents

1. Introduction	15
1.1. Basics of quantum computing	15
1.1.1. Basic facts from theory of computation	16
1.1.2. What is a quantum computer?	16
1.1.3. Universality	17
1.1.4. Optimality	19
1.2. Structure of the thesis	20
2. Mathematical preliminaries	23
2.1. Basic concepts	23
2.1.1. Basic definitions from classical number theory	23
2.1.2. Basic concepts from group theory	25
2.1.3. Quaternions	26
2.1.4. Dirichlet's approximation theorem	27
2.2. Field theory	29
2.2.1. Algebraic numbers and minimal polynomials	29
2.2.2. Field extensions	30
2.2.3. Companion matrices	31
2.3. Theory of Lie groups and Lie algebras	33
2.3.1. Introduction to differential geometry	34
2.3.2. Lie groups	35
2.3.3. Representation theory of Lie groups and Lie algebras	40
2.3.4. Semisimple Lie groups and Lie algebras	41
2.4. Main facts about $SU(d)$ and $SO(d)$	43
2.5. Spectral gaps of averaging operators	49
3. Field theory and universality	53
3.1. Problem reformulation	54
3.2. Special classes of minimal polynomials	55
3.3. Proof of universality	62
3.4. Summary and open problems	64
4. Universality of single qudit gates	65
4.1. Necessary universality criterion	66
4.1.1. Universality criterion for compact, semisimple Lie algebras	67
4.1.2. Necessary universality condition for compact semisimple Lie groups	68
4.1.3. Gates and their Lie algebra elements	69
4.2. Sufficient universality criterion	72
4.2.1. Conditions for $\langle \mathcal{S} \rangle$ to be infinite	73
4.2.2. Universal sets for G	75
4.2.3. Maximal exponent N_G	77

4.3.	The algorithm for checking universality	82
4.3.1.	Upper bound for l and the spectral gap	83
4.4.	Universality criteria for one-qubit gates	87
4.5.	Universality of 2-mode beamsplitters	92
4.5.1.	Spaces $\mathcal{C}(\text{Ad}_{\mathcal{S}_3})$ and $\mathcal{C}(\text{ad}_{\mathcal{X}_3})$	92
4.5.2.	The case of the orthogonal group	92
4.5.3.	The case of the unitary group	93
4.5.4.	When is \mathcal{S}_3 universal?	94
4.6.	Summary and open problems	96
5.	Summary and outlook	99
6.	Appendix	101
6.1.	Appendix 1: alternative version of the proof of Fact 3.4	101
6.2.	Appendix 2: generators of finite subgroups of $SU(2)$	103
6.3.	Appendix 4: Implementation of the algorithm for deciding universality of $\mathcal{S} = \{U(\phi_1, \vec{k}_1), U(\phi_2, \vec{k}_2)\}$	103

List of symbols and abbreviations used in this thesis

Symbol	Explanation
\mathbb{Z}	Ring of integers
\mathbb{Z}_+	Set of positive integers
\mathbb{Q}	Field of rational numbers
\mathbb{R}	Field of real numbers
\mathbb{C}	Field of complex numbers
\mathbb{H}	Field of Hamilton quaternions
$\mathbb{R}^d, \mathbb{C}^d$	d -dimensional real or complex space
$M_d(\mathbb{K})$	Space of $d \times d$ matrices over the field \mathbb{K}
\mathbb{A}	Set of algebraic numbers
\mathbb{T}	Set of transcendental numbers
$\lfloor x \rfloor$	The greatest integer less than or equal to x (floor function)
$\lceil x \rceil$	The smallest integer larger than or equal to x (ceiling function)
$\mathbb{Z}[x], \mathbb{Q}[x]$	Ring of polynomials with integer or rational coefficients, respectively
$\mathbb{Q}(\alpha)$	Field extension over rational numbers with α
$\psi_n(x)$	Minimal polynomial of $\cos \frac{2\pi}{n}$
$\Psi_n(x)$	Minimal polynomial of $e^{2i\pi/n}$
$\eta_n(x)$	Minimal polynomial of $\cos 2\frac{\pi}{n}$
$T_n(x)$	Chebyshev polynomial of the first kind of order n
$m_\alpha(x)$	Minimal polynomial of an algebraic number α
M_α	Companion matrix of $m_\alpha(x)$
χ_M	Characteristic polynomial of M
$\det M$	Determinant of M
$\deg m(x)$	Degree of a polynomial $m(x)$
$\ \cdot\ $	Frobenius norm
$\ \cdot\ _{op}$	Operator norm
$Z(G)$	Center of a group G
\mathcal{S}	Set of group elements
\mathcal{S}_l	Set of words of length l , built from \mathcal{S}
$<\mathcal{S}>_l$	Set of words of length at most l , built from \mathcal{S}
$<\mathcal{S}>$	Set generated by \mathcal{S}
$\overline{<\mathcal{S}>}$	Topological closure of $<\mathcal{S}>$
\mathcal{X}	Set of elements of a Lie algebra
$ \mathcal{S} , \mathcal{X} $	Number of elements of \mathcal{S} and \mathcal{X} , respectively
$\Pi_G, \pi_{\mathfrak{g}}$	Representation of a Lie group G and Lie algebra \mathfrak{g} , respectively
Ad, ad	Adjoint representation of a Lie group and Lie algebra, respectively
\exp	Exponential map, $\exp : \mathfrak{g} \mapsto G$
$B(\cdot, \cdot)$	Killing form
$f(c) = O(g(c))$	There are constants $c_1 > 0, c_2$ such, that for all $c > c_1$, $f(c) \leq c_2 g(c)$

Chapter 1

Introduction

Quantum computing belongs to the fastest developing areas of physics. A great interest in this topic in recent years comes from the fact, that they have many possible applications in various areas of science and economy, e.g. in [65]:

- quantum cryptography [34, 35, 74],
- simulating quantum systems in natural sciences and medicine,
- encoding and decoding in quantum communication,
- quantum machine learning and deep learning in business and robotics,
- solving computationally hard mathematical problems.

For many years theoretical models of quantum computation were ahead of experiments and prototypes of quantum computers. The main problem for their designers is possibly ideal isolation of a quantum system from the environment, otherwise the quantum system subjects to *quantum decoherence*, which can be thought as information loss from the system [60]. Another obstacles are difficulty with precise control of quantum objects and a very high cost of cooling to temperatures close to the absolute zero. These problems have resulted in the development of many computational models. It is worth emphasizing that quantum computers have recently been not only theoretical concepts, but genuinely existing devices, e.g. Bristlecone¹ by Google or IBM Q, that belong to circuit quantum computers, or D-Wave as an example of a quantum annealer.

Below we present the main concepts and the main motivation of our thesis. In the following sections we explain a simple model of quantum computation and introduce a concept of *universality* and *optimality*. All the presented definitions will be used in Chapters 3 and 4. Throughout the following sections we will assume the notation that is conventional in quantum information theory.

1.1. Basics of quantum computing

In this section we present the model of a quantum computer that we use in this thesis and define the concepts of universality and optimality in quantum computing.

¹Bristlecone is the largest currently existing quantum processor, that operates on 72 qubits

1.1.1. Basic facts from theory of computation

Theory of computation is a subject of theoretical computer science and it answers the question, how efficiently problems can be solved using the appropriate algorithm and model of computation [78]. The best known model of computation is the *Turing machine*, which was proven to solve an arbitrary computable problem and simulate every physical process (more details can be found e.g. in Chapter III in [60]). However, the Turing machine was defined as a device with an infinite size and infinite memory capacity. A more realistic and commonly used model of computation is a *circuit model*.

Definition 1.1. A circuit is a model of computation in which input values goes through wires and a sequence of gates, i.e. objects computing a function on an input value.

In classical information theory gates are called *logic gates*, e.g. of XOR, NOT, AND etc., and they implement Boolean functions on input values. An example Boolean circuit is depicted in Figure 1.1. A set of logic gates is called *universal* if it can be used to construct an arbitrary

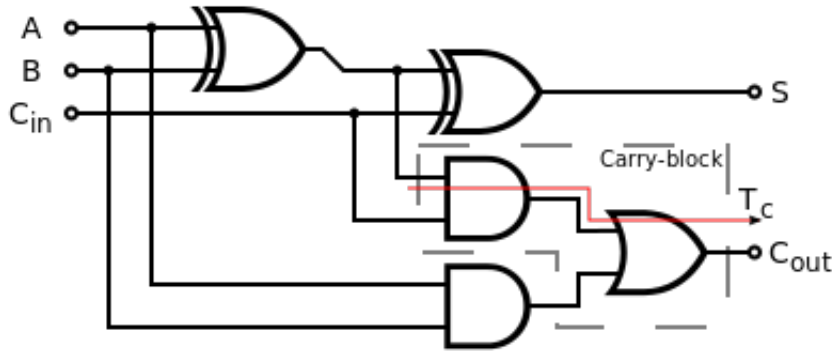


Figure 1.1: A Boolean circuit adding two bits, denoted by A and B .

logic gate. Examples of universal one-element sets of gates are NAND and NOR [60].

1.1.2. What is a quantum computer?

From a purely theoretical point of view a quantum computer is a device that operates on an isolated system of d -level quantum objects called *qudits*. All the currently existing quantum computers are built from *qubits*, i.e. objects that have two available degrees of freedom. Physical realizations of qubits include e.g. photons, electrons, low-energy ions. However, the ability to effectively manufacture optical gates using e.g. optical networks that couple modes of light [14, 64, 67] is a natural motivation to consider not only qubits but also higher dimensional systems in the quantum computation setting (see also [61, 62] for the case of fermionic linear optics and quantum metrology).

Throughout this thesis, we ignore technical details and restrict ourselves only to the general idea of quantum computers. More details concerning these topics can be found in Chapter 7 in [60].

The necessary ingredient for a quantum computer to realize quantum algorithms is the ability to perform an arbitrary unitary operation on the system of qudits. In quantum information community such operations are typically called *quantum gates*. One can distinguish two types of operations: one-qudit gates that act on a single qudit and n -qudit gates acting on n -qudits simultaneously. An n -qudit gate is called *nontrivial* (or, equivalently, *entangling*) if it does not transform a separable state to a separable state. A commonly used entangling gate that act on

two qubits is the CNOT gate, that changes a state of the second qubit depending on the state of the first qubit as follows:

$$\begin{aligned} CNOT : |00\rangle &\mapsto |00\rangle, & CNOT : |01\rangle &\mapsto |01\rangle, \\ CNOT : |10\rangle &\mapsto |11\rangle, & CNOT : |11\rangle &\mapsto |10\rangle \end{aligned}$$

In what follows we will denote by \mathcal{H} the Hilbert space corresponding to the system of qudits, on which our quantum computer operates. \mathcal{H} has a structure of a tensor product:

$$\mathcal{H} = \mathcal{H}_1 \otimes \dots \otimes \mathcal{H}_n, \quad (1.1)$$

where $\mathcal{H}_i \simeq \mathbb{C}^d$, $i = 1, \dots, n$ are one-qudit Hilbert spaces. Hence unitary operations performed on single qubits are elements of the group $SU(\mathcal{H}_i) \simeq SU(d)^2$. Similarly the qudit gates acting on the qubits represented by $\mathcal{H}_{i_1}, \dots, \mathcal{H}_{i_k}$ belong to $SU(\mathcal{H}_{i_1} \otimes \dots \otimes \mathcal{H}_{i_k}) \simeq SU(d^k)$. One- and many-qudit quantum gates are building blocks of *quantum circuits*. An example of a quantum circuit is presented in Figure 1.2. A circuit-based quantum computer is one of possible models of quantum computation and it is the only model considered throughout this thesis.

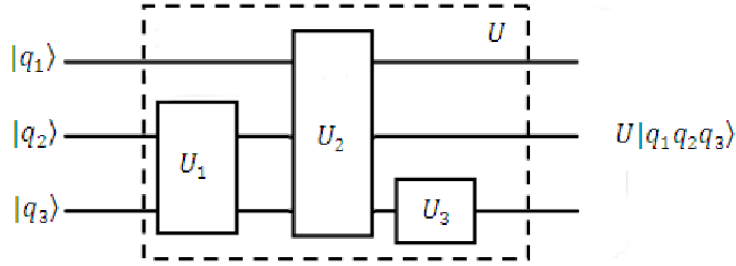


Figure 1.2: An example quantum circuit built from a one-qudit gate, denoted by U_3 , a two-qudit gate U_1 and a three-qudit gate U_2 . An output state is an entangled state of $|q_1\rangle, |q_2\rangle, |q_3\rangle$.

1.1.3. Universality

Deciding universality of a set of quantum gates is a problem of great importance in quantum computing [6, 12, 6, 8, 13, 20, 23, 27, 32, 54, 75, 76]. An analogous problem is known also in group theory as a problem of generating a group from its finite subset, a.k.a. of finding topological generators of a group [31, 33, 51]. In this section we present the concept of universality and give its interpretation in the context of quantum computers.

Let

$$\mathcal{S} = \{g_1, \dots, g_n\} \subset SU(d), \quad (1.2)$$

be a finite subset of $SU(d)$ or, equivalently, a finite set of qudit gates.

Problem 1.1. *Is it possible to construct every gate $g \in SU(d)$ from elements of \mathcal{S} with an arbitrarily small error ϵ ?*

²More precisely, unitary operations on the system \mathcal{H} belong to the group $U(\mathcal{H})$, however we restrict ourselves to $SU(\mathcal{H})$ by neglecting global phases of qudits.

In order to answer this question notice, that every composition of g_1, \dots, g_n is again a one-qudit gate. In quantum information community such compositions are called *words*. Throughout this thesis we will denote the set of words of length l by \mathcal{S}_l

$$\mathcal{S}_l = \{g_{a_1}g_{a_2} \dots g_{a_l} : a_i \in \{1, \dots, n\}\}, \quad (1.3)$$

and the set of words of length $1 \leq k \leq l$ by $\langle \mathcal{S} \rangle_l$

$$\langle \mathcal{S} \rangle_l = \bigcup_{k=1}^l \mathcal{S}_k. \quad (1.4)$$

Definition 1.2. [26, 60] A set generated by \mathcal{S} is the set of all possible words constructed from the elements of \mathcal{S} :

$$\langle \mathcal{S} \rangle := \bigcup_{l=1}^{\infty} \mathcal{S}_l. \quad (1.5)$$

An attentive reader may notice, that it is impossible to express an arbitrary gate $g \in SU(d)$ as a word of a finite length. Instead, we allow to *approximate* quantum gates with a nonzero error ϵ , where ϵ is defined as a distance³ in $SU(d)$ between the approximated gate g and an element of $\langle \mathcal{S} \rangle_l$ for some l . In particular, we can introduce the concept of a *net*.

Definition 1.3. [26] Let G be a Lie group and H be its finite subset. H is an ϵ -net of G if for every $g \in G$ there is $h \in H$ such, that

$$\|g - h\| \leq \epsilon, \quad (1.6)$$

where $\|\cdot\|$ is a distance between two group elements.

Definition 1.4. [26] A set $\langle \mathcal{S} \rangle \subset G$ is dense in a group G if for every $\epsilon > 0$ there is a set $\langle \mathcal{S} \rangle_l \subset \langle \mathcal{S} \rangle$ that forms an ϵ -net in G .

$$\mathcal{S} - \text{dense} \Leftrightarrow \forall \epsilon > 0, \forall g \in SU(d), \exists h \in \langle \mathcal{S} \rangle: \|g - h\| < \epsilon. \quad (1.7)$$

Intuitively speaking, $\mathcal{S} \subset G$ is dense in G if every element of G can be approximated with an arbitrary accuracy using elements of $\langle \mathcal{S} \rangle$. By analogy to classical information theory such sets are often called *universal*.

Definition 1.5. A set $\mathcal{S} \subset G$ is universal if $\langle \mathcal{S} \rangle$ is dense in G .

It is worth stressing, however, that $\langle \mathcal{S} \rangle$ usually does not have a group structure. The condition for $\langle \mathcal{S} \rangle \subset G$ to be a Lie group is provided by Cartan's closed subgroup theorem.

Theorem 1.1 (Cartan [19, 59]). If H is a closed subgroup of a Lie group G , then H is an analytic submanifold of G , with the induced analytic structure, which implies that H is again a Lie group.

The proof of Theorem 1.1 can be found in e.g. [19, 52, 59]. An immediate conclusion is that $\langle \mathcal{S} \rangle$ is not a Lie group unless it is *topologically closed*. In what follows we will denote the closure of $\langle \mathcal{S} \rangle$ by $\overline{\langle \mathcal{S} \rangle}$ and assume the natural topology for the space of $d \times d$ real or complex matrices.

Definition 1.6. $\mathcal{S} \subset SU(d)$ is a universal set of one-qudit gates if $\overline{\langle \mathcal{S} \rangle}$ is equal to $SU(d)$.

³Throughout this thesis we assume that $\|\cdot\|$ is the Frobenius distance (see more in Section 2.3.2).

In a general case we are interested in quantum gates operating on an arbitrarily large number of qudits. However, the following theorem allows us to restrict our considerations only to one-qudit gates.

Theorem 1.2. *[17] A universal set for n -qudit quantum computing consists of all one-qudit gates and an additional 2-qudit entangling gate.*

Intuitively speaking, Theorem 1.2 claims that a universal set for quantum computation on an arbitrary number of qudits can be constructed simply from a universal set of one-qudit gates, say \mathcal{S} , and a single entangling gate, e.g. the CNOT gate.

Literature on the universality problem includes a huge number of papers and textbooks from quantum optics, group theory, algebraic number theory and representation theory of Lie groups and Lie algebras. One of the first results concerning universality was published in 1949 by Kuranishi who had proven that a two-element subset of compact semisimple Lie group or Lie algebra was sufficient to be universal. This result was extended in [31, 51] in the context of Lie group theory and [12, 27, 54] in the context of quantum optics. It has been proven i.a. that probability of choosing a non-universal set of group elements is equal to zero. In other words universal sets \mathcal{S} of the given cardinality c form a dense open set in $SU(d)^{\times c}$. On the other hand [31, 51] gave some criteria for distinguishing non-universal sets from universal sets. In particular, they defined non-universal elements of G as characterized by vanishing of a finite number of polynomials in the gates entries and their conjugates. However, the criterion turned out to be non-applicable as these polynomials are still unknown. Recently there were also approaches providing algorithms for deciding universality of a given set of quantum gates that can be implemented on quantum automatas [23]. The main obstacle in using this approach is the fact that it requires deep knowledge from algebraic number theory.

Quantum information and quantum optics community present much more practical approach to the problem of deciding universality. They provided numerous examples of universal and non-universal one- and many-qubit sets of quantum gates [8, 48, 49, 20] and their experimental realizations [14, 64, 18, 67] (see also [61, 62] for the case of fermionic linear optics). A particular emphasis was put on qubit gates, however development of experimental techniques allows to construct quantum computers based on systems of qudits for $d > 2$. Hence there is a motivation to construct universality criteria for quantum gates operating on systems of an arbitrary degrees of freedom.

The main motivation of our thesis was to combine the approaches presented by mathematicians and physicists and formulate a universality criterion that would be as general as possible and easily applicable at the same time. We also wanted from our criteria to be possible to apply to other interesting problems. The first one is the universality problem on the level of Lie algebras, that plays a prominent role in theory of control systems [2, 16, 44] and Hamiltonian systems (see e.g. [20, 73, 82, 84]). The last problem we wanted to contribute to was the classification of finite subgroups of unitary and orthogonal groups, which are unknown for $SO(d)$, $d > 6$ and $SU(d)$, $d > 3$ [29].

1.1.4. Optimality

In Section 1.1 we mentioned that quantum computer was a very expensive and difficult to build device, which arose from the fact that a quantum system cannot be completely isolated from the environment. In a realistic case interaction with the environment results in information loss from the system. This phenomenon is known as quantum decoherence and is inevitable in a real world. For this reason it is required from quantum algorithms to be robust for errors⁴ or

⁴Using quantum error correcting codes, see more in Chapter 8 in [60]

to be performed as fast as possible, i.e. *optimally*. In this short section we will concentrate on the idea of optimality.

It has been proven by Solovay for $SU(2)$ (unpublished results [26]) and by Kitaev [47] for $SU(d)$ that a generic universal set of one-qudit gates allows to approximate an arbitrary one-qubit gate with the error ϵ using words of the length, which scales with ϵ as follows:

Theorem 1.3 (Solovay-Kitaev, [26, 47, 60]). *Let \mathcal{S} be a universal set for $SU(d)$ and let a desired accuracy $\epsilon > 0$ be given. There is a constant c such that for any $g \in SU(d)$ there exists a finite sequence $g_l \in \mathcal{S}_l$ such, that $\|g - g_l\| < \epsilon$, where*

$$l = O\left(\log^c \frac{1}{\epsilon}\right), \quad c > 0. \quad (1.8)$$

The value of c derived by Chuang and Nielsen is $c = \frac{\log 5}{\log(3/2)} = 3.97 \simeq 4$ [60]. In [26] it is presented the algorithm that allows to approximate qudit gates from $SU(d)$ with words of the length $l = O\left(\log^{3.97} \frac{1}{\epsilon}\right)$. However, it was shown by Harrow in his PhD thesis, that the exponent c can be decreased to $2 \leq c < 4$, depending on the approximating algorithm [39]. A reader interested in history of Solovay-Kitaev theorem is advised to read Section 6 of [26].

Among all universal sets of gates one can distinguish a class *optimal* (equivalently, *efficiently universal*) sets that allow to approximate quantum gates even faster than (1.8). The scaling $l(\epsilon)$ for such sets is the best possible scaling in quantum computation, in other words there is no possibility to approximate quantum gates using words shorter than (1.9).

Definition 1.7. *A universal set $\mathcal{S} \subset SU(d)$ is efficiently universal if every gate $g \in SU(d)$ can be approximated with the error ϵ using an element from \mathcal{S}_l , where*

$$l = O\left(\log \frac{1}{\epsilon}\right). \quad (1.9)$$

It is worth stressing, however, that definition of optimal universal sets is not constructive and does not provide any approximating algorithm. According to our knowledge, classification of efficiently universal sets has not been finished yet, but there are known some conditions for $\mathcal{S} \subset SU(d)$ to be efficiently universal [9, 10, 39, 63, 68]. In particular, the following conjecture has not been proven or rejected.

Conjecture 1.4 (Sarnak's conjecture:). *Every universal set of quantum gates is efficiently universal.*

1.2. Structure of the thesis

As we mentioned in Section 1.1.3 the main motivation of our thesis was to formulate an easily applicable universality criterion that would work for an arbitrary set of one-qudit gates. We are aware that the universality problem and the problem of generating infinite groups have been studied intensively both in quantum information community and among mathematicians. However, we believe that our reasoning, which is based on the set of basic properties of compact connected simple Lie groups, is explicit and direct and provides a simple and easily implemented algorithm for deciding universality.

In **Chapter 2** we present all the mathematical concepts that are used in the thesis, i.e.:

1. basic concepts from classical number theory and group theory, quaternions, Dirichlet approximation theorem,
2. theory of fields extensions and minimal polynomials,
3. theory of Lie groups, Lie algebras and their representations, with particular emphasis on compact semisimple Lie groups, Lie algebras and their representations,
4. useful facts about special unitary and special orthogonal groups,
5. spectral gap theory.

The mathematical background of this thesis was presented in a brief way, however they are often illustrated with pedagogical examples to make them easier to understand for a reader.

The concepts presented in Chapter 2 are crucial in understanding the methods, that are described in Chapters 3 and 4. The first one includes a method for deciding if the set of one-qubit gates generated by two or three particular gates is finite or infinite, whereas Chapter 4 presents general universality criteria. All the results included in this thesis were published [45, 70, 71].

In **Chapter 3** we formulate the universality criterion for two special sets of one-qubit gates, depending on a parameter ϕ , that play an important role in quantum information theory and quantum optics. To this end we use methods of number theory and field theory. This approach was inspired by the proof of universality, that was presented for $\phi = \frac{\pi}{8}$ in [13] and in Section 4.5.3 in [60]. However, our method differs significantly from the original proof and is efficiently tractable for an arbitrary value of ϕ .

The main result presented in **Chapter 4** is an algorithm for deciding universality for an *arbitrary* set of one-qubit gates, that *always* terminates after a finite number of steps. Using Definition 1.6 we divided the proof of universality into two steps:

Step 1 We distinguish the case when $\mathcal{S} \subset G$ generates a nontrivial subgroup of G from the case when \mathcal{S} is universal assuming, that $\langle \mathcal{S} \rangle$ is infinite.

Step 2 We check whether $\langle \mathcal{S} \rangle$ is infinite.

Section 4.1 is devoted to Step 1, whereas Section 4.2 includes discussion about Step 2. After presenting the algorithm we discuss the number of its iterations depending on an initial set \mathcal{S} . To this end we use the concept of a spectral gap (see Section 2.5). In Section 4.4 we apply the universality criteria for the case when \mathcal{S} is a two-element set of qubit gates. We also list all the possible situations, when such \mathcal{S} is non-universal and show, how to deal with this problem.

Chapter **Appendix** includes some additional results that are not related directly to the universality problem, but extend our considerations and can be interesting for a reader. We present i.a. a different version of the proof of Fact 3.4. We also include a full list of two-element sets of qubit gates that generate finite subgroups of $SU(2)$.

Chapter 2

Mathematical preliminaries

The main purpose of this chapter is to introduce the mathematical concepts that will be used in our thesis. In Section 2.1 we present basic definitions from number theory and group theory. We also include a brief section devoted to quaternions and present Dirichlet approximation theorem in one and many dimensions. Section 2.2 contains a survey of basic facts from field theory and companion matrix formalism. Section 2.3 is the most important part of this chapter. It includes representation theory of Lie groups and their Lie algebras and starts from a short review of basic facts and definitions. In the latter part we put particular emphasis on compact, semisimple Lie groups and Lie algebras. Section 2.4 is devoted to special unitary and special orthogonal Lie groups, i.e. the groups that play a significant role in quantum information theory. Finally, in Section 2.5 we briefly describe theory of spectral gaps of averaging operators over compact Lie groups and explain its importance in quantum computing.

It is worth emphasizing that in this chapter we restrict ourselves to the concepts, that are essential for the purpose of this thesis. In many cases, however, we illustrate them with proofs and examples for pedagogical reasons.

2.1. Basic concepts

This section is a review of concepts from various fields of mathematics. We start our introduction from presenting basic definitions from the classical number theory and group theory. In Section 2.1.3 we briefly define the field of quaternions. Section 2.1.4 is devoted to a problem of approximating real numbers with rational numbers, which was an object of interest of mathematicians from ancient to modern times.

The notation used in this thesis is in accordance with most of mathematical textbooks, i.e. \mathbb{Z} denotes the ring of integers and \mathbb{Z}_+ is the set of positive integers. $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{H}$ are fields of rational, real, complex and quaternion numbers, respectively. Symbols $\mathbb{Q}[x], \mathbb{Z}[x]$ denote the rings of polynomials with rational or integer coefficients.

2.1.1. Basic definitions from classical number theory

Let us restrict our interest to integers and define some specific *arithmetic functions* that operate on these numbers. We start for recalling the most fundamental result of Arithmetics [38]. Its proof can be found in every textbook from classical number theory, therefore we skip it in this thesis.

Theorem 2.1 (Fundamental Theorem of Arithmetics [38, 77]). *Every integer number $n \in \mathbb{Z}_+$*

can be decomposed uniquely as a product of prime numbers

$$n = p_1^{n_1} \cdot \dots \cdot p_k^{n_k}. \quad (2.1)$$

n is said to be square-free if $n_1 = \dots = n_k = 1$.

Definition 2.1. An arithmetic function $f(n)$ is a function whose domain is the set of positive integers and whose range is a subset of complex numbers.

Examples of arithmetic functions include i.a. the greatest common divisor, Möbius function, Euler function and the least common multiple. All of these functions are described in this section.

Definition 2.2. Let p_1, \dots, p_n be integers. The greatest common divisor $\gcd(p_1, \dots, p_n)$ is the largest integer, that divides p_1, \dots, p_n . If $\gcd(p_1, \dots, p_n) = 1$, the numbers are said to be relatively prime.

If n is an arbitrary integer, the greatest common divisor satisfies [38, 77]

$$\gcd(p_1, p_2) = 1 \Rightarrow \gcd(np_1 + p_2, p_1) = 1. \quad (2.2)$$

Definition 2.3. Let p_1, \dots, p_n be integers. The least common multiple $\text{lcm}(p_1, \dots, p_n)$ is the smallest integer, that is divisible by p_1, \dots, p_n . In particular if p_1, \dots, p_n are relatively prime numbers, then $\text{lcm}(p_1, \dots, p_n)$ is equal to their product.

Definition 2.4. Euler's totient function $\phi(n)$ is a function that counts the positive integers up to n that are relatively prime to n .

$$\phi(n) = \sum_{\substack{k=1 \\ \gcd(k, n)=1}}^n 1. \quad (2.3)$$

In particular, $\phi(n) = n - 1$ if n is a prime number.

Definition 2.5. Möbius function $\mu(n)$ is a function that takes values in $\{1, 0, -1\}$ depending on the factorization of n into prime factors:

- $\mu(n) = 1$ if n is square-free with an even number of prime factors,
- $\mu(n) = -1$ if n is square-free with an odd number of prime factors,
- $\mu(n) = 0$ if n is not square-free.

Theorem 2.2. [38] The Möbius function $\mu(n)$ satisfies the identity

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & n = 1 \\ 0 & n > 1 \end{cases}, \quad (2.4)$$

where $\sum_{d|n}$ is the sum over all divisors of n .

Proof of Theorem 2.2 can be found as a proof of Theorem 263 in [38]. The importance of the Möbius function becomes evident in the *Möbius inversion formula* which, intuitively speaking, inverses relation between two arithmetic functions.

Theorem 2.3. [38] Let f, g be arithmetic multiplicative functions, i.e. $f(n)f(m) = f(nm)$, $g(n)g(m) = g(nm)$ if m, n are relatively prime. Assume that f, g are related by

$$g(n) = \prod_{d|n} f(d). \quad (2.5)$$

Then the Möbius inversion of $g(n)$ has the form

$$f(n) = \prod_{d|n} g\left(\frac{n}{d}\right)^{\mu(d)}. \quad (2.6)$$

2.1.2. Basic concepts from group theory

Throughout this thesis we will usually denote groups using capital letters, e.g. G, H , whereas lowercase g, h denote group elements. Let us start from recalling the definition of a group.

Definition 2.6. A group G is a set equipped with a group operation, denoted by \cdot , that satisfies the following axioms:

1. A group G contains the neutral element I satisfying $g \cdot I = I \cdot g = g$ for all $g \in G$.
2. Every $g \in G$ has its inverse in G , i.e. $\forall g \in G$ there is $g^{-1} \in G$ such, that $g \cdot g^{-1} = g^{-1} \cdot g = I$.
3. G is closed with respect to \cdot , this means for all $g, h \in G$ the result of the group operation $g \cdot h$ also belongs to G .
4. Group operation is associative, i.e. for all $g, h, u \in G$ holds

$$(g \cdot h) \cdot u = g \cdot (h \cdot u).$$

G is called *abelian* in case when the group operation is *commutative*, i.e. for all $g, h \in G$ we have $g \cdot h = h \cdot g$. In this thesis we usually consider groups that consists of invertible matrices with real or complex entries. Such groups are called *matrix groups* and are generally non-abelian.

In the following we present basic definitions from the group theory:

Definition 2.7. The center of a group G , denoted by $Z(G)$ is a subgroup of G such, that

$$\forall h \in Z(G) \forall g \in G \quad g \cdot h = h \cdot g, \quad (2.7)$$

i.e. elements of $Z(G)$ commute with all elements of G with respect to the group operation.

Definition 2.8. A subgroup H of a group G is called *normal* if for all $g \in G$ and all $h \in H$ the following holds:

$$ghg^{-1} \in H. \quad (2.8)$$

In particular, $Z(G)$ is a normal subgroup of G .

Definition 2.9. Let H be a normal subgroup of G . A quotient group G/H is a set of all left cosets H in G :

$$G/H = \{gH, h \in G\}. \quad (2.9)$$

Definition 2.10. A group element $g \in G$ has a finite order if there exists $q \in \mathbb{Z}_+$ such, that $g^q = I$, where I is the neutral element of G . A group consisting of only finite order elements is called periodic.

Definition 2.11. A group G is finite if G consists of a finite number of elements. Otherwise G is infinite.

Definition 2.12. A group G is finitely generated if every element of G can be obtained from a finite set $\mathcal{S} \subset G$ as a composition of elements of \mathcal{S} .

In order to make these concepts clearer we illustrate them by the following example.

Example 2.4. Let G be a group of rotations in \mathbb{R}^3 . Its elements are parameterized by the rotation angle, denoted by ϕ , and a rotation axis \vec{k} . Assume that ϕ is a rational multiple of π , i.e. $\phi = \frac{2k\pi}{n}$ for some $k, n \in \mathbb{Z}$. Then a rotation $O(\phi, \vec{k})$ has a finite order as

$$O^n(\phi, \vec{k}) = O(n\phi, \vec{k}) = O(2k\pi, \vec{k}) = I.$$

The group generated by single $O(\phi, \vec{k})$ consists of the rotations

$$\langle O(\phi, \vec{k}) \rangle = \{O(\phi, \vec{k}), O(2\phi, \vec{k}), \dots, O((n-1)\phi, \vec{k}), I\},$$

which means that $\langle O(\phi, \vec{k}) \rangle$ is a periodic group.

Assume now that ϕ is an irrational multiple of π , i.e. there is no $n \in \mathbb{Z}_+$ such, that $O^n(\phi, \vec{k}) = O(2k\pi, \vec{k}) = I$, hence $O(\phi, \vec{k})$ has infinite order and the generated group is infinite. What is more, in this case $\langle O(\phi, \vec{k}) \rangle$ is a group of all rotations around \vec{k} .

In 1902, William Burnside asked about the order of elements of infinite, but finitely generated groups. His question turned out to be one of the most important and influential problems in group theory.

Problem 2.1 (Burnside Problem). Assume that G is a periodic, finitely generated group. Is G necessarily finite?

The answer that was given by Schur was positive for matrix groups whose entries were complex numbers (see more details in Chapter VI in [22])

Theorem 2.5 (Schur [22]). A matrix group with complex entries G generated from a finite number of elements is infinite if and only if G contains infinite order elements.

Schur's arguments are true i.a. for real and complex Lie groups that are our object of interest throughout this thesis. However, the answer to Problem 2.1 is negative in general. An example of a finitely generated but infinite periodic group was found in 1964 by Evgeny Golod and Igor Shafarevich [1] among groups over p -adic numbers. Such groups, however, are beyond the scope of this thesis.

2.1.3. Quaternions

In this short section we present a concept of quaternions, i.e. a number system that is an extension of complex number and forms a noncommutative ring. Quaternions were introduced by Hamilton as quotients of vectors in three-dimensional space [37] but then their concept was generalized. A formal definition of quaternions is the following:

Definition 2.13. A ring of complex dimension $\dim_{\mathbb{C}} = 2$ and real dimension $\dim = 4$ that contains \mathbb{C} , in which every nonzero element has a multiplicative inverse, but multiplication is non-commutative is called the quaternion algebra \mathbb{H} . Quaternions are associative and they form the quaternion group.

Every quaternion is represented as $q = c_0 + \vec{1} + c_1\vec{i} + c_2\vec{j} + c_3\vec{k}$ such, that

$$i^2 = a, j^2 = b, k = -ab, \quad c_0, c_1, c_2, c_3 \in \mathbb{R}, \quad (2.10)$$

The complex conjugation of q , denoted by \bar{q} is defined as $\bar{q} = \vec{1} - c_1\vec{i} - c_2\vec{j} - c_3\vec{k}$ and the norm $|q| = q \cdot \bar{q}$. Quaternions whose norm is equal to one are called *unit quaternions*. In particular the quaternions satisfying

$$i^2 = j^2 = k^2 = ijk = -1, \quad (2.11)$$

are called *Hamilton quaternions* and play especially important role in quantum and classical mechanics. They also have strong connections with theory of Lie groups, e.g.

Fact 2.1. Elements from $SU(2)$ are the matrix representation of unit quaternions, i.e. there is an injective homomorphism:

$$\Omega : q = a + b\vec{i} + c\vec{j} + d\vec{k} \rightarrow U = \begin{pmatrix} a + ib & c + id \\ -c - id & a - ib \end{pmatrix}, \quad (2.12)$$

$$\text{where } a, b, c, d \in \mathbb{R}, |q| = 1. \quad (2.13)$$

2.1.4. Dirichlet's approximation theorem

This section is devoted to the problem of approximating real numbers with rational numbers, which has a great importance in mathematics from ancient times. The first one who is known to formulate this problem formally was Diophantus of Alexandria in III-rd century B.C.

Problem 2.2 (Diophantine problem). Let ζ be an irrational real number, $p, q \in \mathbb{Z}$ and $\epsilon \in \mathbb{R}$. We ask about the bound of q such, that ζ can be approximated by $\frac{p}{q}$ with the accuracy ϵ :

$$\left| \frac{p}{q} - \zeta \right| \leq \epsilon. \quad (2.14)$$

It is worth mentioning that ϵ can be arbitrarily small as the set of rational numbers is dense in the set of real numbers. Originally, Diophantus formulated this problem setting $\epsilon = \frac{1}{q^2}$. There are also many other formulations of Diophantine approximation problem (for more details and historical remarks see Chapter XI in [38]). An elegant proof that (2.14) has infinitely many solutions if ζ is an irrational number and $\epsilon = \frac{1}{q^2}$ was given by Dirichlet. He used famous *Dirichlet's box principle* in his proof:

Lemma 2.6 (Dirichlet's box principle). Let k and m be positive integers. If $n = km + 1$ objects are distributed among m sets, then at least one of the sets will contain at least $k + 1$ objects.

Proof. The proof is immediate. Suppose that each set contains the maximal number of elements that is smaller than $k + 1$, i.e. k elements. This gives us km elements in total. But $km < km + 1$, hence at least one set must contain $k + 1$ elements. \square

In the Dirichlet's formulation of Problem 2.2 we express ϵ in terms of a positive integer $N \in \mathbb{Z}_+$ and ask about relation between q and N . Then Dirichlet's theorem takes the form:

Theorem 2.7 (Dirichlet [25, 38]). *Given any real number ζ and any positive integer N , there exist integers p and q with $0 < q \leq N$ such that*

$$|q\zeta - p| \leq \frac{1}{N}. \quad (2.15)$$

Proof. We will apply Dirichlet's box principle to prove this theorem. To this end let us define $N + 1$ numbers $z_i = i\zeta - i\lfloor\zeta\rfloor$, $i = 0, 1, \dots, N$, where $\lfloor\zeta\rfloor$ is the floor function defined as the integer part of ζ . They are contained in the interval $z_i \in [0, 1]$, which can be divided into N equal parts $[\frac{m}{N}, \frac{m+1}{N})$ of the length $\frac{1}{N}$, where $m = 0, \dots, N - 1$. Dirichlet's box principle implies that at least one interval $[\frac{m}{N}, \frac{m+1}{N})$ contains two numbers z_i . Let us denote them by z_k, z_l and assume, without loss of generality, that $l > k$. Then z_k, z_l satisfy the relation

$$|z_l - z_k| \leq \frac{1}{N} \Rightarrow \quad (2.16)$$

$$|l\zeta - \lfloor l\zeta \rfloor - (k\zeta - \lfloor k\zeta \rfloor)| \leq \frac{1}{N}, \quad (2.17)$$

$$|(l - k)\zeta - \lfloor (l - k)\zeta \rfloor| \leq \frac{1}{N}. \quad (2.18)$$

Comparing (2.18) with (2.15) we get $q = l - k$ and $p = \lfloor (l - k)\zeta \rfloor$. As l, k are both positive and bounded by N , their difference is also at most N . \square

As we will show in Section 4.2.3 Dirichlet's approximation theorem in one dimension is not sufficient for the purpose of this thesis. In most cases we will need to approximate *simultaneously* n real numbers, where $n \geq 2$. For this reason we present a simultaneous version of Theorem 2.7 in the following.

Theorem 2.8 (Simultaneous Dirichlet's approximation theorem [25, 38]). *For given real numbers ζ_1, \dots, ζ_n and an integer N there exist integers p_1, \dots, p_n and $1 \leq q \leq N^n$ such, that*

$$|q\zeta_i - p_i| \leq \frac{1}{N}. \quad (2.19)$$

Proof. The method of proving Theorem 2.8 is analogous as for Theorem 2.7 but in this case we consider an N -dimensional hypercube with the edges of length $l = 1$ and one vertex at point $\mathbf{0} = (0, 0, \dots, 0)$. In this hypercube we embed a lattice such, that the distance between neighboring points that is measured along one dimension, is equal to $\frac{1}{N}$. This is exactly an n -dimensional analogy of the construction from the proof of Theorem 2.7. The lattice divides the hypercube into N^n cells of the volume $\frac{1}{N^n}$.

Define the points $\mathbf{z}_{\mathbf{i}, \mathbf{j}} = (j_1\eta_1 - \lfloor j_1\eta_1 \rfloor, j_2\eta_2 - \lfloor j_2\eta_2 \rfloor, \dots, j_n\eta_n - \lfloor j_n\eta_n \rfloor)$, where elements of \mathbf{j} take values from 0 to N . The number of such points is equal to $(N + 1)^n$, thus by Dirichlet's box theorem some of the cells of the hypercube contain at least two numbers, say $z_{\mathbf{i}, \mathbf{k}}$ and $z_{\mathbf{i}, \mathbf{l}}$. In order to get the inequality in the form of (2.19) let us redefine $z_{\mathbf{i}, \mathbf{k}}$ and $z_{\mathbf{i}, \mathbf{l}}$ by multiplying their vector elements by $k_{-i} = \prod_{j \neq i} k_j$ or $l_{-i} = \prod_{j \neq i} l_j$ and denote $k = \prod_{j=1}^n k_j$, $l = \prod_{j=1}^n l_j$. Then the vector elements of $z_{\mathbf{i}, \mathbf{k}}$ and $z_{\mathbf{i}, \mathbf{l}}$ satisfy for each dimension

$$\begin{aligned} \forall_{i=1, \dots, d} |l\zeta_i - \lfloor l\zeta_i \rfloor - (k\zeta_i - \lfloor k\zeta_i \rfloor)| &\leq \frac{1}{N}, \\ \forall_{i=1, \dots, d} |(l - k)\zeta_i - (\lfloor l\zeta_i \rfloor - \lfloor k\zeta_i \rfloor)| &< \frac{1}{N} \end{aligned}$$

and set $p_i = \lfloor l\zeta_i \rfloor - \lfloor k\zeta_i \rfloor$. As k_i 's and l_i 's are bounded by l , we get immediately that k and l are bounded by N^n as well as the absolute value of their difference. This completes the proof. \square

2.2. Field theory

In this section we present fundamental concepts from theory of field extensions over commutative rings, which is called the *field theory*. For the purpose of this thesis we restrict our considerations to the ring of rational numbers and its finite dimensional field extensions. This formalism will be essential to formulate a universality criterion in Chapter 3.

2.2.1. Algebraic numbers and minimal polynomials

We start Section 2.2 from introducing basic concepts from field theory.

Definition 2.14. An algebraic number α is a complex number that is a root of a polynomial with rational coefficients, $p \in \mathbb{Q}[x]$. A complex number that is not algebraic is called transcendental.

Throughout this thesis we denote the set of algebraic numbers by \mathbb{A} and the set of transcendental numbers by \mathbb{T} . The set \mathbb{A} is obviously infinite, but countable and its measure in \mathbb{C} is equal to zero. The set \mathbb{T} is uncountable and dense in \mathbb{C} . Although almost all complex numbers belong to \mathbb{T} , it is much more difficult that a number is algebraic than transcendental (see Liouville construction and related discussion in Chapter XI in [38]).

Examples of algebraic numbers include i.a. all rational numbers, n -th roots of rational numbers, trigonometric functions of $\phi = \frac{p}{q}\pi$, $p, q \in \mathbb{Z}$. On the other hand numbers such as π and the Euler number e are known to be transcendental [38].

In the following we list some important facts about algebraic numbers. Their proofs are left to Section 2.2.3, where we introduce a tool that enables to determine minimal polynomials of products, sums, differences and inverses of algebraic numbers.

Fact 2.2. Let $a \in \mathbb{A}$. Then $-a$ and a^{-1} (unless $a = 0$) are algebraic numbers.

Fact 2.3. Let a_1, a_2 be algebraic numbers. Then $a_1 + a_2$ and $a_1 \cdot a_2$ are also algebraic numbers.

An immediate conclusion from Facts 2.2 and 2.3 is that \mathbb{A} is an additive group. Similarly, $\mathbb{A} \setminus \{0\}$ has the structure of a multiplicative group. Having defined algebraic numbers we can introduce the concept of a minimal polynomial.

Definition 2.15. The minimal polynomial m_α of an algebraic number α is a monic polynomial¹ from $\mathbb{Q}[x]$, of the least degree, annihilated by α , i.e. $m_\alpha(\alpha) = 0$ and unique for α .

It is worth emphasizing that every algebraic number α is a root of an infinite number of polynomials, however the minimal polynomial of α is *unique*.

Definition 2.16. The degree of an algebraic number α is the degree of its minimal polynomial.

Example: To make the concept of a minimal polynomial clearer we present some examples

- Let $\alpha = \frac{2}{3}$, then m_α is simply $m_\alpha(x) = x - \frac{2}{3}$.
- Let $\alpha = 3i$, then $m_\alpha(x) = x^2 + 3$.
- Let $\alpha = \cos \frac{2\pi}{5}$. Then the minimal polynomial m_α is of the form $m_\alpha(x) = x^2 + \frac{x}{2} - \frac{1}{4}$.

Minimal polynomials with integer coefficients belong to a wider class of polynomials called *primitive* and they have several special properties.

¹A monic polynomial is a polynomial with the leading term equal to one.

Definition 2.17. A primitive polynomial $p \in \mathbb{Z}[x]$ is a polynomial whose coefficients are relatively prime

$$p(x) = c_n x^n + c_{n-1} x^{n-1} + \dots + c_1 x + c_0, \quad \gcd(c_n, c_{n-1}, \dots, c_1, c_0) = 1.$$

The set of primitive polynomials is closed under multiplication in $\mathbb{Z}[x]$, i.e. a product of any two primitive polynomials is also a primitive polynomial. Another fact that plays an important role is that every polynomial $f(x) \in \mathbb{Q}[x]$ can be associated *uniquely* with a primitive polynomial $\tilde{f}(x)$ as follows:

$$f(x) = \alpha \tilde{f}(x), \quad \alpha \in \mathbb{Q}. \quad (2.20)$$

This fact enables to prove Gauss lemma:

Theorem 2.9 (Gauss lemma, [28, 33]). Let $f(x)$ be a polynomial with integer coefficients. Then $f(x)$ is reducible over \mathbb{Q} , i.e. it can be represented as a product $f(x) = g(x)h(x)$, where $g(x), h(x) \in \mathbb{Q}[x]$ and $g(x), h(x) \notin \mathbb{Z}[x]$, if and only if it is reducible over \mathbb{Z} .

Proof. The first part of the proof is trivial as $\mathbb{Z} \subset \mathbb{Q}$. Therefore it suffices to prove that reducibility over \mathbb{Q} implies reducibility over \mathbb{Z} .

Let us assume, without loss of generality, that $f(x) \in \mathbb{Z}[x]$ is a primitive polynomial, reducible over \mathbb{Q} (otherwise there exists a pair $(\tilde{f}(x), \alpha)$ such, that $\tilde{f}(x)$ is primitive and $\alpha \in \mathbb{Q}$). Suppose that $f(x)$ decomposes as $f(x) = g(x)h(x)$, where $g(x), h(x) \in \mathbb{Q}(x)$. Using (2.20) we can rewrite these polynomials as $g(x) = \gamma \tilde{g}(x)$, $h(x) = \chi \tilde{h}(x)$, where $\gamma, \chi \in \mathbb{Q}$ and $\tilde{g}(x), \tilde{h}(x)$ are primitive polynomials and obtain this way

$$f(x) = g(x)h(x) = \gamma\chi\tilde{g}(x)\tilde{h}(x),$$

where $\tilde{g}(x)\tilde{h}(x)$ is a primitive polynomial. In the next step we substitute $\gamma\chi = \frac{p}{q}$ for some $p, q \in \mathbb{Z}$, $\gcd(p, q) = 1$. Hence

$$qf(x) = p\tilde{g}(x)\tilde{h}(x). \quad (2.21)$$

Because $f(x)$ and $\tilde{g}(x)\tilde{h}(x)$ are primitive polynomials, the greatest common divisors for the left and right hand side of (2.21) are equal to q and p respectively, thus $p = q$. This implies immediately that $\gamma\chi = 1$ and $f(x) = \tilde{g}(x)\tilde{h}(x)$. This completes the proof. \square

2.2.2. Field extensions

In this section we introduce a fundamental concept in algebraic number theory, i.e. a field extension. To this end assume that \mathbb{L} is a field that contains \mathbb{Q} as a subfield and let \mathcal{S} be a subset of \mathbb{L} that does not belong to \mathbb{Q} .

Definition 2.18. A field extension of a ring \mathbb{Q} obtained by adjoining elements of \mathcal{S} , denoted by $\mathbb{Q}(\mathcal{S})$, is the smallest field that contains both \mathbb{Q} and \mathcal{S} . In case when all elements in $\mathbb{Q}(\mathcal{S})$ are algebraic numbers, $\mathbb{Q}(\mathcal{S})$ is called an algebraic field extension. Otherwise $\mathbb{Q}(\mathcal{S})$ is called transcendental.

Intuitively speaking, $\mathbb{Q}(\mathcal{S})$ can be thought as a vector space over \mathbb{Q} . The dimension of this space, denoted by $[L : \mathbb{Q}]$, is called a *degree* of L over \mathbb{Q} . If $[L : \mathbb{Q}] < \infty$ the extension is a *finite extension* and it is related to degrees of minimal polynomials of elements from \mathcal{S} . Therefore a finite extension is always algebraic.

The only field extensions that we deal with throughout this thesis are the algebraic field extensions generated by a single algebraic number. In what follows they will be denoted by $\mathbb{Q}(\alpha)$. Algebraically, $\mathbb{Q}(\alpha)$ is isomorphic $\mathbb{Q}[x]/(m)$, where (m) is an ideal of polynomials vanishing on α . $\mathbb{Q}[x]/(m)$ has a structure of a field and $\mathbb{Q} \subset \mathbb{Q}[x]/(m) \subset \mathbb{Q}(\alpha)$. Since $\mathbb{Q}[x]/(m)$ contains α we have $\mathbb{Q}(\alpha) = \mathbb{Q}[x]/(m)$. In order to show it one should notice, that among elements belonging to $\mathbb{Q}(\alpha)$ are, in particular, all polynomial expressions in α . Assume that $\mathbb{Q}(\alpha)$ contains an element β . Using the polynomial division formula β can be written as

$$\beta = m(\alpha)f(\alpha) + r(\alpha),$$

where $m(x)$ denotes a divisor, $f(x)$ is a dividend and $r(x)$ is the remainder satisfying by definition $\deg(r) < \deg(m) = n$. Next, notice that $m(\alpha) = 0$, hence any element of $\mathbb{Q}(\alpha)$ is a polynomial in α of degree less than n with coefficients in \mathbb{Q} . Therefore $\mathbb{Q}(\alpha)$ is finite extension whose basis is $\{1, \alpha, \dots, \alpha^{n-1}\}$ and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$. This implies that any element $\beta \in \mathbb{Q}(\alpha)$ is algebraic and $\mathbb{Q}(\beta) \subseteq \mathbb{Q}(\alpha)$. The order of β is a divisor of the order of α , i.e. a divisor of n and is given by

$$\deg(m_\beta) = [\mathbb{Q}(\beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}] / [\mathbb{Q}(\alpha) : \mathbb{Q}(\beta)]. \quad (2.22)$$

Example 2.10. As an example we will find a basis for two field extensions that are generated by a single algebraic number.

- For $\mathbb{Q}(\sqrt[3]{5})$ the basis consists of $\sqrt[3]{5}^0 = 1$, $\sqrt[3]{5}^1 = \sqrt[3]{5}$ and $\sqrt[3]{5}^2$. Notice that $\sqrt[3]{5}^k$ for $k > 2$ reduces to $\sqrt[3]{5}^{k'}$, where $k' = k \bmod 3$. In particular $\sqrt[3]{5}^3 = 5 \in \mathbb{Q}$.
- For $\mathbb{Q}(\cos \frac{2\pi}{7})$ the basis consists of $\cos \frac{2\pi}{7}$, $\cos \frac{4\pi}{7}$, $\cos \frac{6\pi}{7}$, $\cos \frac{8\pi}{7}$, $\cos \frac{10\pi}{7}$ and $\cos \frac{12\pi}{7}$, which means $[\mathbb{Q}(\cos \frac{2\pi}{7}) : \mathbb{Q}] = 6$. The dimension obtained this way is equal to degree of the minimal polynomials of $\cos \frac{2\pi}{7}$, which was obtained by symbolic computation software.

Finally, we consider the extension $\mathbb{Q}(e^{i\phi})$ where ϕ is a rational multiple of π , i.e. $\phi = \frac{2k\pi}{n}$ for some integers k, n . It is known that such $\mathbb{Q}(e^{i\phi})$ is an algebraic finite field extension as $e^{i\phi}$ is a root of unity. Using this fact we can show that $\mathbb{Q}(\cos \phi)$ and $\mathbb{Q}(\sin \phi)$ are also algebraic finite field extension. Notice that $\sin \phi$, $\cos \phi$ depend on $e^{i\phi}$ as

$$\cos \phi = \frac{e^{i\phi} + e^{-i\phi}}{2}, \quad \sin \phi = \frac{e^{i\phi} - e^{-i\phi}}{2i}.$$

By the virtue of Fact 2.3 trigonometric functions of ϕ are algebraic as they can be expressed as sums and products of algebraic numbers. Hence we get immediately that $\mathbb{Q}(\cos \phi)$ and $\mathbb{Q}(\sin \phi)$ are real subfields of $\mathbb{Q}(e^{i\phi})$.

2.2.3. Companion matrices

In this section we show, how to express minimal polynomials in terms of matrix entries of a special class of matrices called *companion matrices*. As we will show in the following this formalism enables to compute the minimal polynomial for a sum and a product of two algebraic numbers.

We say that a square matrix $M \in M_n(\mathbb{Q})$ is a root of a polynomial $p \in \mathbb{Q}[x]$ if $p(M) = 0$ (in other words p annihilates M). Let $\chi_M \in \mathbb{Q}[x]$ be a characteristic polynomial of $M \in M_n(\mathbb{Q})$, $\chi_M(x) = \det(xI - M)$. By the Cayley-Hamilton theorem M is a root of its own characteristic polynomial, i.e. $\chi_M(M) = 0$.

Definition 2.19. [3] A monic polynomial $m_M \in \mathbb{Q}[x]$ of the smallest degree that is irreducible over \mathbb{Q} and annihilates M is the minimal polynomial of M . The minimal polynomial of M divides the characteristic polynomial of M .

On the other hand, every minimal polynomial $m_\alpha \in \mathbb{Q}[x]$ has an associated matrix called the *companion matrix* M_α , defined as follows:

Definition 2.20. [3] Let $m_\alpha(x)$ be a minimal polynomial of a root α of degree $\deg m_\alpha(x) = n$. The companion matrix M_α is an $n \times n$ matrix over \mathbb{Q} such, that

$$\chi_{M_\alpha} = m_{M_\alpha} = m_\alpha = \sum_{i=0}^{n-1} c_i x^i + x^n, \quad (2.23)$$

and is of the form

$$M_\alpha = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & -c_0 \\ 1 & 0 & 0 & \dots & 0 & -c_1 \\ 0 & 1 & 0 & \dots & 0 & -c_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 & -c_{n-2} \\ 0 & 0 & 0 & \dots & 1 & -c_{n-1} \end{pmatrix}. \quad (2.24)$$

In what follows we will apply the companion matrix formalism to find minimal polynomials of $-\alpha$, α^{-1} , $\alpha + \beta$ and $\alpha\beta$ under the assumption that α, β are algebraic numbers and their minimal polynomials m_α, m_β are known. Let us start from the minimal polynomial of $-\alpha$ and denote its coefficients by d_0, \dots, d_{n-1} . We can write:

$$\begin{aligned} m_\alpha(\alpha) &= c_0\alpha^0 + c_1\alpha + c_2\alpha^2 + \dots + c_{n-1}\alpha^{n-1} + \alpha^n = 0, \\ m_{-\alpha}(-\alpha) &= d_0(-\alpha)^0 + d_1(-\alpha) + d_2(-\alpha)^2 + \dots + d_{n-1}(-\alpha)^{n-1} + (-\alpha)^n, \\ m_{-\alpha}(-\alpha) &= d_0\alpha - d_1\alpha + d_2\alpha^2 + \dots + (-1)^{n-1}d_{n-1}\alpha^{n-1} + (-1)^n\alpha^n = 0. \end{aligned}$$

Comparing the minimal polynomials of m_α and $m_{-\alpha}$ we can see immediately that if n is an even number, then $c_{2k} = d_{2k}$ and $c_{2k+1} = d_{2k+1}$, where $k = 0, \dots, \frac{n-2}{2}$. In the case when n is an odd number the coefficients of m_α and $m_{-\alpha}$ satisfy $-c_{2k} = d_{2k}$ and $-c_{2k+1} = d_{2k+1}$.

We find the minimal polynomial of α^{-1} in a similar way. It is known from linear algebra theory [3] that when α is a root of the characteristic polynomial of M_α , then α^{-1} is a root of the characteristic polynomial of $M_{\alpha^{-1}} = M_\alpha^{-1}$. As M_α is a matrix with rational coefficients, M_α^{-1} is also a rational matrix and its characteristic polynomial belongs to $\mathbb{Q}[x]$. This implies that α^{-1} is an algebraic number.

The above arguments show that the minimal polynomials of $-\alpha$ and α^{-1} exist, hence $-\alpha$ and α^{-1} are algebraic numbers if α is algebraic. This way we have proven Fact 2.3.

In what follows we use the companion matrix formalism to find the minimal polynomials for a sum and a product of two algebraic numbers in some special cases. Assume $\alpha, \beta \in \mathbb{A}$ and their minimal polynomials are m_α and m_β , respectively. It is known from linear algebra theory that $\alpha\beta$ is a root of the characteristic polynomial of the matrix

$$M_{\alpha\beta} = M_\alpha \otimes M_\beta, \quad (2.25)$$

and $\alpha + \beta$ is a root of the characteristic polynomial of the matrix

$$M_{\alpha+\beta} = M_\alpha \otimes I_\beta + I_\alpha \otimes M_\beta, \quad (2.26)$$

where I_β is the identity $[\mathbb{Q}(\beta) : \mathbb{Q}] \times [\mathbb{Q}(\beta) : \mathbb{Q}]$ matrix and I_α is the identity $[\mathbb{Q}(\alpha) : \mathbb{Q}] \times [\mathbb{Q}(\alpha) : \mathbb{Q}]$ matrix. It is worth emphasizing that $M_{\alpha\beta}$ and $M_{\alpha+\beta}$ are not companion matrices in the true sense of this word, therefore $m_{\alpha\beta}$ and $m_{\alpha+\beta}$ may not be equal to characteristic polynomials of $M_{\alpha\beta}$ and $M_{\alpha+\beta}$, respectively. The only case when the equality holds is when α or β is a rational number.

Fact 2.4. [45] Assume that $\alpha \in \mathbb{Q}$ and $\beta \notin \mathbb{Q}$. Then $[\mathbb{Q}(\alpha + \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha\beta) : \mathbb{Q}] = [\mathbb{Q}(\beta) : \mathbb{Q}]$ and the minimal polynomials of $\alpha\beta$ and $\alpha + \beta$ are given by the characteristic polynomials of

$$M_{\alpha\beta} = \alpha M_\beta, \quad M_{\alpha+\beta} = \alpha I_\beta + M_\beta, \quad (2.27)$$

where M_α and M_β are the companion matrices of α and β .

Proof. Notice that $m_\alpha(x)$ is the first order polynomial $m_\alpha(x) = x - \alpha$ if α is a rational number. Hence M_α is a 1×1 matrix $M_\alpha = \alpha$. Using the companion matrix formalism we know that the characteristic polynomials of the matrices (2.27) annihilate $\alpha\beta$ and $\alpha + \beta$ respectively. We also know that $\mathbb{Q}(\beta) = \mathbb{Q}(\alpha + \beta) = \mathbb{Q}(\alpha\beta)$. Using formula (2.22) we get that $\deg m_{\alpha+\beta} = \deg m_{\alpha\beta} = [\mathbb{Q}(\beta) : \mathbb{Q}] = \deg m_\beta$. But the degrees of $\chi_{M_{\alpha\beta}}$ and $\chi_{M_{\alpha+\beta}}$ are also $\deg m_\beta$. The result follows. \square

In a general case the degrees of $m_{\alpha\beta}$ and $m_{\alpha+\beta}$ are bounded by

$$\max(\deg m_\alpha(x), \deg m_\beta(x)) \leq \deg m_{\alpha+\beta, \alpha\beta}(x) \leq \deg m_\alpha(x) \deg m_\beta(x).$$

Thus typically we need to find $\chi_{M_{\alpha\beta}}$ or $\chi_{M_{\alpha+\beta}}$ and factorize it over \mathbb{Q} obtaining $\chi_{M_{\alpha+\beta}} = m_{\alpha+\beta, \alpha\beta}(x) \cdot p_1(x) \cdot \dots \cdot p_k(x)$ or $\chi_{M_{\alpha\beta}} = m_{\alpha\beta, \alpha\beta}(x) \cdot p'_1(x) \cdot \dots \cdot p'_k(x)$ respectively. According to our knowledge there is no general method for computing the degree of $m_{\alpha\beta}$ and $m_{\alpha+\beta}$ if at least one of α, β is not a rational number.

2.3. Theory of Lie groups and Lie algebras

The role of Lie groups, Lie algebras and their representations is prominent in physics, especially in classical and quantum mechanics. Lie groups describe symmetries of physical systems, e.g. symmetry of translations in space and time, rotational symmetry, isospin and flavour symmetry etc. Throughout this thesis a particular emphasis is placed on the group of unitary matrices, which represents unitary operations, called quantum gates, performed on a system of qudits. Recall, that one- and many-qudit gates are building blocks for quantum computation and are one of the most fundamental concepts in quantum information theory.

The current section presents a survey of fundamental facts from theory of Lie groups, Lie algebras and their representations. The section is structured as follows: Sections 2.3.1 and 2.3.2 include main definitions from differential geometry and theory of Lie groups and Lie algebras, respectively. In Section 2.3.3 we will introduce a concept of representations of Lie groups and Lie algebras and formulate an extended version of Schur's lemma. Section 2.3.4 is devoted to semisimple Lie groups and Lie algebras. Finally, in Section 2.4 we describe in detail the groups of unitary and orthogonal matrices.

The content of the current section is presented in a brief and compact way. A more detailed introduction to representation theory of Lie groups and Lie algebras can be found in [15, 29, 36, 50] and in a more general setting in [22].

2.3.1. Introduction to differential geometry

Let us start from a basic object called a *topological space*. Intuitively speaking, it is defined as a set \mathcal{X} whose elements (which are often called *points*) satisfy a system of the following axioms.

Definition 2.21. [40, 57] A topological space (\mathcal{X}, τ) is a set \mathcal{X} with collection of open subsets τ satisfying the following conditions:

1. The empty set belongs to τ .
2. \mathcal{X} belongs to τ .
3. The intersection of a finite number of sets from τ belongs to τ .
4. The intersection of an arbitrary number of sets from τ belongs to τ .

A special kind of topological spaces are *differential manifolds*, i.e. topological spaces that *locally* resemble a linear space \mathbb{R}^n near each point. We define them in a more formal way as follows:

Definition 2.22. [52] A differential manifold \mathcal{M} is a topological space equipped with an equivalence class of pairs (U_α, ϕ_α) , called charts, where U_α is the open covering of \mathcal{M}

$$\forall_\alpha U_\alpha \subset \mathcal{M} \text{ is open and } \bigcup_\alpha U_\alpha = \mathcal{M}.$$

Maps $\phi_\alpha : U_\alpha \rightarrow \mathbb{R}^n$, called coordinate maps, are homeomorphisms² onto open subsets of \mathbb{R}^n and a transition map $\phi_{\alpha_2 \rightarrow \alpha_1}$ defined as

$$\forall_{\alpha_1, \alpha_2} U_{\alpha_1} \cap U_{\alpha_2} \neq \emptyset \Rightarrow \phi_{\alpha_2 \rightarrow \alpha_1} : \phi_{\alpha_2}(U_{\alpha_1} \cap U_{\alpha_2}) \rightarrow \phi_{\alpha_1}(U_{\alpha_1} \cap U_{\alpha_2}),$$

is infinitely differentiable.

The following example spaces may be counted among differential manifolds:

- Unit sphere in $n + 1$ dimensions \mathbb{S}^n , $\mathbb{S}^n = \{x_1, x_2, \dots, x_{n+1} : x_1^2 + x_2^2 + \dots + x_{n+1}^2 = 1\}$.
- Real coordinate space \mathbb{R}^n of dimension n and every open subset of \mathbb{R}^n .
- The space of $d \times d$ orthogonal matrices of determinant $\det = 1$, denoted by $SO(d)$. The family $\{SO(d), d = 2, 3, \dots\}$ of such manifolds plays an important role in this thesis.

In the following we show, how to assign a linear space to each point m of a manifold \mathcal{M} . To this end we define first, what is a smooth function on \mathcal{M} .

Definition 2.23. A function f on \mathcal{M} is called smooth if and only if the function composition $f \circ \phi_\alpha^{-1}$ is a smooth real-valued function on $\phi_\alpha(U_\alpha)$ for all coordinate functions ϕ_α . The set of smooth functions on \mathcal{M} is usually denoted by $\mathcal{C}^\infty(\mathcal{M})$.

Definition 2.24. Let f, g be smooth functions on \mathcal{M} . A derivation D is a linear map $D : \mathcal{C}^\infty(\mathcal{M}) \rightarrow \mathbb{R}$ satisfying Leibniz identity

$$D(f \cdot g)(m) = D(f(m)) \cdot g(m) + f(m) \cdot D(g(m)), \quad m \in \mathcal{M}.$$

Space of derivations is called tangent space of \mathcal{M} at point m and is denoted by $T_m \mathcal{M}$.

Given a coordinate system on the manifold $\phi_\alpha = (x_1, \dots, x_n)$ we can identify derivations with partial derivatives $\frac{\partial}{\partial x_i}|_m$. Such derivations form a basis for $T_m \mathcal{M}$ and hence the dimensions of \mathcal{M} and its tangent space at an arbitrary point are equal. The concept of differential manifolds can be generalized to complex manifolds, which can be done by defining finite dimensional complex spaces with an atlas of holomorphic maps.

²A homeomorphism is a continuous bijective function $f : X \rightarrow Y$ between two topological spaces X and Y such, that the inverse function f^{-1} is also continuous.

2.3.2. Lie groups

Having defined differential manifolds and tangent spaces we are ready to introduce the concept of a Lie group and a Lie algebra. In general, these structures can be considered independently both in mathematics and in physics. However, in this thesis Lie groups play a prominent role and Lie algebras are considered only as the related spaces of a much simpler structure.

Definition 2.25. *A real Lie group G is a differentiable manifold equipped with the group operations*

$$\cdot : G \times G \rightarrow G, \quad (g_1, g_2) \rightarrow g_1 \cdot g_2, \quad (2.28)$$

$$(\cdot)^{-1} : G \rightarrow G, \quad g \rightarrow g^{-1} \quad (2.29)$$

that are smooth maps. Similarly, a complex Lie group G is a complex manifold equipped with the group operations (2.28, 2.29) that are holomorphic maps.

A Lie group acts on itself with the following operations:

- *Left multiplication $L_g : G \times G \rightarrow G$ defined as $L_g(h) = gh$, $g, h \in G$,*
- *Right multiplication $R_g : G \times G \rightarrow G$ defined as $R_g(h) = hg$,*
- *Adjoint action Ad defined as $\text{Ad}_g(h) = ghg^{-1}$,*
- *Group commutator $[\cdot, \cdot]_\bullet$ defined as $[g, h]_\bullet = ghg^{-1}h^{-1}$.*

A particularly important class of Lie groups are matrix Lie groups. It is known [36] that every matrix Lie group is a closed subgroup of $GL(d, \mathbb{R})$ or $GL(d, \mathbb{C})$ that are spaces of $d \times d$ invertible matrices with real or complex entries, respectively. Matrix multiplication plays the role of the group operation and the identity matrix, denoted by I , is the neutral element. As it was mentioned in the previous section, all matrix Lie groups are algebraic groups. In what follows we will always assume that G is a matrix Lie group. To be more precise, we concentrate on the real matrix Lie groups that play a vital role in quantum mechanics and quantum information theory. They are collected in the below list:

- Unit circle in \mathbb{C} , denoted by $U(1)$ with multiplication as the group operation.
- Group of unitary matrices $U(d)$, i.e. the matrices preserving the inner product on \mathbb{C}^d

$$\forall x, y \in \mathbb{C}^d \quad \langle x, y \rangle = \langle Ux, Uy \rangle \quad (2.30)$$

$$U(d) \ni U : UU^* = I, \quad (2.31)$$

where U^* denotes conjugate transposition of U . Equivalently, the column vectors of U are orthonormal (here $\overline{U_{ji}}$ denotes complex conjugation of U_{ji})

$$\sum_{j=1}^d \overline{U_{ji}} U_{jk} = \delta_{ik}. \quad (2.32)$$

- Group of unitary matrices with determinant $\det = 1$, denoted by $SU(d)$.
- Group of orthogonal matrices $O(d)$ i.e. the matrices preserving the inner product on \mathbb{R}^d

$$\forall x, y \in \mathbb{R}^d \quad \langle x, y \rangle = \langle Ox, Oy \rangle \quad (2.33)$$

$$O(d) \ni O : OO^t = I, \quad (2.34)$$

where O^t denotes transposition of O . Equivalently, the column vectors of O are orthonormal

$$\sum_{j=1}^d O_{ji} O_{jk} = \delta_{ik}. \quad (2.35)$$

- Group of orthogonal matrices with determinant $\det = 1$, denoted by $SO(d)$.
- $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ which can be identified with $GL(1, \mathbb{R})$.

At the end of this section we will introduce the concept of a *continuous path* in a Lie group G . It is defined as a continuous function from the interval $[0, 1]$ to G , $\gamma : [0, 1] \rightarrow G$, which satisfies the composition law

$$\gamma(s)\gamma(t) = \gamma(s+t).$$

The image of γ is a subgroup of G and in what follows we will call it *one-parameter subgroup of G* .

2.3.2.1. Compactness

There are many equivalent definitions of compactness for matrix Lie groups. Let us start from the most general one, which is valid also for non-matrix Lie groups and is expressed in the language of topology.

Definition 2.26. *A Lie group G is compact if it is compact as a manifold, i.e. every open cover $\{U_\alpha\}$ of G has a finite subcover.*

In case of matrix Lie groups a more practical definition of compactness can be formulated. To this end let us introduce Heine-Borel theorem (its proof can be found in e.g. [72]).

Theorem 2.11 (Heine-Borel [72]). *A subset of Euclidean space, $E \subset \mathbb{R}^n$ is compact if and only if it is closed and bounded.*

Notice that every subgroup G of $GL(d, \mathbb{R})$ and $GL(d, \mathbb{C})$ can be thought as a subspace of \mathbb{R}^{n^2} and \mathbb{C}^{n^2} , respectively. Then Heine-Borel theorem implies that G is compact if G is closed and bounded. Equivalently, G is compact if the space of parameters, that parameterize elements of G , is closed and bounded.

Examples of compact Lie groups include: $U(d)$, $O(d)$ and their subgroups $SU(d)$, $SO(d)$. Compactness can be shown in these cases using Heine-Borel theorem and identities (2.32), (2.35) respectively. For instance, assume that d^2 entries of $U \in U(d)$ form a parameter space for $U(d)$. As the identity (2.32) is satisfied for all possible pairs of matrix columns, we get immediately that all entries of U are bounded by $|U_{j,k}| \leq 1$. Hence the parameter space of $U(d)$ has a finite volume and by Heine-Borel theorem $U(d)$ and $SU(d)$ are compact groups. An analogous reasoning allows to show compactness of $O(d)$ and $SO(d)$. On the other hand $GL(d, \mathbb{R})$ and $GL(d, \mathbb{C})$ belong to non-compact Lie groups.

2.3.2.2. Connectedness

Definition 2.27. *A Lie group G is said to be connected³ if for any two elements $g, h \in G$ there exists a continuous path $\gamma(t)$, $t_1 \leq t \leq t_2$ belonging to G such, that $\gamma(t_1) = g$ and $\gamma(t_2) = h$.*

³Definition 2.27 concerns actually *path-connectedness* which may differ from the connectedness defined with respect to group topology. However, in case of matrix Lie groups connectedness and path-connectedness are equivalent.

A Lie group that is not connected consists of connected subspaces called *connected components*. It is worth stressing that they are not necessarily subgroups of G . Using Definition 2.26 we easily conclude that:

Fact 2.5. *A compact Lie group consists of a finite number of connected components.*

The connected component of G that contains I is distinguished among all the connected components and called the *identity component*. Throughout this thesis we denote it by G_0 .

Fact 2.6. *The identity component of a Lie group G is a subgroup of G .*

Proof. Recall that subgroup of a group G is a subspace of G that contains a neutral element and is closed with respect to group multiplication and inversion. The first condition is satisfied by G_0 by definition. In order to check the second one, assume that $g, h \in G_0$, thus there are continuous paths $\gamma_g(t), \gamma_h(t)$ in G_0 that join the neutral element with g and h . Composing $\gamma_g(t)$ with $\gamma_h(t)$ we get a continuous path from I to gh , thus $gh \in G_0$. Similarly, $gg^{-1} = g^{-1}g = I \in G_0$ and $hh^{-1} = h^{-1}h = I \in G_0$. Thus using the argument with composing continuous paths we see that $g^{-1}, h^{-1} \in G_0$, which implies that G_0 is a group. \square

Examples of connected Lie groups include i.a. $U(d)$, $SU(d)$, $SO(d)$, $SL(d, \mathbb{R})$ and $SL(d, \mathbb{C})$. The groups $GL(d, \mathbb{R})$ and $O(d)$ belong to non-compact groups.

Example: In order to make the concept of connectedness clearer we show that

1. $SU(d)$ is connected,
2. $O(d)$ is a non-connected Lie group.

The proofs of 1. and 2. can be found in many textbooks devoted to Lie groups and Lie algebras theory, e.g. in [36].

1. A fundamental theorem of algebra (see e.g. Theorem B3. in [36]) states that every unitary matrix is diagonalizable, i.e. for every $U \in SU(d)$ there exists a matrix $D \in SU(d)$ such, that $U = D \begin{pmatrix} e^{i\phi_1} & 0 & \dots \\ \vdots & \ddots & \vdots \\ \dots & 0 & e^{i\phi_d} \end{pmatrix} D^*$. Define a continuous path in $SU(d)$ from U to the group identity:

$$\gamma(t) = \{U(t) = D \begin{pmatrix} e^{it\phi_1} & 0 & \dots \\ \vdots & \ddots & \vdots \\ \dots & 0 & e^{it\phi_d} \end{pmatrix} D^*, 0 \leq t \leq 1\}.$$

Similarly, let $\gamma'(t)$ be a continuous path from I to $U(d) \ni U' = D' \begin{pmatrix} e^{i\phi'_1} & 0 & \dots \\ \vdots & \ddots & \vdots \\ \dots & 0 & e^{i\phi'_d} \end{pmatrix} (D')^*$.

Then U and U' are joined by a continuous path $\gamma_{UU'}(t) = \gamma(t) \cup \gamma'(t)$. The result follows.

2. By definition of an orthogonal matrix $OO^t = I$ we can find its determinant as $\det O \det O^t = (\det O)^2 = \det I = 1$. We used the fact, that transposition does not change the determinant. The condition $\det^2 O = 1$ shows, that $O(n)$ consists of the space of matrices with determinant $\det = -1$ and the space of matrices with $\det = 1$. Let us denote them by $O_-(d)$ and $O_+(d)$ respectively. Notice that there cannot be any continuous path $\gamma(t)$

connecting $O_-(d)$ and $O_+(d)$ because otherwise $\gamma(t)$ would contain a matrix with determinant zero which does not belong to $O(d)$.

The proof that $O_-(d)$ and $O_+(d)$ are connected components of $O(d)$ is analogous to the case 1. In particular, $O_+(d)$ is the identity component of $O(d)$ and is typically denoted by $SO(d)$.

An important class of non-connected groups are *discrete subgroups* of Lie groups, defined as follows:

Definition 2.28. A discrete subgroup of a Lie group G is a closed subgroup $H \subset G$ such, that there exists an open cover of G for which every open subset contains exactly one element from H .

Fact 2.7. If G is a compact Lie group, every discrete subgroup of G must be finite.

Proof. The proof of this fact results immediately from Definition 2.26. Let us assume that a cover of G is a union of a discrete open cover of H and the open set, that does not contain H . If H was infinite, then the open cover of G defined in such a way would not have a finite subcover. Hence we get a contradiction. \square

2.3.2.3. Lie algebras

The main obstacle in studying Lie groups is the fact, that they are not linear spaces but they may have a very nontrivial topological structure. For this reason one can consider simpler objects called *Lie algebras* instead. This approach is fruitful especially in the case when we restrict our interest to the neighborhood of the neutral element. In this section we give a brief introduction to theory of Lie algebras, starting from a purely algebraic definition.

Definition 2.29. A Lie algebra is a vector space over the field \mathbb{K} , equipped with a product $[X, Y]$ called a Lie bracket, that is linear in each variable and satisfies the following conditions

1. $[X, Y]$ is antisymmetric, $[X, Y] = -[Y, X]$,
2. $[X, Y]$ satisfies Jacobi identity

$$[X, [Y, Z]] + [Y, [Z, X]] + [Z, [X, Y]] = 0 \quad \forall X, Y, Z \in \mathfrak{g}. \quad (2.36)$$

Especially important and deep theorem concerning Lie algebras was formulated by Ado [36, 50]. Intuitively speaking, it states that every Lie algebra over a field of characteristic zero can be viewed as a Lie algebra of square matrices under the commutator bracket.

For any Lie group G one can assign a *unique* Lie algebra \mathfrak{g} called *the Lie algebra of G* . On the other hand \mathfrak{g} enables to recover uniquely *only* the neighborhood of the group neutral element. [36, 50]. G acts on its Lie algebra \mathfrak{g} in a canonical way by the *adjoint action*

$$\text{Ad} : G \times \mathfrak{g} \rightarrow \mathfrak{g}, \quad \text{Ad}_g X = gXg^{-1}, \quad g \in G, \quad X \in \mathfrak{g}. \quad (2.37)$$

Definition 2.30. The Lie algebra \mathfrak{g} of a Lie group G is a tangent space to G at the group neutral element.

Example 2.12. Below we list examples of Lie algebras the Lie groups that are considered throughout this thesis.

- Lie algebra of $GL(d, \mathbb{R})$ ($GL(d, \mathbb{C})$), denoted by $\mathfrak{gl}(d, \mathbb{R})$ ($\mathfrak{gl}(d, \mathbb{C})$ respectively) is the space of $d \times d$ real (complex) matrices.

- Lie algebra of $U(d)$, denoted by $\mathfrak{u}(d)$ is the space of $d \times d$ antihermitian matrices.

$$\mathfrak{u}(d) \ni u : u^* = -u.$$

- Lie algebra of $O(d)$ and $SO(d)$, denoted by $\mathfrak{so}(d)$ is the space of $d \times d$ antisymmetric matrices.

$$\mathfrak{so}(d) \ni o : o^T = -o.$$

Definition 2.31. A subalgebra of a Lie algebra \mathfrak{g} is the subspace $\mathfrak{h} \subset \mathfrak{g}$ that is closed under the Lie bracket.

2.3.2.4. Exponential map

Exponential map is an essential ingredient in studying relations between Lie groups and their Lie algebras. Its canonical definition expressed in terms of one-parameter subgroups is very straightforward.

Definition 2.32. Let G be a Lie group and \mathfrak{g} be the Lie algebra of G . The exponential map $\exp : \mathfrak{g} \rightarrow G$ is a unique homomorphism defined as

$$\exp(X) = \gamma(1), \quad (2.38)$$

where X is an element of \mathfrak{g} and $\gamma(t)$ is the unique one-parameter subgroup such, that the tangent vector to $\gamma(t)X$ at $t = 0$ is equal to X .

If G is a compact group, \exp enables to attain every element of the identity component of G from the level of \mathfrak{g} . In particular, \exp is a surjective map if G is also connected. In this case every element of G can be expressed as $\exp(X)$ for some $X \in \mathfrak{g}$.

2.3.2.5. Distances and volume in matrix Lie groups

Distance between two group elements is defined with a norm, i.e. a function acting in a vector space V that assigns *length* to every element of this space and is characterized with the following properties:

Definition 2.33. [11] Let v be an element of n -dimensional vector space V . A norm $\|\cdot\|$ is a real-valued function $\|\cdot\| : V \rightarrow \mathbb{R}_+ \cup \{0\}$, such, that

1. $\|\cdot\|$ is point-separative $\|v\| = 0 \Leftrightarrow v = 0 \ v \in V$.
2. $\|\cdot\|$ is absolutely scalable $\|cv\| = |c| \cdot \|v\|, c \in \mathbb{C}$.
3. $\|\cdot\|$ is subadditive $\|v_1 + v_2\| \leq \|v_1\| + \|v_2\|, v_1, v_2 \in V$.

The norm that we use in this thesis is the *Frobenius norm* defined as

$$\|U\| = \sqrt{\text{tr}UU^*} = \sqrt{\sum_{j=1}^d \sum_{k=1}^d |U_{j,k}|^2}, \quad U \in \mathbb{M}_d(\mathbb{C}), \quad (2.39)$$

where $\mathbb{M}_d(\mathbb{C})$ is the space of $d \times d$ matrices over \mathbb{C} . In what follows we introduce a concept of a *Haar measure* μ on G , where G is a compact Lie group. Haar measure enables to define integration on G and, intuitively speaking, compute *volumes* of subsets of G as

$$V(S) = \int_S d\mu(g) f(g), \quad S \subset G. \quad (2.40)$$

Definition 2.34. Let G be a compact matrix Lie group. Then there exists a bi-invariant Haar measure which is a Borel measure on G such, that for any Borel subset⁴ $S \subset G$ and any $g \in G$ holds

$$\mu(S) = \mu(gS) = \mu(Sg), \quad (2.41)$$

where $gS = \{h \in G, h = gs, s \in S\}$ and $Sg = \{h \in G, h = sg, s \in S\}$. Haar measure is unique up to a constant factor.

2.3.3. Representation theory of Lie groups and Lie algebras

In this section we present main concepts from the representation theory of Lie groups and Lie algebras. As the representation theory includes a wide range of topics, the reader is advised to consult the relevant literature [15, 29, 36, 50]. We begin our survey from general definitions, then we present the adjoint representation and its significance on the level of Lie groups and Lie algebras. The final part of this section is devoted to the concept of irreducibility and to Schur's lemma.

Definition 2.35. A representation Π of a Lie group G on a vector space V is a group homomorphism $\Pi : G \rightarrow GL(V)$, where $GL(V)$ is the group of linear transformations on V .

Definition 2.36. A representation π of a Lie algebra \mathfrak{g} on a vector space V is a Lie algebra homomorphism $\pi : \mathfrak{g} \rightarrow \mathfrak{gl}(V)$, where $\mathfrak{gl}(V)$ is the space of endomorphisms of V , equipped with the Lie bracket.

Definition 2.37. A representation Π or π , respectively is called faithful if it is injective.

Definition 2.38. Let $\Pi : G \rightarrow GL(V)$ be a representation of a Lie group G . Π is called reducible if there exists a proper subspace $W \subsetneq V$ that is preserved by G , i.e. $\Pi : W \rightarrow W$.

Assume that G is a compact and connected Lie group. In this case every element of G can be expressed as $\exp(X)$, where X belongs to the Lie algebra of G . In such a case representations of the Lie algebra can be derived from representations of the group by differentiation at the neutral element:

$$\pi(X) = \left. \frac{d}{dt} \right|_{t=0} \Pi(\exp(tX)). \quad (2.42)$$

In what follows we take particular emphasis on representations of compact connected matrix Lie groups and their Lie algebras. Among all possible representations a special role in Lie theory is played by the adjoint representation Ad , that arises naturally from the adjoint action of G on its Lie algebra \mathfrak{g} .

Definition 2.39. The adjoint representation of a Lie group G is a group homomorphism $\text{Ad} : G \rightarrow \text{Aut}(\mathfrak{g})$ given by the adjoint action

$$\text{Ad}_g X = gXg^{-1}, \quad g \in G, X \in \mathfrak{g}. \quad (2.43)$$

Definition of the adjoint representation of \mathfrak{g} has an analogous for and it can be obtained directly from Ad by differentiation at the neutral element. To show this, assume that $g = \exp(tX)$, where X belongs to \mathfrak{g} . Then for any $Y \in \mathfrak{g}$ we can write

$$\left. \frac{d}{dt} \right|_{t=0} \text{Ad}_g Y = \left. \frac{d}{dt} \right|_{t=0} (\exp(tX)Y \exp(-tX)) = XY - YX = \text{ad}_X Y.$$

⁴Borel set is a set that can be constructed from open or closed sets by taking countable intersections and unions [21].

Definition 2.40. The adjoint representation of a Lie algebra \mathfrak{g} is a Lie algebra homomorphism from \mathfrak{g} to the space of endomorphisms of \mathfrak{g} , $\text{ad} : \mathfrak{g} \rightarrow \text{End}(\mathfrak{g})$, given by the adjoint action of \mathfrak{g} on itself.

$$\text{ad}_X(Y) = [X, Y], \quad X, Y \in \mathfrak{g}. \quad (2.44)$$

2.3.3.1. Schur's lemma for complex, real and quaternion representations

In this section we introduce the concept of a real, complex and quaternion representation and define, what is the *type* of representation. All the presented facts and concepts are true for representations of compact Lie groups and Lie algebras, however we restrict the notation only to representations of Lie groups for brevity.

Definition 2.41. A complex representation Π of a Lie group G is a group homomorphism $\Pi : G \rightarrow GL(V)$, where V is a complex vector space.

Definition 2.42. A real vector space V can be thought as a complex vector space equipped with an invariant real structure, i.e. an antilinear map $j : V \rightarrow V$ commuting with a group multiplication that satisfies $j^2 = 1$.

Definition 2.43. A quaternionic vector space V can be thought as a complex vector space equipped with an invariant quaternionic structure, i.e. an antilinear map $j : V \rightarrow V$ commuting with a group multiplication that satisfies $j^2 = -1$.

Definition 2.44. A real/quaternionic representation Π of a Lie group G is a group homomorphism $\Pi : G \rightarrow GL(V)$, where V is a real or quaternionic vector space, respectively.

Definition 2.45. A representation Π which possess an additional structure that is a nonsingular symmetric (or skew-symmetric, respectively) G -invariant bilinear form $\Omega : \Pi \times \Pi \rightarrow \mathbb{K}$, where $\mathbb{K} = \mathbb{R}, \mathbb{C}, \mathbb{H}$ is of real (quaternionic) type. Otherwise Π is of complex type.

A fundamental result concerning representations of compact, semisimple Lie groups and Lie algebra is Schur's lemma. Its original formulation concerns complex representations however, in the latter part of this section we will show, how to generalize this result to real and quaternionic representations.

Lemma 2.13 (Schur [50]). Let Π, Π' be irreducible representations of a Lie group G on finite dimensional vector spaces V, V' , respectively. Assume that V, V' are the vector spaces over \mathbb{C} . Let $\omega : V \rightarrow V'$ be a linear map satisfying $\omega \Pi(g) = \Pi'(g) \omega$ for all $g \in G$. Then ω is either bijective or $\omega = 0$.

An immediate conclusion from Schur's lemma is that if Π is an irreducible complex representation of G on V , then $\omega : V \rightarrow V$ is a complex scalar. Theorem II.6.7 in [15] generalizes this result for real representations.

Theorem 2.14. [15] For a real irreducible representation of (1) real, (2) complex, (3) quaternion type the algebra of endomorphisms commuting with the representation matrices is isomorphic to (1) \mathbb{R} , (2) \mathbb{C} , (3) \mathbb{H} , respectively.

2.3.4. Semisimple Lie groups and Lie algebras

In this section we present an important class of Lie groups and their Lie algebras.

Definition 2.46. Ideal \mathfrak{i} of a Lie algebra \mathfrak{g} is a subalgebra of \mathfrak{g} such, that for every $X \in \mathfrak{g}$ and every $Y \in \mathfrak{i}$ holds $[X, Y] \in \mathfrak{i}$. An ideal is proper if it is different from \mathfrak{g} and $\mathbf{0}$.

It is worth stressing that for every Lie group G , normal subgroups of G correspond to ideals in $\mathfrak{g} = \text{Lie}(G)$, which can be easily shown by differentiation [50].

Definition 2.47. *A Lie algebra \mathfrak{g} is semisimple if it is a direct sum of ideals. If the only ideals in \mathfrak{g} are \mathfrak{g} and $\mathbf{0}$, then \mathfrak{g} is called simple.*

Examples of simple Lie algebras include i.a. $\mathfrak{su}(d)$ and $\mathfrak{so}(d)$ for $d \neq 4$. A canonical example of a semisimple Lie algebra is $\mathfrak{so}(4) = \mathfrak{so}(3) \oplus \mathfrak{so}(3)$ (more details can be found e.g. in Chapter 5 in [79]).

Fact 2.8. *Ideals in a Lie algebra \mathfrak{g} are invariant spaces for the adjoint representation of \mathfrak{g} .*

This fact results directly from the definition of ad and the invariance condition. Assume that X belongs to \mathfrak{i} which is an ideal of \mathfrak{g} and Y is an arbitrary element of \mathfrak{g} . By definition of the ideal we have immediately that $[X, Y] = \text{ad}_X(Y) = 0$. In particular, ad is an irreducible representation of \mathfrak{g} if \mathfrak{g} is a simple Lie algebra.

2.3.4.1. Killing form for semisimple Lie algebras

In this section we introduce the concept of a Killing form and present its useful properties for semisimple Lie algebras.

Definition 2.48. [29] *A Killing form $B(\cdot, \cdot)$ is a bilinear and symmetric form defined as*

$$B(X, Y) = \text{tr}(\text{ad}_X \cdot \text{ad}_Y), \quad X, Y \in \mathfrak{g}, \quad (2.45)$$

that is invariant under automorphisms of \mathfrak{g}

$$B(f(X), f(Y)) = B(X, Y), \quad f \in \text{Aut}(\mathfrak{g}). \quad (2.46)$$

and satisfies the associativity property

$$B([X, Y], Z) = B(X, [Y, Z]), \quad B(\text{ad}_X(Y), Z) = B(X, \text{ad}_Y(Z)). \quad (2.47)$$

Theorem 2.15 (Cartan's criterion). [19, 30] *A compact Lie algebra \mathfrak{g} over a field of characteristic zero is semisimple if and only if $B(\cdot, \cdot)$ on \mathfrak{g} is non-degenerate, i.e. $B(X, Y) = 0$ for all $Y \in \mathfrak{g}$ if and only if $X = 0$.*

Fact 2.9. [30] *Let \mathfrak{g} be a compact simple Lie algebra, then every bi-invariant form on \mathfrak{g} is proportional to the Killing form on \mathfrak{g} .*

Fact 2.10. [30] *Let \mathfrak{g} be a compact semisimple Lie algebra and $\mathfrak{i}, \mathfrak{j}$ be two ideals in \mathfrak{g} with zero intersection. Then $\mathfrak{i}, \mathfrak{j}$ are orthogonal with respect to the Killing norm.*

Proof. This fact results from associativity property of the Killing form (2.47). Let $X \in \mathfrak{i}, Y \in \mathfrak{j}$ and $Z \in \mathfrak{g}$ and notice that $[X, Y] = 0$ by definition of \mathfrak{i} and \mathfrak{j} . Then by (2.47) we get

$$B([X, Y], Z) = B(X, [Y, Z]) = 0, \quad \text{where } [Y, Z] \in \mathfrak{j}.$$

This means \mathfrak{i} and \mathfrak{j} are orthogonal with respect to the Killing form. □

Important conclusion from Fact 2.10 is that the Killing form enables to decompose a semisimple Lie algebra \mathfrak{g} to a direct sum of non-intersecting ideals. In particular, if $\mathfrak{g} = \mathfrak{i} \oplus \mathfrak{j}$, then \mathfrak{j} is called an *orthogonal complement* of \mathfrak{i} . In what follows we will denote it by \mathfrak{i}^\perp .

Finally, let us mention relations between the Killing form and topology of compact semisimple Lie groups. Assume that G is such a group and let \mathfrak{g} be the Lie algebra of G . Recall that if \mathfrak{g} is compact and semisimple, then $B(\cdot, \cdot)$ is a non-degenerate and negative definite bilinear form. Inverting its sign to $-B(\cdot, \cdot)$ we obtain a Riemannian metric called *Cartan-Killing metric* on a group manifold. Then elements of the metric tensor can be found as

$$g_{ij} = -B(X_i, X_j),$$

where $X_i, X_j, i, j = 1, \dots, \dim \mathfrak{g}$ are basis elements of \mathfrak{g} . By the fact that the Killing form is Ad-invariant we can conclude that the adjoint action of a Lie group G preserves distances on \mathfrak{g} , this implies $\text{Ad} : G \rightarrow SO(\mathfrak{g})$.

2.4. Main facts about $SU(d)$ and $SO(d)$

In this section we give a survey of main facts about the groups $SU(d)$ and $SO(d)$, which play a prominent role in this thesis, and their Lie algebras. We start from recalling the definitions:

$$SO(d) = \{O \in \text{Gl}_d(\mathbb{R}) : O^t O = I, \det O = 1\}, \quad (2.48)$$

$$SU(d) = \{U \in \text{Gl}_d(\mathbb{C}) : U^* U = I, \det U = 1\}. \quad (2.49)$$

Their corresponding Lie algebras are the spaces formed by the following matrices:

$$\mathfrak{so}(d) = \{X \in \text{Mat}_d(\mathbb{R}) : X^t = -X, \text{tr } X = 0\}, \quad (2.50)$$

$$\mathfrak{su}(d) = \{X \in \text{Mat}_d(\mathbb{C}) : X^* = -X, \text{tr } X = 0\}. \quad (2.51)$$

In what follows we will introduce an orthonormal basis in $\mathfrak{su}(d)$ and $\mathfrak{so}(d)$. Let $E_{k,l} = |k\rangle\langle l|$ be a $d \times d$ matrix whose only nonzero (and equal to 1) entry is (k, l) . Such matrices satisfy the commutation relation $[E_{ij}, E_{kl}] = \delta_{jk} E_{il} - \delta_{li} E_{kj}$. $E_{k,l}$'s are building blocks for basis elements of $\mathfrak{su}(d)$ and $\mathfrak{so}(d)$.

$$\mathfrak{su}(d) = \text{Span}\{X_{j,k}, Y_{j,k}, Z_{j,k}\}, \quad j \neq k, j, k = 1, \dots, d, \quad (2.52)$$

$$X_{j,k} = E_{j,k} - E_{k,j}, \quad Y_{j,k} = i(E_{j,k} + E_{k,j}), \quad Z_{j,k} = i(E_{j,j} - E_{k,k}). \quad (2.53)$$

Notice that $\mathfrak{so}(d)$ is a subgroup of $\mathfrak{su}(d)$ consisting of only real matrices, thus the orthonormal basis of $\mathfrak{so}(d)$ is restricted to $\{X_{j,k}\}$. We will call these two bases the standard basis of $\mathfrak{su}(d)$ and $\mathfrak{so}(d)$ respectively.

Fact 2.11. [36, 50] *The center of $SU(d)$ is finite and given by $Z(SU(d)) = \{\alpha I : \alpha^d = 1\}$.*

Fact 2.12. [36, 50] *The center of $SO(d)$ is either trivial for $d = 2k+1$ or $Z(SO(d)) = \{-I, I\}$ for $d = 2k$.*

It is worth recalling that groups $SU(d)$ for $d \geq 2$ and groups $SO(d)$ for $d \geq 3$ and $d \neq 4$ are compact connected simple Lie groups, what has been shown in Sections 2.3.1 and 2.3.4.

Fact 2.13. *The Killing form on $\mathfrak{su}(d)$ and $\mathfrak{so}(d)$ is equal to $B(X, Y) = \text{tr } XY$ up to a constant positive factor.*

In the rest of this section we present additional facts about the adjoint representation of unitary and orthogonal groups. Recall that for $g \in G$, where $G = SU(d)$ or $G = SO(d)$, Ad_g is an orthogonal transformation acting on $\dim G$ dimensional vector space \mathfrak{g} . Upon a choice of an orthonormal basis $\{X_i\}_{i=1}^{\dim G}$ in \mathfrak{g} , i.e. basis that satisfies $(X_i | X_j) = -\text{tr}(X_i X_j) = \delta_{ij}$ the

transformation Ad_g can be expressed in this basis as a matrix belonging to $SO(\dim \mathfrak{g})$. The entries of this matrix, denoted by $(\text{Ad}_g)_{ij}$, are defined by the identity:

$$\text{Ad}_U X_j = U^{-1} X_j U = \sum_{i=1}^d (\text{Ad}_U)_{ij} X_i, \quad (2.54)$$

therefore they are given by

$$(\text{Ad}_U)_{ij} = -\frac{1}{2} \text{tr} (X_i U X_j U^{-1}). \quad (2.55)$$

The following result, that we have proven in [71], turns out to be essential in formulating the universality criteria in Chapter 4.

Fact 2.14. [71] *The adjoint representation of $SU(d)$ and $SO(d)$, $d \neq 4$, such as the adjoint representation of $\mathfrak{su}(d)$ and $\mathfrak{so}(d)$, $d \neq 4$, is a (1) real, (2) irreducible representation (3) of real type.*

Proof. In what follows we will denote $G = SO(d)$, $d \neq 4$ or $G = SU(d)$ and $\mathfrak{g} = \mathfrak{so}(d)$, $d \neq 4$ or $\mathfrak{g} = \mathfrak{su}(d)$. Properties (1) and (2) come from the fact that G is a compact, connected real simple Lie group.

In order to prove (3) we can use facts presented in [15]. From Table II.6.2 we learn that Ad is of real type if its complexification is a complex representation of real type. This condition can be checked using Proposition II.6.4

Proposition 2.16 (Proposition II.6.4. [15]). *A complex representation $\Pi : G \rightarrow GL(V)$ of a Lie group G is of real/quaternionic type if and only if there exists a nonsingular symmetric or skew-symmetric, respectively G -invariant bilinear form $B : V \times V \mapsto \mathbb{C}$.*

Recall that for $\mathfrak{g} = \mathfrak{su}(d)$ and $\mathfrak{g} = \mathfrak{so}(d)$, $d \neq 4$ such a symmetric bi-invariant form is precisely the Killing form. Thus in order to apply Proposition 2.16 we need to define the Killing form for the complexification of \mathfrak{g} :

$$B^{\mathbb{C}}(X, Y) = \text{tr}(\text{ad}_X \text{ad}_Y), \quad X, Y \in \mathfrak{g}^{\mathbb{C}}.$$

However, we can assume here that the basis of \mathfrak{g} over \mathbb{R} is a basis of $\mathfrak{g}^{\mathbb{C}}$ over \mathbb{C} . Thus we get immediately that $B^{\mathbb{C}}(\cdot, \cdot)$ is a non-degenerate, symmetric, Ad -invariant bilinear form on $\mathfrak{g}^{\mathbb{C}}$. Hence by Proposition 2.16 the complexification of Ad (and ad , respectively) is a complex representation of real type. The result follows. \square

2.4.0.2. Distance inequality for the group commutator

This paragraph includes a distance inequality that will play an essential role in Section 4.2.1. The inequality describes, how the distance between the group commutator of two unitary matrices U_1, U_2 and I depends on the distances between these matrices and I .

Lemma 2.17. [22] *Let $U_1, U_2 \in SU(d)$ and let $U = [U_1, U_2]_{\bullet}$ (see definition of $[\cdot]_{\bullet}$ in Section 2.3.2). We have the following:*

$$\|[U_1, U_2]_{\bullet} - I\| \leq \sqrt{2} \|U_1 - I\| \|U_2 - I\|, \quad (2.56)$$

$$\text{If } [U_1, [U_1, U_2]_{\bullet}]_{\bullet} = I \text{ and } \|U_2 - I\| < 2, \text{ then } [U_1, U_2]_{\bullet} = I. \quad (2.57)$$

Proof. The proof presented in this thesis is based on [22]. In what follows we will denote the matrix elements by $U_{1;j,k}$, $U_{2;j,k}$ and assume, without loss of generality, that U_2 is diagonal. Let us start from (2.56). Unitary invariance of the Frobenius norm allows to transform the left hand side of (2.56) as

$$|[U_1, U_2]_{\bullet} - I| = \|U_1 U_2 U_1^{-1} U_2^{-1} - I\| = \|U_1 U_2 - U_2 U_1\| = \|(U_1 - I)U_2 + U_2(I - U_1)\|.$$

Next, use formula (2.39) to make the norm dependent on matrix elements.

$$\begin{aligned} \|(U_1 - I)U_2 + U_2(I - U_1)\| &= \sqrt{\text{tr}((U_1 - I)U_2 + U_2(I - U_1)) \cdot ((U_1^* - I)U_2^* + U_2^*(I - U_1^*))} = \\ &= \sqrt{\sum_{j,k} |(U_{1;j,k} - \delta_{j,k})U_{2;k,k} + U_{2;j,j}(U_{1;j,k} - \delta_{j,k})|^2} = \sqrt{\sum_{j,k} (|U_{1;j,k} - \delta_{j,k}|^2 |U_{2;k,k} - U_{2;j,j}|^2)}. \end{aligned}$$

Notice that $\sqrt{\sum_{j,k} |U_{1;j,k} - \delta_{j,k}|^2} = \sqrt{\text{tr}(U_1 - I)(U_1^* - I)} = \|U_1 - I\|$. On the other hand for any $j, k = 1, \dots, d$ we have

$$\begin{aligned} |U_{2;k,k} - U_{2;j,j}|^2 &= |(1 - U_{2;k,k}) - (1 - U_{2;j,j})|^2 \leq (|1 - U_{2;k,k}| + |1 - U_{2;j,j}|)^2 \leq \\ &\leq 2(|1 - U_{2;k,k}|^2 + |1 - U_{2;j,j}|^2), \end{aligned}$$

hence $\sqrt{\sum_{j,k} |U_{2;k,k} - U_{2;j,j}|^2} \leq \sqrt{2} \sqrt{\sum_j |1 - U_{2;j,j}|} = \sqrt{2} \|U_2 - I\|$. Summing up we get the final formula (2.56).

In order to prove (2.57) we start from the following observation: if U_1 commutes with $[U_1, U_2]_{\bullet}$, it commutes also with $U_2 U_1 U_2^{-1}$, thus we can replace U_1 and $U_2 U_1 U_2^{-1}$ with their diagonalized forms. Note that, however, U_1 and $U_2 U_1 U_2^{-1}$ have the same roots of the characteristic polynomial, hence one can find a permutation matrix P such, that

$$U_2 U_1 U_2^{-1} = P^{-1} U_1 P.$$

Let us define the matrix $V = P U_2$ and notice that $U_1 V = V U_1$. Hence we can assume without loss of generality that V is also diagonal. On the other hand, let $[U_1, U_2]_{\bullet} \neq I$, which implies also that $[U_2, P]_{\bullet} \neq I$. Assuming that P is of the form

$$P = \begin{pmatrix} P_{1,1} & \dots & P_{1,d} \\ \vdots & \ddots & \vdots \\ P_{d,1} & \dots & P_{d,d} \end{pmatrix},$$

this means that some $P_{j,k}$'s above the diagonal and below the diagonal must be nonzero. There must be at least two non-zero non-diagonal entries of P . In what follows we will denote them by $P_{j,k} = 1$ and $P_{l,m} = 1$. We get

$$\begin{aligned} \|I - U_2\| &= \|P(I - U_2)\| = \|P - V\| \geq \\ &\geq \sqrt{|P_{j,k} - V_{j,k}|^2 + |P_{l,m} - V_{l,m}|^2 + \sum_n |P_{j,n} - V_{j,n}|^2 + \sum_n |P_{l,n} - V_{l,n}|^2}. \end{aligned}$$

As V is diagonal we have $|P_{j,k} - V_{j,k}|^2 = 1 - 0 = 1$, $|P_{l,m} - V_{l,m}|^2 = 1 - 0 = 1$ and

$$\sum_n |P_{j,n} - V_{j,n}|^2 + \sum_n |P_{l,n} - V_{l,n}|^2 = \sum_n V_{j,n}^2 + \sum_n V_{l,n}^2$$

and each of these sums is equal to one, which stems from (2.32). Hence $\|P - V\| \geq \sqrt{4} = 2$. \square

2.4.0.3. Fundamental facts about $SU(2)$ and $SO(3)$

In this section we restrict our interest to the smallest nonabelian unitary group $SU(2)$ and its adjoint representation $\text{Ad} : SU(2) \rightarrow SO(3)$. Both of these groups have interesting physical interpretation. First, $SU(2)$ is known in quantum information community as the group of unitary operations acting on a single qubit. In physicists' formalism every pure state of a qubit can be represented as a point on a Bloch sphere, i.e. a two-dimensional sphere in a space of states [60] (see Figure 2.1), where the north pole and south pole correspond to states $|0\rangle$ and $|1\rangle$, respectively. In this formalism unitary operations can be thought as rotations on the Bloch sphere. On the other hand elements of $SO(3)$ describe rotations in 3-dimensional real space. Therefore in the rest of this thesis we will often call elements of $SU(2)$ and $SO(3)$ *rotation matrices* or *rotations*. In the following we present commutator relations for the Lie algebras

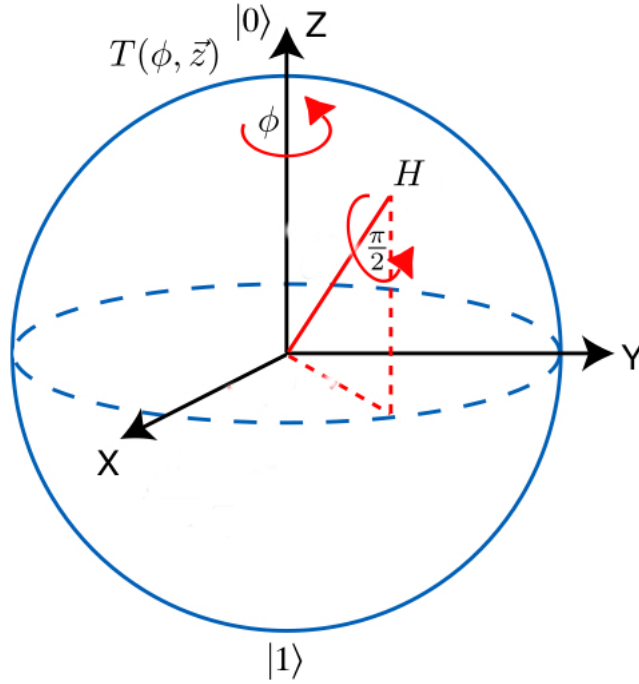


Figure 2.1: Bloch sphere with denoted Hadamard matrix and the rotation matrix by angle ϕ around the axis \vec{k}_z . In general every unitary gate $U(\phi, \vec{k})$ is a rotation by angle ϕ around the axis $\vec{k} = (k_x, k_y, k_z)$.

$\mathfrak{su}(2)$ and $\mathfrak{so}(3)$ and show the relations between the corresponding Lie groups.

Definition 2.49. The Lie algebra $\mathfrak{su}(2)$ is a real 3-dimensional space of 2×2 anti-Hermitian matrices, equipped with a matrix commutator $[\cdot, \cdot]$. The canonical orthogonal basis of $\mathfrak{su}(2)$ consists of

$$X = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad (2.58)$$

which satisfy the commutation relations

$$[X, Y] = 2Z, \quad [Y, Z] = 2X, \quad [X, Z] = -2Y. \quad (2.59)$$

It is worth mentioning differences in notation in mathematical and physical textbooks. In physicists' notation elements of $SU(d)$ are defined as $\exp(iH)$, where H is a Hermitian matrix. The difference stems from the fact that Hermitian matrices have interpretation as the finite-dimensional operators representing observables like energy, spin etc. As for example, physicists

often considered *Pauli matrices* $\sigma_x, \sigma_y, \sigma_z$ as basis elements of $\mathfrak{su}(2)$ and in this setting the commutation relations take the form $[\sigma_j, \sigma_k] = i2\epsilon_{jkl}\sigma_l$, when ϵ_{jkl} is the Levi-Civita symbol.

Definition 2.50. *The Lie algebra $\mathfrak{so}(3)$ is a real space of 3×3 anti-symmetric matrices, of the dimension $\dim \mathfrak{so}(3) = 3$, equipped with a matrix commutator $[\cdot, \cdot]$.*

The canonical orthogonal basis of $\mathfrak{so}(3)$ consists of the vectors

$$X_{1,2} = \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad X_{1,3} = \begin{pmatrix} 0 & 0 & -1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad X_{2,3} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}, \quad (2.60)$$

which satisfy the commutation relations

$$[X_{23}, X_{13}] = -X_{12}, \quad [X_{23}, X_{12}] = X_{13}, \quad [X_{13}, X_{12}] = X_{23}. \quad (2.61)$$

Fact 2.15. *Adjoint representation of $\mathfrak{su}(2)$ is the standard representation of $\mathfrak{so}(3)$.*

Fact 2.15 can be easily proven by direct calculations. Notice, that the commutation relations (2.59) and (2.61) are identical up to a constant factor $c = 2$. This means $\mathfrak{su}(2)$ and $\mathfrak{so}(3)$ are isomorphic through the adjoint representation. The isomorphism is established by:

$$X \rightarrow \text{ad}_X = -2X_{23},$$

$$Y \rightarrow \text{ad}_Y = 2X_{13},$$

$$Z \rightarrow \text{ad}_Z = -2X_{12}.$$

On the level of Lie groups $SU(2)$ is a *double cover* of $SO(3)$, i.e. the map $\text{Ad} : SU(2) \rightarrow SO(3)$ is a continuous group homomorphism and $SO(3)$ has index 2 in $SU(2)$ ⁵. The relation between elements of $SU(2)$ and $SO(3)$ is the following:

$$e^X \rightarrow \exp(\text{ad}_X) = \exp(-2X_{23}), \quad (2.62)$$

$$e^Y \rightarrow \exp(\text{ad}_Y) = \exp(2X_{13}), \quad (2.63)$$

$$e^Z \rightarrow \exp(\text{ad}_Z) = \exp(-2X_{12}). \quad (2.64)$$

2.4.0.4. Parameterization of $SU(2)$ and $SO(3)$

There are many equivalent parameterizations of elements of $SU(2)$ and $SO(3)$. We will use throughout this thesis the axis-angle parameterization as the most appropriate for our needs. According to the axis-angle representation, every element $O \in SO(3)$ and $U \in SU(2)$ depends on parameters ϕ , which will be called *spectral angle* or the *angle of rotation* interchangeably, and $\vec{k} = (k_x, k_y, k_z)$, $|\vec{k}| = 1$, which is the rotation axis. The axis-angle parameterization arises naturally from the Cayley-Hamilton theorem, which was mentioned in Section 2.2.3.

Theorem 2.18 (Cayley-Hamilton). *Every $d \times d$ matrix M over a commutative ring (such as the real or complex field) is annihilated by its characteristic polynomial $\chi_M(x) = \det(Ix - M) = \sum_{i=0}^d c_i x^i$, i.e.*

$$\chi_M(M) = \sum_{i=0}^d c_i M^i = 0 \quad (2.65)$$

⁵In other words, adjoint representation maps two elements of $SU(2)$ to one element from $SO(3)$, see also Fact 2.16.

An immediate consequence of Theorem 2.18 is that $\exp(M)$ can be expressed as a polynomial of degree $d - 1$ in M . Direct calculations for $SU(2)$ and $SO(3)$ provide:

$$SU(2) : U(\phi, \vec{k}) = e^{\phi \vec{k} \cdot (X, Y, Z)} = I \cos \phi + \vec{k} \cdot (X, Y, Z) \sin \phi, \quad (2.66)$$

$$SO(3) : O(\phi, \vec{k}) = e^{\phi(-k_x X_{2,3} + k_y X_{1,3} - k_z X_{1,2})} = \quad (2.67)$$

$$I + \vec{k} \cdot (-X_{2,3}, X_{1,3}, -X_{1,2}) \sin \phi - 2 \sin^2 \frac{\phi}{2} \left(\vec{k} \cdot (-X_{2,3}, X_{1,3}, -X_{1,2}) \right)^2. \quad (2.68)$$

The angle-axis parameterization enables to compute easily a product of two unitary gates

$$U(\phi_1, \vec{k}_1) \cdot U(\phi_2, \vec{k}_2) = U(\gamma, \vec{k}_{12}), \quad \text{where} \quad (2.69)$$

$$\cos \gamma = \cos \phi_1 \cos \phi_2 - \sin \phi_1 \sin \phi_2 \vec{k}_1 \cdot \vec{k}_2, \quad (2.70)$$

$$\vec{k}_{12} = \frac{1}{\sin \gamma} \left(\vec{k}_1 \sin \phi_1 \cos \phi_2 + \vec{k}_2 \sin \phi_2 \cos \phi_1 + \vec{k}_1 \times \vec{k}_2 \sin \phi_1 \sin \phi_2 \right). \quad (2.71)$$

Fact 2.16. Let $U(\phi, \vec{k}) \in SU(2)$. Then the adjoint representation of $U(\phi, \vec{k})$ expressed in the axis-angle parameterization is of the form

$$\text{Ad} : U(\phi, \vec{k}) \rightarrow O(2\phi, \vec{k}) \in SO(3), \quad (2.72)$$

which is a direct generalization of (2.62, 2.63, 2.64).

We should emphasize that the image of Ad_G is the group of all automorphisms of G by Definition 2.40. In case of $SU(2)$ this implies, that automorphisms of $SU(2)$ are in one to one correspondence with elements of $SO(3)$. Let us denote an example automorphism by $\Phi_{O(\gamma, \vec{k}')} : SU(2) \rightarrow SU(2)$, where $O(\gamma, \vec{k}') \in SO(3)$. Then $\Phi_{O(\gamma, \vec{k}')}$ is defined as

$$\Phi_{O(\gamma, \vec{k}')} (U(\phi, \vec{k})) = U(\phi, O(\gamma, \vec{k}') \vec{k}). \quad (2.73)$$

2.4.0.5. Finite subgroups of $SU(2)$

In this section we briefly describe finite subgroups of $SU(2)$. To this end we need to define first what is a *group extension*.

Definition 2.51. Let A, B be groups. A group extension of A by B is the group G such, that

$$1 \rightarrow A \rightarrow G \rightarrow B \rightarrow 1, \quad (2.74)$$

where the homomorphism $A \rightarrow G$ is injective, i.e. A is isomorphic to its image, and the homomorphism $G \rightarrow B$ is surjective such, that B is isomorphic to a quotient group G/A .

Definition 2.52. A group extension is central if, for the same notation as for Definition 2.51, $A \subset G$ is contained in the center of G .

The finite subgroups of $SU(2)$ are strongly related to the finite subgroups of $SO(3)$, which are defined in terms of so called *von Dyck groups*.

Definition 2.53. [56] The von Dyck groups have the following geometric interpretation. Consider a triangle with the sides $\{\frac{\pi}{l}, \frac{\pi}{m}, \frac{\pi}{n}\}$. Then a von Dyck group (l, m, n) is a group of rotations by angles $\frac{2\pi}{l}, \frac{2\pi}{m}, \frac{2\pi}{n}$ about the corresponding vertices. The canonical representation of this group is numbered by three integers. The von Dyck group (l, m, n) is a finite group with the following presentation:

$$(l, m, n) = \{a, b, c | a^l = b^m = c^n = abc = e\}, \quad (2.75)$$

where e is the identity element of the group.

Nonabelian finite subgroups of $SO(3)$ include $(2, 2, n)$, $n \geq 3$, $(2, 3, 3)$, $(2, 3, 4)$ and $(2, 3, 5)$. The first of these groups is called *dihedral group* and is a symmetry group of the plane. The following three groups are the symmetry group of a tetrahedron, an octahedron and an icosahedron, respectively.

By the homomorphism $\text{Ad} : SU(2) \rightarrow SO(3)$ the finite nonabelian subgroups of $SU(2)$, denoted by $\langle l, m, n \rangle$, can be regarded as central extensions of the finite nonabelian subgroups of $SO(3)$ by the group \mathbb{Z}_2 . The extension has a structure of the Cartesian product

$$\langle l, m, n \rangle = (l, m, n) \times \mathbb{Z}_2. \quad (2.76)$$

The following list includes all finite nonabelian subgroups of $SU(2)$:

- Dicyclic group $\langle 2, 2, n \rangle = (2, 2, n) \times \mathbb{Z}_2$ is the central extension of the dihedral group $(2, 2, n)$. The group $(2, 2, n)$ is generated by two rotations by $\pm\pi$ about axes \vec{k}_1 and \vec{k}_2 separated by an angle $\frac{\pi}{n}$. Their product is a rotation along $\vec{k}_1 \times \vec{k}_2$ by $\frac{2\pi}{n}$. The spectral angles for elements in $\langle 2, 2, n \rangle \subset SU(2)$ are therefore $\frac{k\pi}{2}$ and $\frac{k\pi}{n}$ whereas the possible angles between axes are equal $\{\frac{\pi}{2}, \frac{\pi}{n}\}$.
- Binary tetrahedral group $\langle 2, 3, 3 \rangle = (2, 3, 3) \times \mathbb{Z}_2$ is the central extension of the tetrahedral group $(2, 3, 3) \simeq A_4$. The group $(2, 3, 3)$ is a symmetry group of the regular tetrahedron and consists of rotations by $\frac{2k\pi}{3}$ about axes $\vec{k}_1, \vec{k}_2, \vec{k}_3$ and \vec{k}_4 such that $\vec{k}_i \cdot \vec{k}_j = -\frac{1}{3}$ and of rotations by $k\pi$ about axes \vec{l}_1, \vec{l}_2 and \vec{l}_3 such that $\vec{l}_i \cdot \vec{l}_j = 0$ and $\vec{k}_i \cdot \vec{l}_j = \pm\frac{1}{\sqrt{3}}$. The spectral angles for elements in $\langle 2, 3, 3 \rangle$ are therefore: $\frac{k\pi}{3}$ and $\frac{k\pi}{2}$. The axes and angles between them are as in $(2, 3, 3)$ albeit $\vec{k}_i \cdot \vec{k}_j = \pm\frac{1}{3}$.
- Binary octahedral group $\langle 2, 3, 4 \rangle = (2, 3, 4) \times \mathbb{Z}_2$ is a central extension of the octahedral group $(2, 3, 4) \simeq S_4$. The group $(2, 3, 4)$ is a symmetry group of the regular octahedron (or, equivalently, of a cube) and consists of rotations by $k\pi$ and $\frac{k\pi}{2}$ about axes $\vec{k}_1, \vec{k}_2, \vec{k}_3$ and \vec{k}_4 such that $\vec{k}_i \cdot \vec{k}_j = 0$, of rotations by $k\pi$ about the axes $\vec{l}_1, \dots, \vec{l}_6$ for which $\vec{l}_i \cdot \vec{l}_j = 0$ and of rotations by $\frac{2k\pi}{3}$ about axes $\vec{v}_1, \vec{v}_2, \vec{v}_3$ and \vec{v}_4 such that $\vec{v}_i \cdot \vec{v}_j = \pm\frac{1}{3}$. The angles between the axes corresponding to different rotations are the following: $\vec{k}_i \cdot \vec{l}_j = \pm\frac{1}{\sqrt{2}}$, $\vec{k}_i \cdot \vec{v}_j = \pm\frac{2}{\sqrt{6}}$ and $\vec{l}_i \cdot \vec{v}_j = \pm\frac{1}{\sqrt{3}}$. The spectral angles for elements in $\langle 2, 3, 4 \rangle$ are therefore: $\frac{k\pi}{3}$, $\frac{k\pi}{4}$ and $\frac{k\pi}{2}$. The axes and angles between them are as in $(2, 3, 4)$.
- Binary icosahedral group $\langle 2, 3, 5 \rangle = (2, 3, 5) \times \mathbb{Z}_2$ is a central extension of the symmetry group of a regular icosahedron (or, equivalently, a regular dodecahedron) $(2, 3, 5) \simeq A_5$. The group $\langle 2, 3, 5 \rangle$ consists of rotations by $\frac{k\pi}{2}$ with the angles between rotation axes $\vec{k}_i \cdot \vec{k}_j \in \{0, \pm\frac{1}{3}, \pm\frac{\sqrt{5}}{3}\}$, of rotations by $\frac{2k\pi}{3}$ with the angles between rotation axes $\vec{l}_1, \dots, \vec{l}_{10}$ take values $\vec{l}_i \cdot \vec{l}_j = \pm\frac{\sqrt{5}}{3}$ and of rotations by $\frac{k\pi}{5}$ and $\frac{2k\pi}{5}$ where k is an odd number and the angle between rotation axes $\vec{v}_1, \dots, \vec{v}_6$ is equal $\vec{v}_i \cdot \vec{v}_j = \pm\frac{1}{\sqrt{5}}$.

2.5. Spectral gaps of averaging operators

In this section we present basic concepts from theory of spectral gaps of averaging operators on compact Lie groups. We start from presenting basic definitions and next we discuss connections between the spectral gaps and efficiently universal sets of gates (see Definition 1.7).

In Section 2.3.3 we presented examples of finite dimensional representations of compact matrix Lie groups. However, this concept can be extended to infinite dimensional spaces, i.e. spaces

of functions. To this end assume, that f is a square-integrable function acting on a space V . Then the infinite-dimensional representation of $SU(d)$ can be defined as

$$\Pi_U^\infty(f)(V) = f(U^{-1}V), \quad U, V \in SU(d). \quad (2.77)$$

Definition 2.54. Denote the space of square-integrable functions acting on $SU(d)$ by $L^2(SU(d))$ and let $\mathcal{S} = \{U_1, \dots, U_k\}$ be a finite subset of $SU(d)$. An averaging operator $T_{\mathcal{S}}$ acting on a function $f \in L^2(SU(d))$ is defined as

$$(T_{\mathcal{S}}f)(V) = \frac{1}{2|\mathcal{S}|} \sum_{U_i \in \mathcal{S}} (f(U_i V) + f(U_i^{-1}V)), \quad V \in SU(d). \quad (2.78)$$

In what follows we will call $(\tilde{U}f)(g) = f(U^{-1}g)$ *shifting operators*.

It is known [41] that eigenvalues of a Hermitian operator are bounded by its norm. Hence, in order to find the largest eigenvalue of $T_{\mathcal{S}}$ we first calculate its norm. The operator norm is defined as

$$\|T\|_{\text{op}} := \sup_{f \in L^2(SU(d))} \frac{\|Tf\|_2}{\|f\|_2},$$

where $\|\cdot\|_2$ is the usual L^2 norm. As U, g are elements of a unitary group the shifting operators $(\tilde{U}f)(g) = f(U^{-1}g)$ are also unitary and hence their operator norm is 1. Using triangle inequality, we get

$$\|T_{\mathcal{S}}\|_{\text{op}} \leq \frac{1}{2|\mathcal{S}|} \cdot 2|\mathcal{S}| = 1$$

as the sum is over $2|\mathcal{S}|$ shifting operators. However, by the fact that the constant function $f = 1$ is the eigenvector of $T_{\mathcal{S}}$ with the eigenvalue $\lambda_0 = 1$, we get that $\|T_{\mathcal{S}}\|_{\text{op}} = 1$.

Let $L_0^2(SU(d))$ denote the subspace of $L^2(SU(d))$ containing functions with the vanishing mean:

$$L_0^2(SU(2)) = \{f \in L^2(SU(2)) : \int_{SU(2)} f d\mu = 0\}.$$

Consider the operator $T_{\mathcal{S}}$ restricted to this space. We will denote it by $T_{\mathcal{S}}|_{L_0^2(SU(d))}$. The norm of this operator is $\|T_{\mathcal{S}}|_{L_0^2(SU(d))}\| = 1$ if and only if 1 is an accumulation point of the spectrum of $T_{\mathcal{S}}$. Otherwise it is strictly less than 1 and we will denote it by λ_1 . In this case we say that $T_{\mathcal{S}}$ has a spectral gap.

Definition 2.55. A spectral gap $\text{Gap}_{\mathcal{S}}$ is defined as


$$\text{Gap}_{\mathcal{S}} = 1 - \sup_f \{\|T_{\mathcal{S}}f\| : f \in L_0^2(SU(2))\}. \quad (2.79)$$

Equivalently,

$$\text{Gap}_{\mathcal{S}} = 1 - \lambda_1, \quad (2.80)$$

where λ_1 is either the second largest eigenvalue, if exists, or $T_{\mathcal{S}}$ or the accumulation point of the eigenvalues of $T_{\mathcal{S}}$.

As we mentioned at the beginning of this section, a spectral gap of $T_{\mathcal{S}}$ for a given set \mathcal{S} of audit gates gives us information if \mathcal{S} is efficiently universal. Recall from Section 1.1, that \mathcal{S} is

$$\left| \sigma \left(T_{\mathcal{S}}|_{L_0^2(SU(d))} \right) \right|$$


said to be efficiently universal if every unitary operation $U \in SU(d)$ can be approximated with accuracy ϵ using words of the length

$$L = O \left(\log \frac{1}{\epsilon} \right),$$

which is significantly better than the scaling $L = O \left(\log^c \frac{1}{\epsilon} \right)$, $c \simeq 4$ provided by Solovay-Kitaev theorem. For this reason, the problem of computing a spectral gap of $T_{\mathcal{S}}$ for an arbitrary \mathcal{S} is of great practical importance in quantum computing.

The history of the spectral gap theory started in 1958 with the PhD thesis of Harry Kesten [46] who was studying symmetric random walks on countable groups. Another important paper about this topic presented joint work of Lubotzky and Sarnak [55] and considered distribution of points on two-dimensional sphere under the action of $SO(3)$. This problem can be easily translated to the problem of qubit gates as the adjoint representation maps qubit gates to elements of $SO(3)$, $\text{Ad} : SU(2) \rightarrow SO(3)$, and $SO(3)$ acts transitively on a sphere in 3-dimensional real space [58].

As it was shown in [46] and [55], the absolute value of λ_1 in case, when

$$\mathcal{S} = \{U(\phi_1, \vec{k}_1), \dots, U(\phi_n, \vec{k}_n), U^{-1}(\phi_1, \vec{k}_1), \dots, U^{-1}(\phi_n, \vec{k}_n)\} \subset SU(2)$$

is bounded by

$$\sqrt{\frac{2n-1}{n^2}} \leq \lambda_1 \leq 1, \quad (2.81)$$

and it corresponds to the case, when elements of \mathcal{S} are uniformly distributed in the group. However, computing a spectral gap is a very difficult task in general and the only group for which some efficiently universal sets have been already found is $SU(2)$ [55, 63, 68].

According to our knowledge one of the first papers connecting existence of a spectral gap with optimality of a universal set was [39]. Its authors have proven that a universal set is efficiently universal if the averaging operator defined for \mathcal{S} has a nonzero spectral gap.

Theorem 2.19 (Harrow et. al., '02). [39] *A universal set \mathcal{S} is efficiently universal if the averaging operator $T_{\mathcal{S}}$ has a nonzero spectral gap.*

However, the presented proof is not constructive and it does not provide an algorithm that allows to approximate an arbitrary gate from $SU(d)$ with elements of \mathcal{S} [39]. In next years Bourgain and Gamburd gave a condition for matrix entries of \mathcal{S} providing that $T_{\mathcal{S}}$ has a nonzero spectral gap. The proof of this theorem can be found in [9, 10] for $SU(2)$ and $SU(d)$, respectively.

Theorem 2.20 (Bourgain-Gamburd, '15). *The averaging operator defined on a universal set $\mathcal{S} \subset SU(d)$ has a nonzero spectral gap if all elements of \mathcal{S} have algebraic matrix entries.*

Chapter 3

Field theory and universality

In this chapter we present a simple and mathematically strict method of deciding universality for two sets of one-qubit gates that play a particularly important role in quantum information theory. Our approach is inspired by the proof presented by Nielsen and Chuang (see [13] and Section 4.5.3 in [60]) and based on elements of field theory and number theory. In our approach we also apply the solution of Burnside problem (see Theorem 2.5) and companion matrix formalism. Finally, we use special classes of minimal polynomials, i.e. *trigonometric* and *cyclotomic* polynomials as the main tool of our proof. They will be described in details in Section 3.2.

The first set that we consider in this chapter consists of the Hadamard gate H , where H is defined in (3.2), and the phase shift gate (T-gate) $T(\phi)$. In what follows we will denote this set by $\mathcal{S}_\phi^{H,T}$, where ϕ plays a role of a parameter:

$$\mathcal{S}_\phi^{H,T} = \{H, T(\phi)\}, \quad (3.1)$$

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} i & i \\ i & -i \end{pmatrix}, \quad T(\phi) = \begin{pmatrix} e^{i\phi} & 0 \\ 0 & 1 \end{pmatrix} = e^{i\phi/2} \begin{pmatrix} e^{i\phi/2} & 0 \\ 0 & e^{-i\phi/2} \end{pmatrix}. \quad (3.2)$$

In the rest of this chapter we will omit the factor $e^{i\phi/2}$ and consider the T-gate as the rotation on the Bloch sphere about \vec{k}_z by angle $\frac{\phi}{2}$. This substitution simplifies the calculations but does not change the result.

According to our knowledge, the first field theory approach to the universality problem was proposed by Boykin et. al. [13] and included in Nielsen and Chuang's book [60] for the set $\mathcal{S}_{\pi/8}^{H,T}$. Our aim was to simplify their method and make it tractable for arbitrary ϕ .

Another set of gates that plays a significant role in quantum information theory was studied e.g. by Sawicki [69] and Sarnak [68]. It consists of three orthogonal rotations on the Bloch sphere by an angle ϕ . In the rest of this chapter we will denote this set by $\mathcal{S}_\phi^{x,y,z}$.

$$\mathcal{S}_\phi^{x,y,z} = \{U(\phi/2, \vec{k}_x), U(\phi/2, \vec{k}_y), U(\phi/2, \vec{k}_z)\}, \quad (3.3)$$

$$U(\phi/2, \vec{k}_x) = \begin{pmatrix} \cos \phi/2 & \sin \phi/2 \\ -\sin \phi/2 & \cos \phi/2 \end{pmatrix}, \quad U(\phi/2, \vec{k}_y) = \begin{pmatrix} \cos \phi/2 & i \sin \phi/2 \\ i \sin \phi/2 & \cos \phi/2 \end{pmatrix}, \quad (3.4)$$

$$U(\phi/2, \vec{k}_z) = \begin{pmatrix} e^{i\phi/2} & 0 \\ 0 & e^{-i\phi/2} \end{pmatrix}. \quad (3.5)$$

Having defined the sets $\mathcal{S}_\phi^{H,T}$ and $\mathcal{S}_\phi^{x,y,z}$ we can formulate the main problem of the current chapter:

Problem 3.1. Find angles ϕ such, that the sets $\mathcal{S}_\phi^{H,T}$ and $\mathcal{S}_\phi^{x,y,z}$ are universal.

An attentive reader may notice that Problem 3.1 has an immediate solution when ϕ is an irrational multiple of π . In such a case both $\mathcal{S}_\phi^{H,T}$ and $\mathcal{S}_\phi^{x,y,z}$ contain elements of infinite order (recall Example 2.4 from Section 2.1.2) and by the virtue of Theorem 2.5 they generate an infinite group. Next, elements of $\mathcal{S}_\phi^{H,T}$ neither commute nor anticommute if $\phi \neq \frac{k\pi}{2}$, $k \in \mathbb{Z}$. As we will show in Section 4.4 these conditions provide that $\mathcal{S}_\phi^{H,T}$ is universal. The same arguments are valid for $\mathcal{S}_\phi^{x,y,z}$, hence this set is also universal for $\phi = a\pi$, $a \in \mathbb{R} \setminus \mathbb{Q}$.

Corollary 3.1. Let ϕ be an irrational multiple of π . Then the sets $\mathcal{S}_\phi^{H,T}$ and $\mathcal{S}_\phi^{x,y,z}$ are universal.

In the rest of this chapter we will introduce the mathematical concepts and ideas that help us to solve Problem 3.1 in case, when ϕ is a rational multiple of π . In Section 3.1 we will reformulate Problem 3.1 in terms of rotations in three dimensional space using adjoint representation. In Section 3.2 we will present cyclotomic and trigonometric polynomials and prove from scratch essential facts about these functions. Section 3.3 includes the main result of this chapter, i.e. a proof of universality of $\mathcal{S}_\phi^{H,T}$ and $\mathcal{S}_\phi^{x,y,z}$ in case, when ϕ is a rational multiple of π .

3.1. Problem reformulation

In order to make the calculations simpler we transform Problem 3.1 from the level of unitary gates to the level of orthogonal gates from $SO(3)$ using the adjoint representation. In what follows we will assume the standard orthonormal basis of $\mathfrak{su}(2)$, defined in (2.58)

Matrices $H, T(\phi)$ expressed in the adjoint representation have the form

$$\text{Ad}_H = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad \text{Ad}_{T(\phi)} = \begin{pmatrix} \cos \phi & \sin \phi & 0 \\ -\sin \phi & \cos \phi & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

where Ad_H is the rotation by angle π around the axis $\frac{\vec{k}_y + \vec{k}_z}{\sqrt{2}}$ and $\text{Ad}_{T(\phi)}$ is the rotation by angle ϕ around z -axis.

Let us denote a composition of Ad_H and $\text{Ad}_{T(\phi)}$ by $O(\gamma, \vec{k})$. Our aim is to decide if γ is a rational multiply of π . By the fact that equality of matrices implies equality of their traces we get the equation relating γ with ϕ :

$$\text{tr } \text{Ad}_H \cdot \text{Ad}_{T(\phi)} = \text{tr } O(\gamma, \vec{k}), \quad (3.6)$$

$$-\cos \phi = 2 \cos \gamma + 1 \Rightarrow \quad (3.7)$$

$$-2 \cos \gamma = \cos \phi + 1. \quad (3.8)$$

In order to remove the negative sign from (3.8) we substitute γ by $\gamma' = \gamma + \pi$. From basic trigonometric identities we know that $\cos \gamma' = -\cos \gamma$, hence

$$2 \cos \gamma' = \cos 2\phi + 1. \quad (3.9)$$

Similarly, rotation matrices corresponding to $U(\phi/2, \vec{k}_x), U(\phi/2, \vec{k}_y), U(\phi/2, \vec{k}_z)$ are given by

$$\begin{aligned} O(\phi, \vec{k}_x) &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos \phi & \sin \phi \\ 0 & -\sin \phi & \cos \phi \end{pmatrix}, \quad O(\phi, \vec{k}_y) = \begin{pmatrix} \cos \phi & 0 & \sin \phi \\ 0 & 1 & 0 \\ -\sin \phi & 0 & \cos \phi \end{pmatrix}, \\ O(\phi, \vec{k}_z) &= \begin{pmatrix} \cos \phi & \sin \phi & 0 \\ -\sin \phi & \cos \phi & 0 \\ 0 & 0 & 1 \end{pmatrix}, \end{aligned} \quad (3.10)$$

where $O(\phi, \vec{k}_j) = \text{Ad}_{U(\phi/2, \vec{k}_j)}$, $j \in \{x, y, z\}$. We can again denote a product of any two rotations from (3.10) by $O(\gamma, \vec{k})$. Comparing the traces we get

$$2 \cos \gamma + 1 = \cos^2 \phi + 2 \cos \phi. \quad (3.11)$$

Using trigonometric identities we can transform (3.11) to a linear equation

$$2 \cos \frac{\gamma}{2} = \cos \phi + 1. \quad (3.12)$$

Notice that (3.12) has exactly the same form as (3.9), therefore we can consider only one of these equations in the rest of this chapter.

Before we go to the next section we will briefly describe our idea, how to prove universality of $\mathcal{S}_\phi^{H,T}$ and $\mathcal{S}_\phi^{x,y,z}$. First, we use the fact that Theorem 2.5 holds for $SU(2)$ and $SO(3)$ [22]. However, we cannot apply it for the sets $\mathcal{S}_\phi^{H,T}$ and $\mathcal{S}_\phi^{x,y,z}$ directly as they consist only of finite order rotations. Instead, we can construct words from elements of $\mathcal{S}_\phi^{H,T}$ and $\mathcal{S}_\phi^{x,y,z}$ and search for a word having an infinite order. We start obviously with words of length two, denoted by $O(\gamma, \vec{k})$.

Recall from Section 2.1.2 that $O(\gamma, \vec{k})$ has an infinite order if γ is an irrational multiple of π . In order to check this we apply the following procedure:

Step 1 Write an equation relating ϕ and γ , e.g. (3.12).

Step 2 For ϕ - a rational multiple of π show that at least one coefficient of the minimal polynomial of $\cos \phi$ is noninteger (see Section 3.2.0.7).

Step 3 Prove that the minimal polynomial for $2 \cos \frac{\gamma}{2}$ has integer coefficients when γ is rational multiple of π (see Section 3.2.0.8).

Step 4 Using the companion matrix formalism find formulas for coefficients of the minimal polynomial of $1 + \cos \phi$ in terms of the coefficients of the minimal polynomial for $\cos \phi$ (see Section 3.3).

Step 5 Show that coefficients of the minimal polynomial for $1 + \cos \phi$ are not all integers if ϕ is a rational multiple of π and $\phi \notin \{\frac{k\pi}{2} : k \in \mathbb{Z}\}$ (see Section 3.3).

3.2. Special classes of minimal polynomials

The main purpose of this section is to present briefly the minimal polynomials that will be used to prove universality of $\mathcal{S}_\phi^{H,T}$ and $\mathcal{S}_\phi^{x,y,z}$. We will put special emphasis on minimal polynomials of $\cos \frac{2\pi}{n}$ and $2 \cos \frac{\pi}{n}$ and we will prove from scratch the main facts about them.

3.2.0.6. Cyclotomic polynomials

One of the possible ways to prove universality of $\mathcal{S}_\phi^{H,T}$ and $\mathcal{S}_\phi^{x,y,z}$ is to use the approach presented in [13, 60, 69] which is based on theory of cyclotomic polynomials. As we show in this section, this method leads to very complex formulas and is effectively not tractable.

Definition 3.1. A cyclotomic polynomial $\Phi_n(x)$ is the minimal polynomial of $e^{2i\pi/n}$, $n \in \mathbb{Z}_+$ with integer coefficients, defined as

$$\Phi_n(x) = \prod_{\substack{1 \leq k \leq n \\ \gcd(k, n) = 1}} (x - e^{2ik\pi/n}). \quad (3.13)$$

Cyclotomic polynomials satisfy the fundamental identity

$$\prod_{1 \leq k \leq n} \Phi_k(x) = x^n - 1, \quad \gcd(k, n) = 1. \quad (3.14)$$

Recall that we want to show for which ϕ the product $O(\gamma, \vec{k})$, defined in Section 3.1, is a rotation by an angle γ which is an irrational multiple of π .

Assume that $\phi = \frac{2k\pi}{n}$, where $k, n \in \mathbb{Z}$ and $\gcd(k, n) = 1$. In such a case the polynomial $\Phi_n(x)$ is the minimal polynomial of $e^{i\phi}$. In order to decide whether γ is an irrational multiple of π we should search for a minimal polynomial of $e^{i\gamma}$ and check if it is cyclotomic. In particular, if we are able to show that the coefficients of this polynomial are non-integer, the polynomial is not cyclotomic and therefore γ cannot be a rational angle. However, this task turns out to be very difficult in general. In order to show it we combine the Euler formula and (3.11) and arrive at the following equation

$$e^{i\gamma} = \cos \gamma + \sqrt{\cos^2 \gamma - 1} = \cos \phi + \frac{\cos 2\phi}{4} - \frac{1}{4} + i \sin \phi \sqrt{\frac{\cos 2\phi}{8} + \cos \phi + \frac{7}{8}}.$$

Substitution $(\cos \phi, \sin \phi) \rightarrow (e^{i\phi}, e^{-i\phi})$ yields a complicated formula relating $e^{i\gamma}$ with $e^{i\phi}$

$$e^{i\gamma} = 2(e^{i\phi} + e^{-i\phi}) + \frac{e^{2i\phi} + e^{-2i\phi}}{2} - \frac{1}{4} - 2(e^{i\phi} - e^{-i\phi}) \sqrt{2(e^{i\phi} + e^{-i\phi}) + \frac{7}{8} + \frac{e^{2i\phi} + e^{-2i\phi}}{8}}. \quad (3.15)$$

Computing the minimal polynomial of $e^{i\gamma}$ from (3.15) poses many difficulties, i.a.:

1. We do not know the relation between the degree of the polynomial $\chi_{M_{e^{i\gamma}}}$ and the algebraic degree of $\mathbb{Q}(e^{i\gamma})$. Therefore we have no guarantee that $m_{e^{i\gamma}} = \chi_{M_{e^{i\gamma}}}$.
2. Even if $m_{e^{i\gamma}} = \chi_{M_{e^{i\gamma}}}$ the use of the companion matrix formalism requires us to know the matrix $M_{\sqrt{\frac{\cos 2\phi}{8} + \cos \phi + \frac{7}{8}}}$ which is very hard to determine analytically for an arbitrary $\phi = \frac{2k\pi}{n}$.

Cyclotomic polynomials fail to provide tractable approach. However, they still could be used in case, when the minimal polynomial of $\cos \phi$ is linear or quadratic. For example, the reasoning presented in [69] concerns the simplest nontrivial case, when the minimal polynomial for $m_{\cos \phi}(x) = \psi_n(x)$ is quadratic. Then $\cos \phi = a + b\sqrt{c}$ and $\cos \gamma = A + B\sqrt{c}$, where $a, b \in \mathbb{Q}$ and A, B depend on a and b . The equations (3.11) and the polynomial $p(x) = x^2 - 2\cos \phi x + 1$, that is annihilated by $e^{\pm i\phi}$, allow us to compute $m_{e^{i\gamma}}$. As a result we get

$$m_{e^{i\gamma}}(x) = x^4 - 4Ax^3 + (4A^2 + 2)x^2 - 4Ax - 4B^2c + 1.$$

The only possible quadratic minimal polynomials for $\cos \phi$ are of the form

$$\psi_5(x) = x^2 + \frac{1}{2}x - \frac{1}{4} \Rightarrow \cos \phi = a + b\sqrt{c} = -\frac{1}{4} \pm \frac{\sqrt{5}}{4}, \quad (3.16)$$

$$\psi_8(x) = x^2 - \frac{1}{2} \Rightarrow \cos \phi = a + b\sqrt{c} = \frac{1}{\sqrt{2}}, \quad (3.17)$$

$$\psi_{12}(x) = x^2 - \frac{3}{4} \Rightarrow \cos \phi = a + b\sqrt{c} = \frac{\sqrt{3}}{2}. \quad (3.18)$$

We insert the coefficients a, b, c from (3.16), (3.17), (3.18) respectively and use (3.11) to compute A, B . Applying this procedure we easily check, that $m_{e^{i\gamma}}$ has at least one non-integer coefficient all cases, hence it is not a cyclotomic polynomial for any ϕ having quadratic $\psi_n(x)$. A more general approach that is tractable for arbitrary ϕ is possible using trigonometric polynomials.

3.2.0.7. Minimal polynomials of $\cos \frac{2k\pi}{n}$

By trigonometric polynomials we will understand the minimal polynomials for $\cos \phi$, $\sin \phi$, $2 \cos \frac{\phi}{2}$ and $\tan \phi$, where ϕ is a rational multiple of π . A detailed description of their properties can be found in e.g. [7, 83]. In this chapter we will concentrate on minimal polynomials for $\cos \phi$ and $2 \cos \frac{\phi}{2}$. We will also show their relations with Chebyshev polynomials of the first kind.

Definition 3.2. [83] A minimal polynomial $\psi_n(x)$ of $\cos \frac{2\pi}{n}$ is a polynomial defined as

$$\psi_1(x) = x - \cos 2\pi = x - 1, \quad \psi_2 = x - \cos \pi = x + 1, \quad (3.19)$$

$$\psi_n(x) = \prod_{\substack{1 \leq k \leq \lfloor n/2 \rfloor \\ \gcd(k, n) = 1}} \left(x - \cos \frac{2k\pi}{n} \right), \quad n \geq 3, \quad (3.20)$$

$$\deg \psi_n(x) = \begin{cases} 1 & n = 1, 2 \\ \frac{\varphi(n)}{2} & n \geq 3 \end{cases}, \quad (3.21)$$

where $\varphi(n)$ is the Euler totient function (see Definition 2.4).

Remark 3.1. It is worth emphasizing that the sum in (3.20) is over $1 \leq k \leq \lfloor n/2 \rfloor$, $\gcd(k, n) = 1$ instead of $1 \leq k \leq n$. It stems from the symmetry of cosine, i.e. $\cos \phi = \cos(-\phi)$. Notice that for every $\phi = \frac{2k\pi}{n}$ the opposite angle is defined as $-\phi = -\frac{2k\pi}{n} = \frac{2(n-k)\pi}{n}$. From (2.2) we get that every root of $\psi_n(x)$ which is of the form $\cos \frac{2k\pi}{n}$ is equal to the root $\cos \frac{2(n-k)\pi}{n}$. Therefore $\cos \frac{2k\pi}{n}$ for $1 \leq k \leq \lfloor n/2 \rfloor$ are all the possible roots of $\psi_n(x)$.

Definition 3.2, however, does not enable us to compute coefficients of $\psi_n(x)$ for $n > 5$ efficiently. In order to avoid this problem we will introduce Chebyshev polynomials of the first kind and use them to find explicit formulas for $\psi_n(x)$, $n > 5$.

Definition 3.3. Chebyshev polynomials of the first kind $T_k(x)$, $k = 0, 1, \dots$ are defined by the recurrence formula

$$T_k(x) = 2xT_{k-1}(x) - T_{k-2}(x), \quad T_0(x) = 1, \quad T_1(x) = x. \quad (3.22)$$

Equivalently, $T_k(x)$'s are the polynomials satisfying

$$T_k(\cos \phi) = \cos k\phi. \quad (3.23)$$

Using formula (3.22) we deduced properties of the coefficients of Chebyshev polynomials.

Fact 3.1. Let $T_k(x) = \sum_{i=0}^k c_i x^i$ be the Chebyshev polynomial of the first kind of the degree k . The coefficients c_0, \dots, c_k satisfy:

1. c_0, \dots, c_k are integer numbers.
2. The leading coefficient c_k is equal to 2^{k-1} .
3. $T_k(x)$ has only odd/even powers of x if k is an odd/even number respectively.
4. If k is even, then the free term c_0 is given by $c_0 = \pm 1$.
5. If k is odd, then the coefficients c_0, c_1 are equal $c_0 = 0$, $c_1 = \pm k$ respectively.

Formula (3.23) implies that Chebyshev polynomials can be expressed in terms of minimal polynomials of $\cos \phi$ and vice versa. Historically, the first such relation was given by Waitkins and Zeitlin [83] and is an analogue of (3.14) for cyclotomic polynomials.

Fact 3.2. [83] Let k, n be integers, $k, n \geq 1$. The canonical identities relating $T_{k+1}(x)$ and $T_k(x)$ or $T_{k+1}(x)$ and $T_{k-1}(x)$ with minimal polynomials $\psi_n(x)$ have the form

$$2^k \prod_{d|n} \psi_d(x) = T_{k+1}(x) - T_k(x), \quad n = 2k + 1, \quad (3.24)$$

$$2^k \prod_{d|n} \psi_d(x) = T_{k+1}(x) - T_{k-1}(x), \quad n = 2k. \quad (3.25)$$

For the purpose of this chapter we need to reverse identities (3.25) and (3.24) using the Möbius inversion formula. This allows us to express $\psi_n(x)$ for every $n \in \mathbb{Z}_+$ in terms of Chebyshev polynomials.

Fact 3.3. [7] Let $n \geq 3$, odd and $m \geq 1$, $m, n \in \mathbb{Z}_+$. Then $\psi_n(x)$, $\psi_{2^m n}(x)$ are given by

$$\psi_n(x) = \prod_{d|n} [2^{-\lfloor d/2 \rfloor} (T_{\lfloor d/2 \rfloor + 1}(x) - T_{\lfloor d/2 \rfloor}(x))]^{\mu(n/d)}, \quad (3.26)$$

$$\psi_{2^m n}(x) = \prod_{d|n} \left[\frac{2^{-\lfloor 2^{m-1}d \rfloor} (T_{\lfloor 2^{m-1}d \rfloor + 1}(x) - T_{\lfloor 2^{m-1}d \rfloor - 1}(x))}{2^{-\lfloor 2^{m-2}d \rfloor} (T_{\lfloor 2^{m-2}d \rfloor + 1}(x) - T_{\lfloor 2^{m-2}d \rfloor - 1}(x))} \right]^{\mu(n/d)}, \quad m > 1, \quad (3.27)$$

$$\psi_{2^m n}(x) = \prod_{d|n} \left[\frac{2^{-d} (T_{\lfloor d \rfloor + 1}(x) - T_{\lfloor d \rfloor - 1}(x))}{2^{-\lfloor d/2 \rfloor} (T_{\lfloor d/2 \rfloor + 1}(x) - T_{\lfloor d/2 \rfloor}(x))} \right]^{\mu(n/d)}, \quad m = 1. \quad (3.28)$$

In what follows we present a fact about minimal polynomials for $\cos \frac{2k\pi}{n}$ that will be essential in proving Theorem 3.5.

Lemma 3.2. At least one coefficient of $\psi_n(x)$, i.e. the constant term c_0 , is non-integer if $n \notin \{1, 2, 4\}$.

Proof. First, notice that cosines of 2π , π and $\frac{\pi}{2}$ are integers, therefore the corresponding minimal polynomials $\psi_n(x)$ belong to $\mathbb{Z}[x]$. In all other cases we can distinguish the following situations:

1. n is an odd prime number,
2. n is an odd composite number,
3. n is an even composite number.

In the following we consider all of these situations separately and provide their proofs using (3.26), (3.27), (3.28).

1. In case 1. n has exactly two divisors and the formula (3.24) simplifies to

$$\psi_1(x)\psi_n(x) = (x - 1)\psi_n(x) = 2^{-\lfloor n/2 \rfloor} (T_{\lfloor n/2 \rfloor + 1}(x) - T_{\lfloor n/2 \rfloor}(x)). \quad (3.29)$$

Notice that $T_{\lfloor n/2 \rfloor + 1}(x) - T_{\lfloor n/2 \rfloor}(x)$ is a difference of Chebyshev polynomials, where one of them is of the even degree and the second one has the odd degree. By the virtue of Fact 3.1, $T_{\lfloor n/2 \rfloor + 1}(x) - T_{\lfloor n/2 \rfloor}(x)$ has a free term equal ± 1 . hence the free term of the right hand side of (3.29) is $\pm \frac{1}{2^{\lfloor n/2 \rfloor}}$.

Notice also that the free term of left hand side is determined by the free term of $\psi_n(x)$. Comparing the left and right side of (3.29) one can see that the free term of $\psi_n(x)$ is equal to $c_0 = \pm \frac{1}{2^{\lfloor n/2 \rfloor}}$, thus it is a rational number as we assume $n \geq 3$.

2. In case 2. we will prove that $\psi_n(x)$ has a non-integer free term by applying formula (3.26) and using properties of the Möbius function. Let $n = p_1^{n_1} \dots p_m^{n_m}$ be the prime factorization of n and $\mathcal{D}_n^+, \mathcal{D}_n^-$ be the sets of all square free divisors of n that have even and odd number of prime divisors, respectively. By the virtue of (2.4) we have $|\mathcal{D}_n^+| = |\mathcal{D}_n^-|$. Notice that the free term of the right hand side of (3.26) can be written in the form

$$c_0 = \pm \prod_{d|n} \left(\frac{1}{2^{\lfloor d/2 \rfloor}} \right)^{\mu(n/d)} = \pm \prod_{\frac{n}{d} \in \mathcal{D}_n^+ \cup \mathcal{D}_n^-} \left(\frac{1}{2^{\lfloor d/2 \rfloor}} \right)^{\mu(n/d)} = \frac{2^{\sum_{\frac{n}{d} \in \mathcal{D}_n^-} \lfloor d/2 \rfloor}}{2^{\sum_{\frac{n}{d} \in \mathcal{D}_n^+} \lfloor d/2 \rfloor}}. \quad (3.30)$$

We next raise c_0 to the power $p = 2p_1 \cdot \dots \cdot p_m$

$$c_0^p = \frac{2^{\sum_{\frac{n}{d} \in \mathcal{D}_n^-} p \lfloor d/2 \rfloor}}{2^{\sum_{\frac{n}{d} \in \mathcal{D}_n^+} p \lfloor d/2 \rfloor}} = \frac{2^{\sum_{\frac{n}{d} \in \mathcal{D}_n^-} p(d-1)/2}}{2^{\sum_{\frac{n}{d} \in \mathcal{D}_n^+} p(d-1)/2}} = \frac{2^{-\frac{pk}{2} + \sum_{\frac{n}{d} \in \mathcal{D}_n^-} \frac{pd}{2}}}{2^{-\frac{pk}{2} + \sum_{\frac{n}{d} \in \mathcal{D}_n^+} \frac{pd}{2}}} = \frac{2^{\sum_{\frac{n}{d} \in \mathcal{D}_n^-} \frac{pd}{2}}}{2^{\sum_{\frac{n}{d} \in \mathcal{D}_n^+} \frac{pd}{2}}}. \quad (3.31)$$

It is worth stressing that c_0 is non-integer if and only if $c_0^p < 1$. In order to find the appropriate condition we use the fact that if $x = \frac{n}{d}$ belongs to \mathcal{D}_n^- or \mathcal{D}_n^+ then

$$p \cdot d = p \frac{n}{x} = 2n \cdot y, \quad (3.32)$$

where y is the square-free product of such prime divisors of n that do not appear in prime factorization of x . In particular, if m is an even number and $x \in \mathcal{D}_n^+$, then y must also belong to \mathcal{D}_n^+ . Similarly $x \in \mathcal{D}_n^-$ implies that $y \in \mathcal{D}_n^-$. When m is odd one easily checks that $x \in \mathcal{D}_n^+$ implies that $y \in \mathcal{D}_n^-$ and *vice versa*.

Let us consider the case when m is an even number. Taking $pd = 2ny$ one can rewrite (3.31) as

$$c_0^p = \frac{2^{\sum_{\frac{n}{d} \in \mathcal{D}_n^-} \frac{pd}{2}}}{2^{\sum_{\frac{n}{d} \in \mathcal{D}_n^+} \frac{pd}{2}}} = \frac{2^{\sum_{y \in \mathcal{D}_n^-} ny}}{2^{\sum_{y \in \mathcal{D}_n^+} ny}} = \frac{2^{n \sum_{y \in \mathcal{D}_n^-} y}}{2^{n \sum_{y \in \mathcal{D}_n^+} y}}. \quad (3.33)$$

As one can easily see $c_0^p < 1$ if the following holds

$$\sum_{y \in \mathcal{D}_n^+} y - \sum_{y \in \mathcal{D}_n^-} y > 0. \quad (3.34)$$

Note that this expression is equivalent to the product

$$\sum_{y \in \mathcal{D}_n^+} y - \sum_{y \in \mathcal{D}_n^-} y = (1 - p_1) \dots (1 - p_m), \quad (3.35)$$

which is always larger than zero if m is even, thus c_0 is non-integer in this case.

Next let us consider n such, that m is an odd number. Doing *mutatis mutandis* to the case when m is even one can transform (3.31) to the form

$$c_0^p = \frac{2^{\sum_{\frac{n}{d} \in \mathcal{D}_n^-} pd}}{2^{\sum_{\frac{n}{d} \in \mathcal{D}_n^+} pd}} = \frac{2^{\sum_{y \in \mathcal{D}_n^+} ny}}{2^{\sum_{y \in \mathcal{D}_n^-} ny}} = \frac{2^{n \sum_{y \in \mathcal{D}_n^+} y}}{2^{n \sum_{y \in \mathcal{D}_n^-} y}}, \quad (3.36)$$

thus the condition for $c_0^p < 1$ is given by

$$\sum_{y \in \mathcal{D}_n^+} y - \sum_{y \in \mathcal{D}_n^-} y = (1 - p_1) \dots (1 - p_m) < 0. \quad (3.37)$$

Note that this is always satisfied if m is odd, which means that c_0^p is indeed smaller than one. This way we have proven Lemma 3.2 for the case when $n > 1$ and n is odd.

3. In case 3. we will use the similar approach as for case 2. Recall that every even number n can be represented as $n = 2^\eta k$, where k - odd and $\eta \in \mathbb{Z}_+$. This allows us to define $\psi_n(x)$ by the formula (3.27). Let us define the sets \mathcal{D}_n^+ and \mathcal{D}_n^- like previously. Using fact 3.1 one can extract the free terms from (3.27) and (3.28) as

$$c_0 = \prod_{d|k} \left(\frac{2}{2^{2^{\eta-2}d}} \right)^{\mu(k/d)} = \frac{2^{2^{\eta-2} \sum_{\frac{n}{d} \in \mathcal{D}_n^-} d}}{2^{2^{\eta-2} \sum_{\frac{n}{d} \in \mathcal{D}_n^+} d}}, \quad \eta > 1, \quad (3.38)$$

$$c_0 = \prod_{d|k} \left(\frac{1}{2^{\lfloor d/2 \rfloor}} \right)^{\mu(k/d)} = \frac{2^{\sum_{\frac{n}{d} \in \mathcal{D}_n^-} \lfloor d/2 \rfloor}}{2^{\sum_{\frac{n}{d} \in \mathcal{D}_n^+} \lfloor d/2 \rfloor}}, \quad \eta = 1. \quad (3.39)$$

By properties of the Möbius function all the sums and products are over the same number of divisors. Note that (3.39) and (3.30) are exactly equal, whereas (3.38) has a very similar form to (3.30). Using very similar reasoning as in the case 2) we obtain immediately that c_0 is non-integer unless $n = 2, 4$, which completes the proof. \square

Example: In this paragraph we will illustrate the method presented in the proof of Lemma 3.2 with the example for $n = 15$. First, $\mathcal{D}_n^+ = \{1, 15\}$ and $\mathcal{D}_n^- = \{3, 5\}$. The coefficient c_0 of $\psi_{15}(x)$ is given by

$$c_0 = \frac{2^{\lfloor 5/2 \rfloor + \lfloor 3/2 \rfloor}}{2^{\lfloor 15/2 \rfloor + \lfloor 1/2 \rfloor}}. \quad (3.40)$$

Using the reasoning presented for the case 2) we raise c_0 to the power $p = 30$ and obtain the condition

$$c_0^{30} = \frac{2^{15(5+3)-15}}{2^{15(15+1)-15}} = \frac{2^{15 \sum_{y \in \mathcal{D}_{15}^-} y}}{2^{15 \sum_{y \in \mathcal{D}_{15}^+} y}} < 1 \Leftrightarrow \sum_{y \in \mathcal{D}_{15}^+} y - \sum_{y \in \mathcal{D}_{15}^-} y = 16 - 8 > 0.$$

Thus we have shown that $c_0 < 1$. On the other hand one can see immediately from definition (3.40) that c_0 for $\psi_{15}(x)$ is equal to $2^{-8} \notin \mathbb{Z}$.

3.2.0.8. Minimal polynomials of $2 \cos \frac{k\pi}{n}$

Another class of polynomials, that play an important role in proving universality of $\mathcal{S}_\phi^{H,T}$ and $\mathcal{S}_\phi^{x,y,z}$ are minimal polynomials of $2 \cos \frac{\pi}{n}$. The current section will be devoted to main facts about these functions.

Lemma 3.3. [7] *The minimal polynomial of $2 \cos \frac{\pi}{n}$ is a polynomial defined as*

$$\eta_n(x) = 2^{\deg \psi_{2n}(x)} \psi_{2n} \left(\frac{x}{2} \right). \quad (3.41)$$

Using fact 3.2 one can write it explicitly as:

$$\eta_1(x) = x + 2, \quad (3.42)$$

$$\eta_n(x) = \prod_{\substack{1 \leq k \leq n \\ \gcd(k, 2n) = 1}} \left(x - 2 \cos \frac{k\pi}{n} \right), \quad n \geq 2. \quad (3.43)$$

Proof. First, we notice that $\cos \frac{k\pi}{n}$ is a root of the polynomial $\psi_{2n}(x)$ of a degree $d = \deg \psi_{2n}(x) = \frac{\varphi(2n)}{2}$ with the coefficients c_0, \dots, c_{d-1}, c_d for arbitrary $1 \leq k \leq n$ such, that $\gcd(k, 2n) = 1$. As $2 \cos \frac{\pi}{n}$ is a product of $2 \in \mathbb{Z} \subset \mathbb{Q}$ and a root of $\cos \frac{k\pi}{n}$, the companion matrix $M_{2 \cos \frac{k\pi}{n}}$ is given by (2.26)

$$M_{2 \cos \frac{k\pi}{n}} = 2 \cdot M_{\cos \frac{k\pi}{n}}$$

and by the virtue of Fact 2.4 the minimal polynomial $\eta_n(x)$ is equal to the characteristic polynomial $\chi_{M_{2 \cos \frac{k\pi}{n}}}$. Let us write this matrix explicitly. The polynomial $\eta_n(x)$ is given by

$$\eta_n(x) = \chi_{M_{2 \cos \frac{k\pi}{n}}} = \det \begin{pmatrix} -x & 0 & \dots & -2c_0 \\ 2 & -x & \dots & -2c_1 \\ 0 & 2 & \dots & -2c_2 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 2 & -2c_{d-1} - x \end{pmatrix}. \quad (3.44)$$

The substitution $x \rightarrow 2y$ transforms (3.44) to the form $\eta_n(2y) = \chi_{2M_{\cos \frac{k\pi}{n}}}$. On the other hand $M_{\cos \frac{k\pi}{n}}$ is a $d \times d$ matrix, therefore we arrive at

$$\eta_n(2y) = \det 2(M_{\cos \frac{k\pi}{n}} - yI) = 2^d \psi_{2n}(y) = 2^d \psi_{2n}\left(\frac{x}{2}\right), \quad (3.45)$$

which is exactly (3.41). The proof is complete. \square

For the purposes of this chapter we restrict our interest to one essential fact about minimal polynomials $\eta_n(x)$, i.e.

Lemma 3.4. *All the coefficients of $\eta_n(x)$ are integers.*

According to our knowledge this fact is already known in number theorists community, however we have not found its mathematically strict proof. For this reason we include in this thesis two versions of the proof. The first one that is based on properties of cyclotomic polynomials and Gauss Lemma will be presented in the following. The second version is included in Appendix 6.1.

Proof of Lemma 3.4. We start from pointing that $2 \cos \frac{k\pi}{n} = 2 \cos \frac{2k\pi}{2n}$, $\gcd(k, 2n) = 1$ can be expressed as a sum

$$2 \cos \frac{2k\pi}{2n} = e^{ik\pi/n} + e^{-ik\pi/n},$$

where both $e^{ik\pi/n}$ and $e^{-ik\pi/n}$ are roots of the cyclotomic polynomial $\Psi_{2n}(x)$ which stems from (2.2). Denote the companion matrix of $\Psi_{2n}(x)$ by $M_{\Psi_{2n}(x)}$. As $\Psi_{2n}(x)$ is by definition a polynomial with integer coefficients, $M_{\Psi_{2n}(x)}$ has only integer entries.

In the next step one needs to see that $2 \cos \frac{\pi}{n}$ is a root of the characteristic polynomial of the matrix defined as

$$M = M_{\Psi_{2n}(x)} \otimes I + I \otimes M_{\Psi_{2n}(x)}, \quad (3.46)$$

which stems from (2.26). As M is an integer matrix its characteristic polynomial χ_M belongs to $\mathbb{Z}[x]$. The degree of the minimal polynomial of $2 \cos \frac{\pi}{n}$ is smaller than the degree of χ_M as $\mathbb{Q}(2 \cos \frac{k\pi}{n}) \subset \mathbb{Q}(e^{ik\pi/n})$ (see discussion in Section 2.2.2). This means, the characteristic polynomial of M can be factorized as a product of at least two polynomials, namely

$$\chi_M = \eta_n(x) \cdot p(x), \text{ where in general } p(x), \eta_n(x) \in \mathbb{Q}[x].$$

Since χ_M belongs to $\mathbb{Z}[x]$, then by Lemma 2.9 the polynomials $\eta_n(x)$ and $p(x)$ have also integer coefficients. As χ_M is monic, $p(x)$ and $\eta_n(x)$ are also monic. The result follows. \square

3.3. Proof of universality

In this section we will prove the following theorem

Theorem 3.5. *Assume ϕ is a rational multiple of π . Then γ given by (3.12) is a rational multiple of π if and only if $\phi \in \{\frac{k\pi}{2} : k \in \mathbb{Z}\}$.*

To this end we use the machinery presented in Sections 2.2 and 3.2. The main idea is to show that the left hand side of (3.12) is *not* a root of any minimal polynomial $\eta_m(x)$.

Proof. Notice the minimal polynomials of $2 \cos \frac{\gamma}{2}$ and $\cos \phi + 1$ are equal. The minimal polynomial $m_{\cos \phi + 1}(x)$ can be found using the companion matrix formalism. It follows that $\cos \phi + 1$ is a root of the characteristic polynomial of the matrix $M_{\cos \phi + 1} = M_{\cos \phi} + I$, where

$$M_{\cos \phi} = \begin{pmatrix} 0 & 0 & \dots & -c_0 \\ 1 & 0 & \dots & -c_1 \\ 0 & 1 & \dots & -c_2 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & -c_{d-1} \end{pmatrix}.$$

Following a discussion from Section 2.2.2 one can conclude that the field extension $\mathbb{Q}(\cos \phi + 1)$ has the same algebraic degree as $\mathbb{Q}(\cos \phi)$ (see Fact 2.4). On the other hand $\mathbb{Q}(2 \cos \frac{\gamma}{2})$ has the same algebraic degree as $\mathbb{Q}(\cos \phi + 1)$, which stems from equality of these numbers. Therefore the characteristic polynomial of $M_{\cos \phi + 1}$ is *exactly* the minimal polynomial $m_{2 \cos \frac{\gamma}{2}}(x)$.

One can compute $\chi_{M_{\cos \phi + 1}}$ as the determinant of the following matrix:

$$M_{\cos \phi + 1} - Ix = \begin{pmatrix} 1-x & 0 & 0 & \dots & 0 & -c_0 \\ 1 & 1-x & 0 & \dots & 0 & -c_1 \\ 0 & 1 & 1-x & \dots & 0 & -c_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 1-x & -c_{d-2} \\ 0 & 0 & \dots & 0 & 1 & 1-c_{d-1}-x \end{pmatrix}. \quad (3.47)$$

Expansion with respect to the first row gives us to the following expression:

$$m_{2 \cos \frac{\gamma}{2}}(x) = \chi_{M_{\cos \phi + 1}}(x) = \det(M_{\cos \phi + 1} - Ix) = \sum_{i=0}^d \omega_i \cdot x^i = \quad (3.48)$$

$$= - \left[\sum_{i=0}^{d-3} c_i (-1)^{d+i+1} (1-x)^i \right] + (1-x)^{d-2} [x^2 + x(c_{d-1} - 2) + c_{d-2} - c_{d-1} + 1]. \quad (3.49)$$

In the next step we simplify (3.49) using the binomial formula. As a result we derive the

following relations between the coefficients of $\psi_n(x)$ and $\chi_{M_{\cos \phi+1}}$:

$$\begin{aligned}
\omega_0 &= \sum_{i=0}^{d-3} c_i (-1)^{d+i} + (c_{d-2} - c_{d-1} + 1) (-1)^d, \\
\omega_1 &= \sum_{i=1}^{d-3} c_i (-1)^{d+1+i} + \binom{d-2}{0} (c_{d-1} - 2) - \binom{d-2}{1} (c_{d-2} - c_{d-1} + 1), \\
\omega_2 &= \sum_{i=2}^{d-3} c_i (-1)^{d+i+2} \binom{i}{2} + \binom{d-2}{0} - \binom{d-2}{1} (c_{d-2} + 1) + \binom{d-2}{2} (c_{d-2} - c_{d-1} + 1), \\
&\vdots \\
\omega_k &= \sum_{i=k}^{d-3} c_i (-1)^{d+i+k} \binom{i}{k} + \binom{d-2}{k} (-1)^k (c_{d-2} - c_{d-1} + 1) + \binom{i}{k-1} (-1)^{k-1} (c_{d-1} - 2) + \binom{d-2}{k-2} (-1)^{k-2} \\
&\vdots \\
\omega_{d-3} &= -c_{d-3} + (c_{d-2} - 2) (-1)^{d-3} (c_{d-2} - c_{d-1} + 1) + \binom{d-2}{d-4} (-1)^{d-4} (c_{d-1} - 2) + (-1)^{d-5} \binom{d-2}{d-5}, \\
\omega_{d-2} &= (-1)^{d-2} (c_{d-2} - c_{d-1} + 1) + (d-2) (-1)^{d-3} (c_{d-1} - 2) + (-1)^{d-4} \binom{d-2}{d-4}, \\
\omega_{d-1} &= (-1)^d (c_{d-1} - 2) + (d-2) (-1)^{d-1}, \\
\omega_d &= (-1)^d.
\end{aligned} \tag{3.50}$$

Recall that by Lemma 3.3 the coefficients of $m_{2\cos \frac{\gamma}{2}}(x)$ must be all integers if γ is a rational multiple of π . One has to check if this condition is satisfied by all ω_i 's starting from ω_{d-1} . For this coefficient we have:

$$(-1)^{d-2} (c_{d-1} - 2) + (d-2) (-1)^{d-3} \in \mathbb{Z} \Rightarrow c_{d-1} \in \mathbb{Z}.$$

Note that $\omega_{d-1} \notin \mathbb{Z}$ if and only if $c_{d-1} \notin \mathbb{Z}$. In this case we are done, however there are polynomials $\psi_n(x)$ for which $c_{d-1} \in \mathbb{Z}_+$. In this case we consider the equation for ω_{d-2} :

$$\omega_{d-2} = (-1)^{d-2} (c_{d-2} - c_{d-1} + 1) + (d-2) (-1)^{d-3} (c_{d-1} - 2) + (-1)^{d-4} \binom{d-2}{d-4} \in \mathbb{Z} \Rightarrow c_{d-2} \in \mathbb{Z}.$$

Assuming that $c_{d-1} \in \mathbb{Z}$, the coefficient ω_{d-2} is non-integer only if $c_{d-2} \notin \mathbb{Z}$. One can use the same reasoning for the other ω_i 's step by step and notice from (3.50) that each ω_i depends on the coefficients $c_{d-1}, \dots, c_{i+1}, c_i$, where c_i is multiplied by the factor $(-1)^{d+2i} \binom{i}{i} = \pm 1$. If all of the coefficients $c_{d-1}, \dots, c_{i+1}, c_i$ are integers, then also ω_i belongs to \mathbb{Z} . Hence all $\omega_1, \dots, \omega_d$ are integers if and only if $c_1, c_2, \dots, c_{d-1}, c_d \in \mathbb{Z}$. On the other hand we have shown in Lemma 3.2 that $\psi_n(x)$ has always at least one non-integer coefficient if $n \notin \{1, 2, 4\}$. Therefore at least one ω_i does not belong to \mathbb{Z} and $m_{2\cos \frac{\gamma}{2}}$ cannot be the minimal polynomial $\eta_m(x)$ for any $m \in \mathbb{Z}$. This means, γ must be an irrational multiple of π . \square

Finally we consider what happens in the exceptional cases, i.e. $\phi = \{\frac{\pi}{2}, \pi, \frac{3\pi}{2}, 2\pi\}$.

1. Let $\phi = \pm \frac{\pi}{2}$. The corresponding minimal polynomial and its companion matrix are of the form $\psi_4(x) = x$ and $M_{\cos \frac{\pi}{2}} = 0$. Thus $M_{\cos \phi+1} = 1$ and its minimal polynomial is $m_{M_{\cos \phi+1}}(x) = x - 1$. We have that $x - 1 = \eta_3(x)$, thus $\gamma = \frac{k\pi}{3}$.
2. Let $\phi = 2\pi$, then $\psi_1(x) = x - 1$, $M_{\cos 2\pi} = 1$. The companion matrix for $M_{\cos \phi+1}$ is a 1×1 matrix equal to $M_{\cos \phi+1} = 1 + 1 = 2$. Thus $m_{M_{\cos \phi+1}}(x) = x - 2$. This polynomial corresponds to $\gamma = 2\pi$.
3. Assume $\phi = \pi$, then $\psi_2(x) = x + 1$, $M_{\cos \pi} = -1$ and $M_{\cos \phi+1} = 1 - 1 = 0$. Thus the minimal polynomial of $m_{\cos \phi+1}(x) = x = \eta_2(x)$ which is the minimal polynomial of $2 \cos \gamma/2$ for $\gamma = \pi$.

Notice, that $\phi \in \{\frac{k\pi}{2} : k \in \mathbb{Z}\}$ implies that matrices $\text{Ad}_{T(\phi)}$, $O(\phi, \vec{k}_x)$, $O(\phi, \vec{k}_y)$, $O(\phi, \vec{k}_z)$ have entries in $\{1, 0, -1\}$. In such a case we see immediately that the sets $\mathcal{S}_\phi^{H,T}$ and $\mathcal{S}_\phi^{x,y,z}$ generate finite groups.

We can summarize this chapter as follows:

Corollary 3.6. Assume ϕ is a rational multiple of π and $\phi \notin \{\frac{k\pi}{2} : k \in \mathbb{Z}\}$. Let Ad_H be the adjoint representation of the Hadamard gate and $\text{Ad}_{T(\phi)}$ be the adjoint representation of the phase change gate by angle ϕ . Then $O(\gamma, \vec{k}) = \text{Ad}_H \text{Ad}_{T(\phi)}$ is the rotation by an angle γ which is an irrational multiple of π . Moreover, the sets $\{\text{Ad}_H, \text{Ad}_{T(\phi)}\}$ and $\{H, T(\phi)\}$ are universal if and only if $\phi \notin \{\frac{k\pi}{2} : k \in \mathbb{Z}\}$.

Corollary 3.7. Assume ϕ is a rational multiple of π and $\phi \notin \{\frac{k\pi}{2} : k \in \mathbb{Z}\}$. Let $O(\phi, \vec{k}_1), O(\phi, \vec{k}_2) \in SO(3)$ be rotations around orthogonal axes $\vec{k}_1 \perp \vec{k}_2$, by the angle ϕ . Then $O(\gamma, \vec{k}) = O(\phi, \vec{k}_1)O(\phi, \vec{k}_2)$ is the rotation by an angle γ which is an irrational multiple of π . Moreover, the set $\{O(\phi, \vec{k}_1), O(\phi, \vec{k}_2)\}$ and the corresponding set of unitary matrices $\{U(\phi/2, \vec{k}_1), U(\phi/2, \vec{k}_2)\}$ is universal if and only if $\phi \notin \{\frac{k\pi}{2} : k \in \mathbb{Z}\}$.

3.4. Summary and open problems

In this chapter we presented a proof of universality of the sets

$$\mathcal{S}_\phi^{H,T} = \{H, T(2\phi)\} \quad \text{and} \quad \mathcal{S}_\phi^{x,y,z} = \{U(\phi, \vec{k}_x), U(\phi, \vec{k}_y), U(\phi, \vec{k}_z)\}$$

are universal. Our approach was based on properties of trigonometric polynomials, cyclotomic polynomials and the companion matrix formalism. Below we list all the obtained results:

1. In Section 3.2 we used adjoint representation to rewrite the problem of universality of one-qubit gates as the problem of composing rotations in three dimensional space.
2. In Section 3.2.0.7 we gave a mathematically strict proof that every minimal polynomial $\psi_n(x)$, where $n \neq 1, 2, 4$ has at least one noninteger coefficient.
3. Section 3.2.0.8 includes the proof that every minimal polynomial $\eta_n(x)$ belongs to $\mathbb{Z}[x]$.
4. Section 3.3 we used the companion matrix formalism and theory of field extensions to prove, that $\mathcal{S}_\phi^{H,T}$ and $\mathcal{S}_\phi^{x,y,z}$ are universal sets of gates if $\phi \notin \{\frac{k\pi}{2}, k \in \mathbb{Z}\}$.

An interesting open problem related to this chapter is generalization of the field theory approach to other sets of one-qubit gates.

Chapter 4

Universality of single qudit gates

In this chapter we provide some simple universality criteria that can be applied to an arbitrary set of one-qudit gates

$$\mathcal{S} = \{g_1, \dots, g_n\} \subset G, \quad n \geq 2,$$

where $G = SU(d)$ or $G = SO(d)$. We restrict our considerations to these groups because of their particular importance in quantum computation and linear quantum optics.

In order to formulate general universality criteria we return to definitions from Section 1.1, according to which \mathcal{S} is universal if the group generated by \mathcal{S} , denoted by $\overline{\langle \mathcal{S} \rangle}$, is equal to G (see Definition 1.2). Our universality criteria must distinguish this case from another possibilities, which are presented in Figure 4.1.

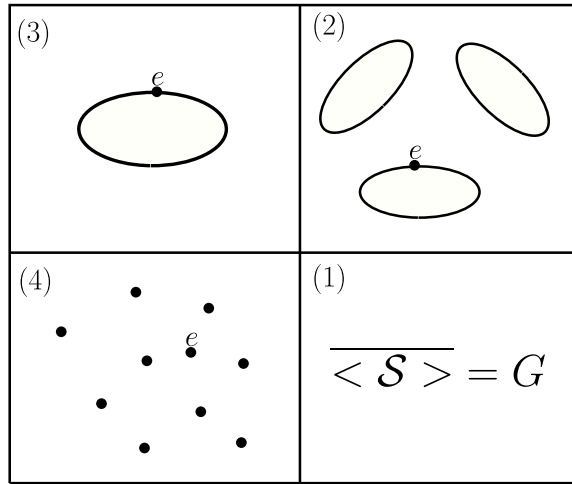


Figure 4.1: Possible groups generated by an initial set $\mathcal{S} \subset G$. Black dots denote isolated elements of G , whereas ellipses represent connected components of a subgroup of G . Case (1) is when $\langle \mathcal{S} \rangle$ is dense in G and hence is universal. Cases (2) and (3) represent situations when the closure of $\langle \mathcal{S} \rangle$ is a compact, disconnected or connected respectively subgroup of G . In cases (1), (2) and (3) $\langle \mathcal{S} \rangle$ is an infinite set. Case (4) represents a situation when \mathcal{S} generates a finite subgroup of G .

The algorithm presented within this chapter divides the universality criterion, $\overline{\langle \mathcal{S} \rangle} = G$, into two steps. In the first one we assume that $\langle \mathcal{S} \rangle$ is infinite (as G is an infinite group) and check, if $\overline{\langle \mathcal{S} \rangle} = G$ under this assumption. In the second step we check if our assumption is actually satisfied. Throughout this thesis these steps will be called the necessary and sufficient criteria, respectively. In the following we will present them in a simple form:

Necessary criterion: If $\overline{\langle \mathcal{S} \rangle} = G$, then the only matrix commuting with $\text{Ad}_{\mathcal{S}}$ is λI , where $\lambda \in \mathbb{R}$.

Sufficient criterion: $\overline{\langle \mathcal{S} \rangle} = G$ if and only if (1) the necessary criterion is satisfied and (2) $\langle \mathcal{S} \rangle$ contains at least one element, that is close enough to a central element of G but is different from this element.

In the rest of this chapter we will derive the necessary and sufficient universality criteria and explain them in details. It is worth emphasizing, that the only operations that are required to check our criteria are matrix multiplication and solving a number of algebraic equations. This is a great advantage of our approach, comparing to methods that require more advanced concepts, e.g. quantum automata [23].

The chapter is organized as follows. Section 4.1 is devoted to the necessary universality criterion and we will start from formulating it on the level of Lie algebras. It is worth stressing, that this problem has a great practical importance in physics and is known as a control problem for dynamical systems. In this formalism elements of a Lie algebra \mathfrak{g} are called *Hamiltonians*. There were many attempts to formulate universality criteria for Hamiltonians, e.g. Lie rank condition [42, 53]. Another possible approaches, that use representation theory of Lie algebras can be found in [82, 81, 84]. Section 4.1.2 includes the necessary universality criterion for quantum gates, that was derived using an analogous approach as in the Section 4.1.1. Next, we will describe in Section 4.1.3 how to construct Hamiltonians from quantum gates and vice versa and show differences between universality criteria on the level of Lie groups and Lie algebras. The main purpose of Section 4.2 is to derive the sufficient universality criterion and express it in terms of spectra of elements of \mathcal{S} . The section is divided into two parts. In the first one we will specify a distance between two elements of \mathcal{S} , say g, h , and the neutral element of G such, that $\langle g, h \rangle = G$. In the latter part of Section 4.2 we will generalize the sufficient universality criterion for the case, when elements of \mathcal{S} are not close enough to the neutral element. We will also introduce some auxiliary concepts, such as a maximal exponent and an exceptional spectrum, that will be used in searching for possible generators of finite subgroups of G . Section 4.3 is the main part of this chapter and it contains an algorithm for deciding universality using the necessary and sufficient universality criterion. We will show that the algorithm always terminates after a finite number of steps and this number will be discussed in the latter part of this section. In Section 4.4 we present the universality criteria formulated for the special case, when $G = SU(2)$ or $G = SO(3)$ and \mathcal{S} is a two-element set. Finally, we will also show, how to deal with non-universal sets by embedding them into groups of higher dimensions.

Results presented in this chapter were published in [70, 71] and are the main part of this thesis.

4.1. Necessary universality criterion

Before we derive the necessary universality criterion using properties of compact semisimple Lie algebras and Lie groups, we introduce the notation used in this chapter. Let $\mathcal{S} = \{g_1, \dots, g_n\} \subset G$ denote a set of group elements and $\mathcal{X} = \{X_1, \dots, X_k\}$ be a set of elements of a Lie algebra \mathfrak{g} . The set consisting of matrices that commute with \mathcal{S} (or \mathcal{X}) will be called *commutant* and denoted by $\mathcal{C}(\mathcal{S})$ (or $\mathcal{C}(\mathcal{X})$, respectively). The concept of the commutant can be generalized for an arbitrary finite or infinite set \mathcal{V} of $d \times d$ matrices over a field \mathbb{K} as:

$$\mathcal{C}(\mathcal{V}) = \{L \in \mathbb{M}_d(\mathbb{K}) : \forall v \in \mathcal{V} [L, v] = 0\}. \quad (4.1)$$

4.1.1. Universality criterion for compact, semisimple Lie algebras

The universality criterion presented in this section is equivalent to the approaches from [42, 53, 82, 81, 84]. The main difference is that it can be easily applied on the level of Lie groups and does not require detailed knowledge about representations of $\mathfrak{su}(d)$ and $\mathfrak{so}(d)$.

Let us start from a definition of a universal set of Hamiltonians.

Definition 4.1. Let $\mathcal{X} = \{X_1, \dots, X_n\}$ be a finite subset of a Lie algebra \mathfrak{g} . \mathcal{X} is said to generate \mathfrak{g} (equivalently, \mathcal{X} is universal) if commutators of finite length between elements of \mathcal{X} , called Hamiltonians, form a basis of \mathfrak{g} , i.e. every $X \in \mathfrak{g}$ can be represented as a finite linear combination of X_i 's and finitely nested commutators of X_i 's:

$$X = \sum_{i=1}^n \alpha_i X_i + \sum_{i,j=1}^n \alpha_{i,j} [X_i, X_j] + \dots, \quad (4.2)$$

where $\alpha_i, \alpha_{i,j} \in \mathbb{R}, \mathbb{C}$ depending if \mathfrak{g} is a real or complex Lie algebra, respectively.

Let $\mathcal{C}(\mathfrak{g})$ denote the commutant of \mathfrak{g} and $\mathcal{C}(\mathcal{X})$ be the commutant of $\mathcal{X} = \{X_1, \dots, X_n\} \subset \mathfrak{g}$. Note first, that obviously $\langle \mathcal{X} \rangle = \mathfrak{g}$ implies that $\mathcal{C}(\mathfrak{g}) = \mathcal{C}(\mathcal{X})$. However, we will show in the following example that the reverse statement is not always true.

Example 4.1. [71] Let us consider a subset \mathcal{X} of $\mathfrak{su}(4)$. The commutant of this algebra is equal to $\mathcal{C}(\mathfrak{su}(4)) = \{\lambda I, \lambda \in \mathbb{C}\}$, which stems from Theorem 2.14.

Assume that $\mathcal{X} = \{X_1 \otimes I, X_2 \otimes I, I \otimes X_1, I \otimes X_2\} \subset \mathfrak{su}(4)$, where $X_1, X_2 \in \mathfrak{su}(2)$ generate $\mathfrak{su}(2)$. Notice, that $\langle \mathcal{X} \rangle \neq \mathfrak{su}(4)$ but $\langle \mathcal{X} \rangle = \mathfrak{su}(2) \oplus \mathfrak{su}(2)$. However, $\mathcal{C}(\mathcal{X})$ is also equal to $\{\lambda I, \lambda \in \mathbb{C}\}$. In order to show it, notice that $\mathfrak{su}(2) \oplus I \subset \langle \mathcal{X} \rangle$ commute with every matrix of the form $I \oplus X$, $X \in \mathfrak{su}(2)$ and elements $I \oplus \mathfrak{su}(2) \subset \langle \mathcal{X} \rangle$ commute with every matrix of the form $X \oplus I$, $X \in \mathfrak{su}(2)$. Hence $\mathcal{C}(\mathcal{X}) = \{\lambda I\} = \mathcal{C}(\mathfrak{su}(4))$ although $\langle \mathcal{X} \rangle \neq \mathfrak{su}(4)$.

The above example shows, that equality of commutants for defining representation is not sufficient to decide universality. It turns out, that the crucial concept is the adjoint representation $\text{ad} : \mathfrak{g} \mapsto \mathfrak{so}(\mathfrak{g})$.

Theorem 4.2 (Universality criterion for Lie algebras [70, 71]). Let \mathfrak{g} be a compact semisimple Lie algebra and $\mathcal{X} = \{X_1, \dots, X_n\} \subset \mathfrak{g}$ its finite subset. \mathcal{X} generates \mathfrak{g} if and only if $\mathcal{C}(\text{ad}_{\mathfrak{g}}) = \mathcal{C}(\text{ad}_{\mathcal{X}})$.

Proof. Assume that \mathfrak{g} is a semisimple Lie algebra with n components, i.e. $\mathfrak{g} = \bigoplus_{i=1}^n \mathfrak{g}_i$. In what follows we will denote by $\mathfrak{h} \subset \mathfrak{g}$ the Lie algebra generated by \mathcal{X} . Assume that $\mathfrak{h} \neq \mathfrak{g}$ but $\mathcal{C}(\text{ad}_{\mathfrak{g}}) = \mathcal{C}(\text{ad}_{\mathcal{X}})$. The equality of commutants implies that \mathfrak{h} has nonzero intersection with every simple component of \mathfrak{g} , otherwise $\mathcal{C}(\text{ad}_{\mathcal{X}})$ must be larger than $\mathcal{C}(\text{ad}_{\mathfrak{g}})$.

Using the Killing form we can decompose \mathfrak{g} into a direct product of orthogonal vector spaces $\mathfrak{g} = \mathfrak{h} \oplus \mathfrak{h}^\perp$. Therefore, for $X \in \mathfrak{h}$ operators ad_X respect the decomposition $\mathfrak{g} = \mathfrak{h} \oplus \mathfrak{h}^\perp$ and have a block diagonal structure:

$$\text{ad}_X = \begin{pmatrix} \text{ad}_X|_{\mathfrak{h}} & 0 \\ 0 & \text{ad}_X|_{\mathfrak{h}^\perp} \end{pmatrix}. \quad (4.3)$$

In the next step of the proof we will find an operator that commutes with any ad_X , $X \in \mathfrak{h}$. Such an operator is the orthogonal, with respect to the Killing form, projection operator onto \mathfrak{h} , which will be denoted by $P : \mathfrak{g} \rightarrow \mathfrak{h}$. Note, however, that $P \in \mathcal{C}(\text{ad}_{\mathfrak{g}})$ implies that \mathfrak{h} would be an ideal of \mathfrak{g} . But the only ideals of \mathfrak{g} are direct sums of its simple components. Thus \mathfrak{h} is either \mathfrak{g} which is a contradiction or \mathfrak{h} is a direct sum of $k < n$ simple components of \mathfrak{g} which is again a contradiction. \square

In particular, if \mathfrak{g} is a simple Lie algebra, then by the virtue of Theorem 2.14 and by the Fact 2.8 we obtain immediately:

Corollary 4.3. *Let \mathfrak{g} be a compact simple Lie algebra and $\mathcal{X} = \{X_1, \dots, X_n\} \subset \mathfrak{g}$ be its finite subset. \mathcal{X} generates \mathfrak{g} if and only if $\mathcal{C}(\text{ad}_{\mathfrak{g}}) = \{\lambda I : \lambda \in \mathbb{R}\}$.*

Remark 4.1. *It is worth stressing that universality criteria on the level of Lie groups require additional conditions comparing to the level of Lie algebras. In particular, the analogous criteria to Theorem 4.4 and Corollary 4.5 can be satisfied also by a set \mathcal{S} generating a finite group. Therefore in case of Lie groups we need an additional criterion providing that $\langle \mathcal{S} \rangle$ is infinite.*

4.1.2. Necessary universality condition for compact semisimple Lie groups

The main purpose of this section is to formulate an analogous criterion as Theorem 4.2 on the level of Lie groups. To this end we assume that a considered Lie group is compact and connected, which implies that the exponential map is surjective.

Let $\mathcal{C}(\text{Ad}_G) = \{L \in \text{End}(\mathfrak{g}) : \forall g \in G [\text{Ad}_g, L] = 0\}$, where $\text{Ad} : G \mapsto SO(\mathfrak{g})$ is the adjoint representation of G , be the space of endomorphisms of \mathfrak{g} that commute with all Ad_g , where $g \in G$. From Jacobi identity we know, that:

- $\mathcal{C}(\text{Ad}_G)$ is a Lie subalgebra of $\text{End}(\mathfrak{g})$.
- If $L \in \text{End}(\mathfrak{g})$ commutes with Ad_g and Ad_h then it also commutes with Ad_{gh} .

In what follows we will denote by $\mathcal{C}(\text{Ad}_{\mathcal{S}})$ the solution set of

$$[\text{Ad}_{g_1}, \cdot] = 0, \dots, [\text{Ad}_{g_n}, \cdot] = 0.$$

Again, it is clear that $\mathcal{C}(\text{Ad}_G) = \mathcal{C}(\text{Ad}_{\mathcal{S}})$ if \mathcal{S} generates G . As we will show in the following, the converse is true only if G is compact, connected, semisimple and infinite.

Theorem 4.4 (Necessary universality condition [70, 71]). *Let G be a compact connected semisimple Lie group and $\mathcal{S} = \{g_1, \dots, g_n\} \subset G$ be its finite subset such that $\langle \mathcal{S} \rangle$ has infinite number of elements and the projection of $\langle \mathcal{S} \rangle$ onto every simple component of G is also infinite. \mathcal{S} generates G if and only if $\mathcal{C}(\text{Ad}_G) = \mathcal{C}(\text{Ad}_{\mathcal{S}})$.*

Proof. The proof of Theorem 4.4 is analogous to the proof of Theorem 4.2. Let us denote by H the group generated by \mathcal{S} , i.e. $H = \langle \mathcal{S} \rangle$ and by H_e the identity component of H . Recall that H_e is a normal subgroup of H . By our assumption H is a compact but not necessarily connected Lie group that contains infinite number of elements, like in Figure 4.2. Let $\mathfrak{h} \subset \mathfrak{g}$ be

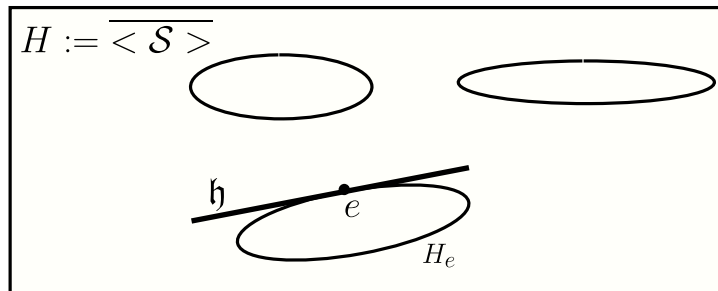


Figure 4.2: The proof of Theorem 4.2.

the Lie algebra of H_e and let m be the number of simple components of $\mathfrak{g} = \text{Lie}(G)$. Under the assumption $\mathcal{C}(\text{Ad}_G) = \mathcal{C}(\text{Ad}_S)$, \mathfrak{h} has nonzero intersection with every simple component of \mathfrak{g} . By the analogy to Theorem 4.2 assume that $\mathfrak{h} \neq \mathfrak{g}$ but $\mathcal{C}(\text{Ad}_G) = \mathcal{C}(\text{Ad}_S)$. Using the Killing form we can decompose \mathfrak{g} into a direct product of vector spaces $\mathfrak{g} = \mathfrak{h} \oplus \mathfrak{h}^\perp$. For any $g \in H$, $X \in \mathfrak{h}$ and $Y \in \mathfrak{h}^\perp$ we have $\text{Ad}_g Y \in \mathfrak{h}$ and $\text{Ad}_g Y \in \mathfrak{h}^\perp$. The latter is true as $B(\text{Ad}_g Y, X) = B(Y, \text{Ad}_{g^{-1}} X) = 0$, for any $X \in \mathfrak{h}$. Therefore, for $h \in H$ the operators Ad_h respect the decomposition $\mathfrak{g} = \mathfrak{h} \oplus \mathfrak{h}^\perp$ and have a block diagonal structure:

$$\text{Ad}_h = \begin{pmatrix} \text{Ad}_h|_{\mathfrak{h}} & 0 \\ 0 & \text{Ad}_h|_{\mathfrak{h}^\perp} \end{pmatrix}. \quad (4.4)$$

Let $P : \mathfrak{g} \rightarrow \mathfrak{h}$ be the orthogonal projection with respect to the Killing form onto \mathfrak{h} . Then obviously $[P, \text{Ad}_h] = 0$ for any $h \in H$. Note, however, that if P belonged to $\mathcal{C}(\text{Ad}_G)$ then \mathfrak{h} would be Ad_G invariant subspace of \mathfrak{g} . But the only Ad -invariant subspaces of \mathfrak{g} are simple components of \mathfrak{g} . Hence either $\mathfrak{h} = \mathfrak{g}$ which is a contradiction or \mathfrak{h} is a direct sum of $k < n$ simple components of \mathfrak{g} which again is a contradiction as \mathfrak{h} has nonzero intersection with all m simple components. \square

If G is a simple Lie group, then using Theorem 2.14 we can simplify Theorem 4.4 as follows:

Theorem 4.5. [70, 71] *Let G be a compact connected simple Lie group and $\mathcal{S} = \{g_1, \dots, g_n\}$ be its finite subset. Assume $\langle \mathcal{S} \rangle$ is infinite. The set \mathcal{S} generates G if and only if $\mathcal{C}(\text{Ad}_G) = \{\lambda I : \lambda \in \mathbb{R}\}$.*

Let us finish this section with some additional remarks regarding calculation of $\mathcal{C}(\text{Ad}_S)$. Assume that $\text{vec}(L)$ is the vectorization of matrix L , i.e. the vector obtained by stacking the columns of the matrix L on top of one another. One easily calculates that

$$[L, \text{Ad}_g] = 0 \Leftrightarrow (I \otimes \text{Ad}_g - \text{Ad}_{g^\dagger} \otimes I) \text{vec}(L) = 0.$$

Next, we define the matrix

$$L_{\mathcal{S}} = \begin{pmatrix} I \otimes \text{Ad}_{g_1} - \text{Ad}_{g_1^\dagger} \otimes I \\ \vdots \\ I \otimes \text{Ad}_{g_n} - \text{Ad}_{g_n^\dagger} \otimes I \end{pmatrix}. \quad (4.5)$$

Then the problem of checking the necessary universality criterion simplifies to computing the kernel of $L_{\mathcal{S}}$ and it can be reformulated as follows:

Lemma 4.6. [71] *$\mathcal{C}(\text{Ad}_S) = \{\lambda I : \lambda \in \mathbb{R}\}$ if and only if the kernel of $L_{\mathcal{S}}$ is one-dimensional.*

4.1.3. Gates and their Lie algebra elements

Assume that we have a n -element set \mathcal{X} of d -level Hamiltonians and we want to use them to construct a set \mathcal{S} of one-qudit gates (or vice versa). In this section we will describe such a construction in details and show, when the spaces $\mathcal{C}(\text{Ad}_S)$ and $\mathcal{C}(\text{ad}_{\mathcal{X}})$ can be different.

First, we will explain how to assign the set of Lie algebra elements \mathcal{X} to any set of gates \mathcal{S} and easily compute their adjoint representation. In what follows, whenever we speak about the Lie algebra elements associated to gates we mean matrices constructed according to the procedures presented in this section.

It is known [41] that every unitary matrix $U \in SU(d)$ is diagonalizable, i.e. there is a unitary matrix $V \in SU(d)$ such that $D = V^\dagger U V = \text{diag}\{e^{i\phi_1}, \dots, e^{i\phi_d}\}$, where the nonzero entries of D constitute the spectrum of U and ϕ_1, \dots, ϕ_d are called *spectral angles*. The corresponding Lie algebra element $X \in \mathfrak{su}(d)$ can be derived by calculating a logarithm of U . This can be done using the decomposition $U = V D V^\dagger$ and it boils down to calculating logarithms of the diagonal matrix D . As the logarithm of $z \in \mathbb{C}$ is not uniquely defined we will use the convention that $\log z = \arg(z)$, where $\arg(z)$ is the argument of z and we assume $\arg(z) \in [0, 2\pi)$.

Let us choose $X \in \mathfrak{su}(d)$ that satisfies $U = e^X$. Using the decomposition $U = V D V^\dagger$ we get

$$X = V \tilde{D} V^\dagger, \quad \tilde{D} = \text{diag}\{i\phi_1, \dots, i\phi_d\}, \text{ where } \phi_i \in [0, 2\pi).$$

This way we assign the set of Lie algebra elements $\mathcal{X} = \{X_1, \dots, X_n\} \subset \mathfrak{su}(d)$ to any set of gates $\mathcal{S} = \{U_1, \dots, U_n\} \subset SU(d)$.

Matrices in $SO(d)$ typically cannot be diagonalized by the orthogonal group as their eigenvalues are complex numbers [41]. Nevertheless orthogonal transformation allows to transform any $O \in SO(d)$ to a block diagonal form $R = V^t O V$ with two types of blocks:

1. one identity matrix I_k of dimension $0 \leq k \leq d$,
2. 2×2 rotations by angles $\phi_i \in (0, 2\pi)$, i.e. matrices $O(\phi_i)$ from $SO(2)$.

Let us again find $X \in \mathfrak{so}(d)$ such that $O = e^X$. Throughout this chapter we choose $X = V \tilde{R} V^t$, where \tilde{R} has the same block diagonal structure as R and

1. the block corresponding to the identity block of R is the zero matrix 0_k of dimension $0 \leq k \leq d$,
2. the blocks corresponding to 2×2 ϕ_i -rotation blocks of R are matrices $\begin{pmatrix} 0 & \phi_i \\ -\phi_i & 0 \end{pmatrix} \in \mathfrak{so}(2)$, where every $\phi_i \in (0, 2\pi)$.

Using the above procedure, to any set of gates $\mathcal{S} = \{O_1, \dots, O_n\} \subset SO(d)$ we assign the set of Lie algebra elements $\mathcal{X} = \{X_1, \dots, X_n\} \subset \mathfrak{so}(d)$.

In Sections 4.1.3.1 and 4.1.3.2 we will compute adjoint representation for diagonalized elements of the groups $SU(d)$, $SO(d)$ and their Lie algebra elements.

4.1.3.1. The case of $SU(d)$

Let us diagonalize a matrix $U_i \in \mathcal{S}$ as $U_i = V_i D_i V_i^\dagger$, where $V_i \in SU(d)$ and $D_i = \{e^{i\phi_1^i}, \dots, e^{i\phi_d^i}\}$, $\phi_j^i \in [0, 2\pi)$. Next, notice that the adjoint representation is a group homomorphism, therefore it satisfies

$$\text{Ad}_{U_i} = \text{Ad}_{V_i D_i V_i^\dagger} = O_i \text{Ad}_{D_i} O_i^t, \quad O = \text{Ad}_{V_i} \in SO(d^2 - 1).$$

Let us order the standard basis of $\mathfrak{su}(d)$ as follows

$$\{X_{12}, Y_{12}, \dots, X_{d-1,d}, Y_{d-1,d}, Z_{1,2}, \dots, Z_{d-1,d}\}.$$

Direct calculations show that the matrix Ad_{D_i} in this basis has a block diagonal form:

$$\text{Ad}_{D_i} = \begin{pmatrix} O(\phi_{1,2}^i) & & & & \\ & \ddots & & & \\ & & O(\phi_{1,d}^i) & & \\ & & & \ddots & \\ & & & & O(\phi_{2,d}^i) & \\ & & & & & \ddots & \\ & & & & & & O(\phi_{d-1,d}^i) \\ & & & & & & & I_{d-1} \end{pmatrix}, \quad (4.6)$$

where

$$O(\phi_{k,l}^i) = \begin{pmatrix} \cos(\phi_{k,l}^i) & \sin(\phi_{k,l}^i) \\ -\sin(\phi_{k,l}^i) & \cos(\phi_{k,l}^i) \end{pmatrix}, \text{ where, } \phi_{k,l}^i := \phi_k^i - \phi_l^i, \quad (4.7)$$

and I_{d-1} is the $(d-1) \times (d-1)$ identity matrix. Note that $\phi_{k,l}^i \in (-2\pi, 2\pi)$ as $\phi_k, \phi_l \in [0, 2\pi)$.

Similarly, elements of \mathcal{X} corresponding to elements of \mathcal{S} are given by $X_i = V_i \tilde{D}_i V_i^\dagger$ and $\tilde{D}_i = i\{\phi_1^i, \phi_2^i, \dots, \phi_d^i\}$. Hence $\text{ad}_{X_i} = \text{ad}_{V_i \tilde{D}_i V_i^\dagger} = O \text{ad}_{\tilde{D}_i} O^t$, and we have (in the standard basis of $\mathfrak{su}(d)$ ordered as previously):

$$\text{ad}_{\tilde{D}_i} = \begin{pmatrix} X(\phi_{1,2}^i) & & & & \\ & \ddots & & & \\ & & X(\phi_{1,d}^i) & & \\ & & & \ddots & \\ & & & & X(\phi_{2,d}^i) & \\ & & & & & \ddots & \\ & & & & & & X(\phi_{d-1,d}^i) \\ & & & & & & & 0_{d-1} \end{pmatrix}, \quad (4.8)$$

where

$$X(\phi_{k,l}^i) = \begin{pmatrix} 0 & \phi_{k,l}^i \\ -\phi_{k,l}^i & 0 \end{pmatrix}, \text{ where, } \phi_{k,l}^i = \phi_k^i - \phi_l^i, \quad (4.9)$$

and 0_{d-1} is $(d-1) \times (d-1)$ zero matrix.

Comparing structures of matrices Ad_{D_i} and $\text{Ad}_{\tilde{D}_i}$ we deduce that the only situation when $\mathcal{C}(\text{Ad}_{\mathcal{S}})$ can be larger than $\mathcal{C}(\text{ad}_{\mathcal{X}})$ is when at least one spectral angle of $\text{Ad}_{\tilde{D}_i}$ satisfies $\phi_{k,l}^i = \pm\pi$. In this case Ad_{D_i} has additional degeneracy compared to $\text{ad}_{\tilde{D}_i}$ as $O(\phi_{k,l}^i) = O(\pm\pi) = -I_2$ and one can construct a rotation matrix from $SO(d^2 - 1)$ that commutes with Ad_{D_i} .

Let $P_{k,l}$ be the rotation plane corresponding to the angle $\phi_{k,l}^i = \pm\pi$. Define a rotation $O^{k,l} \in SO(d^2 - 1)$ whose elementary rotation planes are exactly as in $\text{Ad}_{\tilde{D}_i}$ except $P_{k,l}$ which is replaced by a plane P' such, that $P_{k,l} \perp P'$. This can be achieved using available $d-1$ directions corresponding to I_{d-1} . As we will show in Section 4.4 orthogonal rotations by angle π commute with each other, therefore $[\text{Ad}_{U_i}, O^{k,l}] = 0$ and $[\text{ad}_{X_i}, O^{k,l}] \neq 0$. Hence the space $\mathcal{C}(\text{Ad}_{U_i})$ is larger than $\mathcal{C}(\text{ad}_{X_i})$ and there is possibility that it might be true also for sets $\mathcal{C}(\text{Ad}_{\mathcal{S}})$ and $\mathcal{C}(\text{ad}_{\mathcal{X}})$. As a conclusion we get

Fact 4.1. [70, 71] Let $S = \{U_1, \dots, U_n\} \subset SU(d)$ and $\mathcal{X} = \{X_1, \dots, X_n\}$ be the corresponding set of Lie algebra elements (constructed as described in Section 4.1.3). The space $\mathcal{C}(\text{Ad}_S)$ can be larger than $\mathcal{C}(\text{ad}_{\mathcal{X}})$ if and only if the difference between spectral angles for at least one of the matrices $U_i \in \mathcal{S}$ is equal to $\pm\pi$.

4.1.3.2. The case of $SO(d)$

The procedure presented in this paragraph consists of the same steps as in Section 4.1.3.1. Again, let $O_i \in \mathcal{S}$ be put into a block diagonal form $O_i = V_i R_i V_i^\dagger$, where $V_i \in SO(d)$ and R_i is a block diagonal matrix described in the beginning of this section. Note next that

$$\text{Ad}_{O_i} = \text{Ad}_{V_i R_i V_i^\dagger} = \text{Ad}_{V_i} \text{Ad}_{R_i} \text{Ad}_{V_i}^t.$$

Direct calculations show that each matrix Ad_{R_i} can be brought to the standard block diagonal form containing the following blocks

1. $O(\phi_{a,b}^i)$ and $O(\psi_{a,b}^i)$, where $\phi_{a,b}^i = \phi_a^i - \phi_b^i$, $\psi_{a,b}^i = \phi_a^i + \phi_b^i$, $a < b$. The number of these blocks is $k(k-1)$.
2. The identity block of dimension $k + \frac{(d-2k)(d-2k-1)}{2}$.
3. $k(d-2k)$ blocks $O(\phi_j^i)$, where $j \in \{1, \dots, k\}$.

Matrices ad_{X_i} have the same structure as matrices Ad_{O_i} , i.e. they consist of

1. $k(k-1)$ blocks of the form $\begin{pmatrix} 0 & \phi_{a,b}^i \\ -\phi_{a,b}^i & 0 \end{pmatrix} \in \mathfrak{so}(2)$ and $\begin{pmatrix} 0 & \psi_{a,b}^i \\ -\psi_{a,b}^i & 0 \end{pmatrix} \in \mathfrak{so}(2)$, where $\phi_{a,b}^i = \phi_a^i - \phi_b^i$, $\psi_{a,b}^i = \phi_a^i + \phi_b^i$, $a < b$.
2. The zero block of dimension $k + \frac{(d-2k)(d-2k-1)}{2}$.
3. $k(d-2k)$ blocks $\begin{pmatrix} 0 & \phi_j^i \\ -\phi_j^i & 0 \end{pmatrix} \in \mathfrak{so}(2)$, where $j \in \{1, \dots, k\}$.

Repeating the reasoning for $SU(d)$ we get:

Fact 4.2. [71] Let $S = \{O_1, \dots, O_n\} \subset SO(d)$ and $\mathcal{X} = \{X_1, \dots, X_n\} \subset \mathfrak{so}(d)$ be the corresponding set of Lie algebra elements (constructed as described in Section 4.1.3). The space $\mathcal{C}(\text{Ad}_S)$ can be bigger than $\mathcal{C}(\text{ad}_{\mathcal{X}})$ if and only if the difference or the sum of spectral angles ϕ_a^i and ϕ_b^i for at least one of the matrices $O_i \in \mathcal{S}$ is an odd multiple of π .

4.2. Sufficient universality criterion

Having defined the necessary universality criterion, we can formulate criteria providing that $\langle \mathcal{S} \rangle$ is infinite. It is worth stressing that the problem of deciding if a finitely generated group is infinite has been studied intensively and there are some algorithms that allow checking this property (see e.g. [4, 5, 24, 23]). However, our aim was to base our reasoning on the set of basic properties of compact connected simple Lie groups and make it as simple as possible. Therefore our inspiration was rather a result of Kuranishi [51] who proved that $\mathcal{S} \subset G$ generated G if its elements did not commute and were *close enough* to the neutral element of G (see also [31]). In the following we will specify this distance and express it in terms of spectra of elements from \mathcal{S} . On the other hand our approach for checking if $\langle \mathcal{S} \rangle$ is infinite is also related to [32, 43], however the conceptual differences in both approaches are significant and the methods should be treated as independent.

4.2.1. Conditions for $\langle \mathcal{S} \rangle$ to be infinite

We start this section from defining open balls in G of radius $r = 1/\sqrt{2}$ that are centered around elements from $Z(G)$:

$$B_\alpha = \{g \in G : \|g - \alpha I\| < 1/\sqrt{2}\}, \quad \alpha I \in Z(G), \quad (4.10)$$

$$\mathcal{B} = \bigcup_{\alpha I \in Z(G)} B_\alpha. \quad (4.11)$$

As we will show in the following a finite subset of B_1 generates G if and only if the corresponding Lie algebra elements generate \mathfrak{g} .

Lemma 4.7. [71] *Let $g, h \in B_1$ and assume $[g, h]_\bullet \neq I$. The group $\overline{\langle g, h \rangle}$ generated by g, h is infinite.*

Proof. We will prove this lemma by induction. Define the sequence $g_0 = g$, $g_1 = [g_0, h]_\bullet$, $g_n = [g_{n-1}, h]_\bullet$. By our assumptions $\|h - I\| = d \leq 1/\sqrt{2}$. Therefore using Lemma 2.17 we get

$$\|g_n - I\| \leq \sqrt{2}d \|g_{n-1} - I\|.$$

Thus $\|g_n - I\| \leq (\sqrt{2}d)^n \|g - I\|$ and $g_n \rightarrow I$, when $n \rightarrow \infty$. Now assume that the sequence is finite, i.e. for some N we have $g_N = I$. By Lemma 2.17 that means $[g_{N-1}, h]_\bullet = I$. But $g_{N-1} = [g_{N-2}, h]_\bullet$, hence $[g_{N-2}, h]_\bullet = I$. Repeating this argument for any $1 < k < N - 1$ we get $[g, h]_\bullet = I$ which is a contradiction. Therefore $\langle g, h \rangle$ is infinite. \square

This result can be generalized for g, h that are close enough to *arbitrary* elements of $Z(G)$.

Corollary 4.8. *Let $g \in B_{\alpha_1}$ and $h \in B_{\alpha_2}$, where α_1 and α_2 are such that $\alpha_1 I, \alpha_2 I \in Z(G)$ and assume $[g, h]_\bullet \notin Z(G)$. Then the group $\overline{\langle g, h \rangle}$ is infinite.*

Proof. If $\alpha_1 = \alpha_2 = 1$ the result follows directly from Lemma 4.7. For all other α_i 's let $g' = \alpha_1^{-1}g$ and $h' = \alpha_2^{-1}h$. Then $h', g' \in B_1$ and $[g', h']_\bullet \neq I$. Thus by Lemma 4.7, $\langle g', h' \rangle$ is infinite. Note that $\langle g, h \rangle$ equal to $\langle g', h' \rangle$ is up to the finite covering and therefore is infinite too. \square

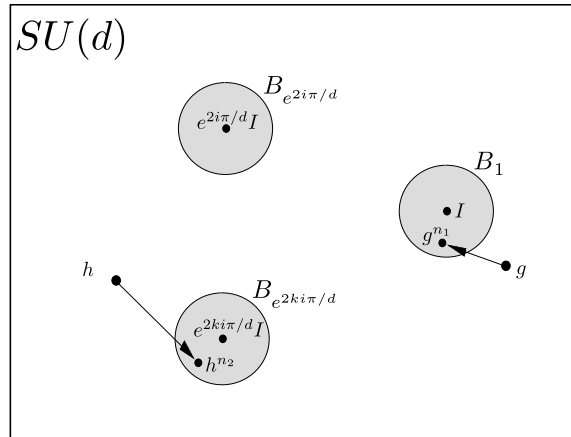


Figure 4.3: The group $SU(d)$ with the exemplary open balls B_α centered at elements from $Z(SU(d))$.

In what follows we provide explicit conditions for elements of G to belong to balls B_α in terms of their spectra. To this end let $\alpha_m I$ be the elements of $Z(G)$. By the definition of the Frobenius norm (2.39):

$$\|g - \alpha_m I\|^2 = \text{tr}(g - \alpha_m I)(g^* - \alpha_m^* I) = 2\text{tr}I - \alpha_m^* \text{tr}g - \alpha_m \text{tr}g^*. \quad (4.12)$$

Recall that central elements of $SU(d)$ are of the form αI , where $\alpha_m = e^{2im\pi/d}$. Let $\{e^{i\phi_1}, e^{i\phi_2}, \dots, e^{i\phi_d}\}$ be the spectrum of $U_d \in SU(d)$. The conditions for $U_d \in SU(d)$ to belong to the ball B_{α_m} read:

$$U_d \in B_{\alpha_m} \Leftrightarrow \sum_{i=1}^d \sin^2 \frac{\phi_i - 2m\pi/d}{2} < \frac{1}{8}, \quad \sum_{i=1}^d \phi_i = 0 \pmod{2\pi}. \quad (4.13)$$

The center of $SO(2k+1)$ is trivial and hence we have only one ball B_1 . Let $\{1, e^{i\phi_1}, e^{-i\phi_1}, \dots, e^{i\phi_k}, e^{-i\phi_k}\}$ be the spectrum of $O_{2k+1} \in SO(2k+1)$. We have

$$O_{2k+1} \in B_1 \Leftrightarrow \sum_{i=1}^k \sin^2 \frac{\phi_i}{2} < \frac{1}{16}. \quad (4.14)$$

Finally $Z(SO(2k)) = \{I, -I\}$ and we have two balls B_1, B_{-1} . Let

$$\{e^{i\phi_1}, e^{-i\phi_1}, \dots, e^{i\phi_k}, e^{-i\phi_k}\},$$

be the spectrum of O_{2k} . The conditions for the spectral angles are for the form

$$O_{2k} \in B_1 \Leftrightarrow \sum_{i=1}^k \sin^2 \frac{\phi_i}{2} < \frac{1}{16}, \quad (4.15)$$

$$O_{2k} \in B_{-1} \Leftrightarrow \sum_{i=1}^k \sin^2 \frac{\phi_i - \pi}{2} < \frac{1}{16}. \quad (4.16)$$

Theorem 4.9. [71] Let $\mathcal{S} = \{g_1, \dots, g_n\} \subset G$ be such that $g_i \in B_\alpha$, where $\alpha I \in Z(G)$ and let $\mathcal{X} = \{X_1, \dots, X_n\} \subset \mathfrak{g}$ be the Lie algebra elements assigned to \mathcal{S} (constructed as described in Section 4.1.3). \mathcal{S} generates G if and only if \mathcal{X} generates \mathfrak{g} .

Proof. Assume that matrices from \mathcal{S} generate an infinite subgroup and $\mathcal{C}(\text{Ad}_{\mathcal{S}}) = \mathcal{C}(\text{Ad}_G)$. Then by Theorem 4.4 we have $\overline{\langle \mathcal{S} \rangle} = G$. The situations when spaces $\mathcal{C}(\text{Ad}_{\mathcal{S}})$ and $\mathcal{C}(\text{ad}_{\mathcal{X}})$ can be different are characterized by Facts 4.1 and 4.2. Recall that for $\mathcal{S} \subset SU(d)$ the spaces $\mathcal{C}(\text{Ad}_{\mathcal{S}})$ and $\mathcal{C}(\text{ad}_{\mathcal{X}})$ may differ if and only if for one of the matrices $g_i \in \mathcal{S}$ we have $\phi_{a,b}^i = (2k+1)\pi$ and $\phi_{a,b}^i$ is a spectral angle of Ad_{g_i} . But then $\phi_a^i = \phi_b^i \pm \pi$ and for some m we arrive at

$$\sin^2 \frac{\phi_b^i \pm \pi - 2m\pi/d}{2} + \sin^2 \frac{\phi_b^i - 2m\pi/d}{2} = 1,$$

which means g_i does not satisfy (4.13).

Assume next that $\mathcal{S} \subset SO(d)$, then $\mathcal{C}(\text{Ad}_{\mathcal{S}})$ and $\mathcal{C}(\text{ad}_{\mathcal{X}})$ can differ if and only if the difference or the sum of spectral angles ϕ_a^i and ϕ_b^i is equal to an odd multiple of π . Then we get the conditions:

1. For odd d

$$\sin^2 \frac{\pm \phi_b^i \pm \pi}{2} + \sin^2 \frac{\phi_b^i}{2} = 1,$$

2. For even d

$$\begin{aligned} \sin^2 \frac{\pm \phi_b^i \pm \pi}{2} + \sin^2 \frac{\phi_b^i}{2} &= 1, \\ \sin^2 \frac{\pm \phi_b^i \pm \pi - \pi}{2} + \sin^2 \frac{\phi_b^i - \pi}{2} &= 1, \end{aligned}$$

which means g_i does not satisfy (4.14), (4.15) or (4.16). □

4.2.2. Universal sets for G

In this section we consider situation when not all the matrices belonging to \mathcal{S} are contained in \mathcal{B} . We already know that if there are two elements $g, h \in \overline{\langle S \rangle} \cap \mathcal{B}$ such that $[g, h]_\bullet \notin Z(G)$, then the group $\overline{\langle S \rangle}$ is infinite. We will show that for \mathcal{S} that satisfies the necessary universality criterion, i.e. $\mathcal{C}(\text{Ad}_{g_1}, \dots, \text{Ad}_{g_k}) = \{\lambda I\}$ this is actually an equivalence relation.

Lemma 4.10. [71] *Let $\mathcal{S} = \{g_1, \dots, g_k\} \subset G$ be such that $\mathcal{C}(\text{Ad}_{g_1}, \dots, \text{Ad}_{g_k}) = \{\lambda I\}$. The group $\overline{\langle S \rangle}$ is infinite **if and only if** there are at least two elements $g, h \in \overline{\langle S \rangle} \cap \mathcal{B}$ satisfying $[g, h]_\bullet \notin Z(G)$.*

Proof. Assume $\overline{\langle S \rangle}$ is infinite. Then under the assumption $\mathcal{C}(\text{Ad}_{\mathcal{S}}) = \{\lambda I\}$ we have $\overline{\langle S \rangle} = G$. Thus balls B_α must contain elements of $\langle S \rangle$ commuting to noncentral elements and the result follows. On the other hand if there are at least two elements $g, h \in \overline{\langle S \rangle}$ such that they belong to some balls B_α , where $\alpha I \in Z(G)$, and $[g, h]_\bullet \notin Z(G)$. Then $\overline{\langle S \rangle}$ is infinite by Corollary 4.8. \square

We already know that the necessary universality criterion places constraints on the structure of the infinite $\overline{\langle S \rangle}$. It turns out that this happens also when $\langle S \rangle$ is finite. The constraints regard the structure of $\langle S \rangle \cap \mathcal{B}$.

Lemma 4.11. [71] *Let $\mathcal{S} = \{g_1, \dots, g_n\} \subset G$ be such that $\mathcal{C}(\text{Ad}_{g_1}, \dots, \text{Ad}_{g_n}) = \{\lambda I\}$. Then either the intersection of $\langle S \rangle$ with \mathcal{B} is dense in \mathcal{B} or is a subgroup of $Z(G)$. In the first case $\overline{\langle S \rangle} = G$ and in the second one $\overline{\langle S \rangle}$ is finite.*

Proof. The group $\overline{\langle S \rangle}$ can be either infinite or finite. When it is infinite, then by the necessary universality condition, i.e. $\mathcal{C}(\text{Ad}_{g_1}, \dots, \text{Ad}_{g_n}) = \{\lambda I\}$, we have $\overline{\langle S \rangle} = G$ and it is obvious that $\mathcal{B} \cap \langle S \rangle$ is dense in \mathcal{B} . Assume next that $\langle S \rangle$ is finite. By Lemma 4.10 the group commutators of elements from $\mathcal{B} \cap \langle S \rangle$ belong to $Z(G)$. We first show that in fact they are equal to the identity, i.e. elements from $\mathcal{B} \cap \langle S \rangle$ commute. To see this let $h_1 \in B_{\alpha_1}$ and $h_2 \in B_{\alpha_2}$. Assume $[h_1, h_2]_\bullet \in Z(G)$. One can always find $\tilde{h}_1, \tilde{h}_2 \in B_1$ such that $h_1 = \alpha_1 \tilde{h}_1$ and $h_2 = \alpha_2 \tilde{h}_2$. We have:

$$[h_1, h_2]_\bullet = [\alpha_1 \tilde{h}_1, \alpha_2 \tilde{h}_2]_\bullet = \alpha_1 \tilde{h}_1 \alpha_2 \tilde{h}_2 \alpha_1^{-1} \tilde{h}_1^{-1} \alpha_2^{-1} \tilde{h}_2 = [\tilde{h}_1, \tilde{h}_2]_\bullet. \quad (4.17)$$

But by inequality (2.56) we have $[\tilde{h}_1, \tilde{h}_2]_\bullet \in B_1$ and it is also easy to see that B_{α_i} 's are disjoint. Thus $[h_1, h_2]_\bullet = I$. Next we note that each $B_\alpha \cap \langle S \rangle$ is invariant under the conjugation by elements from G . Let $\{h_1, \dots, h_m\}$ be all elements from $B_\alpha \cap \langle S \rangle$. Once again we can find elements $\{\tilde{h}_1, \dots, \tilde{h}_m\} \subset B_1$ satisfying $h_i = \alpha \tilde{h}_i$. Let $\mathfrak{g} \ni X_i = \log \tilde{h}_i$ (constructed as described in Section 4.1.3). Thus elements of $B_\alpha \cap \langle S \rangle$ are of the form $\{\alpha e^{X_1}, \dots, \alpha e^{X_m}\}$. We also know that $B_\alpha \cap \langle S \rangle$ is $\text{Ad}_{\mathcal{S}}$ invariant, i.e.

$$g_i \alpha e^{X_j} g_i^{-1} = \alpha \text{Ad}_{g_i} e^{X_j} = \alpha e^{X_r}, \quad g_i \in \mathcal{S}, \quad (4.18)$$

where $i \in \{1, \dots, n\}$ and $j, r \in \{1, \dots, m\}$. Thus we have $\text{Ad}_{g_i} e^{X_j} = e^{X_r}$. As the distance from the identity of the left and right side is smaller than 1 we have $\log \text{Ad}_{g_i} e^{X_j} = \log e^{X_r}$. By the construction, $\log e^{X_r} = X_r$ and from our definition of logarithm:

$$\log \text{Ad}_{g_i} e^{X_j} = \text{Ad}_{g_i} \log e^{X_j} = \text{Ad}_{g_i} X_j.$$

Hence $\text{Ad}_{g_i} X_j = X_r$ and the subspace $\{X_1, \dots, X_m\} \subset \mathfrak{g}$ is an invariant subspace for all matrices $\{\text{Ad}_{g_1}, \dots, \text{Ad}_{g_n}\}$. By the condition $\mathcal{C}(\text{Ad}_{g_1}, \dots, \text{Ad}_{g_n}) = \{\lambda I\}$ this subspace must be either 0 or \mathfrak{g} . Assume it is \mathfrak{g} . Recall that

$$[\alpha e^{X_i}, \alpha e^{X_j}] = 0, \quad i, j \in \{1, \dots, k\}.$$

Thus there is U such that $\alpha e^{X_i} = \alpha e^{U D_i U^{-1}}$, where D_i is diagonal. Hence $X_i = U D_i U^{-1}$. Thus matrices $\{X_1, \dots, X_m\}$ commute and we get a contradiction. Hence $\langle S \rangle \cap B_\alpha$ is either empty or αI . The result follows. \square

Lemma 4.11 leads to the following conclusion:

Corollary 4.12. *Let $\mathcal{S} = \{g_1, \dots, g_n\} \subset G$ be such that $\mathcal{C}(\text{Ad}_{g_1}, \dots, \text{Ad}_{g_n}) = \{\lambda I\}$. Then $\langle \mathcal{S} \rangle$ is infinite **if and only if** there is an element in $\langle \mathcal{S} \rangle$ that belongs to \mathcal{B} and does not belong to $Z(G)$.*

In general \mathcal{S} may contain elements that do not belong to \mathcal{B} . In the following we will show that we can move every element of G into B_α for some $\alpha I \in Z(G)$ by taking powers. Moreover there is a global upper bound for the required power, which stems from the fact that G is a compact group.

Fact 4.3. [71] *For groups $G = SU(d)$ and $G = SO(d)$ there is $N_G \in \mathbb{N}$ and some $q \in \mathbb{Z}_+$, $1 \leq q \leq N_G$, such that for every $g \in G$, $g^q \in B_{\alpha_m}$ for some $\alpha_m I \in Z(G)$.*

Proof. Let us first recall that by the Dirichlet theorem (see Theorem 2.8) for given real numbers x_1, x_2, \dots, x_n we can find $q \in \mathbb{Z}_+$ so that qx_1, \dots, qx_n all differ from integers by as little as we want. Let $\{\phi_1, \dots, \phi_k\}$ be the spectral angles of $g \in G$ and let $\phi_i = 2\pi x_i$, where $x_i \in [0, 1)$. By Theorem 2.8 we can always find q such that qx_i 's are close enough to integers to make g^q to belong to B_1 . For $g \in G$ let q_g be the smallest positive integer such that $g^{q_g} \in B_\alpha$ for some $\alpha I \in Z(G)$ (by Dirichlet theorem we know that $q_g < \infty$). Let $\mathcal{O}_g^{q_g}$ be an open neighborhood¹ of g such that for any $h \in \mathcal{O}_g^{q_g}$ we have $h^{q_g} \in B_\alpha$.² Let $\{\mathcal{O}_g^{q_g}\}_{g \in G}$ be the resulting open cover of G . As G is compact there is a finite subcover $\{\mathcal{O}_{g_i}^{q_{g_i}}\}$ and hence $N_G = \sup_i q_{g_i}$ is well defined and finite. \square

For $g \in G$ let $1 \leq q \leq N_G$ denote the smallest integer such that $g^q \in \mathcal{B}$. Using Corollary 4.12 we deduce that $\langle \mathcal{S} \rangle$ is finite if and only if for every $g \in \langle \mathcal{S} \rangle$ we have $g^q \in Z(G)$. This in turn places certain constraints on the spectra of elements belonging to $\langle \mathcal{S} \rangle$.

Definition 4.2. [70, 71] *Assume $g \notin \mathcal{B}$. The spectrum of g is exceptional if for some $1 \leq q \leq N_G$ we have $g^q \in Z(G)$.*

In other words the spectrum of g is exceptional if its spectrum satisfy one of the following conditions:

1. $g \in SU(d)$ and all spectral elements of g are q^{th} roots of $\alpha \in \mathbb{C}$, where $\alpha^d = 1$, for some fixed $1 \leq q \leq N_{SU(d)}$.
2. $g \in SO(2k+1)$ and all spectral elements of g are q^{th} roots of unity for some fixed $1 \leq q \leq N_{SO(2k+1)}$.
3. $g \in SO(2k)$ and all spectral elements of g are q^{th} roots of α , where $\alpha^2 = 1$, for some fixed $1 \leq q \leq N_{SO(2k+1)}$.

Notice that in all cases the set of exceptional spectra is a finite set. Using the definition of exceptional spectra we can reformulate Corollary 4.12 as follows:

Theorem 4.13. [71] *Let $\mathcal{S} = \{g_1, g_2, \dots, g_n\} \subset G$, where $G = SO(d)$ and $d \neq 4$ or $G = SU(d)$. Assume $\mathcal{C}(\text{Ad}_{g_1}, \dots, \text{Ad}_{g_n}) = \{\lambda I\}$ and that there is at least one element in \mathcal{S} for which the spectrum is not exceptional. Then $\langle \mathcal{S} \rangle = G$.*

¹This kind of a neighborhood exists as taking powers is a continuous operation.

²Note that there might be some $h \in \mathcal{O}_g^{q_g}$ for which q_g is not optimal but this will not play any role.

4.2.3. Maximal exponent N_G

We mentioned in the previous section that for every compact group G there is the *maximal exponent*, denoted by N_G such, that

$$\forall g \in G, \quad g^q \in Z(G), \quad 1 \leq q \leq N_G. \quad (4.19)$$

In Section 4.2.3.1 we will calculate the maximal exponent for $G = SU(2)$ and $G = SO(3)$ using Dirichlet's approximation theorem for one number (see Theorem [25]). We will also show that this approach enables to find an exact value of N_G . In Section 4.2.3.2 we will use Theorem 2.8 to find an upper bound for N_G in all other cases. We will also compare the obtained bound with numerical results and discuss the error.

4.2.3.1. Maximal exponent for $SU(2)$ and $SO(3)$

In this short section we prove the following fact:

Fact 4.4. $[71]$ $N_{SO(3)} = 12$ and $N_{SU(2)} = 6$.

Proof. Let $O \in SO(3)$ and let $[0, 2\pi) \ni \phi = 2a\pi$ be its spectral angle. By Theorem 2.7, for a given N there are integers p and $1 \leq q \leq N$ such that $|qa - p| \leq \frac{1}{N+1}$. Multiplying this inequality by π we get $|q\frac{\phi}{2} - p\pi| \leq \frac{\pi}{N+1}$. Note that (4.14) simplifies to $|\sin \frac{\psi}{2}| < \frac{1}{4}$, i.e. for a given ϕ we look for n such that $|q\frac{\phi}{2} - p\pi| < \arcsin \frac{1}{4}$. We combine these two observations to find the smallest N such that $\frac{\pi}{N+1} < \arcsin \frac{1}{4}$. Transforming this inequality we get:

$$N = \left\lceil \frac{\pi - \arcsin \frac{1}{4}}{\arcsin \frac{1}{4}} \right\rceil = 12. \quad (4.20)$$

Formula (4.20) gives an upper bound for $N_{SO(3)}$. Note however that for $\frac{\phi}{2} = \arcsin \frac{1}{4}$ the smallest q such that $|q \arcsin \frac{1}{4} - \pi| < \arcsin \frac{1}{4}$ is exactly $q = 12$ (see Figure 4.4(a)), hence $N_{SO(3)} = 12$. Assume next $U \in SU(2)$ and let $[0, 2\pi) \ni \phi = a\pi$ be its spectral angle. By Theorem 2.7 for a given N there are integers p and $1 \leq q \leq N$ such that $|qa - p| \leq \frac{1}{N+1}$. Recall, however, that $Z(SU(2)) = \{I, -I\}$, hence we need to multiply this inequality by $\frac{\pi}{2}$ instead of π , which yields $|q\frac{\phi}{2} - p\frac{\pi}{2}| \leq \frac{\pi}{2(N+1)}$. In this case (4.14) simplifies to $|\sin \frac{\psi}{2}| < \frac{1}{4}$ or $|\sin \frac{\psi-\pi}{2}| < \frac{1}{4}$, i.e. for a given ϕ we look for n such that $|q\frac{\phi}{2} - p\frac{\pi}{2}| < \arcsin \frac{1}{4}$. Combining these two observations we need to find the smallest N such that $\frac{\pi}{2(N+1)} < \arcsin \frac{1}{4}$. It is given by:

$$N = \left\lceil \frac{\frac{\pi}{2} - \arcsin \frac{1}{4}}{\arcsin \frac{1}{4}} \right\rceil = 6. \quad (4.21)$$

Formula (4.21) gives an upper bound for $N_{SU(2)}$, however direct calculations show that for $\frac{\phi}{2} = \arcsin \frac{1}{4}$ the smallest q for which $|q \arcsin \frac{1}{4} - \frac{\pi}{2}| < \arcsin \frac{1}{4}$ is exactly $q = 6$ (see figure 4.4(b)), hence $N_{SU(2)} = 6$. \square

Let us denote the sets of exceptional angles for $SU(2)$ and $SO(3)$ by $\mathcal{L}_{SU(2)}$ and $\mathcal{L}_{SO(3)}$ respectively. Their elements are of the form $\mathcal{L}_G = \{a\pi : a \in \mathcal{L}'_G\}$, where

$$\begin{aligned} \mathcal{L}'_{SU(2)} &= \{0, \frac{1}{2}, 1, \frac{3}{2}, \frac{1}{3}, \frac{2}{3}, \frac{4}{3}, \frac{5}{3}, \frac{1}{4}, \frac{3}{4}, \frac{5}{4}, \frac{7}{4}, \frac{1}{5}, \frac{2}{5}, \frac{3}{5}, \frac{4}{5}, \frac{6}{5}, \frac{7}{5}, \frac{8}{5}, \frac{9}{5}, \frac{1}{6}, \frac{5}{6}, \frac{7}{6}, \frac{11}{6}\}, \\ \mathcal{L}'_{SO(3)} &= \mathcal{L}'_{SU(2)} \cup \{\frac{2}{7}, \frac{4}{7}, \frac{6}{7}, \frac{8}{7}, \frac{10}{7}, \frac{12}{7}, \frac{2}{9}, \frac{4}{9}, \frac{8}{9}, \frac{10}{9}, \frac{14}{9}, \frac{16}{9}, \frac{2}{11}, \frac{4}{11}, \frac{6}{11}, \frac{8}{11}, \\ &\quad \frac{10}{11}, \frac{12}{11}, \frac{14}{11}, \frac{16}{11}, \frac{18}{11}, \frac{20}{11}\}. \end{aligned} \quad (4.22)$$

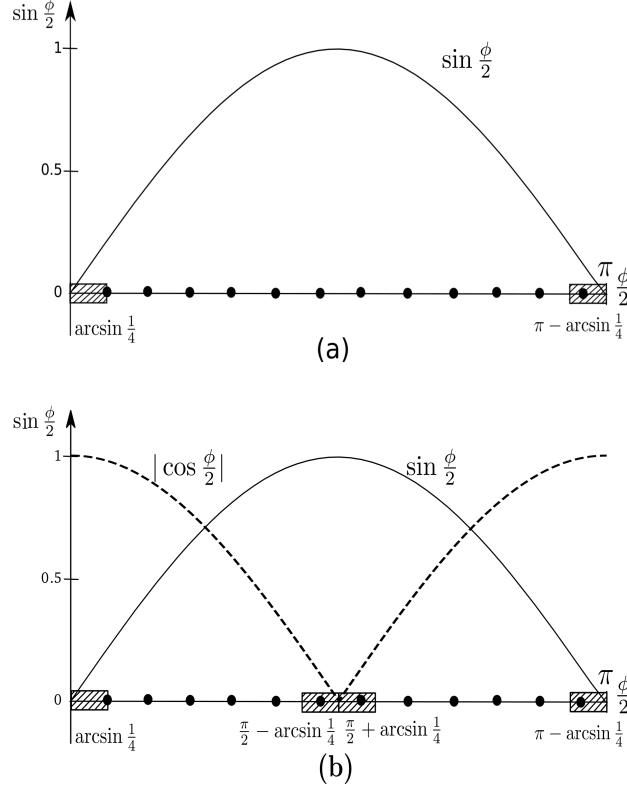


Figure 4.4: (a) Condition (4.14) for $SO(3)$. Black dots correspond to $n \arcsin \frac{1}{4}$ and dashed segments are determined by $|\sin \frac{\phi}{2}| < \frac{1}{4}$, (b) Conditions (4.13) for $U \in SU(2)$. Black dots corresponds to $n \arcsin \frac{1}{4}$ and dashed segments are determined by $|\sin \frac{\phi}{2}| < \frac{1}{4}$ or $|\sin \frac{\phi-\pi}{2}| < \frac{1}{4}$.

Using the Euler totient function we can easily calculate the number of exceptional angles for each group.

$$|\mathcal{L}_{SU(2)}| = \sum_{n=1}^6 \varphi(n) + \sum_{n=4}^6 \varphi(2n) = 24, \quad (4.23)$$

$$|\mathcal{L}_{SO(3)}| = \sum_{n=1}^{12} \varphi(n) = 46. \quad (4.24)$$

4.2.3.2. Maximal exponent for $SU(d)$, $d \geq 3$ and $SO(d)$, $d \geq 4$

In this section we will find upper bounds for N_G in case when $G = SU(d)$, $d \geq 3$ and $G = SO(d)$, $d \geq 4$. To this end we will use Dirichlet's approximation theorem in many dimensions [25, 38]. For reminder, this theorem describes how to approximate points of n -dimensional lattice of the volume $V = 1$ with rational coordinates with a given accuracy. More precisely, the theorem claims that there exists an integer $1 \leq q \leq N$ such, that a set of real numbers ζ_1, \dots, ζ_n can *simultaneously* approximate a set of integers p_1, \dots, p_n as:

$$\forall i = 1, \dots, n \quad |q\zeta_i - p_i| \leq \frac{1}{N^{1/n}}. \quad (4.25)$$

Notice, that we cannot apply Theorem 2.8 directly to our problem. The modifications that we need come from the fact that we cannot approximate *any* points of the lattice. To show this,

let $\phi_1, \phi_2, \dots, \phi_d$ be the spectral angles of $g \in G$ that we want to approximate with $\frac{k\pi}{d}$, $k \in \mathbb{Z}$ using simultaneous multiplication by some $q \in \mathbb{Z}_+$. The point is that the condition $g^q \in Z(G)$ places the following constraint on q :

1. In case when $G = SU(d)$

$$\begin{aligned} q\phi_1 &= \frac{2\pi m}{d} \bmod 2\pi, \\ &\dots \\ q\phi_d &= \frac{2\pi m}{d} \bmod 2\pi. \end{aligned}$$

2. In case when $G = SO(2k)$

$$\begin{aligned} q\phi_1 &= \pm\pi \bmod 2\pi, \\ &\dots \\ q\phi_d &= \pm\pi \bmod 2\pi. \end{aligned}$$

This observation enables to notice that the number of lattice points corresponding to elements of $Z(G)$ is in fact equal to $\frac{1}{|Z(G)|}$ of the number of all lattice points. As an example we consider the group $SU(3)$, for which $Z(SU(3)) = \{I, e^{2i\pi/3}I, e^{4i\pi/3}I\}$. The corresponding lattice is depicted in Figure 4.5.

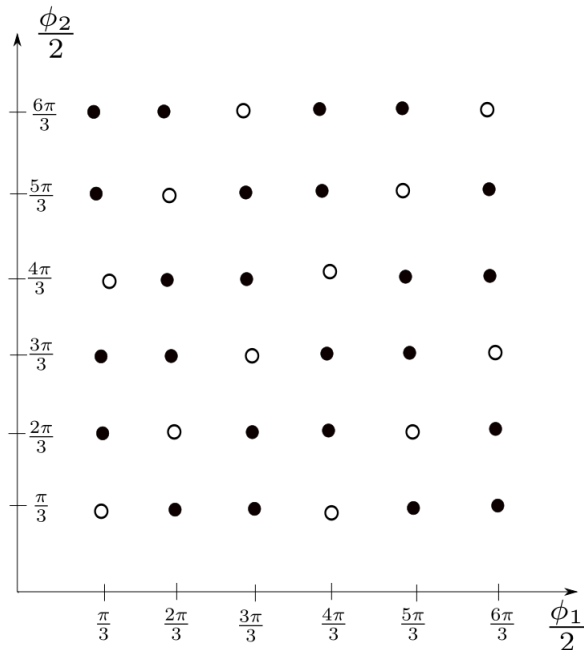


Figure 4.5: Lattice of points for the group $SU(3)$. The axes correspond to independent spectral angles $\frac{\phi_1}{2}, \frac{\phi_2}{2}$ of a matrix U . Dots represent angles $\frac{k\pi}{3}$, $k \in \mathbb{Z}_+$. The values of $\frac{\phi_1}{2}, \frac{\phi_2}{2}$ such, that $U \in Z(SU(3))$ are denoted by circles. It is easy to notice that the number of circles is equal to $\frac{1}{3}$ of the number of all dots.

In order to make these considerations more formal we will modify Theorem 2.8. To this end for any $x \in \mathbb{R}$ and $d \in \mathbb{Z}_+$ we define $\{x\}_k$ to be the difference between x and the largest $p + \frac{k}{d}$ that is smaller or equal to x , where $p \in \mathbb{Z}$, $k \in \{0, 1, \dots, d-1\}$. Clearly $\{x\}_k \in [0, 1)$. For $x = (x_1, \dots, x_n) \in \mathbb{R}^n$ we define $\{x\}_k = (\{x_1\}_k, \dots, \{x_n\}_k)$. Let $\mathcal{L}_{n,d}$ be the lattice in \mathbb{R}^n given by points

$$(q_1, \dots, q_n), (q_1 + \frac{1}{d}, \dots, q_n + \frac{1}{d}), \dots, (q_1 + \frac{d-1}{d}, \dots, q_n + \frac{d-1}{d}),$$

where $q_1, \dots, q_n \in \mathbb{Z}$. An important property of the lattice $\mathcal{L}_{n,d}$ is that for any $p, q \in \mathcal{L}_{n,d}$ we have $p \pm q \in \mathcal{L}_{n,d}$. As a direct consequence of this property we get the following theorem.

Theorem 4.14. [71] For $\zeta = (\zeta_1, \dots, \zeta_n)$ and positive $\epsilon < \frac{1}{2d}$ there exist: integer $1 \leq l \leq \lceil \frac{1}{d\epsilon^n} \rceil$ and a point $p = (p_1, \dots, p_n) \in \mathcal{L}_{n,d}$ such that $\forall i \in \{1, \dots, n\}$:

$$|q\zeta_i - p_i| < \epsilon. \quad (4.26)$$

Proof. For a given point $\zeta = (\zeta_1, \dots, \zeta_n) \in \mathbb{R}^n$ consider $dQ^n + 1$ points:

$$\{q\zeta\}_0, \{q\zeta\}_1, \dots, \{q\zeta\}_{d-1}, \quad q \in \{0, \dots, Q^n\} \quad (4.27)$$

Next, take an n -dimensional cube $[0, 1)^n$ and divide it into dQ^n boxes by drawing planes parallel to its faces at distances $\frac{1}{dQ}$. By Dirichlet's box principle, at least two points from (4.27) fall to the same box. Let us denote points by $\{p_1\zeta\}_i$ and $\{p_2\zeta\}_j$, where $i, j \in \{1, \dots, d-1\}$ and $p_1 < p_2$. Note that p_1 cannot be equal to p_2 as in this case $\epsilon > \frac{1}{2d}$.

As the lattice $\mathcal{L}_{n,d}$ is invariant with respect to addition and subtraction of its points we have $\max_l |\{(p_2 - p_1)\zeta_l\}_k| < \frac{1}{dQ}$, where $k = j - i$ if $i < j$ or $k = d + j - i$ when $i > j$. The result follows. \square

Fact 4.5. [71] The values of $N_{SO(2k+1)}$ and $N_{SO(2k)}$ are bounded from the above by:

$$N_{SO(2k+1)} < \left\lceil \left(\frac{\pi}{\arcsin \frac{1}{4\sqrt{k}}} \right)^k \right\rceil, \quad (4.28)$$

$$N_{SO(2k)} < \left\lceil \frac{1}{2} \left(\frac{\pi}{\arcsin \frac{1}{4\sqrt{k}}} \right)^k \right\rceil. \quad (4.29)$$

Proof. Recall that the spectral angles of $O \in SO(d)$ are $\{\phi_1, -\phi_1, \dots, \phi_k, -\phi_k\}$ in case when $d = 2k$ or $\{\phi_1, -\phi_1, \dots, \phi_k, -\phi_k, 0\}$ if $d = 2k+1$. We start our proof from the case of $SO(2k+1)$ as it has a trivial center. Assume that $\phi_i = a_i\pi$ for all $i \in \{1, \dots, k\}$. The lattice $\pi \cdot \mathcal{L}_{k,1}$ corresponds exactly to points $\{\frac{\phi_1}{2}, \dots, \frac{\phi_k}{2}\}$ at which the ball B_1 (4.15) is centered. Let us next find the smallest hypercube $[-\frac{\beta_k}{2}, \frac{\beta_k}{2}]^{\times k}$ contained in the ball B_1 . To this end one needs to minimize $\sum_i \phi_i^2$ under the condition $\sum_i \sin^2 \phi_i = \frac{1}{16}$. Calculations with the use of the Lagrange multipliers show that the coordinates of the minimizing point are all equal and hence $k \sin^2 \frac{\beta_k}{2} = \arcsin \frac{1}{16}$. That means $\frac{\beta_k}{2} = \arcsin \frac{1}{4\sqrt{k}}$ is the half of the edge length of the largest hypercube contained in B_1 . We next directly apply Theorem 2.8 and get (4.28).

In case of $SO(2k)$ the center of the group consists of $\{I, -I\}$. Therefore we need to define the lattice $\pi \cdot \mathcal{L}_{k,2}$ corresponding to the points $\{\frac{\phi_1}{2}, \dots, \frac{\phi_k}{2}\}$ at which the balls B_1 and B_{-1} defined by (4.15), (4.14). In the next step we use the same construction as for $SO(2k+1)$ for the ball B_1 . By the symmetry of $\pi \cdot \mathcal{L}_{k,2}$ the same arguments are valid for B_{-1} . Looking at the hypercube that is contained in one of the balls given by conditions (4.15) and (4.16) we get the desired result. \square

Fact 4.6. [70, 71] For $d \geq 3$ the value of $N_{SU(d)}$ is bounded from the above by:

$$N_{SU(d)} < \left\lceil \frac{1}{d} \left(\frac{2\pi}{\beta_d} \right)^{d-1} \right\rceil, \quad (4.30)$$

where β_d is such that $(d-1) \sin^2 \frac{\beta_d}{2} + \sin^2 \frac{(d-1)\beta_d}{2} = \frac{1}{8}$.

Proof. For $U \in SU(d)$ let $\{\phi_1, \dots, \phi_d\}$ be the spectral angles of U . Assume that for every $i \in \{1, \dots, d-1\}$ we have $[0, 2\pi) \ni \phi_i = a_i\pi$. As $\sum_i \phi_i = 0 \pmod{2\pi}$ we can always put $\phi_d = -\sum_{i=1}^{d-1} \phi_i$. First, we need to find the edge length of the largest hypercube $[-\frac{\beta_d}{2}, \frac{\beta_d}{2}]^{\times(d-1)}$ contained in the ball B_1 . By symmetry of condition (4.14), this length will be the same for other balls. We need to minimize $\sum_i \phi_i^2$ under the condition $\sum_{i=1}^{d-1} \sin^2 \phi_i + \sin^2(\sum_{i=1}^{d-1} \phi_i) = \frac{1}{8}$. Calculations with the use of the Lagrange multipliers show that the coordinates of the minimizing point are all equal and hence β_d satisfies:

$$(d-1) \sin^2 \frac{\beta_d}{2} + \sin^2 \frac{(d-1)\beta_d}{2} = \frac{1}{8}. \quad (4.31)$$

In order to apply Theorem 4.14 we need to check if $\frac{\beta_d}{2\pi} < \frac{1}{2d}$. By equation (4.31) β_d is clearly close to zero and therefore we can assume that $\sin \frac{\beta_d}{2}$ approximately equals to $\frac{\beta_d}{2}$. Then it can be transformed to $\frac{\beta_d}{2\pi} = \frac{1}{2\pi\sqrt{2d(d-1)}}$ which is clearly smaller than $\frac{1}{2d}$. Thus we can apply Theorem 4.14 to the lattice $\mathcal{L}_{d-1,d}$ and the point $a = (a_1, \dots, a_{d-1})$ with $\epsilon = \frac{\beta_d}{2\pi} < \frac{1}{2d}$. As a result we obtain point $p \in \mathcal{L}_{d-1,d}$ such that:

$$|na_i - p_i| < \frac{\beta_d}{2\pi}, \quad (4.32)$$

where

$$n < \left\lceil \frac{1}{d} \left(\frac{2\pi}{\beta_d} \right)^{d-1} \right\rceil.$$

The result follows. \square

Finally we compared theoretical results with numerics. Our aim was to approximate errors of (4.28), (4.29), (4.30) for the groups $SO(4)$, $SO(5)$ and $SU(3)$, respectively. The results are presented in Table 4.1. Differences between the bounds and values calculated numerically

G	Numerical N_G	Upper bound for N_G
$SU(2)$	6	6
$SU(3)$	49	154
$SO(3)$	12	12
$SO(4)$	86	151
$SO(5)$	172	312

Table 4.1: Comparing the values of N_G derived from numerical calculations with the upper bounds (4.6,4.5) for low dimensional groups.

reflect the fact, that the considered hypercubes are rather brutal approximations of the balls B_α (see Figure 4.6). However, we stress that the choice of hypercubes we made is the most optimal from the perspective of Dirichlet's theorem. Let us also note that the upper bound for N_G seems to be more accurate for $SO(4)$ than for $SU(3)$. We believe this stems from the fact that the 'square-ball' area ratio is smaller for $SU(3)$ than for $SO(4)$ (see Figure 4.6). The way how these ratios should be incorporated into formulas for the upper bound on N_G is left as an open problem. We suppose this should be done by introducing some additional factor that depends on the square-ball ratio.

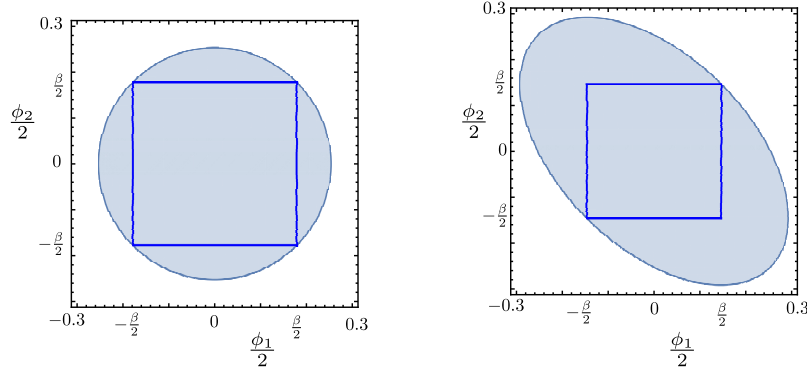


Figure 4.6: The smallest hypercubes contained in the balls B_1 for $SO(4)$ and $SU(3)$, respectively.

4.3. The algorithm for checking universality

In this section we present the algorithm for checking universality of an arbitrary set of one-qudit gates $\mathcal{S} = \{g_1, \dots, g_n\} \subset G$ in a finite number of steps. The algorithm is the main result of this thesis and, additionally, it has been implemented in Octave (see Appendix 6.3) for a special case when $\mathcal{S} = \{U(\phi_1, \vec{k}_1), U(\phi_2, \vec{k}_2)\} \subset SU(2)$.

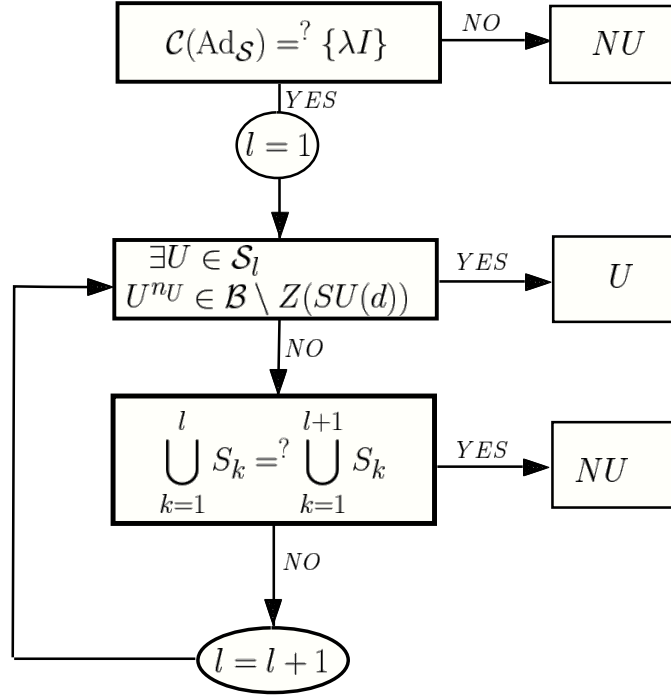
The algorithm consists of the following steps:

- Step 1** Check if $\mathcal{C}(\text{Ad}_{\mathcal{S}}) = \{\lambda I : \lambda \in \mathbb{R}\}$. This can be done by checking the dimension of the kernel of the matrix $L_{\mathcal{S}}$ (4.5) constructed from the entries of matrices $\{\text{Ad}_{g_1}, \dots, \text{Ad}_{g_n}\}$ and thus is a linear algebra problem. If the answer is NO the set \mathcal{S} is not universal. If YES, set $l = 1$ and go to Step 2.
- Step 2** Check if there is a matrix $g \in \mathcal{S}$ for which g^{q_g} belongs to $\mathcal{B} \setminus Z(G)$, where $1 \leq q_g \leq N_G$. This can be done using formula (2.55). If the answer is YES, \mathcal{S} is universal. If the answer is NO, set $l = l + 1$. Notice, that we use in fact the upper bound for N_G that is strictly larger than the exact value, but this not play any role for the result.
- Step 3** Define the new set \mathcal{S} by adding to \mathcal{S} words of length l , i.e. products of elements from \mathcal{S} of length l . If the new \mathcal{S} is equal to the old one, the group $\langle \mathcal{S} \rangle$ is finite³. Otherwise go to Step 2.

The termination step of the algorithm gives us information about the group generated by \mathcal{S} . In case when \mathcal{S} is finite, the algorithm terminates in Step 3 for some $l < \infty$. Otherwise it terminates in Step 2 when \mathcal{S} is universal, or in Step 1.

Let us show that our algorithm always terminates after a finite number of steps and there is no possibility to fall into an infinite loop. To this end notice, that such a situation might happen if and only if $\langle \mathcal{S} \rangle$ would be an infinite group of exceptional matrices. This means that all elements of $\langle \mathcal{S} \rangle$ would have a finite order. However, such a situation is impossible by the virtue of Theorem 2.5 (solution of Burnside problem). The same conclusion comes from Lemma 4.11. Next, assume that \mathcal{S} generates a finite group. As our procedure allows us to create *all possible* products of elements of \mathcal{S} , then by definition of a finite group there must be some $l \in \mathbb{Z}_+$ such, that $\langle \mathcal{S} \rangle = \langle \mathcal{S} \rangle_l$. Summing up we get:

³If \mathcal{S} generate a finite group, then $\langle \mathcal{S} \rangle = \langle \mathcal{S} \rangle$.



Corollary 4.15. *The algorithm terminates after a finite number of steps.*

In what follows we will find the upper and lower bounds for the length l for which our algorithm returns the result. Obviously we omit the case when the necessary criterion is not satisfied. Otherwise \mathcal{S} either generates a finite group or is a universal set. In the first case we get immediately that the upper bound for l is the order of $\langle \mathcal{S} \rangle$. In case, when \mathcal{S} is universal l depends on the spectral gap of the averaging operator $T_{\mathcal{S}}$ (see Section 2.5). We will describe this relation in details in the next section.

4.3.1. Upper bound for l and the spectral gap

In this section we will discuss the upper bound for l in case when \mathcal{S} is a set of one-qudit gates. Next, we will compute l for a set of one-qubit gates for a given spectral gap λ . In Section 4.4 we will compare this result with the numerics.

Fact 4.7. [71] *Assume $\langle \mathcal{S} \rangle$ is dense in $SU(d)$. The length of a word that gives termination of the universality algorithm is at most the length l such that words of length $k \leq l$ form an ϵ -net that covers $SU(d)$, where $\epsilon = \frac{1}{2\sqrt{2}+\delta}$ and $\delta > 0$ is arbitrary small.*

Proof. Assume that words of the length $k \leq l$ built from elements \mathcal{S} form an ϵ -net for $SU(d)$, where $\epsilon = \frac{1}{2\sqrt{2}+\delta}$ and $\delta > 0$ is arbitrary small. Let U be an element of $SU(d)$ whose distance from the identity is exactly $\frac{1}{2\sqrt{2}}$ (see Figure 4.7). Then by Definition 1.3 there must be at least one word $w \in \langle \mathcal{S} \rangle$ of length $k \leq l$ contained in the ball C of radius $\epsilon = \frac{1}{2\sqrt{2}+\delta}$ centered at U . But this ball is contained in $B_1 \setminus I$. Hence w gives termination of the universality algorithm in Step 2. The result follows. \square

Intuitively speaking, the conditions from Fact 4.7 provide that at least one element from $\langle \mathcal{S} \rangle_l$ belongs to \mathcal{B} (similar results are contained in [32]). However, Fact 4.7 does not give a formula for l providing that the desired $\frac{1}{2\sqrt{2}+\delta}$ -net that covers $SU(d)$ is formed. An exact formula for such l was given by Harrow et. al. in [39] in a special case, when \mathcal{S} was a *symmetric* subset of $SU(d)$, i.e. $\mathcal{S} = \{U_1, \dots, U_n, U_1^{-1}, \dots, U_n^{-1}\} \subset SU(d)$. It is worth mentioning that our formulas differs from [39] by a constant factor as we use a different norm.

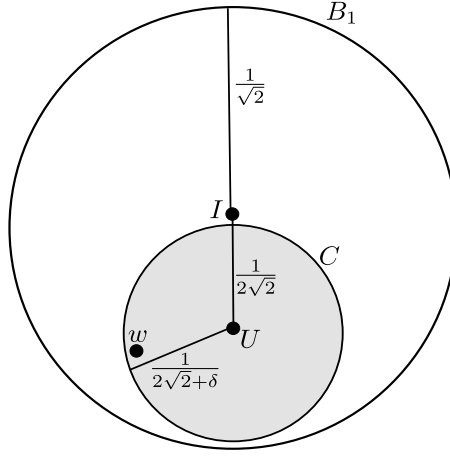


Figure 4.7: The proof of Fact 4.7.

Fact 4.8. [39] Let \mathcal{S} be a universal, symmetric set of gates and assume that $T_{\mathcal{S}}$ has a spectral gap. Let $\lambda_1 = \|T_{\mathcal{S}}|_{L_0^2(SU(d))}\|_{\text{op}}$. For every $U \in SU(d)$, $\epsilon > 0$ and

$$l > A \log \left(\frac{1}{\epsilon} \right) + B$$

there is $U_l \in \langle \mathcal{S} \rangle_l$ such that $\|U - U_l\| < \epsilon$, where

$$A = \frac{d^2 - 1}{\log(1/\lambda_1)}, \quad B = \frac{\log(2^{d^2-1}/a_1) + \frac{1}{2}(d^2 - 1) \log(d^2 - 1)}{\log(1/\lambda_1)},$$

and a_1 is such that for any ball of radius ϵ in $SU(d)$ its volume (with respect to normalized Haar measure) V_{B_ϵ} , satisfies

$$V(B_\epsilon) \geq a_1 \epsilon^{d^2-1}.$$

Notice that the upper bound provided by (4.8) can be very large in case when the spectral gap is very small, e.g. when all elements of \mathcal{S} are very close to some matrix $U \in SU(d)$. But in that case they can be simultaneously introduced to a ball B_α and our algorithm requires actually $l = 1$ to decide their universality. Thus the bound given in 4.8 is useful for the purpose of our algorithm only if λ_1 is well separated from the group neutral element.

In order to find the lower bound for l assume that $\mathcal{S} = \{U_1, \dots, U_n, U_1^{-1}, \dots, U_n^{-1}\}$. Let us denote by $N(d, \epsilon) = \lceil \frac{1}{V(B_\epsilon)} \rceil$ the number of the balls of radius ϵ that fill $SU(d)$. The lower bound for l corresponds to the case when each and every ball B_ϵ contains exactly one element from $\langle \mathcal{S} \rangle_l$, i.e. when elements of $\langle \mathcal{S} \rangle_l$ are uniformly distributed in $SU(d)$. Notice, that a number of words of length l is equal to $|\mathcal{S}_l| = 2n(2n-1)^{l-1} < (2n)^l$. Therefore we get:

$$|\langle \mathcal{S} \rangle_l| < \sum_{i=0}^l (2n)^i = \frac{2^{l+1}n^{l+1} - 1}{2n - 1}. \quad (4.33)$$

In a general case lower bound for l can be found from the condition $|\langle \mathcal{S} \rangle_l| = N(d, \epsilon)$.

Example 4.16. In order to give an idea about possible values for the bound stemming from Fact 4.8, we will find the upper and lower bounds for $V(B_\epsilon)$ in $SU(2)$. First, it is known that for every $\epsilon > 0$ there exist constants k_1 and k_2 such, that $V(B_\epsilon)$ in $SU(2)$ is bounded by:

$$k_1 \epsilon^3 \leq V(B_\epsilon) \leq k_2 \epsilon^3, \quad (4.34)$$

where k_1, k_2 are real positive constants. We are interested in the upper and lower bound for $V(B_\epsilon)$ for $\epsilon \in [0, \frac{1}{2\sqrt{2}}]$.

The upper bound for $V(B_\epsilon)$ can be found directly by integrating an appropriate function on the group. Let F be a function defined on $SU(2)$ and assume that elements of $SU(2)$ are parametrized by the *Euler angles* $\phi, \psi \in [0, \pi)$, $\psi' \in [0, 2\pi)$ where ϕ is a spectral angle:

$$x = \begin{pmatrix} \cos \theta + i \cos \phi \sin \theta & \sin \phi \sin \theta (\cos \phi' + i \sin \phi') \\ \sin \phi \sin \theta (-\cos \phi' + i \sin \phi') & \cos \theta - i \cos \phi \sin \theta \end{pmatrix}. \quad (4.35)$$

In this parameterization the normalized Haar measure on $SU(2)$, $d\mu$, depends on the Euler angles as follows [80]:

$$\int_G F(\theta, \phi, \psi) d\mu = \frac{1}{2\pi^3} \int_0^\pi \int_0^\pi \int_0^{2\pi} F(\theta, \phi, \psi) \sin^2 \phi \sin \phi d\phi d\psi d\phi'. \quad (4.36)$$

In what follows we assume that F is a *central function* satisfying $F(ghg^{-1}) = F(h)$ for all $g, h \in SU(2)$. In this case $F(\theta, \phi, \psi) = F(\phi)$ and the integral (4.36) simplifies to

$$\int_G F(\theta, \phi, \psi) d\mu = \frac{2}{\pi} \int_0^\pi F(\phi) \sin^2 \phi d\phi. \quad (4.37)$$

For our needs we set $F(\phi)$ in the form

$$F(\phi) = \begin{cases} 1 & \text{if } |\sin \frac{\phi}{2}| \leq \frac{\epsilon}{2\sqrt{2}} \\ 0 & \text{otherwise} \end{cases}.$$

Direct calculations using (4.37) provides

$$V(B_\epsilon) = \frac{2}{\pi} \int_0^{2 \arcsin \frac{\epsilon}{2\sqrt{2}}} \sin^2 \phi d\phi = \frac{1}{\pi} \int_0^{2 \arcsin \frac{\epsilon}{2\sqrt{2}}} (1 - \cos \phi) d\phi = \quad (4.38)$$

$$= \frac{1}{\pi} \left(2 \arcsin \frac{\epsilon}{2\sqrt{2}} - \frac{1}{2} \sin 4 \arcsin \frac{\epsilon}{2\sqrt{2}} \right) \quad (4.39)$$

In the next step we apply Taylor expansion of (4.39) around $\epsilon = 0$ up to third order. It is worth emphasizing here that $\frac{1}{2} \sin 4 \arcsin \frac{\epsilon}{2\sqrt{2}}$ can be expanded in three different ways:

1. Expanding \sin up to first order and \arcsin up to third order

$$\frac{1}{2} \sin 4 \arcsin \frac{\epsilon}{2\sqrt{2}} \simeq \frac{1}{2} \sin \left(\frac{2\epsilon}{\sqrt{2}} + \frac{1}{6} \frac{\epsilon^3}{8\sqrt{2}} \right) \simeq \frac{\epsilon}{\sqrt{2}} + \frac{1}{6} \frac{\epsilon^3}{8\sqrt{2}}. \quad (4.40)$$

2. Expanding \sin up to third order and \arcsin up to first order

$$\frac{1}{2} \sin 4 \arcsin \frac{\epsilon}{2\sqrt{2}} \simeq \frac{1}{2} \sin \frac{2\epsilon}{\sqrt{2}} \simeq \frac{\epsilon}{\sqrt{2}} - \frac{\epsilon^3}{3\sqrt{2}}. \quad (4.41)$$

3. Expanding \sin and \arcsin up to third order

$$\frac{1}{2} \sin 4 \arcsin \frac{\epsilon}{2\sqrt{2}} \simeq \frac{1}{2} \sin \left(\frac{2\epsilon}{\sqrt{2}} + \frac{1}{6} \frac{\epsilon^3}{\sqrt{2}} \right) \simeq \frac{\epsilon}{\sqrt{2}} + \frac{1}{6} \frac{\epsilon^3}{8\sqrt{2}} - \frac{\epsilon^3}{3\sqrt{2}}. \quad (4.42)$$

Expansion of the second term of (4.39) is unique and equal to

$$2 \arcsin \frac{\epsilon}{2\sqrt{2}} \simeq \frac{\epsilon}{\sqrt{2}} + \frac{1}{3} \left(\frac{\epsilon}{2\sqrt{2}} \right)^3 = \frac{\epsilon}{\sqrt{2}} + \frac{1}{6 \cdot 8} \frac{\epsilon^3}{\sqrt{2}}. \quad (4.43)$$

Finally we subtract the approximated expressions as in (4.39). One can see immediately that the terms linear in $\frac{\epsilon}{2\sqrt{2}}$ always cancel out. As for the higher order terms

1. In case 1. the expression $\frac{1}{\pi} \left(2 \arcsin \frac{\epsilon}{2\sqrt{2}} - \frac{1}{2} \sin 4 \arcsin \frac{\epsilon}{2\sqrt{2}} \right)$ reduces to zero.
2. Numerical computations (see Figure 4.8) presents differences between exact $V(B_\epsilon)$ and the approximation using formulas (4.42) and (4.42), respectively.

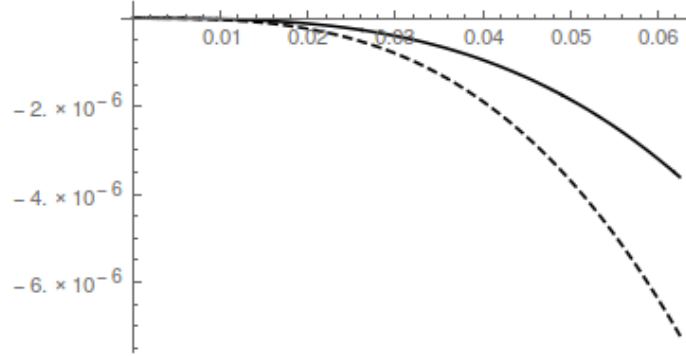


Figure 4.8: Accuracy of approximation of $V(B_\epsilon)$ with the Taylor expansion up to order three. The horizontal axis represents ϵ and the vertical axis represents the numerical accuracy. The thick and dashed lines denote functions $V(B_\epsilon) - \frac{\epsilon}{\sqrt{2}\pi} - \frac{\epsilon^3}{48\pi\sqrt{2}} - f(\epsilon^3)$, where $f(\epsilon^3)$ is given by (4.41) and (4.42), respectively.

As one can see in Figure 4.8 the exact values of $V(B_\epsilon)$ are smaller than the approximated values in any case. This means the approximation gives us an upper bound for $V(B_\epsilon)$. According to Figure 4.8 the best approximation is given by

$$\frac{1}{\pi} \left(2 \arcsin \frac{\epsilon}{2\sqrt{2}} - \frac{1}{2} \sin 4 \arcsin \frac{\epsilon}{2\sqrt{2}} \right) \leq \frac{1}{\pi} \left(\frac{\epsilon^3}{48\sqrt{2}} + \frac{\epsilon^3}{3\sqrt{2}} \right) = \frac{17}{48\sqrt{2}\pi} \epsilon^3,$$

which gives us $k_2 = \frac{17}{48\sqrt{2}\pi}$,

It is worth stressing that this approach does not allow us to find the lower bound for $V(B_\epsilon)$. Instead we can consider the equation $V(B_\epsilon) = k_1 \epsilon^3$ for $\epsilon = \frac{1}{\sqrt{2}}$:

$$\frac{1}{\pi} \left(2 \arcsin \frac{1}{4} - \frac{1}{2} \sin 4 \arcsin \frac{1}{4} \right) = k_1 \left(\frac{1}{\sqrt{2}} \right)^3 \quad (4.44)$$

and compute k_1 from (4.44) obtaining $k_1 = 0.0747$. The function $k_1 \epsilon^3$ is smaller than $V(B_\epsilon)$ for $\epsilon \in [0, \frac{1}{\sqrt{2}}]$ as we show in Figure 4.9. Finally we get the following bounds for $V(B_\epsilon)$

$$0.0736\epsilon^3 \leq V(B_\epsilon) \leq \frac{17}{48\sqrt{2}\pi} \epsilon^3 \simeq 0.07503\epsilon^3. \quad (4.45)$$

Let $\mathcal{S} = \{U(\phi_1, \vec{k}_1), U(\phi_2, \vec{k}_2), U(-\phi_1, \vec{k}_1), U(-\phi_2, \vec{k}_2)\} \subset SU(2)$ be a universal set such, that $\langle \mathcal{S} \rangle_l$ is given by (4.33). The optimal value of l that is necessary to terminate the algorithm is the solution of

$$4^{l+1} = \frac{3}{0.0736\epsilon^3}, \quad \epsilon = \frac{1}{2\sqrt{2}}$$

and is equal to $l = \lceil 3.92456 \rceil = 4$. As we will show in Section 4.4 this result is in perfect agreement with numerical calculations.

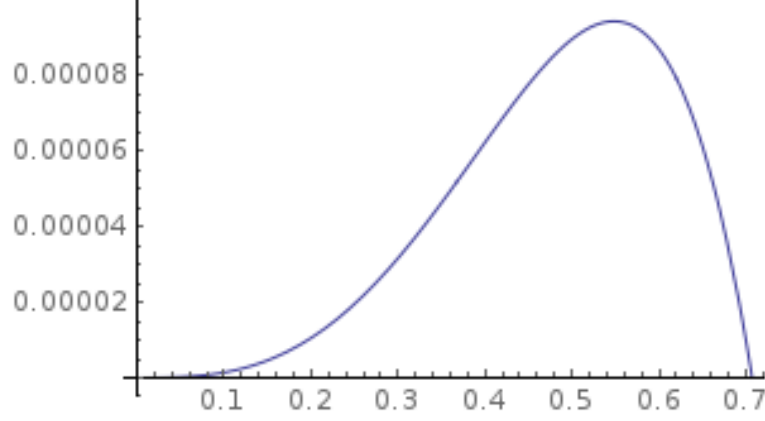


Figure 4.9: Function $F(\epsilon) = V(B_\epsilon) - k_1 \epsilon^3$ for $\epsilon \in [0, \frac{1}{\sqrt{2}}]$. The horizontal axis represents ϵ and the vertical axis represents $F(\epsilon)$. As $F(\epsilon)$ is larger than zero for $\epsilon \in [0, \frac{1}{\sqrt{2}}]$ we conclude that $k_1 \epsilon^3$ is smaller than $V(B_\epsilon)$.

4.4. Universality criteria for one-qubit gates

In this section we restrict our considerations to a set of two qubit gates, denoted by

$$\mathcal{S} = \{U(\phi_1, \vec{k}_1), U(\phi_2, \vec{k}_2)\} \subset SU(2). \quad (4.46)$$

We are interested, how the necessary universality conditions simplify in such a case. We will also find the criteria for \mathcal{S} to be non-universal and show in Section 4.5 how to deal with this problem.

4.4.0.1. Necessary universality criterion

We start from reformulating the necessary universality criterion (see Theorem 4.4 and 4.5) for \mathcal{S} given by (4.46). Next we will list all possible groups that can be generated by \mathcal{S} .

Fact 4.9. *Let $u(\vec{k}_1), u(\vec{k}_2) \in \mathfrak{su}(2)$ and $U(\phi_1, \vec{k}_1) = \exp(\phi_1 u(\vec{k}_1))$, $U(\phi_2, \vec{k}_2) = \exp(\phi_2 u(\vec{k}_2))$. Assume that $[u(\vec{k}_1), u(\vec{k}_2)] \neq 0$. The space $\mathcal{C}(\text{Ad}_{U(\phi_1, \vec{k}_1)}, \text{Ad}_{U(\phi_2, \vec{k}_2)})$ is larger than $\{\lambda I : \lambda \in \mathbb{R}\}$ if and only if:*

1. $\phi_1, \phi_2 \in \{\frac{\pi}{2}, \frac{3\pi}{2}\}$,
2. one of $\phi_i \in \{\frac{\pi}{2}, \frac{3\pi}{2}\}$ and $\vec{k}_1 \perp \vec{k}_2$.

Proof. By the virtue of Fact 4.2 the space $\mathcal{C}(\text{Ad}_{U(\phi_1, \vec{k}_1)}, \text{Ad}_{U(\phi_2, \vec{k}_2)})$ can be larger than $\{\lambda I : \lambda \in \mathbb{R}\}$ if at least one of the spectral angles of $\text{Ad}_{U(\phi_1, \vec{k}_1)}$, $\text{Ad}_{U(\phi_2, \vec{k}_2)}$ is $k\pi$. Therefore we have to consider situation when either two angles ϕ_1 and ϕ_2 are equal to $\frac{k\pi}{2}$ or exactly one of ϕ_i 's is $\frac{k\pi}{2}$, $k \in \{1, 3\}$.

For the case 1. generators are of the form $U\left(\frac{k\pi}{2}, \vec{k}_1\right)$ and $U\left(\frac{k\pi}{2}, \vec{k}_2\right)$, where \vec{k}_1, \vec{k}_2 are arbitrary axes. By the formula (2.72), $\text{Ad}_{U(\frac{k\pi}{2}, \vec{k}_1)} = O(k_1\pi, \vec{k}_1)$ and $\text{Ad}_{U(\frac{k\pi}{2}, \vec{k}_2)} = O(k_2\pi, \vec{k}_2)$ are rotation matrices by angles $k_1\pi, k_2\pi$. Direct calculations shows that a rotation $O(\phi_3, \vec{k}_3)$ by an

arbitrary angle ϕ_3 and about the axis $\vec{k}_3 = \vec{k}_1 \times \vec{k}_2$ commutes with the rotations $O(k\pi, \vec{k}_1)$ and $O(k\pi, \vec{k}_2)$ and is obviously different than λI .

Let us consider the case 2. when exactly one of ϕ_i 's is $\frac{k\pi}{2}$. We are given the generators $U\left(\frac{k\pi}{2}, \vec{k}_1\right)$ and $U\left(\phi_2, \vec{k}_2\right)$. First, note that the rotation $O(\pi, \vec{k})$, where $\vec{k} \parallel \vec{k}_2$, commutes with both $\text{Ad}_{U(\frac{k\pi}{2}, \vec{k}_1)} = O(k\pi, \vec{k}_1)$ and $\text{Ad}_{U(\phi_2, \vec{k}_2)} = O(2\phi_2, \vec{k}_2)$ provided $\vec{k}_1 \perp \vec{k}_2$. Therefore in this case $\mathcal{C}(\text{Ad}_{U(\frac{k\pi}{2}, \vec{k}_1)}, \text{Ad}_{U(\phi_2, \vec{k}_2)})$ is larger than $\{\lambda I : \lambda \in \mathbb{R}\}$. Thus we only need to show that if $\vec{k}_1 \not\perp \vec{k}_2$ and exactly one of ϕ_i 's is an odd multiple of π , then the space $\mathcal{C}(\text{Ad}_{U(\frac{k\pi}{2}, \vec{k}_1)}, \text{Ad}_{U(\phi_2, \vec{k}_2)})$ is equal to $\{\lambda I : \lambda \in \mathbb{R}\}$. To this end we will explain that relaxing orthogonality to an arbitrary endomorphism gives only λI .

Simple analysis shows that endomorphisms commuting with $\text{Ad}_{U(\phi_2, \vec{k}_2)}$ are of the form

$$A = \alpha_2 O(\theta_2, \vec{k}_2) + \beta_2 |\vec{k}_2\rangle\langle\vec{k}_2|, \quad \alpha_2, \beta_2 \in \mathbb{R}, \quad \theta_2 \in [0, 2\pi)$$

On the other hand we know that matrices commuting with $\text{Ad}_{U(\frac{k\pi}{2}, \vec{k}_1)}$ are of the form

$$B = E(\vec{k}_1^\perp) + \beta_1 |\vec{k}_1\rangle\langle\vec{k}_1|,$$

where $E(\vec{k}_1^\perp)$ is an arbitrary matrix acting on the 2-dimensional space perpendicular to \vec{k}_1 such that $E(\vec{k}_1^\perp)\vec{k}_1 = 0$ and $\beta_1 \in \mathbb{R}$. Let $\{\vec{k}_1, \vec{k}_2, \vec{k}_{12}\}$, where $\vec{k}_{12} = \vec{k}_1 \times \vec{k}_2$ be a basis of \mathbb{R}^3 . As A and B must agree on the basis vectors we obtain the following equations:

$$\beta_1 \vec{k}_1 = \alpha_2 O(\theta_2, \vec{k}_2) \vec{k}_1 + \beta_2 \langle \vec{k}_1 | \vec{k}_2 \rangle \vec{k}_2, \quad (4.47)$$

$$(\alpha_2 + \beta_2) \vec{k}_2 = E(\vec{k}_1^\perp) \vec{k}_2 + \beta_1 \langle \vec{k}_1 | \vec{k}_2 \rangle \vec{k}_1, \quad (4.48)$$

$$E(\vec{k}_1^\perp) \vec{k}_{12} = \alpha_2 O(\theta_2, \vec{k}_2) \vec{k}_{12}. \quad (4.49)$$

The left hand side of (4.49) is a vector perpendicular to \vec{k}_1 and the right hand side of (4.49) is a vector perpendicular to \vec{k}_2 . The only vector satisfying both of these conditions is proportional to \vec{k}_{12} and therefore $\theta_2 = n\pi$. Hence $O(\theta_2, \vec{k}_2) = \pm I$. From Equation (4.47) we get

$$\beta_1 \vec{k}_1 = \pm \alpha_2 \vec{k}_1 + \beta_2 \langle \vec{k}_1 | \vec{k}_2 \rangle \vec{k}_2,$$

which implies $\beta_1 = \pm \alpha_2$ and either $\beta_2 = 0$ or $\vec{k}_1 \perp \vec{k}_2$. In the first case $\beta_2 = 0 \Rightarrow A = \pm \alpha_2 I$ and hence the equality between A and B implies

$$\mathcal{C}(\text{Ad}_{U(\frac{k\pi}{2}, \vec{k}_1)}, \text{Ad}_{U(\phi_2, \vec{k}_2)}) = \{\lambda I : \lambda \in \mathbb{R}\}.$$

Therefore the only solution providing a bigger space $\mathcal{C}(\text{Ad}_{U(\frac{k\pi}{2}, \vec{k}_1)}, \text{Ad}_{U(\phi_2, \vec{k}_2)})$ corresponds to $\vec{k}_1 \perp \vec{k}_2$. \square

In what follows we will study the structure of $\overline{\langle U(\phi_1, \vec{k}_1), U(\phi_2, \vec{k}_2) \rangle}$, where $\vec{k}_1 \perp \vec{k}_2$ and $\phi_2 = \pm \frac{\pi}{2}$. In particular we will show that in this case the group is either finite or infinite *dicyclic group*. To this end we set $b := U(\phi_1, \vec{k}_1)$ and $x := U(\frac{\pi}{2}, \vec{k}_2)$ and assume that b is of finite order. Note that the group generated by b and x has the following presentation:

$$H = \langle b, x \mid x^4 = I, b^n = I, xbx^{-1} = b^{-1} \rangle. \quad (4.50)$$

Important is that $-I \in H$, hence $(-b)^n = -I$ for n odd. Setting $a = -b$ we get

$$H = \langle a, x \mid x^4 = I, a^{2n} = I, xax^{-1} = a^{-1} \rangle, \quad (4.51)$$

which is precisely the definition of the dicyclic group of order $4n$. In case when a is of the infinite order we obtain a group consisting of two connected components after closure. The first one is a one-parameter group $\{U(\phi_1, \vec{k}_1) : t \in \mathbb{R}\}$ generated by $U(\phi_1, \vec{k}_1)$ and the second one is its normalizer $\{U(\frac{\pi}{2}, \vec{k}_2)U(t, \vec{k}_1) : t \in \mathbb{R}\}$. The group is presented schematically in Figure 4.10. The only other case when $\mathcal{C}(\text{Ad}_{U(\phi_1, \vec{k}_1)}, \text{Ad}_{U(\phi_2, \vec{k}_2)}) \neq \{\lambda I\}$ corresponds to the situation

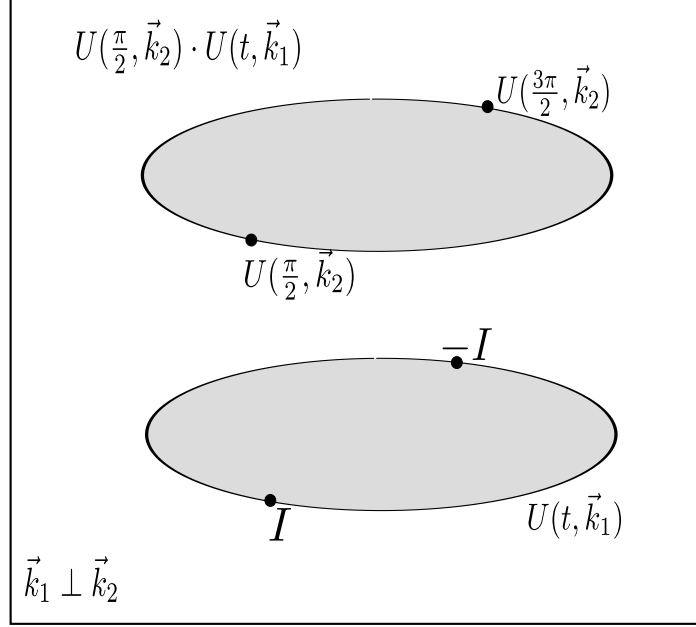


Figure 4.10: An infinite order dicyclic group $\overline{\langle U(\phi_1, \vec{k}_1), U(\frac{\pi}{2}, \vec{k}_2) \rangle}$. The ellipses represent the normalizer $\{U(\frac{\pi}{2}, \vec{k}_2)U(t, \vec{k}_1) : t \in \mathbb{R}\}$ and the one parameter group $\{U(t, \vec{k}_1) : t \in \mathbb{R}\}$, respectively.

when both ϕ_1 and ϕ_2 are odd multiples of $\frac{\pi}{2}$. In this case the group generated by $U(\phi_1, \vec{k}_1)$, $U(\phi_2, \vec{k}_2)$ is the same as the group generated by $U(\gamma, \vec{k}_{12}) = U(\phi_1, \vec{k}_1)U(\phi_2, \vec{k}_2)$ and $U(\phi_2, \vec{k}_2)$. One can easily calculate that $\cos \gamma = \vec{k}_1 \cdot \vec{k}_2$ and $\vec{k}_{12} \perp \vec{k}_2$. Thus the group is once again the dicyclic group of the order $4n$ where n is the order of $U(\gamma, \vec{k}_{12})$.

Lemma 4.17. Assume that $\overline{\langle U(\phi_1, \vec{k}_1), U(\phi_2, \vec{k}_2) \rangle}$ do not commute and $\vec{k}_1 \cdot \vec{k}_2 = 0$ and $\phi_2 \in \{\frac{\pi}{2}, \frac{3\pi}{2}\}$. Then $\langle U(\phi_1, \vec{k}_1), U(\frac{\pi}{2}, \vec{k}_2) \rangle$ is either

1. the dicyclic group of order $4n$

$$n = \max(\text{order}U(\phi_1, \vec{k}_1), \text{order}U(\phi_1 + \pi, \vec{k}_1)), \quad (4.52)$$

when $\text{order}U(\phi_1, \vec{k}_1) < \infty$,

2. the infinite dicyclic group if $\text{order}U(\phi_1, \vec{k}_1) = \infty$.

When $\phi_1, \phi_2 \in \{\frac{\pi}{2}, \frac{3\pi}{2}\}$ the group generated by $U(\phi_1, \vec{k}_1)$ and $U(\phi_2, \vec{k}_2)$ is also the dicyclic group of the order $4n$ where n is the order of $U(\gamma, \vec{k}_{12}) = U(\phi_1, \vec{k}_1)U(\phi_2, \vec{k}_2)$.

Summing up, the group generated by two noncommuting matrices from $SU(2)$ that do not satisfy the necessary criterion for universality is either a finite or an infinite dicyclic group.

4.4.0.2. Sufficient universality criterion

In this section we will continue our study on universality of $\mathcal{S} = \{U(\phi_1, \vec{k}_1), U(\phi_2, \vec{k}_2)\}$, assuming that \mathcal{S} satisfies the necessary universality criterion. In this case one can distinguish two situations:

1. At least one of ϕ_1, ϕ_2 does not belong to $\mathcal{L}_{SU(2)}$.
2. Both ϕ_1 and ϕ_2 belong to $\mathcal{L}_{SU(2)}$.

Note that in the case 1. we get immediately from Theorem 4.13 that \mathcal{S} is universal. Therefore the only problematic situation is when both ϕ_1 and ϕ_2 are exceptional angles. In order to check universality of \mathcal{S} in this case we performed computations for all possible pairs of $\phi_1, \phi_2 \in \mathcal{L}_{SU(2)}$ and arbitrary \vec{k}_1, \vec{k}_2 . Our procedure could be described in the following steps:

Step 1 As $SO(3)$ is the automorphism group of $SU(2)$ we know, that for any $O \in SO(3)$, the group generated by \mathcal{S} is isomorphic with the group generated by $U(\phi_1, O\vec{k}_1)$ and $U(\phi_2, O\vec{k}_2)$. This freedom allows us to choose $O \in SO(3)$ such that $O\vec{k}_1 = [0, 0, 1]$ and $O\vec{k}_2 = [\sin \alpha, 0, \cos \alpha]$, for some $\alpha \in [0, 2\pi)$.

Step 2 We check if our algorithm terminates for $l = 1$, i.e. if $U(\phi_1, O\vec{k}_1)^q \in \mathcal{B}$ or $U(\phi_2, O\vec{k}_2)^q \in \mathcal{B}$, where $1 < q \leq 6$ and \mathcal{B} was defined in Section 4.2.1.

Step 3 Otherwise we compose elements from \mathcal{S} using formula 2.69

$$\cos \alpha = \vec{k}'_1 \cdot \vec{k}'_2 = \frac{\cos \phi_1 \cos \phi_2 - \cos \gamma}{\sin \phi_1 \sin \phi_2}, \quad (4.53)$$

for all $\gamma \in \mathcal{L}_{SU(2)}$ and exclude all the triplets ϕ_1, ϕ_2, γ providing $|\cos \alpha| \geq 1$.

Step 4 For all remaining cases we run our algorithm with matrices \mathcal{S} .

The termination results are as follows:

- The algorithm terminates in Step 2 for $l \leq 4$ and the resulting group is $SU(2)$.
- The algorithm terminates in Step 3 with $5 \leq l \leq 6$ and the resulting group is isomorphic to the binary tetrahedral group.
- The algorithm terminates in Step 3 with $7 \leq l \leq 8$ and the resulting group is isomorphic to the binary octahedral group.
- The algorithm terminates in Step 3 with $8 \leq l \leq 13$ and the resulting group is isomorphic to the binary icosahedral group.

To be more precise, among all 10560 exceptional triplets $\{\phi_1, \phi_2, \gamma\}$ there is 4816 satisfying $|\cos \alpha| < 1$. The number of triplets $\{\phi_1, \phi_2, \gamma\}$ that give termination of the algorithm for the length l and the resulting groups are presented in Table 4.2. A full list of triplets generating finite subgroups of $SU(2)$ is included in Appendix 6.2.

Section 4.4 can be summarized as follows:

Theorem 4.18. *Assume $\mathcal{S} = \{U(\phi_1, \vec{k}_1), U(\phi_2, \vec{k}_2)\} \subset SU(2)$. In order to verify universality of \mathcal{S} it is enough to consider words of the length $l \leq 4$. Moreover, the algorithm terminates for $l \leq 13$. If it terminates in Step 1 the resulting group is either infinite or finite dicyclic group. If it terminates with $1 \leq l \leq 4$ the resulting group is $SU(2)$. For $l \geq 5$ it is binary tetrahedral or binary octahedral or binary icosahedral group.*

l	Step	Number of triplets ϕ_1, ϕ_2, γ	Generated group
—	1	80	dicyclic group
3	2	3232	$SU(2)$
4	2	160	$SU(2)$
5	3	56	$\langle 2, 3, 3 \rangle$
6	3	40	$\langle 2, 3, 3 \rangle$
7	3	144	$\langle 2, 3, 4 \rangle$
8	3	80	$\langle 2, 3, 4 \rangle$
8	3	240	$\langle 2, 3, 5 \rangle$
9	3	352	$\langle 2, 3, 5 \rangle$
10	3	288	$\langle 2, 3, 5 \rangle$
11	3	32	$\langle 2, 3, 5 \rangle$
12	3	80	$\langle 2, 3, 5 \rangle$
13	3	32	$\langle 2, 3, 5 \rangle$

Table 4.2: The number of exceptional triplets $\{\phi_1, \phi_2, \gamma\}$ terminating the universality algorithm for different l 's.

Example 4.19. Let us illustrate methods of Section 4.3 on the set $\mathcal{S}_\phi^{H,T} = \{H, T(\phi)\}$, that was defined first in Chapter 3. In what follows we will recall the matrices H and $T(\phi)$:

$$H = U(\pi/2, \frac{1}{\sqrt{2}}(\vec{k}_y + \vec{k}_z)) = \frac{i}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad T(\phi) = U(\phi, \vec{k}_z) = \begin{pmatrix} e^{-i\phi} & 0 \\ 0 & e^{i\phi} \end{pmatrix}. \quad (4.54)$$

Our goal is to check for which ϕ , $\overline{\langle H, T(\phi) \rangle} = SU(2)$.

Case 1 If $\phi = k\pi$ then $T(\phi) = \pm I$ and the generated group is the finite cyclic group of the order 4 when $\phi = 0$ or the order 8 when $\phi = \pi$.

Case 2 When $\phi = \frac{k\pi}{2}$ and k is odd, by Fact we have that $\mathcal{C}(\text{Ad}_H, \text{Ad}_{T(\phi)})$ is larger than $\{\lambda I : \lambda \in \mathbb{R}\}$ and hence $\overline{\langle H, T(\frac{k\pi}{2}) \rangle} \neq SU(2)$. More precisely, it is the finite dicyclic group of order 16, whose generators are $HT(\frac{k\pi}{2})$ and $T(\frac{k\pi}{2})$. Fixing universality in this case requires, for example, adding a matrix that has a non-exceptional spectrum and whose \vec{k} is neither parallel nor orthogonal to rotation axes of H and $T(\frac{k\pi}{2})$.

Case 3 For $\phi \neq \frac{k\pi}{2}$, again by Fact 4.9, $\mathcal{C}(\text{Ad}_H, \text{Ad}_{T(\phi)}) = \{\lambda I : \lambda \in \mathbb{R}\}$ and we just need to check if $\overline{\langle H, T(\phi) \rangle}$ is infinite. We can distinguish then three possibilities:

1. We first assume that ϕ is not exceptional. Then by Theorem 4.13 $\overline{\langle H, T(\phi) \rangle} = SU(2)$. Our algorithm for deciding universality terminates at step 2 with $l = 1$.
2. We next consider the exceptional angles. For

$$\phi \in \left\{ \frac{k_3\pi}{3}, \frac{k_5\pi}{5}, \frac{k_6\pi}{6} \right\}, \quad \gcd(k_i, i) = 1,$$

we look at the product $U(\gamma, \vec{k}_{HT}) = HT(\phi) = U(\pi/2, \vec{k}_H)U(\phi, \vec{k}_T)$. Using formula (3.9) we calculate $\cos \gamma$, compare it with $\cos \psi$ for all exceptional angles ψ and find out they never agree. Hence γ is not exceptional. Thus by Theorem 4.13 we get $\overline{\langle HT(\phi) \rangle} = SU(2)$. Our algorithm for deciding universality terminates in Step 2 with $l = 2$.

3. We are left with $\phi = \frac{k_4\pi}{4}$ where $\gcd(k_4, 4) = 1$. There are exactly four such angles. Calculations of $U(\gamma, \vec{k}_{HT(\phi)}) = HT(\phi)$ shows that γ is exceptional, i.e. $\gamma = \frac{k_3\pi}{3}$, where $\gcd(k_3, 3) = 1$. Moreover, taking further products results in a finite subgroup consisting of 48 elements (all have exceptional spectra) known as the binary octahedral group. Our algorithm for deciding universality terminates in Step 3 with $l = 8$. Fixing non-universality can be accomplished by, for example, adding one gate $U(\psi, \vec{k}_\psi)$ with a non-exceptional ψ and an arbitrary \vec{k}_ψ .

Notice, that the methods from this section give us much more information about the groups generated by $\mathcal{S}_\phi^{H,T}$ than the approach presented in Chapter 3.

4.5. Universality of 2-mode beamsplitters

In this section we will show, how to deal with non-universal sets of gates from $SU(2)$ or $SO(2)$ by embedding them into gates that act on d -dimensional space, where $d > 2$. More precisely, we consider the Hilbert space $\mathcal{H} = \mathcal{H}_1 \oplus \dots \oplus \mathcal{H}_d$, where $\mathcal{H}_k \simeq \mathbb{C}$, $d > 2$. Next we take a matrix $B \in SU(2)$ or $B \in SO(2)$ (this matrix will be called a 2-mode beamsplitter). In what follows we assume that we can permute *modes* and therefore we have access to matrices B and $B^\sigma = \sigma^t B \sigma$, where σ is the permutation matrix.

In the next step we define matrices B_{ij} or B_{ij}^σ to be the matrices that act on a 2-dimensional subspace $\mathcal{H}_i \oplus \mathcal{H}_j \subset \mathcal{H}$ as B or B^σ , respectively and as the identity on the other components of \mathcal{H} . The indexes i, j can be chosen in $2\binom{d}{2} = d(d-1)$ ways, which gives us the set

$$\mathcal{S}_d = \{B_{ij}, B_{ij}^\sigma : i < j, i, j \in \{1, \dots, d\}\}. \quad (4.55)$$

Let us denote by $\mathcal{X}_d = \{b_{ij}, b_{ij}^\sigma : i < j, i, j \in \{1, \dots, d\}\}$ the set of corresponding Lie algebra elements such, that $B_{ij} = e^{b_{ij}}$, $B_{ij}^\sigma = e^{b_{ij}^\sigma}$ (constructed as in Section 4.1.3). Our goal is to find out when \mathcal{S}_d is universal, i.e. when $\overline{\langle \mathcal{S}_d \rangle} = SO(d)$ or $\overline{\langle \mathcal{S}_d \rangle} = SU(d)$. In particular we focus on showing, for which B the set \mathcal{S}_3 is universal, but \mathcal{S} is not universal. It is known (see [67, 69]) that for such B also any set \mathcal{S}_d with $d > 3$ is universal.

4.5.1. Spaces $\mathcal{C}(\text{Ad}_{\mathcal{S}_3})$ and $\mathcal{C}(\text{ad}_{\mathcal{X}_3})$

In this section we will characterize when $\mathcal{C}(\text{Ad}_{\mathcal{S}_3}) = \{\lambda I\}$ for both orthogonal and unitary beamsplitters. We start our analysis from checking an analogous condition for $\mathcal{C}(\text{ad}_{\mathcal{X}_3})$, which is a simplest problem. Then we will use Facts 4.1 and 4.2 to find $\mathcal{C}(\text{Ad}_{\mathcal{S}_3})$.

4.5.2. The case of the orthogonal group

Let $B \in SO(2)$ be a rotation matrix by an angle $\phi \in (0, 2\pi)$. According to the notation introduced in (4.55) we define

$$\mathcal{S}_3 = \{B_{23}(\pm\phi), B_{13}(\pm\phi), B_{12}(\pm\phi)\}, \quad (4.56)$$

$$\mathcal{X}_3 = \{\pm\phi X_{23}, \pm\phi X_{13}, \pm\phi X_{12}\}. \quad (4.57)$$

It is worth emphasizing that $B_{ij}(\pm\phi)$ correspond to the rotation matrices in three dimensions, i.e. $B_{12}(\phi) = O(\pm\phi, \vec{k}_z)$, $B_{13}(\phi) = O(\pm\phi, \vec{k}_y)$ and $B_{23}(\phi) = O(\pm\phi, \vec{k}_x)$, where $\vec{k}_x = [1, 0, 0]$, $\vec{k}_y = [0, 1, 0]$, $\vec{k}_z = [0, 0, 1]$ and matrices $X_{i,j}$ are defined by (2.52). Note that matrices belonging to \mathcal{X} form a basis of the Lie algebra $\mathfrak{so}(3)$ if and only if $\phi \neq 0$, therefore by Corollary 4.3

$$\mathcal{C}(\text{ad}_{\mathcal{X}_3}) = \{\lambda I\}.$$

Note that the adjoint representation maps $SO(3)$ to $SO(3)$. What is more, the adjoint matrices $\text{Ad}_{O(\pm\phi, \vec{k}_i)}$ are again rotation matrices by angles $\pm\phi$ along axes \vec{k}_i . On the other hand, by Fact 4.2 we know that $\mathcal{C}(\text{Ad}_{\mathcal{S}_3})$ can be different than $\mathcal{C}(\text{ad}_{\mathcal{X}_3})$ only if $\phi = \pm\pi$, which is exactly the case when the adjoint matrices $\text{Ad}_{O(\pm\phi, \vec{k}_i)}$ commute. Summing up we get:

Fact 4.10. [69, 71] *For a 2-mode orthogonal beamsplitter. If $\phi \neq 0$ then $\mathcal{C}(\text{ad}_{\mathcal{X}_3}) = \{\lambda I\}$. On the other hand $\mathcal{C}(\text{Ad}_{\mathcal{S}_3}) = \{\lambda I\}$ if and only if $\phi \notin \{0, \pi\}$.*

4.5.3. The case of the unitary group

Let $B \in SU(2)$, $B = I \cos \phi + \sin \phi (k_x X + k_y Y + k_z Z)$, $\phi \neq 0 \bmod \pi$, $\vec{k} = [k_x, k_y, k_z]$ and $k_x^2 + k_y^2 + k_z^2 = 1$. Permutation of modes for matrices from $SU(2)$ is equivalent to transformation $k_x \mapsto -k_x$, $k_z \mapsto -k_z$ which gives us

$$B^\sigma = I \cos \phi + \sin \phi (-k_x X + k_y Y - k_z Z).$$

According to the notation introduced in (4.55) we define

$$\begin{aligned} \mathcal{X}_3 = \{b_{ij}, b_{ij}^\sigma : 1 \leq i < j \leq 3\} &= \phi \cdot \{k_x X_{ij} + k_y Y_{ij} + k_z Z_{ij}, \\ &\quad -k_x X_{ij} + k_y Y_{ij} - k_z Z_{ij} : 1 \leq i < j \leq 3\}, \end{aligned} \quad (4.58)$$

$$\begin{aligned} \mathcal{S}_3 = \{B_{ij}, B_{ij}^\sigma : 1 \leq i < j \leq 3\} &= \{I_{ij}(\phi) + \sin \phi (k_x X_{ij} + k_y Y_{ij} + k_z Z_{ij}), \\ &\quad I_{ij}(\phi) + \sin \phi (-k_x X_{ij} + k_y Y_{ij} - k_z Z_{ij}) : 1 \leq i < j \leq 3\}, \end{aligned} \quad (4.59)$$

where $I_{ij}(\phi) = \cos \phi (E_{ii} + E_{jj}) + E_{ll}$, $l \in \{1, 2, 3\} \setminus \{i, j\}$ and matrices $\{X_{ij}, Y_{ij}, Z_{ij}\}$ are defined as in (2.52).

In order to find $\mathcal{C}(\text{ad}_{\mathcal{X}_3})$ note that $[b_{ij}, b_{ij}^\sigma] = 4k_y (k_x Z_{ij} - k_z X_{ij})$. We get immediately that $[b_{ij}, b_{ij}^\sigma] \neq 0$ implies that b_{ij} and b_{ij}^σ generate $\mathfrak{su}(2)_{ij}$. Thus we have access to all elements X_{ij} , Y_{ij} and Z_{ij} $1 \leq i < j \leq 3$. Hence \mathcal{X}_3 generates $\mathfrak{su}(3)$, therefore $\mathcal{C}(\text{ad}_{\mathcal{X}_3}) = \{\lambda I\}$.

Let us consider the case $[b_{ij}, b_{ij}^\sigma] = 0$ which happens in the following four situations:

1. $k_y \neq 0$ and $k_x = 0 = k_z$: in this case $b_{ij} = k_y Y_{ij} = b_{ij}^\sigma$, which gives us access to all $\{Y_{ij}\}_{i < j}$, $i, j \in \{1, 2, 3\}$. But by the commutation relations we can derive also $X_{j,k}$'s and $Z_{j,k}$'s, i.e.

$$[Y_{i,j}, Y_{i,k}] = -X_{j,k}, \quad [Y_{i,j}, Y_{j,k}] = -X_{i,k}, \quad [Y_{i,j}, Y_{k,j}] = -X_{i,k}, \quad [X_{i,j}, Y_{i,j}] = 2Z_{i,j}.$$

This means we can generate all basis elements of $\mathfrak{su}(3)$ starting from Y_{ij} 's, thus $\mathcal{C}(\text{ad}_{\mathcal{X}_3}) = \{\lambda I\}$.

2. $k_y = 0$ and $k_x \neq 0$ and $k_z \neq 0$: in this case $b_{ij} = -b_{ij}^\sigma$. Direct calculations show that elements:

$$\begin{aligned} &[b_{12}, [b_{12}, b_{13}]], [b_{12}, [b_{12}, b_{23}]], [b_{13}, [b_{13}, b_{12}]], \\ &[b_{13}, [b_{13}, b_{23}]], [b_{23}, [b_{23}, b_{12}]], [b_{12}, [b_{12}, [b_{13}, b_{23}]]], \\ &[b_{23}, [b_{13}, [b_{23}, b_{12}]]], [b_{13}, [b_{13}, [b_{23}, b_{12}]]], \end{aligned}$$

form a basis of $\mathfrak{su}(3)$. Thus $\mathcal{C}(\text{ad}_{\mathcal{X}_3}) = \{\lambda I\}$.

3. $k_y = 0 = k_z$ and $k_x \neq 0$: in this case the algebra generated by \mathcal{X}_3 is clearly $\mathfrak{so}(3)$, hence $\mathcal{C}(\text{ad}_{\mathcal{X}_3}) \neq \{\lambda I\}$.

4. $k_y = 0 = k_x$ and $k_z \neq 0$: in this case the algebra generated by \mathcal{X}_3 is abelian, hence $\mathcal{C}(\text{ad}_{\mathcal{X}_3}) \neq \{\lambda I\}$.

The above analysis can be summarized as follows:

Fact 4.11. [71] For a 2-mode unitary beamsplitter $B = I \cos \phi + \sin \phi(k_x X + k_y Y + k_z Z)$, where $k_x^2 + k_y^2 + k_z^2 = 1$ we have $\mathcal{C}(\text{ad}_{\mathcal{X}_3}) = \{\lambda I\}$ unless (a) $k_y = 0 = k_z$ and $k_x = 1$, (b) $k_y = 0 = k_x$ and $k_z = 1$.

In the next step we characterize $\mathcal{C}(\text{Ad}_{\mathcal{S}_3})$. One should notice here that the adjoint matrices $\text{Ad}_{B_{ij}}$ and $\text{Ad}_{B_{ij}^\sigma}$ are elements of $SO(\mathfrak{su}(3)) \simeq SO(8)$ and the their rotation angles are $\pm\phi$, 2ϕ and 0 . On the other hand, Fact 4.1 states that $\mathcal{C}(\text{Ad}_{\mathcal{S}_3})$ can be different than $\mathcal{C}(\text{ad}_{\mathcal{X}_3})$ only if the rotation angle is $\pm\pi$, which corresponds to situations when either $\phi = \pm\pi$ or $\phi = \pm\frac{\pi}{2}$. But in the first case $B = -I$, thus obviously $\mathcal{C}(\text{Ad}_{\mathcal{S}_3}) \neq \{\lambda I\}$. The case $\phi = \pm\frac{\pi}{2}$ corresponds to $\mathcal{S}_3 = \mathcal{X}_3$.

Fact 4.12. [71] For a 2-mode unitary beamsplitter $B = I \cos \phi + \sin \phi(k_x X + k_y Y + k_z Z)$ we have $\mathcal{C}(\text{Ad}_{\mathcal{S}_3}) = \{\lambda I\}$ unless (a) $k_y = 0 = k_z$ and $k_x = 1$, (b) $k_y = 0 = k_x$ and $k_z = 1$, (c) $\phi = \pm\frac{\pi}{2}$ and $k_z = 0$.

Proof. Recall that $\mathcal{C}(\text{ad}_{\mathcal{X}_3}) \subseteq \mathcal{C}(\text{Ad}_{\mathcal{S}_3})$. Cases (a) and (b) correspond to situations when $\mathcal{C}(\text{ad}_{\mathcal{X}_3}) \neq \{\lambda I\}$ thus also $\mathcal{C}(\text{Ad}_{\mathcal{S}_3}) \neq \{\lambda I\}$. Case (c) follows from direct calculations for six Ad_g matrices with $\phi = \pm\frac{\pi}{2}$ and $g \in \mathcal{S}_3$ which were done with the help of a symbolic calculation software. In order to verify case (c) we define $\mathfrak{h} = \text{Span}_{\mathbb{R}}\{Z_{12}, Z_{23}\}$, $\dim_{\mathbb{R}} \mathfrak{h} = 2$ and show that for $\phi = \pm\frac{\pi}{2}$ and $k_z = 0$ the space \mathfrak{h} is an invariant subspace for matrices $\text{Ad}_{B_{ij}}$ and $\text{Ad}_{B_{ij}^\sigma}$, i.e. of \mathcal{S}_3 . To this end we calculate

$$\text{Ad}_{B_{12}} Z_{12} = -Z_{12}, \text{Ad}_{B_{13}} Z_{12} = -Z_{23}, \text{Ad}_{B_{23}} Z_{12} = Z_{12} + Z_{23}, \quad (4.60)$$

$$\text{Ad}_{B_{12}} Z_{23} = Z_{23} + Z_{12}, \text{Ad}_{B_{13}} Z_{23} = -Z_{12}, \text{Ad}_{B_{23}} Z_{23} = -Z_{23}. \quad (4.61)$$

and $\text{Ad}_{B_{ij}^\sigma} Z_{kl} = \text{Ad}_{B_{ij}} Z_{kl}$. Therefore the projection operator $P : \mathfrak{su}(3) \rightarrow \mathfrak{h}$ commutes with matrices from \mathcal{S}_3 and thus it belongs to $\mathcal{C}(\text{Ad}_{\mathcal{S}_3})$. \square

As a short exercise we studied the structure of the group $\overline{\langle \mathcal{S}_3 \rangle}$ when $k_z = 0$ and $\phi = \frac{\pi}{2}$. Elements of \mathcal{S}_3 are of the form

$$B_{ij} = e^{i\psi} E_{ij} - e^{-i\psi} E_{ji} + E_{kk}, B_{ij}^\sigma = -e^{-i\psi} E_{ij} + e^{i\psi} E_{ji} + E_{kk}, \quad 1 \leq i < j \leq 3, k \neq i, j, \psi \in [0, 2\pi).$$

Note that if ψ is a rational multiple of π , then $\langle \mathcal{S}_3 \rangle$ is a finite group. Otherwise the group $\overline{\langle \mathcal{S}_3 \rangle}$ is infinite and disconnected. In fact these are groups isomorphic to $\Delta(6n^2)$ and $\Delta(6\infty^2)$ given in [29].

4.5.4. When is \mathcal{S}_3 universal?

Having characterized when the necessary universality criterion is satisfied we want to check when the set $\langle \mathcal{S}_3 \rangle$ is infinite. This way we get the full classification of universal 2-mode beamsplitters.

4.5.4.1. The case of the orthogonal group

Combining Theorem 4.13 with Fact 4.10 for $\phi \notin \mathcal{L}_{SO(3)}$ we obtain immediately that the group generated by \mathcal{S}_3 is exactly $SO(3)$. The only interesting cases are $\phi \in \mathcal{L}_{SO(3)}$. First, note that if $\phi = \frac{(2k+1)\pi}{2}$, $k \in \mathbb{Z}$, then matrices $O(\phi, \vec{k}_x)$, $O(\phi, \vec{k}_y)$ and $O(\phi, \vec{k}_z)$ are permutation matrices

and they form 3-dimensional representation of S_3 . For all remaining $\phi \in \mathcal{L}_{SO(3)}$ we consider the matrix: $O(\gamma, \vec{k}_{xz}) = O(\phi, \vec{k}_x)O(\phi, \vec{k}_z)$. The trace yields the following equation that relating γ and ϕ :

$$\cos \gamma = \frac{\cos^2 \phi + 2 \cos \phi - 1}{2}. \quad (4.62)$$

We calculate $\cos \gamma$ using (4.62) and compare it numerically with the cosines for all angles from $\mathcal{L}_{SO(3)}$. We find out they never agree, therefore $\gamma \notin \mathcal{L}_{SO(3)}$ and we can apply Theorem 4.13 and Fact 4.10 to $U(\gamma, \vec{k}_{xz})$. Summing up:

Theorem 4.20. [69, 71] *Any 2-mode orthogonal beamsplitter with $\phi \notin \{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$ is universal on 3 and hence $n > 3$ modes.*

4.5.4.2. The case of the unitary group

In this paragraph we assume that all the entries of a matrix $B \in SU(2)$ are nonzero and at least one of them belongs to \mathbb{C} , which provides that $\mathcal{C}(\text{Ad}_{\mathcal{S}_3}) = \{\lambda I\}$. For such a case we need to verify if $\langle \mathcal{S}_3 \rangle$ is infinite.

Let $\{e^{i\phi}, e^{-i\phi}\}$ be the spectrum of B . Note that matrices B_{ij} and B_{ij}^σ have the same spectra $\{e^{i\phi}, e^{-i\phi}, 1\}$. By the definition of the open balls B_α , $\alpha^3 = 1$ one can easily see that a matrix from $SU(3)$ with one spectral element equal to one can be introduced (by taking powers) only to the ball B_1 . Moreover, the maximal n that is needed is exactly the same as for $SO(3)$ and the exceptional angles belong to the set $\mathcal{L}_{SO(3)}$. Therefore, by Theorem 4.13, $\phi \notin \mathcal{L}_{SO(3)}$ implies that the group generated by any two elements from \mathcal{S}_3 is infinite, hence \mathcal{S}_3 is universal.

In the following we will show that $\langle \mathcal{S}_3 \rangle$ is infinite in many cases also for $\phi \in \mathcal{L}_{SO(3)}$ (providing ϕ is such that $\mathcal{C}(\text{Ad}_{\mathcal{S}_3}) = \{\lambda I\}$). To this end we use the following procedure:

1. We calculate trace of the product $B_{12}(\phi)B_{23}(\phi)$ and note that it belongs to \mathbb{R} , therefore spectrum of $B_{12}(\phi)B_{23}(\phi)$ is of the form $\{e^{i\gamma}, e^{-i\gamma}, 1\}$, where the relation between ϕ and γ is given by

$$\text{tr} B_{12}(\phi)B_{23}(\phi) = 2 \cos \phi + \cos^2 \phi + k_z^2 \sin^2 \phi = 2 \cos \gamma + 1. \quad (4.63)$$

2. Using (4.63) for each $\gamma \in \mathcal{L}_{SO(3)}$ we compute

$$k_z^2 = \frac{2 \cos \gamma + 1 - 2 \cos \phi - \cos^2 \phi}{\sin^2 \phi}, \quad (4.64)$$

and check whether $0 < k_z^2 < 1$. The pairs (ϕ, γ) that fails this test are excluded from the further considerations. The reason is that that $k_z^2 = 1$ corresponds to diagonal matrices $B_{12}(\phi), B_{23}(\phi)$ and $k_z^2 = 0$ corresponds the situation when $\mathcal{C}(\text{Ad}_{\mathcal{S}_3}) \neq \{\lambda I\}$.

3. For the pairs (ϕ, γ) that give $0 < k_z^2 < 1$ we consider the matrix $U(\gamma') = B_{12}(2\phi)B_{23}(2\phi)$. Its trace is again real and we get

$$\text{tr} B_{12}(2\phi)B_{23}(2\phi) = \frac{1}{2}(2 + 4 \cos(2\phi) + (1 - k_z^2)(\cos(4\phi) - 1)) = 2 \cos \gamma' + 1, \quad (4.65)$$

where k_z^2 is determined by ϕ and γ . Direct computations show that $\gamma' \notin \mathcal{L}_{SO(3)}$ if $\phi \notin \{\pm \frac{\pi}{2}, \pm \frac{2\pi}{3}\}$. In what follows we will treat both of these cases separately.

4. For $\phi = \pm \frac{2\pi}{3}$ and the fixed k_z^2 we consider yet another product of matrices $U(\gamma'') = B_{23}^2(\phi)B_{12}^2(\phi)B_{23}(\phi)B_{12}(\phi)$ with a real trace:

$$\begin{aligned} \text{tr} B_{23}^2(\phi)B_{12}^2(\phi)B_{23}(\phi)B_{12}(\phi) &= \frac{1}{8}(\cos \phi + 3 \cos(2\phi) + 4 \cos(3\phi) + 6 \cos(4\phi) \\ &\quad + 4 \cos(5\phi) + \cos(6\phi) - 2) + 32k_z^4 \sin^4 \phi \cos^2 \phi + 8k_z^2 \sin^2 \phi(-2 \cos \phi + \\ &\quad + 4 \cos(2\phi) + 2 \cos(3\phi) + \cos(4\phi) + 4) = 2 \cos \gamma''. \end{aligned} \quad (4.66)$$

Direct computations show that $\gamma'' \notin \mathcal{L}_{SO(3)}$, thus we are done for $\phi \in \mathcal{L}_{SO(3)} \setminus \{\frac{\pi}{2}, -\frac{\pi}{2}\}$. The same composition for $U_{23}(\frac{\pi}{2}), U_{12}(\frac{\pi}{2})$ may give a matrix of the spectral angle $\gamma = \pm \frac{2\pi}{3}$.

For $\phi = \pm \frac{\pi}{2}$ an additional treatment is needed. It consists of three steps:

1. Assume $B_{ij}(\frac{\pi}{2})$ does not commute with its permutations $B_{ij}^\sigma(\frac{\pi}{2})$ for $1 \leq i < j \leq 3$. In this case we can use $B_{ij}(\gamma) = B_{ij}(\frac{\pi}{2}) B_{ij}^\sigma(\frac{\pi}{2})$, $1 \leq i < j \leq 3$ as the new set of generators. Note that the angle γ depends on the trace of $B_{ij}(\frac{\pi}{2}) B_{ij}^\sigma(\frac{\pi}{2})$ as $\cos \gamma = 1 - 2k_y^2$. Thus $\gamma \neq \pm \frac{\pi}{2}$ if $k_y^2 \neq \frac{1}{2}$ and then we can apply the previous procedure to show that $\langle B_{12}(\gamma), B_{23}(\gamma) \rangle$ is infinite.
2. For $\phi = \pm \frac{\pi}{2}$ and $k_y^2 = \frac{1}{2}$, $k_x^2 + k_z^2 = \frac{1}{2}$ we consider yet another product

$$\text{tr} B_{12}^2\left(\frac{\pi}{2}\right) B_{13}\left(\frac{\pi}{2}\right) B_{23}\left(\frac{\pi}{2}\right) B_{13}^2\left(\frac{\pi}{2}\right) = k_z^2 = 2 \cos \gamma'''$$

We find out that the only $\gamma \in \mathcal{L}_{SO(3)}$ satisfying $2 \cos \gamma = k_z^2 - 1$ for $0 \leq k_z^2 \leq \frac{1}{2}$ are $\gamma = \pm \frac{2\pi}{3}$, but then $k_z^2 = 0$. Therefore by Fact 4.12 the space $\mathcal{C}(\text{Ad}_{\mathcal{S}_3})$ is larger than $\{\lambda I\}$.

3. Finally we assume that matrices $B_{ij}(\frac{\pi}{2})$ commute with their permutations. Recall that it happens if either $k_y = \pm 1$ and $k_x = k_z = 0$ or $k_y = 0$ and $k_x, k_z \neq 0$. The group generated for $k_y = \pm 1$ is of course finite. Therefore we need to consider only the case when $k_y = 0$ and $k_x, k_z \neq 0$. But in this case step 2 of the previous procedure is never satisfied (from Equation (4.64) one can only obtain $k_z^2 = 0$ for $\gamma = \pm \frac{2\pi}{3}$).

The above considerations can be summarized as follows:

Theorem 4.21. [71] *Any 2-mode unitary gate, such that all its entries are nonzero and at least one of them is a complex number is universal on 3 and hence $n > 3$ modes.*

It is worth emphasizing that a non-universal set \mathcal{S} embedded into $SU(3)$ as \mathcal{S}_3 may become universal. It happens when elements of \mathcal{S} anticommute or are generators of a finite subgroup of $SU(2)$. The only exception are generators of $\langle 2, 2, 2 \rangle$.

4.6. Summary and open problems

In this chapter we presented an algorithm for deciding universality of an arbitrary n -element set $\mathcal{S} = \{g_1, \dots, g_n\} \subset SU(d)$ or $\mathcal{S} = \{g_1, \dots, g_n\} \subset SO(d)$ and discussed an upper bound of the number of its iterations. Our algorithm consists of two steps. In the first one we check if the group generated by \mathcal{S} is equal to $SU(d)$ (or $SO(d)$, respectively) assuming, that $\langle \mathcal{S} \rangle$ is infinite. In the second step we check if $\langle \mathcal{S} \rangle$ is finite or not.

The following list contains the most important results contained this chapter.

- **Section 4.1** Formulating the necessary universality criterion on the level of Lie algebras (Theorems 4.2 and 4.3) and Lie groups (Theorems 4.4 and 4.5). In the last part of this section we showed, how to construct Hamiltonians $\mathcal{X} = \{X_1, \dots, X_n\} \subset \mathfrak{g}$ from quantum gates $\mathcal{S} = \{g_1, \dots, g_n\} \subset G$. We also specified the conditions, for which \mathcal{X} is universal, but \mathcal{S} does not satisfy the necessary universality criterion.
- **Section 4.2.1** Formulating the sufficient universality criterion for $\langle \mathcal{S} \rangle$ to be infinite. Defining the *maximal exponent* N_G .
- **Section 4.2.3** Computing exact values of $N_{SU(2)}$ and $N_{SO(3)}$ using one-dimensional Dirichlet approximation theorem. Computing upper bounds of N_G using the modified version of the simultaneous Dirichlet approximation theorem (see Theorem 4.14).
- **Section 4.3** Presenting the algorithm for deciding universality and approximating the upper bound for the number of its steps.
- **Section 4.4** Applying the methods from Sections 4.1 and 4.2 to a 2–element set of qubit gates $\mathcal{S} = \{U(\phi_1, \vec{k}_1), U(\phi_2, \vec{k}_2)\} \subset SU(2)$ or rotation matrices $\mathcal{S} = \{O(\phi_1, \vec{k}_1), O(\phi_2, \vec{k}_2)\} \subset SO(3)$. This section includes also numerical results of the implementation of our algorithm.
- **Section 4.5** Applying the methods from Section 4.1 and 4.2 to unitary one-qubit gates or beam splitters (see more details in [69]) embedded into a gate of a larger number of possible modes. We specified the conditions for which a non-universal set $\mathcal{S} \subset SU(2)$ or $\mathcal{S} \subset SO(2)$ can be used for constructing a universal set of qudit gates or d -mode beamsplitters, respectively.

As we showed in Section 4.3 the algorithm presented in this chapter terminates after a finite number of iterations. However, computing an upper bound for a number of steps of the algorithm for an arbitrary set \mathcal{S} is still an open problem, which requires to find the spectral gap of $T_{\mathcal{S}}$ (see Section 2.5). A related question is *optimality* of our algorithm. It would be interesting to find another algorithm that could work for an arbitrary set of one-qudit gates but would terminate after fewer steps. We believe this can be done using methods of number theory (see e.g. [63, 68]).

Another open problem is how to find a tighter upper bound for N_G . As we expect, N_G actually grows exponentially with the dimension of G , however a different approach to this problem could result in a more optimal upper bound.

Chapter 5

Summary and outlook

The main purpose of this thesis was to formulate universality criteria for an arbitrary set of quantum gates. The starting point for our considerations was a set finite set

$$\mathcal{S} = \{g_1, \dots, g_n\} \subset G,$$

where $G = SU(d)$ or $G = SO(d)$, in particular $G = SU(2)$ and $G = SO(3)$. Moreover, in Chapter 4 we showed, how to construct Hamiltonians corresponding to elements of \mathcal{S} and decide their universality.

Below we present main results included in this thesis.

Chapter 3 In this chapter we considered two particular sets of one-qubit gates:

$$\begin{aligned}\mathcal{S}_\phi^{H,T} &= \{H, T(\phi)\}, \\ \mathcal{S}_\phi^{x,y,z} &= \{U(\phi/2, \vec{x}), U(\phi/2, \vec{y}), U(\phi/2, \vec{z})\},\end{aligned}$$

where ϕ is a rational multiple of π . The universality criteria proposed in this chapter are based on methods of field theory. The main results presented in this chapter include

1. Presentation of cyclotomic and trigonometric polynomials $\psi_n(x)$ and $\eta_n(x)$.
2. Proof that $\psi_n(x)$, $n \notin \{1, 2, 4\}$ has at least non-integer coefficient (Lemma 3.2).
3. Proof that $\eta_n(x)$ is a polynomial with integer coefficients (Lemma 3.4).
4. Proof that $\mathcal{S}_\phi^{H,T}$ and $\mathcal{S}_\phi^{x,y,z}$ are universal sets unless $\phi \in \{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$ (Theorem 3.5 and Corollaries 3.6 and 3.7), otherwise the sets generate finite subgroups of $SU(d)$.

At the end of this chapter we presented open problems that are related to the results. The most interesting question is how to generalize the field theory approach for another sets of one-qubit gates.

Chapter 4 This chapter is the main part of our thesis. It includes universality criteria for an arbitrary set of qudit gates $\mathcal{S} \subset G$, where G is a subgroup of $SU(d)$ or $SO(d)$ and universality criteria for a set of Hamiltonians $\mathcal{X} \subset \mathfrak{g}$, $\mathfrak{g} \subset \mathfrak{su}(d)$ or $\mathfrak{g} \subset \mathfrak{so}(d)$. We also showed that the criteria presented in this chapter could be used to construct a finite-step algorithm. We include its implementation for $\mathcal{S} \subset SU(2)$ in Appendix 6.3.

Below we list the results presented in this chapter.

1. The universality criterion for a set of Hamiltonians, $\mathcal{X} \subset \mathfrak{g}$ (Theorems 4.2 and 4.3).

2. The necessary universality criterion for a set of one-qudit gates, $\mathcal{S} \subset G$ (Theorems 4.4 and 4.5).
3. The criterion for checking whether \mathcal{S} generates an infinite number of elements (Theorem 4.13).
4. Introducing the concept of the maximal exponent N_G and computing an upper bound for N_G using the modified version of simultaneous Dirichlet's theorem (Theorem 4.14).
5. The algorithm for checking universality and proof that the algorithm always terminates after a finite number of steps.
6. Universality criteria in case, when \mathcal{S} is a two-element subset of $SU(2)$ or $SO(3)$ (Lemma 4.17 and Theorem 4.18). We also listed possible cases, when \mathcal{S} generates a finite or infinite subgroup of $SU(2)$ (or $SO(3)$, respectively). In Appendix 6.2 we included a full list of two-elements sets that generate finite subgroups of $SU(2)$.
7. Universality criteria for 2-mode unitary and orthogonal beamsplitters, that were embedded into d -mode beamsplitters, $d \geq 3$ (Theorems 4.20 and 4.21).

$$\mathcal{S}_d = \{B_{ij}, B_{ij}^\sigma : i < j, i, j \in \{1, \dots, d\}\},$$

where $B = \begin{pmatrix} \cos \phi & \sin \phi \\ -\sin \phi & \cos \phi \end{pmatrix} \in SO(2)$ or

$$B = \begin{pmatrix} \cos \phi + ik_z \sin \phi & \sin \phi(k_x + ik_y) \\ \sin \phi(-k_x + ik_y) & \cos \phi - ik_z \sin \phi \end{pmatrix},$$

$$B^\sigma = \begin{pmatrix} \cos \phi - ik_z \sin \phi & \sin \phi(-k_x + ik_y) \\ \sin \phi(k_x + ik_y) & \cos \phi + ik_z \sin \phi \end{pmatrix}.$$

An important conclusion from Section 4.5 is the following. If $B, B^\sigma \in SU(2)$ anticommute or are generators of a finite subgroup of $SU(2)$ different than $\langle 2, 2, 2 \rangle$, then \mathcal{S}_d becomes universal for an arbitrary $d \geq 3$.

At the end of Chapter 4 we pointed out the open problems related to our approach:

- Finding a tighter upper bound for N_G .
- Finding a more optimal algorithm for deciding universality, i.e. an algorithm that allows to decide universality after a fewer steps. A possibly useful approach to this problem is field theory and algebraic number theory approach.

Chapter 6

Appendix

In this chapter we include auxiliary results that extend our considerations from Chapters 3 and 4 but are not necessary to formulate the universality criteria. At the end of this chapter we present the algorithm for deciding universality of a set $\mathcal{S} = \{U(\phi_1, \vec{k}_1), U(\phi_2, \vec{k}_2)\} \subset SU(2)$ implemented in Octave.

6.1. Appendix 1: alternative version of the proof of Fact 3.4

The proof of Fact 3.4 that we presented in Section 3.2.0.8 is based on Gauss lemma and properties of cyclotomic polynomials. In particular, we used the fact that cyclotomic polynomials have integer coefficients, however this property does not result directly from defining formula (3.13). Therefore we present in this section an alternative proof of Fact 3.4, which is based on recurrence formula for Chebyshev polynomials. The first step of the proof concerns properties of Chebyshev polynomials $T_n(x)$. In the second and third step we will use the identity (3.41) and represent $\eta_n(x)$ as a fraction of integer monic polynomials. We start from recalling Fact 3.4.

Fact 6.1. *All the coefficients of $\eta_n(x)$ are integers.*

Proof. We start from proving the following auxiliary fact.

Fact 6.2. *Let $T_k(x)$ be a Chebyshev polynomial of the first kind, defined as $T_k(x) = \sum_{i=0}^k c_i x^i$. Then the coefficients c_i , $i \in \{1, \dots, k\}$ are divisible by 2^{i-1} .*

The proof of Fact 6.2 stems from the recurrence formula (3.22) for Chebyshev polynomials. First, from formula (3.22) we get immediately that the leading term of $T_k(x)$ is equal to $c_k = 2^{k-1}$. The same holds for the coefficients c_0 and c_1 . From (3.22) we have $c_0 \in \{-1, 0, 1\}$ and $c_1 \in \{-k, 0, k\}$, where k is an odd number. therefore the only power of 2 dividing c_0 and c_1 is $2^0 = 1$. In case, when $c_i \notin \{c_0, c_1, c_k\}$ Fact 6.2 can be proven recursively. Let us consider polynomials $T_{k+1}(x)$, $T_k(x)$, where $k \geq 2$, and $T_{k-1}(x)$ and denote their coefficients by $\{c_i^{(k+1)}\}$, $\{c_i^{(k)}\}$, $\{c_i^{(k-1)}\}$, respectively¹. Writing formula (3.22) explicitly we arrive at the equation

$$\sum_{i=0}^{k+1} c_i^{(k+1)} x^i = 2x \sum_{j=0}^k c_j^{(k)} x^j - \sum_{l=0}^{k-1} c_l^{(k-1)} x^l \Rightarrow c_i^{(k+1)} = 2c_{i-1}^{(k)} - c_i^{(k-1)}. \quad (6.1)$$

Let us start from $c_2^{(k+1)}$. By (6.1) $c_2^{(k+1)} = 2c_1^{(k)} - c_2^{(k-1)}$. We assume that $c_1^{(k)}$ is nonzero, but $c_1^{(k)} = \pm k$, then $c_2^{(k+1)} = \pm 2k - c_2^{(k-1)}$. The coefficient $c_2^{(k-1)}$ can be again defined as

¹We skip upper indexes in the rest of the paper

$c_2^{(k-1)} = c_1^{(k-2)} - c_2^{(k-3)} = \mp 2(k-2) - c_2^{(k-3)}$ etc., until we arrive at $c_2^{k-l} = 0$ for $l = k$ or $l = k-1$. Thus we can represent $c_2^{(k+1)}$ as the sum

$$c_2^{(k+1)} = \sum_{i=0}^l (-1)^{\lfloor k/2 \rfloor} 2(k-i),$$

therefore $c_2^{(k+1)}$ must be divisible by $2 = 2^1$ but not by higher powers of 2.

Next we consider $c_3^{(k+1)}$, which is $c_3^{(k+1)} = 2c_2^{(k)} - c_3^{(k-1)}$ by (6.1). We can again represent the coefficient as a sum $c_3^{(k+1)} = 2c_2^{(k)} - (2c_2^{(k-2)} - 2c_2^{(k-4)} - \dots)$ that simplifies to $c_3^{(k+1)} = \sum_{i=0}^l (-1)^i 2c_2^{k-i}$. Because all c_2^{k-i} 's are divisible by 2, then $c_3^{(k+1)}$ is divisible by $4 = 2^2 = 2^{3-1}$. Using the same reasoning for the other $c_i^{(k+1)}$'s iteratively we observe that every $c_i^{(k+1)}$ is divisible by 2^{i-1} .

In the next step we show that $2T_k\left(\frac{x}{2}\right)$ is a monic polynomial with integer coefficients. To this end we write it explicitly as $2T_k\left(\frac{x}{2}\right) = 2 \sum_{i=0}^k c_i \left(\frac{x}{2}\right)^i$. Because each c_i is divisible by 2^{i-1} , it can be rewritten as a product of the form $c_i = 2^{i-1}n_i$, where $n_i \in \mathbb{N}$. Substituting $x \rightarrow \frac{x}{2}$ we arrive at

$$2T_k\left(\frac{x}{2}\right) = 2 \sum_{i=0}^k 2^{i-1}n_i \left(\frac{x}{2}\right)^i = \sum_{i=0}^k n_i x^i.$$

Let us express $\psi_{2n}\left(\frac{x}{2}\right)$ in terms of Chebyshev polynomials as in (3.26,3.27). Denote $P_k\left(\frac{x}{2}\right) = T_{\lfloor \frac{k}{2} \rfloor + 1}\left(\frac{x}{2}\right) - T_{\lfloor \frac{k}{2} \rfloor}\left(\frac{x}{2}\right)$ if k is odd, or $P_k(x) = T_{\frac{k}{2}+1}\left(\frac{x}{2}\right) - T_{\frac{k}{2}-1}\left(\frac{x}{2}\right)$ if k is an even number. Then by (3.41) we get

$$\psi_{2n}\left(\frac{x}{2}\right) = \prod_{k|2n} 2^{-\lfloor k/2 \rfloor} P_k\left(\frac{x}{2}\right)^{\mu(n/d)} = \quad (6.2)$$

$$= \psi_{2n}\left(\frac{x}{2}\right) = 2^{-d} \frac{p(x)}{q(x)}, \text{ where} \quad (6.3)$$

$$p(x) = \prod_{k|2n} P_k\left(\frac{x}{2}\right)^{\mu(2n/k)=1}, \quad q(x) = \prod_{k|2n} P_k\left(\frac{x}{2}\right)^{\mu(2n/k)=-1}, \quad (6.4)$$

where 2^{-d} is the normalizing factor obtained from the normalizing factors of $P_k(x)$'s. Theorem 2.2 and Fact 6.2 imply that both $p\left(\frac{x}{2}\right)$ and $q\left(\frac{x}{2}\right)$ multiplied by 2^m , where m is the number of divisors of $2n$, monic polynomials with integer coefficients.

Recall that $\eta_n(x)$ depends on $p(x)$ and $q(x)$ as:

$$\eta_n(x) = 2^d \psi_{2n}\left(\frac{x}{2}\right) = 2^d 2^{-d} \frac{p(x)}{q(x)} = \frac{p(x)}{q(x)}.$$

Let $p(x) = \sum_{i=0}^{\deg p(x)} p_i x^i$ and $q(x) = \sum_{i=0}^{\deg q(x)} q_i x^i$, where $\deg q < \deg p$. We have shown that $q_{\deg q(x)} = 1$. This fact allows us to find an explicit expression for the coefficients of $\eta_n(x) = \sum_{i=0}^d \eta_i x^i$:

$$p(x) = q(x)\eta_n(x) \Rightarrow \sum_{i=0}^{\deg p(x)} p_i x^i = \sum_{j=0}^{\deg q(x)} q_j x^j \sum_{l=0}^d \eta_l x^l.$$

$q(x)$ is a monomial, thus $q_{\deg q(x)} = 1$ and we have

$$\begin{aligned}\eta_0 &= p_0 - q_0, \\ \eta_0 &= p_{\deg q(x)} - \sum_{i=0}^{\deg q(x)-1} q_i \eta_{\deg q(x)-i}, \\ \eta_j &= p_{\deg q(x)+j} - \sum_{i=0}^{\deg q(x)+j-1} q_i \eta_{\deg q(x)+j-i}\end{aligned}$$

If $\eta_0 \in \mathbb{N}$, then $p_j, q_k \in \mathbb{N}$ for all $j \in \{1, \dots, \deg p(x)\}$, $k \in \{1, \dots, \deg q(x)\}$ implies that all η_i 's are integers. \square

6.2. Appendix 2: generators of finite subgroups of $SU(2)$

In Table 6.1 and Table 6.2 we present a list of all generators of the finite subgroups of $SU(2)$, i.e. $\langle 2, 3, 3 \rangle$, $\langle 2, 3, 4 \rangle$, $\langle 2, 3, 5 \rangle$ and finite dimensional dicyclic groups. All of these generators have been found both numerically (see the procedure from Section 4.4.0.2) and by analysis of the platonic polyhedrons.

6.3. Appendix 4: Implementation of the algorithm for deciding universality of $\mathcal{S} = \{U(\phi_1, \vec{k}_1), U(\phi_2, \vec{k}_2)\}$

This appendix includes the implementation of our algorithm for the case, when \mathcal{S} consists of two arbitrary one-qudit gates. The program that implements the algorithm was written in Matlab/Octave. It consists of several subprograms that are listed below:

1. *adjointRep.m* - takes a matrix from $SU(2)$ and computes its adjoint representation.
2. *commutantChecking.m* - takes two matrices from $SU(2)$ and checks, if they commute or anticommute.
3. *equality.m* - takes \mathcal{S}_l and \mathcal{S}_{l+1} as input and compares these sets
4. *isOfFiniteOrder.m* - checks if a matrix $U(\phi, \vec{k})$ is an exceptional matrix.
5. *setOfGates.m* - computes the sets \mathcal{S}_{l+1} from \mathcal{S}_l , $U(\phi_1, \vec{k}_1)$, $U(\phi_2, \vec{k}_2)$ and l that are set as input.
6. *setU.m* - defines a matrix $U(\phi, \vec{k})$ using the parameters ϕ and \vec{k} .
7. *algorithm.m* - An interactive program that realizes the algorithm from Section 4.3.

Below we attach the code of each program.

adjointRep.m

```
function o = ajoinRep(u)
o = zeros(3);
if (size(u,1)==2 || size(u,2)==2)
%create adjoint representation of U(k,phi)
o(1,1) = (u(1,1)^2-u(1,2)^2+u(2,2)^2-conj(u(1,2)^2) ) ./2;
```

No.	ϕ_1	ϕ_2	$\vec{k}_1 \cdot \vec{k}_2$	γ	$\langle l, m, n \rangle$	No.	ϕ_1	ϕ_2	$\vec{k}_1 \cdot \vec{k}_2$	γ	$\langle l, m, n \rangle$
1	$\pm \frac{\pi}{2}$	$\pm \frac{\pi}{2}$	$(-1, 1)$	$\frac{k\pi}{n}$	$\langle 2, 2, n \rangle$	2	$\pm \frac{\pi}{2}$	$\frac{k\pi}{n}$	0	$\pm \frac{\pi}{2}$	$\langle 2, 2, n \rangle$
3	$\frac{\pi}{3}, \frac{2\pi}{3}$	$\pm \frac{\pi}{2}$	$\mp \frac{1}{\sqrt{3}}$	$\pm \frac{\pi}{3}$	$\langle 2, 3, 3 \rangle$	4	$\frac{\pi}{3}, \frac{2\pi}{3}$	$\pm \frac{\pi}{2}$	$\pm \frac{1}{\sqrt{3}}$	$\frac{2\pi}{3}$	$\langle 2, 3, 3 \rangle$
5	$\frac{4\pi}{3}, \frac{5\pi}{3}$	$\pm \frac{\pi}{2}$	$\pm \frac{1}{\sqrt{3}}$	$\pm \frac{\pi}{3}$	$\langle 2, 3, 3 \rangle$	6	$\frac{4\pi}{3}, \frac{5\pi}{3}$	$\pm \frac{\pi}{2}$	$\mp \frac{1}{\sqrt{3}}$	$\frac{2\pi}{3}$	$\langle 2, 3, 3 \rangle$
3	$\frac{\pi}{3}$	$\pm \frac{\pi}{3}$	$\pm \frac{1}{3}$	$\frac{k\pi}{2}$	$\langle 2, 3, 3 \rangle$	4	$\frac{\pi}{3}$	$\pm \frac{\pi}{3}$	$\mp \frac{1}{3}$	$\pm \frac{\pi}{3}$	$\langle 2, 3, 3 \rangle$
5	$\frac{\pi}{3}$	$\pm \frac{2\pi}{3}$	$\mp \frac{1}{3}$	$\frac{k\pi}{2}$	$\langle 2, 3, 3 \rangle$	6	$\frac{\pi}{3}$	$\pm \frac{2\pi}{3}$	$\pm \frac{1}{3}$	$\pm \frac{2\pi}{3}$	$\langle 2, 3, 3 \rangle$
7	$\frac{2\pi}{3}$	$\pm \frac{2\pi}{3}$	$\pm \frac{1}{3}$	$\frac{k\pi}{2}$	$\langle 2, 3, 3 \rangle$	8	$\frac{2\pi}{3}$	$\pm \frac{2\pi}{3}$	$\mp \frac{1}{3}$	$\pm \frac{\pi}{3}$	$\langle 2, 3, 3 \rangle$
9	$\pm \frac{\pi}{2}$	$\frac{\pi}{3}, \frac{2\pi}{3}$	$\mp \frac{2}{\sqrt{6}}$	$\frac{\pi}{4}, \frac{7\pi}{4}$	$\langle 2, 3, 4 \rangle$	10	$\pm \frac{\pi}{2}$	$\frac{\pi}{3}, \frac{2\pi}{3}$	$\pm \frac{2}{\sqrt{6}}$	$\frac{3\pi}{4}, \frac{5\pi}{4}$	$\langle 2, 3, 4 \rangle$
11	$\pm \frac{\pi}{2}$	$-\frac{\pi}{3}, \frac{2\pi}{3}$	$\pm \frac{2}{\sqrt{6}}$	$\frac{\pi}{4}, \frac{7\pi}{4}$	$\langle 2, 3, 4 \rangle$	12	$\pm \frac{\pi}{2}$	$-\frac{\pi}{3}, \frac{2\pi}{3}$	$\mp \frac{2}{\sqrt{6}}$	$\frac{3\pi}{4}, \frac{5\pi}{4}$	$\langle 2, 3, 4 \rangle$
13	$\pm \frac{\pi}{2}$	$\frac{\pi}{4}, \frac{5\pi}{4}$	$\mp \frac{1}{\sqrt{2}}$	$\frac{\pi}{3}, \frac{5\pi}{3}$	$\langle 2, 3, 4 \rangle$	14	$\pm \frac{\pi}{2}$	$\frac{\pi}{4}, \frac{5\pi}{4}$	$\pm \frac{1}{\sqrt{2}}$	$\frac{2\pi}{3}, \frac{4\pi}{3}$	$\langle 2, 3, 4 \rangle$
15	$\pm \frac{\pi}{2}$	$\frac{\pi}{4}, \frac{5\pi}{4}$	$\pm \frac{1}{\sqrt{2}}$	$\frac{\pi}{3}, \frac{5\pi}{3}$	$\langle 2, 3, 4 \rangle$	16	$\pm \frac{\pi}{2}$	$\frac{\pi}{4}, \frac{5\pi}{4}$	$\mp \frac{1}{\sqrt{2}}$	$\frac{2\pi}{3}, \frac{4\pi}{3}$	$\langle 2, 3, 4 \rangle$
17	$\pm \frac{\pi}{4}$	$\pm \frac{\pi}{4}$	0	$\frac{\pi}{3}, \frac{5\pi}{3}$	$\langle 2, 3, 4 \rangle$	18	$\pm \frac{\pi}{4}$	$\pm \frac{3\pi}{4}$	0	$\frac{2\pi}{3}, \frac{4\pi}{3}$	$\langle 2, 3, 4 \rangle$
19	$\pm \frac{3\pi}{4}$	$\frac{3\pi}{4}$	0	$\frac{\pi}{3}, \frac{5\pi}{3}$	$\langle 2, 3, 4 \rangle$	20	$\pm \frac{3\pi}{4}$	$\pm \frac{\pi}{4}$	0	$\frac{2\pi}{3}, \frac{4\pi}{3}$	$\langle 2, 3, 4 \rangle$
21	$\pm \frac{\pi}{3}$	$\pm \frac{\pi}{3}$	$\mp \frac{\sqrt{5}}{3}$	$\frac{\pi}{5}, \frac{9\pi}{5}$	$\langle 2, 3, 5 \rangle$	22	$\pm \frac{\pi}{3}$	$\pm \frac{\pi}{3}$	$\pm \frac{\sqrt{5}}{3}$	$\frac{3\pi}{5}, \frac{7\pi}{5}$	$\langle 2, 3, 5 \rangle$
23	$\pm \frac{\pi}{3}$	$\pm \frac{2\pi}{3}$	$\mp \frac{\sqrt{5}}{3}$	$\frac{2\pi}{5}, \frac{8\pi}{5}$	$\langle 2, 3, 5 \rangle$	24	$\pm \frac{\pi}{3}$	$\pm \frac{2\pi}{3}$	$\pm \frac{\sqrt{5}}{3}$	$\frac{4\pi}{5}, \frac{6\pi}{5}$	$\langle 2, 3, 5 \rangle$
25	$\pm \frac{2\pi}{3}$	$\pm \frac{2\pi}{3}$	$\mp \frac{\sqrt{5}}{3}$	$\frac{\pi}{5}, \frac{9\pi}{5}$	$\langle 2, 3, 5 \rangle$	26	$\pm \frac{2\pi}{3}$	$\frac{2\pi}{3}$	$\pm \frac{\sqrt{5}}{3}$	$\frac{3\pi}{5}, \frac{7\pi}{5}$	$\langle 2, 3, 5 \rangle$
27	$\pi/5$	$\pm \frac{\pi}{5}$	$\pm \frac{1}{\sqrt{5}}$	$\frac{\pi}{3}, \frac{5\pi}{3}$	$\langle 2, 3, 5 \rangle$	28	$\frac{\pi}{5}$	$\pm \frac{\pi}{5}$	$\mp \frac{1}{\sqrt{5}}$	$\frac{\pi}{5}, \frac{9\pi}{5}$	$\langle 2, 3, 5 \rangle$
29	$\frac{\pi}{5}$	$\pm \frac{2\pi}{5}$	$\pm \frac{1}{\sqrt{5}}$	$\frac{\pi}{2}, \frac{3\pi}{2}$	$\langle 2, 3, 5 \rangle$	30	$\frac{\pi}{5}$	$\frac{2\pi}{5}$	$\mp \frac{1}{\sqrt{5}}$	$\frac{\pi}{3}, \frac{5\pi}{3}$	$\langle 2, 3, 5 \rangle$
31	$\frac{\pi}{5}$	$\pm \frac{4\pi}{5}$	$\pm \frac{1}{\sqrt{5}}$	$\frac{4\pi}{5}, \frac{6\pi}{5}$	$\langle 2, 3, 5 \rangle$	32	$\frac{\pi}{5}$	$\frac{3\pi}{5}$	$\mp \frac{1}{\sqrt{5}}$	$\frac{\pi}{2}, \frac{3\pi}{2}$	$\langle 2, 3, 5 \rangle$
33	$\frac{\pi}{5}$	$\pm \frac{3\pi}{5}$	$\pm \frac{1}{\sqrt{5}}$	$\frac{2\pi}{3}, \frac{4\pi}{3}$	$\langle 2, 3, 5 \rangle$	34	$\frac{2\pi}{5}$	$\pm \frac{2\pi}{5}$	$\mp \frac{1}{\sqrt{5}}$	$\frac{\pi}{5}, \frac{9\pi}{5}$	$\langle 2, 3, 5 \rangle$
35	$\frac{\pi}{5}$	$\pm \frac{4\pi}{5}$	$\mp \frac{1}{\sqrt{5}}$	$\frac{2\pi}{3}, \frac{4\pi}{3}$	$\langle 2, 3, 5 \rangle$	36	$\frac{\pi}{2}$	$\pm \frac{\pi}{5}$	∓ 0.851	$\frac{\pi}{3}, \frac{5\pi}{3}$	$\langle 2, 3, 5 \rangle$
37	$\frac{\pi}{2}$	$\pm \frac{\pi}{5}$	± 0.851	$\frac{2\pi}{3}, \frac{4\pi}{3}$	$\langle 2, 3, 5 \rangle$	38	$\frac{\pi}{2}$	$\pm \frac{\pi}{5}$	∓ 0.526	$\frac{2\pi}{5}, \frac{8\pi}{5}$	$\langle 2, 3, 5 \rangle$
39	$\frac{\pi}{2}$	$\pm \frac{\pi}{5}$	± 0.526	$\frac{3\pi}{5}, \frac{7\pi}{5}$	$\langle 2, 3, 5 \rangle$	40	$\frac{\pi}{2}$	$\pm \frac{2\pi}{5}$	∓ 0.526	$\frac{\pi}{3}, \frac{5\pi}{3}$	$\langle 2, 3, 5 \rangle$
41	$\frac{\pi}{2}$	$\pm \frac{2\pi}{5}$	± 0.526	$\frac{2\pi}{3}, \frac{4\pi}{3}$	$\langle 2, 3, 5 \rangle$	42	$\frac{\pi}{2}$	$\pm \frac{2\pi}{5}$	∓ 0.851	$\frac{\pi}{5}, \frac{9\pi}{5}$	$\langle 2, 3, 5 \rangle$
43	$\frac{\pi}{2}$	$\pm \frac{3\pi}{5}$	∓ 0.526	$\frac{\pi}{3}, \frac{5\pi}{3}$	$\langle 2, 3, 5 \rangle$	44	$\frac{\pi}{2}$	$\pm \frac{3\pi}{5}$	± 0.526	$\frac{2\pi}{3}, \frac{4\pi}{3}$	$\langle 2, 3, 5 \rangle$
45	$\frac{\pi}{2}$	$\pm \frac{3\pi}{5}$	∓ 0.851	$\frac{\pi}{5}, \frac{9\pi}{5}$	$\langle 2, 3, 5 \rangle$	46	$\frac{\pi}{2}$	$\pm \frac{3\pi}{5}$	± 0.851	$\frac{4\pi}{5}, \frac{6\pi}{5}$	$\langle 2, 3, 5 \rangle$
47	$\frac{\pi}{2}$	$\pm \frac{4\pi}{5}$	∓ 0.851	$\frac{\pi}{3}, \frac{5\pi}{3}$	$\langle 2, 3, 5 \rangle$	48	$\frac{\pi}{2}$	$\pm \frac{4\pi}{5}$	± 0.851	$\frac{2\pi}{3}, \frac{4\pi}{3}$	$\langle 2, 3, 5 \rangle$
49	$\frac{\pi}{2}$	$\pm \frac{4\pi}{5}$	∓ 0.525	$\frac{2\pi}{5}, \frac{8\pi}{5}$	$\langle 2, 3, 5 \rangle$	50	$\frac{\pi}{2}$	$\pm \frac{4\pi}{5}$	± 0.525	$\frac{3\pi}{5}, \frac{7\pi}{5}$	$\langle 2, 3, 5 \rangle$

Table 6.1: Generators of finite subgroups of $SU(2)$: $\langle 2, 2, n \rangle$, $\langle 2, 3, 3 \rangle$, $\langle 2, 3, 4 \rangle$, $\langle 2, 3, 5 \rangle$.

```

o(2,1) = i.*(u(1,1)^2-u(1,2)^2-u(2,2)^2+conj(u(1,2)^2))./2;
o(3,1) = u(2,2).*u(1,2)-u(1,1).*u(2,1);
o(1,2) = i.*(-u(1,1)^2-u(1,2)^2+u(2,2)^2+conj(u(1,2)^2))./2;
o(2,2) = (u(1,1)^2+u(1,2)^2+u(2,2)^2+conj(u(1,2)^2))./2;
o(3,2) = (u(2,2).*u(1,2)+u(1,1).*u(2,1)).*i;
o(1,3) = u(2,2).*u(2,1)-u(1,1).*u(1,2);
o(2,3) = -(u(2,2).*u(2,1)+u(1,1).*u(1,2)).*i;
o(3,3) = u(2,2).*u(1,1) + u(2,1).*u(1,2);
end
end

```

commutantChecking.m

```

function v = commutantChecking( u1,u2 )
epsilon = 0.0001;
o1 = adjointRep(u1)

```


No.	ϕ_1	ϕ_2	$\vec{k}_1 \cdot \vec{k}_2$	γ	$\langle l, m, n \rangle$	No.	ϕ_1	ϕ_2	$\vec{k}_1 \cdot \vec{k}_2$	γ	$\langle l, m, n \rangle$
51	$\frac{4\pi}{5}$	$\pm \frac{4\pi}{5}$	$\pm \frac{1}{\sqrt{5}}$	$\frac{\pi}{3}, \frac{5\pi}{3}$	$\langle 2, 3, 5 \rangle$	52	$\frac{2\pi}{5}$	$\pm \frac{2\pi}{5}$	$\pm \frac{1}{\sqrt{5}}$	$\frac{3\pi}{5}, \frac{7\pi}{5}$	$\langle 2, 3, 5 \rangle$
53	$\frac{2\pi}{5}$	$\pm \frac{3\pi}{5}$	$\pm \frac{1}{\sqrt{5}}$	$\frac{2\pi}{3}, \frac{4\pi}{3}$	$\langle 2, 3, 5 \rangle$	54	$\frac{2\pi}{5}$	$\pm \frac{3\pi}{5}$	$\mp \frac{1}{\sqrt{5}}$	$\frac{2\pi}{5}, \frac{8\pi}{5}$	$\langle 2, 3, 5 \rangle$
55	$\frac{2\pi}{5}$	$\pm \frac{4\pi}{5}$	$\mp \frac{1}{\sqrt{5}}$	$\frac{\pi}{2}, \frac{3\pi}{2}$	$\langle 2, 3, 5 \rangle$	56	$\frac{2\pi}{5}$	$\pm \frac{4\pi}{5}$	$\pm \frac{1}{\sqrt{5}}$	$\frac{2\pi}{3}, \frac{4\pi}{3}$	$\langle 2, 3, 5 \rangle$
57	$\frac{2\pi}{3}$	$\pm \frac{3\pi}{5}$	∓ 0.794	$\frac{\pi}{5}, \frac{9\pi}{5}$	$\langle 2, 3, 5 \rangle$	58	$\frac{3\pi}{5}$	$\pm \frac{3\pi}{5}$	$\mp \frac{1}{\sqrt{5}}$	$\frac{\pi}{2}, \frac{3\pi}{2}$	$\langle 2, 3, 5 \rangle$
59	$\frac{2\pi}{3}$	$\pm \frac{3\pi}{5}$	∓ 0.794	$\frac{\pi}{5}, \frac{9\pi}{5}$	$\langle 2, 3, 5 \rangle$	60	$\frac{3\pi}{5}$	$\pm \frac{3\pi}{5}$	$\pm \frac{1}{\sqrt{5}}$	$\frac{3\pi}{2}, \frac{7\pi}{2}$	$\langle 2, 3, 5 \rangle$
61	$\frac{3\pi}{5}$	$\pm \frac{4\pi}{5}$	$\pm \frac{1}{\sqrt{5}}$	$\frac{\pi}{2}, \frac{3\pi}{2}$	$\langle 2, 3, 5 \rangle$	62	$\frac{3\pi}{5}$	$\pm \frac{4\pi}{5}$	$\mp \frac{1}{\sqrt{5}}$	$\frac{2\pi}{3}, \frac{4\pi}{3}$	$\langle 2, 3, 5 \rangle$
63	$\frac{4\pi}{5}$	$\pm \frac{4\pi}{5}$	$\mp \frac{1}{\sqrt{5}}$	$\frac{\pi}{5}, \frac{9\pi}{5}$	$\langle 2, 3, 5 \rangle$	64	$\frac{\pi}{3}$	$\pm \frac{\pi}{5}$	± 0.795	$\frac{\pi}{2}, \frac{3\pi}{2}$	$\langle 2, 3, 5 \rangle$
65	$\frac{\pi}{3}$	$\pm \frac{\pi}{5}$	∓ 0.188	$\frac{\pi}{3}, \frac{5\pi}{3}$	$\langle 2, 3, 5 \rangle$	66	$\frac{\pi}{3}$	$\pm \frac{\pi}{5}$	∓ 0.795	$\frac{\pi}{5}, \frac{9\pi}{5}$	$\langle 2, 3, 5 \rangle$
67	$\frac{\pi}{3}$	$\pm \frac{\pi}{5}$	± 0.188	$\frac{2\pi}{5}, \frac{8\pi}{5}$	$\langle 2, 3, 5 \rangle$	68	$\frac{\pi}{3}$	$\pm \frac{2\pi}{5}$	± 0.188	$\frac{\pi}{2}, \frac{3\pi}{2}$	$\langle 2, 3, 5 \rangle$
69	$\frac{2\pi}{3}$	$\pm \frac{4\pi}{5}$	± 0.188	$\frac{2\pi}{5}, \frac{8\pi}{5}$	$\langle 2, 3, 5 \rangle$	70	$\frac{\pi}{3}$	$\pm \frac{2\pi}{5}$	± 0.795	$\frac{2\pi}{3}, \frac{4\pi}{3}$	$\langle 2, 3, 5 \rangle$
71	$\frac{\pi}{3}$	$\pm \frac{2\pi}{5}$	∓ 0.795	$\frac{\pi}{5}, \frac{9\pi}{5}$	$\langle 2, 3, 5 \rangle$	72	$\frac{\pi}{3}$	$\pm \frac{2\pi}{5}$	∓ 0.188	$\frac{2\pi}{5}, \frac{8\pi}{5}$	$\langle 2, 3, 5 \rangle$
73	$\frac{\pi}{3}$	$\pm \frac{3\pi}{5}$	∓ 0.188	$\frac{\pi}{2}, \frac{3\pi}{2}$	$\langle 2, 3, 5 \rangle$	74	$\frac{\pi}{3}$	$\pm \frac{3\pi}{5}$	∓ 0.795	$\frac{\pi}{3}, \frac{5\pi}{3}$	$\langle 2, 3, 5 \rangle$
75	$\frac{2\pi}{3}$	$\pm \frac{4\pi}{5}$	∓ 0.188	$\frac{\pi}{3}, \frac{5\pi}{3}$	$\langle 2, 3, 5 \rangle$	76	$\frac{2\pi}{3}$	$\pm \frac{4\pi}{5}$	∓ 0.795	$\frac{\pi}{5}, \frac{9\pi}{5}$	$\langle 2, 3, 5 \rangle$
77	$\frac{\pi}{3}$	$\pm \frac{3\pi}{5}$	∓ 0.188	$\frac{3\pi}{5}, \frac{7\pi}{5}$	$\langle 2, 3, 5 \rangle$	78	$\frac{\pi}{3}$	$\pm \frac{3\pi}{5}$	∓ 0.795	$\frac{4\pi}{5}, \frac{6\pi}{5}$	$\langle 2, 3, 5 \rangle$
79	$\frac{\pi}{3}$	$\pm \frac{4\pi}{5}$	∓ 0.795	$\frac{\pi}{2}, \frac{3\pi}{2}$	$\langle 2, 3, 5 \rangle$	80	$\frac{\pi}{3}$	$\pm \frac{4\pi}{5}$	∓ 0.188	$\frac{2\pi}{3}, \frac{4\pi}{3}$	$\langle 2, 3, 5 \rangle$
81	$\frac{\pi}{3}$	$\pm \frac{4\pi}{5}$	∓ 0.188	$\frac{3\pi}{5}, \frac{7\pi}{5}$	$\langle 2, 3, 5 \rangle$	82	$\frac{\pi}{3}$	$\pm \frac{4\pi}{5}$	∓ 0.795	$\frac{4\pi}{5}, \frac{6\pi}{5}$	$\langle 2, 3, 5 \rangle$
83	$\frac{2\pi}{3}$	$\pm \frac{\pi}{5}$	∓ 0.795	$\frac{\pi}{2}, \frac{3\pi}{2}$	$\langle 2, 3, 5 \rangle$	84	$\frac{2\pi}{3}$	$\pm \frac{\pi}{5}$	∓ 0.188	$\frac{2\pi}{3}, \frac{4\pi}{3}$	$\langle 2, 3, 5 \rangle$
85	$\frac{2\pi}{3}$	$\pm \frac{\pi}{5}$	∓ 0.795	$\frac{4\pi}{5}, \frac{6\pi}{5}$	$\langle 2, 3, 5 \rangle$	86	$\frac{\pi}{3}$	$\pm \frac{4\pi}{5}$	∓ 0.795	$\frac{4\pi}{5}, \frac{6\pi}{5}$	$\langle 2, 3, 5 \rangle$
87	$\frac{2\pi}{3}$	$\pm \frac{2\pi}{5}$	∓ 0.188	$\frac{\pi}{2}, \frac{3\pi}{2}$	$\langle 2, 3, 5 \rangle$	88	$\frac{2\pi}{3}$	$\pm \frac{2\pi}{5}$	∓ 0.795	$\frac{\pi}{3}, \frac{5\pi}{3}$	$\langle 2, 3, 5 \rangle$
89	$\frac{2\pi}{3}$	$\pm \frac{4\pi}{5}$	± 0.795	$\frac{\pi}{2}, \frac{3\pi}{2}$	$\langle 2, 3, 5 \rangle$	90	$\frac{2\pi}{3}$	$\pm \frac{3\pi}{5}$	∓ 0.188	$\frac{2\pi}{5}, \frac{8\pi}{5}$	$\langle 2, 3, 5 \rangle$
91	$\frac{2\pi}{3}$	$\pm \frac{2\pi}{5}$	± 0.188	$\frac{3\pi}{5}, \frac{7\pi}{5}$	$\langle 2, 3, 5 \rangle$	92	$\frac{2\pi}{3}$	$\pm \frac{2\pi}{5}$	± 0.795	$\frac{4\pi}{5}, \frac{6\pi}{5}$	$\langle 2, 3, 5 \rangle$
93	$\frac{2\pi}{3}$	$\pm \frac{3\pi}{5}$	± 0.188	$\frac{\pi}{2}, \frac{3\pi}{2}$	$\langle 2, 3, 5 \rangle$	94	$\frac{2\pi}{3}$	$\pm \frac{3\pi}{5}$	± 0.795	$\frac{2\pi}{3}, \frac{4\pi}{3}$	$\langle 2, 3, 5 \rangle$

Table 6.2: Generators of $\langle 2, 3, 5 \rangle$.

```
o2 = adjointRep(u2)
v = 1;
comm = o1*o2-o2*o1;
acomm = o1*o2+o2*o1;
```

```
if (norm(comm)<epsilon || norm(acomm)<epsilon)
v = 0;
end
```

```
end
```

equality.m

```
function res = equality(newSet,S)
res=0;
epsilon=0.0001;
%definig matrix of differences
differences = ones(1,size(newSet,3));
```

```
for m=1:size(newSet,3)
for n=1:size(S,3)
if norm(newSet(:, :,m)-S(:, :,n))<epsilon %equality of elements of S and newSet
differences(m) = 0;
```

```

break;
end
end
end
if norm(differences)==0
res=1;
end
end

```

isOfFiniteOrder.m

```

function res = isOfFiniteOrder(u)
res = 1;
nmax=44;
epsilon = 0.0001;
I = eye(2);
n=1;

while ( norm(u^n-I)>1/sqrt(2)  && n<=nmax )
n = n+1;
end

if (norm(u^n-I)<epsilon|| norm(u^n+I)<epsilon)
res=0;
end

end

```

setOfGates.m

```

function s = setOfGates(s_prev,u1,u2,n)
s = zeros(2,2,2^(n+1));
for k=1:2^n
s(:,:,k)=s_prev(:,:,k)*u1;
s(:,:,k+2^n)=s_prev(:,:,k)*u2;
end
end

```

setU.m

```

function u = setU(k,phi)
u = zeros(2,2);

if (size(k,1) == 1  && size(k,2)==3 )
% 2-norm vector k
n = norm(k);
k = k/sqrt(n);

%%fill matrix elements
u(1,1) = cos(phi)+i*k(1,3)*sin(phi);
u(1,2) = sin(phi)*(k(1,1)+i*k(1,2));

```

```

u(2,1) = sin(phi)*(-k(1,1)+i*k(1,2));
u(2,2) = cos(phi)-i*k(1,3)*sin(phi);
end
end

```

algorithm.m

```

clear all;
prompt='Set axis k1 - horizontal 3D vector [x,y,z] \n';
k1=input(prompt);
prompt='Set angle phi1 (real)\n';
phi1=input(prompt);
prompt='Set axis k2 - horizontal 3D vector [x,y,z] \n';
k2=input(prompt);
prompt='Set angle phi2 (real)\n';
phi2=input(prompt);

u1=setU(k1,phi1);
u2=setU(k2,phi2);
l=1;

%first step
if commutantChecking( u1,u2 )== 0
disp('U1,U2 - Non-universal set');
else %second and third step
S = zeros(2,2,2);
S(:,:,1)=u1;
S(:,:,2)=u2;
isFinite=1;
while isFinite==1
for n=1:2^l
if isInfinite(S(:,:,n))==1
isFinite=0;
disp('U1,U2 - Universal set');
break;
end
newSet = setOfGates(S,u1,u2,l);
if equality(newSet,S)==1
isFinite=0;
disp('U1,U2 - Non-universal set');
break;
end
S=newSet;
l=l+1;
end

end

end

disp('Length necessary to decide universality');

```

1-1

List of Figures

1.1.	A Boolean circuit adding two bits, denoted by A and B .	16
1.2.	An example quantum circuit built from a one-qudit gate, denoted by U_3 , a two-qudit gate U_1 and a three-qudit gate U_2 . An output state is an entangled state of $ q_1\rangle, q_2\rangle, q_3\rangle$.	17
2.1.	Bloch sphere with denoted Hadamard matrix and the rotation matrix by angle ϕ around the axis \vec{k}_z . In general every unitary gate $U(\phi, \vec{k})$ is a rotation by angle ϕ around the axis $\vec{k} = (k_x, k_y, k_z)$.	46
4.1.	Possible groups generated by an initial set $\mathcal{S} \subset G$. Black dots denote isolated elements of G , whereas ellipses represent connected components of a subgroup of G . Case (1) is when $\langle \mathcal{S} \rangle$ is dense in G and hence is universal. Cases (2) and (3) represent situations when the closure of $\langle \mathcal{S} \rangle$ is a compact, disconnected or connected respectively subgroup of G . In cases (1), (2) and (3) $\langle \mathcal{S} \rangle$ is an infinite set. Case (4) represents a situation when \mathcal{S} generates a finite subgroup of G .	65
4.2.	The proof of Theorem 4.2.	68
4.3.	The group $SU(d)$ with the exemplary open balls B_α centered at elements from $Z(SU(d))$.	73
4.4.	(a) Condition (4.14) for $SO(3)$. Black dots correspond to $n \arcsin \frac{1}{4}$ and dashed segments are determined by $ \sin \frac{\phi}{2} < \frac{1}{4}$, (b) Conditions (4.13) for $U \in SU(2)$. Black dots corresponds to $n \arcsin \frac{1}{4}$ and dashed segments are determined by $ \sin \frac{\phi}{2} < \frac{1}{4}$ or $ \sin \frac{\phi-\pi}{2} < \frac{1}{4}$.	78
4.5.	Lattice of points for the group $SU(3)$. The axes correspond to independent spectral angles $\frac{\phi_1}{2}, \frac{\phi_2}{2}$ of a matrix U . Dots represent angles $\frac{k\pi}{3}$, $k \in \mathbb{Z}_+$. The values of $\frac{\phi_1}{2}, \frac{\phi_2}{2}$ such, that $U \in Z(SU(3))$ are denoted by circles. It is easy to notice that the number of circles is equal to $\frac{1}{3}$ of the number of all dots.	79
4.6.	The smallest hypercubes contained in the balls B_1 for $SO(4)$ and $SU(3)$, respectively.	82
4.7.	The proof of Fact 4.7.	84
4.8.	Accuracy of approximation of $V(B_\epsilon)$ with the Taylor expansion up to order three. The horizontal axis represents ϵ and the vertical axis represents the numerical accuracy. The thick and dashed lines denote functions $V(B_\epsilon) - \frac{\epsilon}{\sqrt{2\pi}} - \frac{\epsilon^3}{48\pi\sqrt{2}} - f(\epsilon^3)$, where $f(\epsilon^3)$ is given by (4.41) and (4.42), respectively.	86
4.9.	Function $F(\epsilon) = V(B_\epsilon) - k_1\epsilon^3$ for $\epsilon \in [0, \frac{1}{\sqrt{2}}]$. The horizontal axis represents ϵ and the vertical axis represents $F(\epsilon)$. As $F(\epsilon)$ is larger than zero for $\epsilon \in [0, \frac{1}{\sqrt{2}}]$ we conclude that $k_1\epsilon^3$ is smaller than $V(B_\epsilon)$.	87
4.10.	An infinite order dicyclic group $\langle U(\phi_1, \vec{k}_1), U(\frac{\pi}{2}, \vec{k}_2) \rangle$. The ellipses represent the normalizer $\{U(\frac{\pi}{2}, \vec{k}_2)U(t, \vec{k}_1) : t \in \mathbb{R}\}$ and the one parameter group $\{U(t, \vec{k}_1) : t \in \mathbb{R}\}$, respectively.	89

List of Tables

4.1.	Comparing the values of N_G derived from numerical calculations with the upper bounds (4.6,4.5) for low dimensional groups.	81
4.2.	The number of exceptional triplets $\{\phi_1, \phi_2, \gamma\}$ terminating the universality algorithm for different l 's.	91
6.1.	Generators of finite subgroups of $SU(2)$: $\langle 2, 2, n \rangle$, $\langle 2, 3, 3 \rangle$, $\langle 2, 3, 4 \rangle$, $\langle 2, 3, 5 \rangle$	104
6.2.	Generators of $\langle 2, 3, 5 \rangle$	105

Bibliography

- [1] S. I. Adian, *The Burnside problem and identities in groups*, Translated from the Russian by John Lennox and James Wiegold, *Ergebnisse der Mathematik und ihrer Grenzgebiete [Results in Mathematics and Related Areas]*, 95. Springer-Verlag Berlin-New York, 1979
- [2] F. Albertini, D. D'Alessandro, *Notions of controllability for bilinear multilevel quantum systems*, IEEE Automat. Contr. 48, 1399-1403, 2003
- [3] S. Axler, *Linear algebra done right*, Undergraduate Texts in Mathematics, Springer, 2015
- [4] L. Babai, *Deciding finiteness of matrix groups in Las Vegas polynomial time*, Proceedings of the Third Annual ACM SIAM Symposium on Discrete Algorithms, ACM, New York, 33-40, 1992
- [5] L. Babai, R. Beals, D. N. Rockmore, *Deciding finiteness of matrix groups in deterministic polynomial time*, Proc. of International Symposium on Symbolic and Algebraic Computation. ISSAC-93. ACM Press, pp. 117-126, 1993
- [6] A. Barenco *et al.*, *Elementary gates for quantum computation*, Phys. Rev. A 52, 3457-3467, 1995
- [7] A. Bayad, I. N. Cangul, *The minimal polynomial of $2\cos(p/q)$ and Dickson polynomials*, Appl. Math. Comp. 218, 7014-7022, 2013
- [8] A. Bocharov *et al.*, Phys. Rev. A 88, 012313, 2013
- [9] J. Bourgain and A. Gamburd, *A spectral gap theorem in $SU(d)$* , J. Eur. Math. Soc. 014.5, 1455-1511, 2012
- [10] J. Bourgain and A. Gamburd, *On the spectral gap for finitely-generated subgroups of $SU(2)$* , Invent. Math., 171, Issue 1, 83-12, 2008
- [11] A. Böttcher, D. Wenzel, *The Frobenius norm and the commutator*, Linear Algebra Appl. 429, 1864-1885, 2008
- [12] A. Bouland, S. Aaronson, *Generation of Universal Linear Optics by Any Beam Splitter*, Phys. Rev. A 89, 062316, 2014
- [13] P. O. Boykin *et. al.*, *On Universal and Fault-Tolerant Quantum Computing*, arXiv:quant-ph/9906054, 1999
- [14] Y. Bromberg *et al.*, *Quantum and Classical Correlations in Waveguide Lattices*, Phys. Rev. Lett. 102, 253904, 2009
- [15] T. Bröcker, T. tom Dieck, *Representations of Compact Lie Groups*, Springer-Verlag, New York, MR 86i:22023, 1985

- [16] R. W. Brockett, *System Theory on Group Manifolds and Coset Spaces*, SIAM J. Control 10-2, 265-284, 1972
- [17] R. Brylinski, G. Chen, *Mathematics of Quantum Computation*, Boca Raton, FL: Chapman and Hall/CRC Press, 2002
- [18] M. Burrello, G. Mussardo, X. Wan, *Topological quantum gate construction by iterative pseudogroup hashing*, New J. Phys. 13, 025023, 2011
- [19] E. Cartan, *La théorie des groupes finis et continus et l'Analysis Situs*, Mémoires Sc. Math. XLII, 1-6, 1930
- [20] A. M. Childs *et al.*, *Characterization of universal two-qubit Hamiltonians*, Quantum Info. Comput. 11, 19-39, 2011
- [21] H. T. Croft, K. J. Falconer, R. K. Guy, *Unsolved Problems in Geometry*, New York: Springer-Verlag, p. 3, 1991
- [22] W. Curtis, I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*, Interscience Publishers, John Wiley and sons, 1962
- [23] H. Derksen, E. Jeandel, P. Koiran, *Quantum automata and algebraic groups*, Journal of Symbolic Computation 39, 357-371, 2005
- [24] A. S. Detinko, D. L. Flannery, *On deciding finiteness of matrix groups*, Journal of Symbolic Computation 44, 1037-1043, 2009
- [25] T. W. Cusick, *Dirichlet's diophantine approximation theorem*, Bull. Aust. Math. Soc. 16, 219-224, 1977
- [26] C. M. Dawson, M. A. Nielsen, *The Solovay-Kitaev algorithm*, Quant. Inf. Comp. 6, 81-95, 2006
- [27] D. Deutsch, A. Barenco, A. Ekert, *Universality in Quantum Computation*, Proc. Roy. Soc. Lond. A 425, 73-90, 1989
- [28] H. M. Edwards, *Galois theory*, Graduate Texts in Mathematics, Springer, 1998
- [29] W. M. Fairbairn, T. Fulton, W. H. Klink, *Finite and Disconnected Subgroups of $SU(3)$ and their Application to the Elementary-Particle Spectrum*, J. Math. Phys. 5, 1038-1051, 1964
- [30] W. Fulton, J. Harris, *Representation theory. A first course*, Springer Graduate Texts in Mathematics 129, 2004
- [31] M. Field, *Generating Sets for compact semisimple Lie Groups*, Proc. Amer. Math. Soc. 127, 3361-3365, 1999
- [32] M. H. Freedman, A. Kitaev, J. Lurie, *Diameters of Homogeneous Spaces*, Math. Res. Lett. 10, 11, 2003
- [33] D. Gilat, *Gauss's Lemma and the Irrationality of Roots Revisited*, Math. Mag. 85, 114-116, 2012
- [34] L. K. Grover, *A Fast Quantum Mechanical Algorithm for Database Search*, STOC'96 Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, 212-219, 1996

- [35] L. K. Grover, *A Framework for Fast Quantum Mechanical Algorithms*, STOC'98 Proceedings of the thirtieth annual ACM symposium on Theory of computing, 53-62, 1998
- [36] B. C. Hall, *Lie Groups, Lie Algebras and Representations: An Elementary Introduction*, Springer, GTM, 2nd ed., 2015
- [37] W. R. Hamilton, *Lectures on Quaternions*, Hodges and Smith, Dublin, 1853
- [38] G. H. Hardy, E. M. Wright, *An introduction to the Theory of Numbers*, Oxford at the Clarendon Press, 1960
- [39] A. W. Harrow, B. Recht, I. L. Chuang, *Efficient discrete approximations of quantum gates*, J. Math. Phys. 43:9, 4445-4451, 2002
- [40] F. Hausdorff, *Set Theory* 2nd ed. New York: Chelsea, 1962
- [41] R. A. Horn, C. R. Johnson, *Norms for Vectors and Matrices*, Ch. 5 in Matrix Analysis. Cambridge, England: Cambridge University Press, 1990
- [42] T. Ionescu, *On the generators of Semisimple Lie Algebras*,
- [43] E. Jeandel, *Universality in Quantum Computation*, In: Díaz J., Karhumäki J., Lepistö A., Sannella D. (eds) *Automata, Languages and Programming. ICALP 2004*, Lect. Notes Comp. Sc. 3142, Springer, 2004
- [44] V. Jurdjevic, H. Sussmann, *Control systems on Lie groups*, J. Differ. Equat. 12, 313-329, 1972
- [45] K. Karnas, A. Sawicki, *When is a product of finite order qubit gates of infinite order?*, J. Phys. A: Math. Theor. 51, 2018
- [46] H. Kesten, *Symmetric random walks on groups*, Thesis (Ph. D.), Cornell University, 1958
- [47] A. Yu. Kitaev, *Quantum computations: algorithms and error correction*, Russ. Math. Surv. 52, 1191-1249, 1997
- [48] V. Kliuchnikov *et al.*, *A framework for approximating qubit unitaries*, arXiv:1510.03888, 2015
- [49] V. Kliuchnikov *et al.*, *Practical approximation of single-qubit unitaries by single-qubit quantum Clifford and T circuits*, IEEE Transactions on Computers, vol.65, no. 1, 161-172, 2016
- [50] A. W. Knap, *Lie groups beyond an introduction*, Progress in Mathematics vol. 140, Birkhäuser, 1996
- [51] M. Kuranishi, *On everywhere dense imbedding of free groups in Lie groups*, Nagoya Mathematical J. 2, 63-71, 1951
- [52] J. M. Lee, *Introduction to Smooth manifolds*, Springer Graduate Texts in Mathematics, 218, 2000
- [53] F. Silva Leite, P. E. Crouch, *Controllability on Classical Lie Groups*, Math. Control Signals Systems 1:31-42, 1988
- [54] S. Lloyd, *Almost Any Quantum Logic Gate is Universal* Phys. Rev. Lett. 75, 2, 1995

- [55] A. Lubotzky, P. Sarnak, *Hecke operators and distributing points on the sphere I,II*, Commun. Pur. Appl. Math. 39(40), S1, S149-S186, 1986
- [56] W. Magnus, *II. Discontinuous groups and triangle tessellations. Noneuclidean tessellations and their groups*, Academic Press, 1974
- [57] J. R. Munkres, *Topology: A First Course*, 2nd ed. Upper Saddle River, NJ:Prentice-Hall, 2000
- [58] D. Montgomery, H. Samelson, *Transformation Groups of Spheres*, Ann. Math. 44, 454-470, 1943
- [59] J. von Neumann, *Über die analytischen Eigenschaften von Gruppen linearer Transformationen und ihrer Darstellungen*, Mathematische Zeitschrift 30, 3-42, 1929
- [60] M. Nielsen, I. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2000
- [61] M. Oszmaniec, J. A. Gutt, M. Kuś, *Classical simulation of fermionic linear optics augmented with noisy ancillas* Phys. Rev. A, vol. 90, p. 020302, 2014
- [62] M. Oszmaniec *et al.*, Random bosonic states for robust quantum metrology, Phys. Rev. X 6, 041044, 2016
- [63] O. Parzanchevski, P. Sarnak, *Super Golden-Gates for $PU(2)$* , Adv. Math. 327, 869-901, 2018
- [64] A. Politi *et al.*, *Silica-on-Silicon Waveguide Quantum Circuits*, Science 320, 646-649, 2008
- [65] J. Preskill, *Quantum Computing in NISQ era and beyond*, arXiv:1801.00862v2, 2018
- [66] C. Radin, L. Sadun, *On 2-generator subgroups of $SO(3)$* , Trans. Amer. Math. Soc. 351, 4469-4480, 1999
- [67] M.Reck *et al.*, *Experimental realization of any discrete unitary operator*, Phys. Rev. Lett. 73, 58-61, 1994
- [68] P. Sarnak, Letter to Scott Aaronson and Andy Pollington on the Solovay-Kitaev theorem, 2015
- [69] A. Sawicki, *Universality of beamsplitters*, Quantum Info. Comput. 16, 291-312, 2016
- [70] A. Sawicki, K. Karnas, *Criteria for universality of quantum gates*, Phys. Rev. A 95, 062303, 2017
- [71] A. Sawicki, K. Karnas, *Universality of Single-Qudit Gates*, Annales Henri Poincare 11, 3515-3552, 2017
- [72] E. Schechter, *Handbook of Analysis and Its Foundations*, Academic Press, 1997
- [73] S. G. Schirmer, H. Fu, A. I. Solomon, *Complete controllability of quantum systems*, Phys. Rev. A 63, 063410, 2001
- [74] P. w. Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, SIAM J. Comput. 26(5), 1484-1509, 1997

- [75] N. Schuch, J. Siewert, *Natural two-qubit gate for quantum computation using the XY interaction*, Phys. Rev. A 67, 032301, 2003
- [76] P. Selinger, *Efficient Clifford+T approximation of single-qubit operators*, Quant. Inf. Comp. 15, 159-180, 2015
- [77] W. Sierpiński, *Teoria liczb*, Monografie Matematyczne Tom XIX, Warszawa–Wrocław, 1950
- [78] M. Sipser, *Introduction to the Theory of Computation*, 3rd edition, Cengage Learning, 2013
- [79] J. Stillwell, *Naive Lie Theory*, Undergraduate Texts in Mathematics, Springer, 2008
- [80] L. Wei et. al., *From Random Matrix Theory to Coding Theory: Volume of a Metric Ball in Unitary Group*, arXiv:1506.07259
- [81] R. Zeier, T. Schulte-Herbrüggen, *Symmetry principles in quantum systems theory*, J. Math. Phys. 52, 113510, 2011
- [82] R. Zeier, Z. Zimborás, *On squares of representations of compact Lie algebras*, J. Math. Phys. 56, 081702, 2015
- [83] W. Waitkins, J. Zeitlin, *The Minimal Polynomial of $\cos(2\pi/n)$* , The American Mathematical Monthly 100, 5, 471-474, 1993
- [84] Z. Zimborás et al., *Symmetry criteria for quantum simulability of effective interactions*, Phys. Rev. A 92, 042309, 2015