Quantum information theory (20110401)

Lecturer: Jens Eisert

Chapter 1: Introduction

Contents

Chapter 1

Introduction

1.1 Some introductory words

1.1.1 Quantum information theory

This course will be concerned with quantum information science, or quantum information theory, for that matter. This is a comparably new field of research that enjoys tremendous attention that explores the consequences of a compelling idea: The idea at the heart of the field is the premise that new modes of information processing could emerge if the single carries of information are not classical systems that can take discrete values such as bits, but single quantum systems. Such quantum systems – atoms, ions, light modes, superconducting systems – can be in superpositions, can feature entanglement, the most quantum of all properties. It may hence be perfectly conceivable to think that making use of such single quantum systems as carriers of information that new applications and modes of information processing emerge. It is the key insight of the field that this is indeed the case. And this is what we are going to explore in this course.

- *Quantum key distribution* allows to establish a secure key to transmit classical information from one place to another (based on a shorter shared key). The security of the scheme is not based on unproven mathematical assumptions, but on very basic and fundamental properties of quantum physics. This is an idea that is not entirely new: Already in 1984, C. H. Bennett and G. Brassard formulated a first scheme for quantum key distribution, based on the idea of quantum money due to S. Wiesner. The basic idea at the heart of quantum key distribution is that one cannot learn a quantum state without to some extent disturbing it. We will come back to such notions in great detail.

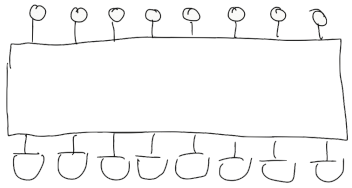
  Quantum key distribution is no far-fetched dream: It is already reality. One can commercially buy quantum cryptographic devices: The company IDQuantique is only one out of many offering such products. It has been one of the early successes of the field of quantum cryptography to implement a BB84 scheme (the simplest and most used scheme for quantum key distribution that we will discuss

soon) making use of an installed optical fibre cable linking Geneva and Nyon over 23 km through Lake Geneva in 1995, at remarkably low quantum bit error rates. This effort basically started the development of long-distance quantum key distribution. In the meantime, satellite-based quantum key distribution is being pursued.

- In *quantum metrology*, one makes use of intricate quantum properties to improve the accuracy in certain sensing and metrology tasks. This is again a field of research that has much matured and has already found, say, medical applications.
- In *quantum simulation* one takes the insight seriously that one cannot efficiently keep track of the dynamics of interacting quantum many-body systems as they are ubiquitous in quantum chemistry, in condensed matter physics and quantum materials. Surely, there are powerful approximate methods available, methods that actually make use of a significant proportion of the available computing power of our super-computers. Still, there are limits to this, even provably so (under mild complexity-theoretic assumptions), as we will see. It has been an interesting idea to let quantum systems simulate other quantum systems – going back to ideas of R. Feynman – which is the core insight of the flourishing field of quantum simulation. One distinguishes analog quantum simulators, where one basically reconstructs a given Hamiltonian under precisely controlled conditions – from so-called digital quantum simulators, which can be seen as basically quantum computers that perform Hamiltonian simulation.
- The most challenging and at the same time most intriguing idea is that of a *quantum computer*. Early suggestions of quantum computers have again been made by R. Feynman and D. Deutsch: This is a computational device the elementary carriers of information are single quantum systems, so when bits are being replaced by quantum bits, *qubits* in short. Indeed, such a computational device challenges the Church Turing thesis, in that there are problems intractable on classical computers (in that the computational effort grows faster than any polynomial with the input length), while a quantum computer, once realized, could solve the problem in polynomial time. Shor's famous efficient quantum algorithm for factoring (finding the factors a and b of a product ab of two primes) that classically is intractable and at the basis of modern cryptographic systems, has firmly placed this foundational idea into the realm of technology.

  Surely, for many years this has been an enormously fruitful theoretical idea mainly, with significant spin-offs in various aspects of quantum physics. It was rather recently when protagonists set out to actually build such devices on a medium scale. The last years have seen the development of trapped ion systems up to 50 ions. Companies such as IBM, Google, and Rigetti moved on to present data of 53 qubit machines, with larger ones already being developed. Such a device has arguably already shown a "quantum computational advantage" of quantum computers of classical supercomputers, resorting to rigorous statements in computational complexity. These problems are still paradigmatic and of little practical use, to say the least. But there is an enormous interest in trying to find out what near-term quantum computers can computationally achieve

and what they are good for, e.g., in notions of quantum machine learning or with applications in quantum chemistry. The key challenge here is to deal with imperfections and errors, which points into the direction that some notion of quantum error correction will be required.



1.1.2 How to use these lecture notes

This course will be dedicated to the foundations and the roots of this field. All of the above applications will be mentioned and discussed as well.

Entanglement as a resource in quantum information theory: We will see that the structure element of quantum mechanics that is responsible for much if not all of the advantages of quantum over classical systems in information processing is *entanglement*. This is also the reason why we dedicate significant time to its understanding, before we move on to study quantum algorithms, of a variational kind and not, quantum error correction, or notions of quantum networks.

While this may sound somewhat cryptic, it will become clear later what this means. This lecture will be accompanied by these lecture notes.

How to use these lecture notes: It is the point of these lecture notes to summarize the content of the course. Important definitions or results will be highlighted using boxes that look like this.

These lecture notes will be dynamically evolving along with the course and are not set in stone. This comes along with the advantage that not even the course content is fully set in stone, there is some flexibility here. The course is not based on any specific book. Having said that, a lot of content will be shamelessly copied from other sources, for which I apologize (but of course, credit is given then). These lecture notes are strictly meant to be of good use concomitant with the lecture and are only meant to fulfill this aim. They are no draft for a book in the making, they are raw, dirty, and incomplete. Still, they should fulfill a good purpose, I would think, while no copyright claim is made whatsoever.

1.1.3 Hints at literature

The subsequent list is by no means comprehensive, and just gives a few hints where to look for. Recommended general texts are the following.

- *Quantum computation and quantum information*, M. A. Nielsen and I. L. Chuang, Cambridge Series on Information and the Natural Sciences, 2000.

  This book is still remarkably up to date, given that it is 20 years old. It stayed away from hypes and fashions, and therefore, the content given has not aged much. It is still the definitive text on the subject matter, and also to my knowledge the most sold book of Cambridge University Press.

- *Quantum information theory*, M. M. Wolf, script of a lecture given in the WS 2005/2006.

  This script is excellent and will serve us as a guidance (and often more than that) for several parts of the course.

- *Quantum information theory – an invitation*, R. F. Werner, quant-ph/0101061.

  This is also an excellent and much shorter text. The compelling example of the impossible machines in the next section is taken from that text.

We will have a look at special literature as well, however, along the way.

1.2 Quantum information: A new kind of information?

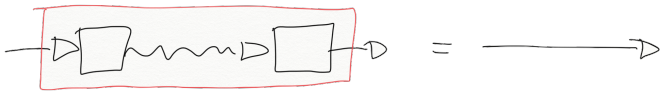
1.2.1 Carriers of information

Information theory usually abstracts from the underlying physical carriers of information: There is no "hard-drive information" any different from "newspaper information". And this for a good reason: This is because one type of information can be transformed into another one in a lossless fashion, and hence the actual physical carrier does not matter when it comes to thinking about what ways of processing of information are possible. Therefore, we can safely abstract from the carrier of information. There is only "one kind of information".

But how far does this idea carry if we allow for quantum systems as elementary carriers of information? The premise at hand is a simple one: Let us assume for a moment that "quantum information" is the same as classical information. The former is the type of information that is carried by quantum systems between preparation and measurement. We will denote this as a a wiggly line.

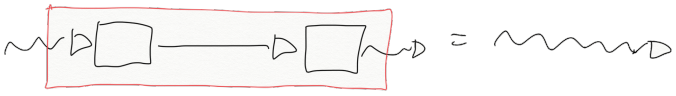
And if it is the same as classical information, it can be losslessly transformed into classical information and back. We will represent classical information as a straight line.

Can classical information be transformed into quantum information? Surely, this is called a preparation. We will not go into detail here, but it should be clear that the information encoded in a classical system can also be encoded in a quantum one. We can then transform this information back into classical information. This is called a measurement. We can think of the entire process and see that the classical particle coming in and out of the box contain the same information and are statistically distinguishable. Hence, we can "translate classical information into quantum information".

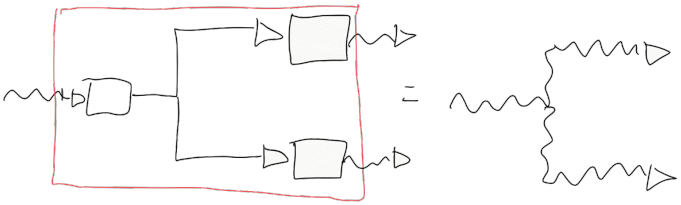


1.2.2 Impossible machines

But is the converse also true? Let us think what that would mean. It would mean that we had a quantum particle prepared in an arbitrary state. This quantum information would have to be translated into classical information, and then back to quantum information. This is a machine that we call *classical teleporter*. Before we continue, let us be precise for a moment what it means to translate quantum information into classical one and back in a lossless fashion. Since quantum mechanics is a statistical theory, it means that we cannot statistically distinguish the input from the output of the classical teleporter. Let us hence for a moment assume such we can losslessly translate classical information into quantum information and such a classical teleporter existed.

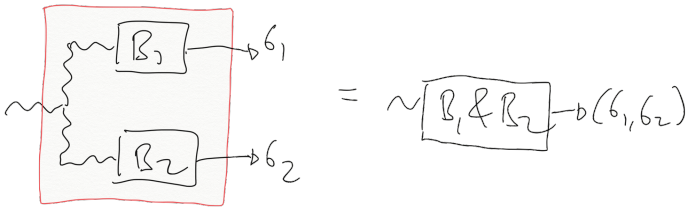


If we had such a device, we can also build a new device: A *quantum copier*. We can build that using a classical copier which does what we think it does: It takes classical information and makes two copies out of them. Since we have assumed that we can losslessly transform quantum into classical information, this means that we can, using this machine, also build a *quantum copier*: This again means that we have an input, and each of the outputs is statistically indistinguishable from the input. Having such a classical teleporter, it is perfectly possible to build a quantum copier.



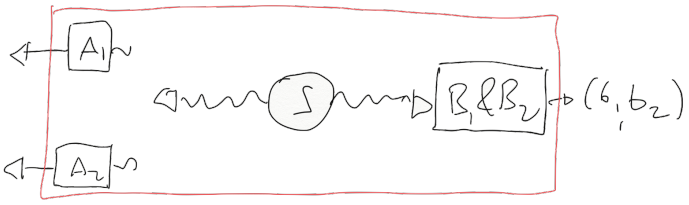
Yet again using this machine, we can build a *joint measurement device*: This allows us to perform arbitrary measurements of observables B_1 and B_2 on the same system, at the

same time. We will refer to this device as implementing the joint measurement $B_1 \& B_2$. Now one would think that it is not remarkable to be able to perform measurements on quantum systems. But the joint measurement device spits out results a with the same statistics as if we had only measured B_1, as well as outcomes b_1 again with the same statistics if we had only measured B at the same time. Only that in each measurement, the pair (b_1, b_2) is generated, as $B_1 \& B_2$ are measured at the same time. Again, from the classical teleporter over the quantum copier, we can build such a machine.



So far so good. We will now construct a last machine out of this, which we will call *Bell's telephone*. There is a good reason that we call it Bell's telephone. The argument that we are going through now is based on Bell's theorem, one of the most important statements that relate to quantum physics. We will here use it in a slightly different and paradoxical way.

To remind you, the setting of Bell's theorem is a distributed one, where two parties, let us name them Alice and Bob, have two measurement apparata at their disposal. Alice can make use of A_1 or A_2, while Bob can use B_1 or B_2. Each of these measurement devices produces the result ± 1. It may be convenient to think of these apparata as Stern-Gerlach-type apparata.



We will denote by $P(a, b|A_i, B_j)$ the probability for Alice to obtain result a and Bob to see b, in a measurement in which Alice makes use of A_i and Bob of B_j. This is a correlation measurement. We will now define the correlation coefficient of such a measurement in which Alice resorts to A_i and Bob to B_j as

$$C(A_i, B_j) = \sum_{a,b} abP(a, b|A_i, B_j). \tag{1.1}$$

It is easy to see that this takes values between -1 and 1. The combination

$$\beta = C(A_1, B_1) + C(A_1, B_2) + C(A_2, B_1) - C(A_2, B_2) \tag{1.2}$$

has a particular significance, as it features in a reading of Bell's inequality. In fact, the CHSH Bell inequality precisely states that

$$\beta \leq 2. \tag{1.3}$$

It is important to note that usually Bob cannot tell from the data he obtained whether Alice has chosen the apparatus A_1 or A_2. On the formal level, this is reflected by the constraint

$$\sum_a P(a,b|A_1,B_j) = \sum_a P(a,b|A_2,B_j) =: P(b|B_j). \tag{1.4}$$

Let us now come back to our theme of machines: Let us assume that Bob now makes use of a joint measurement device $B_1\&B_2$ that allows him to measure B_1 and B_2 at the same time, producing outcomes (b_1,b_2), again with the same statistics as if B_1 and B_2 were measured separately. More formally put, this means that the probabilities

$$p_i(a_i,b_1,b_2) = P(a_i,(b_1,b_2)|A_i,B_1\&B_2) \tag{1.5}$$

when Alice chooses apparatus A_i have to fulfil

$$\sum_{b_1} p_i(a_i,b_1,b_2) = P(a_i,b_2|A_i,B_2), \tag{1.6}$$

$$\sum_{b_2} p_i(a_i,b_1,b_2) = P(a_i,b_1|A_i,B_1), \tag{1.7}$$

for $i=1,2$. How can we turn this into a telephone? We follow the subsequent protocol:

> Suppose Alice wants to send a bit to Bob. If her bit is 0, she makes use of A_1, if it is 1, she resorts to the apparatus A_2. Then Bob, far away, performs a joint measurement $B_1\&B_2$ to get (b_1,b_2) and interprets it as "A_1" whenever $b_1=b_2$ and as "A_2" if $b_1\neq b_2$.

We denote with $p_{\rm ok}$ the probability that Bob is actually right with his guess, assuming that the bits that Alice encodes are uniformly distributed, so that the bits are chosen with probability $1/2$ each. Let us assume for a moment that Alice takes A_1, then Bob will be right with his guess with probability

$$\sum_{a_1,b_1,b_2} \frac{b_1+b_2}{2}|a_1|p_1(a_1,b_1,b_2). \tag{1.8}$$

Here, the first factor takes into account the condition $b_1=b_2$, while the second one is introduced here for a later use, as clearly $|a_1|=1$. In total, averaged over the random bits, we have

$$p_{\rm ok} = \frac{1}{2}\sum_{a_1,b_1,b_2} \frac{|b_1+b_2|}{2}|a_1|p_1(a_1,b_1,b_2) \tag{1.9}$$

$$+ \frac{1}{2}\sum_{a_2,b_1,b_2} \frac{|b_1-b_2|}{2}|a_2|p_2(a_2,b_1,b_2). \tag{1.10}$$

Using that obviously, $|a_1| \geq a_1$ and $|a_2| \geq a_2$, we find

$$\begin{aligned} p_{\rm ok} &\geq \frac{1}{4} \sum_{a_1,b_1,b_2} (b_1 + b_2) a_1 p_1(a_1, b_1, b_2) \\ &+ \frac{1}{4} \sum_{a_2,b_1,b_2} (b_1 - b_2) a_2 p_2(a_1, b_1, b_2) \\ &= \frac{1}{4} \left(C(A_1, B_1) + C(A_1, B_2) + C(A_2, B_1) - C(A_2, B_2) \right) \\ &= \frac{\beta}{4}. \end{aligned} \tag{1.11}$$

Bob will guess better than chance whenever $p_{\rm ok} > 1/2$: Then he can in fact using an appropriate coding to deterministically receive bits. This will be guaranteed as soon as $\beta > 2$, i.e., as soon as the CHSH Bell inequality is violated. Experiments find for suitable preparations of (entangled) states $\beta = 2.8$. That is to say, if Bob could indeed perform a joint measurement, then Alice and Bob could signal and send bits faster than the speed of light, fiercely violating relativity and causality. So this machine must be an impossible machine.

But we have made no other assumption than that quantum information can be losslessly transformed into quantum information, at the hand of the classical teleporter. We must conclude that this is also an impossible machine. And, after all, the following is true. It will be the point of the rest of the course to find out what that means.

Quantum information: Quantum information is a different kind of information.