ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta jaderná a fyzikálně inženýrská

Chaotická dynamika purifikačních protokolů

Diplomová práce

Bc. Martin Malachov

Vedoucí práce: Prof. Ing. Igor Jex, DrSc.

Praha, 4.5.2015

Poděkování

Rád bych poděkoval prof. Igoru Jexovi za vedení práce a poskytování cenných rad a konzultací. Za podnětné diskuze děkuji také svým mad'arským kolegům, které vede dr. Tamás Kiss. Poděkování patří i rodině a přátelům za jejich podporu.

Prohlášení

Prohlašuji, že jsem svou diplomovou práci vypracoval samostatně a použil jsem pouze podklady uvedené v přiloženém seznamu.
Nemám závažný důvod proti použití 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 ....
podpis

Contents

Abstrakt

Kvantová fyzika s sebou přinesla nové efekty neznámé pro fyziku klasickou. Jedním z nich je kvantové provázání. To umožňuje částicím sdílet v jistém smyslu pouto, které prostřednictvím změření jedné částice dovoluje získat informaci o částici druhé. Proto mohou kvantové bity - qubity v provázaném stavu být použity k zajímavým procesům, například kvantové teleportaci či při superhustém kódování.

Při přenosu qubitu realistickým kvantovým kanálem dochází k narušování provázanosti, proto je třeba procesů, které během kvantové komunikace narušené provázání opraví. Tyto procesy se nazývají purifikační protokoly a využívají měření k žádaným úpravám částic. Měření může vést k nelinearitám. Tato práce se zabývá jedním protokolem, při kterém tyto nelinearity indukují chaotické chování, které jinak v lineární kvantové teorii není přítomné.

Tato práce nejprve shrnuje základní poznatky z kvantové fyziky a informace, teorie chaosu a matematického aparátu. Druhá část práce přidává ke konkrétnímu purifikačnímu protokolu několik modifikací prostřednictvím tzv. twirlingových operátorů. Indukované chaotické chování je studováno s využitím teorie funkcí jedné komplexní proměnné, případné uplatnění v praxi je diskutováno. Během práce je také vytvořen podpůrný matematický aparát a jsou nalezeny zajímavé matematické vztahy.

Klíčová slova: kvantové provázání, qubit, chaos, Juliova množina

Abstract

Quantum physics gives rise to special effects not presented in classical physics, one of them is quantum entanglement. This phenomenon enables particles to share a kind of bond which allows to get information about one of particles by observing another one. Hence quantum analogues of bits - qubits in entangled state can be used for various interesting phenomena, e.g. quantum teleportation or superdense coding.

Entanglement of qubits generally decays when transported through realistic quantum channels, therefore processes for reestablishing of the entanglement during quantum communication are needed. Such processes are called purification protocols, they use measurement to modify particles in desired manner. Measurement can lead to nonlinearities. This thesis handles one particular protocol, for which these nonlinearities induce chaotic behaviour which is otherwise not present in linear quantum theory.

This thesis first aims on gathering and organising current basic knowledge of quantum physics and information, theory of chaos and other mathematical background. In next chapters, the particular protocol is modified by twirling operators. Induced chaotic behaviour is analysed utilising theory of functions of one complex variable, potential for practical use is discussed. Supportive mathematical background is also developed and interesting mathematical connections are found.

Key words: quantum entanglement, qubit, chaos, Julia set

Notation

general algebraic symbols

$\mathbb{F}^{m,n}$	vector space of matrices of order m, n over field $\mathbb{F}$
$\mathscr{H}_A^d$	abstract Hilbert space (corresponding to system A, with dimension d)
$\|\psi\rangle$	vector, element of $\mathscr{H}$
$\langle\phi\|$	covector, element of dual space $\mathscr{H}^*$
$\langle\phi, \psi\rangle$	scalar product of vectors ϕ and ψ, elements of $\mathscr{H}^*$
A	means an operator on $\mathscr{H}$ as well as its matrix representation
A^*	Hermitian adjoint of A (the conjugate transpose $A^* = \bar{A}^T$)
$\mathscr{B}(\mathscr{H})$	space of all bounded operators on $\mathscr{H}$
$\otimes$	tensor product
$\odot$	Hadamard (elementwise) product
$\oplus_n$	addition modulo n
$\ominus_n$	subtraction modulo n

symbolic notation for sets (of operators, matrices, vectors...):

$\mathscr{S}_n$ the set of all permutations of n elements (permutation matrices of order n)

$\mathcal{M} \otimes \mathcal{N} = \{A \otimes B \,|\, A \in \mathcal{M}, B \in \mathcal{N}\}$

$A\mathcal{M} = \{AB \,|\, B \in \mathcal{N}\}$

$\mathcal{M} \circ \mathcal{N} = \{AB \,|\, A \in \mathcal{M}, B \in \mathcal{N}\}$

and so on...

special operator

$S_{m,n} :=$ such an operator that $S_{m,n} \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} = \frac{1}{N} \begin{pmatrix} a_{11}^2 & a_{12}^2 & \dots & a_{1n}^2 \\ a_{21}^2 & a_{22}^2 & \dots & a_{2n}^2 \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}^2 & a_{m2}^2 & \dots & a_{mn}^2 \end{pmatrix}$,

where N is a suitable renormalization factor; specially $S := S_{4,1}$

Chapter 1

Introduction

A world without string is chaos. — *Rudolph Smuntz*

Far away, in times of ancient gods, people were looking to the sky wondering, whether they could only understand secrets which rule the Universe. Even with very limited experimental possibilities they developed philosophies considering atomic character of mass, they found important physical and mathematical relationships (motion of planets, geometry...). Even today with extremely accurate apparatuses, devices of monster or nano sizes we are not able to reveal some eternal mysteries of being.

On the other hand, in the last century physics developed significantly. For example theory of relativity or nuclear sciences, which allowed us to understand life of stars, or geometry and evolution of cosmos. Another part of physics has however gained much more importance, part of physics which handles with measures small beyond imagination. Quantum physics is a great challenge and an important milestone in understanding of the microcosmos. Particle/wave duality was one of the first steps to a revolution of human thinking. Various unprecedented phenomena were theoretically derived and these sometimes denied seemingly unshakable perception of reality. Through years, many of these microcosmos effects were observed and thus have confirmed some of the quantum theory predictions. Moreover, quantum concept (for example in [1]) has also brought explanation for some problems of classical physics (spin).

At the very beginning of the last century, Max Planck explained light spectra of atoms using not continuous energies but only discrete quanta. Niels Bohr with his first quantum model of atom has tried to clarify existence of electrons in atom shells. Many physicists and mathematics started to develop a brand new quantum theory. Heisenberg, Dirac and other theoretical physicists and mathematics are responsible for mathematical construction of this theory. Schrödinger's equation has become a symbol for quantum success for physicists and Schrödinger's cat has become a symbol of strangeness of quantum theory for all people.

During the first half of the 20^{th} century, basic concept of quantum theory was finished and many famous people participated in finding and reasoning consequences of the quantum theory. Even Albert Einstein has contributed and his name is connected with the Einstein-Podolsky-Rosen paradox [2], which is in fact the historical origin of the reason for this thesis. Quantum physics is a source to a new phenomenon - the *quantum entanglement* [3]. This feature is connected with formal definitions in Hilbert spaces. When taking a system composed of two subsystems, there can be found such states that cannot be decomposed into two separate substates. This property has

serious consequences: Two entangled particles are bound in a way that one contains information about the other. When one particle is measured, the wave function of the other collapses. This information is transferred instantaneously without any respect to time and distance and thus seem to contradict theory of relativity. Einstein hoped this conflict to be explained by theory of hidden variables. That is, particles are sharing some non observable parameters that determine their behaviour even when they are not in contact. This can be simply said in the manner that entangled particles agree from the very beginning to this seemingly entangled behaviour. They would then exhibit this exotic behaviour but in fact information about particles would travel with sublight speed together with both particles since their entangling.

In the seventies, John Bell challenged the theory of hidden variables [4]. He proposed series of experiments which proved that hidden variables theory is not correct. His electrons showed entangled behaviour as foretold by quantum theory. Quantum entanglement can be viewed as a fact that makes structure of our physical world more complicated but also more exciting.

With progresses in computation and information theory, physicists started to think of a computer based on quantum physics principles. It took some time before they realised that entanglement can be a very powerful tool for quantum computation and information. Indeed, such a bond between two particles could be used to some desired state alteration that enhances information processing. Up today, many practical applications have been proposed. Lets name here quantum teleportation, super-dense coding, number factorisation or various problems in quantum cryptography. These topics make quantum information and computation very interesting and promising.

Alas, there are some problematic issues in these new branches of science. Quantum theory itself brings some issues (e.g. impossibility to copy a state) but other problems are connected to realistic realisation of quantum computers. Our technologies are inferior to employ much advantages of the quantum computation, some of the biggest problems are: reliable source of particles used as information carriers, realisation of gates for information processing, the noise. Realistic channels for information transmitting cause the entanglement to decay. Even if this noise might be somewhat diminished in the future, it will be always present and thus processes to restore the entanglement are needed. These process of entanglement restoration are usually referred to as *quantum purification* or *quantum distillation*[5].

Purification protocols generally work in a following way: We take a big system of particles and we measure some of them (this may destroy the quantum information state of the particle) in order to get some information of the system. This information we use to modify the system back to a more entangled state. Many purification protocols have already been proposed, mostly they are suitable for special situations (purification of only special sets of states, purification for ion traps, ...). Practical realisation of the protocols may be very difficult or even (with contemporary level of technology) impossible at the moment.

As purification protocols use the measurement of some of the particles, this has important consequences. Quantum theory is a linear theory up to the moment we measure the system. Outer interventions typically break linear behaviour and nonlinear features are brought to the system. Purification protocols are in fact a way to use this effect for our purposes. However, nonlinear behaviour induced in the system may have unpredicted effects. It is therefore important to study the exact behaviour of

purification protocols. Recent articles [6–8], prove that chaotic behaviour may be induced. Chaos in the sense of sensitivity to initial conditions is a new feature to quantum theory.

Mathematics and physics started to explore new unknown waters at the beginning of the last century. Starting with Poincaré's work on celestial mechanics, soon it was clear that some mathematical and physical problems posses very unpredictable behaviour. Theory of chaos arose. As an example of a chaotic behaviour, lets mention so called logistic map [9] $f_r : (0,1) \to (0,1); r \in (0,4)$

$$f_r(x) = rx(1-x) \tag{1.1}$$

When iterating this function on x_0 and $x_0 + \varepsilon$, we suppose we get different results. However for almost any parameter $r > 3.6$ the results seem totally random, not depending on ε. This extreme sensitivity to initial conditions is a typical feature of chaos. Many others examples of chaotic behaviour were found. Some of them are the most fundamental problems of our everyday life (weather, financial market,...).

Another theory touched chaos not long after the first progresses of the chaos theory. Two French mathematicians, Julia and Fatou investigated functions of one complex variable. Despite the fact they had no computer in possession, they developed admirable theory which is today mostly connected with the word "fractal". Sadly, they could never see the beautiful results of their work.

In this work we try to bring together theory of chaos and purification protocols. Because of the extensive scopes of connected theories, we would like to introduce the reader to the most basic facts in the theoretical chapter. Quantum physics is established postulatively and then issues of quantum information and computation are discussed in detail. Quantum entanglement purification with inspection of studied protocol is accented. Matters of chaos in physics and mathematical definition are briefly discussed. Theory of one complex variable is then presented mentioning the most elementary tools needed to handle at least a little bit of the chaos that emerges in next chapters.

In the next two chapters we try to modify given purification protocol with different local twirling operators. At first (chapter 3), we summarise information of one already examined operator, formed of Hadamard gate. Next, we generalise the situation using tensor product of special one-qubit unitary matrices (rotations). We develop long theory to simplify examinations of bigger amount of operators at once. Dynamics of 16 considerable Hadamard matrices is showed to be similar to the already known behaviour of the first operator. Pauli matrices are then involved into consideration. Another two new dynamics are determined.

In the second of the non-theoretical chapters (chapter 4), more general rotation matrices are used to form new groups of local twirling operators. Knowledge of special cases is used. New dynamics are obtained.

The author hopes that this thesis will serve for readers who are new to the topics and will give them basic information about the issues. However, experienced reader should also find new and interesting information from the field. The thing is that question of truechaos in quantum physics is brand new.

Chapter 2

Theory

This chapter summarizes basic theoretical concepts that are essential for the following work. First of all, it describes basic definitions and terminology connected to linear and nonlinear operators. Then it reminds the postulative character of quantum physics and introduces mathematical background connected to this particular branch of physics. Special attention is then payed to quantum information and computation, disciplines that have a potential to make a revolution in information technologies. Finally, space is given to mathematical theories and concepts from chaos theory that are needed for this work.

2.1 Mathematical background and formalism

At first, lets remind the reader some basic terms, definitons, notations etc. We work with complex vector (Hilbert) spaces, we will always be restricted to spaces of finite dimensions, usually 2 or 4. Issue of infinite dimensions is peripherally mentioned in 2.2 but only as a formal issue.

Concerning complex numbers $z = re^{i\varphi} \in \mathbb{C}$, we call r the magnitude and φ the phase of z.

For linear operators, there is an established machinery with eigenvalues, eigenvectors and so on. This thesis handles nonlinear operators and so we have to generalise and also present some own terminology. Iterative application of nonlinear operators simply does not oblige usual behaviour known from linear theory but analogues of eigenvectors do exist. In this thesis we call vectors satysfying

$$A\left|\psi\right\rangle = \lambda\left|\psi\right\rangle \tag{2.1}$$

fixed states. It is due to the quantum character of vectors and their correspondence to physical states, see more in paragraph 2.2.

Sequence

$$\left|\psi\right\rangle, A\left|\psi\right\rangle, A^2\left|\psi\right\rangle, \ldots \tag{2.2}$$

is called the *orbit* of $\left|\psi\right\rangle$¿

A *cycle* is taken to mean a sequence of vectors

$$\left(\left|\psi\right\rangle, A\left|\psi\right\rangle, A^2\left|\psi\right\rangle, \ldots, A^{n-1}\left|\psi\right\rangle\right) \tag{2.3}$$

while $A^n |\psi\rangle = |\psi\rangle \neq A^k |\psi\rangle$ for $k \in \widehat{n-1}$. Such n is called the *length* of the cycle or *period*. These terms are chosen to correlate with the theory of one complex variable ([10], [11]), which this thesis also relies on.

Unitary matrices play crucial role in the quantum theory. We call an unitary element $U \in \mathbb{C}^{2,2}$ *rotation*. That is of course because of the link to physical rotation, however this is a little bit hidden in complex variables. Rotation is up to a global phase (mutiplication by a complex number with magnitude 1) described by three angles, let us denote them $\varphi, \vartheta_1, \vartheta_2$. Rotation matrix than looks like

$$R_{\varphi,\vartheta_1,\vartheta_2} = \begin{pmatrix} e^{i\vartheta_1}\cos\varphi & e^{i\vartheta_2}\sin\varphi \\ -e^{-i\vartheta_2}\sin\varphi & e^{-i\vartheta_1}\cos\varphi \end{pmatrix} \tag{2.4}$$

One special case of rotation is obtained when $\vartheta_1 = 0 = \vartheta_2$. We see that $R_{\varphi,0,0}$ is indeed a usual rotation.

$$R_{\varphi,0,0} = \begin{pmatrix} \cos\varphi & \sin\varphi \\ -\sin\varphi & \cos\varphi \end{pmatrix} \tag{2.5}$$

Another special rotations belong to an interesting set of matrices, *Hadamard matrices*. These are defined as follows: Matrix $H \in \mathbb{C}^{n,n}$ is Hadamard matrix if $(\forall i, j \in \hat{n})(H_{ij} \in \{1, -1\})$ and $HH^T = n\mathbb{1}$. A whole theory is devoted to this type matrices because of their convenient properties, see more in appendix C. Following matrices are all Hadamard matrices of order 2.

$$H_1 := \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{2.6}$$

$$H_2 := \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \tag{2.7}$$

$$H_3 := \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \tag{2.8}$$

$$H_4 := \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix} \tag{2.9}$$

Another set of special rotations are Pauli matrices. In spite of usual definitions, we do not care for global factor because of quantum character of this work that is described in 2.2.

$$\sigma_1 := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{2.10}$$

$$\sigma_2 := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \tag{2.11}$$

$$\sigma_3 := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{2.12}$$

$$\sigma_4 := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{2.13}$$

Relations between angle choices and mentioned matrices is demonstrated below

$$H_2 = R_{\frac{\pi}{4},0,0}, H_3 = R_{\frac{3\pi}{4},0,0}, \sigma_2 = -R_{\frac{\pi}{2},0,0}, \sigma_4 = R_{0,0,\vartheta_2} = \mathbb{1}, \dots \tag{2.14}$$

Operators on $\mathbb{C}^{2,2}$ mentioned so far will be sufficient for this thesis. That is because we are interested in operators on $\mathbb{C}^{4,4}$ and we would like to construct them form these operators using tensor product, see appendix A. We shall denote

$$S_{ij} = \sigma_i \otimes \sigma_j \tag{2.15}$$
$$H_{ij} = H_i \otimes H_j \tag{2.16}$$
$$M_{ij} = H_i \otimes \sigma_j \tag{2.17}$$
$$W_{ij} = \sigma_i \otimes H_j \tag{2.18}$$

2.2 Brief introduction to quantum physics

Hilbert space is a big space. — *Carlton Caves*

In this paragraph, the basic facts from quantum theory [1], [12] are introduced, including historical notes [13]. As a revolution in physics, we would like to give more space to it but we shall try to not surpass the scope related to the topic of the thesis.

Quantum physics was established at the beginning of the last century. Starting with works of Max Planck[1] who studied black body radiation [14] and later with work of Niels Bohr[2] who forged the first quantum model of atom [15], quantum theory started to develop its position of one of the most important philosophies of physics. Manifestation of quanta, a discrete world instead of the continuous has shaken pillars of classical physics and its instrumental use of mathematics. Mortal strike to classical view of matter was dealt by de Broglie [3] in [16], who claimed that elementary particles have not only their corporeal structure but also act as waves.

This evolution to an abstract wave in some abstract space started building of quantum theory as we know it today. Later, Max Born[4] linked this wave with its actual physical meaning - its magnitude corresponds to the probability of finding of particle within certain phase space cell. In 1926, one of the most famous relationship was derived in work [17] of Erwin Schrödinger[5]. His wave equation connected time evolution of a wave with Hamiltonian of the system and thus brought microcosmos to living.

[1]Max Karl Ernst Ludwig Planck, 1858-1947; talented German physicist, one of the first who understood great importance of theory of relativity; started with thermodynamics. He was the first to use discrete quanta and thus justified his equation for black body radiation. Nobel prize in 1918.

[2]Niels Henrik David Bohr, 1885-1962; Danish, son of professor of mathematics, good football goalkeeper. He devoted his life to atoms, studied their transmutation, tried to explain thermal expansivity, electrical and magnetical properties of metals. Developed the first (and accepted) quantum model of atom with electrons on stable trajectories. Awarded Nobel prize in 1922.

[3]Louis Victor Pierre Raymond de Broglie, 1892-1987; French aristocrat. Realised that electrons act as wave and introduced general corpuscular-undulatory dualism. Derived relations and equations for "massive wave", core of the dualism. Nobel prize in 1929.

[4]Max Born, 1882-1970; German physicist, friend of Einstein and Heisenberg. He developed matrix mechanics and connected probability density with quantum formalism. Nobel prize in 1954.

[5]Erwin Schrödinger, 1887-1961; Austrian physicist and mathematician. He defined wave function, key term of quantum mechanics. Derived famous equation for time evolution of wave function. Developed a whole new theory - wave mechanics and proved its equivalence with matrix mechanics. Famous for his thought experiment with a cat. Nobel prize in 1933.

Further quantum surprise was made by Werner Heisenberg [6] who in [18] derived restriction on possible correlations between two observables. His uncertainty principle has erased idea of phase space of classical physics. We are condemned to rely on "probabilities clouds" when describing a physical system. Thanks to this transformation of physics one could make such an progress in electron microscopy, lasers and many others part of common business of contemporary technology.

Another great man of the quantum theory was Paul Dirac [7] who integrated mathematical formalism of Schrödinger and Heisenberg and unified them into a consistent mathematical theory. He also introduced widely used bra-ket notation and proposed quantum equation for $1/2$ spin particles which later led to discovery of the antiparticles.

New particles became a mantra of physicists. Quantum theory developed further to give explanations for new discoveries of atomic and subatomic nature. Probably the most important person of the quantum physics of the second half of the last century was Richard Feynman[8]. He and few others established quantum electrodynamics, new level of physics. He also gave the quantum theory very illustrative and powerful tool, the Feynman diagrams.

Research and further development gave rise or at least inspired few deeply specialised and maybe exotic contemporary theories (e.g the string theory, quantum information) but as a whole, quantum physics still have some flaws (quantum gravity). Thus we are still motivated to improve the quantum physics, branch of science that shook the world.

Now lets start with the postulative definition of quantum physics. That is, we declare that following mathematical apparatus indeed describes our physical world. First of all, it is necessary to determine mathematical structure suitable for our needs.

Axiom (P1a)**.** *There is a separable complex Hilbert space $\mathscr{H}$ corresponding to the given quantum system.*

Axiom (P1b)**.** *There is a ray in $\mathscr{H}$ corresponding to the given state of considered system.*

This means, that (mathematically) the world where we live is *a complete topological space*, which is furthermore *equipped with scalar product*. As will be soon seen, this scalar product plays crucial role in probability character of quantum physics. Space $\mathscr{H}$ from P1a is called the *state space*. It is important to understand that $\mathscr{H}$ is not composed of vectors such that each one would correspond to some physical state. A physical state is instead represented by *one-dimensional subspace* of the state space. Should we denote the ray representing given state Ψ, we can reduce this complication representing the whole subspace as a (complex) linear envelope of one vector $|\psi\rangle \in \Psi$.

[6] Werner Karl Heisenberg, 1901-1976; talented German theoretic and mathematician. Developed observable formalism, implemented matrix computation into mechanics and used it to derive famous uncertainty principle. He has in fact built quantum mechanics. Nobel prize 1932.

[7] Paul Adrien Maurice Dirac, 1902-1984; English theoretic with Swiss roots. Discoverer of half-integer spin particles and Dirac equation. He forecast antiparticles, improved and generalised formalism of quantum mechanics. Nobel prize with Schrödinger in 1933.

[8] Richard Philips Feynman, 1918-1988; American physicist, one of the greatest man of modern physics. Besides quantum electrodynamics and other quantum branches, he participated in nuclear research. Famous for his personality, brilliant intuition. He brought closer quantum physics and public with his popular lectures. Nobel Prize in 1965.

Because of equation simplification, this vector is usually furthermore chosen to satisfy $|| \, |\psi\rangle \, || = 1$, although this condition is not necessary - state can be represented by any its element! Due to the complexness of $\mathscr{H}$ there are infinitely many unit vectors, they differ in phase factor $e^{i\varphi}$. Arbitrarity in the choice of representing vector will be abundantly exploited in this thesis.

In the quantum physics, one fact is vital and this fact is also crucial for this thesis. Measurements influence the state of the system. When performing a measurement of some observable on a state Ψ, system is transformed into some state Φ. For unit vectors $|\psi\rangle, |\phi\rangle$ representing these states, number $P(\Psi, \Phi) = |\langle\psi \,|\, \phi\rangle|^2$ has the meaning of *transition probability*, i.e. probability, that system undergoes the change from Ψ to Φ because of the measurement. This probabilistic character (measurement results are not certain) is another typical feature of quantum theory.

Scalar product enables us to search for orthonormal basis of $\mathscr{H}$, let us name one $\{|\phi_j\rangle\}_{j=1}^N$, where $N \in \mathbb{N} \cup \{+\infty\}$ generally. Any vector can thus be written as

$$|\psi\rangle = \sum_{j=1}^{N} \langle\phi_j \,|\, \psi\rangle \, |\phi_j\rangle \overset{label}{=} \sum_{j=1}^{N} c_j \, |\phi_j\rangle \,. \tag{2.19}$$

This equation means that transition probabilities for $|\psi\rangle \to |\phi_j\rangle$ are $p_j = |c_j|^2$ and of course $\sum_{j=1}^N |c_j|^2 = 1$. Numbers $\{c_j\}_{j=1}^N$ are called *Fourier coefficients* of vector $|\psi\rangle$ with respect to the basis $\{|\phi_j\rangle\}_{j=1}^N$.

Now we need to properly introduce observables and their connections to values that can be measured. For that we have to present concept of identity decomposition and projection-valued measure. Only brief overview and basic definitions are given here, details can be found in [1] or its english version [12]

Definition 2.2.1 (Projection)**.** Projection *is such an operator E on $\mathscr{H}$ that $Dom(E) = \mathscr{H}$, $E = E^*$ and $E = E^2$.*

It is possible to define an operator on $\mathscr{H}$ in a following way:

$$A = |\psi\rangle \, \langle\phi| \,, \tag{2.20}$$

where $|\psi\rangle, |\phi\rangle \in \mathscr{H}$. When orthonormal basis $\{|\psi_i\rangle\}_{i=1}^N$ of $\mathscr{H}^N$ is chosen, particular operators can be constructed according to 2.20 and combined, we obtain so called *completeness relation*:

$$\sum_{i=1}^{N} |\psi_i\rangle \, \langle\psi_i| = \mathbb{1}. \tag{2.21}$$

With two orthonormal bases $\{|\phi_i\rangle\}_{i=1}^N$ and $\{|\psi_i\rangle\}_{i=1}^N$ of $\mathscr{H}^N$, any given operator A on $\mathscr{H}^N$ can be expressed as

$$A = \mathbb{1}A\mathbb{1} = \sum_{i,j=1}^{N} |\phi_i\rangle \, \langle\phi_i| \, A \, |\psi_j\rangle \, \langle\psi_j| = \sum_{i,j=1}^{N} \langle\phi_i| \, A \, |\psi_j\rangle \, |\phi_i\rangle \, \langle\psi_j| \,, \tag{2.22}$$

A is then said to have matrix elements $\langle\phi_i| \, A \, |\psi_j\rangle$ with respect to input basis $\{|\psi_i\rangle\}_{i=1}^N$ and output basis $\{|\phi_i\rangle\}_{i=1}^N$.

Suppose now $\mathscr{H}_1^M$ subspace (of $\mathscr{H}^N$) with orthonormal basis $\{|\phi_i\rangle\}_{i=1}^M$. Operator $P : \mathscr{H} \to \mathscr{H}_1$ can be defined as

$$P = \sum_{i=1}^{M} |\phi_i\rangle \langle\phi_i| . \tag{2.23}$$

It is not difficult to find out, that this operator is a projection and it is not dependent on the choice of the $\mathscr{H}_1$ basis. It projects any vector $|\psi\rangle$ from $\mathscr{H}$ into the subspace $\mathscr{H}_1$ and thus separates $\psi = \psi_1 + \psi^\perp$ where $\psi_1 \in \mathscr{H}_1$, $\psi^\perp \in \mathscr{H}_1^\perp = \mathscr{H}^N \setminus \mathscr{H}_1^M$. This subspace $\mathscr{H}_1^\perp$ is usually called orthogonal complement of $\mathscr{H}_1$ and has dimension $N - M$.

Extreme caution is needed when handling spaces of infinite dimensions! We now switch to "continuous formalism":

Definition 2.2.2 (Projection-valued measure)**.** *Let us label $\mathcal{B}$ the σ-algebra of all Borel sets on $\mathbb{R}$. Map $E(.) : \mathcal{B} \to \mathscr{B}(\mathscr{H})$ is called* projective-valued measure *on $\mathbb{R}$ with values in $\mathscr{B}(\mathscr{H})$ if*

1. *$\forall M \in \mathcal{B}$, $E(M)$ is a projection,*
2. *$E(\mathbb{R}) = I$,*
3. *for any at most countable system $\{M_n\} \subset \mathcal{B}$ equality*

$$E(\bigcup_n M_n) = \sum_n E(M_n)$$

is satisfied. For infinite system, the sum is substituted with the strong limit of partial sums.

Note 2.2.3. *Projection-valued measure can be defined more generally on measurable spaces. It is also called the spectral measure.*

Definition 2.2.4 (Unity decomposition)**.** *Map $E_t : \mathbb{R} \to \mathscr{B}(\mathscr{H})$ is called* decomposition of unity *(spectral decomposition) if*

1. *$(\forall t \in \mathbb{R})$($E_t$ is a projection),*
2. *$(\forall t \in \mathbb{R})(\underset{u\to t+}{\text{s-lim}}\, E_u = E_t)$,*
3. *$\underset{u\to-\infty}{\text{s-lim}}\, E_u = \Theta \wedge \underset{u\to+\infty}{\text{s-lim}}\, E_u = \mathbb{1}$*

Lemma 2.2.5. *Let $\{E_t\}$ be a unity decomposition, B bounded operator. If B commutes with $\{E_t\}$, it also commutes with any $E_{a,b} := E_b - E_a$.*

Of course, each projection-valued measure determines some unity decomposition. Exact relationship is given by

Proposition 2.2.6. *Each unity decomposition generates exactly one projection-valued measure on $\mathbb{R}$ with values in $\mathscr{B}(\mathscr{H})$. This assignment is a bijection of the set of all unity decompositions and the set of all projection-valued measures on $\mathbb{R}$ with values in $\mathscr{B}(\mathscr{H})$.*

Theorem 2.2.7 (Spectral theorem for self-adjoint operators)**.** *For each self-adjoint operator A there is one and only one projection-valued measure $E^A(.)$ on $\mathbb{R}$ such that*

$$A = \int t \, dE^A(t) \tag{2.24}$$

Note 2.2.8. *Using the preceding proposition we see there is a corresponding unity decomposition E_t^A.*

For finite dimensions (discrete situation), spectral theorem tells $A = \sum_{i=1}^{N} \lambda_i \left|i\right\rangle \left\langle i\right|$ where λ_i are eigenvalues of A and $\{\left|i\right\rangle\}_{i=1}^{N}$ is basis formed from the eigenvectors corresponding to eigenvalues $A\left|i\right\rangle = \lambda_i \left|i\right\rangle$.

Now we can proceed and introduce the observables.

Axiom (P2a)**.** *An observable of the physical system is represented as some self-adjoint operator on the corresponding $\mathscr{H}$.*

Axiom (P2b)**.** *Possible values for measurement of observable A are elements of the spectrum of A.*

Axiom (P3a)**.** *For operator A, probability that a value from $(a, b) \subset \mathbb{R}$ is measured on a state described by unit vector $\left|\psi\right\rangle$, is equal to $p = \int_a^b 1 \, d\left\langle \psi \,\middle|\, E_t^A \psi \right\rangle$.*

Axiom (P3b)**.** *The mean value of an observable A on a state given by unit vector $\left|\psi\right\rangle$ is $\left\langle A\right\rangle_\psi = \left\langle \psi \,\middle|\, A\psi \right\rangle$.*

Axiom (P3c)**.** *Let a state of the system be determined by $\left|\psi\right\rangle$, A be an observable. When measured A has the result in (a, b), system is transformed due to the measurement to a state described by $E_A(a, b)\left|\psi\right\rangle$. If measured result is not from (a, b), system ends up in a state determined by $(\mathbb{1} - E_A(a, b))\left|\psi\right\rangle$.*

It is obvious that the decomposition of unity applies here as $\left\langle \psi \,\middle|\, A\phi \right\rangle = \int t \, d\left\langle \psi \,\middle|\, E_t^A \phi \right\rangle$ and truly $\left\langle \psi \,\middle|\, E_t^A \phi \right\rangle$ forms a measure on $\mathbb{R}$. Because we can measure only values from the spectrum of the corresponding operator, it is only natural that we demand it to be self-adjoint, this restricts measured values to be real.

Let us now present an example of a system described in quantum mechanics; we would like to study an electron. For its position and momentum, there is a Hilbert space but when we want to study only spin, there is another Hilbert space describing our "system". When studying all at once, there is another Hilbert space again. This corresponds to an ambiguity in the state space definition. Sometimes, system is described only to capture some of its properties, sometimes the system can be viewed as a part of some bigger system. We usually suit the Hilbert space to our needs. Consider pions π^+, π^-, π^0. They can be viewed as three particles but also as a single particle with three possible states of existence.

For this moment, let our system be determined by spin states of electron. Hilbert state corresponding to this system is $\mathbb{C}^2$. Projection of the spin into j-th axis is represented by Pauli matrix (in correct form, not 2.10-2.13; Planck constant set to 1):

$$S_j = \frac{1}{2}\sigma_j \tag{2.25}$$

These operators have simple spectrum $\sigma(S_j) = \{\frac{1}{2}, -\frac{1}{2}\}$, spectral decomposition has form $S_j = \frac{1}{2}E_j^+ - \frac{1}{2}E_j^-$ where $E_j^\pm = \frac{1}{2}(\mathbb{1} \pm \sigma_j)$. Lets suppose that the system is in a state described by $|\psi\rangle$. When measuring observable S_j, we can only get eigenvalues, that is $\pm\frac{1}{2}$. Probabilities of measuring these values are equal to the transition probabilities $w(\pm\frac{1}{2}; |\psi\rangle, S_j) = \langle \psi \,|\, E_j^\pm \psi \rangle$. Obviously $w(+\frac{1}{2}; |\psi\rangle, S_j) + w(-\frac{1}{2}; |\psi\rangle, S_j) = 1$. The mean value is equal to $\langle S_j \rangle = \frac{1}{2}w(\pm\frac{1}{2}; |\psi\rangle, S_j) + (-\frac{1}{2})w(-\frac{1}{2}; |\psi\rangle, S_j)$ which indeed is equal to $\langle \psi \,|\, S_j \psi \rangle$.

Another, very similar system is a photon with its horizontal/vertical polarisation, it is associated to $\mathbb{C}^2$ Hilbert space as well.

As we have already mentioned, measurements affect the quantum system projecting it on some state. Problematic nature of this situation can be simply viewed on following exaggerated examples: When checking the position of Jupiter, we need some photons that are reflected from its atmosphere to our telescope. Jupiter is however so massive that impact and reflection of a few photons does not influence visibly its position nor momentum. When checking the position of atom within electron microscope, electron can have such energy that it can change the state of the atom. We do not mean only excitation of some valence electrons but the whole atom can be shot out of its crystal lattice. Such measurement drastically afflicts the position and momentum of the observed particle.

From P3a it is also obvious that if we measure a value from (a, b), we obtain value from (a, b) in the subsequent measurement. This property is easily seen from projection property $P = P^2$. However, when measuring two observables A_1, A_2, it is possible that sets of eigenvectors do not coincide. In that case it is possible that state $|\psi\rangle \in \mathscr{H}$ is changed due to first measurement somehow and next measurement results into some state $|\psi_1\rangle \sim \sigma(A_1)$. When measuring A_2 first, $|\psi\rangle$ is changed and after measurement of A_1 it is converted into $\sigma(A_2) \sim |\psi_2\rangle \neq |\psi_1\rangle$. We obtain two different results after two same measurements up to ordering.

Because of this effect it is suddenly important in which order the measurements of different observables are performed. This property is connected with *commutator* ($[A, B] := AB - BA$; bilinear, antisymmetrical operation on $\mathscr{B}(\mathscr{H})$ satisfying Jacobi identity; extreme caution must be taken when handling operator domains). For the purpose we define

Definition 2.2.9. *Observables A, B are compatible, if their commutator $[A, B] = 0$.*

Compatible observables can be measured in any sequence and results will be the same. Unfortunately, many observables do not commute. Even position and momentum cannot be simultaneously measured precisely. The measure of how much trouble is caused due to this effect is hidden in a very important and also interesting relationship called *uncertainty principle* [18]. This correlates variances of two variables A_1, A_2 measured on a state Ψ with unit $|\psi\rangle$:

$$(\Delta A_1)_\Psi (\Delta A_2)_\Psi \geq \frac{1}{2} \langle \psi \,|\, i[A_1, A_2]\psi \rangle \tag{2.26}$$

This relation does not allow two non-compatible observables to be measured with arbitrary small precisions simultaneously. For position and momentum relation reduces

$$(\Delta Q)_\Psi (\Delta P)_\Psi \geq \frac{\hbar}{2} \tag{2.27}$$

This inequality is known as Heisenberg relation. Generally, uncertainty principle has one simple but the more grave consequence. It is impossible to copy a state. If we could copy a state, we would produce sufficiently big amount of copies and thus could precise our measurement beyond limit established by 2.26. However, nothing interdicts us from producing the same states, for example in the Stern-Gerlach apparatus.

States that have been described so far are called *pure* because they simply are some rays in the state space. However, sometimes we don't know exactly the state, we only know probabilities that system is in which one particular state. Such statistically described state is called *mixed*. We modify relevant axioms to suit this condition but we will see that this thesis mostly handles pure states and thus already given axioms are sufficient.

Axiom (P1b)**.** *For a state of the physical system $\mathscr{H}$, there is a corresponding statistical operator ρ on $\mathscr{H}$.*

Axiom (P3a)**.** *Probability that value from $(a,b) \subset \mathbb{R}$ for observable A is measured is equal to $p = Tr(E^A_{(a,b)}A)$. If result is from $(a,b) \subset \mathbb{R}$, state after measurement is described by statistical operator $\rho' = \dfrac{E^A_{(a,b)}\rho E^A_{(a,b)}}{Tr(E^A_{(a,b)}\rho)}$.*

Axiom (P3b)**.** *Mean value of an observable A on a state given by ρ is $\langle A\rangle_\rho = Tr(A\rho)$.*

When we have a system that can be in one of states $|\psi_i\rangle$ with probability p_i, statistical operator associated to this mixed state is expressed as

$$\rho = \sum_i p_i \left|\psi_i\right\rangle \left\langle\psi_i\right| \tag{2.28}$$

Statistical operator is often called density operator (matrix). That is of course because the sum/integral of probability density for some distribution is equal to 1, trace of density matrix is also 1 (trace is a norm on square matrix spaces). Pure state can be also viewed as a special case of the mixed states. We can simply distinguish pure and mixed states from their matrix form because $\mathrm{Tr}(\rho^2) = 1$ for the pure states and $\mathrm{Tr}(\rho^2) < 1$ for the mixed states.

Let us suppose now that we have systems A, B with $\mathscr{H}_A$, $\mathscr{H}_B$ corresponding to them respectively. There is a scheme allowing us to construct space $\mathscr{H}$ representing system composed of the subsytems A and B. This procedure is based on tensor product. For general matrices of arbitrary dimensions, tensor product is defined in A. For states of subsystems represented by $|\psi\rangle, |\phi\rangle$, global state is equal to $|\psi\rangle \otimes |\phi\rangle$. Any two observables A_1, A_2 on the subsystems can be composed into a formal observable $A = A_1 \otimes A_2$. Bases $\{\left|\psi^A_i\right\rangle\}^N_{i=1}$ and $\{\left|\psi^B_i\right\rangle\}^M_{i=1}$ of systems $\mathscr{H}_A$, $\mathscr{H}_B$ can be assembled into a special basis of $\mathscr{H}$ that has form $\{\left|\psi^A_i\right\rangle \otimes \left|\psi^B_j\right\rangle\}^{N,M}_{i,j=1}$. We shall simplify notation: $|\psi\rangle \otimes |\phi\rangle =: |\psi\phi\rangle$.

Statement that $\{\left|\psi^A_i\right\rangle \left|\psi^B_j\right\rangle\}^{N,M}_{i,j=1}$ forms a basis of the composed system tells us that any vector $|\phi\rangle$ of composed system $\mathscr{H}$ can be expressed as $|\chi\rangle = \sum_{i,j} \alpha_{ij} \left|\psi^A_i\psi^B_j\right\rangle$. But we cannot say that there is a single vector $|\psi_A\rangle \in \mathscr{H}_A$ and a single vector $|\psi_B\rangle \in \mathscr{H}_B$ such that $|\phi\rangle = |\psi_A\psi_B\rangle$. State vector for which such vectors do exist is called *separable*. But there are many vectors that cannot be written in this way. These states are called

entangled. That is because such the state cannot be disentangled into subsystems that would correspond to the global state.

When we take two particles which happen to be in an entangled state and one is measured, it also influences the other one. When speaking in wave function terms, we would say the wave function of the other particle collapses due to the measurement of the first one. This fact has grave consequences because measuring of one of the entangled particles can give infomation (about position, momentum, spin, polarisation...) about the others.

Quantum entanglement is a brand new feature of physics induced by its quantum character. When this issue was discussed at first, it seem to be an exotic quantum phenomenon known today as *EPR paradox*. Albert Einstein argumented that this entanglement violates his theory of relativity, lets see why. In 1935, Einstein[9], Podolsky and Rosen published a paper [2] where following thought experiment is conducted: Let us have two particles that communicate together. They get entangled and then they separate and do not communicate anymore. When momentum of one particle is measured (we know we cannot determine its position precisely), the other particle instantenously comes to know its momentum despite it can be far away from the first particle. The information about the momentum traveled through the Universe faster than light. Einstein thought that there must be some hidden parameters that contain information for the case of such situation since particles separation. By measurement of one particle, this parametr realises and determines the momentum of the other. Einstein himself favoured this theory of hidden variables and so he thought that quantum theory is incomplete.

Almost ten years after Einstein's death, in 1964, John Bell came with a statement, that theory of local hidden variables cannot reproduce all predictions given by quantum mechanics and in consequence cannot hold. He derived inequalities which must be satisfied when theory of hidden variables is true. But simple experiment with spins violated these inequalities, [4]. Quantum entanglement suddenly started to be accepted as a new physical fact. Since then, more confirmative experiments have been performed.

Now an example of system with entangled particles is to be presented. Let us consider photons with polarisation, that is either vertical or horizontal. Hilbert space $\mathbb{C}^2$ is associated to it and we shall denote $|\uparrow\rangle, |\rightarrow\rangle$ state vectors of the basal polarisation states. Any state is then a superposition of these states

$$|\psi\rangle = \alpha\,|\uparrow\rangle + \beta\,|\rightarrow\rangle \tag{2.29}$$

which can be asked to satisfy normalisation condition $|\alpha|^2 + |\beta|^2 = 1$. On the other hand, photon of unpolarised light is an example of mixed state. It is an equal superposition of basal states and thus has density matrix

$$\rho = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix} \tag{2.30}$$

Lets now consider light beams, one of vertical and the other of horizontal polarisation. If we take two photons form the first beam, we would surely measure

[9] Albert Einstein, 1879-1955; German legend. Spent his life also in Switzerland, the Czech Republic and the United States. Explained series of physical problems (photoelectric effect, stimulated emission, ...). He contributed significantly to qunatum mechanics, cosmology and many parts other of physics. His greatest achivement is the theory of relativity. He got famous for his work and personality. Awarded Nobel prize in 1921

$\uparrow\uparrow$ values. For two photons from the other beam, we would surely measure $\rightarrow\rightarrow$ values. But when we let the two beams blend and then we take two photons, we can with the same probabilities measure $\uparrow\uparrow$, $\uparrow\rightarrow$, $\rightarrow\uparrow$, $\rightarrow\rightarrow$. We obtain state $|\psi\rangle = \frac{1}{2}(|\uparrow\rangle|\uparrow\rangle + |\uparrow\rangle|\rightarrow\rangle + |\rightarrow\rangle|\uparrow\rangle + |\rightarrow\rangle|\rightarrow\rangle)$. When we apply special operator to this state ($H_1 \otimes H_1$, 2.6), we get $|\psi_1\rangle = |\uparrow\uparrow\rangle$. If this state is further modified by another operator ($\sigma_1 \otimes \sigma_1$, 2.10), it changes to $|\psi_2\rangle = |\rightarrow\rightarrow\rangle$. By blending these two states, one peculiar state is created.

$$\left|\Phi^+\right\rangle = \frac{|\uparrow\uparrow\rangle + |\rightarrow\rightarrow\rangle}{\sqrt{2}}, \tag{2.31}$$

Similar states can be produced by slight modification of the described process:

$$\left|\Phi^-\right\rangle = \frac{|\uparrow\uparrow\rangle - |\rightarrow\rightarrow\rangle}{\sqrt{2}}, \tag{2.32}$$

$$\left|\Psi^+\right\rangle = \frac{|\uparrow\rightarrow\rangle + |\rightarrow\uparrow\rangle}{\sqrt{2}}, \tag{2.33}$$

$$\left|\Psi^-\right\rangle = \frac{|\uparrow\rightarrow\rangle - |\rightarrow\uparrow\rangle}{\sqrt{2}}. \tag{2.34}$$

These states are called Bell states or EPR pairs. They are entangled states, as reader can easily verify that they cannot be decomposed into tensor product of two single-photon vectors. But furthermore, Bell states are maximally entangled states (we do not care for entanglement meaures in this thesis, meaning of "maximally" is left rather to reader's intuition).

2.3 Introduction to quantum information

Quantum information and computation [20] are relatively new branches of science that are superior to classic information theory in some aspects. Their profound idea is to use quantum theory instead of classical physics. Quantum information studies processing tasks performed on machines based on quantum physics, the quantum character is favourably exploited. Not only that some special features of quantum physics are introduced, but even the core of the information - bits are changed to quantum entities. The aim of following paragraphs is to bring basic information about consequences of blending of quantum theory with the information theory and computation. Basic concepts and definitions are given, examples of quantum algorithms are given together with suggestions of practical use of quantum information in the future. More algorithms and detailed information are given in [20] where this paragraph is inspired from.

It is difficult to the beginnings of computer science. Even ancient cultures proposed interesting algorithms and devised interesting structures to accomplish some calculations. However, modern computer science (including electric buzzing squealing winking micro and mega magical boxes) has much clearer beginning. It is deeply associated with the name of Alan Turing[10]. This man published a paper [21] in 1936 where he de-

[10] Alan Mathison Turing, the Codebreaker, 1912-1954; British mathematician, logician, pioneer and father of computation sciences. Known for breaking Enigma code and other great cryptology successes, he also interfered with, philosophy, mathematical biology and marathon runs. Granted posthumous pardon by Queen Elisabeth II in 2013 for being prosecuted for homosexuality

veloped an abstract model of first "programmable computer". This model is therefore called *the Turing machine*. Turing himself also showed that there is a machine that can simulate any other Turing machine, it is *the Universal Turing machine*, and it can perform equivalent algorithm that mirrors same task on any other piece of hardware. This assertion is called Church-Turing thesis and it brings together physical realisation of algorithms with the model of Turing machine.

Breakthrough in computer development happened in 1947 with the invention of transistor. Computer development speed since then is very high but one day it has to slow down because the size of computers will begin to suffer from quantum effects. This is where quantum computation takes its opportunity. Its idea to use quantum mechanics makes it a very powerful instrument. Acording to Turing, classical computer can be used to simulate quantum computer. Nonetheless, Turing never said it would be efficient. Many people believe that this effectivity could never be reached by classical computer development.

An efficient algorithm processes task very fast. Inefficient algorithm needs typically time or other resources depending exponentially on the size of the input. Issues of efficiency naturally ask, if Universal Turing machine can efficiently simulate process. The beginning of analog computers showed that these computers may be more powerful than Turing machine was supposed to be. Later it was cleared that with noise and other realistic environment, analog computers cannot be more efficient than Turing machine. However, question whether there is a machine more efficient than universal Turing machine stayed.

In 1984 David Deutsch [11] wanted to construct stronger Church-Turing thesis that would be based on physical theory and would be as holding as the physical theory itself. He attempted to define a computational device that could efficiently simulate any physical system [22]. Because physical laws are quantum in default, his device is quantum analogue of Turing machine. There is also Universal Quantum Computer. On the other hand it is not clear that this device is the most powerful machine. Very pitoresque effects may emerge in quantum theory and they could reach beyond Deutsch's model and thus allow for an even more powerfull device.

We have not said if this Deutsch's machine is indeed more efficient than Turing's one. During later years Deutsch, Peter Shore and many others have brought many examples of problems that can be solved on a quantum computer efficiently while they are NP-complete problems[12] for Turing's machine. Shor's algorithms [23]for integer factoring and for discrete logarithm are glorious examples. Although search in an unstructured base can be performed on Turing machine in polynomial time, quantum computation gives a nonnegligible speed-up. It is important to ascertain our appreciated reader that still very few is known from quantum information and computation. It is not easy to present a new and good quantum algorithm. Experimental difficulties must be also reduced or eliminated before we can buy a new even more magical miraculous box - quantum computer.

The term quantum information is often used for anything that touches information processing and quantum mechanics. However, we should use this collocation more

[11] David Elieser Deutsch, 1953- ; British physicist with Jewish roots. Proposed qantum computer, developed many quantum algorithms

[12] Problems classically solvable with resources exponentially depending on the size of the input, hierarchy of tasks mentioned later

modestly. It refers to the study of elementary quantum information processing tasks. Its aim is not for example to give details of a specified algorithm because these go beyond "elementary". Nevertheless, when mentioning quantum information theory, we are still interested in experimental application of studied schemes.

There are a few fundamental topics of quantum information. The first one is to identify elementary classes of static resources. Of course, resources found in classical information are relevant for quantum information as well. Another fundamental topic is to identify elementary dynamical processes. Important parts of this goal are: memory, information transmission or noise protection. Another topic of quantum information is naturally to quantify resource tradeoffs during the elementary dynamical processes.

One should reconcile with the fact that classic information is just a special case of the quantum information. Therefore anything (resources, processes...) present in classical information is by default included in the quantum information. But new resources, processes etc. can be found. Lets mention here quantum error correction, problem of distinguishing quantum states, entanglement transformation. Still, question of existence and usability of new resources is without proper answer.

2.4 Qubit

Elementary term of classical information is the *bit*. This is the smallest unit of information and one of the most important resources. Any information can be coded into series of bits. Bit has two levels of existence, in the classical computation systems it is usually represented as an on - off pair. That is especially useful in systems based on electricity but we can represent bit with any two level "system". Plus - minus sign, up - down pairs are also often used especially in written concept and 0 - 1 is almost always used in mathematical parts of information theory (binary numeral system). Another one of many others is yes - no representation, this is illustrative to the fact that any information of the system is obtained by answering a sequence of yes no questions.

Although bit is also a resource for quantum information, there exists a more powerful quantum analogue of a bit. It is called *qubit*. It is a two level system with Hilbert space $\mathbb{C}^2$, but instead of classical bit which exist only as 0 or 1 value, qubit may exist in a superposition of these values (although measured can be oly one of them), thus has the form

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{2.35}$$

with additional condition $\alpha^2+\beta^2 = 1$ [13]. Because of the simplification, we shall identify $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. These indeed form an orthonormal basis of $\mathbb{C}^2$.

Two qubits form space $\mathbb{C}^2 \otimes \mathbb{C}^2 = \mathbb{C}^4$, its orthonormal basis is for example

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \tag{2.36}$$

[13] In this thesis we relieve this condition thanks to the fact that physical state may be represented by any vector from the corresponding ray. We do so because suitable reparametrisation of qubits may lead to significant computation simplifications when handling poynomial equations.

Qubit is however not the only option for a new quantum resource. It is possible to consider more-dimensional entity. This analogue of qubit is called qudit. Binary system is substituted with $\mathbb{Z}$ mod n. Basis is usually labelled $|0\rangle, |1\rangle, |2\rangle, \ldots, |n-1\rangle$.

Qubits can be realised with any two-dimensional system. We have already mentioned photons with vertical/horizontal polarisation, electrons with spin projection, another option is an atom with two levels of excitation. Atoms with more energy levels can serve as qudits.

In classical information, bits (electrical impulses) are transmitted through channels (wires) and processed by logical gates (relays, transistors). A quantum circuit works the same way. Qubits are transmitted through quantum channels (waveguides, particles themselves, time itself, ...) and processed by quantum logical gates.

Shannon[14] defined mathematically concept of classical information and derived few very important statements. One very remarkable deed is that he introduced entropy concept into information sciences [24]. His noiseless channel theorem quantified resources needed to store some information from its source. The noise channel coding theorem than quantifies the amount of information that is possible to transmit through a noisy communication channel. He proposed that error-correcting codes could prevent negative noise effects. This question is very relevant for quantum channels as well. Indeed, the environment afflicts quantum information in worse way than classical information, no noiseless quantum channel does exist. Noise causes decoherency of wave functions, decay of the entanglement. Search for quantum error-correcting code is thus very desired. Some results have been achieved, [20, 25–27].

For actual processing of the information, the role of quantum gates is simple: to change the given information with respect to the input. Example of classical gate is the NOT gate which changes bit 1 to 0 and vice versa. It is in fact the only nontrivial example of single-bit gates. Quantum NOT gate designated by X works similarly, that is qubit $\alpha|0\rangle + \beta|1\rangle$ is changed to $\beta|0\rangle + \alpha|1\rangle$. This operation is well defined, is indeed linear and furthermore unitary as can be seen from matrix representation

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{2.37}$$

In contrast to the classical case, there are more nontrivial single-qubit gates, an example is the Hadamard gate represented by matrix

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \tag{2.38}$$

This gate is also unitary but possesses one special property. It transform basis qubits into their equal superpositions, see more in appendixC. The fact that it can be used for discrete Fourier transform makes it one of the most important and used gates.

The study of properties of single-qubit gates resulted in following statement

Proposition 2.4.1. *Unitarity is sufficient property for a matrix* $\in \mathbb{C}^2$ *to serve as a valid single-qubit gate.*

[14] Claude Elwood Shannon, 1916-2001; American mathematician, engineer and cryptographer, father of the information theory. Credited for digitalisation of computers. Programmed interesting robotic device - Shannon's mouse Theseus which was the first piece of self-learning artificial intelligence. He also proposed a chess playing program and earned a lot of money using the game theory in Las Vegas.

When this is supplemented by

Proposition 2.4.2. *It is possible to build up any single qubit gate using finite set of gates.*

we have described single qubit processing completely.

As for a two-qubit gate example, we present the CNOT (controlled-not) gate

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \tag{2.39}$$

This gate changes the second, the *target qubit* but in contrast to NOT gate, only according to the value of the first, the *control qubit*. This gate is very important as we will see later. In classical case, any process can be performed by composition of NAND gates. However NAND gate (given by the input/output table Tab.1) is irreversible - it is impossible to determine inputs form output and some information is lost by this gate action.

INTPUT		OUTPUT
A	B	A *NAND* B
0	0	1
0	1	1
1	0	1
1	1	0

Tab.1.: The table representing action of the NAND gate

Therefore, it cannot serve as a quantum gate which must be reversible (invertible). CNOT satisfies this and is a universal gate.

Proposition 2.4.3. *Any multiple qubit gate may be composed from the CNOT and single qubit gates. Two-qubit states are thus able to simulate any system.*

Quantum computer can be constructed easily, then we could suspect because no excessive gate arsenal is needed (of course practical realisation of the computer is not easy). Only small set of gates and qubits is needed.

We shall now consider folowing issue. We are discussing qubit as a state that is a combination of bases states of some Hilbert space. Could we change the basis? The answer is positive. Consider an example of a new basis $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}, |-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$. Then $\alpha|0\rangle + \beta|1\rangle = \frac{\alpha+\beta}{\sqrt{2}}|+\rangle + \frac{\alpha-\beta}{\sqrt{2}}|-\rangle$. Of course, the state $|+\rangle$ can be then measured wih probability $\frac{|\alpha+\beta|^2}{2}$ etc. Given any new basis we can express qubit as a linear combination of the states. For orthonormal basis only it is possible to perform measurements with respect to the basis. This observation is connected to one very important fact, it is only possible to apply CNOT gate when having certain orthonormal computational basis. As only in such case we can perform measurement of the control qubit and modify the target one.

Of course, there are some problems connected to the quantum computation. First trouble we get with state indistinguishability. Generally, we can not determine coefficients α, β of unknown qubit superposition. Even infinitely many measurements are

not enough because of probabilistic character of qubit's quantum nature (measurements results into a sequence like 101100101100... which approximately determines mean value, but may not faithfully ascertain probabilities $|\alpha|^2, |\beta|^2$). Thus it is also problematic to distinguish unknown states. This is rigorously proven in [20] but here we just mention a basic mark leading to this fact. Lets assume two states with normalised vectors $|\psi_1\rangle = \alpha_1 |0\rangle + \beta_1 |1\rangle, |\psi_2\rangle = \alpha_2 |0\rangle + \beta_2 |1\rangle$. If we measure these states, we obtain values either 0 or 1. Lets choose $\alpha_1 = 1, \beta_1 = 0, \alpha_2 = \frac{1}{\sqrt{2}} = \beta_2$. Simply told, we can be so unlucky that we measure thousands of zeros and we still cannot decide which state do we have. But of course after measuring a single one, we are certain to have the $|\psi_2\rangle$. We consider worth of notice that some algorithms have been developed to distinguish or reconstruct quantum states.... These algorithms are regrettably suitable for some special situations only, none works generally.

In contrast to classical information, there is one distracting fact in quantum computation. It is impossible to copy a state. We have already mentioned that if we could copy a state, we might precise our measurements (we would measure "position" on one qubit and "momentum" on another one) and finally overcome uncertainty relations. However, lets show in detail, why quantum copy algorithm must fail. Classical bit X is copied via CNOT gate - when taken with initial 0 bit and processed by CNOT gate, we obtain two X bits. Suppose qubit is in state 2.35. Together with $|0\rangle$ qubit they form a state $\alpha |00\rangle + \beta |10\rangle$. Now we apply the CNOT gate which swaps values of the second qubit when the value of the first is 1. We get $\alpha |00\rangle + \beta |11\rangle$. But we wanted to get $(\alpha |0\rangle + \beta |1\rangle) \otimes (\alpha |0\rangle + \beta |1\rangle) = \alpha^2 |00\rangle + \alpha\beta |01\rangle + \alpha\beta |10\rangle + \beta^2 |11\rangle$. Equality holds for a single choice $\alpha = 0 \vee \beta = 0$ only. We have not copied general state successfully. It turns out to be impossible to make a copy of an unknown state. This statement is known as *no-cloning theorem*. However, quantum communication and computation can be effectively performed even with this complication. And in quantum cryptography, we are allowed to secure the information right because of this fact.

2.5 Quantum algorithms

As already mentioned, quantum behaviour may give chance to develop new types of algorithms. These have reduced resource demands for solving some tasks compared to classical algorithm. Moreover, thanks to quantum computation we might be able to write algorithms to solve some NP-complete problems. Issues of complexity of classical taks is very extensive and its connection to quantum complexity is unclear. It is known that quantum computer can solve quickly any P-problem [15] but cannot solve any problem outside PSPACE[16]. When allowed to work with some bounded probability of error, we can define class of quantum efficiently solvable problems as BQP. It is supposed that there is a lot of NP-problems that are efficiently solvable but there are also NP tasks that cannot be efficiently solved even with the quantum computer. However, there may exist even problems outside NP (and inside PSPACE) that might be solvable. But it is fair to remind that actual relation between P, NP and PSPACE problems has not yet been understood. It is supposed that P$\subsetneq$NP$\subsetneq$PSPACE but

[15] Problems classically solvable in resources polynomially dependent on the size of the input

[16] Problems classically solvable with spatial resources exponentially depending on the size of the input, i.e. tasks requiring classical computer of excessive size

nobody has ever proven even that PSPACE is bigger than P! There can be found some articles dedicated to the relationship between quantum theory and the complexity hierarchy of tasks, e.g. [28].

One very powerful algorithm is called the Deutsch-Jozsa algorithm [20, 29] which handles so called Deutsch problem. That is, having two communication parties A and B, A chooses a number x from $\{0, 1, 2, \ldots, 2^n - 1\}$ and sends it using mailing pigeon to B. B calculates $f(x)$ and sends this number back. However, B promises to use either constant function, or function that is balanced. That means $f(x) = 0$ in exactly half cases while $f(x) = 1$ in the other half. Party A now needs to determine which function B used, communicating with them at least as possible.

Of course, mailing pigeon can carry only a letter with a single cipher. It is possible that A may have such bad luck that their first 2^{n-1} choices give the same value even for balanced function. However, after the $2^{n-1} + 1$ correspondences A certainly knows, whether the balanced or he constant function has been used. So much for the classical way. If A and B were able to exchange qubits (probably delivered by some kind of a quantum pigeon) and if B promised to calculate $f(x)$ using unitary transform $U_f : |x, y\rangle \to |x, y \oplus f(x)\rangle$, A could achieve their goal in a single correspondence.

Suppose A has a n-qubit register $|0\rangle^{\otimes n}$ to store their query and one qubit register $|1\rangle$ to store the answer. First, A must prepare a superposition state of the query and answer qubits. Such a task is carried out using Hadamard transform on the query register and Hadamard gate on the answer register

$$|0\rangle^{\otimes n} |1\rangle \to \sum_{x \in \{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}} \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \tag{2.40}$$

B applies U_f, giving

$$\sum_x \frac{(-1)^{f(x)} |x\rangle}{\sqrt{2^n}} \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \tag{2.41}$$

Result amplitude is now stored in the superposition state amplitude. To get the result, Hadamard transform is needed once more. After short argumentation (see [20] for details) it can be seen that we obtain

$$\sum_y \sum_x \frac{(-1)^{xy+f(x)} |y\rangle}{\sqrt{2^n}} \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \tag{2.42}$$

For f constant, amplitude of $|0\rangle^{\otimes n}$ is equal to ± 1, others are zero. That implies that observations of query register qubits will yield 0 only. For f balanced, the amplitude of $|0\rangle^{\otimes n}$ is zero and so there is a query register qubit that yields 1 when measured.

This example illustrates very well possibilities of quantum computation. Resources needed for same tasks are greatly reduced ($2^{n-1}+1$ bits to 1 qubit). Power of Hadamard transform as the discrete Fourier transform is obvious here.

Another important example describes phenomenon not present in classical physics, quantum teleportation [20, 30, 31]. That is, a quantum state is measured (destroyed) at one place and reconstructed at another place, only classical communication is used. Imagine following situation: A possesses one of entangled particles (Bell pair 2.31) and some unknown qubit $|\psi\rangle$. B possesses the other entangled particle. A is supposed to deliver the $|\psi\rangle$ to B using classical communication. Even if A knew exact constants α, β,

the classical communication might prevent A sending these values precisely. Anyway, situation is redeemed by the entanglement. Suppose initial state described as

$$|\psi_0\rangle = |\psi\rangle \frac{|00\rangle + |11\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}[\alpha(|000\rangle + |011\rangle) + \beta(|100\rangle + |111\rangle)] \tag{2.43}$$

where we take convention that the first qubit position is the unknown qubit, the second position is the entangled particle belonging to A and the third position corresponds to the entangled particle in possession of B. Now, A applies CNOT gate (with the unknown as the control qubit) on their qubits yielding

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}[\alpha(|000\rangle + |011\rangle) + \beta(|110\rangle + |101\rangle)] \tag{2.44}$$

Using the Hadamard gate on the unknown qubit, system transforms into

$$\begin{aligned} |\psi_2\rangle &= \tfrac{1}{2}[\alpha(|000\rangle + |011\rangle + |100\rangle + |111\rangle) + \beta(|010\rangle + |001\rangle - |110\rangle - |101\rangle)] = \\ &= \tfrac{1}{2}[|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)] \end{aligned} \tag{2.45}$$

A now performs measurement of both qubits. If values 00 are obtained, than the B's qubit is obviously in state $\alpha|0\rangle + \beta|1\rangle = |\psi\rangle$. That is B indeed now has the unknown qubit! In case that A measures other values, situation must be slightly modified as B particle is in a different state. Therefore B applies to their qubit some appropriate transformation according to the measured values. Of course, A is needed to send measured values to B, so that B can choose the correct transform. But the only thing needed to be communicated are two numbers, results of measurements. We see that this task would be impossible using classical communication only.

We might present here other algorithms, for example Shor's algorithm [23] for integer factorisation and discrete logarithm (both taking advantage of Fourier transoform). As this and many other algorithms are easily found in literature, we consider presented examples to be sufficient to demonstrate advantages of quantum information and computation. We only now mention a few practical/experimental achievements [30, 32].

2.6 Entanglement purification

It is impossible to create qubits with general prescribed α, β precisely. Although it is possible to produce some special states reliably (consider filter trasnimtting photons with certain polarisation only) or even precisely (suitable measurement projects system onto some known state), we simply do not have machine capable of producing arbitrary state precisely. Furthermore, experimental processes inherently work with some error. Because of these reasons, Bell states are not at disposal with absolute precision, entanglement is damaged and thus cannot be fully exploited. Furthermore, qubits needed for quantum computation are supposed to be realised through ions or photons. When transmitted through realistic environment, they are subject to noise and various outer environmental influences. Thus their wave function decays (decoherence). And so does the quantum entanglement. Therefore some process is needed to "repair" this entanglement release. Such purification of entanglement suddenly became target for studies. People started to solve this problem at the end of the last century and the work resulted in a few of so called purification protocols.

Briefly told, entanglement purification (also called entanglement distillation[17]) is done in a following way. Each party A, B possesses several copies of their parts of entangled states. In their corresponding laboratories they perform some measurement, local operations on some of them, then they communicate classically. As a result they have fewer qubits which are more entangled. Only local operations and classical communication are needed, this is usually shortened to LOCC.

Many of entanglement purification protocols, i.e. schemes to perform purification, have already been developed: [5, 33–37]... They rely on iterative application of nonlinear operators on systems of qubits. These protocols take set of qubits divided into control and target qubits. Control qubits are measured and according to the results, target qubits are modified. This reminds application of CNOT gate described in 2.39. However, measured qubits may be in fact destroyed and generally are not usable anymore. Therefore, big set of qubits is needed when more iterations of purification protocols are supposed to be applied. In general, the amount of qubits needed grows exponentially with the number of iterations. It is good to realise this price for entanglement purification. But when we have some good sources of starting qubits, this price can be accepted. Of course there may be situations that only few copies of states are given to the parties. Another strategies must be applied then.

In this thesis, we are not interested in entanglement measures [38], i.e. characterisation of the amount of entanglement that is shared by particles. Various concepts of measures have been developed, for example fidelity or entropy-like measures. Although we will not give any precise numbers of entanglement improvement, still we hope that the purification results will be clear.

We might ask a question if there exist states that can not be purified. Unfortunately, the answer is positive. It is known (check e.g. [39]) that there exist states which are entangled, but not distillable. Study and development of the entanglement purification is justified - for general multipartite qudit cases, there are no criteria for separability of states, level of entanglement or distillability. Only some bounds of distillability are known [40, 41].

From the developed protocols let us accentuate the first purification protocol and work [27] of Bennett generally discussing quantum entanglement. Then, specialised protocols were developed, for example [42] which purifies efficiently Fourier states, [43] which is concerned with two-qubit mixed states or [44] which is suitable for some unknown states.

Now we shall concentrate on purification protocol that is used in this thesis. It is based on scheme described in [45]. In that paper, XOR[18] gate is generalised. Action of the two qubit XOR gate can be expressed in following way:

$$\mathrm{XOR}_2 \left|i, j\right\rangle = \left|i, i \oplus_2 j\right\rangle \tag{2.46}$$

This gate can be generalised for qudits of dimension D in which case we get

$$\mathrm{GXOR}_D \left|i, j\right\rangle = \left|i, i \oplus_D j\right\rangle \tag{2.47}$$

which is unitary but not self-adjoint for $D > 2$. Inverse gate to this GXOR has to be expressed by iteration $\mathrm{GXOR}^{-1} = \mathrm{GXOR}^{D-1}$. This inconveniency can be bypassed by

[17] These two terms developed parallelly

[18] XOR=CNOT, the names come from different aspects of the view

redefining the gate using modular subtraction:

$$\mathrm{GXOR}_D \left|i,j\right\rangle := \left|i, i \ominus_D j\right\rangle \tag{2.48}$$

Such a modified operator is unitary and self-adjoint. Realisation of the protocol [45] is then described by operator

$$\mathcal{S}(\rho_c,\rho_t) = \frac{[(\mathbb{1}_c \otimes \left|s\right\rangle_t \left\langle s\right|_t)\mathrm{GXOR}_{ct}][\rho^c \otimes \rho^t][(\mathbb{1}_c \otimes \left|s\right\rangle_t \left\langle s\right|_t)\mathrm{GXOR}_{ct}]^*}{\mathrm{Tr}([(\mathbb{1}_c \otimes \left|s\right\rangle_t \left\langle s\right|_t)\mathrm{GXOR}_{ct}][\rho^c \otimes \rho^t][(\mathbb{1}_c \otimes \left|s\right\rangle_t \left\langle s\right|_t)\mathrm{GXOR}_{ct}]^*)} \tag{2.49}$$

where ρ_c/ρ_t are the control/target states, $P := \left|s\right\rangle_t \left\langle s\right|_t$ is the projection onto $\left|s\right\rangle$ state of the target system. When the control and target states are the same, $\rho^t = \rho^c =: \rho = \sum_{i,j}^{D-1} \sigma_{ij}^c \left|i\right\rangle \left\langle j\right|$ we obtain

$$\mathcal{S}(\rho,\rho) = \rho_{out} \otimes P \tag{2.50}$$

while ρ_{out} depends on the chosen projection state. If projected on $\left|0\right\rangle$, output density matrix has up to norm following form:

$$\rho_{out} = \rho \odot \rho = \begin{pmatrix} \rho_{11}^2 & \rho_{12}^2 & \cdots & \rho_{1n}^2 \\ \rho_{21}^2 & \rho_{22}^2 & \cdots & \rho_{2n}^2 \\ \vdots & \vdots & \ddots & \vdots \\ \rho_{n1}^2 & \rho_{n2}^2 & \cdots & \rho_{nn}^2 \end{pmatrix} \tag{2.51}$$

That is, from starting density matrix we have got a new matrix, which has its element squared (so this process dependes on the input matrix only). This is indeed nonlinear operation and we shall assign to this squaring operation following notation (in arbitrary dimensions m, n), N is suitable normalisation constant.

$$S^{m,n}\begin{pmatrix} \rho_{11} & \rho_{12} & \cdots & \rho_{1n} \\ \rho_{21} & \rho_{22} & \cdots & \rho_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \rho_{m1} & \rho_{m2} & \cdots & \rho_{mn} \end{pmatrix} = \frac{1}{N}\begin{pmatrix} \rho_{11}^2 & \rho_{12}^2 & \cdots & \rho_{1n}^2 \\ \rho_{21}^2 & \rho_{22}^2 & \cdots & \rho_{2n}^2 \\ \vdots & \vdots & \ddots & \vdots \\ \rho_{m1}^2 & \rho_{m2}^2 & \cdots & \rho_{mn}^2 \end{pmatrix} \tag{2.52}$$

According to [46], squaring operator $S^{n,n}$ on density matrices has following properties

1. S indeed maps density matrices onto density matrices
2. S is not injective
3. S is not linear
4. there are states invariant to this transformation

S is physically realised in three steps. First, we divide qubits into pairs of control and target qubits. The second step consists of application of the CNOT gate on the pairs. The third step is filtering - we measure the control qubit. If the value is 0, we keep the pair, otherwise we discard it. As there is a chance of measuring 1, here comes the price for entanglement purifying.

Now we need to discuss renormalisation. Suitable factor N in equation 2.52 guarantees the first property. It justifies usage of operator $S^{m,n}$ on density matrices as well as on pure states. However, if we discuss the action of general $S^{m,n}$, we could demand any norm to be preserved. Moreover we can also demand that one chosen element is real. This is motivated by the fact that for density matrices probability given by $|\gamma|^2$ does not change while $\gamma \to e^{i\varphi}\gamma$. For $n = 1$ (i.e. pure states), arbitrarity of the phase factor of $|\psi\rangle$ representing the state has been discussed in 2.2.

An example of $S^{m,n}$ action on element of $\mathbb{C}^{2,2}$ is now presented. At first, iterations of $S^{2,2}$ preserving Frobenius norm are shown, then iterations of $S^{2,2}$ preserving trace norm are demonstrated on the same matrix. Our special element chosen to obtain real values is the first one.

$$\begin{pmatrix} 2 & 2i \\ -i & 4 \end{pmatrix} \xrightarrow{S^{2,2}} \frac{5}{\sqrt{289}} \begin{pmatrix} 4 & -4 \\ -1 & 16 \end{pmatrix} \xrightarrow{S^{2,2}} \frac{5}{\sqrt{66049}} \begin{pmatrix} 16 & 16 \\ 1 & 256 \end{pmatrix} \xrightarrow{S^{2,2}} ... \rightsquigarrow \begin{pmatrix} 0 & 0 \\ 0 & 5 \end{pmatrix}$$

$$\begin{pmatrix} 2 & 2i \\ -i & 4 \end{pmatrix} \xrightarrow{S^{2,2}_{Tr}} \frac{6}{20} \begin{pmatrix} 4 & -4 \\ -1 & 16 \end{pmatrix} \xrightarrow{S^{2,2}_{Tr}} \frac{6}{272} \begin{pmatrix} 16 & 16 \\ 1 & 256 \end{pmatrix} \xrightarrow{S^{2,2}_{Tr}} ... \rightsquigarrow \begin{pmatrix} 0 & 0 \\ 0 & 6 \end{pmatrix}$$

We see that $S^{m,n}$ acts in a very simple manner. Basically, it finds elements that have maximal absolute value and shifts them closer to some number related to the norm. All smaller elements are on the contrary sent closer to zero.

This behaviour may be changed by adding some modifying operation. For purification protocols, we demand this operation to be unitary and we call it twirling operator. If twirling operator can be disassembled into tensor product of twirling operators on each of considered qubits, we say the twirling operator is local. A single step of purification protocol we consider in this work has the form

$$\rho \to US\rho = U(\rho \odot \rho) \tag{2.53}$$

or for the pure states

$$|\psi\rangle = \begin{pmatrix} a \\ b \\ \vdots \end{pmatrix} \to US\,|\psi\rangle = U \begin{pmatrix} a^2 \\ b^2 \\ \vdots \end{pmatrix} \tag{2.54}$$

Definitely, choice of U has an important role on the convergency of purification protocol. Not only speed of convergence, but it may induce chaotic behaviour, [6]. U then modifies asymptotic behaviour, invariant states and so on. Quadrats of components are then responsible for chaotic behaviour of the purification protocol.

Articles [7, 8] find special set of states that is invariant to the action of HS, H the tensor product of Hadamard gates, $H = H_1 \otimes H_1$, 2.6. In author's former work [47] we elaborated this local twirling operator behaiviour in more details. Now we continue and generalise the situation considering different twirling operators.

No doubt, theoretical algorithm describing purification protocol and its experimental realisation are two different things. Realisation of measurements and operations on qubits can be very complicated. [48] describes experimental difficulties suggesting some improvements to application og CNOT gate. Despite brilliant theory, we may not benefit from purification protocol as the papers suggest. Still, quantum purification and error correcting codes seem nowadays to be the future of quantum computation.

2.7 Chaos in physics and mathematics

The word *chaos* comes from Greek mythology, where it described infinite and indescribable emptiness before our Universe was created. Today, using this word we usually mean disorder, randomness, fluctuations, unpredictability. However, this is no physical definition. Exact definition of chaotic system will be given in this paragraph together with examples of chaotic systems and issues of chaos in classical and quantum physics.

In history, symmetries and some kind of harmony always were some desired properties. Laws and equations were supposed to give us some exact predictions. Universe should have obeyed simple harmonic patterns, e.g. the sun rises each morning. However, there were some (even unexplained) flaws. Remember Brown motion which we can take as a motivation to introduce statistical physics, which works only with probabilities and randomness, but in principle allows precise solution. Nevertheless, also some more fundamental mathematical description failed in some problems. Since Newton, no significant progress had occurred in celestial mechanics until Poincaré[19], who in [49] studied the problem of three bodies. This problem has no analytical solution and started a new chapter of the classical physics. Poincaré's results were summarised in [50], the chaos he introduced shocked the physical public.

There are many examples of chaotic behaviour. The weather or climate is probably the best known. Even simple differential equations result in evolution extremely sensitive to initial conditions. That is a typical attribute of chaos. It is in principle possible to determine weather but we would need to know the pressure, temperature, humidity and so on in every point of the atmosphere. Even the smallest imprecision leads to a very different weather, that is known as the butterfly effect.

Another and maybe less obvious examples of chaotic systems are turbulences in fluids, stock exchange price evolution or population growths. We shall discuss celestial mechanics once more [51]. In Lagrange or Hamilton mechanics, we can study system evolution in phase space. Equations of motion put restrictions on the manifold, where motion can occur. For integrable systems this manifold has topological structure of (multidimensional) toroid. Canonical action-angle variables can be defined that motion orbits through this so called invariant toroid. Chaotic behaviour (as a result of dissipative or some outer forces) destroys this structure.

Lets consider three bodies where one body serves as a perturbation to the two particle system. Phase space of two bodies will be deformed due to perturbation. When the third body is small enough (like in Sun - Earth - Moon situation), the toroid in phase space will suffer from small deformation, but under rough measures, the main toroidal structure is preserved. When the perturbation is big, the structure of toroid is shattered and does not resemble toroid in any measure. The small deformation case is ussually called soft chaos while destroyed structure of manifold is reason to call this situation hard chaos.

There is an interesting statement from the soft chaos theory. This so called KAM theorem (named after Kolmogorov, Arnold and Moser) says that for very small perturbation there exist regions, "stability islands" in phase space where motion is realised almost like in not perturbed case. These are the reason for our solar system not to

[19]Henri Poincaré, 1854-1912; great French mathematician, physicist, astronomer; called the last polyhistor. He stood at the birth of modern physics - theory of relativity, theory of chaos, algebraic topology and geometry, even quantum physics

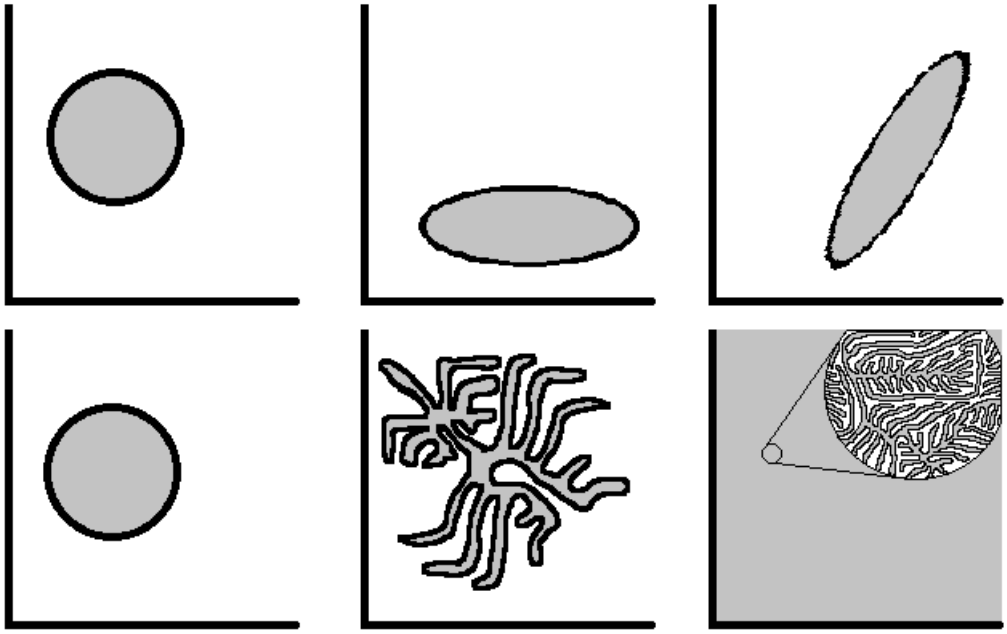

Figure 2.1: Evolution of a "bubble" of initial conditions for integrable systems (up) and chaotic systems (down) in the phase space.

be torn into pieces by gravity. Moon would be catapulted away form Earth instead of being forced to orbit almost Kepler ellipses.

Evolution in the phase space is different for integrable systems and chaotic systems is illustrated in figure 2.1. In both cases, the Liouville theorem holds. That means that a set of initial conditions represented as some "bubble" in the phase space evolve as incompressible liquid. For integrable system this initial-state-bubble will preserve relatively decent shape while for chaotic system this bubble would fill uniformly whole phase space in limit of infinite time. Two arbitrarily close starting points will eventually get as far away as wanted. This is one of motivation to define chaos as below.

Of course, the topic of this thesis is quantum information. How does chaos appear in quantum physics? Quantum mechanics as described in chapter 2.2 is theory of linear operators. In such case, operator cannot induce chaotic behaviour in the sense of sensitivity to initial conditions (see below). Correspondence principle however states that there must exist some quantum system corresponding to classical (even chaotic) system. Study of this correspondence, search for the existence and form of suitable quantum systems is business of a branch of physics that is called quantum chaology. Although we mentioned chaos cannot emerge in linear theory, we have not told whether we can or cannot bring nonlinear behaviour to the system. Answer goes with measurements. As a manifestation of outer forces, measurements disrupt the system changing it in general i.e. nonlinear (and usually unknown) manner. That is exactly what purification protocol takes advantage of.

Now it is finally time to properly define what is a chaotic system. Many physicists and mathematics since Poincaré tried to define, what is chaos. During time, many

different but (usually) equivalent definitions have been established. In this work, we will use following definition according to Devaney [9] (resp. adjusted for metric spaces, [52]). First we must define mathematical structure, where chaotic behaviour will occur.

Definition 2.7.1 (Dynamical system)**.** *Let X be a complete metric space, $\mathbb{F}$ be one of $\mathbb{R}$, $\mathbb{R}^+$, $\mathbb{Z}$, $\mathbb{N}_0$. A pair $(\{S_t\}, X)$ is called a* dynamical system *when $\{S_t\}$ is a set of continuous maps from X into itself such as following conditions are satisfied:*

1. $(\forall m, n \in \mathbb{F})(S_{m+n} = S_m \circ S_n)$,
2. $S_0 = \mathbb{1}$ *is identical map.*

Set S_t forms evolutionary operator while parameter t has the role of time. According to $\mathbb{F}$ we call dynamical system to be reversible continuous, irreversible continuous, reversible discrete or irreversible discrete respectively.

As described in 2.6, the whole problem of our purification protocol action can be reduced to iterated (i.e. discrete) action of "squaring" operator S. Evolutionary operator is determined as the powers of S, however we will modify the S operators by adding some local twirling operator. We can take the whole operator as some map f on the space X which will be usually $\mathbb{C}^4, \mathbb{C}^2$ or $\mathbb{C}$:

$$S_n = f^{\circ n} =: f^n \tag{2.55}$$

We will label such dynamical systems simply (f, X). We will not work with any other systems in this thesis. Now we need to give additional definitions connected to systems whose dynamics is prescribed by a single map action.

Definition 2.7.2. *A point $x \in X$ is* periodic*, if $(\exists n \in \mathbb{N})(f^n(x) = x)$. A point $x \in X$ is* preperiodic *if $(\exists j \neq k \in \mathbb{N})(f^j(x) = f^k(x))$ but x is not periodic.*

Definition 2.7.3. *Let $f : X \to X$, $g : Y \to Y$ be maps. f and g are said to be* topologically conjugate *if there is a homeomorphism h such that $f \circ h = h \circ g$. Homeomorphism h is then called topological conjugate.*

Definition 2.7.4. *$f : X \to X$ is* topologically transitive *if for any nonempty open sets $U, V \in X$ there exists such $k > 0$ that $f^k(U) \cap V \neq \emptyset$*

Definition 2.7.5 (Chaotic dynamical system)**.** *Let (X, ρ) be a complete metric space with metric ρ, f be a map $f : X \to X$. The dynamical system (f, X) is* chaotic *if*

1. *set of preperiodic points of f is dense in X,*
2. *f is topologically transitive.*

Note 2.7.6. *The original Devaney's definition contained one more point:*

3. *f has sensitive dependence on initial conditions.*

This point means that there is ε such that, for any $x \in X$ and any its neighbourhood U, there exist $y \in U$ and $n \in \mathbb{N}$ so that $\rho(f^{\circ n}(x), f^{\circ n}(y)) > \varepsilon$. Nonetheless, later it was proven [11] that this point is a consequence of the first two points and thus not needed in the definition.

It is convenient to realise that a chaotic dynamical system has three important properties: unpredictability, indecomposability, regularity. While regularity is meant as the existence and density of the periodic points, indecomposability is a result of topological transitivity - system cannot be divided into two noninteracting subsystems (invariant open sets), any two chosen open sets will eventually intersect under iterations. The most important point however is the unpredictability which is connected to the sensitivity on initial conditions. This property is crucial for chaotic systems and in fact this property is the chaotic nature itself.

2.8 Dynamics in one complex variable

For systems where only one variable describes evolution of the system, entire behaviour-description machinery has been developed. It is widely known today as the theory of dynamics of one complex variable iterated functions. This theory was developed during the last century and is connected with names like Julia[20], Fatou[21] or Mandelbrot [22]. Many books are dedicated to this problematic ([10, 11],...); this paragraph adopts widely used notation as presented in [10]. Unfortunately, no such developed theory exists for more complex variables. Only some facts are known, see for example [11], [53]. Giving only some special signs of behaviour, these rare results are not sufficient. In this paragraph we discuss foremost the theory of one complex variable and apparatus suitable to sufficiently describe many special cases in chapters 3,4.

First of all, let us settle the manifold which will serve as a domain for given one complex variable function. In this work we will ask for a so called Riemann surface, that is a connected complex analytic manifold of (complex) dimension one. Furthermore, we will request simple connectedness, because we will usually consider components of vector $\in \mathbb{C}^n$. That is, we are concerned in numbers from $\hat{\mathbb{C}} = \mathbb{C} \cup \infty$. We include infinity into the set for special cases[23]. This set $\hat{\mathbb{C}}$ is called the *Riemann sphere* because topologically it indeed is a sphere. We might demand that our vector is normalised to one. All components would then be complex numbers with magnitude smaller than one. Set of considered numbers would then be a unit disk $\mathbb{D} = \{z = x+iy \in \mathbb{C} \,|\, x^2+y^2 < 1\}$.

Definition 2.8.1 (Uniformisation theorem)**.** *Every simple connected Riemann surface is conformally isomorphic (i.e. there exists an manifold isomorphism holomorphic also with its inverse) to one of following manifolds:*

1. *a field* $\mathbb{C}$*,*
2. *a disk* $\mathbb{D}$*,*
3. *a Riemann sphere* $\hat{\mathbb{C}}$*.*

[20]Gaston Maurice Julia, 1893-1978; French mathematician born in Algeria, suffered heavy injury in the World War I. He studied rational functions of one complex variable. His work got appreciated (thanks to Mandelbrot) long time after publication, when computers could depict his results.

[21]Pierre Joseph Louis Fatou, 1878-1929; French mathematician and astronomer. He engaged a lot in mathematical analysis.

[22]Benoît Mandelbrot, 1924-2010; French mathematician with Polish roots. He studied theory of information, fluid dynamics, economics but made his name with fractal geometry.

[23]We use some special state parametrisations in next chapters.

Note 2.8.2. *For a general case, without simple connectedness, theorem can be modified in the sense that each Riemann surface is conformally isomorphic to a factormanifold* $S = \tilde{S}/_{\Gamma}$*, where* $\tilde{S}$ *is a simply connected Riemann surface and* Γ *is a discrete group of conformal automorphisms such that each its nonidentical element has no fixed point.*

In this thesis, the Riemann surface will usually be $\hat{\mathbb{C}}$ because we consider components of complex vectors[23]. As for the functions, we will consider rational polynomial functions solely. We will write $f(z) = P(z)/Q(z)$ with P, Q polynomials (without common roots) when needed.

Definition 2.8.3. *Degree of the function* $f(z) = P(z)/Q(z)$ *is taken to mean maximum of degrees of polynomials* P*,* Q*.*

Definition 2.8.4 (Normal family of functions)**.** *Suppose* X*,*Y *be Riemann surfaces,* $\mathcal{A}$ *be a set of continuous maps* $X \to Y$*.* $\mathcal{A}$ *is called a normal family of functions, if for any infinite sequence of functions* $\{f_n\}_{n=1}^{\infty} \in \mathcal{A}$ *there exists a subsequence which converges locally uniformly to a continuous map* $f : X \to Y$*.*

Note 2.8.5. *This is an important property. Existence of the locally uniformly convergent subsequence in iterated function implies regular dynamics.*

Note 2.8.6. *Definitions given so far can be generalised to complete metric spaces.*

Definition 2.8.7 (Julia set & Fatou set)**.** *Let* $f : S \to S$ *be a non-constant holomorphic map on a Riemann surface* S*. For a point* $z_0 \in S$ *there is following dichotomy:*

1. *There exists a neighbourhood* U *of* z_0 *such that* $f^n/_U$ *forms a normal family of functions. We say that point* z_0 *is regular or normal.*

2. *Such the neighbourhood does not exist.*

Set of regular points forms Fatou set*,* $\mathcal{F}(f)$*. The points satisfying the second condition form* Julia set*,* $\mathcal{J}(f)$*.*

Julia set is a crucial term in the theory of complex variables and is connected to chaotic behaviour. Julia set has many properties that earned it its popularity amongst wide public. The most interesting is its self-similarity feature, fractal-like structure which adds to this thesis inomittable element of esthetic value. Of course, following properties of Julia set are much more important for this thesis.

Lemma 2.8.8. *Julia set is fully invariant. This means:* $(\forall n \in \mathbb{Z})(f^n(\mathcal{J}(f)) = \mathcal{J}(f))$*. Furthermore, Julia set of a function and its n-fold iterate coincide. That means:* $(\forall n \in \mathbb{N})(\mathcal{J}(f)) = \mathcal{J}(f^n))$*.*

Corollary 2.8.9. *Because* $\mathcal{F}(f) \cup \mathcal{J}(f) = \mathbb{C}$*, the same statement holds for* $\mathcal{F}(f)$ *too.*

Lemma 2.8.10. *For function* f *of degree at least 2, the Julia set has following properties:* $\mathcal{J}(f) \neq \emptyset$*,* $\mathcal{J}(f) = \overline{\mathcal{J}(f)}$ *and* $\mathcal{J}(f)$ *has no isolated points.*

Definition 2.8.11. *An* orbit *of a point* z *is the sequence of its forward images, i.e.* $\mathcal{O}(z) = \{f^n(z)\}_{n=1}^{\infty}$*. If* $(\exists n \in \mathbb{N})(f^n(z) = f(z) \wedge (\forall k \in \widehat{n-1})(f^k(z) \neq z))$*, orbit is said to be periodic, or is shortly called a* cycle*; number* n *is called the* period *of the cycle. Number* $\lambda = (f_n)'(z)$ *is called the* multiplier *or eigenvalue of the cycle.*

Definition 2.8.12. *A cycle whose multiplier is*

1. $\lambda = 0$, *is called superattractive,*
2. $0 < |\lambda| < 1$, *is called attractive,*
3. $|\lambda| = 1$, *is called indifferent,*
4. $|\lambda| > 1$, *is called repelling.*

A cycle for which $\lambda = 1$ but none of f^n is identical map (i.e. $\lambda = e^{i\varphi}$, $\varphi \in \mathbb{R} \setminus \mathbb{Q}$) is called parabolic.

This definition is very illustrative. When a small perturbation is given to a (super)attractive cycle, the orbit will tend back to the unperturbed situation. When an indifferent cycle is perturbed, orbit will evolve to a different orbit, which however stays near the original orbit. For a perturbation of a repelling orbit, new and original orbit will diverge.

Definition 2.8.13. *For each attractive cycle, there is a nonempty open set of points, whose orbits tend in limit to some point of the cycle. This set is called* basin of attraction, Ω. *Each point $z \in \mathcal{F}(f)$ can be associated with one connected component Ω_z of some basin of attraction, so that $z \in \Omega_z$. This component is called* immediate basin of attraction. *Immediate basin of attraction of a cycle is meant to be a union of immediate basins of all points of the cycle.*

Theorem 2.8.14. *Each attractive cycle is contained in the Fatou set. Each parabolic and each repelling cycle is contained in the Julia set. A whole basin of attraction Ω of an attracting cycle is contained in the Fatou set. But the boundary of the basin $\partial\Omega$ is a part of the Julia set. Even, topological boundary of basin of attraction of any single attractive cycle is equal to the entire Julia set.*

Proposition 2.8.15. *Rational polynomial function of degree $d \geq 2$ has at most $2d-2$ attractive or parabolic cycles. There is only finite number of non-repelling cycles.*

According to [10], one can use so called critical points for investigation of Fatou set.

Definition 2.8.16. Critical point *z is any point such that the first derivative of f vanishes there, i.e. $f'(z) = 0$.*

Proposition 2.8.17. *Let f be a rational polynomial function of degree $d \geq 2$. Each immediate basin of attraction contains at least one critical point. Forward orbit of critical points converge to an attractive or parabolic cycle, if it converges at all.*

Definition 2.8.18. *A property is said to be true for* generic *$x \in \mathcal{M}$ if it is true for all points in some countable intersection of dense open subsets of $\mathcal{M}$.*

Theorem 2.8.19. *For each $z_0 \in \mathcal{J}(f)$: $\overline{\{z|(\exists n \in \mathbb{N}_0)(f^n(z) = z_0)\}} = \mathcal{J}(f)$.*

Theorem 2.8.20. *For generic $z_0 \in \mathcal{J}(f)$: $\overline{\{z|(\exists n \in \mathbb{N}_0)(f^n(z_0) = z)\}} = \mathcal{J}(f)$.*

Note 2.8.21. *This means that Julia set can be sufficiently approximated by iterating inverse function on any single point. However, one can choose a point, whose (forward) orbit will not give a good picture of the Julia set. A program that would serve to find enough Julia set points would thus have to find preimages of a single known point. It is convenient to realise that there are many preimages of one point and so this procedure is usually quite fast.*

Lemma 2.8.22. *If Julia set has an interior point, then* $\mathcal{J}(f) = \mathbb{C}$.

This whole apparatus now presents a simple dynamics investigation method which is now to be summarised. A function of one complex variable splits its domain ($\hat{\mathbb{C}}$) into two disjoint parts - Fatou and Julia set. Julia set contains the essence of chaotic behaviour. To find the Fatou set one can use critical points. These are situated in connected components of basin of attraction, other components cannot exist. Evolution of critical points also gives information of the few existing attracting cycles. Boundary of their basins of attraction forms entire Julia set but this method can hardly be successful to describe (or rather display) Julia set well. Therefore one has to find at least one point of Julia set. That can be done by finding repelling or parabolic cycles. The whole Julia set then can be approximated by reverse images of this single point.

One can naturally ask how to define a measure of chaotic behaviour, that is if we can compare how much chaotic the function is. A widely used way is to use Lyapunov exponent $\lambda(x_0) = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln |(f^i)'(x)|$. Roughly speaking, this number gives the information about how much exponentially do two close initial points separate. We shall not study Lyapunov exponent in this thesis because of computational difficulties. We shall get by with cycle classification.

An example of investigating of a function and some pictures are presented in appendix D.

Chapter 3

Chaotic dynamics - special rotations

Following chapters present results of author's work. In this thesis pure states are considered. This is because of very troubling problematics. Polynomial equations inducing chaotic behaviour are very difficult to handle and vectors (4 components for pure states) represent an utmost convenient simplification compared to density matrices (16 components for mixed states). Some remarks for the mixed states are mentioned in the original article [45] and in [46]. Even for the pure states, there is a plenty of interesting phenomena to study.

From mathematical point of view in following chapters, the origin and precise formulation of the important part of purification protocol are not important. We can turn aside from the tensor product over the bigger system and consider that a step of purification is based on squaring represented by nonlinear squaring operator $S^{m,n}$ on given space $\mathbb{C}^{m,n}$. Physical part of problem is neglected during computations and is discussed when interesting consequences or physical relationships are found.

Author's former work [47] studied H_{11} as the local twirling operator for the purification protocol [45], important findings are accented first. These results are improved. Then we consider sets of local twirling operators generated by rotations with particular angles 2.6-2.13. These are studied concerning their action on Bell states and possible sets of invariant states.

3.1 General characterisation of squaring operator

Lets suppose the simplest possible version of purification protocol based on the element squaring. That means we consider only $S^{m,n}$ that acts on a matrix, which is an element of $\mathbb{C}^{m,n}$. This is the only place in this thesis where we do not make any restrictions on dimensions m, n. First of all lets discuss problem of renormalisation applied together with $S^{m,n}$. Suitability of factor N is at our hands. As we want to simplify computation, we will not care much for proper physical normalisation and will use more convenient parametrisations. We will usually demand that S uses such a normalisation factor that (after each one iteration of protocol) a specially chosen nonzero component of vector is set to 1. This indeed is possible because we can relieve the norm condition and represent state Ψ by any vector ψ from corresponding ray. So we will write sign =

(instead of more correct $\sim$) for vectors that are not equal but represent the same state.

Simply told, iterated action of $S^{m,n}$ finds components with the largest magnitude and sends them to some norm (parametrisation)-related numbers. Smaller magnitude components are sent to zero. In fact, situation is a little bit complicated when two or more components have the largest magnitude, but these special occasions will be discussed later when needed.

It is worth of notice that plus/minus signs of elements of matrix have no importance thanks to squaring. Therefore with any vector (as solution of some equations or so), all vectors with sign variations are automatically taken into account and this fact is not explicitely reminded any further. For formal furhter purposes, we write

$$S \circ \mathrm{diag}(d_1, d_2, d_3, d_4) = S, \quad (\forall j \in \hat{4})(d_j \in \{1, -1\}) \tag{3.1}$$

We see that at least 16 inputs give the same output when subject to an aciton of US, U arbitrary unitary matrix.

We remind another important fact: $S\vec{x} = \vec{0} \Leftrightarrow \vec{x} = \vec{0}$, modification by an additional unitary operator does not change this fact. As a consequence, when looking for a fixed states or cycles, that is $(US)^n |\psi\rangle = k |\psi\rangle$ anywhere in this work, it is possible to divide this equation by k as the operation $\frac{1}{k}$. could be problematic for the zero vector only. But this vector is not in our concern. Usually when discussing fixed states, we will refer to zero vector for simplicity as to the trivial state although zero vector does not determine any physical state.

We remind that Bell states 2.31-2.34 in vector notation have forms

$$\left|\Phi^{\pm}\right\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \pm 1 \end{pmatrix} \tag{3.2}$$

$$\left|\Psi^{\pm}\right\rangle = \begin{pmatrix} 0 \\ 1 \\ \pm 1 \\ 0 \end{pmatrix} \tag{3.3}$$

It follows from 3.1 that the both 3.2 (resp. 3.3) are transformed into the same vector for any choice of local twirling operator. Therefore, we will usually treat them as a single vector. Another consequence is that no operator can have both of 3.2 (resp. 3.3) as the fixed states.

Proposition 3.1.1. *Operator AS composed of general matrix $A = (a_{ij})$ has the 3.2 as the fixed state if and only if $a_{11} + a_{14} = \pm(a_{41} + a_{44}) \neq 0 \wedge a_{21} + a_{24} = 0 = a_{21} + a_{24}$.*

Proof. Lets apply one iteration of general matrix protocol.

$$AS \begin{pmatrix} 1 \\ 0 \\ 0 \\ \pm 1 \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} a_{11} + a_{14} \\ a_{21} + a_{24} \\ a_{31} + a_{34} \\ a_{41} + a_{44} \end{pmatrix} \overset{!}{=} k \begin{pmatrix} 1 \\ 0 \\ 0 \\ \pm 1 \end{pmatrix} \tag{3.4}$$

Obviously, as $k \neq 0$ we obtain desired equation. □

Note 3.1.2. *Analogous condititons for 3.3 states are*
$a_{22} + a_{23} = \pm(a_{32} + a_{33}) \neq 0 \wedge a_{12} + a_{13} = 0 = a_{42} + a_{44}$.

3.2 Properties of operator H

In [47], operator H_{11} (for definition, check 2.6, 2.16, or list in appendix A)

$$H := H_1 1 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \tag{3.5}$$

was investigated as the local twirling operator. First of all, fixed states were found. That means solutions of

$$HS \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} a^2+b^2+c^2+d^2 \\ a^2-b^2+c^2-d^2 \\ a^2+b^2-c^2-d^2 \\ a^2-b^2-c^2+d^2 \end{pmatrix} \stackrel{!}{=} k \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} \tag{3.6}$$

were determined. The most important property is that Bell states 3.2, 3.3 are prepe-riodic, after at most two iterations they become the positive 3.2 which is fixed. This is behaviour that is desired from a purification protocol. For H it is obvious that the first row is privileged to the others. This led to one special set of fixed states

$$\begin{gathered} \begin{pmatrix} 1 \\ \mu_{1,2,3} \\ \mu_{1,2,3} \\ \mu_{1,2,3} \end{pmatrix}, \text{ where} \\ \mu_1 = \tfrac{1}{9}\left(-1 - 4\sqrt[3]{\tfrac{4}{67+9\sqrt{57}}} + 2\sqrt[3]{\tfrac{67+9\sqrt{57}}{4}}\right) \\ \mu_{2,3} = \tfrac{1}{9}\left(-1 + 2(1 \pm i\sqrt{3})\sqrt[3]{\tfrac{4}{67+9\sqrt{57}}} - (1 \mp i\sqrt{3})\sqrt[3]{\tfrac{67+9\sqrt{57}}{4}}\right) \end{gathered} \tag{3.7}$$

That is because the numbers $\mu_{1,2,3}$ are radices of $\mathcal{P}_1(x) = 3x^3 + x^2 + x - 1$. These algebraic numbers have very complicated analytic form and that is why we will label such numbers with greek letters. We will see that some other important states will be defined by various polynomial radices in a similar way. Another interesting set of fixed states is obtained for $a = 0$ which yields two solutions

$$\begin{pmatrix} 0 \\ \frac{-1+i\sqrt{3}}{2} \\ \frac{-1-i\sqrt{3}}{2} \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ \frac{-1-i\sqrt{3}}{2} \\ \frac{-1+i\sqrt{3}}{2} \\ 1 \end{pmatrix} \tag{3.8}$$

determined by radices of $\mathcal{P}_2(x) = x^2 + x + 1 = 0$. The rest of fixed states was found using Mathematica software. In total, the fixed state equations have the trivial solution and nontrivial 15 solutions (numerical forms may be found in [47]. Analytic forms may be determined, they are too complicated to be presented here).

Stabilities of the solutions were checked numerically. Using Matlab software, iterations of HS were applied to the fixed states given with precision to 10^{-15}. This served as ε for checking the asymptotic behaviour. Except the zero vector and the Bell state,

all other states evinced to be unstable. However, using some random inputs, the Bell state seems to be very attractive vector. Analytical analysis of stability has not been performed (may indicate instability).

From the cycles of length two, only some special cases were found in [47]:

$$\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \leftrightarrow \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} \leftrightarrow \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} \tag{3.9}$$

More, we claim to find all cycles of length two as they have been determined using Mathematica (we do not present numerical values here). In total, there are 104 cycles of length two (containing all fixed states). Numerical stability checking suggests that only 3.9 may be stable. Analytical proof of the stability of the solutions is not presented, however numerical simulations have never shown convergency to another cycle or state than 3.9 which indicate their attractiveness. We consider very important to analytically verify the attractivenesses of the mentioned states in future.

Special sets of vectors were found. They are invariant on the action of HS or $(HS)^2$.

$$\mathcal{C}_1 = \left\{ \left(\begin{array}{c} 1 \\ z \\ z \\ 1 \end{array} \right) \middle| z \in \mathbb{C} \right\}, \mathcal{C}_2 = \left\{ \left(\begin{array}{c} 1 \\ z \\ 1 \\ z \end{array} \right) \middle| z \in \mathbb{C} \right\}, \mathcal{C}_3 = \left\{ \left(\begin{array}{c} 1 \\ 1 \\ z \\ z \end{array} \right) \middle| z \in \mathbb{C} \right\}, \tag{3.10}$$

$$\mathcal{D}_1 = \left\{ \left(\begin{array}{c} 1 \\ 0 \\ 0 \\ z \end{array} \right) \middle| z \in \mathbb{C} \right\}, \mathcal{D}_2 = \left\{ \left(\begin{array}{c} 1 \\ z \\ 0 \\ 0 \end{array} \right) \middle| z \in \mathbb{C} \right\}, \mathcal{D}_3 = \left\{ \left(\begin{array}{c} 1 \\ 0 \\ z \\ 0 \end{array} \right) \middle| z \in \mathbb{C} \right\}. \tag{3.11}$$

$$\mathcal{E} = \left\{ \left(\begin{array}{c} 1 \\ z \\ z \\ z \end{array} \right) \middle| z \in \mathbb{C} \right\}. \tag{3.12}$$

They are linked by the action of HS

$$(HS)\mathcal{E} \subset \mathcal{E} \tag{3.13}$$

$$(HS)\mathcal{C}_i \subset \mathcal{D}_i\,,\ (HS)\mathcal{D}_i \subset \mathcal{C}_i \tag{3.14}$$

$$(HS)^2\mathcal{C}_i \subset \mathcal{C}_i\,,\ (HS)^2\mathcal{D}_i \subset \mathcal{D}_i \tag{3.15}$$

These invariances allowed us to investigate problem of chaotic behaviour on special subsets characterised by only one complex variable. For $\mathcal{C}_i, \mathcal{D}_i$ the relevant function is $f(z) = \frac{2z^2}{1+z^4} = g(g(z))$ where $g(z) = \frac{1-z^2}{1+z^2}$[1]. Julia set and properties are described in [47]. For $\mathcal{E}$, the dynamics is determined by $f(z) = \frac{1-z^2}{1+3z^2}$. Dynamics of this function is also described in [47] in detail. Julia set and basins of attraction are drawed in fig... There is one superattractive cycle (only in $\mathcal{E}$!) reached by both critical points $0, \infty$. This cycle is the first of 3.9. Fatou set is split into two parts - interior of Julia set which corresponds to states that converge to $z_\infty = 0$ in even number of iterations, states from exterior set converge to $z_\infty = 0$ in odd number of iterations.

[1]This function has an interesting property, see in D

3.3 Properties of Pauli matrices and permutations

Before generalising previous results and investigation of other operators, we shall examine important classes of matrices. Suppose a permutation matrix $P \in \mathbb{C}^{4,4}$. That is of course an unitary operator and we can consider it to be part of our "purification protocol" regardless of physical meaning now (discussion made in 3.8). As an example of permutation matrix we can use P_2 from the list B.2 (the CNOT matrix). More on permutation matrices in B.

Supposing one step of purification looks like

$$|\psi'\rangle = PS\,|\psi\rangle\,, \tag{3.16}$$

we can easily see that an example

$$P_2 S \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} d^2 \\ b^2 \\ d^2 \\ c^2 \end{pmatrix} = S P_2 \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} \tag{3.17}$$

illustrates very convenient property. For any permutation matrix $P \in \mathscr{S}_4$:

$$[P, S] = 0. \tag{3.18}$$

When n steps of permutation "protocol" are realised, we obtain

$$(PS)^n\,|\psi\rangle = P^n(S^n\,|\psi\rangle) = S^n(P^n\,|\psi\rangle) \tag{3.19}$$

Whence permutation does not afflict dynamics of system. It only manifests as some final permutation of components of vector. Or can be viewed as a permutation of basal vectors before we start purification. Dynamics of operator S is known and no new behaviour is brought to the system.

Situation slightly changes as we take matrices σ_j and construct operators 2.15 (A.5). Obviously, these matrices can be expressed as

$$S_{ij} = DP = PD' \tag{3.20}$$

where $D, D' \in \{\pm\sigma_k \otimes \pm\sigma_l | k, l \in \{3, 4\}\}$ and P, P' are some permutation matrices. It is utmost convenient that D, D' are diagonal with entries ± 1 and thus using 3.1 we write $SD = S$ (but not $DS = S$!). Together with 3.19 we get

$$(S_{ij}S)^n\,|\psi\rangle = (DPS)^n\,|\psi\rangle \overset{SD=S}{=} DPSPS...PS\,|\psi\rangle = DP^n(S^n\,|\psi\rangle) \tag{3.21}$$

Permutations and tensor products of Pauli matrices behave in a very similar way. They do not modify chaotical behaviour of purification protocol, but simply permute componets of vectors after application of S (can be viewed as basis change before purification) and using of S_{ij} changes signs of some result vector components. It is worth of notice that only one sign change represented by D is applied.

Moreover, when order of permutation matrix P or its arbitrary multiple is taken as a number of iterations of purification protocol $S_{ij}S$, it has no other effect then changing signs of some components of vector resulted form the action of S. This sign exchange has no important result for measuring probabilities. We conclude that "permutation protocols" are useless for entanglement purification.

3.4 Properties of generalised Hadamard operators

As we can notice, matrices 2.6-2.9 have interesting forms. They are not only rotations but also Hadamard type matrices (more information in appendix C). We can construct operators H_{ij} (2.16, A.6) which are more general form of H_{11} that has been discussed.

To determine the behaviour modification of this set of twirling operators we need to realise (maybe more than) few connections. And we will use special set of matrices which were already discused in previous paragraph and which we will for simplicity refer to as prepermutation matrices

Definition 3.4.1. *We call matrix $D \in \mathbb{C}^{n,n}$* preidentical*, if $D \odot D = \mathbb{1}$. Preidentical matrix D is said to be* balanced*, if $Tr(D) = 0$. We call $Q \in \mathbb{C}^{n,n}$* prepermutation matrix*, if there exist a preidentical matrix D and a permutation matrix $P \in \mathscr{S}_n$ such that*

$$Q = DP \tag{3.22}$$

Set of all prepermutation matrices of order n will be denoted $\widetilde{\mathscr{S}_n}$.

Note 3.4.2. *Preidentical matrix is a diagonal matrix with (diagonal) entries from $\{-1, 1\}$. Prepermutation matrix $Q = DP$ has entries from $\{-1, 0, 1\}$ and can be also written as $Q = PD'$, for some (generally $D \neq$) D' preidentical. If element $Q_{ij} \neq 0$, then $D_{jj} = Q_{ij} = D'_{ii}$. Obviously, each preidentical matrix and each permutation matrix is also a prepermutation matrix. $\#\{D \in \mathbb{C}^{n,n} | D$ is preidentical$\} = 2^n$, $\#\widetilde{\mathscr{S}_n} = 2^n n!$.*

Proposition 3.4.3. *Each balanced preidentical matrix can be expressed as some tensor product of elements from $\{\pm\sigma_3, \pm\sigma_4\}$.*

Proof. If not obvious, check $\pm\sigma_3 \otimes \sigma_4, \pm\sigma_4 \otimes \sigma_3, \pm\sigma_3 \otimes \sigma_3$. □

Proposition 3.4.4. $(\forall i, j, k, l \in \hat{4})(\exists P, Q \in \mathscr{S}_4)(H_{ij} = QH_{kl}P)$.

Proof. Because of permutation composition, it is sufficient to show the case $k = l = 1$. We shall consider H_i for $i \in \hat{4}$. Lets denote X_1 the nontrivial permutation from $\mathscr{S}_2$. From 2.6-2.9 it is easy to see

$$\left.\begin{array}{c} H_2 = H_1 X_1 \\ H_3 = X_1 H_1 \\ H_4 = X_1 H_1 X_1 \end{array}\right\} \tag{3.23}$$

Now we use rule for mixed products A.0.1. We get $P, Q \in \mathscr{S}_2 \otimes \mathscr{S}_2 \subset \mathscr{S}_4$[2]. For example $H_{34} = H_3 \otimes H_4 = (X_1.H_1.\mathbb{1}) \otimes (X_1.H_1.X_1) = (X_1 \otimes X_1)(H_1 \otimes H_1)(\mathbb{1} \otimes X_1) =: PH_{11}Q$. We have thus proven that P, Q are not only permutations, but they are tensor products of "local" permutations. □

Note 3.4.5. *This proposition is not true for general Hadamard matrices H', H''. Consider $H' = H$ and H'' equal to H with first row negated. While the first matrix has 6 minus signs, the other has 10 minus signs and no row and column swapping can induce new minus signs.*

[2]This relation is in fact proved in 3.5.2.

Proposition 3.4.6. $(\forall P \in \mathscr{S}_4)(\exists Q \in \widetilde{\mathscr{S}_4})(HP = QH)$.

Proof. From group $\mathscr{S}_4$ we choose two special elements:

$$R := P_{19} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad X := P_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{3.24}$$

Matrix R is the *primary permutation matrix* and X is the matrix of our well known CNOT gate. These two permutations can be composed into any permutation $\in \mathscr{S}_4$, see apendix B.3. Therefore we show existence of Q prepermutation matrix for cases $P = R, P = X$ at first. These situations are simple. Since H has the property

$$H = H^T = H^{-1}, \tag{3.25}$$

we are allowed to use for arbitrary matrix M

$$HM = HM\mathbb{1} = HM(HH) = (HMH)H \tag{3.26}$$

which we will use very often. In this proof we use it to determine Q.

$$HRH = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \mathrm{diag}(1,-1,-1,1)X =: Q_1 \in \widetilde{\mathscr{S}_4} \tag{3.27}$$

$$HXH = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} = XR^2XR =: Q_2 \in \mathscr{S}_4 \subset \widetilde{\mathscr{S}_4} \tag{3.28}$$

Pay attention to the fact $\mathrm{diag}(1,-1,-1,1) = \sigma_3 \otimes \sigma_3$.

For general permutation we can write $HR^{i_1}X^{i_2}R^{i_3}X^{i_4}R^{i_5} = Q_1^{i_1}Q_2^{i_2}Q_1^{i_3}Q_2^{i_4}Q_1^{i_5}H$. Using $\widetilde{\mathscr{S}_4} \circ \widetilde{\mathscr{S}_4} = \widetilde{\mathscr{S}_4}$ we finish the proof of the statement. □

Note 3.4.7. *This proposition is obviously valid also for matrices of order 2, when used H_1 instead of H. Only two permutation matrices of order 2 exist - the identity, which trivially satisfies the statement $H_1\mathbb{1} = \mathbb{1}H_1$; the other is the X_1 which gives $H_1X_1 = \sigma_3H_1$. As H_{ij} is formed from H via some tensor products of $\mathbb{1}, X_1$, we can use the mixed product rule(A.0.1) to transfer tensor product of permutations, see example:*

$$\begin{aligned}(H_1 \otimes H_1)(\mathbb{1} \otimes X_1) = (H_1\mathbb{1}) \otimes (H_1X_1) = (\mathbb{1}H_1) \otimes (\sigma_3 H) = \\ = (\mathbb{1} \otimes \sigma_3)(H_1 \otimes H_1).\end{aligned} \tag{3.29}$$

Therefore: $H_{ij} = DPH$, where D is preidentical and P permutation, implies that P is a tensor product of order 2 permutations.

These two propositions give following important statement:

Theorem 3.4.8. $(\forall i,j \in \hat{4})(\exists Q \in \widetilde{\mathscr{S}_4})(H_{ij} = QH)$.

Note 3.4.9. *Using this equation and existence of inverse matrix (3.25) we see that $Q = H_{ij}H$. Q can be expreesed as $Q = PD$ for some D preidentical and P permutation. Using $D^{-1} = D$, $P^{-1} = P^T$ we see $H_{ij} = PDH \Leftrightarrow H = DP^T H_{ij}$.*

Note 3.4.10. *Last proposition is valid for H_{ij} matrices only, as it relies on 3.4.4. Of course, for a Q prepermutation matrix, QH is Hadamard matrix again. But we consider appropriate to mention that it is known that any Hadamard matrix of order 4 can be expressed as QH, where Q is some prepermutation matrix. We do not claim this statement to be true for general Hadamard matrices regardless dimensions $H_A H_B \overset{?}{\in} \widetilde{\mathscr{S}_n}$ where H_A, H_B are arbitrary Hadamard matrices, although it is possible for some subsets (consider orthogonality of columns and rows of the matrix with suitable sign changes).*

Proposition 3.4.11. *Expression $H_{ij} = DPH$, where P is permutation and D preidentical, implies D is balanced or $\pm\mathbb{1}$.*

Proof. We use previous statements 3.4.4, 3.4.6: $H_{ij} = QHP$ for some permutations P, Q. We decompose P into multiplex of R, X and transfer it through H.

At first, suppose $P = X$ or $P = R$. As we have already seen, X is transferred into permutation matrix, no preidentical matrix is involved, $D = \mathbb{1}$. Supposing $P = R$ we have $H_{ij} = D'P'H$. We have seen $D' = \mathrm{diag}(1, -1, -1, 1)$ and thus is balanced.

For P general composition of X,R matrices, transformation $HP = P'H$, $P' \in \widetilde{\mathscr{S}}$ yields only matrices D' combined with permutations. After taking all these preidentical matrices in front of the permutations (using property from 3.4.2 we see number of minus signs does not change) and mutual multiplication we can get only diagonal matrix with zero/two/four plus ones and four/two/zero minus ones which grants the statement. □

Proposition 3.4.12. $(\exists Q \in \mathscr{S}_4)(\forall P \in \mathscr{S}_4)(QH \neq HP)$,
$(\exists Q \in \widetilde{\mathscr{S}_4} \setminus \mathscr{S}_4)(\forall P \in \mathscr{S}_4)(HP \neq QH)$.

Proof. We shall present examples. Consider $Q = R$. Using $P = HRH$ thanks to 3.24, 3.26, we obtain $P = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \notin \mathscr{S}_4$. Consider $Q = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$. Then $P = \begin{pmatrix} 1 & -1 & -1 & -1 \\ -1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 \\ -1 & -1 & -1 & 1 \end{pmatrix} \notin \mathscr{S}_4$, even $P \notin \widetilde{\mathscr{S}_4}$. □

Note 3.4.13. *We can also in analogue prove that there is Q' prepermutation such that $H_{ij} = HQ'$. But this direction is useless for further purposes because $Q'S \neq SQ'$.*

Taking into consideration one iteration of protocol given by $H_{ij}S$, we want to find fixed states

$$H_{ij}S\,|\psi\rangle = QHS\,|\psi\rangle = |\psi\rangle \tag{3.30}$$

Theorem 3.4.14. *Let M be an arbitrary matrix, D be an arbitrary preidentical matrix. Operator MS has a fixed state $|\psi\rangle$ if and only if operator DMS has a fixed state $D\,|\psi\rangle$.*

Proof. We can easily show that equations for fixed states are equivalent:

$$\begin{aligned} MS\left|\psi\right\rangle = MSD\left|\psi\right\rangle &= \left|\psi\right\rangle \\ \Updownarrow \quad /D. &\quad (D \text{ is regular}) \\ DMS\left|\psi\right\rangle = DMSD\left|\psi\right\rangle &= D\left|\psi\right\rangle . \end{aligned}$$

□

Theorem 3.4.15. *There exists a prepermutation matrix $Q \in \widetilde{\mathscr{S}_4}$ such that for any fixed state $\left|\psi\right\rangle$ of given H_{ij} there is a fixed state $\left|\psi'\right\rangle$ of H satisfying $\left|\psi'\right\rangle = Q\left|\psi\right\rangle$. There is a bijection between sets of fixed states of H_{ij} and H.*

Proof. Suppose fixed state of HS expressed as $PD\left|\psi\right\rangle$ for some permutation matrix P and preidentical D. Then (using previous theorem)

$$HSPD\left|\psi\right\rangle = PD\left|\psi\right\rangle \Leftrightarrow (P^THP)SD\left|\psi\right\rangle = D\left|\psi\right\rangle \Leftrightarrow (DP^THP)S\left|\psi\right\rangle = \left|\psi\right\rangle \quad (3.31)$$

If $DP^THP = H_{ij}$, we have the statement with $Q = PD \in \widetilde{\mathscr{S}_4}$. However existence and actual form of such P, D is not intuitive.

First of all, we do not have to care for D matrix thanks to the previous theorem. We want to study $P^THP = H_{ij} = Q'H$ while we know Q' are only special prepermutation matrices (tensor products). Therefore we track the action of a map $P_i \to Q' = P_i^THP_iH$, $\forall i \in \widehat{24}$. Lets label preidentical matrices with their minus signs positions:

$$D_{12} = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, D_{13} = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, D_{24} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \dots \quad (3.32)$$

Now we can write

$$\left.\begin{array}{lll} P_1^THP_1H = \mathbb{1} & P_2^THP_2H = P_4 & P_3^THP_3H = \mathbb{1} \\ P_4^THP_4H = P_4 & P_5^THP_5H = P_5 & P_6^THP_6H = P_5 \\ P_7^THP_7H = D_{14}P_{12} & P_8^THP_8H = D_{13}P_8 & P_9^THP_9H = D_{14}P_{16} \\ P_{10}^THP_{10}H = D_{13}P_{20} & P_{11}^THP_{11}H = D_{12}P_{17} & P_{12}^THP_{12}H = D_{12}P_{21} \\ P_{13}^THP_{13}H = D_{14}P_{12} & P_{14}^THP_{14}H = D_{13}P_8 & P_{15}^THP_{15}H = D_{14}P_{16} \\ P_{16}^THP_{16}H = D_{13}P_{20} & P_{17}^THP_{17}H = D_{12}P_{17} & P_{18}^THP_{18}H = D_{12}P_{21} \\ P_{19}^THP_{19}H = D_{34}P_9 & P_{20}^THP_{20}H = D_{34}P_9 & P_{21}^THP_{21}H = D_{24}P_{13} \\ P_{22}^THP_{22}H = D_{23}P_{24} & P_{23}^THP_{23}H = D_{24}P_{13} & P_{24}^THP_{24}H = D_{24}P_{24} \end{array}\right\} \quad (3.33)$$

For simplicity, set of permutation matrices P' obtained as $P^THPH = D'P'$ for some D' preidentical will be denoted

$$\mathscr{S} := \{P_1, P_4, P_5, P_8, P_9, P_{12}, P_{13}, P_{16}, P_{17}, P_{20}, P_{21}, P_{24}\}. \quad (3.34)$$

Only those Hadamard matrices H', that have decomposition $H' = D'P'$ for D' arbitrary preidentical and $P' \in \mathscr{S}$ can be decomposed into DP^THP.

Fortunately, H_{ij} are bound to H via tensor product of permutations 3.4.7. That means the decomposition into $D'P'$ involves $\{P_1, P_8, P_{17}, P_{24}\} \subset \mathscr{S}$. Therefore H_{ij} have decomposition DP^THP and fixed states are connected by a prepermutation matrix $Q = PD$. Because each prepermutation matrix is regular, such a map is a bijection. □

Corollary 3.4.16. *The fixed states of H_{ij} for $\forall i,j \in \hat{4}$ are determined from the knowledge of the fixed states of H. They are up to a prepermutation matrix multiplication (component swapping and minusing) equal to the fixed states of H. There is the same number of the states. The only thing we need to determine are the exact forms of Q matrices defined in the proof, that is we need to decompose $H_{ij} = DP^THP$ using relations 3.33 to determine suitable P, D.*

Corollary 3.4.17. *The found decomposition $H_{ij} = DP^THP$ and corresponding Q in fact perform much more then connection of the fixed states. Q is regular and transforms the whole vector space $\mathbb{C}^4$ allowing us to determine image of arbitrary vector under $H_{ij}S$ only from knowledge of images of all vectors under HS:*

$$H_{ij}S\left|\phi\right\rangle = (Q)^{-1}HSQ\left|\psi\right\rangle. \tag{3.35}$$

Note 3.4.18. *This is possibly the most important theorem of this work. It shows that some set of operators may have similar dynamics up to a global space transformation. Analogy of this statement will appear further even for other operators.*

Note 3.4.19. *There indeed are operators $H'S$ that do not have their fixed states related to the fixed states of HS. As $\#\mathscr{S} = \frac{\#\widetilde{\mathscr{S}_4}}{2}$ we can see that exactly half of Hadamard matrices have the decomposition DP^THP and exactly half do not. We admit a considerable fact, that $\mathscr{S}$ are all even permutations. This fact is mysterious at the moment as I have not been able to find any connections in literature and I can not see deeper relations of permutation matrices and Hadamard matrices. Therefore, deeper investigation of this observation is suggested.*

Next step of studying H_{ij} operators as the local twirling modifiers of purification protocol is finding cycles of H_{ij} (with periods > 1).

Theorem 3.4.20. *There exists a prepermutation matrix $Q \in \widetilde{\mathscr{S}_4}$ such that for any n-length cycle of H_{ij} determined by $\left|\psi\right\rangle$ there is a n-length cycle of H determined by $\left|\psi'\right\rangle$ satisfying $\left|\psi'\right\rangle = Q\left|\psi\right\rangle$. There is a bijection between sets of n-cycles of H_{ij} and H.*

Proof. In 3.4.15 we have discussed existence of decomposition $H_{ij} = DP^THP$. For we prooved such a decomposition exists, we can write

$$\begin{aligned}(H_{ij}S)^n = (DP^THPS)^n = DP^TH(PSDP^TH)^{n-1}PS = \\ = DP^TH(SPP^TH)^{n-1}PSD = DP^T(HS)^nPD\end{aligned} \tag{3.36}$$

This implies that for vector $\left|\psi\right\rangle$ satisfying $(HS)^nQ\left|\psi\right\rangle = Q\left|\psi\right\rangle$ ($Q = PD$ again)

$$(H_{ij}S)^n\left|\psi\right\rangle = \left|\psi\right\rangle \tag{3.37}$$

We see that the whole cycle $(Q\left|\psi\right\rangle, HSQ\left|\psi\right\rangle, (HS)^2Q\left|\psi\right\rangle, \ldots, (HS)^{n-1}Q\left|\psi\right\rangle)$ of HS is joint to the cycle $(\left|\psi\right\rangle, H_{ij}S\left|\psi\right\rangle, (H_{ij}S)^2\left|\psi\right\rangle, \ldots, (H_{ij}S)^{n-1}\left|\psi\right\rangle)$. □

Note 3.4.21. *The same situation concerning the whole space $\mathbb{C}^4$ transformation for single iteration occurs for multiple iterations as well.*

Corollary 3.4.22. *We conclude there is an universal space transformation of $\mathbb{C}^4$ allowing to determine the whole behaviour of $H_{ij}S$ from the knowledge of behaviour of HS. All considered vectors and vectors set (e.g. Julia set...) are only transformed using map determined by Q. It is therefore sufficient to study only H when concerning H_{ij} matrices. However, there exist another set of Hadamard matrices that are not connected with H in this way (expressed as an odd pemutation of H, see note 3.4.19).*

Motivated by this situation we give following definition.

Definition 3.4.23. *We say twirling operators A_1, A_2* induce equivalent dynamics*, if there exists a decomposition $A_2 = DP^T A_1 P$ for some D preidentical matrix, $P \in \mathscr{S}_4$.*

Note 3.4.24. *The use of word "equivalent" is correct here as this relation satisfies reflexivity: trivially $D = P = \mathbb{1}$; symmetry: $A_2 = DP^T A_1 P \Leftrightarrow A_1 = PDA_2P^T = D'PA_2P^T$; transitivity: $A_2 = DP^T A_1 P \wedge A_3 = D'P'^T A_2 P' \Rightarrow A_3 = D'P'^T DP^T A_1 PP' = D'D''(PP')^T A_1 PP'$. It is therefore sufficient to examine only one matrix of the class of equivalence when investigating dynamics; rest can be obtained using 3.4.20, 3.9.*

Because of 3.4.22 and relationship of H_{ij} and H mentioned in the proof of 3.4.15, all these operators have one of the Bell states as a fixed state and have two particular length 2 cycles composed of separable states or equal superpositions of the basis states.

3.5 Combination of Hadamard and Pauli matrices

Now we shall change our local twirling operator more dramatically. Lets consider matrices M_{ij}, W_{ij} defined in 2.17, 2.18 (or listed in A.7, A.8). They have following general property:

Note 3.5.1. *Matrices M_{ij}, W_{ij} have exactly half of entries equal to 0 (consequence of tensor product of 2.6-2.9, 2.10-2.13). We present here two representative elements*

$$M_{11} = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{pmatrix}, W_{42} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & -1 & 1 \end{pmatrix} \tag{3.38}$$

Lemma 3.5.2. *$\widetilde{\mathscr{S}_m} \otimes \widetilde{\mathscr{S}_n} \subset \widetilde{\mathscr{S}_{m+n}}$. In particular, $(\forall i,j \in \hat{4})(\sigma_i \otimes \sigma_j \in \widetilde{\mathscr{S}_4})$.*
If $\sigma_i \otimes \sigma_j = DP$, P permutation, D preidentical, then D is balanced or $\pm\mathbb{1}$.

Proof. If $P \in \widetilde{\mathscr{S}_m}, Q \in \widetilde{\mathscr{S}_n}$, then they have exactly one nonzero element in each row and each column. Suppose $(P)_{kl} \neq 0 \wedge (Q)_{pr} \neq 0$, for some $k,l \in \hat{m}$, $p,r \in \hat{n}$. Then tensor product has

$(P \otimes Q)_{(k-1)n+p,s} \begin{cases} = (P)_{kl}(Q)_{pr} \neq 0 & \text{for } s = (l-1)n + r, \\ = 0 & \text{for } s \neq (l-1)n + r \end{cases}$. Thus there is only one nonzero element in the $(k-1)n+p$ row of $P \otimes Q$. The same property can be verified for columns, $P \otimes Q$ is therefore up to signs a permutation matrix.

Tensor product of $\pm\sigma_i$ matrices can yield only matrix with 4, 2 or 0 minus signs. Factoring these minuses out into diagonal D implies

$$\mathrm{Tr}(D) = -4 \ \vee \ \mathrm{Tr}(D) = 0 \ \vee \ \mathrm{Tr}(D) = 4 \tag{3.39}$$

which gives the last part of the lemma. □

Note 3.5.3. $(\forall i,j \in \hat{4})(\exists k \in \hat{4})(\sigma_i H_j, H_j\sigma_i \in \{-H_k, H_k, -\sigma_3 H_k, \sigma_3 H_k | k \in \hat{4}\})$, $(\forall i,j \in \hat{4})(\exists k \in \hat{4})(\sigma_i\sigma_j \in \{-\sigma_k, \sigma_k | k \in \hat{4}\})$. *The later statement are in fact well Pauli matrices commutation relations. The first statement can be verified easily. As a consequence,* $(\forall i,j \in \hat{4})(\exists k \in \hat{4})(H_i H_j \in \{-\sigma_k, \sigma_k | k \in \hat{4}\})$.

Proposition 3.5.4. $(\forall i,j \in \hat{4})(\exists Q, Q' \in \widetilde{\mathscr{S}_4})(M_{ij} = QM_{11}, W_{ij} = Q'W_{42})$

Proof.

$$\begin{aligned} M_{ij} &= H_i \otimes \sigma_j = H_i H_1 H_1 \otimes \sigma_j\sigma_1\sigma_1 = (H_i H_1 \otimes \sigma_j\sigma_1)(H_1 \otimes \sigma_1) = \\ &= \pm(\sigma_k \otimes \sigma_l) M_{11} \end{aligned} \tag{3.40}$$

$$\begin{aligned} W_{ij} &= \sigma_i \otimes G_j = \sigma_i\sigma_4 \otimes H_j H_3 H_2 = (\sigma_i\sigma_1 \otimes H_j H_3)(\sigma_4 \otimes H_2) = \\ &= \pm(\sigma_k \otimes \sigma_l) W_{14} \end{aligned} \tag{3.41}$$

is granted form previous note. The previous lemma then completes the proof. □

Proposition 3.5.5. $(\exists i,j \in \hat{4})(\forall P \in \mathscr{S}_4)(\forall D$ *preidentical*$)(M_{ij} \neq DPM_{11}P)$, $(\exists i,j \in \hat{4})(\exists P \in \mathscr{S}_4)(\forall D$ *preidentical*$)(W_{ij} \neq DPW_{42}P)$.

Proof. Have been checked manually. One of failing example for M_{11} is M_{24}, for W_{42} one cannot decompose for example W_{11}. □

Note 3.5.6. *We emphasize this to be an analogue to 3.4.15. However, not valid now. Permutation "envelope" does not exist this time, it is not sufficient to pick some* $M_{\bullet\bullet}$ *and some* $W_{\bullet\bullet}$ *and examine only their dynamics.*

However, we will show that there exist two universal matrices M, W, such that the dynamics of $A \in M_{ij} \cup W_{ij}$ is equivalent to one of the dynamics generated by M, W.

Note 3.5.7. *For* $M' = DM$ *with* D *preidentical, we know* M' *and* M *induce equivalent dynamics (3.4.14). As a consequence, operators inside sets* $\{M_{11}, M_{12}, M_{21}, M_{22}\}$, $\{M_{14}, M_{13}, M_{23}, M_{24}\}$, $\{M_{41}, M_{42}, M_{32}, M_{31}\}$, $\{M_{44}, M_{43}, M_{33}, M_{34}\}$, $\{W_{11}, W_{12}, W_{21}, W_{22}\}$, $\{W_{14}, W_{13}, W_{23}, W_{24}\}$, $\{W_{41}, W_{42}, W_{32}, W_{31}\}$, $\{W_{44}, W_{43}, W_{33}, W_{34}\}$ *must induce the same dynamics.*

Theorem 3.5.8. *Operators in set* $\{M_{11}, M_{12}, M_{21}, M_{22}, M_{31}, M_{32}, M_{41}, M_{42}, W_{11}, W_{12}, W_{13}, W_{14}, W_{21}, W_{22}, W_{23}, W_{24}\}$ *induce equivalent dynamic; operators from* $\{M_{13}, M_{14}, M_{23}, M_{24}, M_{33}, M_{34}, M_{43}, M_{44}, W_{31}, W_{32}, W_{33}, W_{34}, W_{41}, W_{42}, W_{43}, W_{44}\}$ *also induce equivalent dynamics. Dynamics induced by these two sets are not mutually equivalent in the sense of the definition 3.4.23*

Proof. First we conveniently define new matrices:

$$M := \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 \\ -1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}, W := \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & -1 & 1 \\ 1 & -1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix} \tag{3.42}$$

Now, we present existence of suitable decomposition matrices for certain elements of sets mentioned in the previous note.

$$M = P_6^T M_{24} P_6 = P_{19}^T M_{34} P_{19} = P_5^T W_{42} P_5 = P_9 W_{43} P_9 \tag{3.43}$$

$$W = P_4^T M_{11} P_4 = P_{13}^T M_{41} P_{13} = P_2^T W_{11} P_2 = P_7^T W_{14} P_7 \tag{3.44}$$

Equivalence properties of relation "induce the same dynamics" complete the proof of the first part of the theorem. Nonequivalence of dynamics will be clear when investigating M and W in detail. □

3.6 Cycles of operator M

Single iteration of MS transforms

$$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 \\ -1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} S \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} a^2 + c^2 \\ b^2 - d^2 \\ -a^2 + c^2 \\ b^2 + d^2 \end{pmatrix} \tag{3.45}$$

Furthermore, because of the zero element structure of M we can cut the dynamics into two independent parts:

$$MS \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = MS \begin{pmatrix} a \\ 0 \\ c \\ 0 \end{pmatrix} + MS \begin{pmatrix} 0 \\ b \\ 0 \\ d \end{pmatrix}. \tag{3.46}$$

This relation is a single piece of linear behaviour, we will take advantage of it of course. As a, c and b, d pairs play similar roles, system is virtually split into two subsystems[3]. Iterations mix components so that a, c and b, d are independent pairs. Now operator S manifests again suppressing subsystem with component of smaller magnitude, if there is one. If both subsystems have components with the highest magnitude, behaviour is more complicated. However, this allows us to study these subsystems individually and then compose global vectors from them.

Consider situation $b = 0 = d$. Search for fixed states reduces impressively to

$$\begin{pmatrix} a \\ c \end{pmatrix} = \begin{pmatrix} a^2 + c^2 \\ -a^2 + c^2 \end{pmatrix}. \tag{3.47}$$

This system for $a = 0$ gives $c = 0$ yielding only the trivial solution. For $a \neq 0$ we can choose $a = 1$ and we solve system

$$k = c^2 + 1\,, \quad kc = c^2 - 1 \tag{3.48}$$

for which we find out that c is a root of

$$\mathcal{P}(x) = x^3 - x^2 + x + 1, \tag{3.49}$$

that is

$$\begin{aligned} c_1 &= \tfrac{1}{3}\left(1 + \sqrt[3]{3\sqrt{33} - 17} - \tfrac{2}{\sqrt[3]{3\sqrt{33}-17}}\right) =: \kappa_1 \\ c_{2,3} &= \tfrac{1}{6}\left(2 + (-1 \pm i\sqrt{3})\sqrt[3]{3\sqrt{33} - 17} + \tfrac{2(1 \pm i\sqrt{3})}{\sqrt[3]{3\sqrt{33}-17}}\right) =: \kappa_{2,3} \end{aligned} \tag{3.50}$$

[3] not physically!

Same situation happens for $a = 0 = c$. We get trivial solution or $d = 1$ and b roots of 3.49, $b_i = \kappa_i$. As we have two independent subsystems fixed states, we can now try to compose any global fixed state.

1. combination of trivial subsolutions

   We get single fixed state, the trivial.

2. combination of trivial and nontrivial subsolutions

   Lets choose $a = 0 = c$, then we can choose any subsolution for b, d. This way we obtain three solution with $a = 0 \neq d$, swapping the trivial and nontrivial part we get another three solutions with $a \neq 0 = d$.

3. combination of nontrivial subsolutions

   We try to put together

$$\vec{m}_{1,2,3} = \begin{pmatrix} 1 \\ 0 \\ \kappa_{1,2,3} \\ 0 \end{pmatrix}, \vec{m'}_{1,2,3} = \begin{pmatrix} 0 \\ \kappa_{1,2,3} \\ 0 \\ 1 \end{pmatrix}. \tag{3.51}$$

   This is the only place where we have to care for the "eigenvalues" $k_i = 1 + c_i^2 = 1 + b_i^2$, because relative ratio $d : a =: q$ cannot be arbitrary. Fixed states equations

$$MS \begin{pmatrix} 1 \\ q_{ij} b_j \\ c_i \\ q_{ij} \end{pmatrix} = MS \begin{pmatrix} 1 \\ 0 \\ c_i \\ 0 \end{pmatrix} + q_{ij}^2 MS \begin{pmatrix} 0 \\ b_j \\ 0 \\ 1 \end{pmatrix} = k_i \begin{pmatrix} 1 \\ 0 \\ c_i \\ 0 \end{pmatrix} + q_{ij} k_j \begin{pmatrix} 0 \\ q_{ij} b_j \\ 0 \\ q_{ij} \end{pmatrix} \tag{3.52}$$

   give possible values of q_{ij}. That is, we see we must combine solutions $\vec{m}_i, \vec{m'}_j$ in $q_{ij} = \frac{k_i}{k_j}$ ratio.

Other fixed states cannot exist, we conclude there is 1 trivial fixed state and 15 nontrivial fixed states of MS:

$$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ \kappa_i \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ \kappa_i \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ q_{ij}\kappa_j \\ \kappa_i \\ q_{ij} \end{pmatrix}; \qquad i, j \in \hat{3} \tag{3.53}$$

For the complicated form fixed states reader can verify that highest magnitude components of the vectors are contained in both subsystems.

Cycles of length two can again be composed of cycles of subsystems. Subsystem has following cycles: trivial subsolution and then 5 nontrivial solutions ($a \neq 0$). They come from

$$k \begin{pmatrix} 1 \\ c \end{pmatrix} = \begin{pmatrix} 1 + c^4 \\ -2c^2 \end{pmatrix}, \tag{3.54}$$

where we find the first solution $c = 0, k = 1$. For $c \neq 0$ system can be reduced

$$c^4 + 2c + 1 = (c - 1)\mathcal{P}(c) = 0\,, \quad k = -2c \tag{3.55}$$

It is not that surprising that polynomial 3.49 emerged here again as we know that each fixed state must emerge from longer cycle investigation. Therefore values $c_{1,2,3} = \kappa_{1,2,3}$ for fixed states remain but new solutions arises: $c_4 = 0, c_5 = 1$. Now lets compose the 6 subcycles as in previous.

1. trivial compositions

   Combining the trivial a, c with the trivial b, d subsolution we gain the trivial cycle. We can also add all 5 nontrivial b, d subsolutions (no need to care for k as trivial part can be multiplied arbitrarily) to trivial a, c cycle. The same way we can add 5 nontrivial a, c subsolutions to trivial b, d subsolution. We gained 11 cycles.

2. nontrivial compositions

   When composing nontrivial susolutions, we need to adjust ratios $q = d : a$ again. This time

$$\begin{aligned}(MS)^2 \begin{pmatrix} 1 \\ qb_j \\ c_i \\ q \end{pmatrix} = (MS)^2 \begin{pmatrix} 1 \\ 0 \\ c_i \\ 0 \end{pmatrix} + q^4 (MS)^2 \begin{pmatrix} 0 \\ b_j \\ 0 \\ 1 \end{pmatrix} = \\ = k_i \begin{pmatrix} 1 \\ 0 \\ c_i \\ 0 \end{pmatrix} + q^3 k_j \begin{pmatrix} 0 \\ qb_j \\ 0 \\ q \end{pmatrix}.\end{aligned} \tag{3.56}$$

   We stress that k_j are now different numbers given by solving 3.55. Ratio q must be chosen to satisfy $q^3 = \frac{k_i}{k_j}$ which can be done in three different ways for each given pair of subsolutions. This gives three cycles for each subsolution pair. As there are 25 nontrivial pairs, we obtain 75 solutions.

We conclude there are intotal 85 nontrivial and 1 trivial cycles of length 2 for operator MS.

$$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ c_j \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ c_j \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ q_{ijp} c_j \\ c_i \\ q_{ijp} \end{pmatrix}; \qquad m, n \in \hat{5}, p \in \hat{3} \tag{3.57}$$

As $c_5 = 0$ we see why we have chosen operator M as a representant of all the equivalent operators. It has Bell states 3.2 as parts of the length 2 cycles. Further discussion will be performed later. We are not concerned now in higher length cycles as we have already determined action of MS on Bell states which is our point of interest. Higher length cycles are determined by system of 4 polynomial equations with exponentially growing degree.

Suppose now vector with $b = c = 0 \neq a, d$. We can set $a = 1$ and so we see

$$(MS)^2 \begin{pmatrix} 1 \\ 0 \\ 0 \\ d \end{pmatrix} = MS \begin{pmatrix} 1 \\ -d^2 \\ -1 \\ d^2 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ d^4 \end{pmatrix}. \tag{3.58}$$

Taking $\mathcal{D}_1$ (see 3.11) we see that two iterations of $(MS)^2\mathcal{D}_1 \subset \mathcal{D}_1$. If d has magnitude $|d| > 1$ than even iterations converge to $\begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$. If $|d| > 1$ then the state converges to $\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$. Only as $|d| = 1$, the evolution is described by function $z \to z^4$. This function has its Julia set just equal to the unit circle. There is elementary dichotomy when we express $d = e^{i\varphi}$. For $\varphi \in \mathbb{Q}$ the state converges to $\begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$. For irrational angle φ state does not converge, d jumps along the unit circle (this does not change measuring probabilities), iterations fill the circle densely.

More detailed inspection of invariant sets in 3.9.

3.7 Cycles of operator W

As we change the class of operators, we await nonequivalent dynamics. Fixed state equation confirms our suspicions.

$$\begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & -1 & 1 \\ 1 & -1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} c^2 + d^2 \\ -c^2 + d^2 \\ a^2 - b^2 \\ a^2 + b^2 \end{pmatrix} \tag{3.59}$$

Again we see that a, b and d, c pairs are similar but this time the system does not split into two independent subsystems. Instead, subsystems are swapped by action of W. Hence, hunting for fixed states is now more difficult. Still we have a piece of linear behaviour, this time as:

$$WS \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = WS \begin{pmatrix} a \\ b \\ 0 \\ 0 \end{pmatrix} + WS \begin{pmatrix} 0 \\ 0 \\ c \\ d \end{pmatrix} \tag{3.60}$$

Suppose $a = 0$. We obtain system

$$0 = c^2 + d^2, kb = d^2 - c^2, kc = -b^2, kd = b^2. \tag{3.61}$$

Last two equations give $c + d = 0$ which when put together with the first equation gives the only one fixed state, trivial solution.

Case $0 \neq a \stackrel{!}{=} 1$ is more problematic. We shall inspire ourselves in 3.47 and rename $d \to q, c \to qc$. System of equations must be carefully simplified. As $k \neq 0$ we can express first $q = \dfrac{1 + b^2}{k}$. We obtain system

$$k^3 = (1 + b^2)^2(1 + c^2)\,,\; k^3 b = (1 + b^2)^2(1 - c^2)\,,\; (1 + b^2)c = (1 - b^2) \tag{3.62}$$

As first of these straightly gives k^3 we can put this equation easily into the second relation. $b = \pm i \vee c = \pm i$ yield no solution and for $b \neq \pm i \neq c$ we get interesting system

$$b = \frac{1-c^2}{1+c^2}\,, \qquad c = \frac{1-b^2}{1+b^2} \tag{3.63}$$

These euquations mean that b is a radix of a polynomial $x(x-1)\mathcal{P}(x)$. That makes 5 possibilities, $b_{1,2,3} = \kappa_{1,2,3,}, b_4 = 0, b_5 = 1$. Each b_m generates single value of c, three possible k (from first of 3.62) and thus three possible q. So we get 15 solutions determined by 5 values b_m. We see that they are

$$\vec{w}_{mn} = \begin{pmatrix} 1 \\ b_m \\ q_{mn}c_m \\ q_{mn} \end{pmatrix} ;\, c_m = \frac{1-b_m^2}{1+b_m^2},\, q_{mn} = \frac{1+b_m^2}{\sqrt[3]{(1+b_m^2)^2(1+c_m^2)}e^{\frac{2\pi i}{3}n}} \tag{3.64}$$

Together with the trivial state, there are 16 fixed states. That is the same amount as for M operator. But we indeed see that they are not equivalent, no prepermutation matrix can transform

$$\vec{m}_1 = \begin{pmatrix} 1 \\ 0 \\ \kappa_1 \\ 0 \end{pmatrix} \leftrightarrow \begin{pmatrix} 1 \\ b_m \\ q_{mn}c_m \\ q_{mn} \end{pmatrix} = \vec{w}_{mn} \tag{3.65}$$

because $q_{mn} \neq 0$ and at most one of b_m, c_m can be zero.

With these complications for single iteration, our search for length 2 cycles may seem now as a tough task. Nevertheless, we help ourselves again using equivalent dynamics.

Theorem 3.7.1. *Cycles of even length for operators MS and WS are the same up to a prepermutation matrix.*

Proof. We consider matrix $\tilde{M}$ defined as

$$\tilde{M} := \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} = P_{24}W = WP_{24} \tag{3.66}$$

This matrix induces the same dynamics as M because

$$M = D_{23}P_3^T\tilde{M}P_3 \tag{3.67}$$

For $2k$ number of iterations of $\tilde{M}S$, $k \in \mathbb{N}$

$$(\tilde{M}S\tilde{M}S)^k = (WP_{24}SP_{24}S)^k = (WSP_{24}P_{24}WS)^k = (WS)^{2k} \tag{3.68}$$

As even number of application of W is not only equivalent but even equal to the application of the same number of $\tilde{M}$ which is equivalent with M, statement is prooved. □

Corollary 3.7.2. *The nonequivalent behaviour of operators equivalent to M and operators equivalent to W is restricted to odd iterations only.*

We conclude there are 86 cycles of length 2 (including trivial state) that are up to a prepermutation matrix transformation equal to the cycles of M. Relation of Bell states, invariant sets and W will also be discussed later (section 3.9).

3.8 Exclusion of locality constriction

The exact forms of M and W have been chosen to be 3.42 because some of their properties are simply seen and will be used in further text. However, these matrices cannot be decomposed into a tensor product of two unitary matrices and thus do not satisfy condition on local twirling operator. In principle, this condition is essential because it allows to modify particles of EPR pairs individually. They do not need to be placed in some small spatial negihbourhood. They can be in different gallaxies and A and B can perform on them their one qubit operations, that are combined into the prescribed local twirling operator.

As the locality restriction is condemned, only unitarity is required from the twirling operator. However, modified particles need to be close enough so that the quantum gate may be applied. This compromises this purification protocol for use in quantum communication. There is no need for quantum communication when A and B must be at one place.

Nevertheless, we still are interested in general twirling operators, as we see that their dynamics may be equivalent to dynamics of systems with local twirling operator. Moreover, global twirling operators may be used in the case we can produce entangled pairs but we need to increase their entanglement immediately. That is our apparatus for producing entangled pairs is very imprecise. We can then refine states even before sending them to A and B. This option is not supposed to be realised in future, as we hope for a source of good EPR pairs.

We conclude that it is still worth to give up locality of twirling operator in order to find their dynamics which are equivalent to dynamics of some local twirling operators. If a protocol given by a nonlocal twirling operator is far superior to other local purification possibilities, we suggest to use it to purify states before sending them into the communication channels. In this case, the locality condition is not neccessary. However, another purification protocols are then needed to purify particles on their way through channels.

As we give up the locality restriction, we can search for general unitary operator with some desired properties. We present few constructions based on behaviour expected from a purification protocol. Some of them are not constructed as tensor product of rotations, but they are still somehow composed of them. We will always demand that the Bell state 3.2 is a fixed state. First of all suppose rotation generalising the CNOT gate

$$\tilde{A} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & a_{11} & a_{12} \\ 0 & 0 & a_{21} & a_{22} \end{pmatrix} \tag{3.69}$$

The submatrix must be some rotation matrix A. Fixed state condition on Bell states implies $a_{22} = 1, a_{12} = 0$. Unitarity then implies $a_{21} = 0, a_{11} = e^{i\varphi}$ for some $\varphi \in \langle 0, 2\pi)$. Such an operator AS does not mix the components of vector neither changes their magnitude. It manifests noteworthly only on special vectors which have the third and at least one another component posses the highest magnitude. In this case only slight modification to S is added, Julia set of $z \to e^{i\varphi}z^2$ is still the unit circle, just rotated. The vector will not converge unless meeting special angles. Similar construction may

be performed for other positions of $a_{11}, \ldots, a_{22}$ elements. See for example

$$A_1 = \begin{pmatrix} e^{i\tau_1}\cos\varphi_1 & 0 & 0 & e^{i(\tau_1+\vartheta_1)}\sin\varphi_1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -e^{i(\tau_1-\vartheta_1)}\sin\varphi_1 & 0 & 0 & e^{i\tau_1}\cos\varphi_1 \end{pmatrix} \tag{3.70}$$

which for $\varphi \neq \frac{k\pi}{2}$ for some $k \in \mathbb{Z}$ does not have state 3.2 as the fixed state. However, the choice $\varphi = \frac{k\pi}{2}$ makes A_1 a prepermutation matrix which significantly reduces remarkableness of the operator. Another suggestion for a twirling operator may be

$$A_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & e^{i\tau_2}\cos\varphi_2 & e^{i(\tau_2+\vartheta_2)}\sin\varphi_2 & 0 \\ 0 & -e^{i(\tau_2-\vartheta_2)}\sin\varphi_2 & e^{i\tau_2}\cos\varphi_2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{3.71}$$

with very similar properties like A_1. Or we can try to construct some convenient combination $A := A_1 + A_2 - \mathbb{1}$.

3.9 Invariant sets, operator $\mathfrak{O}$

There are certainly many interesting choices for the angles for A_1, A_2 to modify A. However as we would like to have the Bell states to be the fixed states, the only possibility is an uneventful diagonal matrix. Therefore we weaken our demands and want the Bell state 3.2 to be part of some short length cycle. One of possible choices is $\tau_1 = \tau_2$, $\vartheta_1 = 0 = \vartheta_2$, $\varphi_1 = \frac{\pi}{2} = \varphi_2$.

$$\mathfrak{O}_1 = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & -1 & 1 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix} \tag{3.72}$$

with 3.2 Bell state in length 2 cycles. We see that this operator is something we have not met yet. But it shows up that dynamics of this operator is already known. That is because

$$\mathfrak{O}_1 = P_4^T W_{42} P_4 \tag{3.73}$$

We now extend our knowledge of dynamics on a new set of operators. This set contains only nonlocal operators, however they will have very convenient behaviour. We now define some types of matrices according to their structural properties.

Definition 3.9.1. *Let $\bullet$ stand for an element $\in \{-1, 1\}$. We sort unitary matrices into sets according to their zero element structure defining*

$$\mathcal{M}_1 \textit{ type:} \begin{pmatrix} \bullet & 0 & \bullet & 0 \\ 0 & \bullet & 0 & \bullet \\ \bullet & 0 & \bullet & 0 \\ 0 & \bullet & 0 & \bullet \end{pmatrix}, \quad \mathcal{M}_2 \textit{ type:} \begin{pmatrix} 0 & \bullet & 0 & \bullet \\ \bullet & 0 & \bullet & 0 \\ 0 & \bullet & 0 & \bullet \\ \bullet & 0 & \bullet & 0 \end{pmatrix},$$
$$\mathcal{W}_1 \textit{ type:} \begin{pmatrix} \bullet & \bullet & 0 & 0 \\ \bullet & \bullet & 0 & 0 \\ 0 & 0 & \bullet & \bullet \\ 0 & 0 & \bullet & \bullet \end{pmatrix}, \quad \mathcal{W}_2 \textit{ type:} \begin{pmatrix} 0 & 0 & \bullet & \bullet \\ 0 & 0 & \bullet & \bullet \\ \bullet & \bullet & 0 & 0 \\ \bullet & \bullet & 0 & 0 \end{pmatrix}, \tag{3.74}$$
$$\mathcal{O}_1 \textit{ type:} \begin{pmatrix} \bullet & 0 & 0 & \bullet \\ 0 & \bullet & \bullet & 0 \\ 0 & \bullet & \bullet & 0 \\ \bullet & 0 & 0 & \bullet \end{pmatrix}, \quad \mathcal{O}_2 \textit{ type:} \begin{pmatrix} 0 & \bullet & \bullet & 0 \\ \bullet & 0 & 0 & \bullet \\ \bullet & 0 & 0 & \bullet \\ 0 & \bullet & \bullet & 0 \end{pmatrix}.$$

Note 3.9.2. *Unitarity grants correct ratio and placing of $+1$ and -1. Every W_{ij} and M_{ij} and their equivalent matrices mentioned so far belong to some of these sets. We mention $W \in \mathcal{W}_2$, $M \in \mathcal{M}_1$.*

Note 3.9.3. *We have not classified all matrices! There exist more types of unitary matrices with elements from $\{-1, 1\}$. See the example*

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & \bar{1} \\ 1 & \bar{1} & 0 & 0 \end{pmatrix} \in \begin{pmatrix} \bullet & \bullet & 0 & 0 \\ 0 & 0 & \bullet & \bullet \\ 0 & 0 & \bullet & \bullet \\ \bullet & \bullet & 0 & 0 \end{pmatrix} \tag{3.75}$$

These other types of matrices are beyond the scope of this thesis as they contain no considerable local twirling operator. However, it might be interesting to study their behaviour as global twirling operators. We know they must have some different dynamics than operators presented in this thesis.

Conjecture 3.9.4. *Denoting $\sim$ the "induce equivalent dynamics" relation and $\mathcal{G}_i := \mathcal{M}_i \cup \mathcal{W}_i \cup \mathcal{O}_i$ for $i = 1, 2$: $(\forall A_1, B_1 \in \mathcal{G}_1)(A_1 \sim B_1)$. $(\forall A_2, B_2 \in \mathcal{G}_2)(A_2 \sim B_2)$. $(\forall i \in \hat{2})((A \in \mathcal{G}_i \wedge B \notin \mathcal{G}_i) \Rightarrow A \nsim B)$.*

Note 3.9.5 (Kind of a proof)**.** *We shall work up to a preidentical matrix. Then set $\mathcal{G}$ has 12 different elements[4]. Each matrix $G \in \mathcal{G}_i$ is mapped to 24 matrices via all possible combinations $G \to DP^TGP$. However, each matrix is mapped onto a single matrix exactly twice. That is because of a statement we leave unproved:*

$$(\forall G \in \mathcal{G}_i)(\exists! P \in \mathscr{S}_4 \wedge \exists! D \textit{ preidentical})(P \neq \mathbb{1} \wedge DP^TGP = G). \tag{3.76}$$

As an example supporting this statement we present one of manually checked example: $W = P_{24}^T W P_{24}$, $(\forall i \in 2, 3, \ldots, 23)(\forall D \textit{ preidentical})(DP_i^T W P_i \neq W)$. We do not (try to) prove this latter statement as we consider it to be far beyond the scope of this thesis. Manual checking of tenths of matrices supports this statement, rigorous proof would require too much effort.

[4]Because there are 4 (up to a preidentical matrix) different unitary matrices in each matrix type.

As equivalent dynamics are related to transformation of the vector space, it is obvious that there may be at most one operator that has (the most) desirable action on the Bell states. We can say that the desired operator will certainly be elements of $\mathcal{G}_1$. $\mathcal{G}_2$ operators are not good candidates because of the component swapping already mentioned in 3.7. This argument can be easily seen from 3.74 because while $\mathcal{G}_1$ operators have nonzero diagonal elements (that is, the component itself influences its evolution during each protocol iteration), diagonal elements of $\mathcal{G}_2$ are equal to zero and thus component is influenced only by values of the other components for a single iteration. At least two iterations are needed to reflect value of a component into the component itself. For such operators it is however posssible to jump between Bell states.

Proposition 3.9.6. *For operators from $\mathcal{G}_1 \cup \mathcal{G}_2$, orbits generated by Bell states are preperiodic. The periods of corresponding periodic cycles are equal to two or four and jump through following set of states:*

$$\begin{pmatrix} \bullet \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ \bullet \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ \bullet \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ \bullet \end{pmatrix}, \tag{3.77}$$

$$\begin{pmatrix} \bullet \\ \bullet \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} \bullet \\ 0 \\ \bullet \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ \bullet \\ 0 \\ \bullet \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ \bullet \\ \bullet \end{pmatrix}, \tag{3.78}$$

$$\begin{pmatrix} \bullet \\ 0 \\ 0 \\ \bullet \end{pmatrix}, \begin{pmatrix} \bullet \\ \bullet \\ \bullet \\ \bullet \end{pmatrix}, \begin{pmatrix} 0 \\ \bullet \\ \bullet \\ 0 \end{pmatrix}, \tag{3.79}$$

where $\bullet$ stands for ± 1 again. Some periods of the preperiodic orbits do not have to contain the Bell states.

Proof. Results from the structure of the nonzero elements in the sets. Periods containing 3.77 are possible for $\mathcal{O}_i$ only. On contrary, equal superpositions (the middle structure from 3.79) are not contained in the periods of operators from $\mathcal{O}_i$. Oppositely for $\mathcal{M}_i \cup \mathcal{W}_i$ sets. As these facts may be not so obvious, we use illustrative examples; squares denote components from $\{-1, 0, 1\}$, exactly half of empty and half of filled boxes is equal to zero in the vectors.

$$\begin{pmatrix} \bullet & 0 & \bullet & 0 \\ 0 & \bullet & 0 & \bullet \\ \bullet & 0 & \bullet & 0 \\ 0 & \bullet & 0 & \bullet \end{pmatrix} : \quad \begin{pmatrix} \bullet \\ 0 \\ 0 \\ \bullet \end{pmatrix} \rightarrow \begin{pmatrix} \bullet \\ \bullet \\ \bullet \\ \bullet \end{pmatrix} \leftrightarrow \begin{pmatrix} \square \\ \blacksquare \\ \square \\ \blacksquare \end{pmatrix} \leftrightarrow \begin{pmatrix} \bullet \\ \bullet \\ \bullet \\ \bullet \end{pmatrix} \leftarrow \begin{pmatrix} 0 \\ \bullet \\ \bullet \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} \bullet & 0 & 0 & \bullet \\ 0 & \bullet & \bullet & 0 \\ 0 & \bullet & \bullet & 0 \\ \bullet & 0 & 0 & \bullet \end{pmatrix} : \quad \begin{pmatrix} \bullet \\ 0 \\ 0 \\ \bullet \end{pmatrix} \leftrightarrow \begin{pmatrix} \square \\ 0 \\ 0 \\ \square \end{pmatrix}, \begin{pmatrix} 0 \\ \bullet \\ \bullet \\ 0 \end{pmatrix} \leftrightarrow \begin{pmatrix} 0 \\ \square \\ \square \\ 0 \end{pmatrix} \tag{3.80}$$

□

From the last proposition we see that for the Bell state cycle analysis it is at most convenient to study operators from $\mathcal{O}_1$; $\mathcal{M}_i$ and $\mathcal{W}_i$ operators can only have separable states for cycles. For sign reasons we choose following operator:

$$\mathbf{\Theta}_2 = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & -1 & 0 \\ 1 & 0 & 0 & -1 \end{pmatrix} \tag{3.81}$$

We see that action of this operator indeed splits vector into two noninteracting subsystems: pairs a, d suitable for the first Bell states 3.2 and b, c pair suitable for the second states 3.3. As we have already discussed fixed states of this type of operator, we do now some notes on cycles. We have following important length two cycles the system might converge to:

$$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \leftrightarrow \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \leftrightarrow \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \leftarrow \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix} \leftarrow \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \tag{3.82}$$

$$\left.\begin{array}{l} \begin{pmatrix} 1 \\ \bullet \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ \bullet \\ 0 \end{pmatrix} \rightarrow \begin{pmatrix} 1 \\ \bullet \\ \bullet \\ 1 \end{pmatrix} \\ \begin{pmatrix} 0 \\ \bullet \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ \bullet \\ 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 \\ \bullet \\ \bullet \\ -1 \end{pmatrix} \end{array}\right\} \rightarrow \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} \leftrightarrow \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} \tag{3.83}$$

All separable states 3.78 are changed to a single cycle. Now we seek for invariant sets. We have

$$\mathbf{\Theta}_2 S\mathcal{C}_1 \subset \mathcal{D}_2\,,\, \mathbf{\Theta}_2 S\mathcal{D}_2 \subset \mathcal{C}_1. \tag{3.84}$$

Because these are suitable combination of vectors from our virtual subsystems a, d , b, c. In consequence: $(\mathbf{\Theta}_2 S)^2\mathcal{D}_2 \subset \mathcal{D}_2$, $(\mathbf{\Theta}_2 S)^2\mathcal{C}_1 \subset \mathcal{C}_1$. Relevant function is $f(z) = z^4$:

$$\begin{pmatrix} 1 \\ z \\ 0 \\ 0 \end{pmatrix} \overset{(\mathbf{\Theta}_2 S)^2}{\rightarrow} \begin{pmatrix} 1 \\ z^4 \\ 0 \\ 0 \end{pmatrix} \tag{3.85}$$

It is obvious that behaviour of the states from these sets is determined by prevailing component - $|z| < 1$ makes pair

$$\begin{pmatrix} 1 \\ z \\ 0 \\ 0 \end{pmatrix} \rightarrow \begin{pmatrix} 1 \\ z^2 \\ z^2 \\ 1 \end{pmatrix} \tag{3.86}$$

converge to the first of cycle 3.82. For $|z| > 1$ pair converges the second cycle of 3.82. Points $|z| = 1$ belong to Julia set of $f(z) = z^4$. Pair remains similar to 3.83 with the components jumping in some way over the unit circle.

There are another two invariant sets. One is $\mathcal{D}_1$ while the other one is

$$\mathcal{D}_4 := \left\{ \left(\begin{array}{c} 0 \\ b \\ c \\ 0 \end{array} \right) \middle| b, c \in \mathbb{C} \right\} \; ; \; \left(\begin{array}{c} 0 \\ b \\ c \\ 0 \end{array} \right) =: \left(\begin{array}{c} b \\ c \end{array} \right) \tag{3.87}$$

We shall now study this one, although it has the same properties as $\mathcal{D}_1$ as there are the same states only in different subsystems (just substitute a, d with b, c). Iterations of the purification protocol on the $b = 0$ is clear from 3.82, this leads to a length two cycle containing a Bell state. For $a \neq 0$, vectors evolve under a single iteration:

$$\left(\begin{array}{c} 1 \\ z \end{array} \right) := \left(\begin{array}{c} 1 \\ \dfrac{1 - z^2}{1 + z^2} \end{array} \right) \tag{3.88}$$

Therefore we are concerned in function

$$f(z) = \frac{1 - z^2}{1 + z^2}. \tag{3.89}$$

We remind that such a function has already been studied in [8, 47], 3.2 but were needed only under even number of iterations, that is $f(f(z)) = \dfrac{2z^2}{1 + z^4}$. Julia set is depicted on the figure 3.1 as the border of the blue regions.

There are two critical points, $z_1 = 0, z_2 = \infty$. These converge to the same superattractive cycle $0 \leftrightarrow 1$ but after different number of iterations. The whole system then converges to a length two cycle containing a Bell state 3.3 (if the a, d sybsystem would prevail, it would similarily go to the other Bell state 3.2). Points z is in the blue region, it approaches 0 in odd number of iterations, 1 in even number of iterations. Points from white region converges to 0 in even and to1 in od number of iterations. It is obvious that for relatively big perturbations (at least 0.2 but we are restricted to $\mathcal{D}_4$ only!), system is drawn back to the Bell state. In figure 3.2 one can see how fast different states of $\mathcal{D}_4$ converge to the Bell state 3.3 (or $\mathcal{D}_1$ states to 3.2).

We conclude that we have studied a very convenient operator $\mathbf{\Theta}_2$ which forms a purification protocol suitable for purifying the Bell states. We have found indirectly the fixed sets and length two cycles - relation of must be used on 3.53, 3.57 with $Q = P_5 D_{34}$ (and substituting M for H of course).

Dynamics of this operator determine (via prepermutation matrices) dynamics of 192 operators in total. Another 192 operators were also investigated, whose dynamics is equivalent to the previous dynamics when taking only even number of iterations. As operator $\mathbf{\Theta}_2$ has very convenient behaviour concerning Bell states, it is obvious that other operators cannot have such fancy behaviour (due to the prepermutation transformation of the space). That includes operators M_{ij}, W_{ij}. For these, Bell states are not preserved and separable states are gained instead. This is given by nonzero element structure 3.74 which is suitable for $\mathcal{O}_i$ operators only.

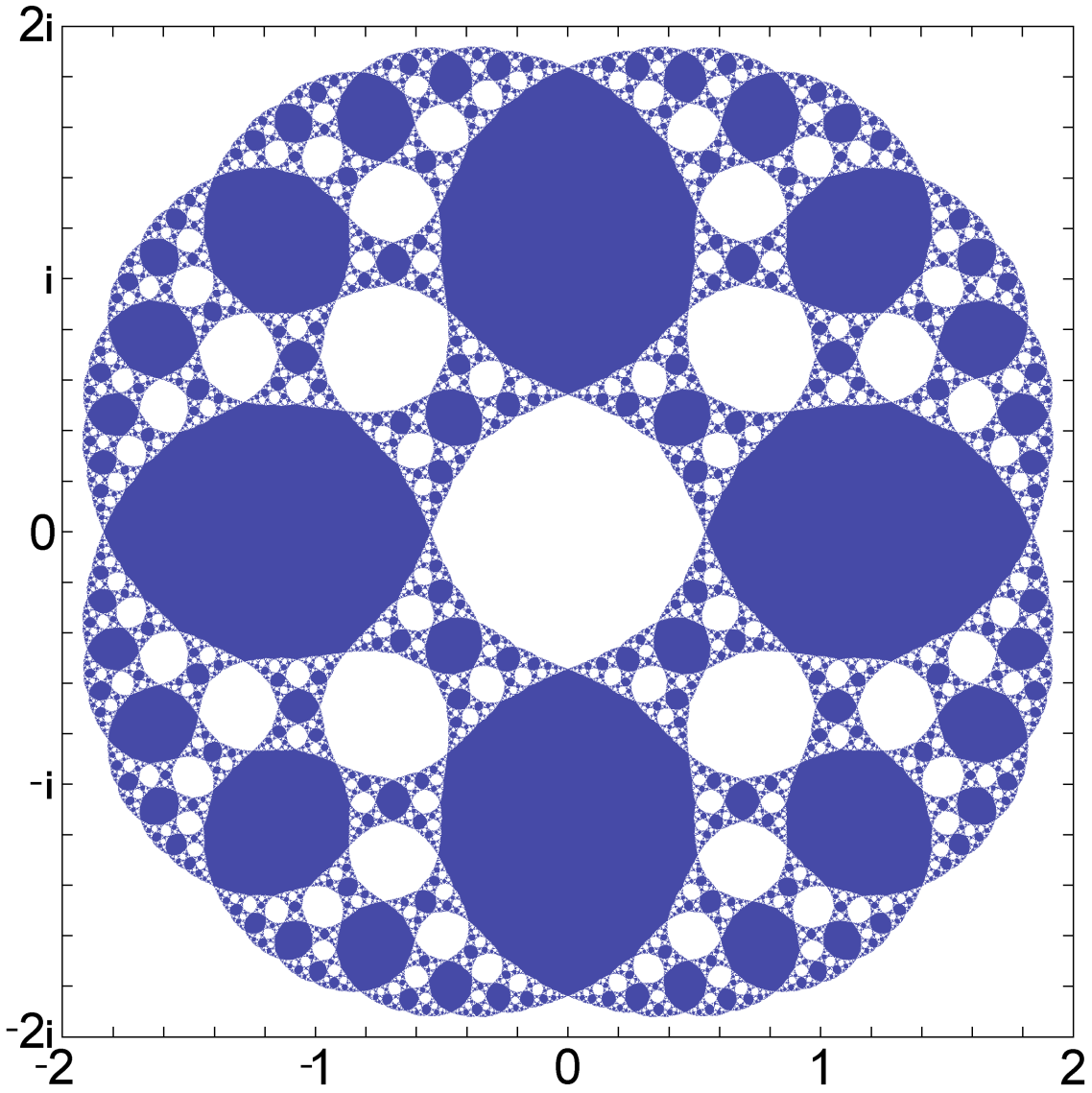

Figure 3.1: Fatou set of 3.89 is split into blue and white regions corresponding to odd- and even- convergence to 0. Their borders form the Julia set.

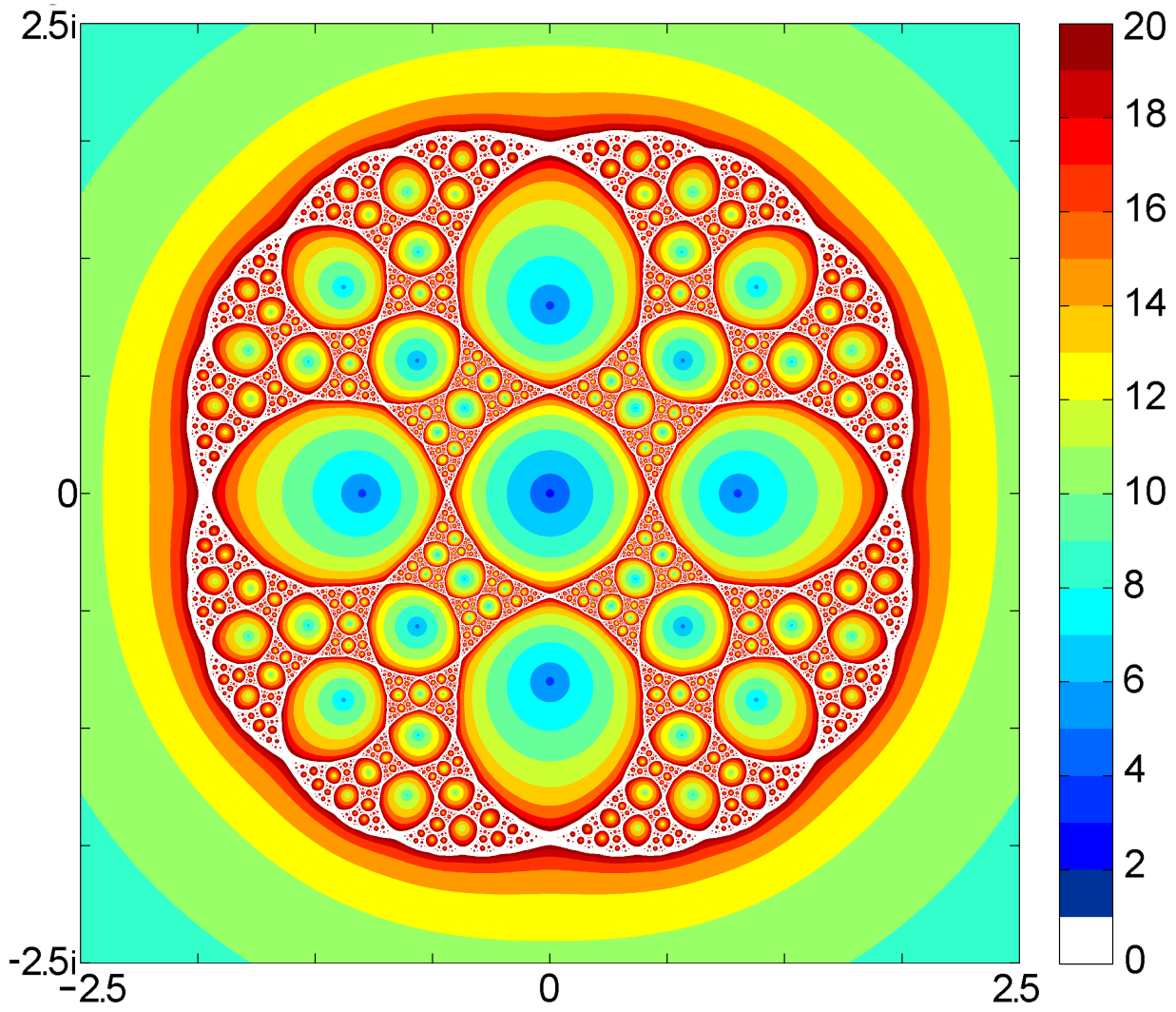

Figure 3.2: Illustration of speed of convergence. A point z is assigned colour that corresponds to n number of iteratoins needed so that point is brought close to 0, i.e. $|f^n(z)| < 0.001$. Points for which more than 20 iterations are needed and points from the Julia set are marked with white colour.

Chapter 4

Chaotic dynamics - general rotations

4.1 Generalised rotations

We would like to use some new local twirling operators to find new (and possibly better) behaviour. We will now take into account more general unitary operators on $\mathbb{C}^{2,2}$, 2.4. In comparison to previous chapter we will now do not choose the parameters in such a simple way. We will however discuss some special occasions as the general two-qubit matrix form is very intricate. One of the interesting forms is

$$R_{\varphi,0,0} = \begin{pmatrix} \cos\varphi & \sin\varphi \\ -\sin\varphi & \cos\varphi \end{pmatrix} \tag{4.1}$$

Or we can choose $\varphi = \frac{\pi}{2} \pm \frac{\pi}{4}$ so operator simplifies up to multiplication constant to

$$R_{\frac{\pi}{2}\pm\frac{\pi}{4},0,\vartheta} = \begin{pmatrix} 1 & \mp e^{i\vartheta} \\ \pm e^{-i\vartheta} & 1 \end{pmatrix}, \; R_{\frac{\pi}{2}\pm\frac{\pi}{4},\vartheta,0} = \begin{pmatrix} e^{i\vartheta} & \mp 1 \\ \pm 1 & e^{-i\vartheta} \end{pmatrix} \tag{4.2}$$

Not so apparent but convenient choice is also

$$R_{\frac{\pi}{4},\vartheta+\frac{\pi}{2},\frac{\pi}{2}} = \begin{pmatrix} e^{i\vartheta} & 1 \\ 1 & -e^{-i\vartheta} \end{pmatrix} \tag{4.3}$$

Other but not much interesting choices are generalisations of Pauli matrices

$$R_{\frac{\pi}{2},\vartheta_1,\vartheta_2} = \begin{pmatrix} 0 & e^{i\vartheta_2} \\ -e^{-i\vartheta_2} & 0 \end{pmatrix}, \; R_{0,\vartheta,\vartheta_2} = \begin{pmatrix} e^{i\vartheta_1} & 0 \\ 0 & -e^{-i\vartheta_1} \end{pmatrix} \tag{4.4}$$

Utilising the tensor product, we can certainly construct two-qubit operator composed of two general single qubit rotations, $R := R_{\varphi_1,\varphi_2,\chi_1,\chi_2,\vartheta_1\vartheta_2} = R_{\varphi_1,\chi_1,\vartheta_1} \otimes R_{\varphi_2,\chi_2,\vartheta_2}$. For spatial reasons we denote $\cos(\varphi_i) = C_i, \sin(\varphi_i) = S_i$ Such an operator looks like

$$R = \begin{pmatrix} C_1C_2e^{i(\chi_1+\chi_2)} & C_1S_2e^{i(\chi_1+\vartheta_2)} & S_1C_2e^{i(\chi_2+\vartheta_1)} & S_1S_2e^{i(\vartheta_1+\vartheta_2)} \\ -C_1S_2e^{i(\chi_1-\vartheta_2)} & C_1C_2e^{i(\chi_1-\chi_2)} & -S_1S_2e^{i(\vartheta_1-\vartheta_2)} & S_1C_2e^{i(-\chi_2+\vartheta_1)} \\ -S_1C_2e^{i(\chi_2-\vartheta_1)} & -S_1S_2e^{i(-\vartheta_1+\vartheta_2)} & C_1C_2e^{i(-\chi_1+\chi_2)} & C_1S_2e^{i(-\chi_1+\vartheta_2)} \\ S_1S_2e^{i(-\vartheta_1-\vartheta_2)} & -S_1C_2e^{i(-\chi_2-\vartheta_1)} & -C_1S_2e^{i(-\chi_1-\vartheta_2)} & C_1C_2e^{i(-\chi_1-\chi_2)} \end{pmatrix} \tag{4.5}$$

It is obvious, why we do not (even try to) find some properties for general angles. Again, we use various combinations of more general but still special cases 4.1 - 4.4; we will write only the necessary matrices when we need them and where we need them. This time we will obtain whole sets of operators depending on a parameter (angle).

4.2 Operators with parameter ϑ

As the first matrix type we consider compositions of 4.4, for example:

$$\begin{pmatrix} 0 & e^{i(\vartheta_1+\vartheta_2)} & 0 & 0 \\ -e^{i(-\vartheta_1+\vartheta_2)} & 0 & 0 & 0 \\ 0 & 0 & 0 & -e^{i(\vartheta_1-\vartheta_2)} \\ 0 & 0 & e^{i(-\vartheta_1-\vartheta_2)} & 0 \end{pmatrix}, \dots \tag{4.6}$$

These matrices are more general variants of prepermutational matrices as discussed in previous chapter, lets say they are *complex prepermutational*. Nevertheless, they do not bring any new behaviour when used as local twirling operator. Though the angles change the relative phases of vector components in some less intuitive way and yes, they permute components of vector, they do not mix the components together nor change their magnitudes. They do not modify the behaviour of S in some measurable way (relative phases of the components indeed does not have influence on the transition probabilities). As a consequence, in following sets of examples we in fact ignore behaviour alteration under complex prepermutation matrices, i.e modification by these generalised Pauli products. We might properly generalise the concept of dynamics equivalency.

Now we compose generalisation of M_{ij}, W_{ij} matrices using 2.6 - 2.9 and 4.4. We obtain (factoring out global phase factor)

$$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & -e^{i\vartheta} & 0 & -e^{i\vartheta} \\ 1 & 0 & -1 & 0 \\ 0 & -e^{i\vartheta} & 0 & e^{i\vartheta} \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & -e^{i\vartheta} & -e^{i\vartheta} \\ 0 & 0 & -e^{i\vartheta} & e^{i\vartheta} \end{pmatrix}, \dots \tag{4.7}$$

The nonzero element structure 3.74 is preserved and although the $\bullet$ symbols in the definition now denote arbitrary complex unit, it does not change the fact that Bell states cannot be the fixed states nor members of length two cycle. We might suppose that the fixed states will change. We ask our appreciated reader to be awared of paragraphs 3.6, 3.7. When similar thoughts are performed here, it is easy to see that solutions for the subsystems do not change, however they must be combined in a different ratio: $q_{ij} = e^{2i\vartheta}\dfrac{k_i}{k_j}$. In spite of the fact that nonlocal operator is now to be considered, we examine at this point a generalised variant of our favourite operator $\mathbf{\Theta}_2$ and check the invariant sets. We define

$$\mathbf{\Theta}_3 = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & e^{i\vartheta} & e^{i\vartheta} & 0 \\ 0 & e^{i\vartheta} & -e^{i\vartheta} & 0 \\ 1 & 0 & 0 & -1 \end{pmatrix} \tag{4.8}$$

and we see that $\mathcal{C}_1, \mathcal{D}_2$ share relationship 3.84 again and are still invariant upon two iterations of $\mathbf{\Theta}_3$. This time with relevant function $f(z) = e^{i\vartheta}z^4$ which has the same Julia set and similar behaviour as $f(z) = z^4$, no significant behaviour modification appears. Inside the set $\mathcal{D}_4$, 3.87, relevant function is the same as before - 3.89.

Similar situation happens with another type of matrices, combinations of Pauli matrices 2.10 - 2.13 and 4.2, 4.3. Matrices look like

$$W_\vartheta := \sigma_4 \otimes R_{\frac{\pi}{2}\pm\frac{\pi}{4},0,\vartheta} = \begin{pmatrix} 1 & e^{i\vartheta} & 0 & 0 \\ -e^{-i\vartheta} & 1 & 0 & 0 \\ 0 & 0 & 1 & e^{i\vartheta} \\ 0 & 0 & -e^{-i\vartheta} & 1 \end{pmatrix} \tag{4.9}$$

and as they are still $\mathcal{W}_i, \mathcal{M}_i$ types of matrices, they do not give desired behaviour concerning the Bell states. Moreover, their only piece of good behaviour - that the original separable states are parts of length two cycles is now lost. We are however left with new fixed states, cycles and invariant sets. Fixed states can be again found and combined through the subsystems like in 3.6, 3.7. We obtain subsolutions as results of generalised variants to prior equations 3.47:

$$k \begin{pmatrix} 1 \\ b \end{pmatrix} = \begin{pmatrix} 1 + e^{i\vartheta} b^2 \\ -e^{-i\vartheta} + b^2 \end{pmatrix}. \tag{4.10}$$

These are given as radices of generalised polynomial 3.49: $\mathcal{P}_\vartheta(x) = e^{i\vartheta}x^3 - x^2 + x + e^{-i\vartheta}$. The radices have very beautiful (i.e. long and complicated) analytic expression. We are more interested in the invariant sets which are for W_ϑ $\mathcal{D}_2$ and analogical set (pair c, d) for the other subsystem. The relevant function for evolution inside these sets is

$$f_\vartheta(z) = \frac{z^2 - e^{-i\vartheta}}{e^{i\vartheta}z^2 + 1} \tag{4.11}$$

If we label $p := -e^{-i\vartheta}$, we find that this function was studied in the article [7] (in fact, it was studied for arbitrary $p \in \mathbb{C}$). Therefore we present here only few pictures of Julia sets for various parameters. The reason for this function to emerge here is right the separability of the states in the invariant set. The two qubit system in fact behaves as a single particle and the twirling operators W_ϑ are in fact reduced to some single-qubit operators which are in general discussed in [7].

However, we could formally define

$$\mathbf{\Theta}_4 = \begin{pmatrix} 1 & 0 & 0 & e^{i\vartheta} \\ 0 & 1 & e^{i\vartheta} & 0 \\ 0 & -e^{-i\vartheta} & 1 & 0 \\ -e^{-i\vartheta} & 0 & 0 & 1 \end{pmatrix}. \tag{4.12}$$

which would apply 4.11 when acting on $\mathcal{D}_1$ (3.11) set containing Bell states 3.2. The proper choice of parameter ϑ could then enhance convergence speed. Such an operator could then be used as the desired twirling operator. Alas, rough analysis of Julia sets for all possible angles suggests only $\vartheta = k\frac{\pi}{2}$ to be suitable for purification purposes. Julia set fans out very uniformly defeating detection possibilities of author's program.

Now we come to more intricated matrices, combinations of 2.6 - 2.9 with 4.2, 4.3. We mention that these matrices can be taken as complex Hadamard matrices[1].

$$H_\vartheta := H_1 \otimes R_{\frac{\pi}{4},\vartheta+\frac{\pi}{2},\frac{\pi}{2}} = \begin{pmatrix} e^{i\vartheta} & 1 & e^{i\vartheta} & 1 \\ 1 & -e^{-i\vartheta} & 1 & -e^{-i\vartheta} \\ e^{i\vartheta} & 1 & -e^{i\vartheta} & -1 \\ 1 & -e^{-i\vartheta} & -1 & e^{-i\vartheta} \end{pmatrix} \tag{4.13}$$

[1] i.e. satisfy the orthogonality condition, but their elements are arbitrary complex units.

From 3.1.1 we know that Bell states 3.2 are the fixed states only for $1+e^{i\vartheta}=1+e^{-i\vartheta} \wedge 1-e^{-i\vartheta}=0=e^{i\vartheta}-1$. These are only valid for $\vartheta=0$, that means $H_\vartheta = H_{11}$. Same situation happens for all possible combinations of Hadamard matrices and 4.2, 4.3. The structures (see in short overiew below) of these matrices imply similar equations and allow Bell states to be fixed states only for $\vartheta=0$.

$$\begin{pmatrix} 1 & e^{i\vartheta} & 1 & e^{i\vartheta} \\ e^{-i\vartheta} & -1 & e^{-i\vartheta} & -1 \\ 1 & e^{i\vartheta} & -1 & -e^{i\vartheta} \\ e^{-i\vartheta} & -1 & -e^{-i\vartheta} & 1 \end{pmatrix}, \begin{pmatrix} e^{i\vartheta} & 1 & -e^{i\vartheta} & -1 \\ 1 & -e^{-i\vartheta} & -1 & e^{-i\vartheta} \\ e^{i\vartheta} & 1 & e^{i\vartheta} & 1 \\ 1 & -e^{-i\vartheta} & 1 & -e^{-i\vartheta} \end{pmatrix}, \dots \tag{4.14}$$

4.3 Operators with parameter φ

Disappointed by previous angle choices we now involve matrix 4.1 more into our calculations. For $\cos\varphi \neq 0$ in a single qubit gate (which led to no peculiar behaviour) we can factor this number out and get

$$R_{\varphi,\vartheta} = \begin{pmatrix} 1 & e^{i\vartheta} tg\varphi \\ -e^{-i\vartheta} tg\varphi & 1 \end{pmatrix} \tag{4.15}$$

which we now use to combine tensor products. As we can choose angles so that $e^{i\vartheta}tg(\varphi)$ is some prescribed complex number, we label it furthermore p. Two qubit gate is then

$$U = \begin{pmatrix} 1 & p_2 & p_1 & p_1p_2 \\ -\bar{p}_2 & 1 & -p_1\bar{p}_2 & p_1 \\ -\bar{p}_1 & -\bar{p}_1p_2 & 1 & p_2 \\ \bar{p}_1\bar{p}_2 & -\bar{p}_1 & -\bar{p}_2 & 1 \end{pmatrix} \tag{4.16}$$

We demand this matrix to have Bell state 3.2 as the fixed state. This is satisfied only as $p_1 - \bar{p}_2 = 0 \wedge \bar{p}_1\bar{p}_2 = p_1p_2$ which can happen only for the same magnitudes of $|p_1| = |p_2| =: r$ and phases $\vartheta_1 = -\vartheta_2$. If we further demand the Bell state 3.3 to be the transformed into the 3.2 (like in HS case), we obtain $r = \pm 1 \wedge \vartheta_1 = \vartheta_2$. Together we obtain $p = \pm 1, \vartheta_1 = 0 = \vartheta_2$. But these conditions give $U = H_{22} \vee U = H_{33}$.

We can however try another approach. We shall demand that both states 3.2, 3.3 are actually fixed. In this case we get restrictions $p_1 = p_2 =: r \in \mathbb{R}, \vartheta := \vartheta_1 = -\vartheta_2; \vartheta = \frac{\pi}{2} + k\pi \wedge (\vartheta = k\frac{\pi}{2} \vee \vartheta = \frac{\pi}{4} + k\frac{\pi}{2})$. Therefore we can choose $\vartheta = \frac{\pi}{2} \vee \vartheta = \frac{3\pi}{2}$ and arbitrary r. Matrix U then acquires following forms

$$U_{\vartheta=\pi\pm\frac{\pi}{2}} = \begin{pmatrix} 1 & \pm ir & \mp ir & r^2 \\ \pm ir & 1 & r^2 & \mp ir \\ \mp ir & r^2 & 1 & \pm ir \\ r^2 & \mp ir & \pm ir & 1 \end{pmatrix} \tag{4.17}$$

We notice that these U look like a combination of $\mathcal{O}_i$ matrices (check 3.74). More, we can notice $U_{\frac{\pi}{2}}^{-1} = U_{\frac{3\pi}{2}}$. From the construction we know, that Bell states are fixed states. However, set $\mathcal{C}_1$ (3.10, linear combination of Bell states) is invariant:

$$\begin{pmatrix} 1 \\ z \\ z \\ 1 \end{pmatrix} \to \begin{pmatrix} 1 \\ z^2 \\ z^2 \\ 1 \end{pmatrix} \tag{4.18}$$

The Julia set for a function $f(z) = z^2$ is a unit circle; For $|z| < 1$ the state converges (as $f(z) \to 0$) to the first Bell state 3.2, for $|z| > 1$ the state converges (as $f(z) \to \infty$) to the second type 3.3. Unfortunately, the behaviour in this set is independent of r. We have not found any other invariant states. The parameter r mixes the dynamics in a threedimensional manifold only. We have no tools to analyse the influence of the parameter.

4.4 Notes on operator stability

We consider important to mention that we have studied physical states subject to some nonlinear operation in order to repair some experimental damage caused by the environment. However, we have not said if we can perform the operator action perfectly. Of course these also work with some small error. The sticking point is that even this small error may induce new chaotic behaviour which is very different from the supposed dynamics. It might be interesting to employ perturbation theory and distort local twirling operator in some way.

We observe that we could take matrices from chapter 4 as perturbations of matrices from 3. However, we think that this way is not sufficient. Influence of some general perturbation might enrich dynamics in a more powerful way. We suppose it might be possible that if the local twirling operator is perturbed differently in each iteration of purification protocol, the Julia set may be torn off and disappear. It is unclear and possibly not possible to determine what would then states converge to.

One possible way how to bring new behaviour to the system is discussed in [54]. Time evolution is installed as new modification element. We suppose that time evolution can also be considered as some perturbation.

Chapter 5

Conclusion

Let us summarise what we have done in this thesis. In the theoretical chapter 2 and appendices A - D, we presented a quite extensive overview of theoretical concepts. Factual as well as some historical notes were mentioned. Quantum physics was described from its most fundamental mathematical aspect emphasising quantum entanglement, an interesting quantum phenomenon. Theory of information and computation was linked with quantum mechanics in later paragraphs. The resulting theory of quantum information allows us to search for new and superior algorithms, which exploit entanglement. Some NP-complete problems may be solved efficiently. Two important examples of quantum algorithms were demonstrated. One of important problems of quantum communication is that entanglement decays when particles are transmitted through realistic environment. This led to the invention of purification protocols.

In this thesis we discussed one particular protocol [45] which acts on a density matrix as element squaring. This protocol may be modified by an additional application of so called local twirling operator. This modification may induce chaotic behaviour in the sense of 2.7.6 (sensitivity to initial conditions). Therefore, the last paragraphs of chapter 2 are dedicated to chaos.

This thesis tried to find local twirling operators that have some convenient behaviour. We wanted them to have Bell states 3.2, 3.3 as fixed states or parts of length two cycles. We also wanted to find some invariant sets that would ease on understanding of chaotic behaviour induced by the operator. For a subset containing vectors depending on a single (complex) parameter, we applied theoretical arsenal to exactly find Julia and Fatou set and determine asymptotic behaviour of vectors in the set.

In chapter 3 we constructed local twirling operators from very special one-qubit rotations - Hadamard and Pauli matrices, 2.6-2.13, A.6. First, we have recapitulated known information about Hadamard gate $H = H_{11}$. In particular, we have mentioned the fixed states and invariant sets studied in [47]. In this thesis, we have additionally determined all length two cycles altogether with numerical estimation of their stability. The knowledge of the behaviour of H has been later extended to 15 another operators 2.16 composed of one-qubit Hadamard gates. The dynamics of all these operators are equivalent (theorem 3.4.15), they are connected by a global $\mathbb{C}^4$ space transformation using some suitable prepermutation matrix 3.9. Because of the form of these space transformations, we can pick such an operator H_{ij} which has one chosen Bell state as a fixed state. We conclude that all these operators have the same applicability in the purification protocol.

Next, we investigated the dynamics of combinations of Hadamard matrices and Pauli matrices 2.6 - 2.13. To simplify the situation and create $\mathcal{G}_{1,2}$ sets defined in 3.9.4, we took into account also nonlocal operators. These cannot be used for general purposes of quantum communication because particles must occur in some small spatial neighbourhood to be purified. Yet, we could use such a protocol to purify entangled particles just after their production in some imperfect device. We chose then one particular matrix $\mathbf{\Theta}_2$ (3.81) which indeed has Bell states as parts of length 2 cycles and has very convenient behaviour. Unless meeting very special conditions (vectors from a set with Lebesgue measure 0), operator S itself makes the system converge to one of 3.82 cycles. For examination of the exact modification brought by $\mathbf{\Theta}_2$, it is sufficient to restrict oneself to virtual subset made of component pairs a, d or b, c. These subsets are invariant and evolution inside them is described by function 3.89. Its Julia set has a little bit complicated form, but it splits $\mathbb{C}$ (resp. the Fatou set) into two not connected regions of even-odd convergence. That means that almost each (sub)state converges to a length two cycle that corresponds to jumping between a Bell state and a separable state. From figure 3.1 it is obvious that we can afford relatively big perturbation and the perturbed Bell state still would converge back to the cycle. Calculations suggest that about 10 iterations of the protocol are needed for most of z to be brought close to zero ($|z| < 10^{-3}$).

The benefits of this operator are hindered by the fact that it is not local. As the dynamics of M_{ij}, W_{ij} operators are conected to this one by a not suitable prepermutation matrices in contrast to H_{ij} (thanks to their nonzero element structure), we cannot find a convenient operator for a modification of the purification protocol. No operator has a Bell state as a fixed state or part of a length two cycle. They have their behaviour suitable for "purifying" [1] separable states and equal superpositions of basis states.

In the next chapter (4), we studied local twirling operators composed of more general rotations (one parameter usually left free). We have discussed various compositions but mostly have not found new behaviour. Condition on Bell states to be fixed states mostly led to already discussed operators. One exception is 4.9 which introduced new generalised behaviour but only on useless separable states. Construction of nonlocal operator $\mathbf{\Theta}_3$ applies this feature on Bell states but examination of the new dynamics suggests that this modified behaviour may be not as convenient as supposed.

Finally, set of operators depending on parameter φ is derived. It has convenient properties concerning the Bell states but no invariant sets were found. Multidimensional dynamics thus prevented behaviour analysis.

We also mentioned issues of stability of operators. One should be aware of experimental problems. Imprecisions in operator realisation may have as important effect as perturbations in states. We mentioned that operators discussed in chapter 4 might be considered as perturbations to some ideal operators (e.g. operators from 3).

We conclude we have investigated dynamics of wide classes of operators. We have developed and widely used the concept of equivalent dynamics 3.4.15, 3.9. This property allows us to investigate a single operator (from the equivalence class) and obtain information about many other (max. 383 different) twirling operators. However, these operators do not have to be local. Problems of nonlocality were discused in 3.8. We have determined some operators with suitable action on Bell states.

[1] There is no entanglement in separable states that could be purified! Separable states and entangled states are disjoint sets, see the definition of entangled states in paragraph 2.2.

As for the identified behaviour, the best behaviour concerning purifying abilities leading to Bell states was found for $\mathbf{\Theta}_2$ (prevailing Bell state is picked and converged via $f(z) = z^2$, convergence inside the invariant set is given by $f(z) = \dfrac{1-z^2}{1+z^2}$). We consider realisation of such a protocol to be a good idea although we are aware of its nonlocality. We believe that for current state of technology, realisation of this particular purification protocol could lead to improvements in quantum communication due to saving some resources. When concerning nonlocal operators, there is plenty of unexplored behaviour, consider new matrix types mentioned in 3.9.3, angular generalisation from chapter 4 can be performed on these as well. New possible invariant sets may be found, speed of convergence may be improved.

From the special local twirling operators we conclude that H_{ij} has the most suitable properties of all possible local twirling operators composed of one-qubit rotations (in contrast to $\mathbf{\Theta}_2$, this operator separates the a, d and b, c component pairs using function $f(z) = \dfrac{1-z^2}{1+z^2}$). We can choose particular i, j to take an operator with certain Bell state as the fixed state. Generalised rotations were found to have certain freedom in choice of angles but behaviour may not improve the behaviour as expected.

We suggest and recommend further investigation of the purification protocol [45] in the future. Extension of dynamics investigation to density matrices is only natural. Another projection in the protocol may be taken into account (see [45]); new dynamics may appear as we change the element squaring to some more complicated mixing.

The author hopes that this thesis led the reader through the maze of various operators succesfully. Anyway, for future work we suggest to improve systematisation of study of matrices from chapter 4. The possibilities of how to choose angles for general rotation composition are vast and we might have missed some particular group of operators or some peculiar feature.

We consider an important task for the future to take the findings of this thesis and construct some more sophisticated protocols that take the best possible features. These protocols could use different twirling operators in each step. We regard very important to introduce perturbed operators as they may destroy the ideal behaviour of the unperturbed cases.

We believe it is very important to study deeper connections between permutation matrices and Hadamard matrices as we could not find them in literature. Role of odd and even permutations in equivalence dynamics for H_{ij} is clear (3.4.19) but there may be some unseen fundamental connections. We have not proven a relationship 3.9.4 which describes permutation actions on $\mathcal{G}_i$. However, we did not study exact action, i.e. if there are some special sets ($\mathscr{S}'$, analogues of 3.34) of permutations that $\mathscr{S}'\mathcal{M}_i \subset \mathcal{M}_i$ and so on. Further, we consider important to introduce the concept of complex Hadamard matrices and complex prepermutation matrices that emerged from this work in paragraph 4.2. They may significantly simplify issues of further general rotations investigation.

We consider very interesting that tribonacci constant emerged in the work. We suggest deeper study of connections between polynomials and twirling operators that induce them (consider numbers 3.7, 3.8, 3.50, 3.63 that emerged as radices of some not so complicated polynomials; remember construction of fixe states in 3.7, 3.6). These polynomials could have some common feature useful in some branches of mathematics.

Appendix A

Tensor product

Besides usual matrix multiplication, there are also another operations with some interesting properties and practical use. So called Hadamard or elementwise product $\odot : \mathbb{C}^{m,n} \times \mathbb{C}^{m,n} \to \mathbb{C}^{m,n}$ is defined

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \odot \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & \dots & b_{mn} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} & a_{12}b_{12} & \dots & a_{1n}b_{1n} \\ a_{21}b_{21} & a_{22}b_{22} & \dots & a_{2n}b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}b_{m1} & a_{m2}b_{m2} & \dots & a_{mn}b_{mn} \end{pmatrix} \tag{A.1}$$

This multiplication inherits attributes of complex numbers multiplication - commutativity, associativity... Nevertheless, there is another prevailing operation in this thesis. It is the tensor product $\otimes : \mathbb{C}^{k,l} \times \mathbb{C}^{m,n} \to \mathbb{C}^{k+m,l+n}$ which is defined in block notation:

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \dots & a_{1l}B \\ a_{21}B & a_{22}B & \dots & a_{2l}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{k1}B & a_{k2}B & \dots & a_{kl}B \end{pmatrix} \tag{A.2}$$

Sometimes, another convention is used interchanging roles of A and B, e.g. in [55]. This operation is not commutative but possesses other convenient properties. Lets list several of them. For A, B, C of suitable dimensions

1. $A \otimes (B + C) = (A \otimes B) + (A \otimes C)$, $(A + B) \otimes C = (A \otimes C) + (B \otimes C)$
2. $A \otimes (B \otimes C) = (A \otimes B) \otimes C$
3. $(A \otimes B)^T = A^T \otimes B^T$
4. $(A \otimes B)^* = A^* \otimes B^*$

Lemma A.0.1 (Mixed product rule)**.** *Let A, C and B, D be matrices such that products AC, BD exist. Then*

$$(A \otimes B)(C \otimes D) = AC \otimes BD \tag{A.3}$$

Corollary A.0.2. $(A \otimes B)^{-1} = A^{-1} \otimes B^{-1}$

Lemma A.0.3 (Spectrum of tensor product)**.** *Be $A \in \mathbb{C}^{m,m}, B \in \mathbb{C}^{n,n}$, their spectra: $\sigma(A) = \{\alpha_1, \ldots, \alpha_m\}$, some of them may coincide, $\sigma(B) = \{\beta_1, \ldots, \beta_n\}$, some of them may coincide, let $\lambda, \mu \in \mathbb{C}$. Then spectra $\sigma(A \otimes B) = \{\alpha_i \beta_j | i \in \hat{m}, j \in \hat{n}\}$ and $\sigma(\lambda(A \otimes \mathbb{1}_n) + \mu(\mathbb{1}_m \otimes B)) = \{\lambda\alpha_i + \mu\beta_j | i \in \hat{m}, j \in \hat{n}\}$. If $|a\rangle, |b\rangle$ are eigenvectors corresponding to $\alpha \in \sigma(A), \beta \in \sigma(B)$ respecitvely, then $|a\rangle \otimes |b\rangle$ is eigenvector corresponding to $\alpha\beta$ and also corresponding to $\lambda\alpha + \mu\beta$.*

Corollary A.0.4. *For $A \in \mathbb{C}^{m,m}, B \in \mathbb{C}^{n,n}$: $det(A \otimes B) = (detA)^n (detB)^m$. In particular, tensor product of regular matrices is a regular matrix.*

We do not present prooves as they are easy consequences of definitions. Thay can be also found in many textbooks, for example... The most important relation for this thesis is the mixed product equation. We do not use relationships for the eigenvalues in this thesis but silently we multiplicate matrices without any care for their regularity. But as we always use unitary (i.e. regular) matrices of order 2 to product matrices of order 4, we do not have to care for the regularity. Furthermore, we can use previous properties to verify that a tensor product of two unitary matrices is indeed a unitary matrix.

Lemma A.0.5. *Let $A \in \mathbb{C}^{m,m}$, $B \in \mathbb{C}^{n,n}$ be unitary matrices. Then their tensor product is unitary.*

Proof. From $AA^* = \mathbb{1}_m \wedge BB^* = \mathbb{1}_n$ we easily see

$$(A \otimes B)(A \otimes B)^* = (A \otimes B)(A^* \otimes B^*) = (AA^*) \otimes (BB^*) = \mathbb{1}_m \otimes \mathbb{1}_n = \mathbb{1}. \tag{A.4}$$

□

Now we present a list of tensor product matrices that are studied in this thesis. Using definitions 2.15, 2.16, 2.17, 2.18 and designing $-1 =: \bar{1}$ we put forward

$$S_{11} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \quad S_{12} = \begin{pmatrix} 0 & 0 & 0 & \bar{1} \\ 0 & 0 & 1 & 0 \\ 0 & \bar{1} & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \quad S_{13} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \bar{1} \\ 1 & 0 & 0 & 0 \\ 0 & \bar{1} & 0 & 0 \end{pmatrix} \quad S_{14} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

$$S_{21} = \begin{pmatrix} 0 & 0 & 0 & \bar{1} \\ 0 & 0 & \bar{1} & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \quad S_{22} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & \bar{1} & 0 \\ 0 & \bar{1} & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \quad S_{23} = \begin{pmatrix} 0 & 0 & \bar{1} & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & \bar{1} & 0 & 0 \end{pmatrix} \quad S_{24} = \begin{pmatrix} 0 & 0 & \bar{1} & 0 \\ 0 & 0 & 0 & \bar{1} \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

$$S_{31} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & \bar{1} \\ 0 & 0 & \bar{1} & 0 \end{pmatrix} \quad S_{32} = \begin{pmatrix} 0 & \bar{1} & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & \bar{1} & 0 \end{pmatrix} \quad S_{33} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \bar{1} & 0 & 0 \\ 0 & 0 & \bar{1} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad S_{34} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \bar{1} & 0 \\ 0 & 0 & 0 & \bar{1} \end{pmatrix}$$

$$S_{41} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad S_{42} = \begin{pmatrix} 0 & \bar{1} & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & \bar{1} \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad S_{43} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \bar{1} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \bar{1} \end{pmatrix} \quad S_{44} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{A.5}$$

$$
H_{11} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \bar{1} & 1 & \bar{1} \\ 1 & 1 & \bar{1} & \bar{1} \\ 1 & \bar{1} & \bar{1} & 1 \end{pmatrix} \quad
H_{12} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ \bar{1} & 1 & \bar{1} & 1 \\ 1 & 1 & \bar{1} & \bar{1} \\ \bar{1} & 1 & 1 & \bar{1} \end{pmatrix} \quad
H_{13} = \begin{pmatrix} 1 & \bar{1} & 1 & \bar{1} \\ 1 & 1 & 1 & 1 \\ 1 & \bar{1} & \bar{1} & 1 \\ 1 & 1 & \bar{1} & \bar{1} \end{pmatrix} \quad
H_{14} = \begin{pmatrix} \bar{1} & 1 & \bar{1} & 1 \\ 1 & 1 & 1 & 1 \\ \bar{1} & 1 & 1 & \bar{1} \\ 1 & 1 & \bar{1} & \bar{1} \end{pmatrix}
$$

$$
H_{21} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \bar{1} & 1 & \bar{1} \\ \bar{1} & \bar{1} & 1 & 1 \\ \bar{1} & 1 & 1 & \bar{1} \end{pmatrix} \quad
H_{22} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ \bar{1} & 1 & \bar{1} & 1 \\ \bar{1} & \bar{1} & 1 & 1 \\ 1 & \bar{1} & \bar{1} & 1 \end{pmatrix} \quad
H_{23} = \begin{pmatrix} 1 & \bar{1} & 1 & \bar{1} \\ 1 & 1 & 1 & 1 \\ \bar{1} & 1 & 1 & \bar{1} \\ \bar{1} & \bar{1} & 1 & 1 \end{pmatrix} \quad
H_{24} = \begin{pmatrix} \bar{1} & 1 & \bar{1} & 1 \\ 1 & 1 & 1 & 1 \\ 1 & \bar{1} & \bar{1} & 1 \\ \bar{1} & \bar{1} & 1 & 1 \end{pmatrix}
$$

$$
H_{31} = \begin{pmatrix} 1 & 1 & \bar{1} & \bar{1} \\ 1 & \bar{1} & \bar{1} & 1 \\ 1 & 1 & 1 & 1 \\ 1 & \bar{1} & 1 & \bar{1} \end{pmatrix} \quad
H_{32} = \begin{pmatrix} 1 & 1 & \bar{1} & \bar{1} \\ \bar{1} & 1 & 1 & \bar{1} \\ 1 & 1 & 1 & 1 \\ \bar{1} & 1 & \bar{1} & 1 \end{pmatrix} \quad
H_{33} = \begin{pmatrix} 1 & \bar{1} & \bar{1} & 1 \\ 1 & 1 & \bar{1} & \bar{1} \\ 1 & \bar{1} & 1 & \bar{1} \\ 1 & 1 & 1 & 1 \end{pmatrix} \quad
H_{34} = \begin{pmatrix} \bar{1} & 1 & 1 & \bar{1} \\ 1 & 1 & \bar{1} & \bar{1} \\ \bar{1} & 1 & \bar{1} & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}
$$

$$
H_{41} = \begin{pmatrix} \bar{1} & \bar{1} & 1 & 1 \\ \bar{1} & 1 & 1 & \bar{1} \\ 1 & 1 & 1 & 1 \\ 1 & \bar{1} & 1 & \bar{1} \end{pmatrix} \quad
H_{42} = \begin{pmatrix} \bar{1} & \bar{1} & 1 & 1 \\ 1 & \bar{1} & \bar{1} & 1 \\ 1 & 1 & 1 & 1 \\ \bar{1} & 1 & \bar{1} & 1 \end{pmatrix} \quad
H_{43} = \begin{pmatrix} \bar{1} & 1 & 1 & \bar{1} \\ \bar{1} & \bar{1} & 1 & 1 \\ 1 & \bar{1} & 1 & \bar{1} \\ 1 & 1 & 1 & 1 \end{pmatrix} \quad
H_{44} = \begin{pmatrix} 1 & \bar{1} & \bar{1} & 1 \\ \bar{1} & \bar{1} & 1 & 1 \\ \bar{1} & 1 & \bar{1} & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}
$$

(A.6)

$$
M_{11} = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & \bar{1} \\ 1 & 0 & \bar{1} & 0 \end{pmatrix} \quad
M_{12} = \begin{pmatrix} 0 & \bar{1} & 0 & \bar{1} \\ 1 & 0 & 1 & 0 \\ 0 & \bar{1} & 0 & 1 \\ 1 & 0 & \bar{1} & 0 \end{pmatrix} \quad
M_{13} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & \bar{1} & 0 & \bar{1} \\ 1 & 0 & \bar{1} & 0 \\ 0 & \bar{1} & 0 & 1 \end{pmatrix} \quad
M_{14} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & \bar{1} & 0 \\ 0 & 1 & 0 & \bar{1} \end{pmatrix}
$$

$$
M_{21} = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & \bar{1} & 0 & 1 \\ \bar{1} & 0 & 1 & 0 \end{pmatrix} \quad
M_{22} = \begin{pmatrix} 0 & \bar{1} & 0 & \bar{1} \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & \bar{1} \\ \bar{1} & 0 & 1 & 0 \end{pmatrix} \quad
M_{23} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & \bar{1} & 0 & \bar{1} \\ \bar{1} & 0 & 1 & 0 \\ 0 & 1 & 0 & \bar{1} \end{pmatrix} \quad
M_{24} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ \bar{1} & 0 & 1 & 0 \\ 0 & \bar{1} & 0 & 1 \end{pmatrix}
$$

$$
M_{31} = \begin{pmatrix} 0 & 1 & 0 & \bar{1} \\ 1 & 0 & \bar{1} & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix} \quad
M_{32} = \begin{pmatrix} 0 & \bar{1} & 0 & 1 \\ 1 & 0 & \bar{1} & 0 \\ 0 & \bar{1} & 0 & \bar{1} \\ 1 & 0 & 1 & 0 \end{pmatrix} \quad
M_{33} = \begin{pmatrix} 1 & 0 & \bar{1} & 0 \\ 0 & \bar{1} & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & \bar{1} & 0 & \bar{1} \end{pmatrix} \quad
M_{34} = \begin{pmatrix} 1 & 0 & \bar{1} & 0 \\ 0 & 1 & 0 & \bar{1} \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}
$$

$$
M_{41} = \begin{pmatrix} 0 & \bar{1} & 0 & 1 \\ \bar{1} & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix} \quad
M_{42} = \begin{pmatrix} 0 & \bar{1} & 0 & \bar{1} \\ \bar{1} & 0 & 1 & 0 \\ 0 & \bar{1} & 0 & \bar{1} \\ 1 & 0 & 1 & 0 \end{pmatrix} \quad
M_{43} = \begin{pmatrix} \bar{1} & 0 & 1 & 0 \\ 0 & 1 & 0 & \bar{1} \\ 1 & 0 & 1 & 0 \\ 0 & \bar{1} & 0 & \bar{1} \end{pmatrix} \quad
M_{44} = \begin{pmatrix} \bar{1} & 0 & 1 & 0 \\ 0 & \bar{1} & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}
$$

(A.7)

$$
W_{11} = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & \bar{1} \\ 1 & 1 & 0 & 0 \\ 1 & \bar{1} & 0 & 0 \end{pmatrix} \quad
W_{12} = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & \bar{1} & 1 \\ 1 & 1 & 0 & 0 \\ \bar{1} & 1 & 0 & 0 \end{pmatrix} \quad
W_{13} = \begin{pmatrix} 0 & 0 & 1 & \bar{1} \\ 0 & 0 & 1 & 1 \\ 1 & \bar{1} & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix} \quad
W_{14} = \begin{pmatrix} 0 & 0 & \bar{1} & 1 \\ 0 & 0 & 1 & 1 \\ \bar{1} & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}
$$

$$
W_{21} = \begin{pmatrix} 0 & 0 & \bar{1} & \bar{1} \\ 0 & 0 & \bar{1} & 1 \\ 1 & 1 & 0 & 0 \\ 1 & \bar{1} & 0 & 0 \end{pmatrix} \quad
W_{22} = \begin{pmatrix} 0 & 0 & 1 & \bar{1} \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ \bar{1} & 1 & 0 & 0 \end{pmatrix} \quad
W_{23} = \begin{pmatrix} 0 & 0 & \bar{1} & 1 \\ 0 & 0 & \bar{1} & \bar{1} \\ 1 & \bar{1} & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix} \quad
W_{24} = \begin{pmatrix} 0 & 0 & 1 & \bar{1} \\ 0 & 0 & \bar{1} & \bar{1} \\ \bar{1} & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}
$$

$$
W_{31} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & \bar{1} & 0 & 0 \\ 0 & 0 & \bar{1} & \bar{1} \\ 0 & 0 & \bar{1} & 1 \end{pmatrix} \quad
W_{32} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ \bar{1} & 1 & 0 & 0 \\ 0 & 0 & \bar{1} & \bar{1} \\ 0 & 0 & 1 & \bar{1} \end{pmatrix} \quad
W_{33} = \begin{pmatrix} 1 & \bar{1} & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & \bar{1} & 1 \\ 0 & 0 & \bar{1} & \bar{1} \end{pmatrix} \quad
W_{34} = \begin{pmatrix} \bar{1} & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & \bar{1} \\ 0 & 0 & \bar{1} & \bar{1} \end{pmatrix}
$$

$$
W_{41} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & \bar{1} & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & \bar{1} \end{pmatrix} \quad
W_{42} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ \bar{1} & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & \bar{1} & 1 \end{pmatrix} \quad
W_{43} = \begin{pmatrix} 1 & \bar{1} & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & \bar{1} \\ 0 & 0 & 1 & 1 \end{pmatrix} \quad
W_{44} = \begin{pmatrix} \bar{1} & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & \bar{1} & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}
$$

(A.8)

Appendix B

Permutation matrices

For each n there is special set of matrices $\in \mathbb{C}^{n,n}$:

Definition B.0.6. *Matrix $P \in \mathbb{C}^{n,n}$ with entries $(P)_{ij} \in \{0,1\}$ such that in each row and in each column there is only one entry 1 is called permutation matrix. Set of all permutation matrices in $\mathbb{C}^{n,n}$ is denoted $\mathscr{S}_n$.*

Note B.0.7. *We might also write: $P \in \mathbb{C}^{n,n}$ is a permutation matrix $\Leftrightarrow$*
$\Leftrightarrow (P \in \{0,1\}^{n,n}) \wedge (\forall i \in \hat{n})(\sum_{j=1}^{n}(P)_{ij} = 1) \wedge (\forall j \in \hat{n})(\sum_{i=1}^{n}(P)_{ij} = 1)$.

Permutation matrix is one of many representations of n-element set automorphisms, *permutations*. We will usually not distinguish permutations and these representations which are associated as follows.

Suppose we have a set $M = \{m_1, m_2, m_3, m_4\}$ and a map p given by $p(m_1) = m_3$, $p(m_2) = m_1$, $p(m_3) = m_2$, $p(m_4) = m_4$. Permutations are usually written as (for our example) $p = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$ or in the cycle notation $p = (132)(4)$. We assign a matrix P to this bijection p in the way $(\forall i, j \in \hat{4})((P)_{ij} = 1 \Leftrightarrow p(m_i) = m_j, (P)_{ij} = 0$ otherwise). This matrix has conveniently illustrative property (on given example):

$$P \begin{pmatrix} m_1 \\ m_2 \\ m_3 \\ m_4 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} m_1 \\ m_2 \\ m_3 \\ m_4 \end{pmatrix} = \begin{pmatrix} m_3 \\ m_1 \\ m_2 \\ m_4 \end{pmatrix} \tag{B.1}$$

For each permutation $P \in \mathbb{C}^{n,n}, n < +\infty$, there are numbers $k \in \mathbb{N}$ such that $p^k = \mathbb{1}$. Minimal k with this property is called the order of permutation.

Set of all permutation of n-sets with composition / set of all permutation matrices of order n with multiplication forms a group. We shall denote this group also $\mathscr{S}_n$. It has $n!$ elements. In fact, groups of permutations are very important example of groups. A whole theory is devoted to them and thus many theorems about permuations exist [56, 57]. We shall rely on their group character.

This thesis handles matrices of order 4, therefore we study them closer. We shall order and label permutations lexicographically according to the second row of the two row notation. That is

$$
P_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad P_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad P_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},
$$
$$
P_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad P_5 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \quad P_6 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix},
$$
$$
P_7 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad P_8 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad P_9 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},
$$
$$
P_{10} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad P_{11} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \quad P_{12} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix},
$$
$$
P_{13} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad P_{14} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad P_{15} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},
$$
$$
P_{16} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad P_{17} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \quad P_{18} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix},
$$
$$
P_{19} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad P_{20} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad P_{21} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix},
$$
$$
P_{22} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad P_{23} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad P_{24} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}. \tag{B.2}
$$

We choose two special elements $X := P_2, R := P_{19}$. The order of X is 2, the order of R is 3. We show these two elements form a basis of $\mathscr{S}_4$ (i.e. any permutation matrix can be composed of these two matrices):

$$
\begin{array}{llll}
P_1 = X^2 = P^3 & P_2 = X & P_3 = RXR^3 & P_4 = R^2XR \\
P_5 = R^3XR^2 & P_6 = XR^2XR & P_7 = R^2XR^2 & P_8 = R^2XR^2X \\
P_9 = R^3X & P_{10} = R^3 & P_{11} = RXR & P_{12} = RXRX \\
P_{13} = XR & P_{14} = XRX & P_{15} = RXR^2X & P_{16} = RXR^2 \\
P_{17} = R^2 & P_{18} = R^2X & P_{19} = R & P_{20} = RX \\
P_{21} = R^2XR^3 & P_{22} = R^3XR & P_{23} = XR^2 & P_{24} = XR^2X
\end{array} \tag{B.3}
$$

Appendix C

Hadamard matrices

Hadamard matrices are special type matrices [57] that have wide use in data processing and related branches of science. This appendix gives basic outline of properties and demonstrates practical use as discrete Fourier transform.

Definition C.0.8. *Matrix $A \in \mathbb{C}^{n,n}$ with entries $(A)_{ij} \in \{-1, 1\}$ is called* Hadamard matrix of order n *if it satisfies*

$$A^T A = n\mathbb{1}. \tag{C.1}$$

Corollary C.0.9. *Rows and columns of Hadamard matrix are mutually orthogonal.*

Sometimes (generally in physics papers), condition $H^T H = n\mathbb{1}$ is reduced to $H'^T H' = \mathbb{1}$. Such H' is not only orthogonal, but also orthonormal. Therefore its more useful for physical applications. There is no fundamental reason to distinguish these definitions as H and H' differ only in a global factor related to dimension: $H = \sqrt{n}H'$.

There are only four Hadamard matrices in $\mathbb{C}^{2,2}$. They are (using physical motivated definition in contrast to 2.6-2.9 , obviously $H_i H_i^T = \mathbb{1}$):

$$\begin{aligned} H_1 &= \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad H_2 = \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}, \\ H_3 &= \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, \quad H_4 = \tfrac{1}{\sqrt{2}} \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}. \end{aligned} \tag{C.2}$$

Note C.0.10. *We see that all Hadamard matrices of order 2 are connected via permutations and negation of some rows and columns. This is not generally true. For higher orders (e.g. 16), there may be Hadamard matrices nonequivalent in this sense.*

Note C.0.11. *Because rows of Hadamard matrix are orthogonal and elements can be only ± 1, rows must differ in sign exactly in half cases. That is not possible for odd dimensions. In consequence, there is no Hadamard matrix of even order, except $n = 1$.*

The question of how many Hadamard matrices of general order n exist (or if they even do exist for given n) is still without satisfactory answer. This problem is known as Paley's conjecture or Hadamard matrix conjecture. Two general constructions are known to build Hadamard matrices of some special orders. Paley's conctruction gives Hadamard matrices of order p^n+1 for p^n power of prime number satisfying $p^n \equiv 3 \bmod 4$ and Hadamard matrices of order $2(p^n + 1)$ for p^n power of prime number satisfying $p^n \equiv 1 \bmod 4$. For this thesis, another construction is more important.

Theorem C.0.12 (Sylvester's construction)**.** *Let H, H' be Hadamard matrices. Then $H \otimes H'$ is also a Hadamard matrix. In particular, using $H = H_1$ (given in 2.6) we can construct Hadamard matrices of orders 2^k, $k \in \mathbb{N}$.*

Matrices used in this thesis are constructed using exactly this construction with matrices C.2 (neglecting global factors). Any Hadamard matrix of order 2^k generated via procedure C.0.12 has following properties: symmetry, zero trace, first row and column have only $+1$ elements, others have half $+1$, half -1. Such outputs are called Walsh matrices, they are used for Walsh-Hadamard transform [59] and they are important part of signal processing operations. Rows of the Walsh matrix can be permuted and form one peculiar matrix. It has its first row formed from $+1$ only and each consecutive row has more sign changes than the preceding one.

Hadamard matrices are significantly employed in design theory [58]. The existence of various designs is possible only if some Hadamard matrices exist. Rows (columns) of Hadamard matrices are vectors of lenght $\sqrt{n}$ and they span a parallelotop with maximal volume of all matrices with entries from $\{-1, 1\}$. This is known as the Hadamard's maximal determinant problem and can be used for a few more determinant relations.

In this thesis and in quantum physics there is one important property of Hadamard matrix (Walsh matrix). It is its connection to discrete Fourier transform, [59]. Consider "signal" represented as the first vector of standard basis

$$|e\rangle_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ \vdots \end{pmatrix} \in \mathbb{C}^{2^k}$$

This vector is transformed

$$H_{2^k} |e_1\rangle = \begin{pmatrix} 1 \\ 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} = |e_1\rangle + |e_2\rangle + |e_3\rangle + \cdots + |e_{2^k}\rangle \tag{C.3}$$

which is the equal superposition of basis states. On the other hand, small multiple of this mix can be viewed as noisy background of some signal and this transformation can convert it into the first component (we emphasize $H = H^T = H^{-1} \Rightarrow H^2 = \mathbb{1}$).

Appendix D

Analysis of complex functions

In this appendix we present exact method how to investigate a function of one complex variable. We realise theoretical machinery described in paragraph 2.8. Consider function depending on a parameter $t \in \mathbb{R}$:

$$f_t(z) = \frac{1 - z^2}{1 + tz^2} \tag{D.1}$$

with domain $Dom(f) = \hat{\mathbb{C}}$. We want to determine Julia set and attractive cycles in relation to the parameter t. We do so because Julia set gives information about chaotic behaviour while attractive cycles belong to Fatou set and represent ordinary behaviour.

We see that f is rational polynomial function of degree 2. Thus we know that Julia set is nonempty. We also know that there are at most 2 attractive cycles. Lets find them using the critical points

$$f_t'(z) = -\frac{2(t+1)x}{(1+tx^2)^2} \tag{D.2}$$

We see we have some special cases

1. $t = -1$

   Then $f_1(z) = 1$ which is not an interesting function at all.

2. $t = 0$

   Then $f_0(z) = 1 - z^2$. The only critical point existing is $z_0 = 0$ which forms cycle of length two: $0 \leftrightarrow 1$. This function was however already studied by Julia himself. It is known a lot about functions $f(z) = z^2 + c$, $c \in \mathbb{C}$ their Julia sets and so on. Julia set for our f_0 is displayed in figure D.1. Take notice of the different colors that depict various types of convergences. Set of all constants $c \in \mathbb{C}$ such that Julia set of $f(z) = z^2 + c$ is connected forms the famous Mandelbrot set.

3. $t \in \mathbb{C} \setminus \{-1, 0\}$

   We shall investigate this case further. Critical points are $z_1 = 0, z_2 = \infty$.

Critical points converge to an attractive or a parabolic cycle. Therefore we study orbit of z_1:

$$0 \xrightarrow{f} 1 \xrightarrow{f} 0 \tag{D.3}$$

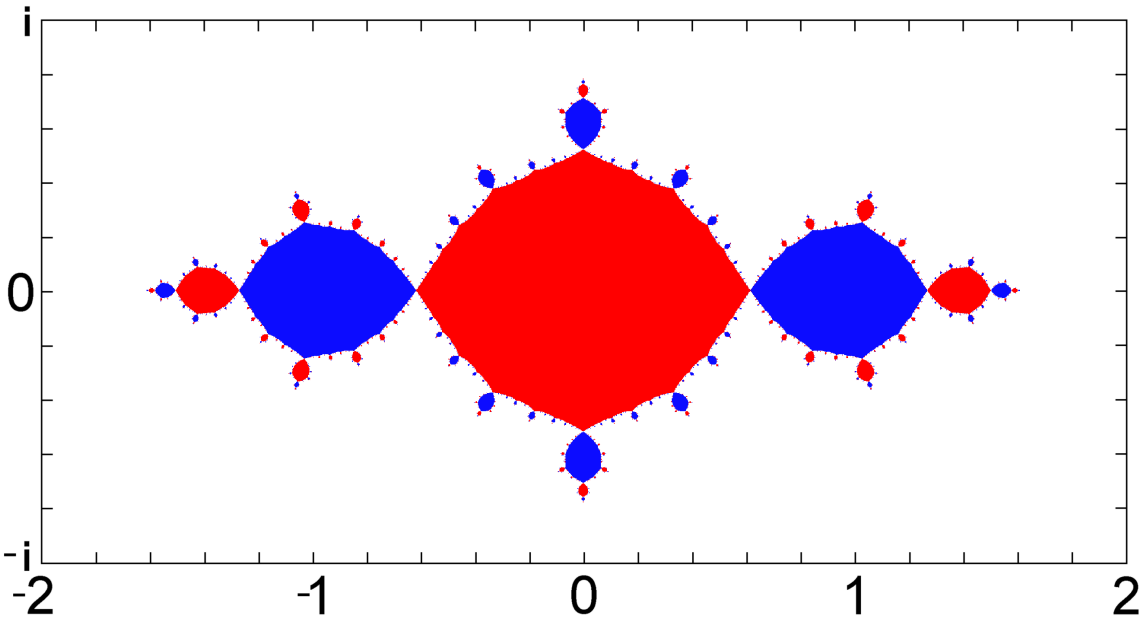

Figure D.1: Julia set of function f_0 splits Fatou set into three areas of different convergences (marked with different colours - red, blue and white). Julia set is the border of these areas.

We see that this ciritical point forms a period 2 cycle for $\forall t$. Its multiplier is $\lambda = f'(0)f'(1) = 0$ and thus this cycle is superattractive. For the other critical point:

$$\infty \xrightarrow{f} \frac{-1}{t} \xrightarrow{f} \frac{t-1}{t} \xrightarrow{f} \frac{2t-1}{t(t^2-t+1)} \xrightarrow{f} \frac{(t-1)^2(t^3-t^2+3t-1)}{t(t^4-3t^3+6t^2-4t+1)} \xrightarrow{f} \dots \tag{D.4}$$

This orbit has a more complicated structure. We do not prove following statements leaving them rather as some more or less obvious observations. Unless special occasions discussed below, this orbit tends toward 0 after odd number of iterations and tends to 1 after even number of iteratons. That is, orbit of $z_1 = \infty$ converges to $0 \leftrightarrow 1$ superattractive cycle as well. We conclude there is only one superattractive cycle. Now we present how does the Julia set depend on t using few examples.

1. $t = 1$

   For $t = 1$ we obtain function 3.89 which is discussed in 3.9. See picture 3.1 for the Julia set and 3.2 to see how many iterations are needed for a point z to get close to zero, $z \to z'$ such that $|z'| < 0.001$. At this place we would like to present one interesting property of f_1. It emerges when looking for the fixed points. Solving

   $$\frac{1-z^2}{1+z^2} = z \tag{D.5}$$

   we get radices of a polynomial $\tilde{\mathcal{Q}}_3$: $\tilde{\mathcal{Q}}_3(z) = z^3+z^2+z-1 = 0$. This polynomial we transform into $\mathcal{Q}_3(z) := -z^3\tilde{\mathcal{Q}}_3(\frac{1}{z}) = z^3-z^2-z-1$. The $\mathcal{Q}_3$ polynomial is very important in number theory [60] as it is a generalisation of the polynomial for the golden ratio $\mathcal{Q}_2 = x^2+x-1$. Real number obtained as a solution of $\mathcal{Q}_3$

is called tribonacci constant as it can be also obtained as a limit of the ratio of two consecutive members of tribonacci sequence

$$T_{-2} = T_{-1} = 0, T_0 = 1; \;\; (\forall n \in \mathbb{N})(T_n = T_{n-1} + T_{n-2} + T_{n-3}) \tag{D.6}$$

In consequence, components of some of the fixed states of H are reciprocal values of tribonacci constant and its conjugate elements, check [47].

$$\begin{aligned} \tau_1 &:= \frac{1}{3}\left(-1 + \sqrt[3]{17+3\sqrt{33}} - \frac{2}{\sqrt[3]{17+3\sqrt{33}}}\right) \\ \tau_{2,3} &:= \frac{1}{6}\left(-2 + (-1 \pm i\sqrt{3})\sqrt[3]{17+3\sqrt{33}} + \frac{2(1\pm i\sqrt{3})}{\sqrt[3]{17+3\sqrt{33}}}\right) \end{aligned} \tag{D.7}$$

2. $t = 2$

This value belongs to one of the "special occasions" mentioned when studying orbits of critical points. In this case:

$$\infty \xrightarrow{f} \frac{-1}{2} \xrightarrow{f} \frac{1}{2} \xrightarrow{f} \frac{1}{2} \tag{D.8}$$

We see that this time there exist another cycle, the fixed point $\frac{1}{2}$. Calculating derivative $f_2'(\frac{1}{2}) = -\frac{4}{3}$ we see that multiplier of this cycle is $\lambda = |f_2'(\frac{1}{2})| = \frac{4}{3} > 1$. This cycle (that is the point $\frac{1}{2}$) is therefore a part of $\mathcal{J}(f_2)$! And as a consequence, so is $z_1 = \infty$. However, z_1 is a good example of the property that forward images of a single point $\in \mathcal{J}(f)$ do not have to be dense in the Julia set, 2.8.20.

Julia set is depicted in figure D.2, compare it to 3.1. Now the Julia set stretches to ∞ which it contains. Why is $t = 2$ so special? Look at the D.4 and compare the second and the third iteration. If we demand that they are equal, we obtain

$$\begin{gathered} \frac{t-1}{t} = \frac{2t-1}{t(t^2-t+1)} \\ (t-1)(t^2-t+1) = (2t-1) \\ t^3 - 2t^2 = 0 \\ t = 0 \quad \vee \quad t = 2 \end{gathered} \tag{D.9}$$

As we have discriminated the case $t = 0$, we see that for $t = 2$ infinity converges to (and indeed reaches) some fixed point after three iterations. We could go further and ask whether exist t such that ∞ reaches some fixed state after three iterations. We solve

$$\begin{gathered} \frac{2t-1}{t(t^2-t+1)} = \frac{(t-1)^2(t^3-t^2+3t-1)}{t(t^4-3t^3+6t^2-4t+1)} \\ t^3(t-2)(-t^3+2t^2-4t+2) = 0 \\ \Downarrow \\ t = 0 \quad \vee \quad t = 2 \quad \vee \\ t = \frac{1}{3}\left(2 - \frac{8}{\sqrt[3]{-1+3\sqrt{57}}} + \sqrt[3]{-1+3\sqrt{57}}\right) \quad \vee \\ t = \frac{2}{3} + \frac{4(1+i\sqrt{3})}{3\sqrt[3]{-1+3\sqrt{57}}} - \frac{1}{6}(1-i\sqrt{3})\sqrt[3]{-1+3\sqrt{57}} \quad \vee \\ t = \frac{2}{3} + \frac{4(1-i\sqrt{3})}{3\sqrt[3]{-1+3\sqrt{57}}} - \frac{1}{6}(1+i\sqrt{3})\sqrt[3]{-1+3\sqrt{57}} \end{gathered} \tag{D.10}$$

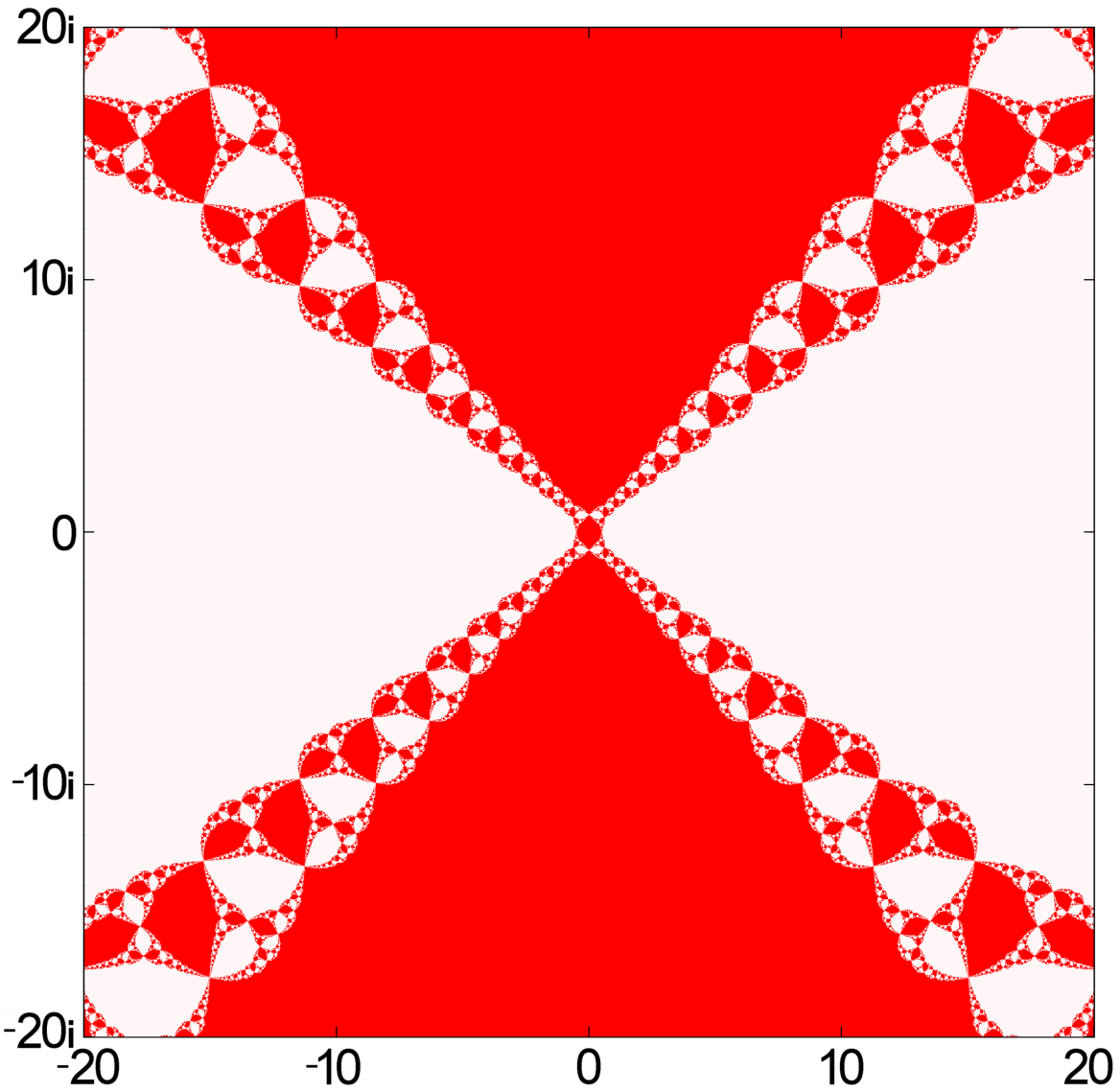

Figure D.2: Julia set of function f_2 stretches to infinity. Fatou set is separated into two different convergence types (red and white colours).

For the three new numbers similar situation concerning ∞ as a part of the Julia set occurs. We could continue with higher iterations yielding polynomials of higher and higher degree and new radices (7 for the next iteration), the already obtained radices must remain as $f^{n+1}(x) = f^n(x)$ is trivially satisfied when satisfied for some iteration $k < n$. $\#\{t \in \mathbb{C} | \infty \in \mathcal{J}(f_t)\} = \aleph_0$, (the cardinality of $\mathbb{N}$).

3. $t = 3$

   Both z_1, z_2 now again converge to the attractive cycle $0 \leftrightarrow 1$. Julia set is depicted in D.3. Fatou set is split into odd-even convergences to the cycles. This function is realised for invariant subset $\mathcal{E}$ (defined in 3.12) for operator H, some details are mentioned in paragraph 3.2. Here we furhtermore present picture that indicates speed of convergence for points z near 0.

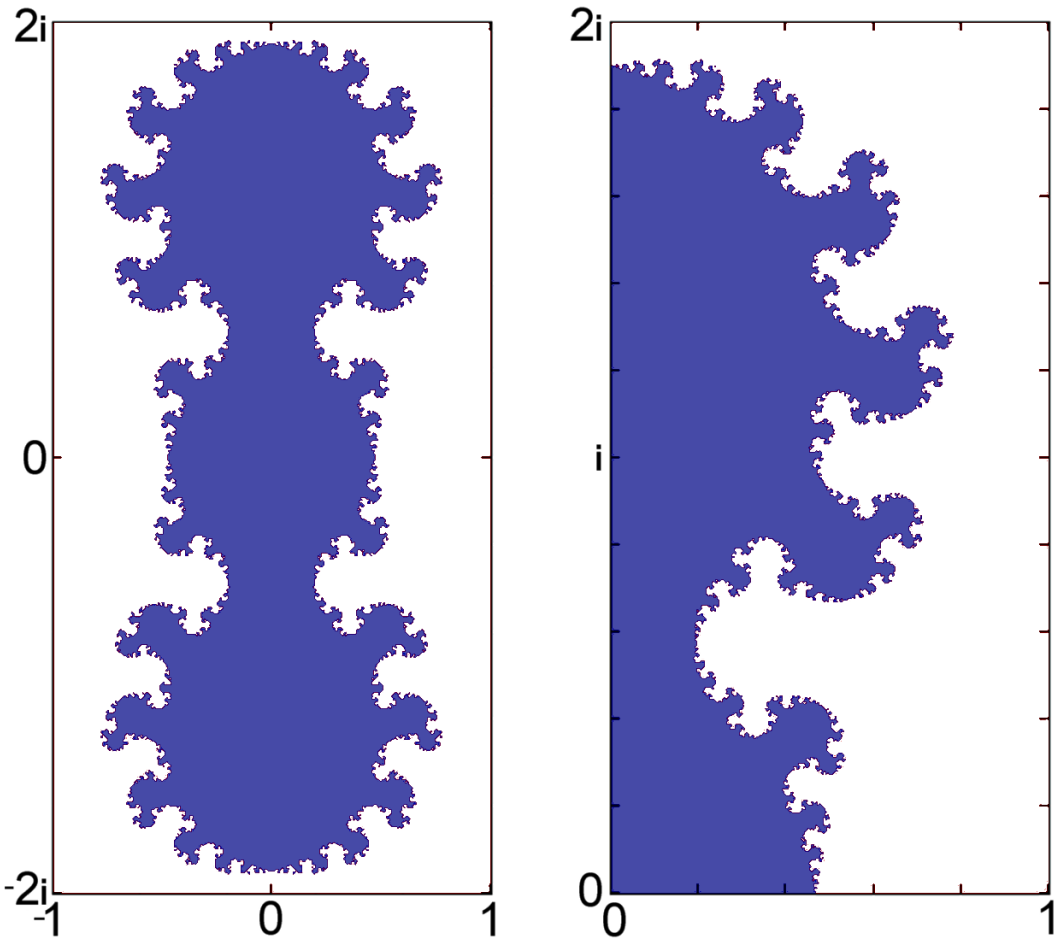

Figure D.3: Julia set of f_3 divides Fatou set into connected components of odd (white) - even (blue) convergence. Left - whole $\mathcal{J}(f_3)$; right - detail.

We conclude that f_t (D.1) is constant for $t = -1$. For $t = 0$ it is a function from a well known set of fucntions. There is only one critical point, zero which forms a cycle $0 \leftrightarrow 1$. For all other parameters this single superattractive cycle remains and up to some set of Lebesgue measure 0, functions f_t gain another attractive cycle starting from infinity. This simple function of degree two hides a lot of interesting behaviour, even for purification protocols.

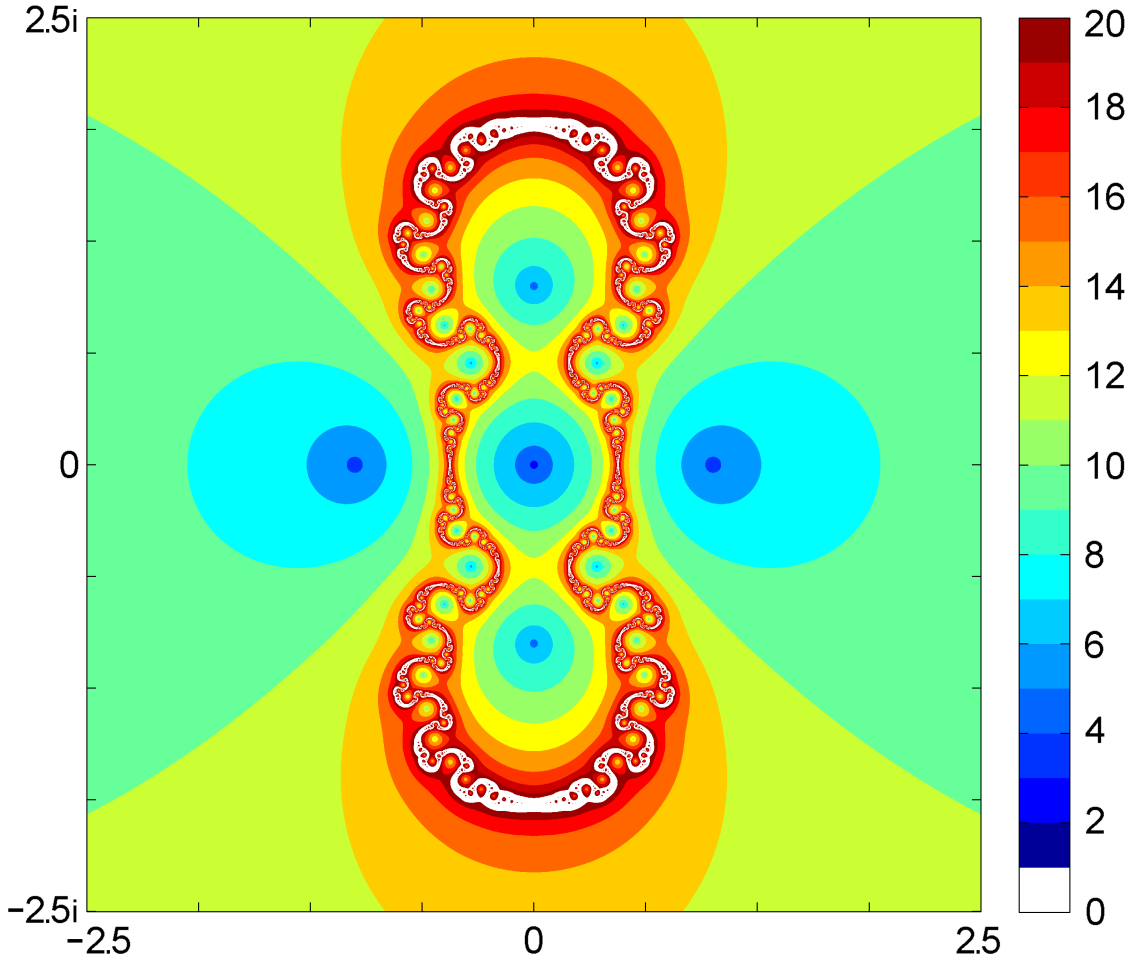

Figure D.4: Speed of convergence for f_3.
Color corresponds to n number of iterations needed for z so that $|f_3^n(z)| < 0.001$.
White color represents points converging with $n > 20$ or points from the Julia set.

Bibliography

[1] Blank J., Exner P., Havlíček M. *Lineární operátory v kvantové fyzice* (Karolinum, Praha) (1993)

[2] Einstein A., Podolsky B., Rosen N. *Phys. Rev.* **47**, 777-780 (1935)

[3] Schrödinger E. *Naturwissenschaften* **23**, 844 (1935)

[4] Bell J. *Physics* **1**, 195-200 (1964)

[5] Deutsch D. et al. *Phys. Rev. Lett.* **77**, 2818 (2006)

[6] Habib S., Jacobs K., Shizume K. *Phys. Rev. Lett.* **96**, 010403 (2006)

[7] Kiss T., Jex I., Alber G., Vymětal S. *Phys. Rev. A* **74**, 040301(R) (2006)

[8] Kiss T., Vymětal S., Tóth L.D., Gábris A., Jex I., Alber G. *Physical Review Letters* **107**, 100501 (2011)

[9] Devaney R.L. *An Introduction to Chaotic Dynamical Systes*, 2^{nd} edition (Addison-Wesley Publishing Company, Inc.)(1989)

[10] Milnor J. W. *Dynamics in One Complex Variable*, 3^{rd} edition (Princeton University Press) (2000)

[11] Morosawa S., Nishimura Y., Taniguchi M., Ueda T. *Holomorphic dynamics* (Cambridge University Press) (2000)

[12] Blank J., Exner P., Havlíček M. *Hilbert Space Operators in Quantum Physics*, 2^{nd} edition, (Springer Science + Business Media B.V.) (2008)

[13] Štoll I. *Dějiny fyziky* (Prometheus, Praha) (2009)

[14] Planck M. *Verhandl. Dtsch. phys. Ges.* **2**, 202 (1900)

[15] Bohr N. *Philosophical Mag.* **26** 1-24 (1913)

[16] de Broglie L. *Recherches sur la Théorie des Quanta*, dissertation, Sorbonne (1924)

[17] Schrödinger E. *Phys. Rev.* **28**, 1049-1070 (1926)

[18] Heisenberg W. *Zeitschrift für Physik* **43** 172-198 (1927)

[19] Dirac P.A.M. *The Principles of Quantum Mechanics* (Oxford University Press) (1930)

[20] Nielsen A. M., Chuang I. L.*Quantum Computation and Quantum Information* (Cambridge University Press)(2000)

[21] Turing A. *Proc. London Math Soc.* **42**, 230-265 (1936)

[22] Deutsch D. *Proc. R. Soc. London A* **400**, 97-117 (1985)

[23] Shor P. *SIAM J. Comput.* **26** 1484-1509 (1994)

[24] Shannon C.E. *The Bell System Tech. J.* **27**, 379-423, 623-656 (1948)

[25] Ekert A., Macchiavello Ch.*Phys. Rev. Lett.* **77**, 2585-2588 (1996)

[26] Weinstein Y.S. *Phys. Rev. A* **89**, 020301(R) (2014)

[27] Bennett Ch.B., DiVincenzo D.P., Smolin J.A., Wootters W.K. *Phys. Rev. A* **54**, 3824-3851 (1996)

[28] Bremner M.J., Jozsa R., Shepherd D.J. *Proc. R. Soc. A* **467**, 2177 (2010);

[29] Deutsch D., Jozsa R. *Proceedings: Mathematical and Physical Sciences A* **439**, 553-558 (1992)

[30] Ikram M., Zhu S.-Y., Zubairy M.S. *Phys. Rev. A* **62**, 022307 (2000)

[31] Knoll L.T., Schmiegelow Ch.T., Larotonde M.A. *Phys. Rev. A* **90**, 042332 (2014)

[32] Ricci M., De Martini F., Cerf J., Filip R., Fiurášek J., Macchiavello C. *Phys. Rev. Lett.* **93**, 170501 (2004)

[33] Horodecki M., Horodecki P., Horodecki R. *Phys. Rev. Lett.* **78**, 574-577 (1997)

[34] Hsieh J. Y., Li Ch. M., Chuu D. S. *Phys. Lett. A* **328**, 94-101 (2004)

[35] Kleinmann M., Kampermann H., Meyer T., Bruß D. *Phys. Rev. A* **73**, 062309 (2006)

[36] Song W., Yang M., Cao Z. L. *Phys. Rev. A* **89**, 062320 (2014)

[37] Pan J.-W., Simon Ch., Brukner Č., Zeilinger A. *Nature* **410**, 1067-1070 (2001)

[38] Plenio M.B., Virmani S. *Quantum Information & Computation* **7**, 1-51 (2007)

[39] Bombin H., Martin-Delgado M.A. *Phys. Rev. A* **72**, 0322313 (2005)

[40] Horodecki M., Horodecki P. *Phys. Rev. A* **59**,4206 (1999)

[41] Horodecki M., Horodecki P., Horodecki R. *Rev. Mod. Phys.* **81**, 865 (2009)

[42] Jones C. *Quantum Information & Computation* **14**, 560-576 (2014)

[43] Jané E. *Quantum Information & Computation* **2**, 348-354 (2002)

[44] Brun A. T., Caves C. M., Schack R. *Phys. Rev. A* **63**, 042309 (2001), arXiv:quant-ph/0010038

[45] Bechmann-Pasquinucci H. et. al. *Phys. Lett. A* **242**, 198-204 (1998)

[46] Alber G., Delgado A., Gisin N., Jex I. *J. Phys. A: Math. Gen.* **34**, 8821 (2001)

[47] Malachov M., *Purifikační protokoly a kvantový chaos*, research assignment, FJFI ČVUT (2014)

[48] Monroe C., Meekhof D.M., King B.E., Itano W.M., Wineland D.J. *Phys. Rev. Lett.* **75**, 4714 (1995)

[49] Poincaré H. *Acta mathematica* **13**, 1-270 (1890)

[50] Poincaré H. *Les Méthodes Nouvelles de la Méchanique Céleste* (Gauthier-Villars, Paris) (1892)

[51] Gutzwiller M. C. *Chaos in Classical and Quantum Mechanic* (Springer-Verlag, New York) (1990)

[52] Vymětal S. *Chaos in the conditional dynamics of purification protocols*, dissertation, FJFI ČVUT (2010)

[53] Fornæs J. E. *Dynamics in several complex variables* (Amer. Math. Soc.) (1994)

[54] Guan Y., Nguyen D.Q., Xu J., Gong J. *Phys. Rev. A* **87**, 052316 (2013)

[55] Fiedler M. *Speciální matice a jejich použití v numerické matematice* (SNTL, Praha) (1981)

[56] Mareš J. *Algebra* (ČVUT, Praha) (2014)

[57] Zhang *Matrix theory* (Springer, New York) (2011)

[58] Hedayat A., Wallis W.D. *The Annals of statistics* **6**, 1184-1238 (1978)

[59] Kunz H.O. *IEEE Transactions on Computers* **28**, 267-268 (1979)

[60] Sharp J. *Mathematical Gazette* **82**, 203-214 (1998)