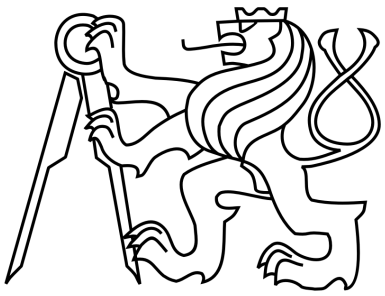
Czech Technical University in Prague
Faculty of Nuclear Sciences and Physical Engineering
Department of Physics



Twirling Operations in Quantum Algorithms

Bachelor's Thesis

Author: Jaroslav Kysela
Supervisor: Ing. Jaroslav Novotný, Ph.D.
Academic Year: 2012/2013

Před svázáním místo téhle stránky vložíte zadání práce s podpisem děkana (bude to jediný oboustranný list ve Vaší práci) !!!!

Prohlášení

Prohlašuji, že jsem svou bakalářskou práci vypracoval samostatně a použil jsem pouze literaturu uvedenou v přiloženém seznamu.

Nemám závažný důvod proti užití tohoto školního díla ve smyslu §60 Zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).

V Praze dne ....

Jaroslav Kysela

Acknowledgement

I would like to express my thanks to my supervisor Ing. Jaroslav Novotný, Ph.D. for his patience, advice and correction of my numerous mistakes and misunderstandings.

Jaroslav Kysela

Název práce:	**Twirlingové operace v kvantových algoritmech**
Autor:	Jaroslav Kysela
Obor:	Matematické inženýrství
Druh práce:	Bakalářská práce
Vedoucí práce:	Ing. Jaroslav Novotný, Ph.D. Katedra fyziky, Fakulta jaderná a fyzikálně inženýrská, České vysoké učení technické v Praze
Konzultant:	prof. Ing. Igor Jex, DrSc. Katedra fyziky, Fakulta jaderná a fyzikálně inženýrská, České vysoké učení technické v Praze

Abstrakt: Kvantové operace představují obecný nástroj pro popis dynamiky otevřených systémů. S jejich pomocí lze zkoumat jevy jako spontánní emise, amplitudové tlumení či různé typy dekoherence. K těmto procesům dochází při nevyhnutelném kontaktu studovaného kvantového systému se svým okolím. Výsledkem je obvykle degradace některých kvantových vlastností systému. Příkladem může být ztráta kvantového provázání, které nachází uplatnění v řadě kvantových algoritmů a informačních protokolů. Na druhé straně otevřené dynamiky rozšiřují množinu fyzikálně realizovatelných transformací kvantových stavů. Lze je proto úspěšně využít pro efektivnější řešení úloh, než by bylo možné v rámci uzavřeného vývoje. Práce se soustřeďuje na twirlingové operace randomizující stavy podél vybrané grupy. Těchto operací se užívá v protokolech pro destilaci neboli purifikaci provázání. Problémem je však jejich efektivní realizace. Hlavním cílem této práce je shrnutí dosavadních implementací twirlingu a analýza nové iterativní metody využívající náhodné unitární operace.

Klíčová slova: twirling, kvantové provázání, purifikace provázání, kvantové operace, asymptotická dynamika kvantových operací.

Title: **Twirling Operations in Quantum Algorithms**

Author: Jaroslav Kysela

Abstract: Quantum operations provide a general tool for a description of an open-system dynamics. They enable us to study quantum phenomena such as spontaneous emission, amplitude damping or various types of decoherence. These processes emerge from an inevitable contact of the quantum system with its environment. It usually leads to degradation of particular quantum system properties. As an example, it may cause quantum entanglement to diminish or vanish completely. On the other hand, open quantum system evolutions allow specific state changes which are unrealizable via closed system dynamics. As such they can be utilized for more efficient solutions of tasks than can be accomplished by closed system evolutions. The thesis focuses on twirling operations randomizing states along a given group. These are harnessed in entanglement purification or distillation protocols. However, problems arise with their efficient realization. The main goal of this thesis is to summarize present twirling implementations and analyze a new iterative method exploiting random unitary operations.

Key words: twirling, quantum entanglement, entanglement purification, quantum operations, asymptotic dynamics of quantum operations.

Contents

List of Symbols

A^*	complex conjugate of matrix A
A^T	transpose of matrix A
$A^\dagger$	Hermitian conjugate of matrix A or operator A
$\mathscr{H}$	Hilbert state space
$\mathscr{H}_{\text{env}}$	state space of an environment
$\mathcal{B}(\mathscr{H})$	Hilbert space of operators acting on Hilbert space $\mathscr{H}$ with $\langle A\|B\rangle = \text{tr}(A^\dagger B)$
ρ	density matrix
$\otimes$	tensor product
$\hat{n}$	set equal to $\{1, 2, \ldots, n\}$ for $n \in \mathbb{N}$
$\sigma(A)$	spectrum of operator A
$\sigma_{\|1\|}(A)$	set of all eigenvalues λ of operator A for which $\|\lambda\| = 1$
$\text{Ker}(A)$	kernel of operator A
$\text{Ran}(A)$	range of operator A
$\text{Attr}(A)$	attractor space of operator A
Φ	random unitary operation
$\mathbf{\Phi}$	matrix representation of random unitary operation

Chapter 1

Introduction

The development of quantum theory in the second half of the twentieth century enabled researchers to think of quantum phenomena in the scope of computing, information processing and cryptography. Such an approach promises the construction of a quantum computer. The device which is able to provide calculations in a way exceeding in efficiency any present classical machine.

Many algorithms have been developed exploiting features of quantum particles such as quantum parallelism or quantum entanglement. Quantum algorithms allow efficient factorization of extremely large numbers, fast database searching or quantum Fourier transformation [1].

In past two decades interest has been raised in quantum entanglement and its applications, especially in the field of quantum information processing and quantum computation. However, for reliable functionality perfectly entangled pairs of particles are needed. In practice, it is hard to handle and store such perfectly entangled pairs. An inevitable interaction with their environment causes their entanglement to diminish. Nonetheless, several techniques for entanglement enhancement exist. Entanglement purification protocols are applied to accomplish this task.

Purification protocols usually make use of many identical partially entangled pairs of particles. These are processed to obtain lesser number of more entangled pairs. As a crucial part of these protocols so-called twirling operations are used. Twirling transforms a general quantum state of particles into one special kind of states which is suitable for subsequent manipulations. There are multiple ways how to implement twirling operations. In this thesis we focus on some of them with the intention to elucidate their design and basic ideas.

This thesis is structured as follows: In the first chapter, we give a brief summary of quantum mechanics fundamentals. Then, we introduce basic terms and objects used for quantum computation description, especially those utilized in this thesis. In the second part, we list several examples of quantum algorithms and explain a basic purification protocol scheme. The third chap-

ter summarizes some important properties of quantum operations including rigorous definition of twirling transformations. The fourth chapter examines the twirling implementations. Moreover, it contains our detailed investigation of the two-qubit twirling realized by the iterative method. We give a complete answer under which conditions this method works and we perform a numerical analysis of its convergence rate. In the final chapter we summarize our results.

1.1 Postulates of Quantum Mechanics

At the fundamental level of quantum mechanics there are four postulates stated to be true about physical systems. They are based on empirical results and their validity has not been experimentally disproved yet [1]

Postulate 1: Associated with any isolated physical system is a Hilbert space $\mathscr{H}$ known as the *state space*. The state of the system is completely described by its *density operator*, i. e. a positive operator acting on $\mathscr{H}$ with a unit trace. If a quantum system is in the state ρ_i (equivalently, if its state is described by density operator ρ_i) with probability p_i, then the density operator for the system is $\rho = \sum_i p_i \rho_i$.

Postulate 2: The evolution of a closed quantum system is described by a unitary transformation. That is, the state ρ of the system at time t_1 is related to the state ρ' of the system at time t_2 by a unitary operator U which depends on the times t_1 and t_2 only, in a way

$$\rho' = U \rho U^\dagger.$$

Postulate 3: Quantum measurements are described by a collection $\{M_m\}$ of *measurement operators*, which are operators acting on the state space of the system being measured. Values of the index m correspond to the measurement outcomes that may occur in the experiment. If the state of the quantum system is ρ immediately before the measurement then the probability that result m occurs is given by

$$p(m) = \mathrm{tr}(M_m^\dagger M_m \rho),$$

and the state of the system after the measurement is

$$\frac{M_m \rho \, M_m^\dagger}{\mathrm{tr}(M_m^\dagger M_m \rho)}.$$

The measurement operators satisfy the *completeness equation*,

$$\sum_m M_m^\dagger M_m = I.$$

Postulate 4: The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. That is, let $\mathscr{H}_i$ be the state space corresponding to the component physical system, $i \in \hat{n}$, then the state space of the composite physical system is of the form $\mathscr{H} = \bigotimes_{i \in \hat{n}} \mathscr{H}_i$.

The first postulate sets the mathematical frame for a physical system description. The second postulate determines how to handle mathematically the evolution of closed quantum systems. However, it is not a sufficient framework neither for real life applications nor for situations where the role of the environment is not negligible. For instance, when entangled particles are transmitted through a noisy channel. In that case one can encompass the observed system and its environment into one larger system and try to describe it as a closed one. An alternative approach is to describe an evolution of the system via quantum operations (see chapter 3).

The third postulate states how a measurement procedure is performed in quantum mechanics. It involves the fact that a measurement, in general, disturbs the original state of a system and leave the system in a given collapsed state with a given probability. The fourth postulate deals with a situation where there are many quantum systems which one wants to study as a one system.

From the very beginning we restrict ourselves to finite dimensional Hilbert spaces. A set of all linear operators acting on $\mathscr{H}$ we denote by $\mathcal{B}(\mathscr{H})$. The $\mathcal{B}(\mathscr{H})$ forms a Hilbert space equipped with the Hilbert-Schmidt inner product $\langle A|B\rangle = \mathrm{tr}(A^\dagger B)$ for $A, B \in \mathcal{B}(\mathscr{H})$.

1.2 Bra-ket Formalism

In quantum mechanics it is convenient to use the so-called *Dirac notation* or *bra-ket notation* for vectors and their corresponding covectors. Let $\mathscr{H}$ be a Hilbert space, then $|\psi\rangle \in \mathscr{H}$ denotes a vector in this space—so-called *ket* vector—and $\langle\psi| \in \mathscr{H}^\dagger$ its associated linear functional—so-called *bra* vector. The following relation holds

$$|\psi\rangle^\dagger = \langle\psi|.$$

The action of an operator A on a vector $|\psi\rangle$ is written as $A|\psi\rangle$. An inner product of $|\psi\rangle$ and $|\varphi\rangle$ reads $\langle\psi|\varphi\rangle$ (or $\langle\psi|A|\varphi\rangle$ for vectors $|\psi\rangle$ and $A|\varphi\rangle$). The names of the ket and the bra vectors were chosen in such a way that expression $\langle\psi|\varphi\rangle$ could be pronounced as "bracket".

1.3 Density Operators

In the first postulate in section 1.1 we introduced density operators. Providing a state space $\mathscr{H}$ is finite-dimensional one can represent density operators by square matrices, so-called *density matrices*.

If there exists a vector $|\psi\rangle \in \mathscr{H}$ such that a density operator ρ is the projector onto one-dimensional vector subspace spanned by $|\psi\rangle$, we call ρ a *pure state*. In the braket notation we have $\rho = |\psi\rangle\langle\psi|$. Otherwise, ρ is a

mixed state. The *maximally mixed state* is the state whose density operator is proportional to the identity matrix.

Consider a quantum system to be in one of pure states $\{|\psi_i\rangle\}_{i=1}^m$ with corresponding probabilities $\{p_i\}_{i=1}^m$. A set $\{p_i\,, |\psi_i\rangle\}_{i=1}^m$ is called the *ensemble of pure states* and the associated density operator is defined as

$$\rho \equiv \sum_{i=1}^{m} p_i |\psi_i\rangle\langle\psi_i|.$$

There is also a simple criterion how to distinguish pure and mixed states. Let ρ be a density operator. Then $\mathrm{tr}(\rho^2) \leq 1$ with equality iff ρ is a pure state.

Assume $\mathcal{B}(\mathscr{H}_A)$ and $\mathcal{B}(\mathscr{H}_B)$ be spaces of operators on state spaces $\mathscr{H}_A$ and $\mathscr{H}_B$, respectively. Moreover, let S_A be a subset of $\mathcal{B}(\mathscr{H}_A)$ which is constituted by operators of the form $|a_1\rangle\langle a_2|$, where $|a_1\rangle, |a_2\rangle \in \mathscr{H}_A$. Similarly for S_B. One can define a map $\mathrm{tr}_B : S_A \otimes S_B \to S_A$ in the following way

$$\mathrm{tr}_B(|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|) \equiv |a_1\rangle\langle a_2| \,\mathrm{tr}(|b_1\rangle\langle b_2|).$$

By the requirement that tr_B is a linear map we can extent its domain to the entire $\mathcal{B}(\mathscr{H}_A) \otimes \mathcal{B}(\mathscr{H}_B)$. Such a mapping is called the *partial trace over the system* $\mathscr{H}_B$. Consider an arbitrary state ρ^{AB} of a composite state space $\mathscr{H}_A \otimes \mathscr{H}_B$. We describe the part corresponding to the system A alone in the way

$$\rho^A \equiv \mathrm{tr}_B(\rho^{AB}),$$

where ρ^A is called the *reduced density operator*.

1.4 Qubits

We denote a quantum system with a two-dimensional state space as a *qubit*. Qubit is taken to be a quantum analogue of a classical bit, therefore its name—a qu(antum) bit. Contrary to a classical bit with two possible values—zero and one—qubit $|\psi\rangle$ can exist not only in these two states marked $|0\rangle$ and $|1\rangle$, but also in their superposition. That is, the general pure state of a qubit can be expressed as

$$\alpha|0\rangle + \beta|1\rangle,$$

where $|0\rangle$ and $|1\rangle$ forms an orthonormal basis of the state space and α, $\beta \in \mathbb{C}$ (so-called *amplitudes*) satisfy the relation $|\alpha|^2 + |\beta|^2 = 1$. As an extension of the qubit to higher dimensions a term *qudit* is used for quantum systems associated with a d-dimensional state space.

1.5 Quantum Entanglement

In general, compared to classical world objects the quantum particles exhibit very strong measurement-outcome correlations. Such a property is referred to as *quantum entanglement*. States which are not entangled are called *separable*. More precisely, a bipartite mixed state $\rho \in \mathscr{H}_A \otimes \mathscr{H}_B$ is separable iff it can be expressed in a form

$$\rho = \sum_{i=1}^{k} p_i \, \rho_i \otimes \tilde{\rho}_i$$

for some $k \in \mathbb{N}$, where ρ_i and $\tilde{\rho}_i$ are states on $\mathscr{H}_A$ and $\mathscr{H}_B$, respectively. A density operator acting on $\mathscr{H}_A \otimes \mathscr{H}_B$ is defined to be *maximally entangled state* whenever it is a pure state and both of its reduced density operators are maximally mixed [2].

Whereas pure state entanglement quantification is an easy task nowadays (for more information see [3]) entanglement of mixed states is still rather unresolved problem, see e. g. [3] or [4].

1.6 The Bell Basis

The Bell basis is a special orthonormal basis of the state space associated with two spin-$\frac{1}{2}$ particles. It consists of four pure maximally entangled states

$$|\,\Psi^-\rangle = \frac{|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle}{\sqrt{2}}, \quad |\,\Psi^+\rangle = \frac{|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle}{\sqrt{2}},$$
$$|\,\Phi^-\rangle = \frac{|\uparrow\uparrow\rangle - |\downarrow\downarrow\rangle}{\sqrt{2}}, \quad |\,\Phi^+\rangle = \frac{|\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle}{\sqrt{2}}.$$

The first state is also known as the *spin singlet* for historical reasons [1] and is used extensively in various quantum computation schemes.

1.7 Werner States and Isotropic States

Consider a set of mixed states representing two subsystems with identical dimension. There is a subset of those which do not change when one applies the same unitary transformation on both subsystems. Specifically, for any unitary U holds

$$\rho = U \otimes U \, \rho \, U^\dagger \otimes U^\dagger.$$

These states are called the *Werner states* (proposed in [5]). Werner showed that they must be of the form [4]

$$\rho_W(d) = \frac{1}{d^2 - \beta d}(I + \beta V),$$

where $-1 \leq \beta \leq 1$, I denotes the identity operator, d denotes the dimensionality of the subsystems and V stands for the flip operator acting on $d \otimes d$ systems in the way: $V(\psi \otimes \phi) = \phi \otimes \psi$.

For two-qubit case, i. e. $d = 2$, the Werner state is of the form

$$W_F = F|\Psi^-\rangle\langle\Psi^-| + \frac{1-F}{3}(|\Psi^+\rangle\langle\Psi^+| + |\Phi^+\rangle\langle\Phi^+| + |\Phi^-\rangle\langle\Phi^-|), \qquad (1.1)$$

where $F \in (0,1)$ is called a *singlet fraction* for given density matrix ρ. It is defined by formula $F = \langle\Psi^-|\rho|\Psi^-\rangle$, where $|\Psi^-\rangle$ is a singlet state, see section 1.6. Werner states play an important role in quantum purification protocols (see later). A mixture of the three remaining Bell states in (1.1) is sometimes called the *triplet*.

Similarly to Werner states for bipartite systems one can define states invariant under application of $U \otimes U^*$, i. e. $\rho = U \otimes U^* \, \rho \, U \otimes U^*$. Such states must be of the form [4]

$$\rho(F,d) = \frac{d^2}{d^2-1}\left(\left(1-F\right)\frac{I}{d^2} + \left(F - \frac{1}{d^2}\right)P_+^d\right), \quad 0 \leq F \leq 1,$$

where d again denotes the dimensionality of subsystems, P_+^d is a projector corresponding to the maximally entangled state $\psi_+^d = \frac{1}{\sqrt{d}}\sum_{i=1}^{d}|i\rangle \otimes |i\rangle$ and F is in this case defined as $F = \langle\psi_+^d|\rho|\psi_+^d\rangle$ [4]. These states are called *isotropic states*.

Chapter 2

Quantum Computation and Communication

Even though nobody has constructed a real quantum computer yet, mostly because of very untrivial problems with the decoherence, manipulation and storage of quantum particles, several classes of algorithms have been developed. On one hand, quantum algorithms have the potential to break at least some of the most popular modern encryption systems. On the other hand, quantum cryptography provides means preventing any possible eavesdropping.

2.1 Quantum Algorithms

What makes the most significant difference between classical algorithms and their quantum counterparts is utilization of quantum particle characteristics. Quantum parallelism or quantum entanglement are used extensively for example. Several algorithms have been developed so far which can be implemented in a much more efficient way than those without employment of quantum effects.

Here we briefly mention two well-known instances of quantum algorithms. We do not want to go into details, our intention is to show the structure and explain the key ingredients of this kind of algorithms [3, 4].

2.1.1 Quantum Dense Coding

Consider two parties, say Alice and Bob. Alice aims to send some information to Bob. Here we discuss the situation where qubits are transmitted, generalization to higher dimensions is straightforward.

Quantum dense coding enables Alice to transmit two classical bits by sending only one qubit. The principal idea of this algorithm is such that Alice and Bob share a maximally entangled pair of particles. Quantum entanglement

allows the transferred qubit to carry effectively two bits of information. The procedure is as follows:

1. Before the information exchange is initiated a maximally entangled pair of particles is distributed between Alice, a sender, and Bob, a receiver. Each of them obtains one particle.

2. Alice then encodes a "message" by applying one of four particular transformations on her particle and send this particle to Bob.

3. Bob receives Alice's particle and performs a combined measurement of his and her particles. The important thing here is that the measurement is performed in the Bell basis. It leads to four unambiguous outcomes, hence by sending one particle two classical bits are transmitted.

Instead of a pair of qubits and the Bell basis one can make use of multidimensional states and bases. What is exploited in this algorithm is a remarkable property of maximally entangled (ME) states that any maximally entangled state can be transformed into any other ME state by local actions only.

2.1.2 Quantum Teleportation

In this protocol, we assume the situation with qubits being teleported. Consider two distant parties, Alice and Bob, who decided to transmit an unknown quantum state. One possibility is to achieve this goal in a classical way, i. e. by sending classical bits only.

Alice, a sender, measures her particle first and then sends an output to Bob. This approach faces some problems. Generally speaking, due to measurement Alice destroys a part of information stored in her particle state. Even if she had virtually infinitely many identical copies of the state she would have to send infinitely many bits to fully describe the state.

However, there exists a procedure which manages these obstacles, the so-called *quantum teleportation*. It exploits additional maximally entangled pairs of particles which do not carry the information. Suppose Alice wants to transmit one quantum state $|\psi\rangle$ to Bob. The transmission involves the following steps:

1. First, one particle of the maximally entangled pair is sent to Alice, the other is sent to Bob. At this moment no information is transmitted yet.

2. Alice then measures both her particles—one in the state $|\psi\rangle$ which she would like to transmit and one of the entangled pair. She performs the measurement in the Bell basis obtaining one of four possible results. Then, she sends her result to Bob through a classical information channel.

3. Bob receives the result of Alice's measurement. According to the obtained value he chooses one of four correcting operations. By application of this operation he recovers the original state $|\psi\rangle$.

Let us summarize basic properties of quantum teleportation protocols. Alice's original state $|\psi\rangle$ is destroyed by the measurement while recovered by Bob on the other side of a communication channel. Bob is unable to reconstruct the state $|\psi\rangle$ until Alice sends him a classical information about the state. It is worth emphasizing that neither Alice nor Bob knows in any stage of the process what the transmitted state looks like.

2.2 Entanglement Purification

Quantum entanglement forms a crucial part of both protocols described above. Alice and Bob make use of maximally entangled singlets shared between them for reliable transfer of the information. Thus, any physical implementation of both protocols faces an interesting challenge. A maximally entangled pair of particles has to be sent to different parties through an environment first. In practice, it is not possible to manage this without reduction of entanglement. Therefore, after the transmission Alice and Bob share partially entangled pairs. At this stage the so-called *quantum purification* (or *quantum distillation*) is applied where given number of entangled pairs of particles turns into a lesser number of more entangled singlets.

The *entanglement purification protocols* are employed to implement this procedure. It should be stressed that purification is required to be practicable by both parties independently. That is, local actions and classical communication (LOCC) are permitted only and no extra shared entanglement can be harnessed. LOCC refers to the fact that parties cannot perform collective measurements on their particles and the only thing they can exchange are classical bits of information.

We restrict ourselves to two-qubit states and describe the entanglement purification protocol introduced in [6]. Here, we state it in the form presented in [4]. At the beginning, both parties share a given (rather large) number of partially entangled pairs. The central idea of the protocol is such that Alice and Bob subsequently sacrifice some of their pairs to recover asymptotically perfect entanglement in the remainder of their particles.

The demonstrated protocol works for partially entangled states with $F > 1/2$ (see section 1.7). Let Alice and Bob share a large number n of qubit pairs, each in the same partially entangled state ρ with $F > 1/2$. Alice and Bob would like to acquire a (smaller) number of pairs with a higher singlet fraction F. It can be performed by iterating these steps:

1. Alice and Bob take two pairs and apply a random unitary transformation of the form $U \otimes U^*$ (i. e. P_{iso} twirling, see later) to each of them. In

particular, Alice chooses at random a transformation U first, applies it to her particle and then says Bob which transformation she has used. Bob then applies U^* to his particle. Similarly for the second pair. The net effect is such that two copies of ρ are transformed into two copies of isotropic state ρ_F with F unchanged, i. e.

$$\rho \otimes \rho \to \rho_F \otimes \rho_F. \tag{2.1}$$

2. Both parties apply XOR operation on their parts of pairs. The XOR operation is given by $(a, b \in \{0, 1\})$

$$U_{\mathrm{XOR}}|a\rangle|b\rangle = |a\rangle|(a+b) \bmod 2\rangle,$$

where the first qubit is called the *source* and the second one the *target*. In other words, Alice possesses two particles at the time (there are two pairs of particles), each of which is entangled with its counterpart in Bob's possession. Alice applies XOR on her two particles. Bob then chooses as a source that particle whose counterpart is the source in Alice's case and applies XOR on his particles as well.

3. Alice and Bob measure their target particles separately in the basis $\{|0\rangle, |1\rangle\}$. If their results agree, the source pair has a greater singlet fraction. This pair is kept and used in the following iteration. If their results do not match with each other, the source pair is discarded.

The entire procedure can be slightly modified—instead of transformation $U \otimes U^*$ in the item 1 one can exploits transformation of the form $U \otimes U$. The only difference is such that (2.1) with isotropic states ρ_F turns into $\rho \otimes \rho \to W_F \otimes W_F$, where W_F is a Werner state (see section 1.7).

In the practical realization of this protocol, complications may arise with the XOR operation and the twirling described in the item 1. This thesis is devoted to implementations of the second operation.

Chapter 3

Quantum Operations

Quantum mechanical postulates stated in section 1.1 constitute a significant tool for study of different phenomena occurring in nature. They can be successfully applied in many physical situations. However, their scope is restricted to closed system dynamics only. Provided we want to deal with real-life processes this framework is not sufficient. In practice, every physical system interacts with its environment. The study of general state changes driven by open system dynamics is therefore an important issue.

In contrast to closed system evolution, the concept of pure states is not in general satisfying for description of open systems. Interactions between the system and its environment cause the system state to evolve in a non-unitary manner and the final state is no longer pure. Density matrices turn out to be ideal objects for description of quantum states subjected to open dynamics. They express our incomplete knowledge about the state of the system.

Quantum operations serve as a powerful instrument enabling us to cope with open system evolutions. In a mathematical sense, they are endomorphisms on space of operators. This chapter focuses on different representations of quantum operations and shows some of their properties.

3.1 Quantum Operation Formalism

Before we proceed, recall notation used in the thesis. As stated in section 1.1, we deal with finite-dimensional state spaces $\mathscr{H}$ only. A symbol $\mathcal{B}(\mathscr{H})$ stands for a Hilbert space of linear operators acting on $\mathscr{H}$ with a Hilbert-Schmidt inner product $\langle A|B\rangle = \mathrm{tr}(A^\dagger B)$, $A, B \in \mathcal{B}(\mathscr{H})$.

First, let us present three approaches one can use for quantum operation description. They are mutually equivalent. Nevertheless, it is convenient to introduce them all as they reveal various quantum operation properties. For more information and theorems which prove equivalence of different approaches see [1].

System coupled to its environment: This approach reflects our intuition that any open system $\mathscr{H}$ can be enclosed by addition of another quantum system $\mathscr{H}_{\text{env}}$. In different contexts, this additional system is called either an *environment* or an *ancilla* (an *ancillary system*). The joint system $\mathscr{H} \otimes \mathscr{H}_{\text{env}}$ is closed already, hence its evolution can be described by a unitary operation U. Any initial state of the joint system is assumed to be in a tensor product form $\rho \otimes \rho_{\text{env}}$. This apparently restricts the set of all possible initial states, but it is usually sufficient in most physically reasonable situations. The quantum operation E acting on the studied system is then defined as

$$E(\rho) = \text{tr}_{\text{env}} \left(U \left(\rho \otimes \rho_{\text{env}} \right) U^{\dagger} \right). \tag{3.1}$$

Axiomatic approach: One can define quantum operations via a set of natural requirements—axioms. This approach is able to describe a vast range of different quantum phenomena due to its abstract form. Let $\mathscr{H}_1$, $\mathscr{H}_2$ be Hilbert spaces and $\mathcal{D}(\mathscr{H}_1)$, $\mathcal{D}(\mathscr{H}_2)$ their associated sets of density operators. A quantum operation E is defined as a map from $\mathcal{D}(\mathscr{H}_1)$ to $\mathcal{D}(\mathscr{H}_2)$ which satisfies the following three axioms:

1. Given the initial state $\rho \in \mathcal{D}(\mathscr{H}_1)$, the probability that the process represented by E occurs is equal to $\text{tr}(E(\rho))$. Thus, for any state ρ:

$$0 \leq \text{tr}(E(\rho)) \leq 1.$$

2. E is a *convex-linear map* on $\mathcal{D}(\mathscr{H}_1)$, i. e. for $\{\rho_i\}_{i=1}^m \in \mathcal{D}(\mathscr{H}_1)$ and probabilities $\{p_i\}_{i=1}^m$ holds

$$E\left(\sum_{i=1}^{m} p_i \, \rho_i \right) = \sum_{i=1}^{m} p_i \, E(\rho_i).$$

3. E is a completely positive map. Linear map is said to be *positive*, if it maps positive operators to positive operators. *Completely positive linear map* E is that satisfying this condition: $(E \otimes I_n)$ is a positive operator for every $n \in \mathbb{N}$, where I_n is the identity mapping acting on an extra n-dimensional Hilbert space.

Operator-sum representation: This approach allows one to describe system dynamics without being interested directly in properties of the environment. To be more specific, quantum operation can be expressed in the form

$$E(\rho) = \sum_{i=1}^{m} E_i \rho E_i^{\dagger}, \tag{3.2}$$

where ρ is the initial state and operators $\{E_i\}_{i=1}^m$ are known as *Kraus operators*. These do not have to be unitary, nevertheless they are required to satisfy

$$\sum_{i=1}^{m} E_i^\dagger E_i \leq I. \tag{3.3}$$

Quantum operations for which the above inequality holds are called *trace-non-increasing*. Those operations for which (3.3) turns into equality are called *trace-preserving* or *(quantum) channels*.

Notice that a unitary evolution of a closed system is equivalent to $m = 1$ and equality holds in (3.3) for this case.

Let us derive (3.2) from (3.1) [1]. Without loss of generality, assume $\{|e_i\rangle\}_{i=1}^m$ be an orthonormal basis for a state space $\mathscr{H}_{\text{env}}$ of the environment and $\rho_{\text{env}} = |e_0\rangle\langle e_0|$ be an initial state of $\mathscr{H}_{\text{env}}$. Then, in accordance with (3.1)

$$\begin{aligned} E(\rho) &= \text{tr}_{\text{env}}\left(U\left(\rho \otimes \rho_{\text{env}}\right) U^\dagger\right) \\ &= \sum_{i=1}^{m} \langle e_i|U(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger|e_i\rangle = \sum_{i=1}^{m} E_i \rho E_i^\dagger, \end{aligned}$$

where $E_i \equiv \langle e_i|U|e_0\rangle$, $i \in \hat{n}$, are operators acting on the state space of the studied system.

Environment effects are incorporated in Kraus operators and researcher does not have to be interested in the environment itself any more. This makes operator-sum representation very useful not only for calculations but also for theoretical analysis.

Quantum operations constitute a convex subset in the vector space of so-called *superoperators*. These are linear endomorphisms on the space of operators $\mathcal{B}(\mathscr{H})$. Hence, it is natural to think of them in terms of matrices. Assume a d-dimensional Hilbert space $\mathscr{H}_d$ with an orthonormal basis $\{|i\rangle\}_{i=1}^d$. A basis of $\mathcal{B}(\mathscr{H})$ can be directly chosen as $\{|i\rangle\langle j|\}_{i,j=1}^d$.

Let A be an operator acting on $\mathscr{H}_d$ and $\{A_{ij}\}_{i,j=1}^d$ be its matrix elements corresponding to the basis above. One can interpret $(A)_{ij}$, i. e. a $d \times d$-matrix, as a vector $\mathbf{A}$ in a space $\mathscr{H}_{d^2}$ with squared dimension

$$\mathbf{A} \equiv (A_{11}, A_{12}, \ldots, A_{1d}, A_{21}, A_{22}, \ldots, A_{2d}, \ldots, A_{d1}, A_{d2}, \ldots, A_{dd}). \tag{3.4}$$

A superoperator can then be represented as a $d^2 \times d^2$-matrix acting on $\mathscr{H}_{d^2}$. In this approach, we can rewrite a product of three matrices in the form

$$ABC = \boldsymbol{M}\mathbf{B}, \text{ where } \boldsymbol{M} = A \otimes C^T.$$

The quantum operation (3.2) can thence be expressed as the following matrix

$$\boldsymbol{E} = \sum_{i=1}^{m} E_i \otimes E_i^*, \tag{3.5}$$

where $\{E_i\}_{i=1}^m$ are matrices of Kraus operators defining E (in the above basis) and an asterisk denotes complex conjugation. Hereafter, for the matrix representation of superoperators we will use symbols in bold.

Let us introduce two important classes of quantum operations. Quantum operations satisfying relation $E(I) = I$, i. e. leaving the maximally mixed state undisturbed, are called *unital*. *Random unitary operations* are completely positive trace-preserving maps which can be expressed in a form of a convex decomposition

$$\Phi(\rho) = \sum_{i=1}^{m} p_i \, U_i \rho \, U_i^\dagger, \tag{3.6}$$

where $\{U_i\}_{i=1}^m$ is a set of unitary operators and $\{p_i\}_{i=1}^m$ satisfies $\sum_{i=1}^m p_i = 1$ and $p_i > 0$ for $i \in \hat{m}$. This can be viewed in a way that unitary operations U_i are applied to the state ρ according to the probability distribution $\{p_i\}_{i=1}^m$. In this case Kraus operators take the form $E_i = \sqrt{p_i} U_i$. In the matrix representation (3.6) turns into (see (3.5))

$$\boldsymbol{\Phi} = \sum_{i=1}^{m} p_i \, U_i \otimes U_i^*. \tag{3.7}$$

In the following, we focus on random unitary operations (RUOs) only. We consider a quantum system evolution generated by successive applications of RUO Φ. We are interested in an asymptotic dynamics of this evolution. That is, our goal is to examine the situation

$$\rho(n) = \Phi^n(\rho(0)), \tag{3.8}$$

where $\rho(0)$ stands for an initial state and n tends to infinity. To this end, we need to understand spectral properties of random unitary operations. It will be found very useful in the discussion about twirling operations.

3.2 Spectral Properties of Random Unitary Operations

Spectral properties of RUOs and the asymptotic regime of dynamics (3.8) were studied in [7]. In this part we briefly summarize obtained results. As already mentioned they will be utilized in the next chapter concerning twirling implementations.

Let Φ be a random unitary operation acting on linear operators, i. e.

$$\Phi(A) = \sum_{i=1}^{m} p_i \, U_i A \, U_i^\dagger, \tag{3.9}$$

where $A \in \mathcal{B}(\mathscr{H})$. One can check that RUO Φ is not a normal map hence it cannot be diagonalized, in general. Nonetheless, various important properties can be inferred for this type of operations.

Indeed, consider a Jordan canonical form of (3.7) (see Appendix B). Let $\{J_j\}_{j=1}^{p}$, $p \in \mathbb{N}$, be its Jordan blocks associated to eigenvalues λ_j and $\{Y_{j,k}\}_{j,k}$ be corresponding generalized eigenvectors. Each eigenvalue of a random unitary operation (3.9) has modulus lesser or equal to one. Assume an eigenvalue λ_j satisfying $|\lambda_j| < 1$. It turns out that all Jordan blocks corresponding to such an eigenvalue vanish completely in the asymptotic limit, i. e. $\lim_{n\to\infty}(J_j)^n = 0$.

On the contrary, any Jordan block corresponding to an eigenvalue λ_j with unit modulus is one-dimensional [7]. Equivalently, all generalized eigenvectors associated to such an eigenvalue are eigenvectors. Therefore, the matrix representation of the map Φ^n in the asymptotic limit ($n \gg 1$) takes the diagonal form $\mathrm{Diag}(\lambda_1^n, \lambda_2^n, \ldots, \lambda_s^n, 0, \ldots, 0)$ for some $s \leq p$.

All these findings lead us to the conclusion that the asymptotic dynamics generated by successive applications of (3.9) is confined to a particular subspace. This subspace is spanned by all eigenvectors corresponding to eigenvalues which modulus equals one. Henceforth, we call such space the *attractor space*. For a given random unitary operation Φ it is defined as

$$\mathrm{Attr}\,(\Phi) = \bigoplus_{\lambda \in \sigma_{|1|}} \mathrm{Ker}(\Phi - \lambda I), \tag{3.10}$$

where $\sigma_{|1|}$ is the *asymptotic* (or *attractor*) *spectrum* of RUO Φ constituted by all eigenvalues of Φ satisfying $|\lambda| = 1$.

It was also shown [7] that eigenvectors corresponding to different eigenvalues $\lambda \in \sigma_{|1|}$ are mutually orthogonal. Moreover, all these eigenvectors are orthogonal to any generalized eigenvector associated to eigenvalue λ_j with modulus lesser than one. Thus, the part of RUO (3.9) which corresponds to the orthogonal complement of the attractor space "dies out" under sufficiently many iterations. In the limit of large n the evolution of the state $\rho(n)$ tends to its asymptotic regime

$$\rho_\infty(n) = \sum_{\lambda \in \sigma_{|1|}, i=1}^{d_\lambda} \lambda^n \, \mathrm{tr}(\rho(0) X_{\lambda,i}^\dagger) X_{\lambda,i}, \tag{3.11}$$

where $\{X_{\lambda,i}\}_{i=1}^{d_\lambda}$ are orthonormal bases of $\mathrm{Ker}(\Phi - \lambda I)$, $\lambda \in \sigma_{|1|}$.

Let us emphasize that the asymptotic dynamics depends on the initial state ρ and the resulting asymptotic behaviour can be in general highly complex.

If the asymptotic spectrum contains eigenvalue $\lambda = 1$ only the asymptotic dynamics is trivial and any initial state approaches some stationary state of RUO Φ.

The last unresolved question is whether there is a technique which allows one to determine the attractor space. That is, a technique which calculates eigenvectors corresponding to eigenvalues with unit modulus. It is useful especially in cases where an analytical solution is required. Fortunately, it can be proved [7] that an operator X is an eigenvector of Φ (3.9) associated to an eigenvalue $\lambda \in \sigma_{|1|}(\Phi)$ if and only if it satisfies the following relation

$$U_i X = \lambda X U_i \quad \text{for each } i \in \hat{m}. \tag{3.12}$$

As one can see, probabilities p_i do not affect the attractor space, provided $p_i \neq 0$, $i \in \hat{m}$. Nonetheless, they influence a rate of convergence of the iterative method (see later).

3.3 General Twirling Operations

In this part we define a special subset of random unitary operations, so-called *twirling operations*. In order to proceed, assume a compact group G equipped with the Haar measure $\mathrm{d}g$, i. e. a normalized left invariant measure. Let $U(g)$ be a unitary representation of G acting on the Hilbert space $\mathscr{H}$. The twirling operation is then defined by formulas (for finite and infinite groups respectively)

$$P'(A) \equiv \frac{1}{|G|} \sum_{g \in G} U(g) A\, U(g)^\dagger \quad \text{or} \quad P(A) \equiv \int_{g \in G} U(g) A\, U(g)^\dagger \mathrm{d}g. \tag{3.13}$$

where $|G|$ stands for the cardinality of the (finite) group G. One can think of twirling operations as procedures randomizing input states along a given group of unitary transformations.

There are two important classes of twirling operations utilized in quantum information theory [8]. In order to define the first class consider $N \in \mathbb{N}$ and the group $G = \mathrm{U}(d)$ of all d-dimensional unitary matrices with the representation $U(V) = V^{\otimes N}$. The twirling operation is now defined as

$$P(A) \equiv \int_{U \in \mathrm{U}(d)} U^{\otimes N} A\, (U^{\otimes N})^\dagger \, \mathrm{d}U. \tag{3.14}$$

Let ρ be a composite state of N qudits. The above operation acting on ρ can be understood as an application of a random transformation U to every qudit in ρ. Consider a situation for $N = 2$. Any bipartite state subjected to the twirling (3.14) becomes a Werner state (section 1.7). Moreover, for

$d = 2$ the singlet state is the only pure state which is left unchanged under this transformation [1].

The second class of twirling operations is defined in the following manner. Assume again the group $G = \mathrm{U}(d)$ and its representation $U(V) = V \otimes V^*$. The twirling operation defined as

$$P_{\mathrm{iso}}(A) \equiv \int_{U \in \mathrm{U}(d)} U \otimes U^*\, A\, (U \otimes U^*)^\dagger \,\mathrm{d}U \tag{3.15}$$

transforms any bipartite state to the isotropic one (see section 1.7), the meaning of the symbols remains the same as in (3.14).

Suppose we want to implement the general twirling operation (3.13). To this end, consider an ensemble of quantum systems in the same initial state. In a practical setup, we implement the twirling by multiple iterations of these two steps: First, we generate a quantum state. Second, we apply a random unitary operation. The execution time of this approach is proportional to a number of systems in the ensemble. This method also converges to the desired twirling polynomially with the number of unitaries and is therefore rather inefficient. Moreover, in many physical realizations of quantum computing is this approach not applicable since the systems cannot be accessed individually, see [8].

Let us emphasize that both classes of twirling operations (3.14) and (3.15) require that all unitaries from $\mathrm{U}(d)$ have to be applied locally and with a uniform distribution according to Haar measure. This additional constraint is very important, see item 1 in section 2.2.

3.3.1 Original Twirling Implementation

In this section we introduce the original implementation of the twirling operation (3.14), proposed in [6] and [3] for two-qubit systems. It consists in replacement of integration in (3.14) by summation over the (finite) T group, i. e. it is again twirling operation (3.14). The output state of this procedure is of the form

$$P(\rho) = \frac{1}{N} \sum_{i=1}^{N} U_i \rho\, U_i^\dagger, \tag{3.16}$$

where $N = 12$ denotes the cardinality of the T group. This group is a subgroup of SU(4), i. e. a group of 4×4 unitary matrices with a unit determinant. For structrure of the T group see below.

To explain the method in details, consider three bilateral rotations B_x, B_y and B_z. They correspond to $\frac{\pi}{2}$-rotations of a cube around x, y and z-axis, respectively. Explicitly, let $R_i(\theta)$ be a rotation around i-axis by an angle θ. That is,

$$R_i(\theta) = \exp\left(i \frac{\theta}{2} \sigma_i \right),$$

	Ψ^-	Φ^-	Φ^+	Ψ^+
I	Ψ^-	Φ^-	Φ^+	Ψ^+
B_x	Ψ^-	Φ^-	$i\Psi^+$	$i\Phi^+$
B_y	Ψ^-	$-\Psi^+$	Φ^+	Φ^-
B_z	Ψ^-	$i\Phi^+$	$i\Phi^-$	Ψ^+

Table 3.1: Basic bilateral $\frac{\pi}{2}$-rotations with the identity acting on Bell states

I	B_xB_y	$B_xB_yB_xB_y$
B_xB_x	B_yB_z	$B_yB_zB_yB_z$
B_yB_y	B_zB_x	$B_zB_xB_zB_x$
B_zB_z	B_yB_x	$B_yB_xB_yB_x$

Table 3.2: The tetrahedral group of rotations utilized in the twirling implementation

where $\{\sigma_i\}_{i=1}^3$ are so-called *Pauli matrices*. These are defined in the following way

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

The bilateral rotations B_x, B_y and B_z are then defined as follows

$$B_i = R_i\left(\frac{\pi}{2}\right) \otimes R_i\left(\frac{\pi}{2}\right), \quad i \in \{x, y, z\}.$$

Actions of B_x, B_y, B_z on Bell states are demonstrated in Table 3.1. It is evident that $B_i^4 = I$ for every $i \in \{x, y, z\}$. These three operations together with the identity represent generators of the 24-element group of rotations known as the octahedral group (O group). It corresponds to rotations of a cube. Let us choose only those rotations which leave a tetrahedron invariant. These $N = 12$ rotations constitute a subgroup of O known as the tetrahedral group (T group) [9]. Elements $\{U_i\}_{i=1}^N$ of this group are used in (3.16). They are listed in Table 3.2, expressed as products of basic bilateral rotations.

We have described the meaning of all symbols presented in (3.16). For clarification of this approach see [9] or later in this thesis. This method seems to be sufficient for the twirling (3.14) implementation, at least for the two-qubit case. However, difficulties may occur in the experimental setup as it is not easy to handle twelve different operations in a short time. Moreover, for higher dimensions, see d and N in (3.14), the number of unitaries needed increases rapidly [8]. In physical realizations, perturbations of employed unitaries may lead to improper results. The iterative method treats this situation since multiple application of particular though disrupted operation can result in an accurate outcome. The iterative method is the main object of the next chapter.

Chapter 4

Iterative Implementation of Twirling Operations

In the previous chapter we discussed drawbacks of the original twirling implementation. This part presents own author's contribution to this issue. It can be divided into three units. In the first unit, we introduce a universal method for an efficient implementation of general twirling operations (3.13). This method consists in iterated applications of random unitary operations, whose properties were studied in chapter 3. It turns out that this approach is robust with respect to imperfections of unitary operations employed in the process. Moreover, it ensures exponentially fast convergence to a desired twirling operation.

In the second unit, the iterative implementation of twirling (3.14) is investigated in details. We focus on the simplest but also nontrivial case of two qubits. As a result, we provide necessary and sufficient condition under which the iterative method converges to twirling (3.14). Then we compare our findings with the original approach discussed in subsection 3.3.1.

As the iterative method works for a huge class of random unitary operations, in the last unit we perform numerical analysis investigating a rate of convergence for different choices of RUOs. We present numerical estimates of speed of convergence and an associated algorithm. Finally, on the basis of obtained results we draw conclusions about the implementation of twirling (3.14) with use of the iterative method.

4.1 Implementation—General Approach

In this part we introduce the iterative method which is capable of an efficient implementation of general twirling operation (3.13). A crucial component of the method is an appropriately chosen random unitary operation Φ which is applied iteratively on an initial state. We demand that the state resulting from iterations tends to the required twirled state with increasing number of

iterative steps. As this method is supposed to work for any initial state we want the asymptotic regime of discrete evolution Φ^n to be precisely the twirling operation P (3.13). That is

$$\lim_{n\to\infty} \Phi^N = P.$$

Let us analyze when this situation occurs. Initially, we have to explore properties of general twirling operation (3.13)

$$P(A) = \int_{g\in G} U(g) A\, U(g)^\dagger \,\mathrm{d}g, \tag{4.1}$$

where G is a compact group, $U(g)$ is its unitary representation and $\mathrm{d}g$ is a normalized Haar measure on G. Using properties of the Haar measure one can show that the superoperator P (4.1) is an orthogonal projector, i. e. $P = P^2$ and $P = P^\dagger$. Indeed, two-fold application of the map P gives

$$\begin{aligned} P^2(A) &= P\left(P(A)\right) = \int_{g\in G} U(g) \left(\int_{h\in G} U(h) A\, U(h)^\dagger \mathrm{d}h \right) U(g)^\dagger \,\mathrm{d}g \\ &= \iint_{g,h\in G} U(g)U(h) A\; U(h)^\dagger\, U(g)^\dagger \,\mathrm{d}h\,\mathrm{d}g \\ &= \iint_{g,h\in G} (U(g)U(h)) A\; (U(g)U(h))^\dagger \,\mathrm{d}h\,\mathrm{d}g \\ &= \iint_{g,h\in G} U(gh) A\; U(gh)^\dagger \,\mathrm{d}h\,\mathrm{d}g \;=\; P(A). \end{aligned}$$

For Hermitian conjugate $P^\dagger$ (with respect to the Hilbert-Schmidt inner product) the following relations hold

$$\begin{aligned} P^\dagger(A) &= \int_{g\in G} U(g)^\dagger A\; U(g) \,\mathrm{d}g \\ &= \int_{g\in G} U(g^{-1}) A\; U(g^{-1})^\dagger \,\mathrm{d}g. \end{aligned}$$

The last expression is equivalent to the definition of $P(A)$, thence $P = P^\dagger$. We have proved that P is a projector (onto $\mathrm{Ran}\,(P)$), therefore its spectrum contains 0 and 1 only, $\sigma(P) = \{0, 1\}$. The fact that twirling operations are projectors plays a crucial role. In particular, their attractor space is composed of P-invariant states, i. e. $\mathrm{Attr}(P) = \mathrm{Ran}(P)$.

Consider a random unitary operation (see (3.9))

$$\Phi(A) = \sum_{i=1}^{m} p_i\, U_i A\, U_i^\dagger, \tag{4.2}$$

where $\{U_i\}_{i=1}^m$ is a set of unitary operators and $\{p_i\}_{i=1}^m$ is a probability distribution. Making use of findings discussed in section 3.2 we can formulate

the following statement. Evolution Φ^n generated by successive applications of RUO Φ tends to desired twirling operation P if and only if

$$\mathrm{Attr}\,(\Phi) = \mathrm{Ran}\,(P) \quad \wedge \quad \sigma_{|1|}(\Phi) = \{1\}. \tag{4.3}$$

It means that the asymptotic spectrum of RUO Φ contains only eigenvalue $\lambda = 1$ and its attractor space contains solely invariant operators of the twirling operation P.

At this moment the main issue is to choose unitaries $\{U_i\}_{i=1}^m$ of RUO Φ in order to satisfy condition (4.3). This choice has to respect three constraints, in principle. First, unitaries $\{U_i\}_{i=1}^m$ have to confine (via (3.12)) the attractor space of RUO Φ to $\mathrm{Ran}(P)$, i. e. $\mathrm{Attr}(\Phi) = \mathrm{Ran}(P)$. Second, the structure of these unitaries has to follow requirements given by the original setting, e. g. if all unitary operations in the twirling are applied locally then also all unitaries of RUO Φ have to be local. Third, the set of these unitaries $\{U_i\}_{i=1}^m$ should be as small as possible and each unitary U_i should be implemented easily.

A natural choice is that these unitaries are elements of the original representation, i. e. $U_i = U(g_i)$. One possibility is to choose unitaries $\{U_i\}_{i=1}^m$ in such a way that they constitute a group. For these unitaries a random unitary operation defined as

$$\widetilde{\Phi}(A) = \frac{1}{m} \sum_{i=1}^{m} U_i \, A \, U_i^\dagger \tag{4.4}$$

is an orthogonal projector and everything inferred for the general twirling P is valid also for $\widetilde{\Phi}$, see P' in (3.13). In the following, we will consider a special case of (4.1) only (see (3.14))

$$P(A) = \int_{U \in \mathrm{U}(d)} U^{\otimes N} A \, (U^{\otimes N})^\dagger \, \mathrm{d}U, \tag{4.5}$$

where $N \in \mathbb{N}$, $d \in \mathbb{N}$ and $\mathrm{U}(d)$ is the group of d-dimensional unitary matrices.

Let $N = d = 2$. Then only states which are left invariant under (4.5) are Werner states (see section 1.7). That is, the attractor space of (4.5) is the linear span of the identity matrix and $|\Psi^-\rangle\langle\Psi^-|$, where $|\Psi^-\rangle$ is the singlet state (see section 1.6). For this special case we can rewrite condition (4.3) in the following way. A random unitary operation Φ approximates twirling (4.5) with $N = d = 2$ if and only if

$$\mathrm{Attr}\,(\Phi) = \mathrm{span}\{|\Psi^-\rangle\langle\Psi^-|, I\} \quad \wedge \quad \sigma_{|1|}(\Phi) = \{1\}, \tag{4.6}$$

where $|\Psi^-\rangle$ is the singlet state and I stands for the identity matrix.

We have shown under which conditions the twirling can be implemented by a random unitary operation. To be more precise, successive applications of RUO Φ tend to twirling (4.1) iff Φ satisfies (4.3). This relation simplifies for two-qubit twirling (4.5) to (4.6). In the next section, we employ these results to investigate implementation of two-qubit twirling (4.5).

4.2 Two-Qubit Twirling—Analytical Part

In the following parts we will analyze whether the dynamics generated by RUO (3.9) leads to the twirling operation (4.5) with respect to different choices of unitaries U_i. From the very beginning we restrict ourselves to two-qubit systems. It corresponds to $N = d = 2$ in (4.5). The presented procedure remains effectively the same even for higher dimensions and higher number of particles. Hereafter, we represent every 4×4 matrix in the Bell basis $\{\Psi^-, \Phi^-, \Phi^+, \Psi^+\}$, see section 1.6.

To start with, consider a random unitary operation Φ (3.6). We assume the simplest case for $m = 2$ number of unitaries. That is,

$$\Phi(\rho) = p\, U_1\, \rho\, U_1 + (1-p)\, U_2\, \rho\, U_2 \tag{4.7}$$

with $0 < p < 1$ and $U_i = u_i \otimes u_i$, where u_i stand for unitary matrices acting on single qubits. It turns out that two nontrivial mutually different unitaries U_i can be sufficient for the twirling implementation. Generalization to an arbitrary number of unitaries is straightforward and we discuss it later.

In order to proceed, recall findings presented in section 3.2 and results of the previous section. Relation (4.6) implies that elements of the attractor space $\mathrm{Attr}(\Phi)$ must be of the form

$$X = \begin{pmatrix} a & 0 & 0 & 0 \\ 0 & b & 0 & 0 \\ 0 & 0 & b & 0 \\ 0 & 0 & 0 & b \end{pmatrix} \tag{4.8}$$

for some $a, b \in \mathbb{C}$. Therefore, we aim to find such Φ (4.7) for which is the condition $X \in \mathrm{Attr}(\Phi)$ equivalent to (4.8) and for which $\sigma_{|1|}(\Phi) = \{1\}$.

Our investigation proceeds as follows. Initially, we choose a suitable parametrization of Φ (4.7). As a next step, we make use of Equation 3.12 to analyze for which values of parameters the attractor space is of the desired form (4.6), i. e. its elements are of the form (4.8).

4.2.1 Parametrization of the RUO

Before we proceed, it is suitable to simplify representation of the RUO (4.7). It will be found useful in both analytical and numerical part. In the analytical part it reduces the number of equations and in the numerical one it shortens computational time.

At the beginning, we present obtained result in the form of the following statement. Matrix representation of any random unitary operation (4.7) can be written in some local basis as

$$\mathbf{\Phi} = p\ (V_1 \otimes V_1^*) + (1-p)\ (V_2 \otimes V_2^*), \tag{4.9}$$

where V_1 and V_2 are matrices parametrized by four real parameters φ, γ, θ and μ. These matrices are of the following form

$$V_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos(2\varphi) & i\,\sin(2\varphi) & 0 \\ 0 & i\,\sin(2\varphi) & \cos(2\varphi) & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

$$V_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & A^- & B^- & -\cos(\theta-\mu)\sin(2\gamma) \\ 0 & B^+ & A^+ & -i\,\sin(\theta-\mu)\sin(2\gamma) \\ 0 & \cos(\theta+\mu)\sin(2\gamma) & i\,\sin(\theta+\mu)\sin(2\gamma) & \cos(2\gamma) \end{pmatrix},$$

where $A^{\pm}$ and $B^{\pm}$ are defined as

$$\begin{aligned} A^- &= \cos(2\theta)\cos^2(\gamma) - \cos(2\mu)\sin^2(\gamma), \\ A^+ &= \cos(2\theta)\cos^2(\gamma) + \cos(2\mu)\sin^2(\gamma), \\ B^- &= i\,\sin(2\theta)\cos^2(\gamma) - i\,\sin(2\mu)\sin^2(\gamma), \\ B^+ &= i\,\sin(2\theta)\cos^2(\gamma) + i\,\sin(2\mu)\sin^2(\gamma). \end{aligned}$$

In order to prove the statement above let us consider a random unitary operation Φ (4.7). As shown in section 3.1 one can express a RUO in the matrix representation

$$\mathbf{\Phi} = p\; U_1 \otimes U_1^* + (1-p)\; U_2 \otimes U_2^*, \tag{4.10}$$

where an asterisk denotes complex conjugation, see (3.7). Since we assume two-qubit states the unitaries $\{U_i\}_{i=1}^2$ in (4.10) are of the form $U_i = u_i \otimes u_i$, where u_i are unitary 2×2 matrices acting on a single qubit. As we can see, a global phase of each u_i is unimportant. Therefore, one can parametrize u_i by three real parameters γ, θ and μ as follows

$$\begin{pmatrix} e^{i\theta}\cos\gamma & -e^{-i\mu}\sin\gamma \\ e^{i\mu}\sin\gamma & e^{-i\theta}\cos\gamma \end{pmatrix}. \tag{4.11}$$

Both unitaries u_i are written in the same basis. In order to simplify a parametrization we choose a local basis in which u_1 is diagonal. That is,

$$u_1 = q \cdot v_1 \cdot q^\dagger,$$

where v_1 is a diagonal matrix and q is a unitary. Since v_1 is now a unitary diagonal 2×2 matrix with $\det v_1 = 1$ it must be of the form

$$v_1 = \begin{pmatrix} e^{i\varphi} & 0 \\ 0 & e^{-i\varphi} \end{pmatrix}, \tag{4.12}$$

for some $\varphi \in \mathbb{R}$. The RUO $\mathbf{\Phi}$ can then be written in the form (see tensor product properties in Appendix A)

$$\begin{aligned}\mathbf{\Phi} &= p\ (Q \otimes Q^*) \cdot (V_1 \otimes V_1^*) \cdot (Q^\dagger \otimes Q^T) \\ &\quad + (1-p)\ (Q \otimes Q^*) \cdot (V_2 \otimes V_2^*) \cdot (Q^\dagger \otimes Q^T) \\ &= (Q \otimes Q^*) \cdot [p\ (V_1 \otimes V_1^*) + (1-p)\ (V_2 \otimes V_2^*)] \cdot (Q^\dagger \otimes Q^T),\end{aligned}$$

where $Q = q \otimes q$, $V_1 = v_1 \otimes v_1$ and $V_2 = Q^\dagger U_2 Q$. The matrix V_2 is still unitary, it is a product of unitary matrices. Since "border" matrices in the previous formula represent a change of a basis we can get rid of them and consider the middle term only. The matrix form of a random unitary operation Φ is therefore

$$\mathbf{\Phi} = p\ (V_1 \otimes V_1^*) + (1-p)\ (V_2 \otimes V_2^*).$$

A RUO representation is now parametrized by five real parameters $p \in (0,1)$, $\varphi, \gamma, \theta, \mu \in [0, 2\pi)$ with the first matrix V_1 diagonal. In the Bell basis, the matrices V_1 and V_2 are of the form demonstrated in the statement at the beginning of this subsection.

4.2.2 Complete Solution for RUOs with Two Unitaries

We have simplified a matrix representation of RUO Φ and reduced the number of parameters needed for its description. The aim of this subsection is to analyze for which values of parameters φ, γ, θ and μ elements of the attractor space Attr(Φ) are in the form (4.8). This condition is equivalent to the fact that Φ approximates the twirling operation (4.5).

We make use of Equation 3.12 to determine the attractor space of Φ (4.7) for given values of parameters. Simultaneously, we exclude those parameter values for which $\sigma_{|1|} \neq \{1\}$ and which allow the existence of attractors lying outside the linear span of the singlet state and the identity matrix, see (4.6). For our two-qubit case with two unitaries V_1 and V_2 (see subsection 4.2.1) equations (3.12) are of the form

$$W_1 \equiv V_1 X - \lambda X V_1 = 0 \quad \wedge \quad W_2 \equiv V_2 X - \lambda X V_2 = 0, \tag{4.13}$$

where $X = (x_{ij})$ is an element of attractor space Attr(Φ). Before we perform all necessary calculations let us present our results in the following theorem.

Theorem 1. *Let Φ be a random unitary operation (4.7) with matrix representation (4.9). Then elements of its attractor space are of the form (4.8) and $\sigma_{|1|}(\Phi) = \{1\}$ if and only if the parameters φ, γ, θ and μ in (4.9) satisfy one of these relations*

1. $\varphi = (2k-1)\frac{\pi}{2} \ \wedge\ \gamma \neq l\frac{\pi}{2} \ \wedge\ \theta \neq m\frac{\pi}{2}, \ \ k,l,m \in \mathbb{Z},$
2. $\varphi \neq k\frac{\pi}{2} \ \wedge\ \gamma \neq l\frac{\pi}{2}\ , \ \ k,l \in \mathbb{Z}.$

The proof of the above statement follows. Consider Φ (4.7) and its matrix representation (4.9) with matrices V_1 and V_2. Let us concentrate on $W_1 = 0$ in (4.13) first. For our choice of V_1 this equation reads

$$\begin{pmatrix} A(x_{11}) & B(x_{12},x_{13}) & B(x_{13},x_{12}) & A(x_{14}) \\ C(x_{21},x_{31}) & D(x_{22},x_{32},x_{23}) & D(x_{23},x_{33},x_{22}) & C(x_{24},x_{34}) \\ C(x_{31},x_{21}) & D(x_{32},x_{22},x_{33}) & D(x_{33},x_{23},x_{32}) & C(x_{34},x_{24}) \\ A(x_{41}) & B(x_{42},x_{43}) & B(x_{43},x_{42}) & A(x_{44}) \end{pmatrix} = 0, \quad (4.14)$$

where A, B, C and D are functions of matrix elements x_{ij} which are defined in the following way

$$\begin{aligned} A(x_{ij}) &:= x_{ij}\,(1-\lambda), & (4.15)\\ B(x_{ij},x_{kl}) &:= x_{ij}\,(1-\lambda\cos(2\varphi)) - i\,\lambda x_{kl}\sin(2\varphi), & (4.16)\\ C(x_{ij},x_{kl}) &:= x_{ij}\,(\cos(2\varphi)-\lambda) + i\,x_{kl}\sin(2\varphi), & (4.17)\\ D(x_{ij},x_{kl},x_{mn}) &:= x_{ij}\,(1-\lambda)\cos(2\varphi) + i\,(x_{kl}-x_{mn}\lambda)\sin(2\varphi). & (4.18) \end{aligned}$$

It is easy to prove that $-\lambda^* C = B|_{\lambda\to\lambda^*}$, see (4.17) and (4.18). The equation $C = 0$ with λ is therefore equivalent to $B = 0$ with λ^*. Conditions imposed on arguments of C for λ are identical to those imposed on arguments of B for λ^*. Hence, we can take into account the condition $C = 0$ only and solutions for $B = 0$ can be obtained immediately. The condition $A = 0$ imposes no constraints on x_{ij}, $i,j \in \{1,4\}$, for $\lambda = 1$. On the contrary, for $\lambda \neq 1$ the relation $x_{ij} = 0$, $i,j \in \{1,4\}$, is the only possible case.

Let us discuss different values of φ. For $\varphi = k\pi$, $k \in \mathbb{Z}$, the unitary V_1 is equal to the identity matrix and therefore there is always some solution which does not belong to the desired attractor space. For $\varphi = (2k-1)\frac{\pi}{2}$, $k \in \mathbb{Z}$, one obtains

$$\begin{aligned} C(x_{ij},x_{kl}) &= -x_{ij}\,(1+\lambda),\\ D(x_{ij},x_{kl},x_{mn}) &= -x_{ij}\,(1-\lambda), \end{aligned}$$

for appropriate $i,j,k,l,m,n \in \hat{4}$. It is easy to see that for $\lambda \neq \pm 1$ there is only trivial solution corresponding to $W_1 = 0$. Equation 4.14 is for $\lambda = 1$ and $\lambda = -1$ solved by

$$X_1 \equiv \begin{pmatrix} x_{11} & 0 & 0 & x_{14} \\ 0 & x_{22} & x_{23} & 0 \\ 0 & x_{32} & x_{33} & 0 \\ x_{41} & 0 & 0 & x_{44} \end{pmatrix}, \quad X_2 \equiv \begin{pmatrix} 0 & x_{12} & x_{13} & 0 \\ x_{21} & 0 & 0 & x_{24} \\ x_{31} & 0 & 0 & x_{34} \\ 0 & x_{42} & x_{43} & 0 \end{pmatrix}, \quad (4.19)$$

respectively. Consider $\varphi \neq k\frac{\pi}{2}$, $k \in \mathbb{Z}$, now. By inspection of Equation 4.14 we see there are two pairs of "C-type" expressions with their arguments interchanged. In particular, we get

$$\begin{aligned} x_{31} = i\,x_{21}K, \quad x_{21} = i\,x_{31}K,\\ x_{34} = i\,x_{24}K, \quad x_{24} = i\,x_{34}K \end{aligned} \quad (4.20)$$

with $K \equiv \frac{\cos(2\varphi)-\lambda}{\sin(2\varphi)}$. We can combine both pairs of equations to obtain

$$x_{31}(1+K^2) = 0 \tag{4.21}$$

and analogously for x_{21}, x_{24} and x_{34}. For $\lambda = \pm 1$ is $K \in \mathbb{R}$ which implies $x_{31} = 0$ etc. If $\lambda \neq \pm 1$ then it is possible that $1 + K^2 = 0$, i. e. $K = \pm i$ and

$$\cos(2\varphi) - \lambda = \pm i \, \sin(2\varphi) \quad \Rightarrow \quad \lambda = e^{\pm i2\varphi}.$$

That is, for $\lambda \neq e^{\pm i2\varphi}$, $\varphi \neq k\frac{\pi}{2}$, $k \in \mathbb{Z}$, any solution for $W_1 = 0$ is of the form X_1 (4.19). Otherwise, when we substitute $\lambda = e^{i2\varphi}$ back into equations (4.20) we obtain relations

$$x_{13} = -x_{12}, \quad x_{31} = x_{21}, \quad x_{34} = x_{24}, \quad x_{43} = -x_{42}$$

and when we substitute $\lambda = e^{-i2\varphi}$ we obtain

$$x_{13} = x_{12}, \quad x_{31} = -x_{21}, \quad x_{34} = -x_{24}, \quad x_{43} = x_{42}.$$

The condition $D(x_{ij}, x_{kl}, x_{mn}) = 0$ (4.18) represents a system of four equations. We still assume $\varphi \neq k\frac{\pi}{2}$, $k \in \mathbb{Z}$. For $\lambda = 1$ relations reduce to $x_{32} = x_{23}$, $x_{33} = x_{22}$ and we can assume $\lambda \neq 1$ henceforth. For $\varphi = (2k-1)\frac{\pi}{4}$, $k \in \mathbb{Z}$, equations $D = 0$ simplify to $x_{kl} = \lambda x_{mn}$ for appropriate indices. Employing steps analogous to those for (4.21) one obtains

$$x_{23}\,(1-\lambda^2) = 0$$

and similarly for x_{32}, x_{22} and x_{33}. That is, for $\lambda \neq \pm 1$ all these x_{kl} equal zero. For $\lambda = 1$ relations $x_{32} = x_{23}$, $x_{33} = x_{22}$ hold and for $\lambda = -1$ holds $x_{32} = -x_{23}$, $x_{33} = -x_{22}$.

At this moment, we have restricted our investigation to $\varphi \neq k\frac{\pi}{4}$, $k \in \mathbb{Z}$, $\lambda \neq 1$ and the system of four equations $D(x_{ij}, x_{kl}, x_{mn}) = 0$ which can be written in the form

$$x_{ij} = -i\,\frac{x_{kl} - \lambda x_{mn}}{1-\lambda}\tan(2\varphi). \tag{4.22}$$

The substitution of this relation for x_{22} and x_{33} into the other two equations yields

$$K_1\,x_{23} - K_2\,x_{32} = 0 \quad \text{and} \quad K_1\,x_{32} - K_2\,x_{23} = 0$$

with $K_1 = 1 + \tan^2(2\varphi)\frac{1+\lambda^2}{(1-\lambda)^2}$ and $K_2 = 2\,\lambda\tan^2(2\varphi)\frac{1}{(1-\lambda)^2}$. Since $K_2 \neq 0$ we apply procedure analogous to (4.21) obtaining $x_{23}\,(K_2^2 - K_1^2) = 0$. Absolutely the same relation holds for x_{32}, x_{22} and x_{33}. The condition $K_2^2 = K_1^2$ is equivalent to

$$\tan^2(2\varphi) = -\left(\frac{\lambda-1}{\lambda+1}\right)^2.$$

Since $\lambda = e^{i\omega}$, $\omega \in [0, 2\pi)$, the right-hand side of the previous formula equals

$$-\left(\frac{e^{i\frac{\omega}{2}} - e^{-i\frac{\omega}{2}}}{e^{i\frac{\omega}{2}} + e^{-i\frac{\omega}{2}}}\right)^2 = \tan^2\left(\frac{\omega}{2}\right).$$

The above expression can be rewritten as $\tan(2\varphi) = \pm\tan(\frac{\omega}{2})$ which implies $\omega = \pm 4\varphi + 2k\pi$, $k \in \mathbb{Z}$. To sum up, considering $\lambda \neq e^{\pm i4\varphi}$, $\varphi \neq k\frac{\pi}{4}$, $k \in \mathbb{Z}$, all x_{ij}, $i, j \in \{2, 3\}$, are equal to zero. By the substitution $\lambda = e^{i4\varphi}$ and $\lambda = e^{-i4\varphi}$ in Equation 4.22 one obtains $x_{22} = -x_{33} = -x_{23} = x_{32}$ and $x_{22} = -x_{33} = x_{23} = -x_{32}$, respectively.

Before we draw an overall conclusion about solutions for $W_1 = 0$ we have to notice there are values of λ which "collide" with each other. It happens when $\lambda = e^{\pm i2\varphi} = e^{\pm i4\varphi}(e^{\mp i4\varphi})$. For $\varphi = \frac{\pi}{3} + k\pi$ or $\varphi = \frac{2\pi}{3} + k\pi$ the equality $e^{\mp i2\varphi} = e^{\pm i4\varphi}$ is satisfied. We excluded $\varphi = k\pi$ at the beginning, for such value holds $e^{\pm i2\varphi} = e^{\pm i4\varphi}$, $k \in \mathbb{Z}$. Results for these values of φ can be seen below.

Finally, we can write down the explicit forms of nontrivial solutions for $W_1 = 0$, see Table 4.1. We have solved equation $W_1 = 0$ for every possible setting of φ and λ. At this moment we proceed to W_2 and continue to find all possible solutions as well. We substitute matrices from Table 4.1 into $W_2 = 0$ and discuss different values of γ, θ and μ. In order to accomplish our goal we would like to extract only those values of φ, γ, θ and μ which ensure that there is no nontrivial solution for $\lambda \neq 1$. In subsequent computation we find out for which values of γ, θ and μ is the matrix which solves $W_2 = 0$ of the form (4.8). For these values we prove there is no other nontrivial solution corresponding to $\lambda \neq 1$.

Let us investigate attractors in the form X_1 first, i. e. $\varphi = (2k-1)\frac{\pi}{2}$, $k \in \mathbb{Z}$, and $\lambda = 1$, see (4.19). The equation $W_2 = 0$ simplifies to

$$\begin{pmatrix} 0 & A^+(x_{14}) & B^+(x_{14}) & C(x_{14}) \\ A^-(x_{41}) & D(x_{23}, x_{32}) & E^-(x_{22}, x_{33}, x_{23}) & F^-(x_{22}, x_{44}, x_{23}) \\ B^-(x_{41}) & E^+(x_{22}, x_{33}, x_{32}) & D(x_{23}, x_{32}) & G^-(x_{32}, x_{33}, x_{44}) \\ C(x_{41}) & F^+(x_{22}, x_{44}, x_{32}) & G^+(x_{23}, x_{33}, x_{44}) & 0 \end{pmatrix} = 0, \tag{4.23}$$

where functions A through G are defined in this way

$$\begin{aligned}
A^\pm(x_{ij}) &:= x_{ij}\cos(\theta \pm \mu)\sin(2\gamma), \\
B^\pm(x_{ij}) &:= x_{ij}\sin(\theta \pm \mu)\sin(2\gamma), \\
C(x_{ij}) &:= x_{ij}\sin^2(\gamma), \\
D(x_{ij}, x_{kl}) &:= (x_{ij} - x_{kl})\cos^2(\gamma)\sin(2\theta) + (x_{ij} + x_{kl})\sin^2(\gamma)\sin(2\mu), \\
E^\pm(x_{ij}, x_{kl}, x_{mn}) &:= i(x_{ij} - x_{kl})\left(\cos^2(\gamma)\sin(2\theta) \pm \sin^2(\gamma)\sin(2\mu)\right) \\
&\quad + 2x_{mn}\sin^2(\gamma)\cos(2\mu), \\
F^\pm(x_{ij}, x_{kl}, x_{mn}) &:= ((x_{ij} - x_{kl})\cos(\theta \pm \mu) + i\,x_{mn}\sin(\theta \pm \mu))\sin(2\gamma), \\
G^\pm(x_{ij}, x_{kl}, x_{mn}) &:= (x_{ij}\cos(\theta \pm \mu) + i\,(x_{kl} - x_{mn})\sin(\theta \pm \mu))\sin(2\gamma).
\end{aligned}$$

$\varphi = (2k-1)\frac{\pi}{2},\ \lambda = 1$	$\varphi \neq k\frac{\pi}{2},\ \lambda = 1$
$\begin{pmatrix} x_{11} & 0 & 0 & x_{14} \\ 0 & x_{22} & x_{23} & 0 \\ 0 & x_{32} & x_{33} & 0 \\ x_{41} & 0 & 0 & x_{44} \end{pmatrix}$	$\begin{pmatrix} x_{11} & 0 & 0 & x_{14} \\ 0 & x_{22} & x_{23} & 0 \\ 0 & x_{23} & x_{22} & 0 \\ x_{41} & 0 & 0 & x_{44} \end{pmatrix}$
$\varphi = (2k-1)\frac{\pi}{2},\ \lambda = -1$	$\varphi = (2k-1)\frac{\pi}{4},\ \lambda = -1$
$\begin{pmatrix} 0 & x_{12} & x_{13} & 0 \\ x_{21} & 0 & 0 & x_{24} \\ x_{31} & 0 & 0 & x_{34} \\ 0 & x_{42} & x_{43} & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & x_{22} & x_{23} & 0 \\ 0 & -x_{23} & -x_{22} & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$
$\varphi \neq k\frac{\pi}{3} \wedge \varphi \neq k\frac{\pi}{2},\ \lambda = e^{i2\varphi}$	$\varphi \neq k\frac{\pi}{3} \wedge \varphi \neq k\frac{\pi}{2},\ \lambda = e^{-i2\varphi}$
$\begin{pmatrix} 0 & x_{12} & -x_{12} & 0 \\ x_{21} & 0 & 0 & x_{24} \\ x_{21} & 0 & 0 & x_{24} \\ 0 & x_{42} & -x_{42} & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & x_{12} & x_{12} & 0 \\ x_{21} & 0 & 0 & x_{24} \\ -x_{21} & 0 & 0 & -x_{24} \\ 0 & x_{42} & x_{42} & 0 \end{pmatrix}$
$\varphi = \frac{\pi}{3} + k\pi \vee \varphi = \frac{2\pi}{3} + k\pi,\ \lambda = e^{i2\varphi}$	$\varphi = \frac{\pi}{3} + k\pi \vee \varphi = \frac{2\pi}{3} + k\pi,\ \lambda = e^{-i2\varphi}$
$\begin{pmatrix} 0 & x_{12} & -x_{12} & 0 \\ x_{21} & x_{22} & x_{22} & x_{24} \\ x_{21} & -x_{22} & -x_{22} & x_{24} \\ 0 & x_{42} & -x_{42} & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & x_{12} & x_{12} & 0 \\ x_{21} & x_{22} & -x_{22} & x_{24} \\ -x_{21} & x_{22} & -x_{22} & -x_{24} \\ 0 & x_{42} & x_{42} & 0 \end{pmatrix}$
$\varphi \neq k\frac{\pi}{3} \wedge \varphi \neq k\frac{\pi}{4},\ \lambda = e^{i4\varphi}$	$\varphi \neq k\frac{\pi}{3} \wedge \varphi \neq k\frac{\pi}{4},\ \lambda = e^{-i4\varphi}$
$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & x_{22} & -x_{22} & 0 \\ 0 & x_{22} & -x_{22} & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & x_{22} & x_{22} & 0 \\ 0 & -x_{22} & -x_{22} & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$

Table 4.1: Nontrivial solutions for $W_1 = 0$ depending on different values of φ and λ, $k \in \mathbb{Z}$.

As previously mentioned, we want to choose only those values of γ, θ and μ which confine a possible solution into the form (4.8), i. e. $x_{14} = x_{41} = x_{23} = x_{32} = 0$ and $x_{22} = x_{33} = x_{44}$. There is no constraint imposed on x_{44} for $\gamma = k\frac{\pi}{2}$, $k \in \mathbb{Z}$, see relations for F and G. That is, we consider $\gamma \neq k\frac{\pi}{2}$, $k \in \mathbb{Z}$, which also implies $x_{14} = x_{41} = 0$, see relations for A, B and C.

Consider $\theta = l\frac{\pi}{2}$, $l \in \mathbb{Z}$. Equations $E^{\pm} = 0$ can then be rewritten in the form

$$2\,x_{32}\cos(2\mu) \pm i(x_{22} - x_{33})\sin(2\mu) = 0.$$

By their addition we obtain $2(x_{23} + x_{32})\cos(2\mu) = 0$. This relation together with the equation for D, i. e. $(x_{23} + x_{32})\sin(2\mu) = 0$, implies $x_{32} = -x_{23}$. Equation 4.23 simplifies under the substitution $x_{32} \to -x_{23}$ to the system of five equations

$$\begin{aligned} x_{23}\cos\left(\pm l\frac{\pi}{2} + \mu\right) + i(x_{33} - x_{44})\sin\left(\pm l\frac{\pi}{2} + \mu\right) &= 0, \\ (x_{22} - x_{44})\cos\left(\pm l\frac{\pi}{2} + \mu\right) - ix_{23}\sin\left(\pm l\frac{\pi}{2} + \mu\right) &= 0, \\ 2x_{23}\cos(2\mu) - i\sin(2\mu)(x_{22} - x_{33}) &= 0. \end{aligned} \tag{4.24}$$

Let us discuss different values of μ. For $\mu = n\frac{\pi}{2}$, $n \in \mathbb{Z}$, the above system is equivalent to these relations

$$\begin{aligned} (x_{33} - x_{44})\sin\left((l \pm n)\frac{\pi}{2}\right) &= 0, \\ (x_{22} - x_{44})\cos\left((l \pm n)\frac{\pi}{2}\right) &= 0, \\ x_{23} &= 0. \end{aligned}$$

It is easy to see that one cannot obtain both conditions $x_{22} = x_{44}$ and $x_{33} = x_{44}$ simultaneously. Hence, this choice of parameter values does not lead to the twirling state. Consider $\mu \neq n\frac{\pi}{2}$, $n \in \mathbb{Z}$. For this value of μ are all sines in (4.24) nonzero. With help of periodicity of cotangent function we can express (4.24) by three equations

$$\begin{aligned} x_{33} - x_{44} + ix_{23}\cot\left(l\frac{\pi}{2} - \mu\right) &= 0, \\ (x_{22} - x_{44})\cot\left(l\frac{\pi}{2} - \mu\right) + ix_{23} &= 0, \\ x_{33} - x_{22} - 2ix_{23}\cot(2\mu) &= 0. \end{aligned}$$

The previous system is solved by $x_{33} = x_{22} + 2ix_{23}\cot(2\mu)$ and $x_{44} = x_{22} + ix_{23}\left(\cot\left(l\frac{\pi}{2} - \mu\right) + 2\cot(2\mu)\right)$ which is, in general, not in the twirling form neither.

We have shown there are solutions which are not in the required form (4.8) for $\theta = l\frac{\pi}{2}$, $l \in \mathbb{Z}$. On the contrary, it turns out that for $\theta \neq l\frac{\pi}{2}$, $l \in \mathbb{Z}$, and an arbitrary value of $\mu \in \mathbb{R}$ the solution of (4.13) is always of the form (4.8).

In order to proceed, let $\theta \neq l\frac{\pi}{2}$, $l \in \mathbb{Z}$. First, assume $\theta - \mu = m\pi$, $m \in \mathbb{Z}$. As a consequence, equations $F^- = 0$ and $G^- = 0$ simplify to $x_{44} = x_{22}$ and $x_{32} = 0$, respectively. Moreover, relations $D = 0$ and $E^+ = 0$ reduce to $x_{23}\sin(2\mu) = 0$ and $(x_{22} - x_{33})\sin(2\mu) = 0$. Conditions $\theta \neq l\frac{\pi}{2}$ and $\theta - \mu = m\pi$, $l, m \in \mathbb{Z}$, imply $\mu \neq n\frac{\pi}{2}$, $n \in \mathbb{Z}$. That is, equalities $x_{23} = 0$ and $x_{33} = x_{22}$ hold and the remainder of relations is satisfied immediately. To conclude, for $\theta - \mu = m\pi$, $m \in \mathbb{Z}$, is the solution of (4.23) in the desired form (4.8).

Consider $\theta - \mu = (2m-1)\frac{\pi}{2}$, $m \in \mathbb{Z}$. Similarly to the previous case we have $x_{23} = 0$ and $x_{44} = x_{33}$ implying $x_{32} = 0$ and $x_{33} = x_{22}$. For $\theta - \mu \neq m\frac{\pi}{2}$, $m \in \mathbb{Z}$, we can use equations $F^- = 0$ and $G^- = 0$ to express

$$\begin{aligned} x_{23} &= i(x_{22} - x_{44})\cot(\theta - \mu), \\ x_{32} &= -i(x_{33} - x_{44})\tan(\theta - \mu) \end{aligned}$$

and substitute them into remaining relations. We obtain

$$\begin{aligned} (x_{22} - x_{33})\left(\sin(2\theta) + \frac{\sin(2\mu)}{\cot^2(\gamma)}\right) - 2(x_{33} - x_{44})\frac{\cos(2\mu)}{\cot^2(\gamma)}\tan(\theta - \mu) &= 0, \\ (x_{22} - x_{33})\left(\sin(2\theta) - \frac{\sin(2\mu)}{\cot^2(\gamma)}\right) + 2(x_{22} - x_{44})\frac{\cos(2\mu)}{\cot^2(\gamma)}\cot(\theta - \mu) &= 0, \\ (x_{22} - x_{44})\left(\frac{\cot^2(\gamma)}{\sin^2(\theta - \mu)}\sin(2\theta) + \cot(\theta - \mu)\sin(2\mu)\right) & \\ -(x_{33} - x_{44})\sin(2\mu)\tan(\theta - \mu) - (x_{22} - x_{33})\cot^2(\gamma)\sin(2\theta) &= 0, \\ (x_{22} - x_{44})\cos(\theta + \mu)\cot(\theta - \mu) + (x_{33} - x_{44})\sin(\theta + \mu) &= 0. \end{aligned}$$

Let $\theta - \mu \neq m\frac{\pi}{2}$ and $\theta + \mu = n\pi$, $m, n \in \mathbb{Z}$. Then the fourth equation above reduces to $x_{44} = x_{22}$ and the second equation is thence in the form $(x_{22} - x_{33})\sin(2\mu) = 0$. Parameter values under consideration imply $\mu \neq p\frac{\pi}{2}$, $p \in \mathbb{Z}$, and the final solution is $x_{44} = x_{33} = x_{22}$ and $x_{23} = x_{32} = 0$. Let $\theta - \mu \neq m\frac{\pi}{2}$ and $\theta + \mu = (2n-1)\frac{\pi}{2}$, $m, n \in \mathbb{Z}$. Similarly to the previous case $x_{44} = x_{33}$ holds implying $x_{33} = x_{22}$ and $x_{23} = x_{32} = 0$.

Finally, assume $\theta - \mu \neq m\frac{\pi}{2}$ and $\theta + \mu \neq n\frac{\pi}{2}$, $m, n \in \mathbb{Z}$. We can extract the matrix element $x_{22} = x_{44} - (x_{33} - x_{44})\tan(\theta - \mu)\tan(\theta + \mu)$ from the fourth equation and substitute it into the other equations. These reduce to two independent relations

$$\begin{aligned} (x_{33} - x_{44})\sin(2\mu) &= 0, \\ (x_{33} - x_{44})\cos(2\mu) &= 0, \end{aligned}$$

which lead to $x_{44} = x_{33}$. To conclude, for $\varphi = (2k-1)\frac{\pi}{2}$, $\gamma \neq l\frac{\pi}{2}$, $\theta \neq m\frac{\pi}{2}$, $k, l, m \in \mathbb{Z}$, and $\mu \in \mathbb{R}$ is a solution of (4.13) in the desired twirled form (4.8).

Let us treat the case for $\varphi \neq k\frac{\pi}{2}$, $k \in \mathbb{Z}$, and $\lambda = 1$, see Table 4.1 for the corresponding solution. The only difference from X_1 (4.19) is such that

$x_{23} = x_{32}$ and $x_{22} = x_{33}$. Analogously to the previous case we demand that $\gamma \neq k\frac{\pi}{2}$, $k \in \mathbb{Z}$. It implies $x_{14} = x_{41} = 0$ and equations $D = 0$ and $E^{\pm} = 0$ simplifies to $x_{23}\sin(2\mu) = 0$ and $x_{23}\cos(2\mu) = 0$. That is, $x_{23} = 0$ and the remaining nontrivial relations $F^{\pm} = 0$ and $G^{\pm} = 0$ can be expressed as

$$\begin{aligned}(x_{22} - x_{44})\sin(\theta \pm \mu) &= 0,\\ (x_{22} - x_{44})\cos(\theta \pm \mu) &= 0,\end{aligned}$$

which means $x_{22} = x_{44}$. To conclude, for $\varphi \neq k\frac{\pi}{2}$, $\gamma \neq l\frac{\pi}{2}$, $k, l \in \mathbb{Z}$, and $\lambda = 1$ we obtain solution of (4.13) in the form (4.8).

We can draw the following conclusion. All solutions of (4.13) for $\lambda = 1$ are in the desired form (4.8) provided that one condition from the list

1. $\varphi = (2k-1)\frac{\pi}{2} \ \wedge \ \gamma \neq l\frac{\pi}{2} \ \wedge \ \theta \neq m\frac{\pi}{2}, \ \ k, l, m \in \mathbb{Z}$,
2. $\varphi \neq k\frac{\pi}{2} \ \wedge \ \gamma \neq l\frac{\pi}{2}, \ \ k, l \in \mathbb{Z}$,

is satisfied. Finally, we have to prove there are no other $\lambda \neq 1$, $|\lambda| = 1$, enabling nontrivial solutions for parameter values shown above. We substitute appropriate matrices from Table 4.1 into $W_2 = 0$ for these parameter values and solve. This procedure is rather lengthy work with linear equations, hence we present verification for $\lambda = -1$ only.

Let $\lambda = -1$ and $\varphi = (2k-1)\frac{\pi}{2}$, $\gamma \neq l\frac{\pi}{2}$, $\theta \neq m\frac{\pi}{2}$, $k, l, m \in \mathbb{Z}$. Any solution for $W_1 = 0$ is of the form X_2 (4.19). After we substitute this partial solution into $W_2 = 0$ we obtain

$$\begin{pmatrix} 0 & A^-(x_{12}, x_{13}) & A^+(x_{13}, x_{12}) & C^-(x_{13}, x_{12}) \\ B^-(x_{21}, x_{31}) & D(x_{42}, x_{24}) & E^+(x_{24}, x_{43}) & G^-(x_{24}, x_{34}) \\ B^+(x_{31}, x_{21}) & E^-(x_{42}, x_{34}) & F(x_{43}, x_{34}) & G^+(x_{34}, x_{24}) \\ C^+(x_{31}, x_{21}) & H^-(x_{42}, x_{43}) & H^+(x_{43}, x_{42}) & I(x_{24}, x_{42}, x_{34}, x_{43}) \end{pmatrix} = 0, \tag{4.25}$$

where

$$\begin{aligned} A^{\pm}(x_{ij}, x_{kl}) &\coloneqq x_{ij}\left(\frac{1}{\sin^2(\gamma)} \pm \cos(2\mu) + \cot^2(\gamma)\cos(2\theta)\right) \\ &\quad + ix_{kl}\left(\cot^2(\gamma)\sin(2\theta) \mp \sin(2\mu)\right), \\ B^{\pm}(x_{ij}, x_{kl}) &\coloneqq x_{ij}\left(\frac{1}{\sin^2(\gamma)} \pm \cos(2\mu) + \cot^2(\gamma)\cos(2\theta)\right) \\ &\quad + ix_{kl}\left(\cot^2(\gamma)\sin(2\theta) \pm \sin(2\mu)\right), \\ C^{\pm}(x_{ij}, x_{kl}) &\coloneqq x_{ij}\sin(\theta \pm \mu) - ix_{kl}\cos(\theta \pm \mu), \\ D(x_{ij}, x_{kl}) &\coloneqq x_{ij}\cos(\theta - \mu) - x_{kl}\cos(\theta + \mu), \\ E^{\pm}(x_{ij}, x_{kl}) &\coloneqq x_{ij}\sin(\theta \pm \mu) + ix_{kl}\cos(\theta \mp \mu), \\ F(x_{ij}, x_{kl}) &\coloneqq x_{ij}\sin(\theta - \mu) - x_{kl}\sin(\theta + \mu), \end{aligned}$$

$$\begin{aligned}
G^{\pm}(x_{ij},x_{kl}) &:= x_{ij}\left(\frac{\cos(2\gamma)}{\cos^2(\gamma)}+\cos(2\theta)\pm\tan^2(\gamma)\cos(2\mu)\right)\\
&\quad + ix_{kl}\left(\sin(2\theta)\pm\tan^2(\gamma)\sin(2\mu)\right),\\
H^{\pm}(x_{ij},x_{kl}) &:= x_{ij}\left(\frac{\cos(2\gamma)}{\cos^2(\gamma)}+\cos(2\theta)\pm\tan^2(\gamma)\cos(2\mu)\right)\\
&\quad + ix_{kl}\left(\sin(2\theta)\mp\tan^2(\gamma)\sin(2\mu)\right),\\
I(x_{ij},x_{kl},x_{mn},x_{op}) &:= x_{ij}\cos(\theta+\mu)-x_{kl}\cos(\theta-\mu)\\
&\quad + ix_{mn}\sin(\theta+\mu)-ix_{op}\sin(\theta-\mu).
\end{aligned}$$

First, let us consider $\theta-\mu=n\pi$, $n\in\mathbb{Z}$. This together with the assumption imposed on θ implies $\mu\neq p\frac{\pi}{2}$, $p\in\mathbb{Z}$. Moreover, the equation $C^-=0$ simplifies to $x_{12}=0$ and the equation $F=0$ simplifies to $x_{34}=0$. Under these conditions relations $A^{\pm}=0$ reduce to $x_{13}=0$ and the equation $G^+=0$ takes the form $x_{24}=0$. For these values of arguments relations $D=0$ and $E^+=0$ are equivalent to $x_{42}=0$ and $x_{43}=0$, respectively. After all simplifications being performed we can express $x_{31}=-ix_{21}\tan(\mu)$ from the equation $B^+=0$ and substitute. As a consequence, we obtain the final relation $x_{21}=0$ (from $B^-=0$ or $C^+=0$) implying $x_{31}=0$. To sum up, there is only the trivial solution of (4.13) for values of parameters φ, γ and θ chosen above, $\lambda=-1$ and $\theta-\mu=n\pi$, $n\in\mathbb{Z}$. For $\theta-\mu=(2n-1)\frac{\pi}{2}$, $n\in\mathbb{Z}$, we perform a similar discussion with the same result.

Let $\theta-\mu\neq n\frac{\pi}{2}$, $n\in\mathbb{Z}$. From $C^-=0$, $D=0$ and $E^+=0$ we can express (in the respective order)

$$\begin{aligned}
x_{13} &= ix_{12}\cot(\theta-\mu),\\
x_{42} &= x_{24}\frac{\cos(\theta+\mu)}{\cos(\theta-\mu)},\\
x_{43} &= ix_{24}\frac{\sin(\theta+\mu)}{\cos(\theta-\mu)}.
\end{aligned}$$

After the substitution, equations $A^{\pm}=0$ are equivalent to relations $x_{12}\sin(\mu)=0$ and $x_{12}\cos(\mu)=0$. It implies $x_{12}=0$. Moreover, relations $E^-=0$ and $F=0$ lead to $x_{34}=ix_{24}\tan(\theta-\mu)$. At this moment, equations $G^{\pm}=0$ are of the form

$$\begin{aligned}
x_{24}\left(2\cos(2\gamma)\cos^2(\theta)-\sin(2\theta)\tan(\theta-\mu)\right) &= 0,\\
x_{24}\left(2\cos(2\gamma)\cos^2(\theta)+\sin(2\theta)\cot(\theta-\mu)\right) &= 0.
\end{aligned}$$

When we subtract those equations we obtain $x_{24}\frac{\sin(2\theta)}{\sin(2(\theta-\mu))}=0$, i. e. $x_{24}=0$. There are still three remaining equations $B^{\pm}=0$ and $C^+=0$. Suppose $\theta+\mu=n\pi$, $n\in\mathbb{Z}$. Then $C^+=0$ reduces to $x_{21}=0$ which implies $x_{31}=0$, see $B^{\pm}=0$. For $\theta+\mu\neq n\pi$, $n\in\mathbb{Z}$, we can express $x_{31}=ix_{21}\cot(\theta+\mu)$

from $C^+ = 0$. Relations $B^\pm = 0$ are now equivalent to $x_{21}\sin(\mu) = 0$ and $x_{21}\cos(\mu) = 0$, hence $x_{21} = 0$. Finally, we see there are only trivial solutions of (4.13) for $\lambda = -1$ and $\varphi = (2k-1)\frac{\pi}{2}$, $\gamma \neq l\frac{\pi}{2}$, $\theta \neq m\frac{\pi}{2}$, $k, l, m \in \mathbb{Z}$.

Let $\lambda = -1$ and $\varphi \neq k\frac{\pi}{2}$, $\gamma \neq l\frac{\pi}{2}$, $k, l \in \mathbb{Z}$. The system of equations $W_2 = 0$ is reduced by the corresponding solution of $W_1 = 0$ to these seven relations

$$x_{22}\cos(2\theta) \pm \tan^2(\gamma)(x_{22}\cos(2\mu) - ix_{23}\sin(2\mu)) = 0, \quad (4.26)$$

$$x_{22}\cos(\theta \pm \mu) \mp ix_{23}\sin(\theta \pm \mu) = 0, \quad (4.27)$$

$$x_{23}\cos(\theta \pm \mu) \mp ix_{22}\sin(\theta \pm \mu) = 0, \quad (4.28)$$

$$x_{23}\cos(2\theta) = 0. \quad (4.29)$$

For $\theta - \mu = m\pi$, $m \in \mathbb{Z}$, equations (4.27) and (4.28) (for the plus sign between two terms) reduce to $x_{22} = 0$ and $x_{23} = 0$, respectively. The other equations are automatically satisfied for these values of x_{22} and x_{23}. For $\theta - \mu = (2m-1)\frac{\pi}{2}$, $m \in \mathbb{Z}$, we perform an analogous discussion obtaining $x_{22} = x_{23} = 0$. Let $\theta - \mu \neq m\pi$, $m \in \mathbb{Z}$. We can express $x_{23} = ix_{22}\cot(\theta - \mu)$ from (4.27) and substitute it to the remainder of equations. We obtain $x_{22} = 0$, see (4.28) with the plus sign between the terms, and thence $x_{23} = 0$.

Therefore, we conclude that for $\lambda = -1$ and values of parameters stated in Theorem 1 there is no nontrivial solution of (4.13). We already know for which values of parameters φ, γ, θ and μ solutions of (4.13) are in the desired form (4.8). This case corresponds to two unitary matrices utilized for construction of random unitary operation Φ. As a next step we discuss iterative implementation of twirling operation (4.5) with an arbitrary number of unitaries.

4.2.3 Generalization to More Unitaries

In the previous part we studied for which choice of RUO Φ (4.7) iterated applications of Φ tend to the two-qubit twirling (4.5). We summarized our results in Theorem 1. This subsection presents a generalization of this theorem. It concerns RUOs Φ (4.2) with an arbitrary number m of unitary matrices

$$\Phi(A) = \sum_{i=1}^{m} p_i U_i A U_i^\dagger, \quad (4.30)$$

where $\{U_i\}_{i=1}^m$ are two-qubit local unitaries $U_i = u_i \otimes u_i$ with $\det u_i = 1$. Without loss of generality we assume that each U_i is different from the identity matrix. Again, our aim is to find out for which unitaries U_i iterated applications of RUO Φ approaches to the two-qubit twirling (4.5).

In order to proceed we introduce the suitable parametrization of unitaries u_i. Analogously to subsection 4.2.1 we can always choose a basis for $\{u_i\}_{i=1}^m$ in which one chosen one-qubit matrix u_{i_0} is diagonal. The unitary operation

u_{i_0} is thence parametrized by one real parameter φ_{i_0}, see (4.12). The other unitaries u_j are described be three parameters $\gamma_j^{(i_0)}$, $\theta_j^{(i_0)}$, $\mu_j^{(i_0)}$, $j \in \hat{m}$, $j \neq i_0$, see (4.11). It is important to stress that this parametrization is fixed by the chosen local basis in which u_{i_0} is diagonal. Therefore, the lower index of the parameter φ and the upper index of parameters γ, θ and μ refer to our choice of the diagonal basis for u_{i_0}. Under these considerations we can formulate the following theorem.

Theorem 2. *Let Φ be a random unitary operation (4.30) with $m \geq 2$ number of two-qubit unitaries $\{U_i\}_{i=1}^m$, where $U_i = u_i \otimes u_i$, $U_i \neq I$ and $\det u_i = 1$. Then elements of the attractor space $\mathrm{Attr}(\Phi)$ are of the form (4.8) and $\sigma_{|1|}(\Phi) = \{1\}$ if and only if Φ satisfies one of the following conditions.*

1. *Assume $\mathrm{tr}\, u_{i_0} \neq 0$ for some $i_0 \in \hat{m}$. Then there is $j \in \hat{m}$, $j \neq i_0$, satisfying $\gamma_j^{(i_0)} \neq l\frac{\pi}{2}$, $l \in \mathbb{Z}$.*

2. *For each $i \in \hat{m}$, $\mathrm{tr}\, u_i = 0$ holds. We fix an arbitrary u_{i_0}. Then there are $j, k_1, k_2 \in \hat{m}$, $j \neq i_0$, $k_1 \neq i_0$, $k_2 \neq i_0$, such that $\gamma_j^{(i_0)} \neq l\frac{\pi}{2}$, $l \in \mathbb{Z}$, and $\mu_{k_1}^{(i_0)} \neq \mu_{k_2}^{(i_0)} + p\frac{\pi}{2}$, $p \in \mathbb{Z}$.*

Proof. The proof of the above theorem is rather lengthy work with different settings of parameters which characterize unitaries u_i. We sketch basic ideas of the proof. Since we already performed similar investigation for simpler case of $m = 2$ in Theorem 1 we want to employ its results even for a generalized setup. The attractor space $\mathrm{Attr}(\Phi)$ is determined by m equations of the form (3.12). We fix one particular $i_0 \in \hat{m}$ and one more index $j \in \hat{m}$. Now we can solve equations (3.12) for these two unitaries U_{i_0} and U_j only. By calculations similar to those in the proof of Theorem 1 we find all possible forms of attractors corresponding to RUO (4.7) for different values of parameters φ, $\gamma_j^{(i_0)}$, $\theta_j^{(i_0)}$ and $\mu_j^{(i_0)}$.

With i_0 kept fixed we can perform such analysis for each $j \in \hat{m}$, $j \neq i_0$. One can see that each pair of unitaries U_{i_0}, U_j restricts via (3.12) the possible attractor spectrum $\sigma_{|1|}(\Phi)$ of the map Φ and its associated attractor space. That is, for one particular $\lambda \in \sigma_{|1|}(\Phi)$ we obtain $m - 1$ sets of solutions of (4.13) corresponding to $W_{i_0} = 0 \wedge W_j = 0$, $j \in \hat{m}$, $j \neq i_0$. We denote such sets as $\mathrm{Attr}(U_j, \lambda)$. The elements of the attractor space $\mathrm{Attr}(\Phi)$ associated with eigenvalue λ are than obtained as all operators lying in the intersection $\bigcap_{j \in \hat{m}, j \neq i_0} \mathrm{Attr}(U_j, \lambda)$. By this procedure we explore attractor sets of the map Φ for different values of parameters and use results obtained in the proof of Theorem 1.

The last issue which stays unresolved is how to choose the index i_0, i. e. which one-qubit unitary u_i is suitable for diagonalization. Recall Theorem 1 and its proof. It is easier to determine whether the RUO (4.7) implements the

two-qubit twirling if the parameter φ of the unitary operation u_1 is not equal to $k\frac{\pi}{2}$, $k \in \mathbb{Z}$. Therefore, if it is possible we choose the index i_0 in such a way that $\varphi_{i_0} \neq k\frac{\pi}{2}$, $k \in \mathbb{Z}$. Provided that u_i is not equal to the identity matrix one can show that $\varphi_i \neq k\frac{\pi}{2}$ iff $\operatorname{tr} u_i \neq 0$, $k \in \mathbb{Z}$. Suppose $\operatorname{tr} u_i = 0$ for each $i \in \hat{m}$ now and recall a general form of a 2×2 unitary matrix (4.11). From this formula one can deduce $\operatorname{tr} u_i = 2\cos\theta_i \cos\gamma_i$. That is, if all unitaries $\{u_i\}_{i=1}^m$ have a zero trace then for any diagonal basis corresponding to some u_i, $i \in \hat{m}$, there are $l_j \in \mathbb{Z}$, $j \in \hat{m}$, $j \neq i$, such that $\gamma_j^{(i)} = (2l_j - 1)\frac{\pi}{2}$ or $\theta_j^{(i)} = (2l_j - 1)\frac{\pi}{2}$. Using approach described above one can analyze this enormously restricted set of parameter values quickly. □

Let us discuss equivalence of Theorem 1 and Theorem 2. Apparently, the second condition in Theorem 2 can be applied for RUOs Φ with $m \geq 3$ unitaries only. On the contrary, it can be proven that the first condition with $m = 2$ is equivalent to Theorem 1 stated in subsection 4.2.2. Indeed, let $m = 2$ and the first statement in Theorem 2 be satisfied. One can diagonalize unitary matrix u_{i_0} which is now parametrized by $\varphi_{i_0} \neq k\frac{\pi}{2}$, $k \in \mathbb{Z}$. Since we assume $\gamma_j \neq l\frac{\pi}{2}$, $l \in \mathbb{Z}$, we obtain the second condition in Theorem 1 immediately. In order to prove the other implication let the RUO Φ follow Theorem 1. The second condition in this theorem directly implies the first condition in Theorem 2.

The first condition requires $\varphi_1 = (2k-1)\frac{\pi}{2}$ for some $k \in \mathbb{Z}$ and $\gamma_2^{(1)} \neq l\frac{\pi}{2}$, $\theta_2^{(1)} \neq m\frac{\pi}{2}$, $l, m \in \mathbb{Z}$. One can show that $\operatorname{tr} u_2 \neq 0$, i. e. $\varphi_2 \neq k\frac{\pi}{2}$, $k \in \mathbb{Z}$. Iterative applications of Φ tend to the two-qubit twirling (4.5). This fact and the second condition of Theorem 1 ($\varphi_2 \neq k\frac{\pi}{2}$) implies $\gamma_1^{(2)} \neq l\frac{\pi}{2}$, $l \in \mathbb{Z}$. We have shown equivalence of both theorems for $m = 2$.

4.2.4 Discussion

We have shown in which cases the iterative method can be harnessed to implement the two-qubit twirling. It turns out that this method converges to the desired twirled state for almost all choices of unitaries which forms a RUO used for iterations.

Within the class of random unitary operations able to implement the twirling (4.5) there are RUOs which converge slower or faster. The speed of convergence is influenced by several factors. Namely, by the number of unitaries in RUO (3.6), their precise forms and by associated probabilities. Generally speaking, more unitaries employed in the definition of RUO allow faster convergence, provided that they follow Theorem 1. Thus, one can gradually enlarge the number of unitaries to achieve a given accuracy of the twirling approximation in less steps. In the extreme situation, one can choose unitaries following Theorem 1 which form a group. Then the precise twirling operation is obtained already after one step. The original implementation introduced in subsection 3.3.1 constitutes such an example.

Indeed, the formula (3.16) used in the original approach represents a random unitary operation whose unitaries form a finite group. Moreover, all unitaries used for the construction of (3.16) are applied locally to both qubits and satisfy conditions stated in Theorem 1. Therefore, the attractor space of (3.16) is spanned by the identity matrix and $|\Psi^-\rangle\langle\Psi^-|$ only, where $|\Psi^-\rangle$ is the singlet state, see section 1.6. If we recall the discussion corresponding to (4.4) it is obvious that one application of (3.16) on an initial state leads immediately to the twirled state.

In view of this discussion, the iterative method can be seen as a trade off between the number of unitaries employed and the number of steps required to achieve a given accuracy. We presented the applicability of the iterative method for the two-qubit twirling implementation. In the next part we focus on its optimal setting with respect to different choices of parameters. We again investigate the special case of RUO (4.7) with two unitaries only.

4.3 Rate of Convergence—Numerical Part

In the previous section, we performed an analytical investigation of the attractor space $\mathrm{Attr}(\Phi)$ corresponding to RUO Φ (4.7). We found out for which values of parameters ϕ, θ, γ and μ the random unitary operation Φ is able to implement the two-qubit twirling, see Theorem 1. Even though Φ tends to twirling (4.5) for almost all values of parameters, Theorem 1 does not deal with the fact how fast such convergence is. With respect to a physical realization of the iterative method it is important to know the dependence of speed of convergence on different parameter values. In this section we cope with this issue.

In order to proceed we need to quantify the rate of convergence with which Φ^n tends to the twirling P (4.5). To this end, let us introduce several notions needed for the subsequent discussion. Let λ_s be the so-called *subleading eigenvalue*, that is the eigenvalue of RUO Φ for which

$$|\lambda_s| = \max\{|\lambda| \,|\, \lambda \in \sigma(\Phi) \wedge \lambda \notin \sigma_{|1|}(\Phi)\},$$

where $\sigma_{|1|}(\Phi)$ is the attractor spectrum of Φ. In other words, the subleading eigenvalue is such an eigenvalue of Φ which has the highest modulus among all eigenvalues λ with $|\lambda| < 1$. Recall Appendix B, let $p \in \mathbb{N}$ be the number of Jordan blocks J_j of $\mathbf{\Phi}$ (4.9) corresponding to the subleading eigenvalue λ_s. Moreover, let $d_s \equiv \max_{j\in\hat{p}}\{d_j\}$, where $d_j = \dim J_j$, $j \in \hat{p}$.

The distance decay between Φ^n and P for increasing number n of iterative steps serves as a measure by which we evaluate the rate of convergence of Φ^n to the twirling P (4.5). In [10] it was shown that the Hilbert-Schmidt norm of the "perturbation" $\Phi^n - P$ is bounded above by a term which depends

exponentially on the modulus of λ_s in the following way

$$\|\Phi^n - P\| \leq C|\lambda_s|^{n-d_s+1} n^{d_s-1}. \tag{4.31}$$

The positive number C appearing in (4.31) is a function of the norm of Φ and for particular choice of RUO is therefore constant. In accordance with the previous inequality we will investigate relation between the subleading eigenvalue λ_s of Φ (4.7) and values of parameters φ, γ, θ and μ. In particular, we will be interested in modulus of λ_s only. Roughly speaking, lesser the $|\lambda_s|$, faster the convergence.

In the following we will construct an algorithm searching for the minimal subleading eigenvalue of Φ. Before we proceed to this task it is reasonable to find out whether we can restrict our survey to some subintervals of parameter ranges with no need to go through all possible parameter values. Such restrictions can significantly shorten computational time of the algorithm.

4.3.1 Restrictions of Parameter Ranges

As mentioned above it is suitable to restrict ranges of parameters used for the description of RUO (4.9). To begin with, recall subsection 4.2.1. For our purposes in the remainder of this section we can simplify the form of (4.9) even more. In the computational basis unitary matrices V_i, $i \in \hat{2}$, are in the form $V_i = v_i \otimes v_i$ where v_1 is diagonal. We will show that by an appropriate choice of a local basis we can get rid of parameter μ which does not influence the spectrum of RUO Φ. Consider $D = d \otimes d \otimes d^* \otimes d^*$ where

$$d = \begin{pmatrix} e^{i\frac{\mu}{2}} & 0 \\ 0 & e^{-i\frac{\mu}{2}} \end{pmatrix}.$$

Multiplication of $\mathbf{\Phi}$ (4.9) by D and $D^\dagger$ yields

$$D \cdot \mathbf{\Phi} \cdot D^\dagger = p\ D \cdot (V_1 \otimes V_1^*) \cdot D^\dagger + (1-p)\ D \cdot (V_2 \otimes V_2^*) \cdot D^\dagger. \tag{4.32}$$

Since D is unitary, (4.32) corresponds to change of a basis of $\mathbf{\Phi}$. Matrix V_1 is diagonal and is thence not affected by multiplication in (4.32). Unitaries V_i, $i \in \hat{2}$, are now of the form $V_i = v_i \otimes v_i$ where

$$v_1 = \begin{pmatrix} e^{i\varphi} & 0 \\ 0 & e^{-i\varphi} \end{pmatrix} \quad \text{and} \quad v_2 = \begin{pmatrix} e^{i\theta}\cos(\gamma) & -\sin(\gamma) \\ \sin(\gamma) & e^{-i\theta}\cos(\gamma) \end{pmatrix}. \tag{4.33}$$

As a next step, we will restrict ranges of remaining parameters φ, γ and θ. First, we narrow down the range of the parameter φ which occurs in v_1 (4.33). It is evident that the substitution $\varphi \to \varphi + \pi$ leaves the matrix $V_1 = v_1 \otimes v_1$ unchanged. Therefore, we can restrict the parameter φ to the $[0, \pi)$. Moreover,

we can restrict φ to the interval $[0, \frac{\pi}{2})$. Indeed, using the substitution $\varphi \to \pi - \varphi$ one obtains

$$v_1 = \begin{pmatrix} e^{i\varphi} & 0 \\ 0 & e^{-i\varphi} \end{pmatrix} \quad \xrightarrow{\varphi \to \pi - \varphi} \quad \begin{pmatrix} -e^{-i\varphi} & 0 \\ 0 & -e^{i\varphi} \end{pmatrix} = -v_1^*, \tag{4.34}$$

which implies transformations $V_1 \to V_1^*$ and $V_1^* \to V_1$ resulting in $V_1 \otimes V_1^* \to (V_1 \otimes V_1^*)^*$. On the other hand, recall matrix v_2 (4.33) and note that by application of the substitution $\theta \to -\theta$ one can obtain a complex conjugate of v_2, i. e. $V_2 \otimes V_2^* \to (V_2 \otimes V_2^*)^*$. If we perform last two substitutions simultaneously, we obtain

$$\mathbf{\Phi} \quad \xrightarrow[\theta \to -\theta]{\varphi \to \pi - \varphi} \quad \mathbf{\Phi}^*.$$

Since we are interested in eigenvalue modulus only we can feel free to restrict the range of φ to $[0, \frac{\pi}{2})$ while keeping in mind the simultaneous transformation of θ.

Arguments for restrictions of γ are similar to the previous case. Substitution $\gamma \to \gamma + \pi$ transforms v_2 into $-v_2$ and $V_2 \otimes V_2^*$ is therefore left unchanged. After the transformation $\gamma \to \pi - \gamma$, the matrix v_2 reads

$$\begin{pmatrix} -e^{i\theta}\cos\gamma & -\sin\gamma \\ \sin\gamma & -e^{-i\theta}\cos\gamma \end{pmatrix}.$$

We can take into account also the parameter θ. By the substitution $\theta \to \theta + \pi$ we recover the original matrix v_2. The simultaneous application of last two substitutions yields

$$v_2 \quad \xrightarrow[\theta \to \theta + \pi]{\gamma \to \pi - \gamma} \quad v_2.$$

It enables us to restrict the range of parameter γ to the interval $[0, \frac{\pi}{2})$. Again, we should not forget that both transformations $\gamma \to \pi - \gamma$ and $\theta \to \theta + \pi$ have to be performed simultaneously.

Another possibility how to check validity of this restriction is to notice

$$v_2 \quad \xrightarrow{\gamma \to \pi - \gamma} \quad -v_2^T,$$

hence $V_2 \otimes V_2^* \to (V_2 \otimes V_2^*)^T$ (see Appendix A). Since $V_1 \otimes V_1^*$ is diagonal, it is equal to its transpose. The net effect of the substitution for γ can be written as

$$\mathbf{\Phi} \quad \xrightarrow{\gamma \to \pi - \gamma} \quad \mathbf{\Phi}^T.$$

It is easy to see that $\mathbf{\Phi}$ has the same spectrum as its transpose, so we can make the restriction $\gamma \in [0, \frac{\pi}{2})$ without any manipulation with parameter θ. Constraints imposed on θ by transformations of φ (and γ) implies that the whole interval $[0, 2\pi)$ has to be analyzed for θ. Similarly, the entire range $(0, 1)$ of the parameter p has to investigated.

Finally, we can conclude it is sufficient to examine only these ranges of parameters when estimating speed of convergence of the iterative method for RUO (4.9)

$$\varphi \in \left[0, \frac{\pi}{2}\right), \quad \gamma \in \left[0, \frac{\pi}{2}\right), \quad \theta \in [0, 2\pi), \quad p \in (0, 1).$$

In the next part we describe an algorithm which explores parameter ranges shown above in order to look for the minimal subleading eigenvalue.

4.3.2 Algorithm

To perform numerical analysis we need to construct an algorithm which goes through restricted intervals of all parameters characterizing Φ (4.9) and calculates modulus of associated subleading eigenvalues. We make use of simplified form of Φ presented in the previous subsection, see (4.33). Using of the subleading eigenvalue in order to estimate the rate of convergence of Φ^n to twirling (4.5) was justified at the beginning of section 4.3. The most simple code accomplishing our goal is demonstrated in Figure 4.1 (we used *Wolfram Mathematica 9.0 Student Edition* software for our computations). In this case we plot subleading eigenvalues as a function of parameters φ and γ.

Let us briefly present all the functions shown in Figure 4.1. Function `UN` returns the ensemble of two matrices under consideration (see V_1 and V_2 in (4.9)), `matrixRepresentation` then takes these matrices to construct $\mathbf{\Phi}$ (4.9). Function `subleadingEigenvalue` is responsible for search of the subleading eigenvalue which corresponds to given parameter values. This function is applied by `subEigPhiGamma` to sufficiently many $\theta \in [0, 2\pi)$ and $p \in (0, 1)$ uniformly distributed with discrete steps `stepTheta` and `stepP`, respectively. The subleading eigenvalue for φ and γ given and for arbitrary θ and p is returned as an output. Finally, the `mainFunction` maps `subEigPhiGamma` onto discretized intervals for $\varphi \in [0, \frac{\pi}{2})$ and $\gamma \in [0, \frac{\pi}{2})$ with steps `stepPhi` and `stepGamma`, respectively.

We have described the algorithm which computes the subleading eigenvalue of RUO Φ (4.9) for different choices of parameters. At this moment, we can proceed to numerical analysis of the rate of convergence with which Φ approximates the twirling operation.

4.3.3 Results

In subsection 4.2.2 we proved that the iterative method converges to the desired twirling operation for almost all values of parameters. Another important issue is the speed of convergence to this desired operation. This part aims to explore regions of parameter values for which is the rate of convergence maximal.

First, we demonstrate how the subleading eigenvalue λ_s of the map Φ (4.7) depends on parameters φ, γ, θ and p. We numerically explore ranges of

```
UN[ϕ_, θ_, γ_] :=
 KroneckerProduct[#, #] & /@ {( e^(i ϕ)   0
                                0   e^(-i ϕ) ), ( e^(i θ) Cos[γ]   -Sin[γ]
                                                  Sin[γ]   e^(-i θ) Cos[γ] )}

matrixRepresentation[U_, p_] :=
 p * KroneckerProduct[U[[1]], U[[1]]*] +
  (1 - p) * KroneckerProduct[U[[2]], U[[2]]*]

subleadingEigenvalue[p_, θ_, ϕ_, γ_] := Module[{ei, i},
  ei = Eigenvalues[matrixRepresentation[UN[ϕ, θ, γ], p]];
  If[Abs[ei[[-1]]] == 1, Return[1]];
  For[i = 1, i ≤ Length[ei], i++, If[Abs@(ei[[i]]) < 1, Break[]]];
  ei[[i]]
 ]

step = 0.01;
stepTheta = step;
stepPhi = step;
stepGamma = step;
stepP = 0.05;

subEigPhiGamma[ϕ_, γ_] := Module[{λMax = 1, θ, p, λ},
  For[θ = 0, θ < 2 π, θ += stepTheta,
    For[p = stepP, p < 1, p += stepP,
     λ = subleadingEigenvalue[p, θ, ϕ, γ];
     If[Abs@λ < Abs@λMax, λMax = λ];
    ]
   ]
   λMax
 ]

mainFunction[] := Module[{output, ϕ, γ},
  output = {};
  For[ϕ = stepPhi, ϕ < π/2, ϕ += stepPhi,
     For[γ = stepGamma, γ < π/2, γ += stepGamma,
       AppendTo[output, {ϕ, γ, subEigPhiGamma[ϕ, γ]}]]
    ]
    output /. {Null → 1}
 ]
```

Figure 4.1: Subleading eigenvalue searching algorithm

parameters φ, γ, θ and p in order to seek for the minimal subleading eigenvalue of RUO Φ. We employ the algorithm presented in the previous subsection with steps $\texttt{step} = \texttt{stepPhi} = \texttt{stepGamma} = \texttt{stepTheta} = 0.01$ and $\texttt{stepP} = 0.05$, see Figure 4.1. Obtained results are presented in Figure 4.2 and Figure 4.3. In both plots the modulus of the minimal subleading eigenvalue λ_s is depicted as a function of parameters φ and γ. It is calculated for φ and γ fixed while going through whole ranges of parameters θ and p. Red colour stands for modulus of subleading eigenvalue λ_s which is close to one, blue colour represents value of modulus close to zero. As Figure 4.2 suggests the lowest subleading eigenvalues lie in two separated regions characterized by these approximate parameter ranges

$$\begin{aligned} &\varphi \in (0.80, 0.90),\ \gamma \in (1.05, 1.25),\ p \in (0.45, 0.60); \\ &\varphi \in (1.15, 1.30),\ \gamma \in (0.75, 0.90),\ p \in (0.40, 0.60); \end{aligned} \tag{4.35}$$

where the value of θ approaches one of values 0, π or 2π. As these regions contain λ_s with significantly smaller modulus than can be achieved in the rest of parameter ranges we call them regions of fast convergence.

If we perform this analysis with smaller steps $\texttt{step} = 0.002$ and $\texttt{stepP} = 0.001$ we encounter the global minimum of modulus of the subleading eigenvalue λ_s for these parameter values

$$\varphi = 1.276,\ \gamma = 0.828,\ \theta = 2.856,\ p = 0.503 \quad \text{with} \quad |\lambda_s| = 0.177193. \tag{4.36}$$

We will refer to this setting of parameters as the ideal case in the remainder of this section. To show the dependence of the subleading eigenvalue on θ and p for given values of φ and γ see Figure 4.4. For this particular case we fix parameters φ and γ with values stated in (4.36). As one can see the minimal values of λ_s are achieved for the parameter p close to one half which is in correspondence with relations (4.35).

The modulus of λ_s for RUOs whose parameters lie in regions of fast convergence (4.35) turns out to be quite sensitive with respect to a particular setting of parameter values. In order to demonstrate this sensitivity, let $\gamma = 0.828$ and $p = 0.503$. When we slightly modify parameters φ and θ lying nearby the ideal case (4.36) we obtain

$$\begin{aligned} \varphi = 1.275,\ \theta = 2.855: &\quad |\lambda_s| = 0.211387, \\ \varphi = 1.275,\ \theta = 2.856: &\quad |\lambda_s| = 0.267982, \\ \varphi = 1.276,\ \theta = 2.855: &\quad |\lambda_s| = 0.264374, \\ \varphi = 1.276,\ \theta = 2.856: &\quad |\lambda_s| = 0.177193. \end{aligned}$$

Even though we change values of φ and θ in order of thousandths, the modulus of λ_s responds as a change by several hundredths.

At this moment, let us demonstrate the difference in the rate of convergence between two appropriate sets of parameters. In the first case we choose

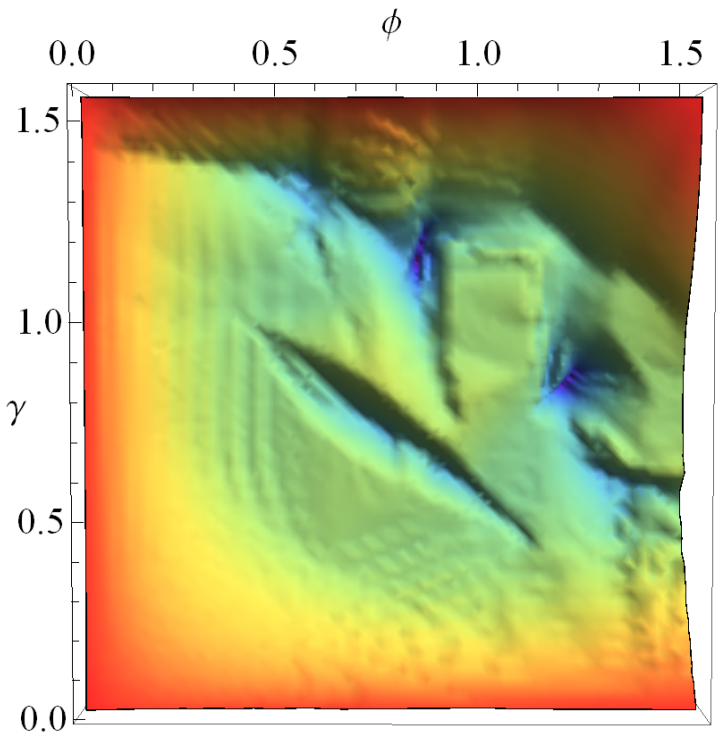


Figure 4.2: Modulus of subleading eigenvalue λ_s (top view) for steps `step` = 0.01 and `stepP` = 0.05—red colour marks the maximal value of λ_s, blue the minimal one.

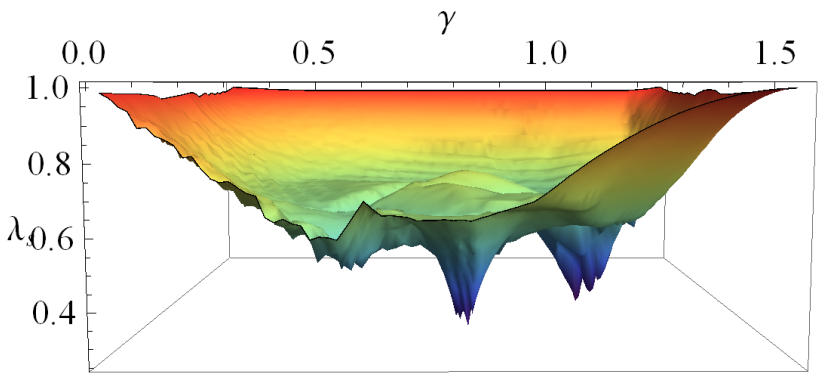


Figure 4.3: Modulus of subleading eigenvalue λ_s (right-hand side view) for steps `step` = 0.01 and `stepP` = 0.05—red colour marks the maximal value of λ_s, blue the minimal one.

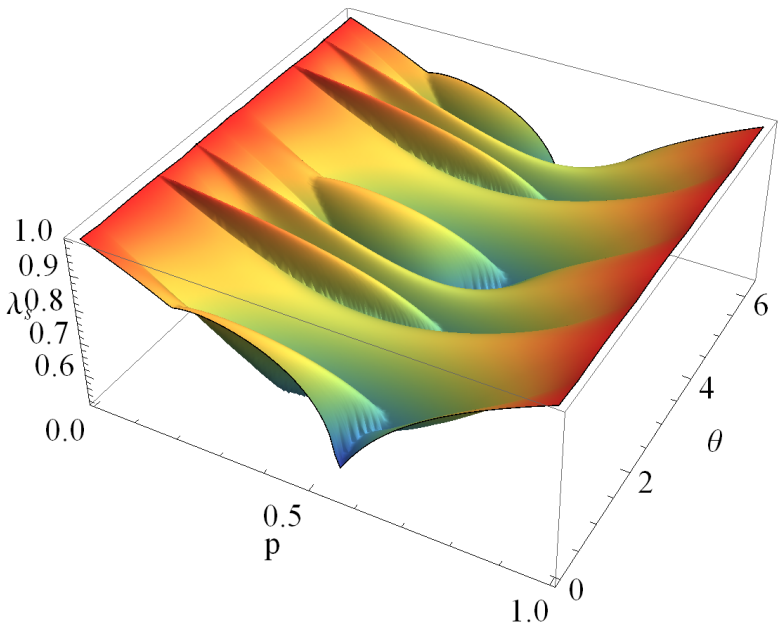


Figure 4.4: Modulus of subleading eigenvalue λ_s for $\varphi = 1.276$, $\gamma = 0.828$ and steps `stepP` $= 0.010$, `stepTheta` $= 0.010$—red colour marks the maximal value of λ_s, blue the minimal one.

parameter values lying far from both regions (4.35). In particular, we use these values

$$\varphi = 0.100,\ \gamma = 0.100,\ \theta = 0.100,\ p = 0.500. \tag{4.37}$$

In the second case we choose values corresponding to the ideal case (4.36). Comparison of both settings can be seen in Figure 4.5. We generate a random density matrix ρ and apply the RUO Φ on it successively, i. e. $\rho(n) = \Phi^n(\rho)$. Parameter d stands for the Hilbert-Schmidt norm of the difference of $\rho(n)$ and ρ_∞ (3.11). In the plot we show the distance d as a function of the number of steps n. It is obvious that $\Phi^n(\rho)$ converges to the twirling (4.5) significantly faster for the ideal choice of parameter values.

As already mentioned the iterative method seems to be quite robust with respect to imperfections of unitaries U_i constituting the RUO Φ which approximates the twirling operation. In order to demonstrate this fact suppose that in each step of the evolution all parameter values specifying the RUO slightly vary from the ideal case (4.36). To describe parameter perturbations we introduce a new parameter Δ. It represents the maximal value by which parameters characterizing the RUO can differ from its ideal counterpart. In Figure 4.6 we can see results obtained for $\Delta = 0.001$ and for the same initial state as in Figure 4.5. Purple dots correspond to the ideal case (4.36), red dots to the varying set of parameter values which differ from the ideal case by $\Delta = 0.001$ at the maximum. By inspection of Figure 4.6 we can see that

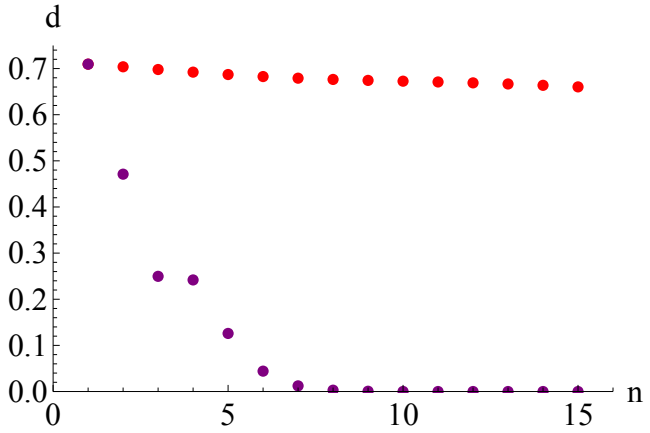


Figure 4.5: Comparison of speed of convergence for two different choices of parameter values describing RUO Φ (4.9); n stands for the number of iterative steps and $d = \|\rho(n) - \rho_\infty\|$. Purple dots correspond to the setting (4.36), red dots to the setting (4.37).

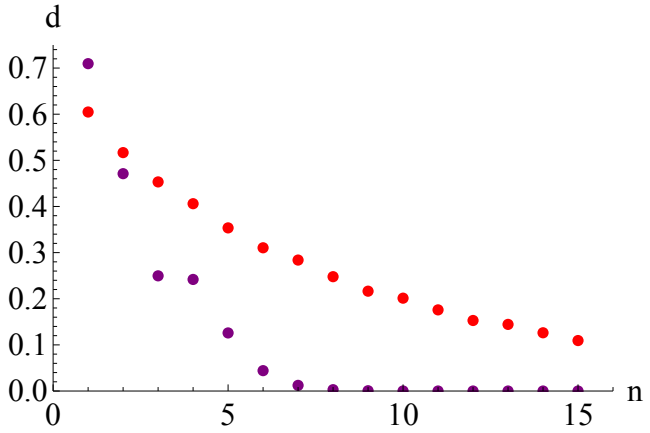


Figure 4.6: Demonstration of evolution with slightly modified RUOs applied in each iterative step; n stands for the number of iterative steps and $d = \|\rho(n) - \rho_\infty\|$. Purple dots correspond to the ideal case (4.36), red dots to the varying set of parameter values which differ from the ideal case by $\Delta = 0.001$ at the maximum.

the disrupted setting with changing parameters converges to the desired state, even though in a slower manner.

In this section we considered the two-qubit twirling operation (4.5) and its implementation by the random unitary operation Φ (4.7). We performed numerical analysis of this setup and presented the most important results.

Chapter 5

Conclusion

General twirling operations represent a useful tool in various fields of quantum information theory. They can be successfully employed in different algorithms such as entanglement purification protocols. In this thesis we have presented a new iterative method which can be efficiently applied to implement the twirling operation. This technique use an appropriate random unitary operation as its key component. In order to provide description of the method in the first chapter we introduced basic terminology and objects studied by quantum information theory. In the second chapter we listed several examples of quantum algorithms, especially quantum entanglement purification protocol.

In the third chapter we studied spectral properties of random unitary operations needed for subsequent discussion. Furthermore, we provided an exact definition of the general twirling operation and its special case useful for applications in quantum algorithms. We presented the original approach of the two-qubit twirling implementation. In the fourth chapter we investigated basic properties of general twirling operations.

On the basis of obtained findings we demonstrated the principle of the iterative method and provided necessary and sufficient conditions a random unitary operation has to satisfy to implement the two-qubit twirling. It turns out that the iterative method for the two-qubit twirling works for a huge class of random unitary operations. Since a rate of convergence of the method is affected significantly by a particular form of the RUO employed we performed corresponding numerical analysis. In the final part of the fourth chapter we showed relation between different values of parameters characterizing the RUO and speed with which the method converges to the two-qubit twirling operation.

Bibliography

[1] M. A. Nielsen, I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2001)

[2] K. G. H. Vollbrecht, R. F. Werner, J. Math. Phys. **41**, 6772 (2000)

[3] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996)

[4] G. Alber *at al.*, *Quantum Information* (Springer, 2004)

[5] R. F. Werner, Phys. Rev. A **40**, 4277 (1989)

[6] C. H. Bennett, G. Brassard, S. Popescu, B Schumacher, J. A. Smolin and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996)

[7] J. Novotný, G. Alber, I. Jex, Cent. Eur. J. Phys. **8**, 1001 (2010)

[8] G. Tóth and J. J. G.-Ripoll, Phys. Rev. A **75**, 042311 (2007)

[9] P. K. Aravind, Phys. Lett. A **233**, 7 (1997)

[10] O. Szehr, D. Reeb, M. M. Wolf, arXiv:1301.4827 [math-ph] (2013)

Appendix A

Tensor Product of Matrices

A tensor product of complex matrices is represented by the *Kronecker product* which is defined as follows. Let $m, n, p, q \in \mathbb{N}$, $A \in \mathbb{C}^{m,n}$ and $B \in \mathbb{C}^{p,q}$, then

$$A \otimes B = \begin{pmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \cdots & a_{mn}B \end{pmatrix}.$$

We list the most important tensor product properties relevant for our purposes.

- The tensor product is bilinear and associative.
- The tensor product of two unitary matrices is unitary.
- Let $A \in \mathbb{C}^{m,n}$ and $B \in \mathbb{C}^{p,q}$ be some matrices, $m, n, p, q \in \mathbb{N}$, then

$$\begin{aligned} (A \otimes B)^* &= A^* \otimes B^*, \\ (A \otimes B)^T &= A^T \otimes B^T, \\ (A \otimes B)^\dagger &= A^\dagger \otimes B^\dagger. \end{aligned}$$

- Let $A \in \mathbb{C}^{m,n}$, $B \in \mathbb{C}^{n,o}$, $C \in \mathbb{C}^{p,q}$ and $D \in \mathbb{C}^{q,r}$ be some matrices, $m, n, o, p, q \in \mathbb{N}$, then the following relation holds

$$(A \cdot B) \otimes (C \cdot D) = (A \otimes C) \cdot (B \otimes D).$$

Appendix B

Jordan Canonical Form

Let $A \in \mathbb{C}^{n,n}$, $n \in \mathbb{N}$. Then there exist a block diagonal matrix J and an invertible matrix T such that $A = TJT^{-1}$ and

$$J = \begin{pmatrix} J_1 & & & \\ & J_2 & & \\ & & \ddots & \\ & & & J_p \end{pmatrix}, \quad \text{where} \quad J_j = \begin{pmatrix} \lambda_j & 1 & & \\ & \lambda_j & \ddots & \\ & & \ddots & 1 \\ & & & \lambda_j \end{pmatrix}$$

and λ_j are (not necessarily different) eigenvalues of A, $j \in \hat{p}$. The matrix J is called the *Jordan canonical form* of A.

The existence of T is equivalent to the existence of the *Jordan basis* $\{Y_{j,k}\}_{j,k}$, $j \in \hat{p}$, $k \in \{1, \dots, \dim J_j\}$. It is formed by generalized eigenvectors of A. In this basis is A represented by the block diagonal matrix J.