Comenius University in Bratislava
Faculty of mathematics physics and informatics

Quantum teleportation and its applications

(Bachelor's Thesis)

Denisa Lampášová

Advisor: Mgr. Daniel Nagaj, PhD.

Bratislava, 2017

Comenius University in Bratislava
Faculty of mathematics physics and informatics

Quantum teleportation and its applications

Bachelor's Thesis

Study programme:	1160 Physics
Field of study:	Physics
Department:	Department of theoretical physics and physics education
Advisor:	Mgr. Daniel Nagaj, PhD.

Bratislava, 2017
Denisa Lampášová

Comenius University in Bratislava
Faculty of Mathematics, Physics and Informatics

THESIS ASSIGNMENT

Name and Surname:	Denisa Lampášová
Study programme:	Physics (Single degree study, bachelor I. deg., full time form)
Field of Study:	Physics
Type of Thesis:	Bachelor´s thesis
Language of Thesis:	English
Secondary language:	Slovak

Title:	Quantum teleportation and its applications
Aim:	We will investigate quantum teleportation and its applications and interpretation. Our main focus will be on entanglement switching and causality, time-space travel, postselection and computation, and gate teleportation as a computational primitive.
Literature:	Nielsen & Chuang, Quantum Information & Computation Kay, Laflamme & Mosca, An Introduction to Quantum Computing
Keywords:	quantum teleportation, quantum computation, causality, signaling

Supervisor:	Mgr. Daniel Nagaj, PhD. (from 2016-09-02)
Department:	FMFI.KTFDF - Department of Theoretical Physics and Didactics of Physics
Head of department:	doc. RNDr. Tomáš Blažek, PhD.
Assigned:	19.10.2016
Approved:	26.10.2016

prof. RNDr. Jozef Masarik, DrSc.
Guarantor of Study Programme

.....
Student

.....
Supervisor

I hereby declare I wrote this thesis by myself, only with the help of referenced literature, under the careful supervision of my thesis supervisor.

.....

Denisa Lampášová

Acknowledgement

I would like to express my heartful “thank you” to my advisor Mgr. Daniel Nagaj, PhD. I really appreciate all the time you gave me. The energy and interest you put into explaining all the problematic matter. I really love all the questions and interesting food for thought you have provided me. Thank you for everything. I honestly cannot imagine a better supervisor.

A very special gratitude goes to my family and friends. Thank you for listening, helping me and discussing my problems you may not always be interested in. Thank you for all the emotional support you have provided me. Without you writing this thesis would be lot more stressful.

Additional thanks goes to all the composers of music I have listened to. Thank you for creating such amazing masterpieces which were filling me with energy and good mood while working on this thesis.

Abstract

This thesis focuses on understanding quantum teleportation and the way it works. We have described the concept of an entangled pair and explored what advantages can we gain, and what, on the other hand, is not achievable by their usage. We have demonstrated that quantum physics brings possibilities that don't exist in classical physics.

In the beginning, we have explained the basic concepts and introduced the required mathematical apparatus. The primary goal was to understand the differences between systems based on quantum mechanics and classical systems we have an intuition for from our daily lives. Next, we have explained in more detail the quantum teleportation and its possible interpretations. We have shown how we can use it to entangle remote particles which could have never met. Based on the impossibility of faster-than-light communication we have demonstrated why the quantum teleportation works the way it does. Further, we have shown that by using entanglement swapping n times we can entangle particles that are extremely distant – the distance between them is greater than distance over which we can successfully, without corruption, transport already entangled pairs. Finally, on a simple CHSH game, we have demonstrated the advantages of quantum-based strategies (leveraging entangled pairs and operations on them), in particular, how these strategies increase our chances of winning the game and discussed the possibility of the existence of even better strategies.

Unfortunately, due to lack of time, we have omitted discussion about time travel, quantum error correction and phase estimation measurements.

Keywords: quantum teleportation, quantum entanglement, quantum computation, causality, signaling

Abstrakt

Táto práca je zameraná na pochopenie, čo je to kvantová teleportácia a ako funguje. Ozrejmili sme v nej taktiež pojem previazaného páru. Zistili sme, čo vieme z vlastností takýchto párov vyťažiť a čo naopak nie. Ukázali sme, že kvantová fyzika nám priniesla možnosti, o ktorých sme bez jej znalosti mohli iba snívať.

Na začiatku sme vysvetlili základné koncepty a matematický aparát. Cieľom bolo najmä pochopenie, že kvantovo-mechanické systémy sú naozaj odlišné od klasických, pre ktoré máme vybudovanú intuíciu. Následne sme podrobnejšie vysvetlili, čo je to kvantová teleportácia a ako ju vieme interpretovať. Vysvetlili sme si, ako ju vieme použiť na previazanie vzdialených častíc, ktoré sa nikdy nemuseli stretnúť. Na základe nemožnosti komunikácie nadvetelnou rýchlosťou sme ukázali, prečo kvantová teleportácia funguje tak ako funguje. Ukázali sme aj, že n-násobným teleportačným previazávaním vieme účinne previazať aj veľmi vzdialené častice – ďaleko za hranicou vzdialenosti, kde by sme vedeli preniesť previazané páry bez poškodenia. Nakoniec sme na jednoduchej hre ukázali, že pomocou kvantových stratégií (použitím previazaného páru, operácií a meraní na nich vykonávaných) vieme zvýšiť šance na výhru a prediskutovali sme, či by bola možná ešte lepšia stratégia.

Žiaľ pre krátkosť času a vyťaženosť sme sa nedostali k diskusiám o cestovaní v čase, k využitiu kvantovej korekcie chýb a k rozoberaniu spôsobu merania veličín pomocou určovania fázy.

Kľúčové slová: kvantová teleportácia, kvantové previazanie, kvantové počítanie, kauzalita, posielanie signálov

Contents

Introduction

> *"It's the questions we can't answer that teach us the most. They teach us how to think. If you give a man an answer, all he gains is a little fact. But give him a question and he'll look for his own answers."*
>
> — Patrick Rothfuss, *The Wise Man's Fear*

This thesis is focused on deeper understanding of what is an entangled pair and quantum teleportation – the key elements of todays quantum computing. It explores some advantages provided by the quantum physics and discusses its differences with classical physics. Structure of this work is driven by the order which in the author's opinion is best for comprehension of the topic.

The purpose of the first chapter is to describe basic concepts as we understand them and prepare the ground for solving problems discussed in the next chapters by introducing the suitable mathematical aparatus.

In the second chapter we provide an explanation of what is quantum teleportation and entanglement swapping. We try to deepen this understanding by discusing why quantum teleportation works the way it does. We also show that we can interconnect several entanglement swappings and demonstrate what advantages it provides.

The third (last) chapter shows the differences between quantum and classical physics by demonstrating that quantum mechanics can help us improve probability of winning in games. At the end we discuss, that there is a possibility of existence of another field of physics which could bring us even more advantages than quantum mechanics does.

Chapter 1

Theoretical Background

Information – a subtle principal concept taken for granted in our everyday life. Information affects our decisions. We want to share it (whether it is true or false). Even the whole world of electronic computing depends on it. It is a common knowledge, that electronic computing is "just processing some *bits*" where the bit – short for *binary digit* – is the smallest unit of information in these systems, having either value 1 or 0. In today's computing devices, each bit is represented by either a presence or absence of a certain physical quantity, most commonly voltage, but in general it can be represented by any system which can be in two possible states. To illustrate this, simply look at the magnetization ($\uparrow$ or $\downarrow$) of sub-micrometer-sized regions of some magnetic medium (e.g. a cobalt-based alloy) used in hard drives, at the presence or absence of holes in predefined positions used in punched cards or at a presence or absence of a reflected laser beam caused by desctructive or non-destructive interference of reflected laser beams from cleverly organized "lands" and "pits" on the metal layer forming a spiral data track on CDs.

1.1 A Quantum Bit

In a quantum mechanical world, imagine a system with two possible states corresponding to two wavefunctions $\psi_1(x)$ and $\psi_2(x)$. The system can also be in a superposition of these states, deribed by a wavefunction $\psi(x) = a \cdot \psi_1(x) + b \cdot \psi_2(x)$, where a and b are complex numbers called *amplitudes* of the basis states $\psi_1(x)$ and $\psi_2(x)$, meeting a not very surprising condition $|a|^2 + |b|^2 = 1$ as $|a|^2$ can be interpreted as the probability of measuring $\psi(x)$ in the state $\psi_1(x)$ and $|b|^2$ as the probability of measuring $\psi(x)$ in the state $\psi_2(x)$.

A short but very important note about measurements

In quantum mechanics, each physical observable has a corresponding operator. *Eigenfunctions* of such an operator – wavefunctions which after aplying the operator stay unchanged or multiplied by some constant[1] (= *eigenvalue*) – form a basis any wavefunction can be expressed in. The eigenvalues are all measurable values of the physical quantity the system can have. The probability of measuring an eigenvalue is equal to the amplitude standing before the corresponding eigenfunction when the state of the system is writen in this basis squared. After measurement, the state of the system collapses into the eigenfunction corresponding to the measured eigenvalue.

Any orthonormal set of all possible eigenfunctions of operator corresponding to measuring quantity $\{\psi_1(x), \psi_2(x), \ldots, \psi_n(x)\}$ represents an n-level system we can use for quantum computing. In analogy to classical computing, we usually use two-level systems – *qubits* (short for *quantum bits*).[2] In comparison to classical bit, qubit can hold any state which is in superposition of the possible (= which we can measure) two. That means qubits can replace classical bits but they provide us more as we will see in the following sections.

Examples of simple two-level systems include linear polarization of light (horizontal or vertical), two levels of an atom (ground or excited),[3] spin of an electron ($\uparrow$ or $\downarrow$) in the Stern-Gerlach experiment or the position of an electron in a double quantum dot.

1.1.1 Hilbert Space and the Dirac Notation

A *Hilbert space* $\mathcal{H}$ is a finite-dimensional vector space. Any quantum system S has a corresponding *state space* (Hilbert space) $\mathcal{H}_S$. A state of the quantum system is described by an one dimensional subspace of $\mathcal{H}_S$, that means a line or *ray* $[\vec{u}]$ where $\vec{0} \neq \vec{u} \in \mathcal{H}_S$. Linearly dependent non zero vectors $\vec{u}$, $\vec{v} \in \mathcal{H}_S$ correspond to the same quantum state, so each quantum state can be decribed by a unit vector in a Hilbert space.

Consider a complete orthonormal basis $\{\psi_1(x), \psi_2(x)\}$ for a two-level quantum system. This wavefunction basis can be represented with two orthonormal vectors $|\psi_1\rangle$ and $|\psi_2\rangle$ generating a two-dimensional Hilbert space – the state space of this system.

[1] "Unchanged" is a special case of multiplying by a constant, where the constant is 1.

[2] We can often transform a multi-level system to two-level system by creating conditions in which the other states, except the two considered states, are highly improbable.

[3] From quantum mechanics we know that the energy levels of the atom are discrete. We can have a system we can tell the atom is either in the ground state or the first excited state because the amount of energy needed to excite the system to higher energy levels is really high and we can take care to help the system at a low temperature so that we rarely find such a highly excited state.

We usually use the Z basis (also called *computational basis*):

$$|\psi_1\rangle = \begin{pmatrix}1\\0\end{pmatrix} = |0\rangle\,, \qquad |\psi_2\rangle = \begin{pmatrix}0\\1\end{pmatrix} = |1\rangle\,, \tag{1.1}$$

where a general state $|\psi\rangle = a\,|\psi_1\rangle + b\,|\psi_2\rangle$ is represented as a unit vector

$$|\psi\rangle = \begin{pmatrix}a\\b\end{pmatrix}. \tag{1.2}$$

Another common one is the X basis:

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} = |+\rangle\,, \tag{1.3}$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix} = |-\rangle\,, \tag{1.4}$$

or the Y basis:

$$|\psi_1\rangle = \frac{1}{2}\begin{pmatrix}1-i\\1+i\end{pmatrix}, \qquad |\psi_2\rangle = \frac{1}{2}\begin{pmatrix}i-1\\1+i\end{pmatrix}. \tag{1.5}$$

Notice that we have changed the notation for vectors from the classical $\vec{\psi}$ to *ket* notation $|\psi\rangle$. Any symbol $\heartsuit$ written inside a *ket* $|\heartsuit\rangle$ represents a vector in $\mathcal{H}$:

$$|\heartsuit\rangle = \begin{pmatrix}x_1\\x_2\\\vdots\\x_N\end{pmatrix} \in \mathcal{H}, \tag{1.6}$$

where $N = \dim \mathcal{H}$. The symbol writen inside a *bra* $\langle\heartsuit|$ symbolizes the *dual vector* of $|\heartsuit\rangle$ defined as

$$|\heartsuit\rangle^\dagger = \begin{pmatrix}x_1\\x_2\\\vdots\\x_N\end{pmatrix}^\dagger = \begin{pmatrix}x_1\\x_2\\\vdots\\x_N\end{pmatrix}^{*\mathrm{T}} = \begin{pmatrix}x_1^*\\x_2^*\\\vdots\\x_N^*\end{pmatrix}^{\mathrm{T}} = \begin{pmatrix}x_1^* & x_2^* & \cdots & x_N^*\end{pmatrix} = \langle\heartsuit| \in \mathcal{H}^*, \tag{1.7}$$

where the Hilbert space $\mathcal{H}^*$ (*dual vector space*) is a complex vector space of linear functions $f : \mathcal{H} \to \mathbb{C}$. The action of an element $\langle\varphi| = \begin{pmatrix}\varphi_1^* & \varphi_2^* & \cdots & \varphi_N^*\end{pmatrix} \in \mathcal{H}^*$ on an element $|\psi\rangle = \begin{pmatrix}\psi_1 & \psi_2 & \cdots & \psi_N\end{pmatrix}^{\mathrm{T}} \in \mathcal{H}$ is:

$$\langle\varphi| : |\psi\rangle \mapsto \langle\varphi|\psi\rangle \in \mathbb{C}, \tag{1.8}$$

where $\langle\varphi|\psi\rangle$ is *the inner-product* (also called *dot product*, *scalar product* or *projection product*), written as a "bra-ket", of $|\varphi\rangle$ with $|\psi\rangle$. In more detail,

$$\langle\varphi|\psi\rangle = |\varphi\rangle \cdot |\psi\rangle = \begin{pmatrix}\varphi_1\\ \varphi_2\\ \vdots\\ \varphi_N\end{pmatrix} \cdot \begin{pmatrix}\psi_1\\ \psi_2\\ \vdots\\ \psi_N\end{pmatrix} = \begin{pmatrix}\varphi_1^* & \varphi_2^* & \cdots & \varphi_N^*\end{pmatrix} \begin{pmatrix}\psi_1\\ \psi_2\\ \vdots\\ \psi_N\end{pmatrix} =$$

$$= \varphi_1^*\psi_1 + \varphi_2^*\psi_2 + \cdots + \varphi_N^*\psi_N = \sum_{i=1}^{N} \varphi_i^*\psi_i. \tag{1.9}$$

The inner product $\langle\varphi|\psi\rangle$ is in terms of the wavefunctions equal to

$$\int \varphi^*(x)\,\psi(x)\,\mathrm{d}x. \tag{1.10}$$

In Hilbert space, it is equal to the length of the projection of the vector $|\varphi\rangle$ on the vector $|\psi\rangle$. We should mention that the *bra-ket* notation we have used so far is called *Dirac notation*, named after Paul Dirac who invented it.

1.1.2 Minimalistic representation of a qubit

Conventionally, a qubit has four real parameters (a, b, c, $d \in \mathbb{R}$): $(a+ib)\,|0\rangle + (c+id)\,|1\rangle$. After rewriting the comlex amplitudes into polar coordinates we obtain: $le^{i\alpha}\,|0\rangle + re^{i\beta}\,|1\rangle$ (with four parameters l, α, r, $\beta \in \mathbb{R}$) where $l = \sqrt{a^2+b^2} \in \mathbb{R}$ and $r = \sqrt{c^2+d^2} \in \mathbb{R}$ are the lengths of the complex numbers and $\alpha = \arctan(b/a)$, $\beta = \arctan(d/c)$ the angles between the numbers and the real axes.

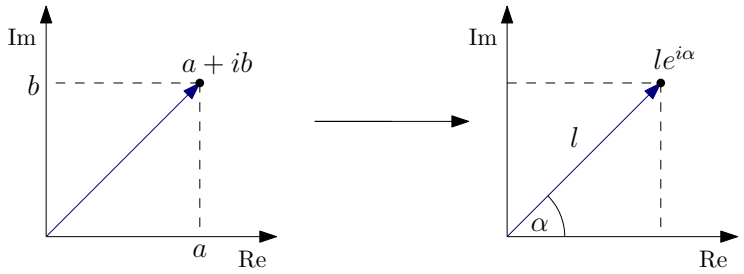


Figure 1.1: Changing a coordinate system from Cartesian ($a + ib$ on the left side) to polar ($le^{i\alpha}$ on the right side).

Because

$$\left|le^{i\alpha}\right|^2 = |l|^2\left|e^{i\alpha}\right|^2 = |l|^2 e^{-i\alpha}e^{i\alpha} = |l|^2 = l^2, \tag{1.11}$$

we can rewrite the condition $\left|le^{i\alpha}\right|^2 + \left|re^{i\beta}\right|^2 = 1$ into $l^2 + r^2 = 1$. Any two real numbers l, r meeting $l^2 + r^2 = 1$ can be transformed into the form $l = \cos\left(\frac{\theta}{2}\right)$ and $r = \sin\left(\frac{\theta}{2}\right)$ as

$\cos^2(\frac{\theta}{2}) + \sin^2(\frac{\theta}{2}) = 1$.[4] Here we have lost one of the four parameters. The state of the qubit has now form $e^{i\alpha}\cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\beta}\sin\left(\frac{\theta}{2}\right)|1\rangle$. After extracting the *global phase* $e^{i\alpha}$ and substituting φ for $\beta - \alpha$, we get

$$e^{i\alpha}\begin{pmatrix}\cos\frac{\theta}{2}\\ e^{i\varphi}\sin\frac{\theta}{2}\end{pmatrix}. \tag{1.12}$$

As $e^{i\alpha}|\psi\rangle$ and $|\psi\rangle$ belong to the same line in the Hilbert space, they represent the same state of a qubit. Basically, the global phase does not affect the probabilities of measurement outcomes so any two states differing only by some global phase are for all practical purposes the same. However, notice that even though the global phase is irrelevant, the *relative phase* $e^{i\varphi}$ between parts of a superposition is highly important. For example, the states $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ are perpendicular and so easily distinguishable when measured in the X basis.

Finally, we end up with two real parameters θ and φ so a general state $|\psi\rangle$ of a qubit can be expressed in the form

$$\begin{pmatrix}\cos\frac{\theta}{2}\\ e^{i\phi}\sin\frac{\theta}{2}\end{pmatrix}. \tag{1.13}$$

One of the useful implications is that we can represent the state of a qubit as a point on the sphere – *Bloch sphere* – instead of a ray (or a vector) in a 2-dimensional complex vector space.

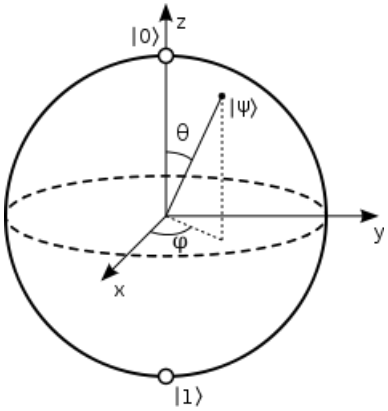


Figure 1.2: State of a qubit on a Bloch sphere.

1.1.3 Operators

Operators on a vector space $\mathcal{H}$ are linear transformations T: $\mathcal{H} \to \mathcal{H}$ of the vector space to itself (i.e. linear transformations mapping vectors in $\mathcal{H}$ to vectors in $\mathcal{H}$). The

[4] We should notice that the reason for choosing $\frac{\theta}{2}$ instead of θ is just conventional so that choosing θ between 0 and 2π does not result in double counting.

simplest operator is an *outer product* which is obtained by multiplying a ket vector $|\psi\rangle = \begin{pmatrix}\psi_1 & \psi_2 & \cdots & \psi_N\end{pmatrix}^{\mathrm{T}}$ on the right by a bra vector $\langle\varphi| = \begin{pmatrix}\varphi_1^* & \varphi_2^* & \cdots & \varphi_N^*\end{pmatrix}$:

$$|\psi\rangle\langle\varphi| = \begin{pmatrix}\psi_1\\ \psi_2\\ \vdots\\ \psi_N\end{pmatrix}\begin{pmatrix}\varphi_1^* & \varphi_2^* & \cdots & \varphi_N^*\end{pmatrix} = \begin{pmatrix}\psi_1\varphi_1^* & \psi_1\varphi_2^* & \cdots & \psi_1\varphi_N^*\\ \psi_2\varphi_1^* & \psi_2\varphi_2^* & \cdots & \psi_2\varphi_N^*\\ \vdots & \vdots & \ddots & \vdots\\ \psi_N\varphi_1^* & \psi_N\varphi_2^* & \cdots & \psi_N\varphi_N^*\end{pmatrix}. \tag{1.14}$$

The action of $|\psi\rangle\langle\varphi|$ on a vector $|\phi\rangle$ is defined by

$$(|\psi\rangle\langle\varphi|)|\phi\rangle = |\psi\rangle\langle\varphi|\phi\rangle = (\langle\varphi|\phi\rangle)|\psi\rangle. \tag{1.15}$$

The outer product of a vector $|\psi\rangle$ with itself, written $|\psi\rangle\langle\psi|$, defines a linear operator that maps

$$(|\psi\rangle\langle\psi|)|\phi\rangle = |\psi\rangle\langle\psi|\phi\rangle = (\langle\psi|\phi\rangle)|\psi\rangle. \tag{1.16}$$

As $|\psi\rangle$ and $|\phi\rangle$ are unit vectors and $\langle\psi|\phi\rangle$ the length of the projection of the vector $|\phi\rangle$ on the vector $|\psi\rangle$, $(\langle\psi|\phi\rangle)|\psi\rangle$ is literally the orthogonal projection of the vector $|\phi\rangle$ in the direction of $|\psi\rangle$. Operators behaving in this way are called *orthogonal projectors* and we most often use them in projective measurements.

Projective measurements

Imagine a photon with an unknown polarization. Vertical and horizontal polarizations represent a basis for this two-level system, so we can assign the vector $|0\rangle$ to the horizontal polarization and $|1\rangle$ to the vertical polarization. If we know that our photon is either in the state $|1\rangle$ or in the state $|0\rangle$, one of the possible ways how to distinguish them is taking a linear (absorptive) polarizer and look whether the photon has passed through or was absorbed. This is a projective measurement.
In general, any state $|\psi\rangle$ of a qubit can be expressed in an orthonormal basis $\{|\varphi_{\mathrm{A}}\rangle, |\varphi_{\mathrm{B}}\rangle\}$ as $|\psi\rangle = \langle\varphi_{\mathrm{A}}|\psi\rangle|\varphi_{\mathrm{A}}\rangle + \langle\varphi_{\mathrm{B}}|\psi\rangle|\varphi_{\mathrm{B}}\rangle$. If we apply a projective measurement into $|\varphi_{\mathrm{A}}\rangle$ on the qubit, the qubit passes through the aparatus with probability $|\langle\varphi_{\mathrm{A}}|\psi\rangle|^2 = \langle\psi|\varphi_{\mathrm{A}}\rangle\langle\varphi_{\mathrm{A}}|\psi\rangle$ with the measurement outcome 1. On the other hand, with probability $|\langle\varphi_{\mathrm{B}}|\psi\rangle|^2 = \langle\psi|\varphi_{\mathrm{B}}\rangle\langle\varphi_{\mathrm{B}}|\psi\rangle$ the outcome is 0 as nothing has passed through the aparatus.

We should mention that in general, a projector on a vector space $\mathcal{H}$ is a linear operator P which meets a condition $P^2 = P$. A projector P is orthogonal if P also satisfies $P^\dagger = P$.

Notice that for any orthonormal basis $\mathrm{B} = \{|b_n\rangle\}$ there is an extremely useful "completeness relation"

$$I = \sum_{b_n\in\mathrm{B}} |b_n\rangle\langle b_n|. \tag{1.17}$$

The usefulness can be seen, for example, in possibility to express each of the projectors to the basis vectors of a two-dimensional Hilbert space $\mathcal{H}$, $\{|b_1\rangle, |b_2\rangle\}$, in terms of the other one:

$$|b_1\rangle\langle b_1| = I - |b_2\rangle\langle b_2|. \tag{1.18}$$

In general, identity minus any projector is also a projector as

$$(I-P)^2 = I - 2P + P^2 = I - 2P + P = I - P \tag{1.19}$$

and any space $\mathcal{H}$ with an orthonormal basis $\mathrm{B} = \{|b_n\rangle\}$ divided into two subspaces $\mathcal{H}_\mathrm{A}$ with basis $\mathrm{B_A} \subset \mathrm{B}$ and $\mathcal{H}_\mathrm{B}$ with basis $\mathrm{B_B} \subset \mathrm{B}$, such that $\mathrm{B_A} + \mathrm{B_B} = \mathrm{B}$, has the projectors into the subspaces ($P_{\mathcal{H}_\mathrm{A}} = \sum_{\mathrm{b_n}\in\mathrm{B_A}} |b_n\rangle\langle b_n|$ and $P_{\mathcal{H}_\mathrm{B}} = \sum_{\mathrm{b_n}\in\mathrm{B_B}} |b_n\rangle\langle b_n|$), thanks to the completeness relation, related by equation

$$\begin{aligned}\sum_{\mathrm{b_n}\in\mathrm{B}} |b_n\rangle\langle b_n| = \sum_{\mathrm{b_n}\in\mathrm{B_A}} |b_n\rangle\langle b_n| + \sum_{\mathrm{b_n}\in\mathrm{B_B}} |b_n\rangle\langle b_n| = I \implies \\ \implies \sum_{\mathrm{b_n}\in\mathrm{B_A}} |b_n\rangle\langle b_n| = I - \sum_{\mathrm{b_n}\in\mathrm{B_B}} |b_n\rangle\langle b_n|.\end{aligned} \tag{1.20}$$

Every linear operator T on a vector space $\mathcal{H}$ can be written in terms of complex constants $T_{n,m}$ and outer products of basis vectors $\mathrm{B} = \{|b_n\rangle\}$ of $\mathcal{H}$ as

$$T = \sum_{b_n, b_m \in \mathrm{B}} T_{n,m} |b_n\rangle\langle b_m| = \begin{pmatrix} T_{1,1} & T_{1,2} & \cdots & T_{1,m} \\ T_{2,1} & T_{2,2} & \cdots & T_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ T_{n,1} & T_{n,2} & \cdots & T_{n,m} \end{pmatrix} \tag{1.21}$$

where $T_{n,m} = \langle b_n| T |b_m\rangle$. The set of all linear operators on a vector space $\mathcal{H}$ forms a new complex vector space $\mathcal{L}(\mathcal{H})$ where "vectors" are the linear operators. The basis for $\mathcal{L}(\mathcal{H})$ is constructed of all possible outer products of basis vectors from B, that is $\{|b_n\rangle\langle b_m|\}$.

The *adjoint* of the operator $T \in \mathcal{H}$, denoted $T^\dagger$, is a linear operator on $\mathcal{H}^*$ which satisfies

$$(\langle\psi| T^\dagger |\varphi\rangle)^* = \langle\varphi| T |\psi\rangle, \quad \forall |\psi\rangle, \forall |\varphi\rangle \in \mathcal{H}. \tag{1.22}$$

Each map in $\mathcal{H}^*$ corresponds to some bra vector $\langle\theta'|$ so $\langle\varphi| T |\psi\rangle = \langle\varphi'|\psi\rangle$. We can consider $T^\dagger$ to be a linear map that sends $|\varphi\rangle \to |\varphi'\rangle$ so we would get

$$\langle\varphi| T |\psi\rangle = \langle\varphi'|\psi\rangle = (\langle\psi|\varphi'\rangle)^* = (\langle\psi| T^\dagger |\varphi\rangle)^*. \tag{1.23}$$

An operator U is called *unitary* if $U^\dagger = U^{-1}$ (or equivalently $U^\dagger U = I$), where U^{-1} is the inverse of U. Unitary operators have several pleasant properties. One of them is

the preservation of lengths and angles between vectors. Another one is orthogonality of its eigenvectors. However, the eigenvalues are not necessarily real. For every unitary operator U there is a *Hermitian* (or *self-adjoint*) operator H – linear operator on $\mathcal{H}$ satisfying $H^\dagger = H$ – such that

$$U = e^{iH}. \tag{1.24}$$

We can prove the previous statement (1.24) using properties of unitary and Hermitian matrices, that both can be written in the form

$$B = P \cdot A \cdot P^{-1} = P \cdot A \cdot P^\dagger, \tag{1.25}$$

where P is a unitary matrix whose columns encode the eigenvectors of B and A is a diagonal matrix whose diagonal entries are the eigenvalues of B. Hence, any unitary matrix U can be writen as $U = P \cdot \mathrm{diag}\,(\lambda_1, \ldots, \lambda_n) \cdot P^\dagger$. Because eigenvalues of unitary matrices have magnitude 1 ($|\lambda| = 1$), there exist real numbers α_j such that $\lambda_j = e^{i\alpha_j}$. Then the matrix

$$H = P \cdot \mathrm{diag}(\alpha_1, \ldots, \alpha_n) P^\dagger \tag{1.26}$$

is Hermitian and due to

$$(e^{iH})^{-1} = e^{-iH} = (e^{iH})^\dagger, \tag{1.27}$$

the matrix e^{iH} is unitary and thus $U = e^{-iH}$.

The *expectation value* of an operator A in a state $|\psi\rangle$ is defined as $\langle\psi| A |\psi\rangle$. If A is Hermitian, the expectation value gives the average result of many repeated measurements on many fresh systems in the state $|\psi\rangle$. Hermitian operators, thanks to their property of having real eigenvalues and expectation values, have all the properties necessary to represent physical observables. Thus each physical observable corresponds to a Hermitian operator. However, as there is an infinite number of Hermitian operators, there is no hope ever finding experiments for all of them.

Two operators A, B are said to *commute* if their *commutator* $[A, B] = AB - BA$ is equal to 0. For any two commuting operators there is a common complete set of eigenvectors. If A and B represent some pair of physical observables, we can measure these observables simultaneously: the expectation value of measuring observable (A) in some state is equal to the expectation value of the same observable (A) in the state on which we first performed a measurement of the second observable (B):

$$\langle\psi| A |\psi\rangle = (\langle\psi| B^\dagger) A (B |\psi\rangle). \tag{1.28}$$

This is true for any pair of commuting observables, because if $|\varphi\rangle$ is an eigenvector of A ($A |\varphi\rangle = a |\varphi\rangle$) then $B |\varphi\rangle$ is also an eigenvector of A, as

$$AB |\varphi\rangle = BA |\varphi\rangle = Ba |\varphi\rangle = aB |\varphi\rangle . \tag{1.29}$$

To be more explicit, we can write $|\psi\rangle$ as a linear combination of eigenvectors of A $\{|\varphi_i\rangle\}$:

$$|\psi\rangle = \sum_i c_i |\varphi_i\rangle , \tag{1.30}$$

so the expectation value transforms into

$$\langle\psi| B^\dagger AB |\psi\rangle = \sum_i \langle\varphi_i| c_i^* B^\dagger ABc |\varphi_i\rangle = \sum_i a_i|c|^2 \langle\varphi_i| B^\dagger B |\varphi_i\rangle = \sum_i a_i|c|^2 =$$
$$= \sum_i a_i|c|^2 \langle\varphi_i|\varphi_i\rangle = \sum_i |c|^2 \langle\varphi_i| A |\varphi_i\rangle = \sum_i \langle\varphi_i| c_i^* Ac_i |\varphi_i\rangle = \langle\psi| A |\psi\rangle . \tag{1.31}$$

Let us look at one common example of commuting observables. The spin of a spin $\frac{1}{2}$ particle with respect to the z axis corresponding to the operator

$$L_z = \frac{\hbar}{2} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} , \tag{1.32}$$

and the total spin angular momentum of this particle represented by

$$\mathbf{L}^2 = \frac{3}{4}\hbar^2 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} . \tag{1.33}$$

Observe that these commute. Indeed they can be measured simultaneously.

Analogously to the commutator, we define the *anticommutator* $\{A, B\} = AB + BA$. Two operators A, B anticommute if $\{A, B\} = 0$. If A and B were non-degenerate Hermitian operators with eigenvalues $\pm x$ acting on two-dimensional Hilbert space with corresponding orthonormal bases $\{|\alpha_1\rangle , |\alpha_2\rangle\}$ and $\{|\beta_1\rangle , |\beta_2\rangle\}$ constructed from eigenvectors, then

$$\begin{aligned} A |\beta_1\rangle &= \text{constant} \cdot |\beta_2\rangle , & B |\alpha_1\rangle &= \text{constant} \cdot |\alpha_2\rangle , \\ A |\beta_2\rangle &= \text{constant} \cdot |\beta_1\rangle , & B |\alpha_2\rangle &= \text{constatnt} \cdot |\alpha_1\rangle . \end{aligned} \tag{1.34}$$

This phenomenon happens because

$$AB |\alpha_1\rangle = -BA |\alpha_1\rangle = -Bx |\alpha_1\rangle = -x(B |\alpha_1\rangle) \tag{1.35}$$

and as we know, A is non-degenerate so if $A |\alpha_2\rangle = -x |\alpha_2\rangle$ and $A(B |\alpha_1\rangle) = -x(B |\alpha_1\rangle)$, then $B |\alpha_1\rangle = \text{constant} \cdot |\alpha_2\rangle$.

Gates

In electronics, a *logic gate* is a device implementing a logical operation on one or more binary inputs. Analogically, a quantum gate (quantum logic gate) takes qubits as input, implements on them some unitary operation and outputs them with changed

state. These gates together with lines representing qubits are base components in quantum circuit notation.

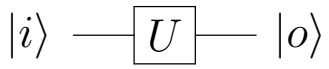


Figure 1.3: A gate implementing an unitary operation U: $U|i\rangle = |o\rangle$.

Measurement applied on a qubit is usually depicted as

where the the double line on the right represents a classical bit.

Here we define the *Pauli gates*:

$$\begin{aligned} I &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & X &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = NOT \\ Y &= \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} & Z &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \end{aligned} \tag{1.36}$$

Except the identity I whose only eigenvalue is 1, each of the Hermitian, unitary Pauli matrices has two eigenvalues of the form: $\pm x$. Concretelly, the X and Z gates have eigevalues ± 1 and the Y gate $\pm i$. The corresponding normalized eigenvectors have been already mentioned in subsection 1.1.1 as possible orthonormal bases for 2-dimensional Hilbert space.

As we have already mention, a general single-qubit state can be represented by a point on a Bloch sphere. In terms of the Bloch sphere, any single-qubit gate U can be thought of as a rotation about an arbitrary axis passing through its centre. However, The Bloch sphere is a pure mathematical structure. Even though the real life implementations can be often thought of as a rotation about an arbitrary axis, too (e.g. changing the spin of an electron). However, the experiments are in the matter of arbitrary axes constrained. Thus we often use the fact that any rotation can be constructed as a sequence of rotations about two non-parallel axes l, m. In the matter of fact, any unitary gate U can be given by

$$U = e^{i\alpha} R_l(\beta) R_m(\gamma) R_l(\delta). \tag{1.37}$$

The Pauli gates X, Y and Z represent a great basis as they act as rotations about very distinctive axes. To be more explicit, the rotation gates about x-, y- and z-axes are

defined as follows:

$$\begin{aligned} R_x(\theta) &= e^{\frac{-i\theta X}{2}}, \\ R_y(\theta) &= e^{\frac{-i\theta Y}{2}}, \\ R_x(\theta) &= e^{\frac{-i\theta Z}{2}}. \end{aligned} \tag{1.38}$$

Using Taylor series and property of Pauli matrices that $P^2 = I$, any of the rotation gates can be written as

$$\begin{aligned} e^{\frac{-i\theta P}{2}} = \sum_{n=0}^{\infty} \frac{\left(-i\frac{\theta}{2}P\right)^2}{n!} = I - i\frac{\theta}{2}P - \frac{1}{2!}\left(\frac{\theta}{2}\right)^2 I + \frac{i}{3!}\left(\frac{\theta}{2}\right)^3 P + \frac{1}{4!}\left(\frac{\theta}{2}\right)^4 I - \\ -\frac{i}{5!}\left(\frac{\theta}{2}\right)^5 P - \frac{1}{6!}\left(\frac{\theta}{2}\right)^6 I + \ldots = \left[1 - \frac{1}{2!}\left(\frac{\theta}{2}\right)^2) + \frac{1}{4!}\left(\frac{\theta}{2}\right)^4 - \frac{1}{6!}\left(\frac{\theta}{2}\right)^6 + \ldots\right] I - \\ -i\left[\frac{\theta}{2} - \frac{1}{3!}\left(\frac{\theta}{2}\right)^3 + \frac{1}{5!}\left(\frac{\theta}{2}\right)^5 - \ldots\right] P = \cos\left(\frac{\theta}{2}\right) I - i\sin\left(\frac{\theta}{2}\right) P. \end{aligned} \tag{1.39}$$

Hence

$$\begin{aligned} R_x(\theta) = e^{\frac{-i\theta X}{2}} &= \cos\left(\frac{\theta}{2}\right) I - i\sin\left(\frac{\theta}{2}\right) X = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -i\sin\left(\frac{\theta}{2}\right) \\ -i\sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix} \\ R_y(\theta) = e^{\frac{-i\theta Y}{2}} &= \cos\left(\frac{\theta}{2}\right) I - i\sin\left(\frac{\theta}{2}\right) Y = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -\sin\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix} \\ R_z(\theta) = e^{\frac{-i\theta Z}{2}} &= \cos\left(\frac{\theta}{2}\right) I - i\sin\left(\frac{\theta}{2}\right) Z = \begin{pmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{pmatrix}. \end{aligned} \tag{1.40}$$

By explicitly acting on a general single-qubit state $\cos\left(\frac{\sigma}{2}\right)|0\rangle + e^{i\tau}\sin\left(\frac{\sigma}{2}\right)|1\rangle$, it is possible to see that the rotation gates really rotate by the angle θ around the corresponding axis. We can see that the Pauli gates X, Y and Z themself represent rotations by π about the respective axes.

Besides the Pauli matrices and rotations, another important, often-used single-qubit gate is the *Hadamard gate*

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{1.41}$$

On the Bloch sphere, the action of the Hadamard gate is represented as a rotation of π about the $\frac{x+z}{\sqrt{2}}$ axis, what is equivalent to rotation of π around the x-axis followed by $\frac{\pi}{2}$ around y-axis. Hadamard is very convenient as it acts as a base-changing matrix between the Z and X basis. This property can be easily seen on the following scheme showing Hadamard acting as rotation of π around the $y = \frac{x}{2}$ axis in the 2-dimensional Hilbert space.

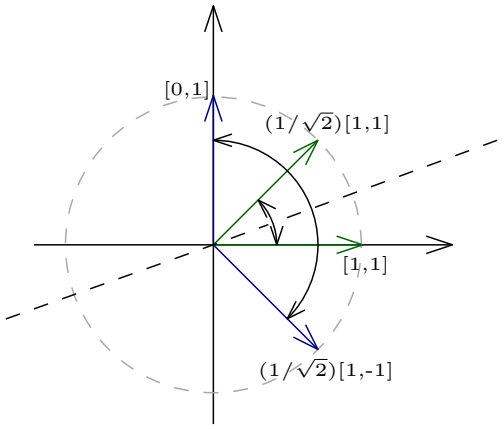


Figure 1.4: Hadamard as a reflection around the dashed axis.

1.1.4 Density Matrix

Probabilistic vs Quantum Bit

A *probabilistic classical bit* – a bit whose value is not known exactly, but is known to be either 0 or 1 with corresponding probabilities p_0 and p_1 satisfying $p_0 + p_1 = 1$. We can represent this bit as a 2-dimensional unit vector

$$\begin{pmatrix} p_0 \\ p_1 \end{pmatrix}, \tag{1.42}$$

or as a point between two possible states 0 and 1.

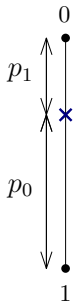


Figure 1.5: A probabilistic bit as a point between the 0 and 1 states with corresponding probabilities p_0 and p_1.

However, what is the difference between the probabilistic classical bit $\begin{pmatrix} 1/2 & 1/2 \end{pmatrix}^{\mathrm{T}}$ and a qubit in a pure state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$?

In order to answer this question we will describe some examples. The probabilistic bit $\begin{pmatrix} 1/2 & 1/2 \end{pmatrix}^{\mathrm{T}}$ can be represented for instance by tossing a coin or by a man wearing white or black socks – both with the same probability. Meanwhile the examples for qubits include a photon polarized in the 45° direction, or the spin of a spin ↑ particle

expressed in the x-basis. The main difference is that while in the case of the probabilistic bit, we can ask just questions like: *Is it a head or a tail?*, *Are the socks white or black?* Questions like: *Are the socks gray?* do not make sense, while in the case of a qubit we can ask about the measurement outcome in multiple different bases. We can measure the spin with respect to the y- or the z-axis or we can even ask about its total spin. The polarization can be measured in the horizontal/vertical basis as well as in $+45°/-45°$ basis. Although there are always just two possible answers, the qubit corresponds to some vector in a space we can look at from different angles, while the probabilistic bit corresponds just to some probabilistic distribution.

Mixed states and density operators

Notice that there are important situations, for which we cannot describe the state of a qubit by a single pure state. In those situations, all we can say is that the qubit is described by one of a specific set of state vectors with corresponding probabilities. We call this states *mixed states*. To illustrate, suppose we know a qubit is in the pure state $|\psi_1\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ with probability $3/4$ and in the pure state $|\psi_2\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$ with probability $1/4$. One way of compact representation of this state is an ensemble

$$\left\{\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, \frac{3}{4}\right), \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle, \frac{1}{4}\right)\right\}. \tag{1.43}$$

However, this representation is not very friendly for calculations. There is a very useful alternative – any mixed state as well as any pure state can be represented in terms of operators on the Hilbert space $\mathcal{H}$ by an operator called *density operator*. The matrix representation of a density operator is called a *density matrix*. The density operator for a pure state $|\psi\rangle$ is defined as

$$\rho = |\psi\rangle\langle\psi|. \tag{1.44}$$

Recall that the probability of measuring qubit in the state $|0\rangle$ is given by

$$\langle 0|\psi\rangle\langle\psi|0\rangle = \langle 0|\rho|0\rangle \in \mathbb{R}. \tag{1.45}$$

Since any number is the trace of a 1×1 matrix whose only entry is that number and since trace is invariant under cyclic permutation (i.e. $\mathrm{Tr}(ABC) = \mathrm{Tr}(BCA) = \mathrm{Tr}(CAB)$) we can write

$$\langle 0|\psi\rangle\langle\psi|0\rangle = \mathrm{Tr}\left(\langle 0|\psi\rangle\langle\psi|0\rangle\right) = \mathrm{Tr}\left(|0\rangle\langle 0|\psi\rangle\langle\psi|\right) = \mathrm{Tr}\left(|0\rangle\langle 0|\rho\right). \tag{1.46}$$

The density operator for a mixed state

$$\{(|\psi_1\rangle, p_1), (|\psi_2\rangle, p_2), \ldots, (|\psi_k\rangle, p_k)\} \tag{1.47}$$

is defined as

$$\rho = \sum_{i=1}^{k} p_i \left|\psi_i\right\rangle \left\langle\psi_i\right|, \tag{1.48}$$

and captures all the relevant information about the state of the system, what can be seen, for example, from computing expectation value:

$$\sum_i p_i \left\langle\psi_i\right| A \left|\psi_i\right\rangle = \sum_i p_i \mathrm{Tr}\big(\left|\psi_i\right\rangle \left\langle\psi_i\right| A\big) = \mathrm{Tr}\Big(\sum_i p_i \left|\psi_i\right\rangle \left\langle\psi_i\right| A\Big) = \mathrm{Tr}\left(\rho A\right), \tag{1.49}$$

as that implies that all that matters for computing statistics associated with measuring any observable quantity is the density operator itself – there is no need to know precise decomposition. Same rules apply for computing density operator of the mixed state after applying the unitary operator U:

$$\sum_{i=1}^{k} p_i U \left|\psi_i\right\rangle \left\langle\psi_i\right| U^\dagger = U \left(\sum_{i=1}^{k} p_i \left|\psi_i\right\rangle \left\langle\psi_i\right|\right) U^\dagger = U\rho U^\dagger. \tag{1.50}$$

As an illustration, compare the density matrix of the pure state $\left|\varphi\right\rangle = \frac{1}{\sqrt{2}}\left|0\right\rangle + \frac{1}{\sqrt{2}}\left|1\right\rangle$:

$$\begin{aligned}\left|\varphi\right\rangle \left\langle\varphi\right| &= \frac{1}{2}\big(\left|0\right\rangle + \left|1\right\rangle\big)\big(\left\langle 0\right| + \left\langle 1\right|\big) = \frac{1}{2}\big(\left|0\right\rangle \left\langle 0\right| + \left|0\right\rangle \left\langle 1\right| + \left|1\right\rangle \left\langle 0\right| + \left|1\right\rangle \left\langle 0\right|\big) = \\ &= \frac{1}{2}\left[\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix} + \begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix} + \begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix} + \begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}\right] = \frac{1}{2}\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix},\end{aligned} \tag{1.51}$$

with the density matrix of the mixed state $\{(\left|0\right\rangle, 1/2), (\left|1\right\rangle, 1/2)\}$

$$\frac{1}{2}\left|0\right\rangle \left\langle 0\right| + \frac{1}{2}\left|1\right\rangle \left\langle 1\right| = \frac{1}{2}\left[\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix} + \begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}\right] = \frac{1}{2}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}. \tag{1.52}$$

Not only are they different, we can distinguish them by measuring X as

$$\left\langle X\right\rangle_{\text{pure state}} = \mathrm{Tr}\left(X\rho\right) = \frac{1}{2}\mathrm{Tr}\left[\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix}\right] = \frac{1}{2}\mathrm{Tr}\left[\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix}\right] = 1 \neq \tag{1.53}$$

$$\neq 0 = \frac{1}{2}\mathrm{Tr}\left[\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\right] = \frac{1}{2}\mathrm{Tr}\left[\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\right] = \left\langle X\right\rangle_{\text{mixed state}}. \tag{1.54}$$

We should mention that each density matrix has trace 1 and is a positive operator (i.e. for any $\left|\phi\right\rangle$, $\left\langle\phi\right| \rho \left|\phi\right\rangle$ is real and non-negative; equivalently, the eigenvalues of ρ are non-negative).

As any pure state of a qubit can be depicted as a point on a Bloch sphere, mixed states correspond to points in the interior of the Bloch sphere. As the Pauli gates span the vector space formed by all 1-qubit operators, any 1-qubit unitary operator can be expressed as a linear combination of the Pauli gates. Since X, Y and Z have trace 0 and I has trace 2, any density operator for a single qubit can be written as

$$\rho = \frac{1}{2}I + \alpha_x X + \alpha_y Y + \alpha_z Z \tag{1.55}$$

where the vector $\left(\alpha_x, \alpha_y, \alpha_z\right)$ gives the coordinates for the point in the Bloch sphere corresponding to the state ρ. The center is the *maximally mixed* (=fully random) state I/2. This state is significant as measuring 0 and 1 have the same probability ($p_0 = p_1 = \frac{1}{2}$) in any basis because

$$U\rho U^{-1} = U\frac{1}{2}IU^{-1} = \frac{1}{2}UU^{-1} = \frac{1}{2}I = \rho. \tag{1.56}$$

1.2 Two Qubits

So far we have discussed 1-qubit systems. However, more interesting and useful phenomenoms happen in systems composed of multiple qubits.

1.2.1 Tensor Products

A *tensor* (or *Kronecker*) *product* is a way of combining spaces, vectors, or operators together. The tensor product of two vector spaces, $\mathcal{H}_\mathrm{A}$ with orthonormal basis $\{|a_i\rangle\}_{i\in\{1,\ldots,n\}}$, and $\mathcal{H}_\mathrm{B}$ with orthonormal basis $\{|b_j\rangle\}_{j\in\{1,\ldots,m\}}$, of dimensions n and m, respectively, is a new vector space $\mathcal{H}_\mathrm{A}\otimes\mathcal{H}_\mathrm{B}$ of dimension $n\times m$ with orthonormal basis $\{|a_i\rangle\otimes|b_j\rangle\}_{i\in\{1,\ldots,n\},j\in\{1,\ldots,m\}}$.

The tensor product meets the following axioms:

1. $\forall c\in\mathbb{C}, |\psi_1\rangle\in\mathcal{H}_1, |\psi_2\rangle\in\mathcal{H}_2$:

$$c\left(|\psi_1\rangle\otimes|\psi_2\rangle\right) = \left(c\,|\psi_1\rangle\right)\otimes|\psi_2\rangle = |\psi_1\rangle\otimes\left(c\,|\psi_2\rangle\right), \tag{1.57}$$

2. $\forall\,|\psi_1\rangle, |\varphi_1\rangle\in\mathcal{H}_1, \forall\,|\psi_2\rangle\in\mathcal{H}_2$:

$$\left(|\psi_1\rangle+|\varphi_1\rangle\right)\otimes|\psi_2\rangle = |\psi_1\rangle\otimes|\psi_2\rangle + |\varphi_1\rangle\otimes|\psi_2\rangle, \tag{1.58}$$

and vice versa: $\forall\,|\psi_1\rangle\in\mathcal{H}_1, \forall\,|\psi_2\rangle, |\varphi_2\rangle\in\mathcal{H}_2$:

$$|\psi_1\rangle\otimes\left(|\psi_2\rangle+|\varphi_2\rangle\right) = |\psi_1\rangle\otimes|\psi_2\rangle + |\psi_1\rangle\otimes|\varphi_2\rangle, \tag{1.59}$$

3. $\forall A\in\mathcal{L}(\mathcal{H}_1), B\in\mathcal{L}(\mathcal{H}_2), |\psi_1\rangle\in\mathcal{H}_1, |\psi_2\rangle\in\mathcal{H}_2$:

$$\left(A\otimes B\right)\left(|\psi_1\rangle\otimes|\psi_2\rangle\right) = A\,|\psi_1\rangle\otimes B\,|\psi_2\rangle. \tag{1.60}$$

Suppose A is an $m\times n$ matrix and B a $p\times q$ matrix. The *left Kronecker product*

of A with B is the $mp \times nq$ matrix

$$A \otimes B = \begin{pmatrix} A_{11}B_{11} & \cdots & A_{11}B_{1q} & \cdots & \cdots & A_{1n}B_{11} & \cdots & A_{1n}B_{1q} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ A_{11}B_{p1} & \cdots & A_{11}B_{pq} & \cdots & \cdots & A_{1n}B_{p1} & \cdots & A_{1n}B_{pq} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ A_{m1}B_{11} & \cdots & A_{m1}B_{1q} & \cdots & \cdots & A_{mn}B_{11} & \cdots & A_{mn}B_{1q} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ A_{m1}B_{p1} & \cdots & A_{m1}B_{pq} & \cdots & \cdots & A_{mn}B_{p1} & \cdots & A_{mn}B_{pq} \end{pmatrix}, \tag{1.61}$$

or more compactly – in block form,

$$A \otimes B = \begin{pmatrix} A_{11}[B] & A_{12}[B] & \cdots & A_{1n}[B] \\ A_{21}[B] & A_{22}[B] & \cdots & A_{2n}[B] \\ \vdots & \vdots & \vdots & \vdots \\ A_{1m}[B] & A_{m2}[B] & \cdots & A_{mn}[B] \end{pmatrix}, \tag{1.62}$$

where [B] represents the $p \times q$ submatrix B. The is illustrated by the following examples:

a) $I \otimes Z = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} Z & 0 \\ 0 & Z \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix},$

b) $Z \otimes I = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} I & 0 \\ 0 & -I \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix},$

c) $X \otimes X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & X \\ X & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix},$

d) $Y \otimes Z = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & -iZ \\ iZ & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & -i & 0 \\ 0 & 0 & 0 & i \\ i & 0 & 0 & 0 \\ 0 & -i & 0 & 0 \end{pmatrix},$

e) $|\psi\rangle \otimes |\varphi\rangle = \begin{pmatrix} \psi_1 \\ \psi_2 \end{pmatrix} \otimes \begin{pmatrix} \varphi_1 \\ \varphi_2 \end{pmatrix} = \begin{pmatrix} \psi_1 |\varphi\rangle \\ \psi_2 |\varphi\rangle \end{pmatrix} = \begin{pmatrix} \psi_1\varphi_1 \\ \psi_1\varphi_2 \\ \psi_2\varphi_1 \\ \psi_2\varphi_2 \end{pmatrix},$

$$\text{f)}\ \ |0\rangle \otimes |0\rangle \otimes |1\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\\0\\0\end{pmatrix} = \begin{pmatrix}1\\0\\0\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\1\\0\\0\\0\\0\\0\\0\end{pmatrix}.$$

Notice that we often leave the $\otimes$ symbol out of expressions. Thus $|\psi\rangle \otimes |\varphi\rangle$ is often conveniently written as $|\psi\rangle\,|\varphi\rangle$ or even $|\psi\varphi\rangle$.

Composite systems

When two physical systems with corresponding state spaces $\mathcal{H}_1$ and $\mathcal{H}_2$ are treated as one combined physical system, the state space of the combined system is the tensor product space $\mathcal{H}_1 \otimes \mathcal{H}_2$. If $|\psi_1\rangle$ is state of the first system and the second system is in the state $|\psi_2\rangle$, then the state of the combined system is

$$|\psi_1\rangle \otimes |\psi_2\rangle\,. \tag{1.63}$$

For example, having two qubits, first in the state $|0\rangle$ and second in the state $|1\rangle$, the state of the 2-qubit system is $|01\rangle$. Any state of a two-qubit system can be writen in the computational basis for two-qubit systems $\{|00\rangle\,, |01\rangle\,, |10\rangle\,, |11\rangle\}$ as

$$|\psi\rangle = a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle\,, \tag{1.64}$$

where the amplitudes a, b, c, d satisfy the normalization condition $|a|^2+|b|^2+|c|^2+|d|^2 = 1$. As the objects of our interest in this thesis are qubits – 2-level systems – all systems we use are of dimension 2^N where N is number of qubits in the system.

We should mention that not all states of 2-qubit composite systems can be written in the tensor product form $|\psi_1\rangle \otimes |\psi_2\rangle$. We can look at an example

$$|\varphi\rangle = \frac{1}{\sqrt{2}}\,|00\rangle + \frac{1}{\sqrt{2}}\,|11\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\0\end{pmatrix} + \frac{1}{\sqrt{2}}\begin{pmatrix}0\\0\\0\\1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix}. \tag{1.65}$$

$|\varphi\rangle$ is a 2-qubit composite system, thus we would like to write it as a tensor product of two 1-qubit states $|\alpha\rangle$ and $|\beta\rangle$:

$$|\alpha\rangle \otimes |\beta\rangle = \begin{pmatrix}\alpha_1\\\alpha_2\end{pmatrix} \otimes \begin{pmatrix}\beta_1\\\beta_2\end{pmatrix} = \begin{pmatrix}\alpha_1\beta_1\\\alpha_1\beta_2\\\alpha_2\beta_1\\\alpha_2\beta_2\end{pmatrix}. \tag{1.66}$$

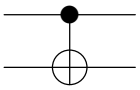
We are looking for complex constants α_1, α_2, β_1 and β_2 satisfying $\alpha_1\beta_1 = 1$, $\alpha_1\beta_2 = 0$, $\alpha_2\beta_1 = 0$, $\alpha_2\beta_2 = 1$. The condition $\alpha_1\beta_2 = 0$ tells us that $\alpha_1 = 0$ or $\beta_2 = 0$. However, it would mean that $\alpha_1\beta_1 = 0$ or $\alpha_2\beta_2 = 0$ what cannot happen in this case. This implies that we really can not write the state $|\varphi\rangle$ as a tensor product of two independent states of a qubit. Two qubits being in such state are said to be *entangled*. One of the most important implications of this phenomenom is that measurement taken on any one of the two qubits are correlated with the measurements of the second qubit as well. To illustrate this, imagine two qubits in the state $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$. If we have decided to measure state of the second qubit in the computational basis $\{|0\rangle, |1\rangle\}$ and the measurement outcome was $|0\rangle$ then we can be sure that the state of the first qubit is $|0\rangle$ and if the measurement outcome was $|1\rangle$, the first qubit would be in the pure state $|1\rangle$, too. In section 1.2.4, we will discuss this remarkable phenomenon in more detail.

1.2.2 Controlled-U Gates

We have already mentioned several 1-qubit gates. However, to build many-qubit unitary gates, we also need gates acting on two (or more) qubits. The most important one is the controlled-NOT (CNOT) gate which behaves as follows:

$$|00\rangle \to |00\rangle, \quad |01\rangle \to |01\rangle, \quad |10\rangle \to |11\rangle, \quad |11\rangle \to |10\rangle. \tag{1.67}$$

Thus, whenever the state of the first (control) qubit is $|1\rangle$, it flips the state of the second (target) qubit. The circuit model representation is



and the matrix form of the CNOT gate is

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{1.68}$$

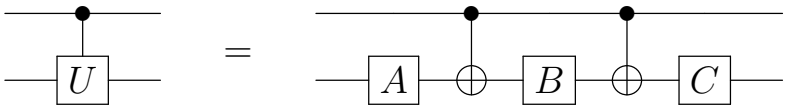
In general, a controlled-U (c-U) gate acts as follows:

$$\begin{aligned} \text{c-}U\,|0\rangle\,|\psi\rangle &= |0\rangle\,|\psi\rangle, \\ \text{c-}U\,|1\rangle\,|\psi\rangle &= |0\rangle\,U\,|\psi\rangle. \end{aligned} \tag{1.69}$$

The operator form of a controlled-U gate is given by

$$|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U. \tag{1.70}$$

Any controlled-U gate can be replaced with a circuit made out of single-qubit gates and the CNOT gate in the following way:



where A, B, C are unitary operators meeting conditions $ABC = I$ and $AXBXC = U$. The proof goes through the statement (1.37) using the z- and x-axes so

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta). \tag{1.71}$$

We can take $A = R_z(\beta)R_y(\frac{\gamma}{2})$, $B = R_y(-\frac{\gamma}{2})R_z(-\frac{\delta+\beta}{2})$ and $C = R_z(\frac{\delta-\beta}{2})$ which satisfy the condition $ABC = I$ as when acting with ABC all rotations will be in the final result cancelled. Since $XR_y(\alpha)R_z(\beta)X = R_y(-\alpha)R_z(-\beta)$ what we can see by explicit computation

$$\begin{aligned} XR_y(\alpha)R_z(\beta)X &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \cos\left(\frac{\alpha}{2}\right) & -\sin\left(\frac{\alpha}{2}\right) \\ \sin\left(\frac{\alpha}{2}\right) & \cos\left(\frac{\alpha}{2}\right) \end{pmatrix} \begin{pmatrix} e^{-i\frac{\beta}{2}} & 0 \\ 0 & e^{i\frac{\beta}{2}} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \\ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} e^{-i\frac{\beta}{2}}\cos\left(\frac{\alpha}{2}\right) & -e^{i\frac{\beta}{2}}\sin\left(\frac{\alpha}{2}\right) \\ e^{-i\frac{\beta}{2}}\sin\left(\frac{\alpha}{2}\right) & e^{i\frac{\beta}{2}}\cos\left(\frac{\alpha}{2}\right) \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} &= \begin{pmatrix} e^{i\frac{\beta}{2}}\cos\left(\frac{\alpha}{2}\right) & e^{-i\frac{\beta}{2}}\sin\left(\frac{\alpha}{2}\right) \\ -e^{i\frac{\beta}{2}}\sin\left(\frac{\alpha}{2}\right) & e^{-i\frac{\beta}{2}}\cos\left(\frac{\alpha}{2}\right) \end{pmatrix} = \\ = \begin{pmatrix} \cos\left(\frac{(-\alpha)}{2}\right) & -\sin\left(\frac{(-\alpha)}{2}\right) \\ \sin\left(\frac{(-\alpha)}{2}\right) & \cos\left(\frac{(-\alpha)}{2}\right) \end{pmatrix} \begin{pmatrix} e^{-i\frac{(-\beta)}{2}} & 0 \\ 0 & e^{i\frac{(-\beta)}{2}} \end{pmatrix} &= R_y(-\alpha)R_z(-\beta). \end{aligned} \tag{1.72}$$

Hence

$$\begin{aligned} AXBXC &= R_z(\beta)R_y(\frac{\gamma}{2})XR_y(-\frac{\gamma}{2})R_z(-\frac{\delta+\beta}{2})XR_z(\frac{\delta-\beta}{2}) = \\ &= R_z(\beta)R_y(\frac{\gamma}{2})R_y(\frac{\gamma}{2})R_z(\frac{\delta+\beta}{2})R_z(\frac{\delta-\beta}{2}) = R_z(\beta)R_y(\gamma)R_z\delta = U. \end{aligned} \tag{1.73}$$

1.2.3 Partial Trace

Consider a two-qubit composite system described by a pure state $|\psi\rangle_{\mathrm{AB}} \in \mathcal{H}_{\mathrm{A}} \otimes \mathcal{H}_{\mathrm{B}}$. There are situations when the knowledge of the state of a subsystem would be really essential. However, as we have already mentioned, we may not always be able to trace out a state vector $|\psi\rangle_{\mathrm{A}}$ characterizing the subsystem we are interested in since not every state of a composite system is a tensor product of pure states. Despite that we can use a mixed state and therefore a density operator ρ_{A} which would provide us complete description of the subsystem. The *reduced density operator* ρ_{A} can be gained from the already known ρ_{AB} (since $\rho_{\mathrm{AB}} = |\psi\rangle_{\mathrm{AB}} \langle\psi|_{\mathrm{AB}} = \rho_{\mathrm{A}} \otimes \rho_{\mathrm{B}} = |a_1\rangle \langle a_2| \otimes |b_1\rangle \langle b_2|$ where the

last step follows from the possibility of writing any matrix as an outer product of two vectors) by computing *partial trace* over the system B:

$$\rho_{\mathrm{A}} = \mathrm{Tr}_{\mathrm{B}}\left(\rho_{\mathrm{AB}}\right) = \mathrm{Tr}_{\mathrm{B}}\left(|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|\right) = |a_1\rangle\langle a_2|\,\mathrm{Tr}\left(|b_1\rangle\langle b_2|\right). \tag{1.74}$$

Because

$$\mathrm{Tr}\left(|b_1\rangle\langle b_2|\right) = \mathrm{Tr}\left(\langle b_2|b_1\rangle\right) = \langle b_2|b_1\rangle\,, \tag{1.75}$$

equation (1.74) can be simplified to

$$\rho_{\mathrm{A}} = |a_1\rangle\langle a_2|\,\langle b_2|b_1\rangle\,. \tag{1.76}$$

The best understanding comes from examples so here is one. We are going to find out the state of the first qubit by tracing out the second qubit of the entangled state

$$\frac{1}{\sqrt{2}}\big(|01\rangle + |10\rangle\big). \tag{1.77}$$

The density matrix for this state is

$$\rho = \frac{1}{2}\big(|01\rangle + |10\rangle\big)\big(\langle 01| + \langle 10|\big) = \frac{1}{2}\big(|01\rangle\langle 01| + |01\rangle\langle 10| + |10\rangle\langle 01| + |10\rangle\langle 10|\big). \tag{1.78}$$

The reduced density operator for the first qubit ρ_1 we are looking for can be easily computed as

$$\begin{aligned}
\rho_1 &= \mathrm{Tr}_2\big(\rho\big) = \frac{1}{2}\mathrm{Tr}_2\big(|01\rangle\langle 01| + |01\rangle\langle 10| + |10\rangle\langle 01| + |10\rangle\langle 10|\big) \\
&= \frac{1}{2}\mathrm{Tr}_2\big(|0\rangle\langle 0| \otimes |1\rangle\langle 1| + |0\rangle\langle 1| \otimes |1\rangle\langle 0| + |1\rangle\langle 0| \otimes |0\rangle\langle 1| + |1\rangle\langle 1| \otimes |0\rangle\langle 0|\big) \\
&= \frac{1}{2}\Big(|0\rangle\langle 0|\,\mathrm{Tr}\big(|1\rangle\langle 1|\big) + |0\rangle\langle 1|\,\mathrm{Tr}\big(|1\rangle\langle 0|\big) + |1\rangle\langle 0|\,\mathrm{Tr}\big(|0\rangle\langle 1|\big) + |1\rangle\langle 1|\,\mathrm{Tr}\big(|0\rangle\langle 0|\big)\Big) \\
&= \frac{1}{2}\big(|0\rangle\langle 0|\langle 1|1\rangle + |0\rangle\langle 1|\langle 0|1\rangle + |1\rangle\langle 0|\langle 1|0\rangle + |1\rangle\langle 1|\langle 0|0\rangle\big) \\
&= \frac{1}{2}\big(|0\rangle\langle 0| + |1\rangle\langle 1|\big) = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.
\end{aligned} \tag{1.79}$$

Quantum channels

Quantum channels (or *superoperators*) are the most general transforms of a quantum state, resulting from any kind of interaction with a quantum environment, that are physically reasonable. When we allow our system to interact with an external system, it is often more appropriate to use mixed states and therefore density operators to desribe the state of our system. So the superoperator takes as input a system described by density operator ρ_{in}, adds an ancilla (or environment) of arbitrary size described by

a density operator ρ_{E} (usually $\rho_{\mathrm{E}} = |00\ldots00\rangle\langle00\ldots0|$), performs a unitary operation U on the joint system and then discards some subsystem.

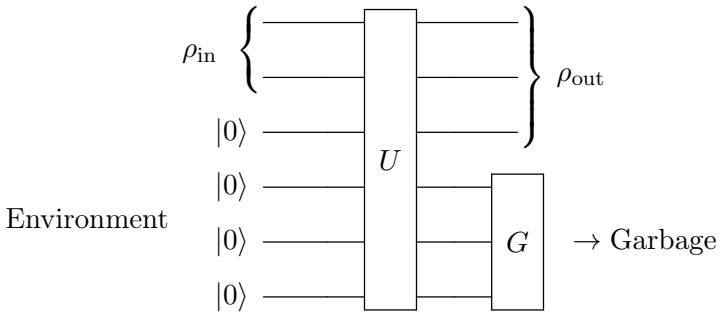


Figure 1.6: A general quantum operation can be realized by adding some ancilla qubits, acting on the system and the environment with a unitary operation and then tracing out part of the output.

The action of a superoperator can be described by a map

$$\rho_{\mathrm{in}} \mapsto \rho_{\mathrm{out}} = \mathrm{Tr}_{\mathrm{G}}\left(U(\rho_{\mathrm{in}} \otimes \rho_{\mathrm{E}})U^{\dagger}\right) \tag{1.80}$$

where G is some subsystem of the joint system. We can also rewrite the action as

$$\begin{aligned}
\rho_{\mathrm{in}} \mapsto \rho_{\mathrm{out}} &= \mathrm{Tr}_{\mathrm{G}}\big(U\left(\rho_{\mathrm{in}} \otimes (|00\ldots0\rangle\langle00\ldots0|)_{\mathrm{E}}\right)U^{\dagger}\big) = \\
&= \mathrm{Tr}_{\mathrm{G}}\big[U\big(\rho_{\mathrm{in}} \otimes (|0\ldots0\rangle\langle0\ldots0|)_{\mathrm{A}} \otimes (|0\ldots0\rangle\langle0\ldots0|)_{\mathrm{G}}\big)U^{\dagger}\big] = \\
&= \sum_k \langle k|\, U\big(\rho_{\mathrm{in}} \otimes (|0\ldots0\rangle\langle0\ldots0|)_{\mathrm{A}} \otimes (|0\ldots0\rangle\langle0\ldots0|)_{\mathrm{G}}\big)U^{\dagger}\,|k\rangle = \\
&= \sum_k \langle k|\, U(|0\ldots0\rangle)_{\mathrm{G}}\left[\rho_{\mathrm{in}} \otimes (|0\ldots0\rangle\langle0\ldots0|)_{\mathrm{A}}\right](\langle0\ldots0|)_{\mathrm{G}}U^{\dagger}\,|k\rangle = \\
&= \sum_k M_k\left[\rho_{\mathrm{in}} \otimes (|0\ldots0\rangle\langle0\ldots0|)_{\mathrm{A}}\right]M_k^{\dagger} = \sum_k K_k\rho_{\mathrm{in}}K_k^{\dagger}
\end{aligned} \tag{1.81}$$

where A and G are subsystems of the environment ($\mathcal{H}_{\mathrm{A}} \otimes \mathcal{H}_{\mathrm{G}} = \mathcal{H}_{\mathrm{E}}$), $\{|b\rangle\}$ is an orthonormal basis of G – the subsystem we are tracing over and K_k linear operators called *Kraus operators* satisfying

$$\sum_k K_k^{\dagger}K_k = I. \tag{1.82}$$

In general, a superoperator is a completely positive trace-preserving linear map between spaces of operators $M : \mathcal{L}(\mathcal{H}_{\mathrm{O}}) \rightarrow \mathcal{L}(\mathcal{H}_{\mathrm{P}})$ where $\dim \mathcal{H}_{\mathrm{O}}$ is not necessarily equal to $\dim \mathcal{H}_{\mathrm{P}}$.

1.2.4 Entangled States

We now analyze the 2-qubit entangled state $\frac{1}{\sqrt{2}}\big(|01\rangle - |10\rangle\big)$ in more detail. First, we should mention that this state is invariant under rotations (= if we would measure the

qubits in whichever basis, if both were measured in the same basis, the results would be always anticorrelated). That means

$$\frac{1}{\sqrt{2}}\big(|01\rangle - |10\rangle\big) = \frac{1}{\sqrt{2}}e^{i\varphi}\big(\big|aa^{\perp}\big\rangle - \big|aa^{\perp}\big\rangle\big). \tag{1.83}$$

To prove it, we simply rewrite the state $\frac{1}{\sqrt{2}}\big(\big|aa^{\perp}\big\rangle - \big|aa^{\perp}\big\rangle\big)$ into the computational basis:

$$\begin{aligned}
&\frac{1}{\sqrt{2}}\left[\begin{pmatrix}a_0\\a_1\end{pmatrix}\otimes\begin{pmatrix}a_0^{\perp}\\a_1^{\perp}\end{pmatrix} - \begin{pmatrix}a_0^{\perp}\\a_1^{\perp}\end{pmatrix}\otimes\begin{pmatrix}a_0\\a_1\end{pmatrix}\right] = \\
&= \frac{1}{\sqrt{2}}\left[(a_0|0\rangle + a_1|1\rangle)\otimes(a_0^{\perp}|0\rangle + a_1^{\perp}|1\rangle) - (a_0^{\perp}|0\rangle + a_1^{\perp}|1\rangle)\otimes(a_0|0\rangle + a_1|1\rangle)\right] = \\
&= \frac{1}{\sqrt{2}}\left[a_0a_0^{\perp}|00\rangle + a_0a_1^{\perp}|01\rangle + a_1a_0^{\perp}|10\rangle + a_1a_1^{\perp}|11\rangle - a_0^{\perp}a_0|00\rangle - a_0^{\perp}a_1|01\rangle - \right. \\
&\left. - a_1^{\perp}a_0|10\rangle - a_1^{\perp}a_1|11\rangle\right] = \frac{1}{\sqrt{2}}\left[(a_0a_0^{\perp} - a_0^{\perp}a_0)|00\rangle + (a_0a_1^{\perp} - a_0^{\perp}a_1)|01\rangle + \right. \\
&\left. + (a_1a_0^{\perp} - a_1^{\perp}a_0)|10\rangle + (a_1a_1^{\perp} - a_1^{\perp}a_1)|11\rangle\right] = \frac{1}{\sqrt{2}}\big(a_0a_1^{\perp} - a_0^{\perp}a_1\big)\big(|01\rangle - |10\rangle\big) = \\
&\qquad\qquad \frac{1}{\sqrt{2}}e^{i\phi}\big(|01\rangle - |10\rangle\big),
\end{aligned} \tag{1.84}$$

where the last step comes from the fact that

$$\begin{aligned}
&\big|a_0a_1^{\perp} - a_0^{\perp}a_1\big|^2 = (a_0a_1^{\perp} - a_0^{\perp}a_1)((a_0a_1^{\perp})^* - (a_0^{\perp}a_1)^*) = \\
&a_0a_1^{\perp}a_0^*a_1^{\perp *} - a_0a_1^{\perp}a_0^{\perp *}a_1^* - a_0^{\perp}a_1a_0^*a_1^{\perp *} + a_0^{\perp}a_1a_0^{\perp *}a_1^* \xrightarrow{a_0a_0^*+a_1a_1^*=1} \\
&a_1^{\perp}a_1^{\perp *} - a_1a_1^{\perp}a_1^*a_1^{\perp *} - a_0a_1^{\perp}a_0^{\perp *}a_1^* - a_0^{\perp}a_1a_0^*a_1^{\perp *} + a_0^{\perp}a_0^{\perp *} - a_0^{\perp}a_0a_0^{\perp *}a_0^* \xrightarrow[a_0a_0^{\perp *}+a_1a_1^{\perp *}=0]{a_0^{\perp}a_0^{\perp *}+a_1^{\perp}a_1^{\perp *}=1} \\
&1 - a_1a_1^{\perp}a_1^*a_1^{\perp *} + a_1a_1^{\perp}a_1^{\perp *}a_1^* + a_0^{\perp}a_0a_0^*a_0^{\perp *} - a_0^{\perp}a_0a_0^{\perp *}a_0^* = 1.
\end{aligned} \tag{1.85}$$

Now, imagine Alice, owner of the first qubit, decided to measure the state of her qubit and suppose that the measurement outcome was x. If Bob who is in possesion of the second qubit, takes the measurement in the same basis, he must measure $\neg x$ (not x). One must admit that these correlations are really extraordinary.

The existence of such correlations was first noticed by Schrödinger in 1935 [11]. In the same year, Einstein, Podolsky and Rosen [5] described a paradox (EPR paradox) where they discussed that the quantum-mechanical description of the world can not be considered complete. They claimed that the impossibility to measure non-commuting observables simultaneously implies that either the quantum-mechanical description of the world can not be considered complete or the non-commuting observables cannot have simultaneous reality. However, if they would measure these properties on a pair of entangled particles – e.g. the position of the first one and the momentum of the other – there is a possibility to know both these observables simultaneously. It is

analogous to measuring a qubit in the computational basis $\{|0\rangle, |1\rangle\}$ or in the basis $\{|+\rangle, |-\rangle\}$. Whichever basis we choose and measure, we never find out what would be the measurement outcome in the second basis. However, if we use the entangled pair $\frac{1}{\sqrt{2}}\big(|01\rangle - |10\rangle\big)$, we can measure the first qubit in the Z basis and the second qubit in the X basis and as the measurement outcomes are always anticorrelated, we know the measurement outcome of the measurement we did not do on the other qubit, in both bases. Therefore the observables look like they have simultaneous reality and thus the theory cannot be complete.

Some physicists believed that the gap could be solved by adding *hidden variables*. A class of these theories, *local hidden variables theories*, claimed that the measurement outcomes are always deterministic and any action on the first qubit cannot modify state of the second qubit. The measurements appear to be probabilistic because there are some degrees of freedom which are not precisely known. However, thanks to Bell [2], we know that local hidden variable theories can be ruled out by an experiment violating *Bell inequalities*. Indeed a series of experiments from Aspect [1] and Zeilinger [12] did exactly this.

Now, let us return to the consideration that if Alice and Bob would measure their qubits in the same basis, their measurement outcomes would be fully anticorrelated. One could ask a question: *Isn't there a possibility to use this phenomenon to create a protocol for faster-than-light communication*? Recall that if we would trace out one of these two qubits, we would find out that the state of the remaining qubit corresponds to the maximally mixed denstity operator $\rho = \frac{I}{2}$. That means for Alice and Bob alone, whenever they do some measurement, the outcome is fully random. If they did not communicate classicaly about their results, they have no idea what their measurement outcomes will be and there is no way to affect them. So the answer to the superluminal communication possibility is: *no*. We can not do it, but we can read about the failed attempts in [7]. However, there is a way how to make entangled pairs useful: use them for secure communication (= how to be sure no-one else can decipher a message adressed to the person with whom we communicate[5]).

One of the possible ways is the following [3]. Alice and Bob want to share a secret key which they could use for encrypted communication. In order to do that, they first share many entangled pairs. Both measure each of his/her qubits in a random basis (either X or Z). Then they publish which basis they used for which measurement (they do not publish the measurement results!). Whenever the bases match, the results must be anticorrelated, but random – so they can form a secret key which Alice adds to her message (in order to keep the message indecipherable for other people, except the owners of the key, she must use the key just once!) to encrypt it and Bob adds to

[5]Do not understand this condition as it can assure you that you really speak with the right person. It does not solve the problem with autentification.

the cipher text to decipher and read it. However, this would not be safe yet. What if there was someone "listening" (= someone who measured their qubits before Alice and Bob did)? Then the results could not remain anticorrelated and Alice and Bob can detect this. Note, that errors could be also caused by noise. Thus Alice and Bob cleverly choose a good statistical sample of the cases where their bases have matched. Subsequently, they inform each other what measurement outcomes they found in this cases. They look whether the results are anticorrelated. If just a small part of the measurement outcomes does not match the pattern, they decide whether they tolerate it as noise or whether they throw it away because someone was "listening" (for example they could have calculated that they have 5% noise tolerance and still are secure). If they consider it safe, they choose the part of the matched cases where they have not revealed and use the measurement results as the key.

1.2.5 Bell Basis

In the study of quantum computation, besides the computational basis, another common orthonormal basis for the Hilbert space of a 2-qubit system is composed of four maximally entangled states

$$\begin{aligned} |\beta_{00}\rangle &= \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle, & |\beta_{01}\rangle &= \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle, \\ |\beta_{10}\rangle &= \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle, & |\beta_{11}\rangle &= \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle, \end{aligned} \tag{1.86}$$

called *Bell states*.

As the suffixes indicate, there is a simple way to implement the basis changing operation from the computational to the Bell basis and vice versa. Concretely, we can do that by circuit made out of 2 gates: Hadamard and controlled-not (CNOT) as follows.

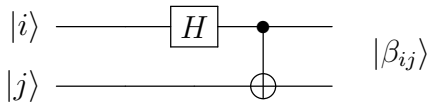


Figure 1.7: A circuit implementing creating entangled pairs (from left to right) and measuring into Bell basis (from right to left).

We should emphasize that we can create an entangled pair or find out which entangled pair we have using the scheme depicted in the Figure 1.7. However, both of these operations depend on interaction of the two qubits (CNOT gate). If the two qubits were separated, one would be in possesion of Alice and second in Bob's, neither of them cannot acquire this information (= by measuring only their qubit). But in spite

of that there is something they can do. They can locally manipulate this information (the state they together own). If Bob would apply the X-gate to his qubit he can change the entangled state in the following manner

$$\begin{aligned} |\beta_{00}\rangle &\overset{\mathrm{I}\otimes\mathrm{X}}{\longleftrightarrow} |\beta_{01}\rangle\,, \\ |\beta_{10}\rangle &\overset{\mathrm{I}\otimes\mathrm{X}}{\longleftrightarrow} |\beta_{11}\rangle \end{aligned} \tag{1.87}$$

and by applying the Z-gate

$$\begin{aligned} |\beta_{00}\rangle &\overset{\mathrm{I}\otimes\mathrm{Z}}{\longleftrightarrow} |\beta_{10}\rangle\,, \\ |\beta_{01}\rangle &\overset{\mathrm{I}\otimes\mathrm{Z}}{\longleftrightarrow} -|\beta_{11}\rangle\,. \end{aligned} \tag{1.88}$$

Of course, Alice can do practically the same as

$$\begin{aligned} |\beta_{00}\rangle &\overset{\mathrm{X}\otimes\mathrm{I}}{\longleftrightarrow} |\beta_{01}\rangle\,, & |\beta_{00}\rangle &\overset{\mathrm{Z}\otimes\mathrm{I}}{\longleftrightarrow} |\beta_{10}\rangle\,, \\ |\beta_{10}\rangle &\overset{\mathrm{X}\otimes\mathrm{I}}{\longleftrightarrow} -|\beta_{11}\rangle\,, & |\beta_{01}\rangle &\overset{\mathrm{Z}\otimes\mathrm{I}}{\longleftrightarrow} |\beta_{11}\rangle\,. \end{aligned} \tag{1.89}$$

1.3 No-cloning theorem

Before Zurek and Wooters published their *no-cloning theorem* [13], there were a lot of protocols which proposed superluminal communication. One of the most famous was Herbert's FLASH protocol [6] based on entangled pairs of photons. However, all of these protocols depended on copying a quantum state, the no-cloning theorem ruled them out. The theorem is based on a simple principle – the linearity of quantum mechanics. It states that if we had a box, which perfectly copies 2 orthonormal states $|\alpha\rangle \to |\alpha\rangle\,|\alpha\rangle$ and $|\beta\rangle \to |\beta\rangle\,|\beta\rangle$, if we would apply it to a state in superposition of the two states, $a\,|\alpha\rangle + b\,|\beta\rangle$, because of the linearity of quantum mechanics, the "copied" state would be $a\,|\alpha\rangle\,|\alpha\rangle + b\,|\beta\rangle\,|\beta\rangle$. This is different from the real copy $(a\,|\alpha\rangle + b\,|\beta\rangle) \otimes (a\,|\alpha\rangle + b\,|\beta\rangle)$. Therefore we cannot copy a general quantum state = there cannot exist a copier which would be able to copy two non-orthogonal states. Thus, all protocols based on cloning are unphysical.

No-signaling condition

Even though there are non-local influences in the quantum-mechanical world, there is no way how to use them for instant signaling or communication with anyone. The no-signaling condition says, that there cannot exist a box

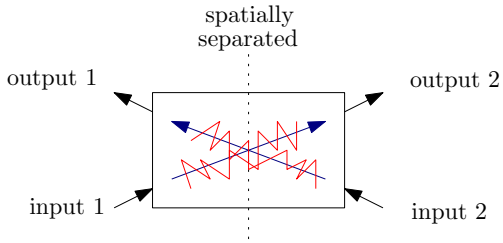


Figure 1.8: There cannot exist a box (operation), which would enable dependency of an input on a spatially separated output.

where output 2 would depend on input 1 (or output 1 would depend on input 2).

Chapter 2

Quantum Teleportation

Suppose Alice wants to transfer an unknown quantum state $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$ to Bob. Since Alice has just a single copy and the no-cloning theorem says that she cannot duplicate it, there's no way to precisely determine the amplitudes a and b through measurement (if they are general and not a special case, e.g. $a = 0$ or $b = 0$). It would seem that Alice has to send the physical qubit itself. However, if Alice and Bob possess a pre-shared entangled state, they can communicate the unknown state $|\psi\rangle$ using a quantum teleportation protocol which involves sending only classical bits of information.

In 1993 Bennet et al.[4] came up with quantum teleportation protocol which enables Alice to send the state of her qubit to Bob by performing a Bell measurement on her qubits – the qubit of the unknown state $|\psi\rangle$ she wishes to communicate and her member of an entangled pair, for example $|\beta_{01}\rangle = \frac{1}{\sqrt{2}}\,|01\rangle + \frac{1}{\sqrt{2}}\,|10\rangle$, which she shares with Bob. Then thanks to communication of the measurement outcomes over a classical channel Bob learns what to do to recover $|\psi\rangle$.

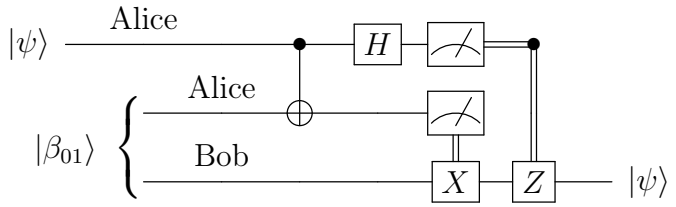


Figure 2.1: A circuit implementing quantum teleportation with an entangled pair $|\beta_{01}\rangle$.

The scenario goes like this. Alice and Bob start with a 3-qubit state

$$|\psi\rangle\,|\beta_{00}\rangle = (a\,|0\rangle + b\,|1\rangle)_{\mathrm{A}} \otimes \left(\frac{1}{\sqrt{2}}\,|01\rangle + \frac{1}{\sqrt{2}}\,|10\rangle\right)_{\mathrm{AB}} =$$
$$= \frac{1}{\sqrt{2}}\left(a\,|001\rangle_{\mathrm{AAB}} + a\,|010\rangle_{\mathrm{AAB}} + b\,|101\rangle_{\mathrm{AAB}} + b\,|110\rangle_{\mathrm{AAB}}\right), \tag{2.1}$$

where the first two qubits are in the possesion of Alice and the last one is Bob's. Alice

measures her qubits in the Bell basis. The 3-qubit state changes into

$$\frac{1}{\sqrt{2}}\left(a\left|001\right\rangle + a\left|010\right\rangle + b\left|101\right\rangle + b\left|110\right\rangle\right) \xrightarrow{\text{CNOT}} \tag{2.2}$$

$$\xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}}\left(a\left|001\right\rangle + a\left|010\right\rangle + b\left|111\right\rangle + b\left|100\right\rangle\right) \xrightarrow{\text{H}} \tag{2.3}$$

$$\xrightarrow{\text{H}} \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}\left(a\left|001\right\rangle + a\left|101\right\rangle\right) + \frac{1}{\sqrt{2}}\left(a\left|010\right\rangle + a\left|110\right\rangle\right) + \frac{1}{\sqrt{2}}\left(b\left|011\right\rangle - b\left|111\right\rangle\right) + \right.$$
$$\left. + \frac{1}{\sqrt{2}}\left(b\left|000\right\rangle - b\left|100\right\rangle\right)\right) = \frac{1}{2}\left(\left|00\right\rangle_{\text{A}}\left(a\left|1\right\rangle + b\left|0\right\rangle\right)_{\text{B}} + \left|01\right\rangle_{\text{A}}\left(a\left|0\right\rangle + b\left|1\right\rangle\right)_{\text{B}} + \right.$$
$$\left. + \left|10\right\rangle_{\text{A}}\left(a\left|1\right\rangle - b\left|0\right\rangle\right)_{\text{B}} + \left|11\right\rangle_{\text{A}}\left(a\left|0\right\rangle - b\left|1\right\rangle\right)_{\text{B}}\right). \tag{2.4}$$

A convenient rewriting shows that Alice's measurement outcomes determine the collapsed state of Bob's qubit.

state of Alice's qubits	state of Bob's qubit		probability
$\left\|00\right\rangle$	$a\left\|1\right\rangle + b\left\|0\right\rangle$	$\text{X}\left\|\psi\right\rangle$	1/4
$\left\|01\right\rangle$	$a\left\|0\right\rangle + b\left\|1\right\rangle$	$\left\|\psi\right\rangle$	1/4
$\left\|10\right\rangle$	$a\left\|1\right\rangle - b\left\|0\right\rangle$	$\text{XZ}\left\|\psi\right\rangle$	1/4
$\left\|11\right\rangle$	$a\left\|0\right\rangle - b\left\|1\right\rangle$	$\text{Z}\left\|\psi\right\rangle$	1/4

Table 2.1: The dependency of the state of Bob's qubit on Alice's Bell measurement outcomes.

Via a classical channel, Alice informs Bob about what she measured. This information is all what Bob needs to reconstruct the unknown state by applying a simple correction:

$$\left|\psi\right\rangle \xrightarrow{\text{I}} \left|\psi\right\rangle \tag{2.5}$$

$$\text{X}\left|\psi\right\rangle \xrightarrow{\text{X}} \left|\psi\right\rangle \tag{2.6}$$

$$\text{Z}\left|\psi\right\rangle \xrightarrow{\text{Z}} \left|\psi\right\rangle \tag{2.7}$$

$$\text{XZ}\left|\psi\right\rangle \xrightarrow{\text{ZX}} \left|\psi\right\rangle \tag{2.8}$$

This is a nice example showing the unusual properties of entangled pairs. Alice and Bob could share some entangled pair long before the need to transfer the quantum state. Then, when the need for this operation comes, Alice performs a few operations on her qubits. Then she sends 2 classical bits of information via a classical communication channel. After the required correction, Bob is in possession of the desired quantum state. Surprisingly, Alice and Bob do not learn what the unknown state $\left|\psi\right\rangle$ is.

We should emphasize that since Alice and Bob have shared the entangled pair, the only communication that happened was classical, whose only purpose was to communicate Alice's measurement outcome. There exists no way how the qubits could tell

each other what they have experienced since they were at the beginning separated. Let us take a look at the state of Bob's qubit at 3 time points.

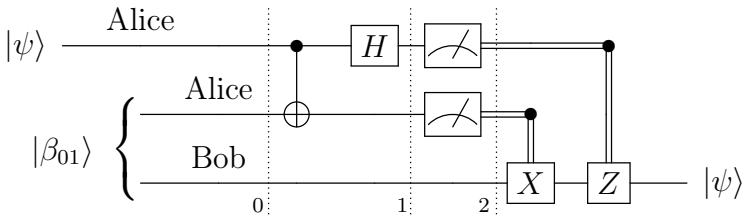


Figure 2.2: Quantum teleportation with an entangled pair $|\beta_{01}\rangle$. The dashes lines represent distinctive time points we are interested in.

At the beginning (time point 0), Bob's qubit is in the entangled state $|\beta_{01}\rangle$ with the second one and the first qubit, communicated one, is independent. The state of Bob's qubit at this point can be expressed by a density matrix $\rho_0 = \frac{1}{2}I$ as a half of an entangled pair locally looks like a maximally mixed state. At time point 1 (after Alice's qubits went through the gates), Bob's qubit is a part of a 3-qubit pure state

$$\begin{aligned}&\frac{1}{2}\left(|00\rangle_{\mathrm{A}}\left(a\,|1\rangle + b\,|0\rangle\right)_{\mathrm{B}} + |01\rangle_{\mathrm{A}}\left(a\,|0\rangle + b\,|1\rangle\right)_{\mathrm{B}} + \right.\\ &\left. + |10\rangle_{\mathrm{A}}\left(a\,|1\rangle - b\,|0\rangle\right)_{\mathrm{B}} + |11\rangle_{\mathrm{A}}\left(a\,|0\rangle - b\,|1\rangle\right)_{\mathrm{B}}\right).\end{aligned} \tag{2.9}$$

By computing a partial trace over Alice's qubits we can express the density matrix of Bob's qubit:

$$\begin{aligned}\rho_1 = \mathrm{Tr}_{1,2}\Big[\frac{1}{2}\Big(&|00\rangle_{\mathrm{A}}\left(a\,|1\rangle + b\,|0\rangle\right)_{\mathrm{B}} + |01\rangle_{\mathrm{A}}\left(a\,|0\rangle + b\,|1\rangle\right)_{\mathrm{B}} + \\ &+ |10\rangle_{\mathrm{A}}\left(a\,|1\rangle - b\,|0\rangle\right)_{\mathrm{B}} + |11\rangle_{\mathrm{A}}\left(a\,|0\rangle - b\,|1\rangle\right)_{\mathrm{B}}\Big)\frac{1}{2}\Big(\langle 00|_{\mathrm{A}}\left(a\,\langle 1| + b\,\langle 0|\right)_{\mathrm{B}} + \\ &+ |01\rangle_{\mathrm{A}}\left(a\,\langle 0| + b\,\langle 1|\right)_{\mathrm{B}} + \langle 10|_{\mathrm{A}}\left(a\,\langle 1| - b\,\langle 0|\right)_{\mathrm{B}} + \langle 11|_{\mathrm{A}}\left(a\,\langle 0| - b\,\langle 1|\right)_{\mathrm{B}}\Big)\Big] = \\ = \frac{1}{4}\Big(&(a\,|1\rangle + b\,|0\rangle)(a\,\langle 1| + b\,\langle 0|) + (a\,|0\rangle + b\,|1\rangle)(a\,\langle 0| + b\,\langle 1|) + \\ &+ (a\,|1\rangle - b\,|0\rangle)(a\,\langle 1| - b\,\langle 0|) + (a\,|0\rangle - b\,|1\rangle)(a\,\langle 0| - b\,\langle 1|)\Big) = \\ = \frac{1}{4}\begin{pmatrix} bb^* & ba^* \\ ab^* & aa^* \end{pmatrix} + \frac{1}{4}\begin{pmatrix} aa^* & ab^* \\ ba^* & bb^* \end{pmatrix} + \frac{1}{4}\begin{pmatrix} bb^* & -ba^* \\ -ab^* & aa^* \end{pmatrix} + \frac{1}{4}\begin{pmatrix} aa^* & -ab^* \\ -ba^* & bb^* \end{pmatrix} = \\ = \frac{1}{4}\begin{pmatrix} 2(aa^* + bb^*) & 0 \\ 0 & 2(aa^* + bb^*) \end{pmatrix} = \frac{1}{4}\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.\end{aligned} \tag{2.10}$$

We can see that nothing has changed as the density matrix for this state is also $\rho_1 = \rho_0 = \frac{1}{2}I$.

Right after the measurement, the state of Bob's qubit collapses into one of the states $\{|\psi\rangle, X\,|\psi\rangle, Z\,|\psi\rangle, XZ\,|\psi\rangle\}$. However, Bob so far does not know which one (only Alice

knows it). For Bob, the state of his qubit is in the mixed state $\{(|\psi\rangle, \frac{1}{4}), (X|\psi\rangle, \frac{1}{4}), (Z|\psi\rangle, \frac{1}{4}), (XZ|\psi\rangle, \frac{1}{4})\}$ which, as we can see from an explicit computation:

$$\begin{aligned}\rho_2 &= \frac{1}{4}|\psi\rangle\langle\psi| + \frac{1}{4}(X|\psi\rangle)(\langle\psi|X) + \frac{1}{4}(Z|\psi\rangle)(\langle\psi|Z) + \frac{1}{4}(XZ|\psi\rangle)(\langle\psi|ZX) = \\ &= \frac{1}{4}\Big((a|0\rangle + b|1\rangle)(a\langle 0| + b\langle 1|) + (a|1\rangle + b|0\rangle)(a\langle 1| + b\langle 0|) + \\ &\quad (a|0\rangle - b|1\rangle)(a\langle 0| - b\langle 1|) + (a|1\rangle - b|0\rangle)(a\langle 1| - b\langle 0|)\Big) = \\ &= \frac{1}{4}\begin{pmatrix} aa^* & ab^* \\ ba^* & bb^* \end{pmatrix} + \frac{1}{4}\begin{pmatrix} bb^* & ba^* \\ ab^* & aa^* \end{pmatrix} + \frac{1}{4}\begin{pmatrix} aa^* & -ab^* \\ -ba^* & bb^* \end{pmatrix} + \frac{1}{4}\begin{pmatrix} bb^* & -ba^* \\ -ab^* & aa^* \end{pmatrix} = \\ &= \frac{1}{4}\begin{pmatrix} 2(aa^* + bb^*) & 0 \\ 0 & 2(aa^* + bb^*) \end{pmatrix} = \frac{1}{4}\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \end{aligned} \tag{2.11}$$

is still the maximally mixed state with density operator $\frac{1}{2}I$. At this point, we start to call the state into which the qubit collapses *the final state*. In fact, if Bob at any time (=before, during or after the measurement) applies any operations to his qubit, in the end, it would behave as if his state was always the final one.

At last, notice that it is in principle impossible to send a general quantum state, not even the complete information about the state, via a classical channel. Even if Alice has a lot of copies of the state, she would not be able to estimate the amplitudes with absolute precision. It was a big surprise to find out that there is a possibility to teleport a quantum state without disturbing it.

2.1 Entanglement swapping

Imagine a situation where instead of a qubit in an unknown quantum state we use a qubit which belongs to some entangled pair, for example $|\beta_{01}\rangle = \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle$.

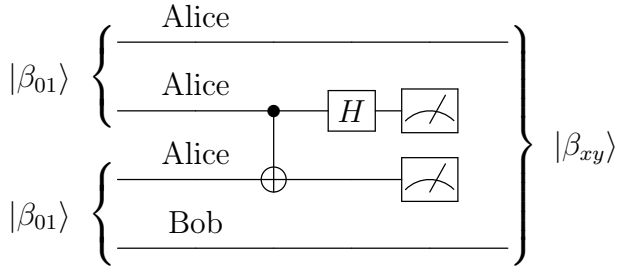


Figure 2.3: A circuit implementing entanglement swapping.

The initial state would be

$$|\beta_{01}\rangle \otimes |\beta_{01}\rangle = \frac{1}{2}|0101\rangle + \frac{1}{2}|0110\rangle + \frac{1}{2}|1001\rangle + \frac{1}{2}|1010\rangle. \tag{2.12}$$

Let us now do a measurement in the Bell basis of the 2 middle qubits. We can do this in 2 steps. First we make a transformation from the Bell to the computational basis which changes the 4-qubit state into

$$\frac{1}{2}\left(|0101\rangle + |0110\rangle + |1001\rangle + |1010\rangle\right) \xrightarrow{\text{CNOT}} \tag{2.13}$$

$$\xrightarrow{\text{CNOT}} \frac{1}{2}\left(|0111\rangle + |0100\rangle + |1001\rangle + |1010\rangle\right) \xrightarrow{\text{H}} \tag{2.14}$$

$$\xrightarrow{\text{H}} \frac{1}{2}\left(\frac{1}{\sqrt{2}}(|0011\rangle - |0111\rangle) + \frac{1}{\sqrt{2}}(|0000\rangle - |0100\rangle) + \frac{1}{\sqrt{2}}(|1001\rangle + |1101\rangle) + \right.$$
$$\left. + \frac{1}{\sqrt{2}}(|1010\rangle + |1110\rangle)\right) = \frac{1}{2}\left(|00\rangle\left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\right) + |01\rangle\left(\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)\right) + \right.$$
$$\left. + |10\rangle\left(\frac{1}{\sqrt{2}}(-|00\rangle + |11\rangle)\right) + |11\rangle\left(\frac{1}{\sqrt{2}}(-|01\rangle + |10\rangle)\right)\right) =$$
$$\frac{1}{2}\left(|00\rangle|\beta_{00}\rangle + |01\rangle|\beta_{01}\rangle + |10\rangle(-|\beta_{10}\rangle) + |11\rangle(-|\beta_{10}\rangle)\right). \tag{2.15}$$

The second step is the measurement itself. If we measure the two middle qubits, the other two collapse into one of the four maximally entangled (Bell) states.

state of the middle qubits	state of boundary qubits	probability
$\|00\rangle$	$\|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$	1/4
$\|01\rangle$	$\|\beta_{01}\rangle = \frac{1}{\sqrt{2}}(\|01\rangle + \|10\rangle$	1/4
$\|10\rangle$	$-\|\beta_{10}\rangle = \frac{1}{\sqrt{2}}(-\|00\rangle + \|11\rangle$	1/4
$\|11\rangle$	$-\|\beta_{10}\rangle = \frac{1}{\sqrt{2}}(-\|01\rangle + \|10\rangle$	1/4

Table 2.2: The dependency of the state of the boundary qubits on the measurement outcomes.

This rewriting highlights two nice implications. First, whatever the measurement outcome will be, the first and the fourth qubit will be entangled – their state will be one of the four Bell states. Second, if Bob is in possesion of the fourth qubit and knows the measurement outcomes, he can choose which entangled state to share with Alice by applying local X or Z gates as we have seen in (1.87) and (1.88).

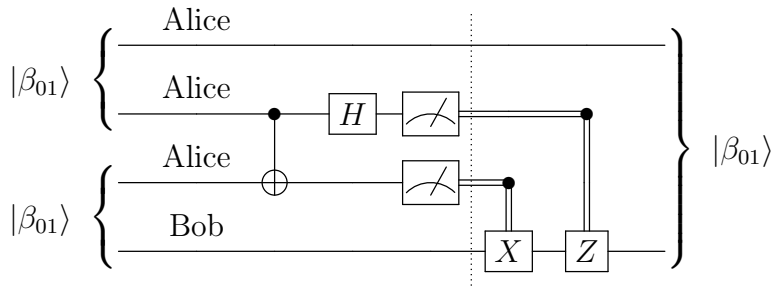


Figure 2.4: A circuit implementing entanglement swapping in the same manner as teleporting an unknown quantum state. At the dashed time point, we can be sure the first and the fourth qubits are entangled. After communication of the measurement outcome, we know which entangled state we posess and with several simple 1-qubit gates we can change it to whichever entangled state we want.

2.2 The implications of the impossibility of superluminal communication

Why does quantum teleportation work the way it works? Is there a reason why Bob's final state (= the state before the corrections) is $\{(|\psi\rangle, \frac{1}{4}), (\mathrm{X}|\psi\rangle, \frac{1}{4}), (\mathrm{Z}|\psi\rangle, \frac{1}{4}), (\mathrm{XZ}|\psi\rangle, \frac{1}{4})\}$ and not, for example, $\{(|\psi\rangle, \frac{1}{3}), (\mathrm{X}|\psi\rangle, \frac{1}{3}), (\mathrm{Z}|\psi\rangle, \frac{1}{3})\}$? Why each gate with $\frac{1}{4}$ probability? Couldn't teleportation work differently, perhaps could we make it more effective?

In this section, we are going to discuss several different scenarios of hypothetical quantum teleportation with intent to answer these questions. We will focus on understanding why quantum teleportation gives basically the best physical results. The scenarios are based on a hypothetical box which would manage to change the state of a 3-qubit composite system to such state which after measurement leaves Bob's qubit in the state we want to discuss.

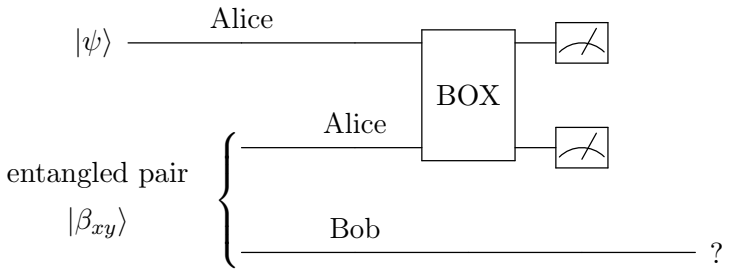


Figure 2.5: A circuit implementing a hypothetical quantum teleportation.

A good point to start is the question: *What would happen, if the final state was* $\{(|\psi\rangle, \frac{1}{2}), (\mathrm{X}|\psi\rangle, \frac{1}{2})\}$? Recall that commuting operators have a common set of eigen-

vectors. As the identity I commutes with all operators, there exist two orthogonal states: the eigenvectors of X, $|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\end{pmatrix}^{\mathrm{T}}$ and $|-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & -1\end{pmatrix}^{\mathrm{T}}$, which Bob receives without change. Neither X nor I changes them (except for a phase). Alice and Bob can agree on assigning value 1 to the state $|+\rangle$ and value 0 to the state $|-\rangle$ and nothing would stand in the way of faster-than-light communication. Thus, it is clear that such a (teleportation) box cannot exist.

In general, if the outcome was $\{(U_1|\psi\rangle, p_1), (U_2|\psi\rangle, p_2)\}$ where U_1, U_2 are unitary operators and p_1, p_2 probabilities that Bob's qubit is in the corresponding state $U_1|\psi\rangle$, $U_2|\psi\rangle$, the situation would be same, because if Bob applies, for example, $U_1^\dagger$ on his qubit, the state changes into $\{(|\psi\rangle, p_1), (U_1^\dagger U_2|\psi\rangle, p_2)\}$. Because

$$U_1^\dagger U_2 \left(U_1^\dagger U_2\right)^\dagger = U_1^\dagger U_2 U_2^\dagger U_1 = U_1^\dagger U_1 = I, \tag{2.16}$$

the operator $U_1^\dagger U_2$ is unitary, too. As we have already mentioned, each unitary operator has orthogonal eigenvectors. The eigenvectors of $U_1^\dagger U_2$ stay unchanged under this "teleportation" procedure as $U_1^\dagger U_2$ and I commute. So Alice teleports to Bob the eigenvectors of the unitary matrix $U_1^\dagger U_2$, Bob applies $U_1^\dagger$ on his member of entangled pair, performs a projective measurement in the eigenvector basis and has the bit of information Alice has sent him! This implies that in order not to violate the no-signaling theorem, there must be more than two possible states (= more than two things that could happen to the state $|\psi\rangle$ in "teleportation").

Now, imagine a situation, where Bob's qubit would be left in the state $\{(|\psi\rangle, \frac{1}{3}), (\mathrm{X}|\psi\rangle, \frac{1}{3}), (\mathrm{Z}|\psi\rangle, \frac{1}{3})\}$. At this point, it is appropriate to mention that the operators X, Z and $XZ = -iY$ anticommute with each other. They all have eigenvalues of the form $\pm x$. Imagine Alice wants to send an eigenvector of one of them. Suppose she is sending the vector $|+\rangle$ in order to communicate a binary value 1. If the final state was $I|+\rangle$ or $X|+\rangle$, she would succeed as they leave the state unchanged. However, if the final state was $Z|+\rangle$ or $XZ|+\rangle$, the communication would fail because as a consequence of anticommutation they change the vector $|+\rangle$ to its orthogonal complement $|-\rangle$ which is assigned to the value 0. In the considered case, $\{(|\psi\rangle, \frac{1}{3}), (\mathrm{X}|\psi\rangle, \frac{1}{3}), (\mathrm{Z}|\psi\rangle, \frac{1}{3})\}$, if Alice would send the eigenvectors of X or the eigenvectors of Z, there is a $\frac{2}{3}$ probability of success, as with probability $\frac{1}{3}$ the state is unchanged by I, and there is a $\frac{1}{3}$ probability of being unchanged by the operator whose eigenvectors Alice sends. On the other hand, there is a $\frac{1}{3}$ probability of failure as the state would be changed by the anticommuting operator. In general, the probability of failure is equal to the probability of anticommuting operators being applied.

However, does the $\frac{1}{3}$ probability of failure represent a big constraint? Not really, if we take into account that Alice and Bob can choose an approach where 1 bit of information would be send via n repetitions of the teleportation protocol. The scenario would go this way. Alice sends the same bit of information n-times. Bob looks at the

outcomes of his projective measurements and chooses the value which appears more often. In general, if the probability of successfully receiving information is $\frac{1}{2}+\epsilon$ and the probability of failure $\frac{1}{2}-\epsilon$, there is a relationship between the number of measurements needed for keeping the probability of failure under some value we are willing to accept. For this purpose, we are going to use *Chernoff-Hoeffding theorem* which tells us that if X_1, X_2, ..., X_n are independent and identically distributed random variables taking values $\{0,1\}$, p probability of error ($p=\frac{1}{2}-\epsilon$) and ϵ positive, non-zero constant, then

$$\Pr\left(\frac{1}{n}\sum X_i \geq p+\epsilon\right) \leq \left(\left(\frac{p}{p+\epsilon}\right)^{p+\epsilon}\left(\frac{1-p}{1-p-\epsilon}\right)^{1-p-\epsilon}\right)^n. \tag{2.17}$$

Notice that Chernoff's theorems work in the manner that the value 1 is assigned to bits which fail. So $\frac{1}{n}\sum X_i$ tells us what part of the sample has failed. As Bob looks which value appears more often, if more than or exactly half of the bits have been flipped ($\frac{1}{n}\sum X_i \geq \frac{1}{2}$), the information transfer fails. In the case $\frac{1}{n}\sum X_i = \frac{1}{2}$ Bob would not be able to decide and in the case $\frac{1}{n}\sum X_i > \frac{1}{2}$ Bob would end up with wrong value. By substitution $\frac{1}{2}-\epsilon$ for p, as probability of failure is $\frac{1}{2}-\epsilon$, we get

$$\Pr\left(\frac{1}{n}\sum X_i \geq \frac{1}{2}\right) \leq \left(\left(\frac{\frac{1}{2}-\epsilon}{\frac{1}{2}}\right)^{\frac{1}{2}}\left(\frac{\frac{1}{2}+\epsilon}{\frac{1}{2}}\right)^{\frac{1}{2}}\right)^n = \left(\sqrt{1-2\epsilon}\cdot\sqrt{1+2\epsilon}\right)^n,$$

$$\Pr\left(\frac{1}{n}\sum X_i \geq \frac{1}{2}\right) \leq \left(\sqrt{1-4\epsilon^2}\right)^n. \tag{2.18}$$

In order to express how many repetitions are needed for keeping the probability of error, $\Pr\left(\frac{1}{n}\sum X_i \geq \frac{1}{2}\right)$, under some value p_e, we simply substitute $\Pr\left(\frac{1}{n}\sum X_i \geq \frac{1}{2}\right)$ for p_e and using the properties of the logarithm, we get the relationship:

$$\log p_\mathrm{e} \leq n\log\sqrt{1-4\epsilon^2} \implies n \geq \frac{\log p_\mathrm{e}}{\log\sqrt{1-4\epsilon^2}}. \tag{2.19}$$

This means that except the case when probability of failure is $\frac{1}{2}$ ($\epsilon=0$) we can always keep the probability of error arbitrarily low with a reasonable growth of the required n with decreasing error tolerance p_e. If the probability of failure was exactly $\frac{1}{2}$, there is no way to lower the probability of error. Each bit is with the same probability correct and wrong and thus useless.

As in our considered case, the probability of error is $\frac{1}{3}$, so by a little repetition, we can lower the value to whichever p_e we want.[1] It implies we can trust the result and for that reason we would be able to reach faster-than-light communication. This protocol (such a box in Figure 2.5) therefore cannot exist, too. The general 3-state case, $\{(U_1|\psi\rangle, p_1), (U_2|\psi\rangle, p_2), (U_3|\psi\rangle, p_3)\}$, is also impossible because we can make any pair of the three unitary operators commute and there must be a pair which

[1] Except that for $p_\mathrm{e}=0$ we would need $n\to\infty$.

gives probability greater than $\frac{1}{2}$ (to be more specific, we can find a pair which gives probability at least $\frac{2}{3}$ because if we break an interval into 3 parts, there must be at least one part that is either exactly $\frac{1}{3}$ of the interval or less and we would choose the other two parts). We must conclude that hypothetical teleportation which would leave Bob with a mixed state made out of three possible states is not achievable.

Finally, as even quantum teleportation itself has four possible outputs, we can ask: *Why is the probability of applying each of the Pauli gates exactly $\frac{1}{4}$? Why the Pauli gates themselves?* Let us start with answering the first question. Imagine one of the gates would have probability of being applied greater than $\frac{1}{4}$ ($p = \frac{1}{4} + \epsilon$). At this point, the worst case would be if the rest of the probability would be divided equally. So if we take any pair of gates which includes the most probable gate, together their probability would be

$$\frac{1-p}{3} + p = \frac{1}{3} + \frac{2}{3}p = \frac{1}{3} + \frac{2}{3}\left(\frac{1}{4} + \epsilon\right) = \frac{1}{2} + \frac{2}{3}\epsilon > \frac{1}{2}. \tag{2.20}$$

As we can make the two gates commute and due to (2.19) decrease the probability of error to arbitralily low value, we would be able to reach faster-than-light communication. Since this clearly violates laws of physics (no-signaling), it cannot be possible. Thus each gate must apply exactly with the $\frac{1}{4}$ probability.

Notice that we can imagine teleportation as a channel which changes the qubit whose state Alice sends into the one Bob ends up with.

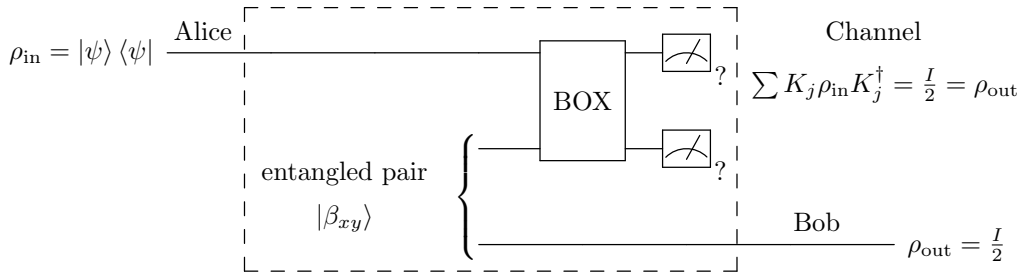


Figure 2.6: Teleportation taken as a quantum channel.

In order not to be able to communicate superluminally, the density operator of the qubit Bob ends up with (ρ_{out}) cannot depend on the density operator ρ_{in} Alice sends. If it would, for different ρ_{in}s (different communicated states) there would be different outcomes (different ρ_{out}s) which we would be able to distinguish and thus receive information immediately (faster-than-light).

The density operator $I/2$ provide us a great compromise. It cannot depend on the ρ_{in} and the channel did not have to destroy all the information (if Bob would communicate with Alice and find out her measurement outcomes he can get (by conditionaly applying a simple single-qubit gate) the desired state). There are channels which can

absolutelly destroy the incomming qubit with his density operator and return always a new qubit whose state can for example always correspond to density matrix $I/3$.

Until now, the only case we have been taking into account was choosing a pair of the operations that did nothing to $|\psi\rangle$ while the rest of the possible operations were considered as errors. However, do they neccesarily mean a failure? If some of the other gates would not anticommute, the gate would not change the communicated state to its fully orthogonal complement and therefore there would exist a non-zero probability that the communicated bit of information stay unchanged. This probability would represent the neccessary epsilon beyond the $\frac{1}{2}$ probability of the two gates needs for superluminal communication. Therefore we can exclude these cases, too.

In the end, we conclude that quantum teleportation does as much as it possibly could and not a bit more. If it did work in a simpler way (fewer possible operators, probabilities not exactly 1/4, or more generally, not completely mixing an input state), it would violate the no-signaling condition.

2.3 Interconnection of multiple entanglement swaps

Imagine Alice and Bob who are a very long distance from each other. However, they strongly wish to share some entangled pair. The quantum communication channel is not very reliable for such distances. In order to solve this problem, we are going to try to interconnect several entanglement swaps. Can we entangle the boundary qubits this way?

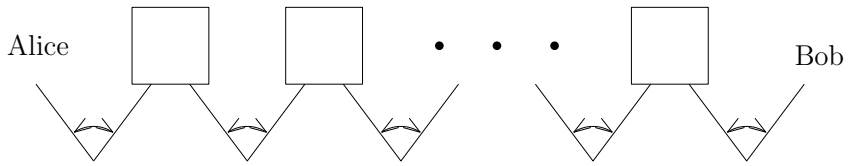


Figure 2.7: Interconnection of multiple entanglement swappings in order to entangle Alice's and Bob's qubits.

Notice, that entanglement swapping is in principle teleportation of the state of the second qubit in the entangled state to the qubit who's owner was usually Bob (see Figure 2.3). As we have already mentioned, the teleportation leaves Bob's qubit by itself in the mixed state $\{(|\psi\rangle, \frac{1}{4}), (X|\psi\rangle, \frac{1}{4}), (Z|\psi\rangle, \frac{1}{4}), (XZ|\psi\rangle, \frac{1}{4})\}$. Due to (1.87) and (1.88), if there is a Pauli gate applied locally on the state of the second qubit, the state of the two qubits will still be one of the four Bell states. This means that Bob's qubit must be entangled with Alice's first qubit. However, we should emphasize that we cannot write a state of a single qubit of an entangled pair as a pure state $|\psi\rangle$. To be correct, the first entanglement swap leaves Alice and Bob with a mixed state

$\{(|\beta_{01}\rangle, \frac{1}{4}), (I \otimes X |\beta_{01}\rangle, \frac{1}{4}), (I \otimes Z |\beta_{01}\rangle, \frac{1}{4}), (I \otimes XZ |\beta_{01}\rangle, \frac{1}{4})\}$. Now if Bob sends the state of his qubit via a teleportation protocol to Cecilia, Cecilia receives another mixed state

$$\Big\{\Big(\{(|\psi\rangle, \frac{1}{4}), (X|\psi\rangle, \frac{1}{4}), (Z|\psi\rangle, \frac{1}{4}), (XZ|\psi\rangle, \frac{1}{4})\}, \frac{1}{4}\Big), \Big(X\{(|\psi\rangle, \frac{1}{4}), (X|\psi\rangle, \frac{1}{4}), (Z|\psi\rangle, \frac{1}{4}), (XZ|\psi\rangle, \frac{1}{4})\}, \frac{1}{4}\Big), \Big(Z\{(|\psi\rangle, \frac{1}{4}), (X|\psi\rangle, \frac{1}{4}), (Z|\psi\rangle, \frac{1}{4}), (XZ|\psi\rangle, \frac{1}{4})\}, \frac{1}{4}\Big), \Big(XZ\{(|\psi\rangle, \frac{1}{4}), (X|\psi\rangle, \frac{1}{4}), (Z|\psi\rangle, \frac{1}{4}), (XZ|\psi\rangle, \frac{1}{4})\}, \frac{1}{4}\Big)\Big\}.$$

If we teleport any state via quantum teleportation, the receiver ends up with the unchanged state with a $\frac{1}{4}$ probability and with the same probability, the state was changed by applying X or Z or XZ. If any of this states, e.g. $X|\psi\rangle$, would be sent to another receiver via the same protocol, the second receiver ends up with $\{(X|\psi\rangle, \frac{1}{4}), (XX|\psi\rangle, \frac{1}{4}), (ZX|\psi\rangle, \frac{1}{4}), (XZX|\psi\rangle, \frac{1}{4})\}$. In case of an entangled pair, more correct would be

$$\{(I \otimes X|\beta_{01}\rangle, \frac{1}{4}), (I \otimes XX|\beta_{01}\rangle, \frac{1}{4}), (I \otimes ZX|\beta_{01}\rangle, \frac{1}{4}), (I \otimes XZX|\beta_{01}\rangle, \frac{1}{4})\}. \quad (2.21)$$

Thanks to the multiplication table:

	I	X	Z	XZ	-I	-X	-X	-XZ
I	I	X	Z	XZ	-I	-X	-X	-XZ
X	X	I	XZ	Z	-X	-I	-XZ	-Z
Z	Z	-XZ	I	-X	-Z	XZ	-I	X
XZ	XZ	-Z	X	-I	-XZ	Z	-X	I

Table 2.3: Multiplication table.

we can clearly see that any state, for example the $X|\psi\rangle$ will after teleportation again become (if we ignore the global phase) the mixed state $\{(|\psi\rangle, \frac{1}{4}), (X|\psi\rangle, \frac{1}{4}), (Z|\psi\rangle, \frac{1}{4}), (XZ|\psi\rangle, \frac{1}{4})\}$. As this will happen with all possible states ($|\psi\rangle$, $X|\psi\rangle$, $Z|\psi\rangle$ and $XZ|\psi\rangle$), even the n-th receiver ends up with the mixed state $\{(|\psi\rangle, \frac{1}{4}), (X|\psi\rangle, \frac{1}{4}), (Z|\psi\rangle, \frac{1}{4}), (XZ|\psi\rangle, \frac{1}{4})\}$. To better illustrate this, we will analyze the Cecilia's state a

little bit deeper:

$$\Big\{\Big(\{(|\psi\rangle, \frac{1}{4}), (X|\psi\rangle, \frac{1}{4}), (Z|\psi\rangle, \frac{1}{4}), (XZ|\psi\rangle, \frac{1}{4})\}, \frac{1}{4}\Big),$$
$$\Big(X\{(|\psi\rangle, \frac{1}{4}), (X|\psi\rangle, \frac{1}{4}), (Z|\psi\rangle, \frac{1}{4}), (XZ|\psi\rangle, \frac{1}{4})\}, \frac{1}{4}\Big),$$
$$\Big(Z\{(|\psi\rangle, \frac{1}{4}), (X|\psi\rangle, \frac{1}{4}), (Z|\psi\rangle, \frac{1}{4}), (XZ|\psi\rangle, \frac{1}{4})\}, \frac{1}{4}\Big),$$
$$\Big(XZ\{(|\psi\rangle, \frac{1}{4}), (X|\psi\rangle, \frac{1}{4}), (Z|\psi\rangle, \frac{1}{4}), (XZ|\psi\rangle, \frac{1}{4})\}, \frac{1}{4}\Big)\Big\} =$$

$$= \Big\{\Big(\{(|\psi\rangle, \frac{1}{4}), (X|\psi\rangle, \frac{1}{4}), (Z|\psi\rangle, \frac{1}{4}), (XZ|\psi\rangle, \frac{1}{4})\}, \frac{1}{4}\Big),$$
$$\Big(\{(|\psi\rangle, \frac{1}{4}), (X|\psi\rangle, \frac{1}{4}), (Z|\psi\rangle, \frac{1}{4}), (XZ|\psi\rangle, \frac{1}{4})\}, \frac{1}{4}\Big),$$
$$\Big(\{(|\psi\rangle, \frac{1}{4}), (X|\psi\rangle, \frac{1}{4}), (Z|\psi\rangle, \frac{1}{4}), (XZ|\psi\rangle, \frac{1}{4})\}, \frac{1}{4}\Big),$$
$$\Big(\{(|\psi\rangle, \frac{1}{4}), (X|\psi\rangle, \frac{1}{4}), (Z|\psi\rangle, \frac{1}{4}), (XZ|\psi\rangle, \frac{1}{4})\}, \frac{1}{4}\Big)\Big\} =$$

$$= \Big\{(|\psi\rangle, \frac{1}{16}), (X|\psi\rangle, \frac{1}{16}), (Z|\psi\rangle, \frac{1}{16}), (XZ|\psi\rangle, \frac{1}{16}),$$
$$(|\psi\rangle, \frac{1}{16}), (X|\psi\rangle, \frac{1}{16}), (Z|\psi\rangle, \frac{1}{16}), (XZ|\psi\rangle, \frac{1}{16}),$$
$$(|\psi\rangle, \frac{1}{16}), (X|\psi\rangle, \frac{1}{16}), (Z|\psi\rangle, \frac{1}{16}), (XZ|\psi\rangle, \frac{1}{16}),$$
$$(|\psi\rangle, \frac{1}{16}), (X|\psi\rangle, \frac{1}{16}), (Z|\psi\rangle, \frac{1}{16}), (XZ|\psi\rangle, \frac{1}{16}),\Big\} =$$

$$= \Big\{(|\psi\rangle, \frac{1}{4}), (X|\psi\rangle, \frac{1}{4}), (Z|\psi\rangle, \frac{1}{4}), (XZ|\psi\rangle, \frac{1}{4})\Big\}.$$

Or analogically we would get

$$\{(|\beta_{01}\rangle, \frac{1}{4}), (I \otimes X|\beta_{01}\rangle, \frac{1}{4}), (I \otimes Z|\beta_{01}\rangle, \frac{1}{4}), (I \otimes XZ|\beta_{01}\rangle, \frac{1}{4})\}. \tag{2.22}$$

Thus we can conclude that Cecilia ends up with the same state as Bob did. If Cecilia would send it to Denda, Denda would receive the same state, too. So the boundary qubits will be necessarily entangled. To see in which state of the 4 Bell states they will be in, they would need the classical info from the measurements.

One lesson to take from here is that a quantum repeater (for propagating quantum information over long distances) is possible, if we are able to prepare many entangled pairs along the way, and separate them over shorter distances [8].

Chapter 3

Quantum Games and Correlations

In this chapter we will show on a simple CHSH game[1] that quantum correlations have provable effects and that they can for example help us to be a really good players in some games (better than we would be without quantum aspects).

Imagine a simple game. Alice and Bob are placed in two separated rooms without possibility of communication. Each of them is asked one of two possible yes-no questions $\{q_1, q_2\}$. For example, each can receive 1 bit ($q_1 = 0$ and $q_2 = 1$). If both are asked the first question (0), to win, they must give the same answer (Alice's answer (a) $\oplus$ Bob's answer (b) $= 0$). Otherwise they must answer differently ($a \oplus b = 1$).

Alice's question (a_1)	Bob's question (a_2)	winning answers
0	0	$=$
0	1	$\neq$
1	0	
1	1	

Table 3.1: How the answers must be correlated in order for Alice and Bob to win (winning answers to question combinations).

First, let us look at the possible classical (memoryless) strategies. There are *pure strategies* which are constructed of answers assigned to individual questions. All other strategies, *mixed strategies*, are just some probabilistic mixtures of the pure ones – they choose among the pure strategies at random, with various proportions.

Let us look at the pure strategies and what probability of winning do they provide. Alice and Bob have just 4 possible pure strategies by themselves.

[1] A class of games constructed to test CHSH inequalities.

Question	Strategy			
	s_1	s_2	s_3	s_4
0	0	0	1	1
1	0	1	0	1

Table 3.2: Pure strategies for one person.

As each of them has 4 possible pure strategies, together they have 16 pure combined strategies. We can simply list them.

Global strategy	Alice's strategy	Bob's strategy	probability of winning
S_1	s_1	s_1	1/4
S_2	s_1	s_2	3/4
S_3	s_1	s_3	1/4
S_4	s_1	s_4	3/4
S_5	s_2	s_1	3/4
S_6	s_2	s_2	3/4
S_7	s_2	s_3	1/4
S_8	s_2	s_4	1/4
S_9	s_3	s_1	1/4
S_{10}	s_3	s_2	1/4
S_{11}	s_3	s_3	3/4
S_{12}	s_3	s_4	3/4
S_{13}	s_4	s_1	1/4
S_{14}	s_4	s_2	3/4
S_{15}	s_4	s_3	1/4
S_{16}	s_4	s_4	1/4

Table 3.3: All pure strategies with their probability of winning.

We can see that the best pure strategies has a **3/4** probability of winning. Notice that all of the mixed strategies can be written as a sum

$$\sum_{i=1}^{16} p_i S_i, \tag{3.1}$$

where p_i is a probability of using a corresponding pure strategy S_i. The expected probability of winning can be expressed as a sum

$$p_{\text{win}} = \sum_{i=1}^{16} p_i P(S_i), \tag{3.2}$$

where $P(S_i)$ is the probability of winning for the corresponding strategy S_i which the players choose with probability p_i. Because

$$p_{\text{win}} = \sum_{i=1}^{16} p_i P(S_i) \leq \sum_{i=1}^{16} p_i \max\big(P(S_i)\big) = \max\big(P(S_i)\big), \tag{3.3}$$

the expected probability of winning of a mixed strategy cannot exceed the probability of winning of the best pure strategy, as $\max\big(P(S_i)\big)$ is exactly its corresponding probability of winning. If probability of winning of a mixed strategy would be same as probability of winning of the best pure strategy, the mixed strategy must choose among the best pure strategies. So this game can be classically won in at most $\frac{3}{4}$ cases n average. However, if we would use the advantages of quantum mechanics – superpositions and entangled pairs – could we make it better? Could quantum mechanics win in more cases (= let us have a greater probability of winning)?

Imagine Alice and Bob share an entangled pair in the Bell state

$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}}\big(|01\rangle - |10\rangle\big) = \frac{1}{\sqrt{2}}\left[\begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} - \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix}\right] = \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\-1\\0\end{pmatrix}. \tag{3.4}$$

If they would just measure it and answer with their measurement outcomes, they would easily reach a $\frac{3}{4}$ probability of winning as they always answer differently. This probability of winning corresponds to the best classical strategies. However, Alice and Bob can also manipulate the states of their qubits before the measurement. Depending on the question they were asked, they rotate their qubits in order to manipulate the probability of having different measurement outcomes (to create some probability of having the same outcome). In general, we can write a rotation by an angle φ as a rotation matrix (operator)

$$\begin{pmatrix}\cos\varphi & -\sin\varphi\\ \sin\varphi & \cos\varphi\end{pmatrix}. \tag{3.5}$$

If Alice rotates the state of her qubit by an angle α and Bob by an angle β, they

change the state of their entangled pair to

$$(\mathrm{R}_\alpha \otimes \mathrm{R}_\beta)\,|\beta_{11}\rangle = \frac{1}{\sqrt{2}}\left[\begin{pmatrix}\cos\alpha & -\sin\alpha\\ \sin\alpha & \cos\alpha\end{pmatrix}\otimes\begin{pmatrix}\cos\beta & -\sin\beta\\ \sin\beta & \cos\beta\end{pmatrix}\right]\begin{pmatrix}0\\1\\-1\\0\end{pmatrix} =$$

$$= \frac{1}{\sqrt{2}}\begin{pmatrix}\cos\alpha\cos\beta & -\cos\alpha\sin\beta & -\sin\alpha\cos\beta & \sin\alpha\sin\beta\\ \cos\alpha\sin\beta & \cos\alpha\cos\beta & -\sin\alpha\sin\beta & -\sin\alpha\cos\beta\\ \sin\alpha\cos\beta & -\sin\alpha\sin\beta & \cos\alpha\cos\beta & -\cos\alpha\sin\beta\\ \sin\alpha\sin\beta & \sin\alpha\cos\beta & \cos\alpha\sin\beta & \cos\alpha\cos\beta\end{pmatrix}\begin{pmatrix}0\\1\\-1\\0\end{pmatrix} =$$

$$= \frac{1}{\sqrt{2}}\begin{pmatrix}\sin\alpha\cos\beta-\cos\alpha\sin\beta\\ \sin\alpha\sin\beta+\cos\alpha\cos\beta\\ -\left[\cos\alpha\cos\beta+\sin\alpha\sin\beta\right]\\ \sin\alpha\cos\beta-\cos\alpha\sin\beta\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}\sin(\alpha-\beta)\\ \cos(\alpha-\beta)\\ -\cos(\alpha-\beta)\\ \sin(\alpha-\beta)\end{pmatrix}. \tag{3.6}$$

Depending on a question, Alice and Bob can rotate their qubits by respective different amounts:

question	0	1
Alice's angle	A_0	A_1
Bob's angle	B_0	B_1

Table 3.4: Angles through which Alice and Bob rotate the state of his/her qubit in the corresponding situation (answering to question 0 or answering to question 1).

Notice that probability of measuring $0_\mathrm{A}0_\mathrm{B}$ is

$$\left((\mathrm{R}_\alpha \otimes \mathrm{R}_\beta)\,|\beta_{11}\rangle\right)^\dagger |00\rangle\langle 00|\,(\mathrm{R}_\alpha \otimes \mathrm{R}_\beta)\,|\beta_{11}\rangle =$$

$$= \frac{1}{\sqrt{2}}\begin{pmatrix}\sin(\alpha-\beta)\\ \cos(\alpha-\beta)\\ -\cos(\alpha-\beta)\\ \sin(\alpha-\beta)\end{pmatrix}^{\mathrm{T}}\begin{pmatrix}1&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}\sin(\alpha-\beta)\\ \cos(\alpha-\beta)\\ -\cos(\alpha-\beta)\\ \sin(\alpha-\beta)\end{pmatrix} = \frac{1}{2}\sin^2(\alpha-\beta), \tag{3.7}$$

the probability of measuring $0_\mathrm{A}1_\mathrm{B}$ is $\frac{1}{2}\cos^2(\alpha-\beta)$, the probability of measuring $1_\mathrm{A}0_\mathrm{B}$ is $\frac{1}{2}\cos^2$
$(\alpha-\beta)$ and the probability of measuring $1_\mathrm{A}1_\mathrm{B}$ is $\frac{1}{2}\sin^2(\alpha-\beta)$. If both, Alice and Bob, are asked the first question ($q_1 = 0$), they want to provide the same answer, so they want to maximize the probability of measuring $0_\mathrm{A}0_\mathrm{B}$ and $1_\mathrm{A}1_\mathrm{B}$ which is equal to $\sin^2(\alpha-\beta)$. In the other cases, they want to maximize the probability of measuring

$0_A 1_B$ and $1_A 0_B$ which is equal to $\cos^2(\alpha - \beta)$. So depending on the questions the probabilities of winning are:

Alice's question	Bob's question	probability of winning
0	0	$\sin^2(A_0 - B_0)$
0	1	$\cos^2(A_0 - B_1)$
1	0	$\cos^2(A_1 - B_0)$
1	1	$\cos^2(A_1 - B_1)$

Table 3.5: Probability of winning as a dependence on the asked questions.

In order to find out what is the greatest probability of winning in the quantum mechanical case, we want to find out for which angles A_0, A_1, B_0, B_2 is the total probability of winning

$$p_{\text{win}} = \frac{1}{4}\Big(\sin^2(A_0 - B_0) + \cos^2(A_0 - B_1) + \cos^2(A_1 - B_0) + \cos^2(A_1 - B_1)\Big) \quad (3.8)$$

maximal. As we will see, it is quite convenient to imagine the angles as 4 vectors in space. The angles are the angles between the vectors and the horizontal plane and relative angles are the relative angles between the vectors. If we try to maximize each member of the equation (3.8) individually, we see which values do the relative angles want to approach:

$$\begin{aligned} A_0 - B_0 &\to \frac{\pi}{2} + k\pi, \\ \left.\begin{aligned} A_0 - B_1 \\ A_1 - B_0 \\ A_1 - B_1 \end{aligned}\right\} &\to 0 + k\pi \end{aligned} \quad (3.9)$$

As our goal is not to find all the possible cases which has the greatest possible probability but to find what the maximal possible probability of winning is, let us take a closer look just at the interval from 0 to $\frac{\pi}{2}$. Any other case always corresponds to a case which has all angles in this interval (it contains all the possible measurement outcomes probabilities). Thus the vectors A_0 and B_0 try to be as far as possible. On the other hand, B_1 wants to be as close as possible to A_0 and A_1 (so do they) and A_1 tries to reach also the vector B_0. Let us depict these conditions graphically.

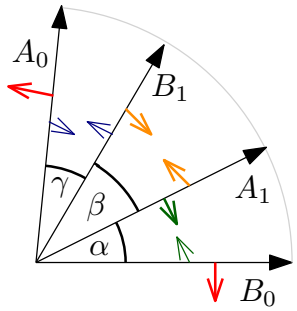


Figure 3.1: In what manner will the vectors be placed.

As α, β and γ try to be as small as possible but the angle $A_0 - B_0$ as large as possible, all the vectors must lie in a plane. Thus the relative angle $A_0 - B_0$ must be equal to $\alpha + \beta + \gamma$. Now, imagine that A_0, B_0 and B_1 are fixed. This implies that $A_0 - B_0 = \alpha + \beta + \gamma$, $A_0 - B_1 = \gamma$ and $B_1 - B_0 = \alpha + \beta$ are constants, so in order to find ideal position for A_1, we try to maximize the function

$$\cos^2(A_1 - B_1) + \cos^2(A_1 - B_0) = \cos^2(\beta) + \cos^2(\alpha). \tag{3.10}$$

As $\alpha + \beta = \text{constant} = K$, we simly rewrite the function to

$$\cos^2(\alpha) + \cos^2(K - \alpha). \tag{3.11}$$

Let us find the maximum. We start by looking for the inflection points:

$$-2\cos(\alpha)\sin(\alpha) + 2\cos(K - \alpha)\sin(K - \alpha) = 0. \tag{3.12}$$

Using the identities $\sin(2x) = 2\sin(x)\cos(x)$ and $\sin(x) - \sin(y) = 2\cos\left(\frac{x+y}{2}\right)\sin\left(\frac{x-y}{2}\right)$ we get

$$\begin{aligned} -\sin(2\alpha) + \sin(2K - 2\alpha) = 2\cos(K)\sin(K - 2\alpha) = 0 \implies \\ \implies K - 2\alpha = k\pi \implies \alpha = \frac{K}{2} + k\frac{\pi}{2}. \end{aligned} \tag{3.13}$$

We are considering just the interval $\left\langle 0, \frac{\pi}{2} \right\rangle$, that means $k = 0$ and $K \in \left\langle 0, \frac{\pi}{2} \right\rangle$ so $\cos(K) > 0$. Because the second derivative of the function is negative at the point $\alpha = \frac{K}{2}$:

$$-4\cos(K)\cos(K - 2\alpha) = -4\cos(K)\cos(0) = -4\cos(K) < 0, \tag{3.14}$$

the function has a maximum here. As $\beta = K - \alpha = K - \frac{K}{2} = \frac{K}{2}$, we conclude that in order to make the probability of winning maximal, $\alpha = A_1 - B_0$ must be equal to $\beta = A_1 - B_1$. We would get to absolutely the same conclusion about β and γ, because if we would fix the vectors A_0, A_1 and B_0, in order to find the maximal possible probability, we will maximize the same function $\cos^2(\gamma) + \cos^2(C - \gamma)$, where

$C = \gamma + \beta$. To sum up, the probability of winning is maximal if $\alpha = \beta$ and $\beta = \gamma$. Thus $\alpha = \beta = \gamma$ is the most ideal case we could get if $\alpha + \beta + \gamma$ is fixed. However, how big these angles should be to reach the real maximum (not just the best possible value in some special situation = when something has been fixed)?

We have got to the point, when we are able to find the probability of winning. All we have to do is find the maximum of the function

$$\sin^2(3x) + 3\cos^2(x). \tag{3.15}$$

As usually, the first step is finding the inflection points. Those are the ones in which the derivation is equal to zero:

$$6\sin(3x)\cos(3x) - 6\cos(x)\sin(x) = 0, \tag{3.16}$$

using the identity $\sin(2x) = 2\sin(x)\cos(x)$ we get

$$3\sin(6x) - 3\sin(2x) = 0. \tag{3.17}$$

By dividing the equation by 3 and using the identity $\sin(x) - \sin(y) = 2\cos\left(\frac{x+y}{2}\right)\sin\left(\frac{x-y}{2}\right)$ we can find the inflection points:

$$2\cos(4x)\sin(2x) = 0 \begin{cases} \cos(4x) = 0 \implies x = \frac{\pi}{8} + k\frac{\pi}{4} \\ \sin(2x) = 0 \implies x = \frac{k\pi}{2}. \end{cases} \tag{3.18}$$

Except the case $x = 0$ which we have already discussed, the only case which meets the condition that both x, $3x \in \left\langle 0, \frac{\pi}{2} \right\rangle$, is when $x = \frac{\pi}{8}$. The probability of winning in this case is

$$p_{\text{win}} = \frac{1}{4}\left[\sin^2\frac{3\pi}{8} + 3\cos^2\frac{\pi}{8}\right] = \frac{1}{4}\left[\left(\frac{\sqrt{2+\sqrt{2}}}{2}\right)^2 + 3\left(\frac{\sqrt{2+\sqrt{2}}}{2}\right)^2\right] = \left(\frac{\sqrt{2+\sqrt{2}}}{2}\right)^2 = \frac{2+\sqrt{2}}{4} \doteq 0.8536 > 0.75, \tag{3.19}$$

i.e. strictly more than the classical optimal strategy's winning percentage (see Table 3.3).

At this point we can definitely conclude that quantum mechanics can make us more succsessful players in this game. However, is this the best probability of winning quantum mechanics allows us? With this purpose, we are going to look at *Tsirelson's bounds*. They tell us exactly what is the upper limit to quantum mechanical correlations between distant events (Alice and Bob measuring in two separated rooms). Concretely, we are interested in Tsirelson's bound for CHSH inequality which is related to our CHSH game. This bound

$$T = \langle a_0 b_0 \rangle + \langle a_0 b_1 \rangle + \langle a_1 b_0 \rangle - \langle a_1 b_1 \rangle \leq 2\sqrt{2}, \tag{3.20}$$

was proven for a very similar game. a_0, a_1 are Alice's observables and b_0, b_1 Bob's observables with eigenvalues ± 1. $[a_i, b_j] = 0$ for all i, j – measurements taken on two different qubits commute. The measured observables depend on the asked questions. If they are asked a pair of questions from the set $\{0_\mathrm{A}0_\mathrm{B}, 0_\mathrm{A}1_\mathrm{B}, 1_\mathrm{A}0_\mathrm{B}\}$ ("+" sign in Tsirelson's bound), in order to increase the value of T, the answer must be (to win) correlated/anticorrelated and if they are asked $1_\mathrm{A}1_\mathrm{B}$ ("-" sign in Tsirelson's bound) in reverse. In order to keep it as much similar to our game as we can, we simply claim that in the 3 cases the answers must be anticorrelated and in the single case correlated in order to win. To correlated answers we assign the value -1 and to anticorrelated $+1$. $\langle X \rangle$ represents an average value. For example, for our state $|\beta_{11}\rangle$ the average value $\langle a_0 b_1 \rangle = (+1)\cos^2 x + (-1)(1 - \cos^2 x)$ where $\cos^2 x$ is the probability that the answers are anticorrelated and thus the result value is $+1$ and $1 - \cos^2 x$ the probability that the answers are correlated.

We have told that the games are very similar. So what are the differences? There are just two of them. First, the eigenvalues of the operators are in this game ± 1 while in our case, they are 0 and 1. This is not a problem as these operators have common eigenvectors, as they are only a shift and rescaling of each other. Let U be an operator with eigenvalues ± 1 corresponding to an operator P whose eigenvalues are 0 and 1, in the manner that

$$P = \frac{I + U}{2} \qquad \Longleftrightarrow \qquad U = 2P - I. \tag{3.21}$$

The same relationship is between their expectation values:

$$\langle \psi | P | \psi \rangle = \frac{1 + \langle \psi | U | \psi \rangle}{2} \qquad \Longleftrightarrow \qquad \langle \psi | U | \psi \rangle = 2 \langle \psi | P | \psi \rangle - 1. \tag{3.22}$$

This means that the probability of measurement outcome 0 when measuring P is equal to the probability of -1 when measuring U as as well as the probability of 1 when measuring P is equal to the probability of 1 when measuring U.

The second difference is just in the notation. The correlated answers are the winning case when both, Alice and Bob, are asked the question 0 in comparision to question 1 in this game. So we just simply rewrite Tsirelson's bound to

$$\langle A_1 B_1 \rangle + \langle A_1 B_0 \rangle + \langle A_0 B_1 \rangle - \langle A_0 B_0 \rangle \leq 2\sqrt{2}. \tag{3.23}$$

As there is already no constraint, we can finally look wheter the case $x = \frac{\pi}{8}$ is really

the case with the greatest possible probability of winning.

$$\begin{gathered}\langle A_1B_1\rangle + \langle A_1B_0\rangle + \langle A_0B_1\rangle - \langle A_0B_0\rangle = \cos^2(A_1 - B_1) - (1 - \cos^2(A_1 - B_1)) + \\ + \cos^2(A_1 - B_0) - (1 - \cos^2(A_1 - B_0)) + \cos^2(A_0 - B_1) - (1 - \cos^2(A_0 - B_1)) - \\ - \left[(1 - \sin^2(A_0 - B_0)) - \sin^2(A_0 - B_0)\right] = \cos^2 x - (1 - \cos^2 x) + \cos^2 x - \\ -(1 - \cos^2 x) + \cos^2 x - (1 - \cos^2 x) - \left[(1 - \sin^2 3x) - \sin^2 3x\right] = \\ = 2\left[3\cos^2 x + \sin^2 3x\right] - 4 = 2\left[4p_{\text{win}}\right] - 4 = 8p_{\text{win}} - 4 = 8 \cdot \frac{2+\sqrt{2}}{4} - 4 = 2\sqrt{2}.\end{gathered} \tag{3.24}$$

Thus it is clear that the $x = \frac{\pi}{8}$ case reached Tsirelson's bound. Thus really the greatest reachable probability of winning in the quantum mechanical case is

$$p_{\text{win}} = \frac{2+\sqrt{2}}{4} \doteq 0.8536. \tag{3.25}$$

What would happen if the probability was a little bit greater? What effect would the possibility of probability of winning equal to 1 have? Is there some reason why it would be physically unacceptable?

It turns out there exists (likely unphysical) a way of assigning correlations that perfectly win the CHSH game [10]. Neverthless, they do not violate no-signaling. Story for another day.

Conclusion

In this work (Chapter 2) we have studied quantum teleportation. We have explained how quantum teleportation works and how can it be interpreted. In the section 2.2 we continued a little bit deeper and discussed why quantum teleportation can not work in a very different manner than we have introduced. Basically, quantum teleportation does as much as it possibly could. If it did work in a simpler way (fewer possible operators, probabilities not exactly $1/4$, or more generally, not completely mixing an input state), it would violate the no-signaling condition. We have introduced also entanglement swapping and in the section 2.3 we have shown that if we repeat the entanglement swapping n times, if Alice is at the beginning of this series and Bob at the end, their qubits will become during this process entangled. This interconnection of entanglement swaps allows us to posses an entangled pair which can be spatially separated by a very long distance.

The aim of this thesis was also to provide a deeper understanding of a very crutial part of quantum teleportation – entangled pairs. Throughout the first chapter, we have explained what they are and what properties they have. We have shown that even though the entangled qubits are correlated, it is impossible to use this correlations for faster-than-light communication. However, we can use them for creating secret keys for encrypted communication or they can allow us to be quite successful in some (specialy constructed) games (See Chapter 3). The third chapter has been created with purpose to emphasize that quantum mechanics cannot be described classicaly (by some hidden variables). The correlations provided by entangled pairs are really something special. This fact has been demonstrated on a simple CHSH game. Probability of winning of a quantum strategy is strictly greater than probability of winning of a classical strategy.

This work was mainly a study of these topics. We did not bring anything new. However, we have provided our opinions and our calulations on why does quantum teleportation work the way it does (section 2.2), the interconnection of multiple entangled swaps (section 2.3) and finding the probability of winning of a quantum strategy in Chapter 3.

Bibliography

[1] A. Aspect, P. Grangier, and G. Roger. Experimental Realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A New Violation of Bell's Inequalities. *Physical Review Letters*, 49(2):91–94, 1982.

[2] J. S. Bell. On the Einstein Podolsky Rosen paradox. *Physics*, 1: 195–200, 1964.

[3] C. H. Bennet and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, 175: 8, 1984.

[4] C. H. Bennet, G. Brassard, C. Crépeau, R. Josza, A. Peres, and W. K. Wooters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channel. *Physical Review Letters*, 70(13):1895–1899, March 1993.

[5] A. Einstein, B. Podolsky, and N. Rosen. Can quantummechanical description of physical reality be considered complete? *Physical Review*, 47: 777–779, 1935.

[6] Nick Herbert. FLASH — A superluminal communicator based upon a new kind of quantum measurement. *Foundations of Physics*, 12(12): 1171–1179, 1982.

[7] David Kaiser. *How the Hippies Saved Physics*. NORTON, 2011.

[8] W. J. Munro, K. Azuma, K. Tamaki, and K. Nemoto. Inside quantum repeaters. *IEEE Journal of Selected Topics in Quantum Electronics*, 21: 1 – 13, May 2015.

[9] R. Laflamme P. Kaye and M. Mosca. *An Introduction to Quantum Computing*. Oxford University Press, 2007.

[10] D. Rohrlich S. Popescu. Nonlocality as an axiom. *Foundations of Physics*, 24: 379–385, 1994.

[11] E. Schrödinger. Die gegenwärtige Situation in der Quantenmechanik. *Naturwissenschaften*, 23: 807–812, 823–828, 844–849, 1935.

[12] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger. Violation of Bell's inequality under strict Einstein locality conditions. *Review Letters*, 81: 5039–5043, 1998.

[13] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299: 802–803, 1982.