THM | CAMPUS GIESSEN
TECHNISCHE HOCHSCHULE MITTELHESSEN

MNI
Mathematik, Naturwissenschaften und Informatik

- Quantum Computing -
Script Spring 2020
Teacher: Prof. Dr. Bettina Just

Script edited
by

Dupleix Takoulegha, Markus Kretsch, Bettina Just, Stephan Weyers

Preface

About this script:

This script was created for the first time in German language during the lecture "Quantum Computing", which was held in spring 2014 at the departement MNI of the THM (Technische Hochschule Mittelhessen) as a master course in computer science. Since then, there is a lecture about quantum computing almost each year at THM.
The area of quantum computing is developing quickly, so the script is adjusted for every new lecture. In spring 2018, many options for programming quantum algorithms online or with freeware were added. The course then was offered as a BSc module for the first time. In spring 2019, for the first time the quantum algorihtms were illustrated also graphically. The method for graphical illustration has been invented by Bettina Just and was published as a Book of Springer in November 2020 (ISBN 9783662618882). In 2020, moreover, the course was given as an online-lecture.
In autumn 2020, the script was translated to English by FH Dortmund. A lecture using the script is to be hold as a course for home and international students in Dortmund.

..... Dear yet unknown teacher, please enter your comments here :). And please add your own ideas to the script.

Bettina Just, November 2020

Contents

1 Quantum Computing in the (Computer Science) World

Origin: quantum physics: Theory developped rooughly in the years $1905 - 1935$. Main players and results:

Planck (radiation law / quanta of of matter or electricity, Nobel Prize 1918),

Heisenberg (uncertainty relation, Nobel Prize 1932),

Schrödinger (cat, and his famous equation, Nobel Prize 1933),

Einstein (photoelectric effect, Nobel Prize 1921),

Born (Copenhagen Interpretation, Nobel Prize 1954),

....

Aim: Description of the processes in the subatomic area.

Question (more specific): How do light "particles" behave? Observation is difficult, since thex are so small that observation may change their state. [1] Therefore often results are statistical and not on a single sspecific electron (but not exclusively).

Experiments: Only the development of the laser made experiments with individual light particles possible. The more laser beams became scalable, the better the experiments.

Main result: It turns out, that quantum particles are

- either not "local". That is, there is an interaction faster than light speed (current experiments: with at least 10,000 times the speed of light, source Wikipedia "Quantum entanglement") between them in certain cases,
- or not "realistic". This means that particles do not have certain physical properties (such as the direction of rotation "spin"), but rather have several of these properties at the same time, and only take a specific one when measured.

Both contradict our classical mechanistic worldview. Therefore:
Bohr: "Anyone who is not appalled by quantum physics has not understood it."
Feynman: "If you think you understand quantum mechanics, you don't understand quantum mechanics."

But experiments repeatedly confirm quantum mechanics and never contradict to it. (Will be deepened in the lecture).

[1] Imagine if Newton could only have observed the properties of falling apples by throwing other apples on them.

Step into IT: Richard Feynmann asked the question, whether quantum mechanics can be computed by classical computers. It turns out that this is not possible. One reason is: Quantum mechanics requires truely random numbers, but computers are deterministic.
So the question arises how to build a "quantum computer", that will be able to compute quantum mechanics.
This was the beginning of the discussion on the computational model of a quantum computer, and of its underlying quantum circuits.
Final definititon of computational model and the "quantum gates" was delivered by Deutsch, 1985.

However, quantum computing was a side issue, both hardware side and software side, until Peter Shor published a quantum polynomial time algorithm for the factorization of natural numbers in 1994. Since then, quantum computing has been studied intensively - on the hardware and software side.
Reason: Fast factorisation breaks the the RSA scheme. RSA is the mostly used encryption system for internet security. So, a quantum computer would not only be able to decipher actual messages in internet, but also all old ones stored at some place.
(There is therefore now the new field of post-quantum cryptography: It develops methods that are immune to quantum computers because they are based on NP-complete problems).

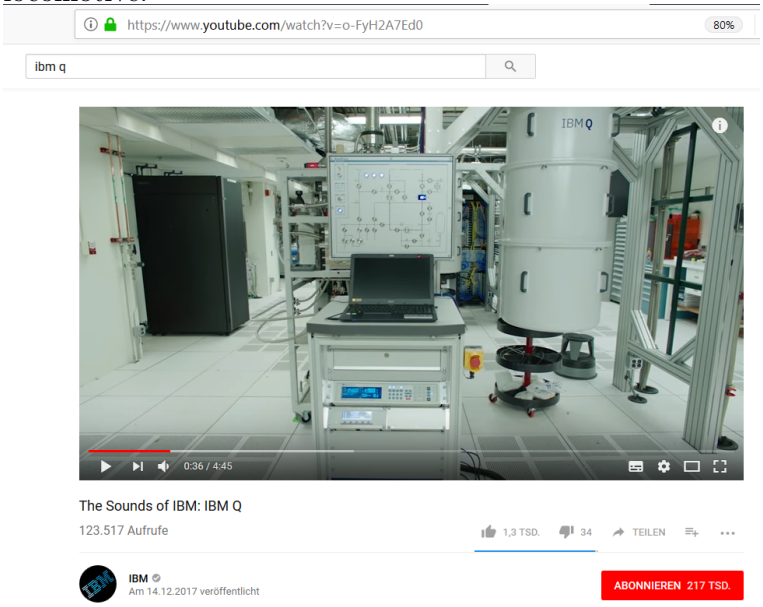
Hardware: Realization of Quantum bits ("qubits" for short) by:

- Trapped ions;
- SQUIDS (systems made of superconductors).
- polarized photons
- Nuclear Magnetic Resonance

Recent developpements: Spring 2018:

- Google presents Google Bristlecone, 72 qubits on a chip
- Intel presents chip with 49 qubits

- ... But a chip doesn't make a computer. Quantum computers were entire rooms, mainly because they have to be cooled to -272 degrees. IBM's Q sounds like a steam locomotive:



Spring 2019:

- IBM presents for the first time a stand alone quantum computer, a cube with a side length of 2 m, the IBM-Q system one.
- D-Wave has an adiabatic quantum computer (with a different calculation model, a completely different approach - some say it sails under a false flag) with over 2000 (target: 4096) bits. Just three years ago, many believed that this was the real future of quantum computing. In the meantime the original calculation model has caught up again and is called "Quantum Technology 2.0".
- **n QBits have the computing power of 2^n normal bits in the same time**

Hardware problem: Instability of the state of quantums leads to a high susceptibility to errors.
The more qubits, the more likely they will interact with each other or with the environment, and then the calculation will be wrong. They are very difficult to isolate. So actual research on the software side

i.) workes on error-correcting algorithms, and

ii.) workes on hybrid algorithms: quantum processors with 50-100 QBits collaborate with classical computers.

The main players:

- Secret services (presumably).
- Google. Bought a D-Wave in 2013 and presented a quantum chip with 72 QBits in 2018. Working in both quantum computing worlds. The goal of Google is to achieve "Quantum Supremacy" , i.e. to have a quantum computer that is better than conventional computers.
  (In 2019 google claimed that with a certain problem, quantum supremacy had been proven. They found a problem that could be solved faster by a quantum computer than by a conventional computer. The task is basically the simulation of a quantum computer. A mocker then wrote his coffee cup is superior to a quantum computer, because it can simulate the splintering of a coffee cup falling on the floor better than a quantum computer.)
- IBM. Up to now the only alone standing quantum computer, IBM-Q, for only for research institutions - it does not yet meet commercial requirements for storage space and correctness. IBM has a Q-Network: Everyone can run own quantum algorithms on up to 20 qubits on IBM-Qs, accessing them via internet on a normal browser. So far 1.7 million experiments from over 60,000 users had been done.
- Microsoft. Want to be equipped with Q #, development platform for quantum algorithms based on Visual Studio, freely available.
- Python: The Python library CIRC for quantum algorithms has existed since 2019.
- Intel. Presented a 49-QBits chip in March 2018.
- The EU. Launched the project "Quantum Technology Flagship" with a volume of EUR 1 billion in mid-2017 (with the sub-areas communication, computing, sensoring, simulation). The first joint conference was in spring 2019, the second online in autumln 2020. EU also focusses on quantum outreach.
- China. Have announced that they will invest 10 billion dollars in the technology (info from January 2018). Are pioneers in technology with photons, for quantum communication and quantum internet.
- Canada. Have the "Canadian Institute for Quantum Computing" since 2016 with start-up funding of 300 million dollars - and D-Wave with an "adiabatic" quantum computer, that uses another model of computation.

- Universities: For a long time above all the University of Innsbruck with scientifically verifiable results.
- Countless other universities, e.g. Berkeley found out in 2010 that plants use quantum effects for photosynthesis - without consuming energy.

World record for teleportation (non-locality): One of the most spectacular applications of quantum computing:

1997 Zeilinger's group in Vienna: First teleportation in the laboratory.

2003 Gisin's group in Geneve: Teleportation over 55m, for the first time outside of laboratory;

2004 Zeilinger's group: Teleportation over a distance of 600m, from one bank of the Danube river to its other bank;

2010 Xian Min Lin's group in Shanghai: Teleportation over 16 km;

2012 Chinese University of Science and Technology with Pan Jian-Wei: Teleportation over a distance of 97 km;

2012 Zeilinger's working group: Teleportation over a distance of 143 km between La Palma and Tenerife;

2017 International working group, i.a. with the participation of Zeilinger and Pan Jian-Wei: Teleportation over 1400 km from Earth to the Chinese quantum satellite Micius;

2017 same working group: 7600 km between Austria and China.

Recent research: Bridging ultra-small distances instead of particularly large ones, for use inside of the computer itself.

World records factoring a number with quantum computers:
2001: 15 factorized (IBM San Jose, trapped ions)
2011: 21 factorized (Univ. Bristol, photons)
2012: 15 factorized again (Univ. California, superconductivity)
2016: 15 factorized again, with 5 instead of 12 QBits (Trapped ions Univ. Innsbruck)
(Remark: Classical computers can factor numbers with over 200 decimal digits easily, D-Waves adiabatic quantum computer can factor numers wit about 7 decimal digits).

Application areas:

- Optimization problems - are solved approximately
- Inverting (one way) functions - can be used for database search
- Simulation of molecules, design of matter
- Big Data Analysis

- Artificial intelligence - still a long way off. Some say this will never be something, others see it revolutionize the world in 5 years and put human intelligence in the shade. The 5 year deadline has been in effect for a long time ;).

Objectives of the lecture: (as stated in the module description)
The students

- Know the differnece between bit and qubit;
- have an idea of quantum entanglement an know the experiments to prove it;
- know the computational model of quantum computing;
- are able to program simple quantum algorithms;
- are also informed about the most important quantum algorithms, their meaning and possible applications;
- know the current situation of the hardware of quantum computers and are thus able to classify information about new developments in quantum computing.

Focus of the lecture : Computational model and basic algorithms.

Computational model of quantum computing is different from the classical computational model (Turing machine), since quantum bits (qubits for short) are different from classical bits. Here is what bits and qubits are, and what are their main differences:

Classical bit: Object that can have exactly two different states, 0 and 1.
Classical circuits are operating with boolean algebra gates on classical bits. They are the basis of classical computers.

Different physical implementation options:
- Wire that has no current or carries current.
- Lamp that lights up or doesn't light up. (From the early days of computer hardware) - Pointer (like the hand of a clock on a dial) which can assume the two positions horizontal or vertical.

The following two properties of classic bits are so self-evident that they are usually not mentioned at all:

- (Realism for bits)
  The value of a bit is clearly defined at each point in time of the calculation. It can be read out and the readout process does not change the value.
- (Locality for bits)
  Changing the value of a particular individual bit does not change the value of any other bit in this moment.

Both properties come from classical mechanics:

- (Realism)
  Objects have properties such as weight, their color, their speed or size, which can be measured and which are not changed by measurement.

- (Locality)
  An action at one point in space does not directly affect physical objects at another point in space. Effects must be transmitted through light or matter, and therefore need at least runtime of light between the two points in space.

Quantum bit: Can take the values $|0\rangle$ or $|1\rangle$ or anything in between.
Quantum circuits are operating with quantum gates on quanatum bits. They are the basis of quantum computers.

Different physical implementation options:
- Photons, trapped ions, superconductivity ...
- Pointer (like clock hands on a dial), which can assume the two positions horizontal or vertical or anything in between.

Quantum bits do NOT have the properties of realism and locality from classical mechanics, but they have the following properties (both are the essential ingredients for quantum computing):

- (Change when measuring)
  If a quantum bit is measured, it delivers one of the two values $|0\rangle$ or $|1\rangle$, and never a value in between. Measurement changes the value of the quantum bit (if it was between $|0\rangle$ and $|1\rangle$ and not exactly one of them).

- (Quantum entanglement)
  A change in a quantum bit at a point in space can change the properties of another quantum bit instantenously (i.e. faster than with light speed).

Classical computer science does not allow objects to change their properties through measurement, but the phenomenon is known in the world around us. There are situations in which the measurement itself changes the situation, e.g. in the quality inspection of components. If a load test is carried out here, the component is no longer as resilient as before. And whoever has children knows they will behave differently when they are being watched.

However, the phenomenon of quantum entanglement is so incredible that it was called by Einstein spooky action at a distance and Bohr allegedly said:
“Anyone who is not appalled by quantum theory has not understood it.”

The properties of the smallest particles can change like the properties of an heir to the throne: He becomes king the moment the old monarch dies. He is immediately king - faster than light needs to overcome the distance between him and the old monarch.

How is the spooky action at a distance proven?
And how does the calculation model of quantum computing work, when it is based on qubits, which have such strange properties?

That is the content of the next chapters.

2 The Model of Computation

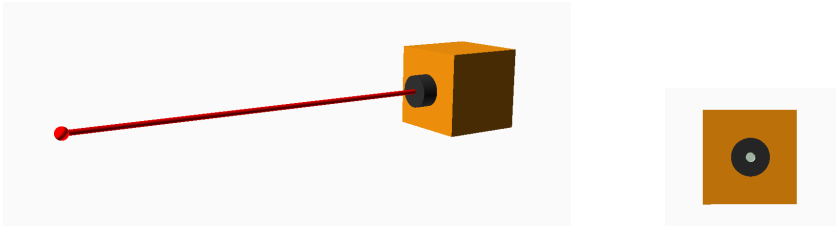
2.1 Physics: Particles communicating ultrafast

In this chapter the (idealized) experiments are presented, which show that qubits do NOT have the properties of realism and locality.

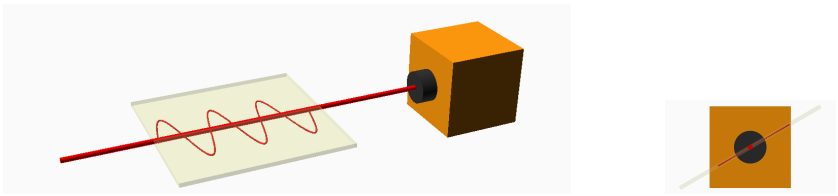
The train of thought goes back to Einstein, Poldolsky and Rozen (1935). Their work was thought experiments. At their time, experimental physics was not yet advanced enough to indeed run the experiments.
In the meantime since then, the experiments have carried out very often, and they delivered the results forecasted in the thought experiments.
Here the experiments are considered idealized. That is, details of the technical implementation, handling of measurement errors etc. are left out of consideration.

For the purpose of this lecture, the particles are photons (light particles). Nowadays, they con be be produced one at a time with a laser. Photons are one example of the physical implementation of qubits (others are superconducting mini-circuits, of trapped ions).

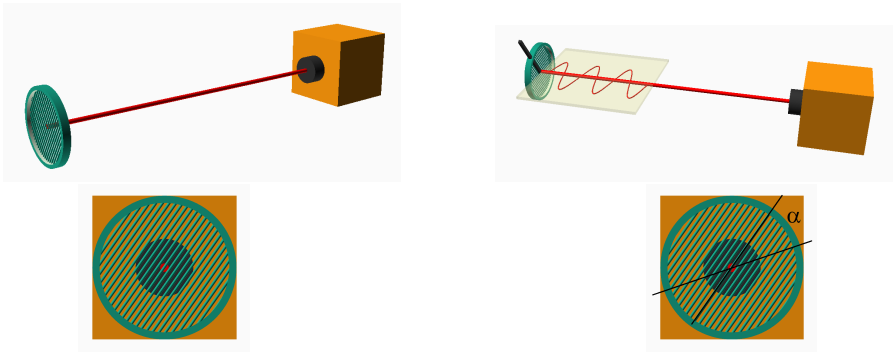
Definition: A photon is (for this lecture) a point-like object that comes out of a box and flies away along a straight line (in its direction of propagation). The following figure shows the situation from the front and from the side.



The photon can (but not necessarily must) have a polarization. This means that it is vibrating within a plane. The plane also contains the line of propagation of the photon.



Definition: A photon can be measured with a polarizer (imagine a refrigerator grille for visualizing the polarizer).



There are two possible results of the measurement:

- Either the photon passes the polarizer. Then it continues flying away in its original direction of propagation, but now is is polarized in the direction of the polarizer.
- Or the photon is absorbed by the polarizer. (Lateron we will imagine that it still flies further, but is polarized perpendicular to the angle of the polarizer).

When does which measurement result occur?

- If the photon is not polarized (or we do not know its polarization), the probability for "passes" and "is absorbed" for each angle of the polarizer is 1/2 .
- If the photon is polarized, the probability for "passes" is the greater, the smaller the angle α between its polarization and the polarization of the polarizer. (Imagine a frisbee passing or not passing a manhole cover).

  If $\alpha = 0$, the photon always passes.

  If $\alpha = 90°$, the photon never passes.

  If $\alpha = 45°$, the photon passes with probability 1/2.

  In general, the photon passes with probability $(\cos \alpha)^2$. The probabilities mentioned above already follow from this. Moreover:

  If $\alpha = 30°$ the photon passes with probability 3/4, and

  If $\alpha = 60°$ the photon passes with a probability 1/4.

Comment:

i.) Measuring in most cases changes the particle (qubit)!

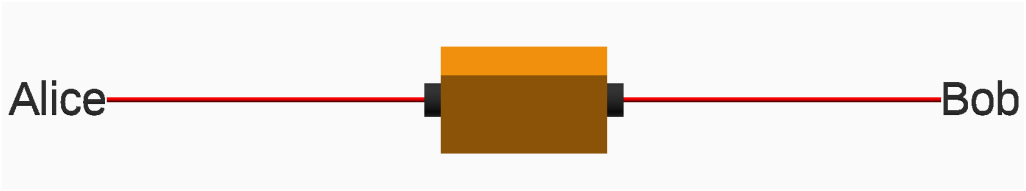
ii.) The definition fits with the law of Malus, cited here from German Wikipedia (as of July 24, 2019):
"The law of Malus (after Etienne Louis Malus), more rarely also called Malus' law, describes the intensity I of a linearly polarized wave of initial intensity I_0 after passing through an ideal polarizer as a function of the angle α, by which the optical axis of the polarizer is rotated against the direction of polarization of the wave: $I = I_0 \cdot \cos^2 \alpha$

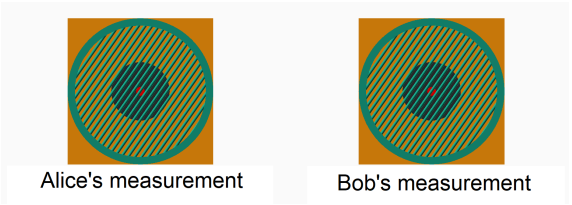
The transmitted radiation is polarized in the direction of the filter, the remaining intensity (proportional to $\sin^2 \alpha$ is absorbed ... ."

iii.) In the lecture the experiment on the law of Malus is illustrated with the help of a refrigerator grid and a pencil.

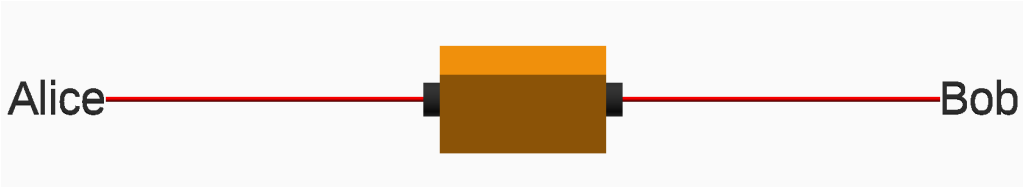
Objective now: Understand how the phenomenon of quantum entanglement is demonstrated in (idealized) experiments.

Experimental setup in all three experiments: A source creates pairs of photons that fly away in two opposite directions and are then measured first on side A (Alice's side), then on side B (Bob's side). The experiments differ in how the particles are generated and at what angle they are measured by Alice and Bob.



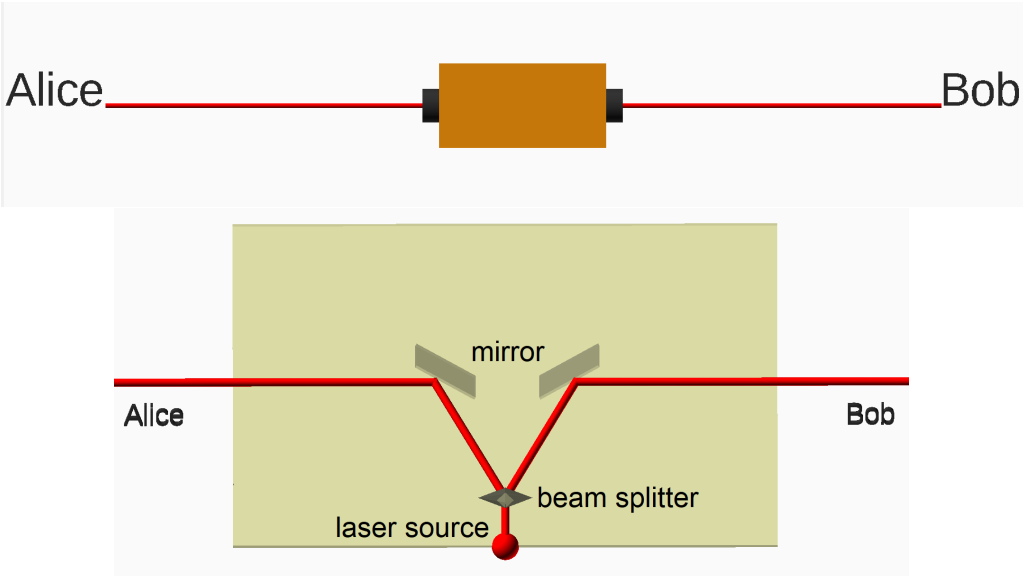


Experiment 1: Pairs of independent particles, measured first at side A (by Alice), then at side B (by Bob), both at the same angle α:



Result (for each angle α): proportion of passing particles is on each side 1/2; no statistical correlation.

Experiment 2: Like experiment 1, but now the pairs entangled.
This means: They are not generated independently, but come from one single original photon, which is sent through a "entanglement crystal" (a kind of beam splitter) and thereby splits into the two photons. (Entangled particles can be produced since the early decades of 20th century. The exact way how to do this is not subject to this lecture).



As in experiment 1, measurements are taken on both sides at the same angle α, where α can be any arbitrary angle (measurement first on side A, then side B).
Result (for each angle α): The proportion of passing particles is on each side 1/2,
but:
Complete correlation of the pairs.

The following applies to every pair and every angle:
Either both pass, or both are absorbed. This is the case even if the angle is determined so late in the experiment, that any communication between the particles would have to take place with velocity faster than the speed of light c (currently: more than $10.000 \cdot c$, quoted from Wikipedia, quantum entanglement).

Possible explanations:

1. Einstein's explanation for this "spooky action at a distance": There are "hidden variables" in the particle pairs which determine the measurement results for each angle α already at the moment the take off from the beam splitter.
   Einstein demanded: How can quantum mechanics be expanded to include these hidden variables? (Einstein-Podolsky-Rozen, EPR, 1935).

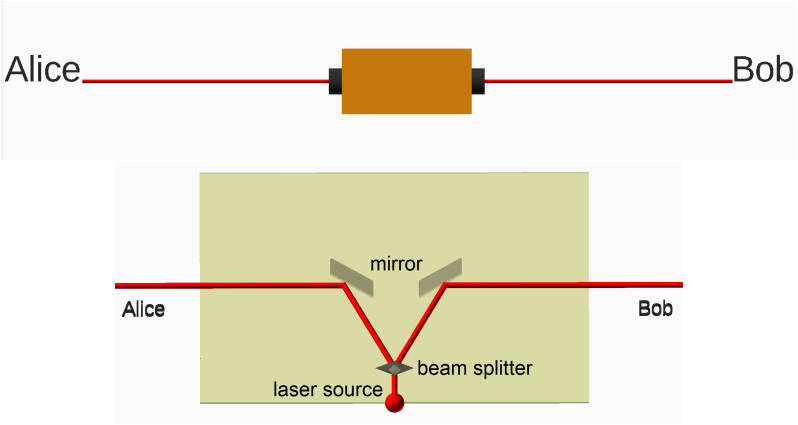
2. Interpretation of quantum mechanic nowadayss: It is not certain from the start whether the particles will pass or not - here real randomness takes place. But in the moment when Alice measures, and her particle therefore gets the polarization in the direction α (or $\alpha^{\perp}$), Bob's particle INSTANTANEOUSLY, at this moment, takes the same polarization. Measuring in the direction α therefore necessarily gives the same result.

   That sounds absurd, how are the two particles able to communicate with such an excessive speed?

   For a single photon this interpretations also significates: Non-realism:
   For the angles α not equal to $0°, 90°, 180°$ and $270°$, a single particle does not have one of the states "passes" or "is absorbed"', but both at the same time (both are possible results). Only with the measurement it assumes one of the states and then oscillates at an angle α or $\alpha + 90°$. (Slightly similar situation in world of human behaviour: Voters who do not yet konw how whom to vote for - only with their measurement (filling the ballot paper) they are voters of one specific party).

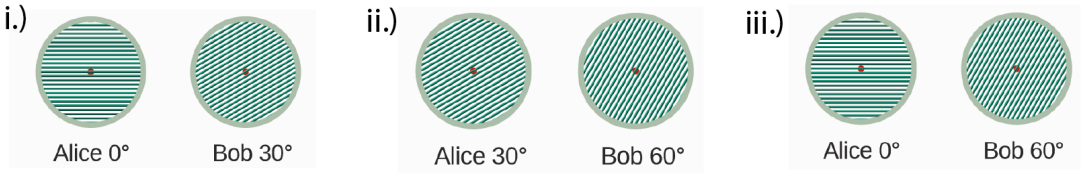
   For the interaction among the particles the result of experiment 2 means: Non-locality:
   The measurement of one particle of an entangled pair of particles instantaneously changes the polarization of the other.

Experiment 3: Two entangled (as in experiment 2) qubits are sent out in opposite directions, to Alice and Bob.



They are first measured randomly by A at 0° or 30°, then immediately measured by B at 30° or 60° - so fast that communication with speed between the location of A and the location of B in speed $\leq c$ is impossible. Test results in which both measured in the direction of 30° are not considered further (these were already dealt with in test 2).

So, the following measurements are can take place:



In order to see whether quantum mechanics is right with its spooky action at a distance, or whether there are hidden variables, the following question is then asked (according to Bell, 1965):

Question: Which part of all measurements answers "yes" to the following question?

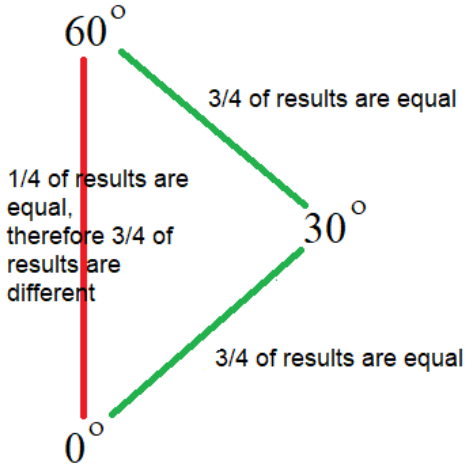
- If Alice measured at 0 degrees and Bob at 30 degrees, are the results of both measurements the same?
- Otherwise, if Alice measured at 30 degrees and Bob at 60 degrees, are the results of both measurements the same?
- Otherwise, if Alice measured at 0 degrees and Bob at 60 degrees, are the results of both measurements different?

Idea behind the question: Quantum theory says (where "most" here means "a proportion of 3/4", but let's leave it at "most" for the sake of understanding the idea):

i.) If Alice measures at 0 and Bob measures at 30, "most" results are the same.

ii.) If Alice measures at 30 and Bob measures at 60, "most" results are the same.

iii.) If Alice measures at 0 and Bob measures at 60, "most" results will be different.



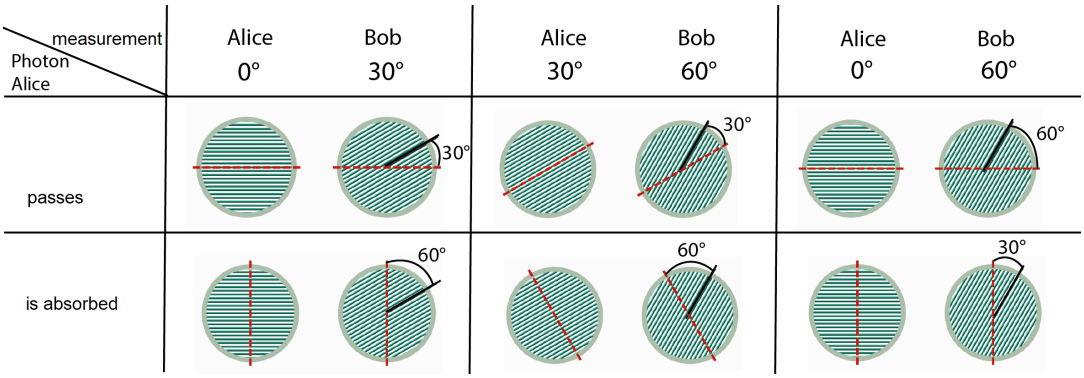
Theory of hidden variables says: If for 0° and 30° "mostly" produce the same results, and for 30° and 60° "mostly" produce the same results, then for 0° and 60° they have to

produce “mostly of mostly” - thus still often - the same results.

Result (quantum theory + experiment):
In the experiment, after experiment 3, the question is statistically answered with “yes” in 3/4 of all cases.

First it is shown that this corresponds perfectly with the quantum mechanical interpretation.

The following measurement results are theoretically possible:



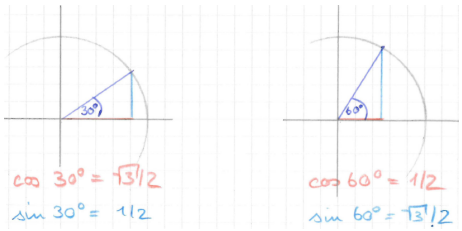
- Bob’s qubit behaves in the following way for the various measurements:

  If the difference angle to Alice’s measurement is 30° (i.e. if he measured at 0° and Alice at 30°, or if he measured at 30° and Alice at 60°), then behaves a statistical part of 3/4 just like the qubit in Alice. That is, in 3/4 of the pairs both pass or both are absorbed. With 1/4 of the pairs, both qubits behave differently.

  If the difference angle to Alice’s measurement is 60° (i.e. if Bob measured at 0° and Alice at 60°), then a statistical part of 3/4 behaves differently than the qubit for Alice. That means, with 3/4 of the pairs the qubit passes with Alice and that with Bob is absorbed, or vice versa. With 1/4 of the pairs, both qubits behave in the same way.

- This observation is perfectly explained by the quantum mechanical interpretation. This since: If Alice’s measurement result gives the result’s polarisation to Bob’s qubit assumes the polarization of Alice’s qubit, and then Bob’s qubit is measured at a difference angle of 30°, it will with probability $\cos^2 30° = 3/4$ behave exactly like Alice’s qubit. If the difference angle is 60°, then with probability $\cos^2 30° = 3/4$ it will behave opposite to Alice’s qubit. (→ below [1] for the memory of sin and cos)

[1] memory sin and cos involved angles:



The question now is, wheater this behaviour can be explained with local hidden variables. But John Bell 1965 showed, that this is not possible.

Proposition, John Bell 1964: Quantum mechanics cannot be extended with local hidden variables.

Proof: We assume that every qubit pair of experiment 3 already in the moment of take off "knows" for each angle whether it will pass or whether it will absorbed. Then the hidden variables for each pair of qubits are one of the following 8 possibilities:

0 °	30 °	60 °
is absorbed	is absorbed	is absorbed
is absorbed	is absorbed	passes
is absorbed	passes	is absorbed
is absorbed	passes	passes
passes	is absorbed	is absorbed
passes	is absorbed	passes
passes	passes	is absorbed
passes	passes	passes

Now, for each assignment we ask whether the measurement results for Alice and Bob are the same (with a difference angle of 30°) or different (with a difference angle of 60°). This can be read out from the table immediately:

0°	30°	60°	Alice 0 Bob 30 Are results equal?	Alice 30 Bob 60 Are results equal?	Alice 0 Bob 60 Are results different?
is absorbed	is absorbed	is absorbed	yes	yes	no
is absorbed	is absorbed	passiert	yes	no	yes
is absorbed	passes	is absorbed	no	no	no
is absorbed	passes	passes	no	yes	yes
passes	is absorbed	is absorbed	no	yes	yes
passes	is absorbed	passes	no	no	no
passes	passes	is absorbed	yes	no	yes
passes	passes	passes	yes	yes	no

One realizes:

- for each triple of hidden variables, and for each way of fixing Alice's and Bob's measurements, the probability of the answer of "yes" to the question, is at most 2/3.
- Therefore a statistical mean of 3/4 is impossible - independently of the weights given to the various tripeles and measurements.
- So, the quantum mechanics explaining the observed experimental results cannot be augmented with hidden variables.
- Hidden variables are possible only if the measurements are dependent on the hidden variables. This is only possible, if there is no observer, who's will is independet of the photons emitted.

Conclusion: World is not "' local "'or not" 'realistic"' (terms from EPR work):

- "Local" means: Nothing (including no information) moves faster than c.
- "Realistic" means: properties of physical objects are fixed, regardless of whether someone perceives them.

Note:

i.) John Bell was nominated for the Nobel Prize in Physics in 1990 for the formulation of the "Bell's inequality" and the proof that quantum mechanics violated it. Unfortunately died before the decision. Bell's inequality generalizes the experimental setup described above to any angle (see Wikipedia article on this, fairly easy to understand).

ii.) Experiments to prove the violation of Bell's inequality have existed since the late 1960s. There are still some being made.

iii.) A lot of work is done on the way from the idealized experiment to real experiments (so-called "filling up loopholes").

iv.) Finally physicians accept: qubits can "coordinate" in some way with velocity faster than the velocity of light. So it doesn't make sense to speak of the properties of a single qubit - qubits have to be considered as a system.
This is very interesting for computer scientists. Self-organizing systems have completely different properties than individual objects. The system is more than the sum of its parts.

2.2 Computer science: The model of computation

2.2.1 Quantum registers

Learning outcomes:

i.) Understand what is a quantum bit in computer science (algebraic representation + graphical representation).

ii.) Understand what is quantum register with n qubits (algebraic representation as the sum of basis states, graphical representation for $n \leq 3$, and representation as a coefficient vector, e.g. for Matlab).

iii.) Being able to compute the states of quantum registers of unentangled qubits.

iv.) Know the difference between entangled and non-entangled register states.

v.) Knowing the outcome of measurement of one or more qubits in a quantum register (be able to calculate it, and have a graphic representation in mind).

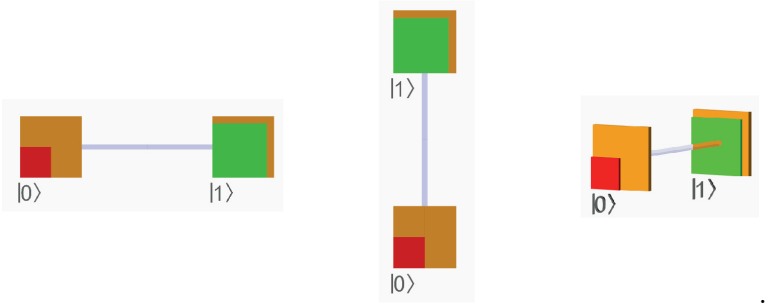
Definition: A qubit $|q\rangle$ is an object that has a state $\beta_0 \cdot |0\rangle + \beta_1 \cdot |1\rangle$, where $\beta_0, \beta_1 \in \mathbb{C}$ (in this lecture almost always: $\beta_0, \beta_1 \in \mathbb{R}$) and $|\beta_0|^2 + |\beta_1|^2 = 1$. $|0\rangle$ and $|1\rangle$ are called basis states or pure states. β_0 and β_1 are called probability amplitudes.

Measuring the qubit delivers the basis state $|0\rangle$ with probability $|\beta_0|^2$, and delivers basis state $|1\rangle$ and with probability $|\beta_1|^2$ the . After the measurement, the qubit is in the corresponding basis state.

Gimmick in the lecture: Imagine, everyone "is" or "has" a qubit What happens, if someone comes around and measures.

Definition : Graphical presentation of the qubit $\beta_0 \cdot |0\rangle + \beta_1 \cdot |1\rangle$:
Connect two unit squares with a line. Label one of the squares with $|0\rangle$, the other with $|1\rangle$. In the square labeled $|0\rangle$ draw a square with side length $|\beta_0|$, in the square labeled $|1\rangle$ a square with side length $|\beta_1|$ Squares green for positive β, red for negative β.

Example for the qubit $-0.5 \cdot |0\rangle + \sqrt{3/4} \cdot |1\rangle$ (three different representations - the arrangement in the room does not matter at the moment):

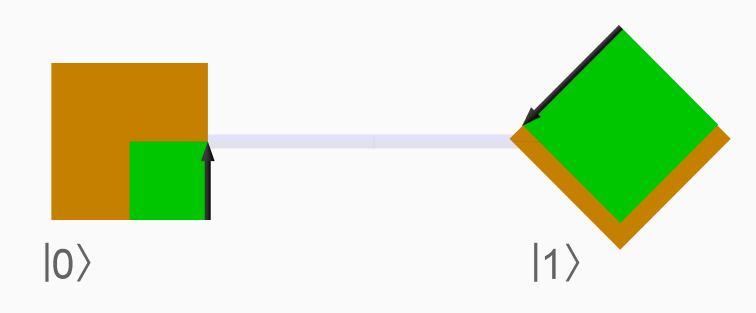


.

Measuring delivers one of the states, the square is then completely red or green (will be explained later in detail).

Remark: Graphical representation of the qubit $\beta_0 \cdot |0\rangle + \beta_1 \cdot |1\rangle$, if β_0 and β_1 are complex numbers (basisd on Feynman's QED):
No colors necessary. The amplitutes are shown as if they where in Gaussian plane, the squares are attached to the left side of the arrow, therefore are rotated.

Example for the qubit $0.5 \cdot e^{i\pi/2} \cdot |0\rangle + \sqrt{3/4} \cdot e^{i \cdot 5/4\pi} \cdot |1\rangle$:



.

Definition: A quantum register $|q_1 q_2 \cdots q_n\rangle$ with n qubits $|q_1\rangle, |q_2\rangle, \cdots, |q_n\rangle$ is an object that has a state

$$\begin{array}{rrl} & \alpha_0 & \cdot|0\ 0\ \cdots\ 0\ 0\rangle \\ + & \alpha_1 & \cdot|0\ 0\ \cdots\ 0\ 1\rangle \\ & \vdots & \\ + & \alpha_{2^n-1} & \cdot|1\ 1\ \cdots\ 1\ 1\rangle \end{array}$$

with $\alpha_0, \cdots, \alpha_{2^n-1} \in \mathbb{C}$ (here mostly: $\in \mathbb{R}$), where $|\alpha_0|^2 + \cdots + |\alpha_{2^n-1}|^2 = 1$.

The states $|0\ \cdots\ 0\ 0\rangle, |0\ \cdots\ 0\ 1\rangle, \cdots, |1\ \cdots\ 1\ 1\rangle$ are called basis states of the register, the coefficients $\alpha_0, \cdots, \alpha_{2^n-1}$ (probability) - amplitudes of the basis states. (Reminds some people of the table of values of a Boolean function with n inputs :).)

Notation:

$$\begin{aligned} |0\ \cdots\ 0\ 0\rangle &:= |0\rangle \cdot |0\rangle \cdot |0\rangle \cdot \cdots \cdot |0\rangle \\ |0\ \cdots\ 0\ 1\rangle &:= |0\rangle \cdot |0\rangle \cdot \cdots \cdot |0\rangle \cdot |1\rangle \\ &\vdots \\ |1\ \cdots\ 1\ 1\rangle &:= |1\rangle \cdot \cdots \cdot |1\rangle \end{aligned}$$

Non-commutative multiplication.

Examples:

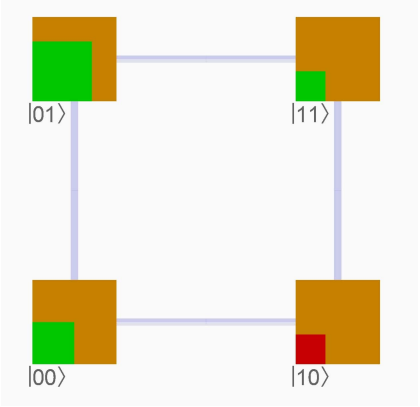
$n = 2$

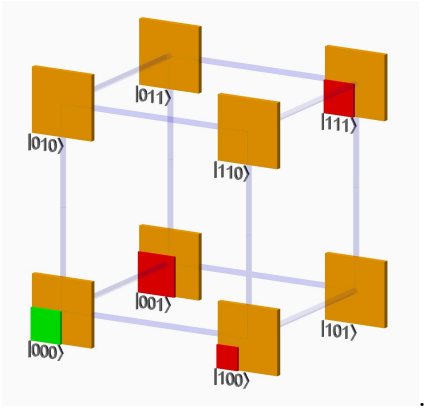
$$\begin{aligned}|q_1\ q_2\rangle &= \frac{1}{2}\cdot|00\rangle + \frac{1}{\sqrt{2}}\cdot|01\rangle - \frac{1}{\sqrt{8}}\cdot|10\rangle + \frac{1}{\sqrt{8}}\cdot|11\rangle \\ &\approx 0.5\cdot|00\rangle + 0.707\cdot|01\rangle - 0.354\cdot|10\rangle + 0.354\cdot|11\rangle.\end{aligned}$$

$n = 3$

$$\begin{aligned}|q_1\ q_2\ q_3\rangle =& \frac{1}{2}\cdot|000\rangle - \frac{\sqrt{3}}{\sqrt{8}}\cdot|001\rangle + 0\cdot|010\rangle + 0\cdot|011\rangle \\ &- \frac{1}{\sqrt{8}}\cdot|100\rangle + 0\cdot|101\rangle + 0\cdot|110\rangle - \frac{1}{2}\cdot|111\rangle \\ &\approx 0.5\cdot|000\rangle - 0.612\cdot|001\rangle - 0.354\cdot|100\rangle - 0.5\cdot|111\rangle.\end{aligned}$$

Graphical representation: Quantum register with n qubits can be illustrated in n-dimensional cubes, each with unit square in the corners, therein squares with side length of the probability amplitudes (and thus the area of the probabilities).
Each qubit is responsible for one of the three directions:
The first qubit for left-right-direction, the second qubit for bottom-top-direction, the third for front-back-direction.
The examples above are graphically represented as follows:

$n = 2$: 

$n = 3$: 

.

Representation as coefficient vector: Often (e.g. in Matlab) the state

$$\begin{aligned} & \alpha_0 \cdot|0\,0\,\cdots\,0\,0\rangle \\ + \quad & \alpha_1 \cdot|0\,0\,\cdots\,0\,1\rangle \\ & \vdots \\ + \quad & \alpha_{2^n-1} \cdot|1\,1\,\cdots\,1\,1\rangle \end{aligned}$$

of a quantum register simply represented as a coefficient vector:

$$\begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{2^n-1} \end{pmatrix}$$

(This vector can then be multiplied with a $2^n \times 2^n$ matrix from the left).

Abbreviated representation of the state as a total: Alternative notations:
If qubits are numbered from 0 to n-1:

$$|q_{n-1}\cdots q_1 q_0\rangle = \sum_{i=0}^{2^n-1} \alpha_i|i\rangle \qquad \text{or} \qquad |q_1\cdots q_n\rangle = \sum_{i=0}^{2^n-1} \alpha_i|i\rangle$$

Here for each $j \in \{1\cdots n\}$ the j-th bit of a basis state $|i\rangle$ is the one at the j-th position from the left in the n-digit binary representation of i. You can see the similarity to the representation of vectors with bases of the vector space: A vector can be represented as its coefficient vector, or as a linear combination of the basis vectors.

Definition: The state $|q_1\ q_2\ \cdots\ q_n\rangle$ is called unentangled if it is generated by multiplication of single qubit states:

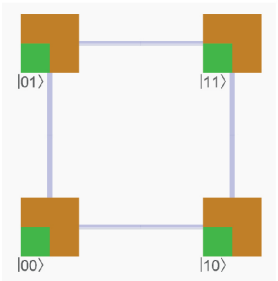
$$\underbrace{(\beta_{1,0}|0\rangle + \beta_{1,1}|1\rangle)}_{\textit{State qubit 1}} \cdot \underbrace{(\beta_{2,0}|0\rangle + \beta_{2,1}|1\rangle)}_{\textit{State qubit 2}} \cdot \cdots \cdot \underbrace{(\beta_{n,0}|0\rangle + \beta_{n,1}|1\rangle)}_{\textit{State qubit n}}$$

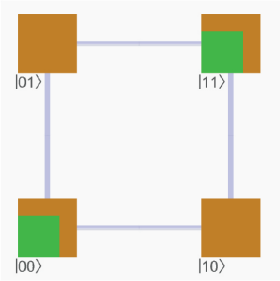
Otherwise the state is called entangled.

Example: $n = 2$: The register states of the two qubits from Experiment 1 and Experiment 2 of the last chapter:

Experiment 1: $|q_1\ q_2\rangle = 0.5 \cdot |00\rangle + 0.5 \cdot |01\rangle + 0.5 \cdot |10\rangle + 0.5 \cdot |11\rangle$

Experiment 2: $|q_1\ q_2\rangle = \sqrt{0.5} \cdot |00\rangle + 0 \cdot |01\rangle + 0 \cdot |10\rangle + \sqrt{0.5} \cdot |11\rangle$.





Example: $n = 3$

$$\begin{aligned}(\beta_0|0\rangle + \beta_1|1\rangle) \cdot (\gamma_0|0\rangle + \gamma_1|1\rangle) \cdot (\delta_0|0\rangle + \delta_1|1\rangle) =& \beta_0\gamma_0\delta_0|000\rangle + \beta_0\gamma_0\delta_1|001\rangle \\ &+\beta_0\gamma_1\delta_0|010\rangle + \beta_0\gamma_1\delta_1|011\rangle \\ &+\beta_1\gamma_0\delta_0|100\rangle + \beta_1\gamma_0\delta_1|101\rangle \\ &+\beta_1\gamma_1\delta_0|110\rangle + \beta_1\gamma_1\delta_1|111\rangle\end{aligned}$$

unentangled.

Excercise an fun in the lecture:

1. Three "qubits" calculate their unentangled state by multiplying their states.
2. Three "qubits" "agree" on an entangled state that is not created by multiplication. For example:
$$\frac{1}{\sqrt{2}}|000\rangle + \frac{1}{2}|101\rangle + \frac{1}{2}|111\rangle$$

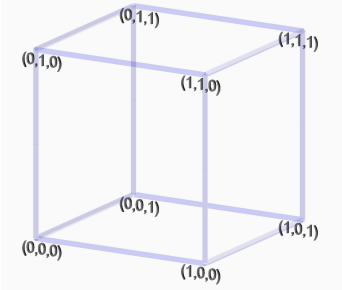
Comment: Multiplication of states of n qubits always results in a state of the register, since $|\alpha_0|^2 + \cdots + |\alpha_{2^n-1}|^2 = 1$ (proof is an exercise).

Up to now, we have: qubits and registers of n qubits. Now we consider what is **measuring** a bit in a register.

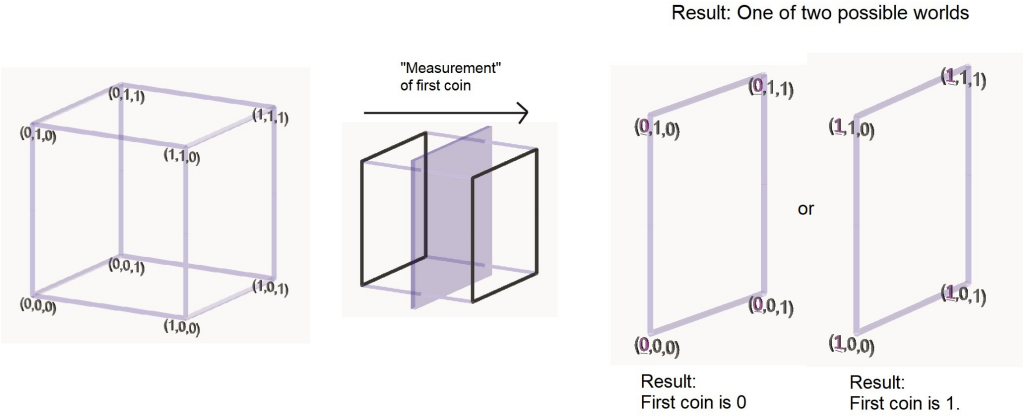
Preliminary consideration: "Measuring" in the state space of a coin flip with three coins:

A usual coin with sides 0 and 1 (and nothing in between) is considered. Imagine it is flipped, so the result is defined, but the result is hidden for the moment. So, we only know it is 0 or 1, but we do not know which of them.
"Measuring" in this case means: Look whether the coin showed 0 or 1.

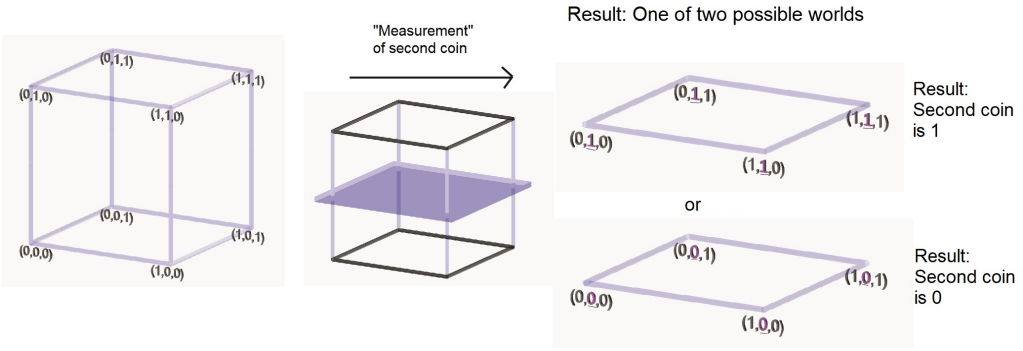
The state space of a flip with three coins can be graphically represented as the corners of a cube as follows, each coin represents the coefficient in one dimension:



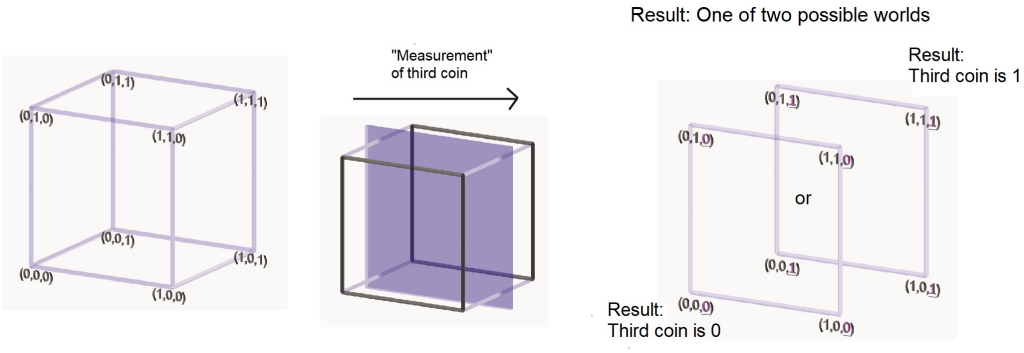
Suppose, the first of the three coins is looked at. The result is one of two possible worlds (so-called "state spaces").



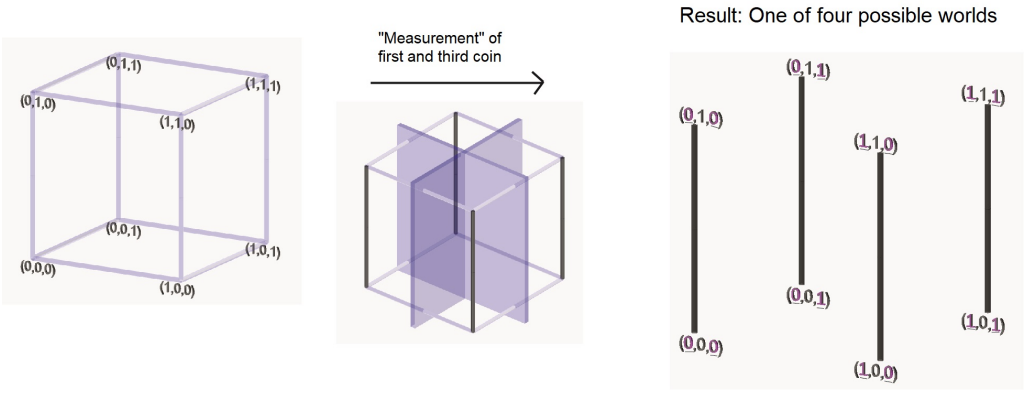
Suppose, not the first, but the second of the three coins is looked at. The result is again one of two possible worlds.



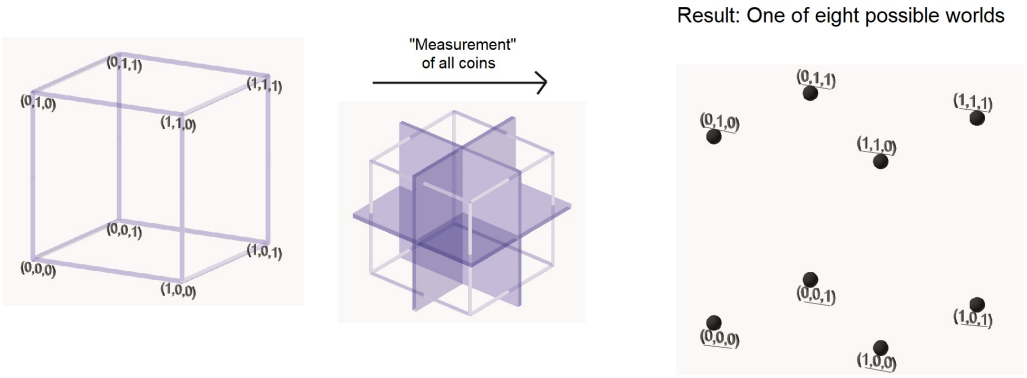
Same effect if the third of the three coins is looked at. The result is the front or the backwards "partial world".



What happens, if we look at the result of two coins, i.e. the first and third of the three coins?
The result is one of four possible worlds.



If we look at all coins, the result is one of eight worlds, there is no longer any uncertainty.



This graphic illustration of the measurement process is transferred to the situation in which not flipped coins, but qubits in quantum registers are measured.

Definition: Let a register with n qubits in the state $|q_1 \cdots q_n\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle$ be given.

For $j \in \{1 \cdots n\}$ let

$I_{j,0} = \{i \in \{0, \cdots, 2^n - 1\} :$ j-th bit from the left in binary represention of i is$|0\rangle\}$

and

$I_{j,1} = \{0, \cdots, 2^n - 1\} \setminus I_{j,0}$

$= \{i \in \{0, \cdots, 2^n - 1\} :$ j-th bit from the left in binary represention of i is$|1\rangle\}$

If the j-th bit of the register measured, it takes the value $|0\rangle$ with probability $\sum_{i \in I_{j,0}} |\alpha_i|^2$.

The register state in this case after measurement is

$$\frac{\sum_{i \in I_{j,0}} \alpha_i |i\rangle}{\sqrt{\sum_{i \in I_{j,0}} |\alpha_i|^2}}$$

Note: all $|i\rangle$ that occur here have a $|0\rangle$ at position j.

With probability $\sum_{i \in I_{j,1}} |\alpha_i|^2$ it takes the value $|1\rangle$. The register state in this case after measurement is

$$\frac{\sum_{i \in I_{j,1}} \alpha_i |i\rangle}{\sqrt{\sum_{i \in I_{j,1}} |\alpha_i|^2}}$$

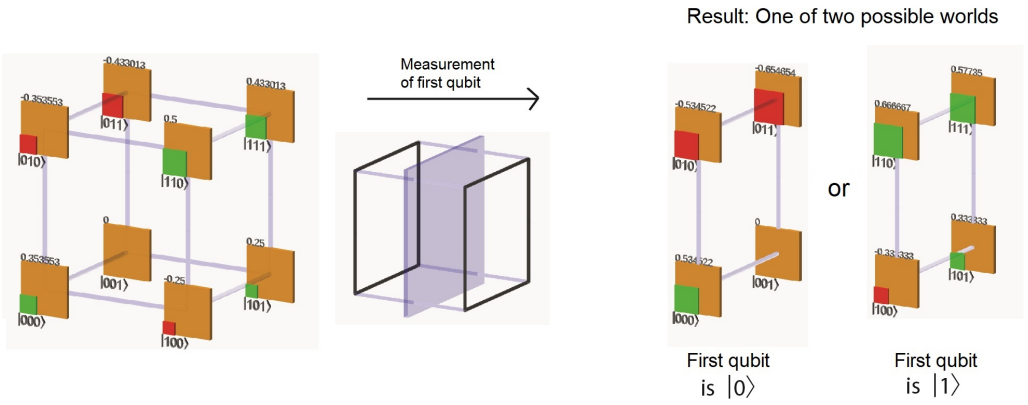
Note: all $|i\rangle$ that occur here have a $|1\rangle$ at position j.

Example:

1.

$$|q_1\ q_2\ q_3\rangle = \frac{\sqrt{2}}{4}\cdot|000\rangle + 0\cdot|001\rangle - \frac{\sqrt{2}}{4}\cdot|010\rangle - \frac{\sqrt{3}}{4}\cdot|011\rangle - \frac{1}{4}\cdot|100\rangle + \frac{1}{4}\cdot|101\rangle + \frac{1}{2}\cdot|110\rangle + \frac{\sqrt{3}}{4}\cdot|111\rangle.$$

The first of the three qubits is measured. The result is one of two worlds.



Measuring the first qubit yields the result $|0\rangle$ with probability

$$\frac{2}{16} + 0 + \frac{2}{16} + \frac{3}{16} = \frac{7}{16}.$$

The quantum register is then in a state that corresponds to the left side of the cube in the graphical representation: The first qubit here is $|0\rangle$. The little squares in this world keep their color. Their size is adjusted so that the sum of the area of the small squares is 1 again. This is achieved by multiplying the areas by $16/7$, i.e. by multiplying the edge lengths by $\sqrt{16/7}$.
(It is a calculation with conditional probabilities, with each basic probability coming from a probability amplitude.)

In the case the measurement of the first qubit yields the result $|0\rangle$, the register is in the state

$$|q_1\ q_2\ q_3\rangle = \sqrt{\frac{16}{7}}\cdot\left(\frac{\sqrt{2}}{4}\cdot|000\rangle + 0\cdot|001\rangle - \frac{\sqrt{2}}{4}\cdot|010\rangle - \frac{\sqrt{3}}{4}\cdot|011\rangle\right)$$
$$= \frac{\sqrt{2}}{\sqrt{7}}\cdot|000\rangle + 0\cdot|001\rangle - \frac{\sqrt{2}}{\sqrt{7}}\cdot|010\rangle - \frac{\sqrt{3}}{\sqrt{2}}\cdot|011\rangle.$$

Measuring the first qubit yields the result $|1\rangle$ with probability.
The quantum register is then in a state which corresponds to the right side face of the cube in the graphical representation.

The state is (after multiplying the probability amplitudes by $\sqrt{16/9}$ to get back to the sum of areas 1):

$$|q_1\ q_2\ q_3\rangle = \frac{1}{3}\cdot|100\rangle + \frac{1}{3}\cdot|101\rangle - \frac{2}{3}\cdot|110\rangle - \frac{\sqrt{3}}{3}\cdot|111\rangle.$$

2. Let $|q_1q_2q_3\rangle = \frac{1}{\sqrt{2}}\cdot\underbrace{|000\rangle}_{\alpha_0} + \frac{1}{2}\cdot\underbrace{|101\rangle}_{\alpha_5} + \frac{1}{2}\cdot\underbrace{|111\rangle}_{\alpha_7}$, and let qubit 2 be measured.

   With a probability of $(\frac{1}{\sqrt{2}})^2 + (\frac{1}{2})^2 = \frac{3}{4}$, qubit 2 takes the value $|0\rangle$. The register is then in the state

$$\begin{aligned}\frac{\frac{1}{\sqrt{2}}|000\rangle + \frac{1}{2}\cdot|101\rangle}{\sqrt{\frac{3}{4}}} &= \frac{2}{\sqrt{3}\cdot\sqrt{2}}\cdot|000\rangle + \frac{1}{\sqrt{3}}|101\rangle \\ &= \sqrt{\frac{2}{3}}\cdot|000\rangle + \sqrt{\frac{1}{3}}|101\rangle\end{aligned}$$

   With the probability $(\frac{1}{2})^2 = \frac{1}{4}$, qubit 2 takes the value $|1\rangle$. The register is then in the state $\frac{\frac{1}{2}|111\rangle}{\sqrt{(\frac{1}{2})^2}} = |111\rangle$.

3. Own examples, entangled and non-entangled states, measure a bit.

Definition: Measuring several qubits means: Measure the bits one after the other. The order is irrelevant for the result ($\rightarrow$ exercise), so the result is well-defined.

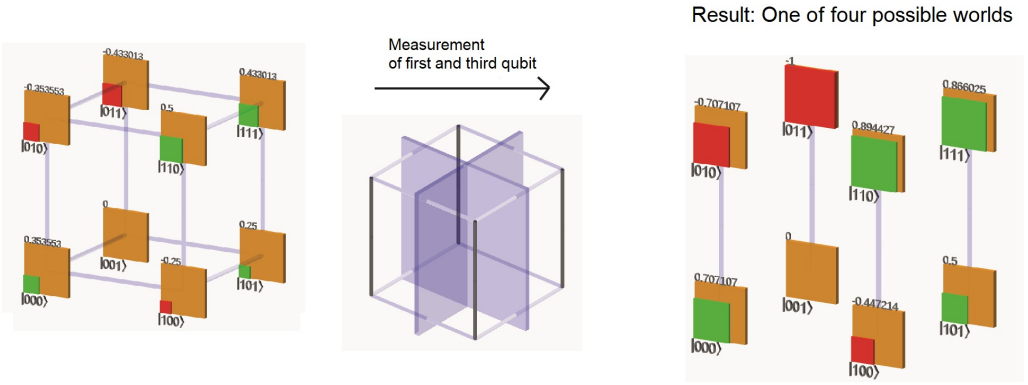
Comment: Exercise is technically difficult. Understanding the statement is important for further lecture. This understanding can also be achieved calculating examples, and also by programming the measurement procedure. There are also exercises for measuring examples.

Example:

i.) Example from above:

$$\begin{aligned}|q_1\ q_2\ q_3\rangle \;=\; & \frac{\sqrt{2}}{4}\cdot|000\rangle + 0\cdot|001\rangle - \frac{\sqrt{2}}{4}\cdot|010\rangle - \frac{\sqrt{3}}{4}\cdot|011\rangle \\ & - \frac{1}{4}\cdot|100\rangle + \frac{1}{4}\cdot|101\rangle + \frac{1}{2}\cdot|110\rangle + \frac{\sqrt{3}}{4}\cdot|111\rangle.\end{aligned}$$

The first and third qubit are measured. There are four possible outcomes.



- With probability 1/4 both qubits are $|0\rangle$.
  The register is then in the state $\sqrt{1/2} \cdot |000\rangle + \sqrt{1/2} \cdot |010\rangle$.
- With probability 3/16 the first qubit is $|0\rangle$, and the third $|1\rangle$.
  The register is then in the state $0 \cdot |000\rangle + 1 \cdot |010\rangle$.
  (So there is no longer any uncertainty regarding the second qubit, it is always in the state $|1\rangle$.)
- With probability 5/16 the first qubit is $|1\rangle$, and the third $|0\rangle$.
  The register is then in the state $\sqrt{1/5} \cdot |100\rangle + \sqrt{4/5} \cdot |110\rangle$.
- With probability 1/4 both qubits are $|1\rangle$.
  The register is then in the state $\sqrt{1/4} \cdot |101\rangle + \sqrt{3/4} \cdot |111\rangle$.

ii.) $|q_1 q_2 q_3\rangle = \frac{1}{\sqrt{2}} \cdot |000\rangle + \frac{1}{2}|100\rangle + \frac{1}{\sqrt{8}}|101\rangle + \frac{1}{\sqrt{8}}|111\rangle$.

Measuring qubits $|q_1\rangle$ and $|q_3\rangle$ yields:

with probability $(\frac{1}{\sqrt{2}})^2 = \frac{1}{2}$: $|q_1\rangle = |q_3\rangle = |0\rangle$.

Register state is then $|000\rangle$.

with probability $(\frac{1}{2})^2 = \frac{1}{4}$: $|q_1\rangle = |1\rangle, |q_3\rangle = |0\rangle$.

The register state is then $|100\rangle$.

with probability $(\frac{1}{\sqrt{8}})^2 + (\frac{1}{\sqrt{8}})^2 = \frac{1}{4}$: $|q_1\rangle = |1\rangle, |q_3\rangle = |1\rangle$.

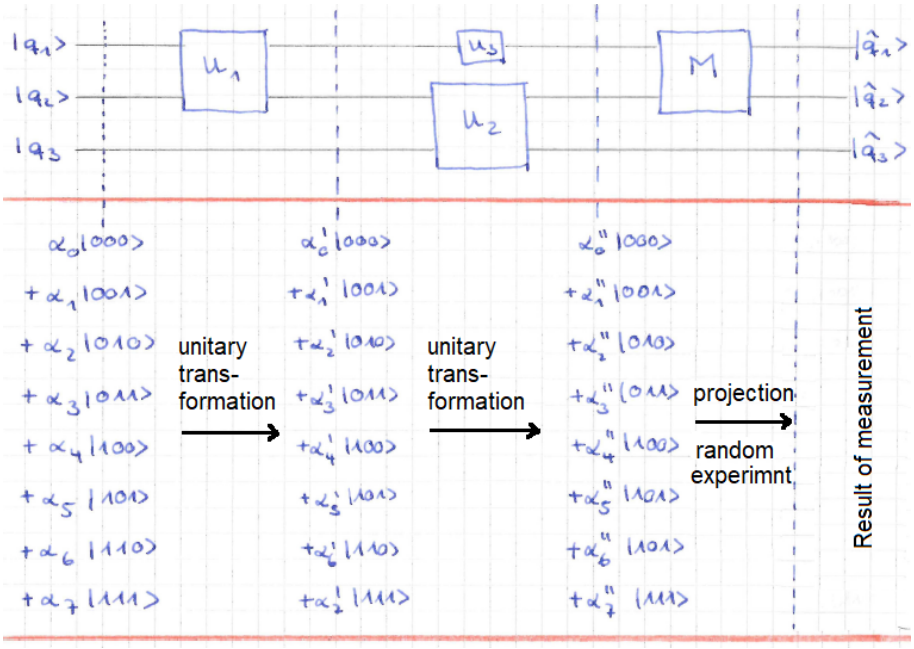
The register state is then $\frac{1}{\sqrt{2}}|101\rangle + \frac{1}{\sqrt{2}}|111\rangle$.

If all three qubits are measured, the state of the register is a basic state. There are eight possibilities for this:
$|000\rangle$, $|001\rangle$, $|010\rangle$, $|011\rangle$, $|100\rangle$, $|101\rangle$, $|110\rangle$ and $|111\rangle$. The probability of each possibility is the square of its probability amplitude.

2.2.2 Quantum algorithms, quantum circuits

Learning outcomes:

- Know the definition of a unitary transformation;
- Know what a quantum circuit looks like and how it is analyzed, e.g.



- Be able to solve exercise sheet 02 completely (and solve it :)).

End of Learning outcomes.

Let's go.

Usually the order is

$$\text{Gate} \longrightarrow \text{Circuit} \longrightarrow \text{Algorithm}.$$

We will proceed an other way round, and first make an excursion to linear algebra.

Reminder Vectors $\{b_1, \cdots, b_N\} \subset \mathbb{R}^N$ (or$\mathbb{C}^N$) are called a basis of $\mathbb{R}^N$, if they are linearly independent. Each vector $v \in \mathbb{R}^N$ (or $\mathbb{C}^N$) then has a unique representation
$v = \sum_{i=1}^{N} \lambda_i b_i$, with $\lambda_i \in \mathbb{R}$ (or $\mathbb{C}$) for $i = 1, \cdots, N$.

end of reminder

Definition: The basis $\{b_1, \cdots, b_N\} \subset \mathbb{R}^N$ (or $\mathbb{C}^N$) is called orthogonal basis, if for all $1 \leq i, j \leq N$ with $i \neq j$ we have $b_i \perp b_j$. It is called orthonormal basis if in addition $\|b_i\| = 1$ holds for $i = 1, \cdots, N$. Here, $\|\cdot\|$ is the Euclidean norm in $\mathbb{R}^N$ (or $\mathbb{C}^N$).

Remark: Orthonormal bases are images of the standard basis under rotations / reflections.

Definition: The $N \times N$ matrix $M = (m_{ij})_{1 \leq i,j \leq N}$ with $m_{ij} \in \mathbb{R}$ (or $\mathbb{C}$) for $1 \leq i, j \leq N$ is called unitary if $M^{-1} = M^{*T}$.

Notations used: $M^{-1} \widehat{=}$ inverse, $M^T \widehat{=}$ transposed, $M^* \widehat{=}$ (element-wise) complex conjugate.

Examples of unitary matrices:

i.)
$$M = \begin{pmatrix} \frac{\sqrt{3}}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{\sqrt{3}}{2} \end{pmatrix}$$

ii.)
$$M = \frac{1}{5} \cdot \begin{pmatrix} 3 & 4i \\ -4 & 3i \end{pmatrix}$$

iii.)
$$M = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

Note:

i.) M is unitary if and only if the rows (as well as the columns) form an orthogonal basis.

ii.) If M is unitary and $m_{ij} \in \mathbb{R}$, then $M^{-1} = M^T$.

Definition: Let U be a unitary matrix. Then the linear mapping
$U : \mathbb{R}^N \to \mathbb{R}^N$ or U: $\mathbb{C}^N \to \mathbb{C}^N$ with $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto U \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$
is called unitary transformation.

Remark: Unitary transformations are rotations and/or reflections of the underlying vector space.

Definition: The state space: of a quantum register with qubits is the vector space spanned by $|0\ldots0\rangle$, $|0\ldots01\rangle$, …, $|1\ldots1\rangle$ over $\mathbb{R}$ or $\mathbb{C}$.

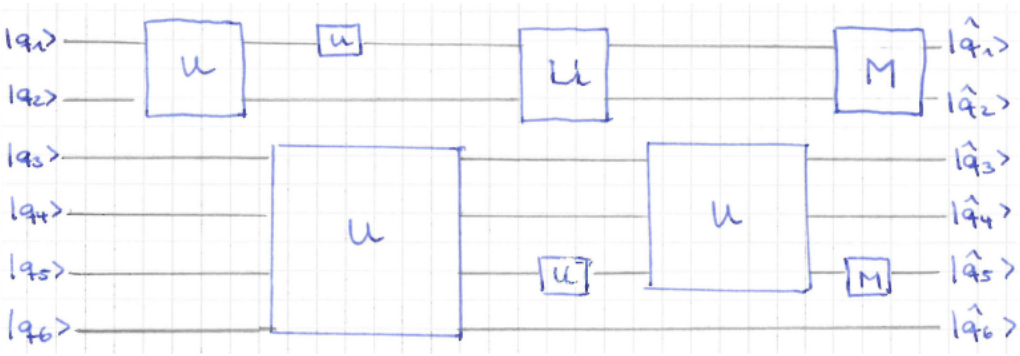
(One easily verifies: All formal linear combinations $\sum_{i=0}^{2^n-1} \lambda_i \cdot |i\rangle$ form a vector space.
Here $|i\rangle$ denotes the basis state with the the binary representation of i in the ket-brackets $|.\rangle$.
Plase note: Not every vector in the state space is a possible state of a quantum register with n qubits. Only vectors with Euclidean length a are register states.)

Definition: A quantum algorithm is a sequence of quantum circuits (see below), the unitary transformations are those correponding to quantum gates. (The connection between algorithm and circuits can be illustrated with sorting algorithms: The algorithm defines one circuit every n). Note: The definition will be expanded a little later.

Definition: A quantum circuit consists of:

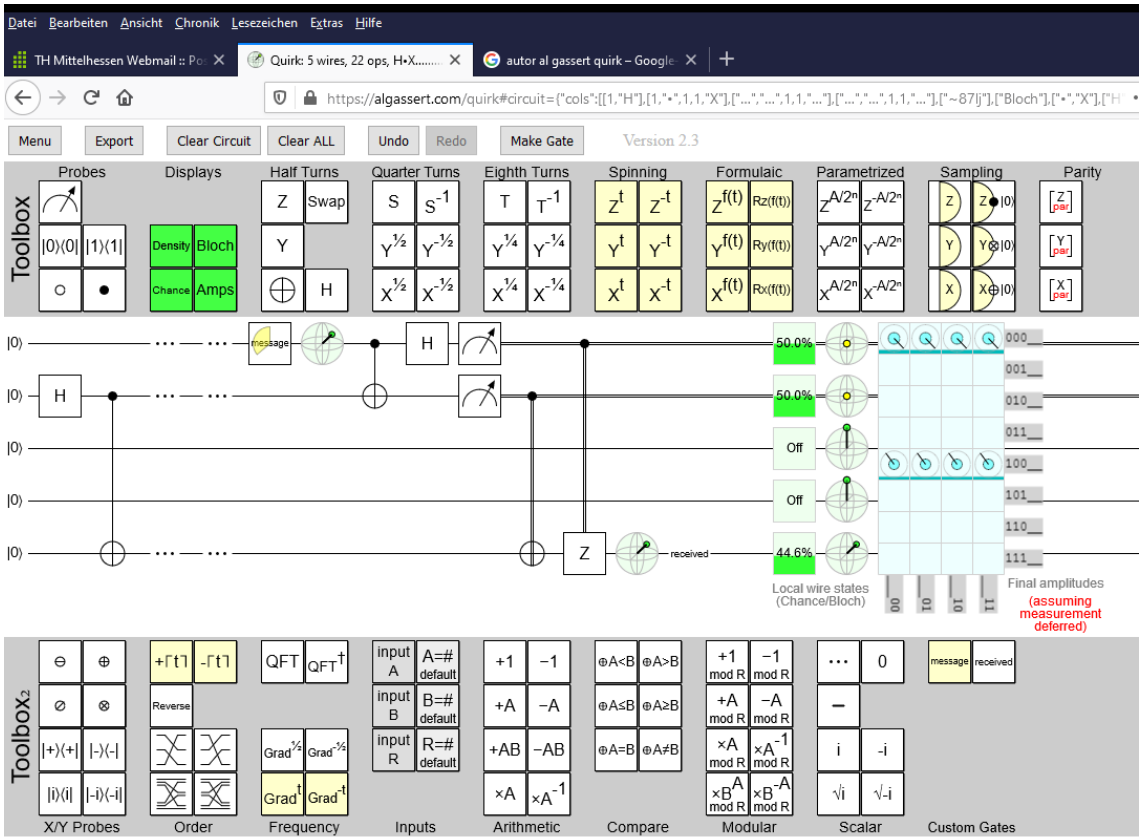
- An input of n qubits, $n \in \mathbb{N}$
- An output of n qubits, measured or not
- A well-defined sequence of unitary transformations of the state space and, at the end, a measurement of qubits.

Illustration (just to have a picture in mind) $n = 6$



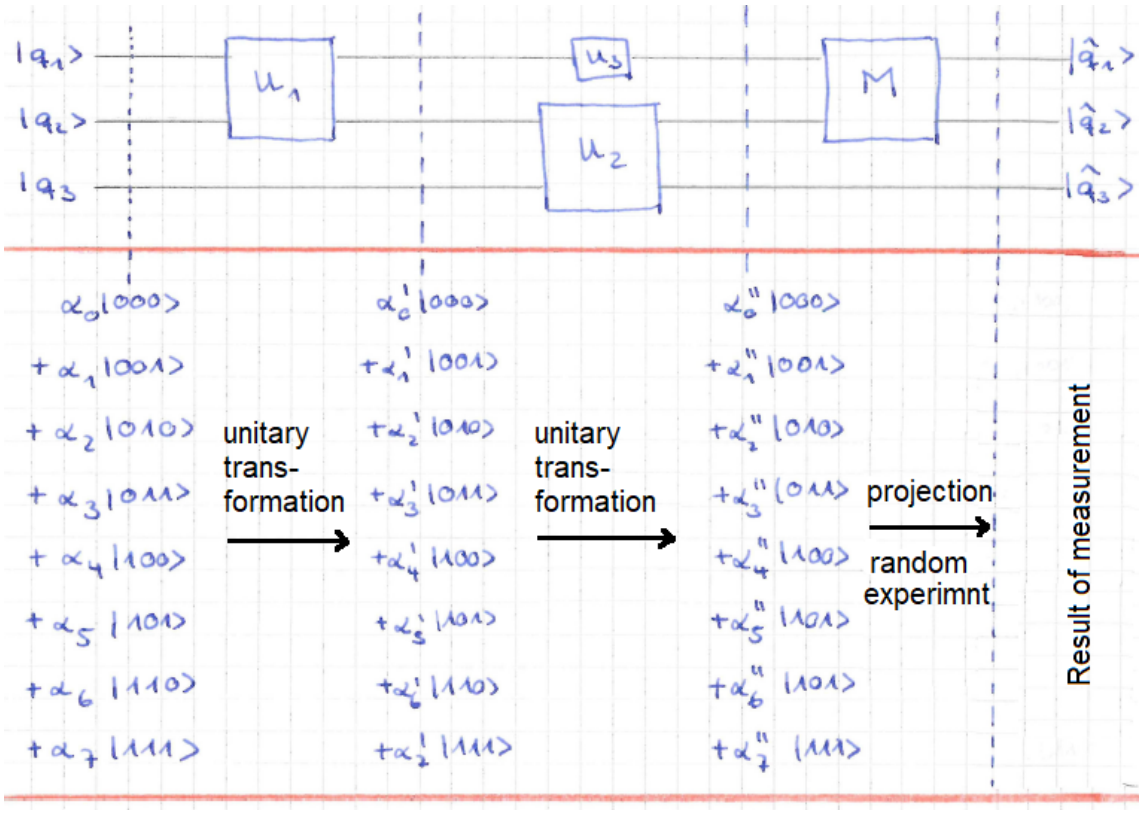
Note: A very nice drag and drop open-source tool that runs directly in the browser can be found at
https://algassert.com/quirk

This is what the quantum circuits look like in quirk:


Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
Quirk: 5 wires, 22 ops, H•X.....
autor al gassert quirk – Google
https://algassert.com/quirk#circuit={"cols":[[1,"H"],[1,"•",1,1,"X"],["...","...",1,1,"..."],["...","...",1,1,"..."],["~87lj"],["Bloch"],["•","X"],["H
Menu
Export
Clear Circuit
Clear ALL
Undo
Redo
Make Gate
Version 2.3
Toolbox
Probes
Displays
Half Turns
Quarter Turns
Eighth Turns
Spinning
Formulaic
Parametrized
Sampling
Parity
Density
Bloch
Chance
Amps
message
received
50.0%
50.0%
Off
Off
44.6%
Local wire states (Chance/Bloch)
Final amplitudes (assuming measurement deferred)
Toolbox2
X/Y Probes
Order
Frequency
Inputs
Arithmetic
Compare
Modular
Scalar
Custom Gates
Reverse

Analysis of quantum algorithms takes place in the state space

Look at the unitary transformations, each between the dashed lines:



and :

$$\begin{pmatrix} \alpha_0' \\ \vdots \\ \alpha_7' \end{pmatrix} = \begin{pmatrix} \text{matrix} \\ \text{for} \\ U_1 \end{pmatrix} \cdot \begin{pmatrix} \alpha_0 \\ \vdots \\ \alpha_7 \end{pmatrix}$$

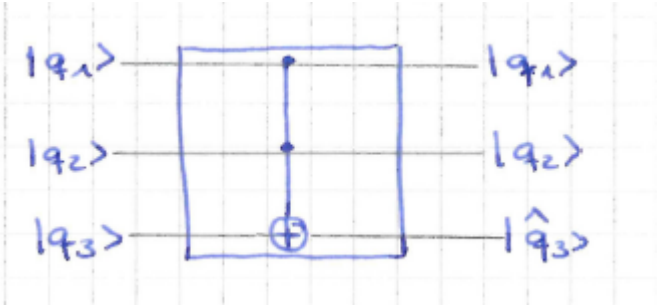
"matrix for U_1" is a unitary $2^3 \times 2^3$ matrix.

$$\begin{pmatrix} \alpha_0'' \\ \vdots \\ \alpha_7'' \end{pmatrix} = \begin{pmatrix} \text{matrix} \\ \text{for } U_2 \\ \text{and at the same time } U_3 \end{pmatrix} \cdot \begin{pmatrix} \alpha_0' \\ \vdots \\ \alpha_7' \end{pmatrix}$$

Here "Matrix for U_1 and at the same time U_2" is again a unitary $2^3 \times 2^3$ matrix.

In order to deepen your understanding of this, examples are useful, so let's look at some examples (lateron, mathematics will make life a little easier later, keyword "tensors" for those who have heard about it).

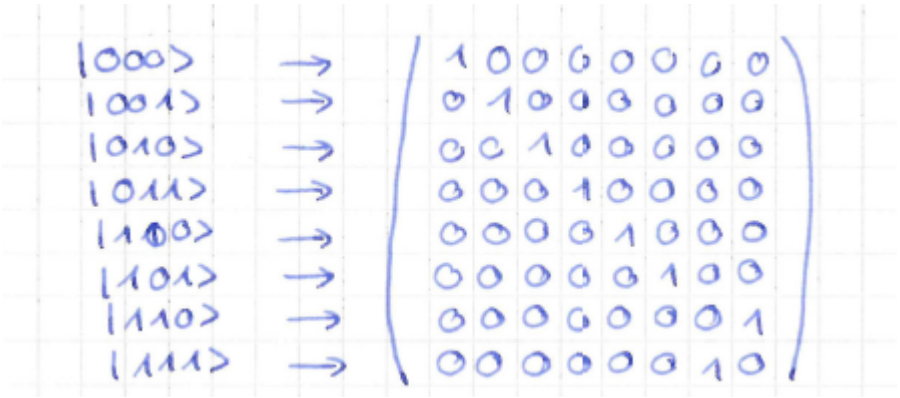
Example: The Toffoli gate



on 3 qubits is defined as follows:

Each basis state $|abc\rangle$ with $(a, b, c) \in \{0,\ 1\}^3$ is transformed to the basis state $|a\ b\ (c \oplus (a \wedge b))\ \rangle$. Here $\oplus$ and $\wedge$ are the logical XOR and AND, respectively. q_1 and q_2 are called control bits, q_3 is called target bit.

So the unitary matrix for the Toffoli gate is, since columns are the images of the basis vectors:



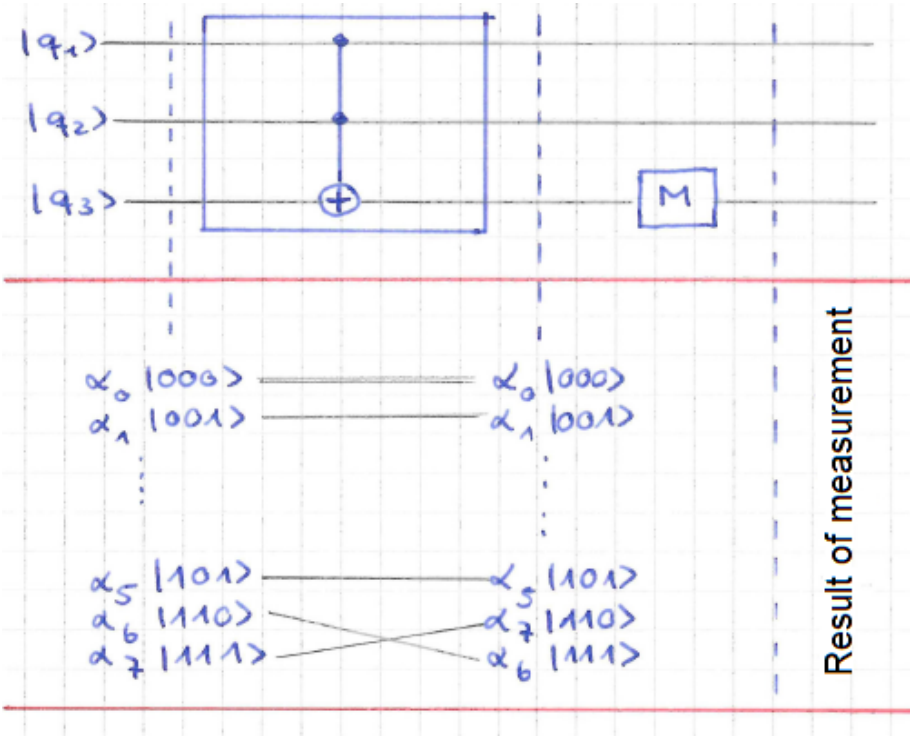
(please convince yourself: it is unitary).

Up to now we know, what happens to basis states when Toffoli is applied to them. Let's see, what happens to a linear combination of two or more basis states (a so called superposition of basis states).

Example: Let

$$|q_1q_2q_3\rangle = \frac{1}{\sqrt{2}}|000\rangle + \frac{1}{2}|100\rangle + \frac{1}{\sqrt{8}}|101\rangle + \frac{1}{\sqrt{8}}|111\rangle$$

be the input of the following quantum circuit:



Question: What is the (measurement) result?

Answer: After using the Toffoli gate, the register is in the state

$$\frac{1}{\sqrt{2}}|000\rangle + \frac{1}{2}|100\rangle + \frac{1}{\sqrt{8}}|101\rangle + \frac{1}{\sqrt{8}}|110\rangle.$$

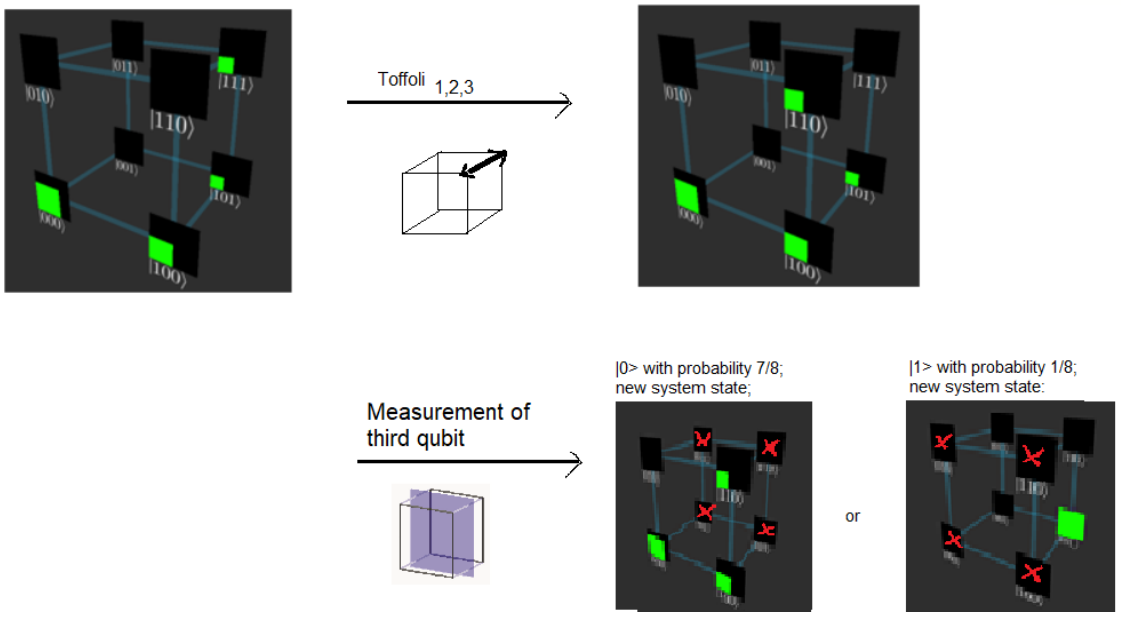
Measuring the third qubit then yields:

$|q_3\rangle = |1\rangle$ with probability 1/8;
the register state then is $|101\rangle$.

$|q_3\rangle = |0\rangle$ with probability 7/8;
the register state then is

$$\begin{aligned}
&\sqrt{\frac{8}{7}} \cdot \left(\frac{1}{\sqrt{2}}|000\rangle + \frac{1}{2}|100\rangle + \frac{1}{\sqrt{8}}|110\rangle\right) \\
&= \frac{2}{\sqrt{7}}|000\rangle + \sqrt{\frac{2}{7}}|100\rangle + \frac{1}{\sqrt{7}}|110\rangle \\
&= \frac{1}{\sqrt{7}} \cdot (2 \cdot |00\rangle + \sqrt{2}|10\rangle + |11\rangle) \cdot |0\rangle
\end{aligned}$$

Graphical representation:



Remark: Why unitary transformations of the STATE space, not of the single qubits? We will see in the next section, how each quantum gate generates a unitary transformation on the state space. Therefore, since untitary transformations form a group, a quantum circuit also performs a unitary transformation of the state space (as long as no measurements are done).

2.2.3 Quantum gates

Learning outcomes:

i.) Know the quantum gates Id, X, (Y), Z, H, CNOT and TOFFOLI with their unitary transformations, their graphical representation in the cube and on algassert;

ii.) Understand the concepts of controlled unitary transformations and quantum oracles, including their unitary transformations;

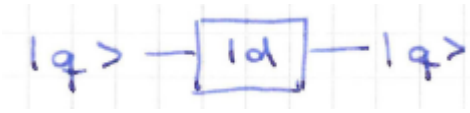
iii.) Having designed and analyzed out your own first quantum circuits on three qubits.

Quantum gates are the elementary components of quantum circuits. Each quantum gate has a fixed number of input qubits. This number may be 1, 2 or 3 qubits.

The unitary transformations performed in quantum circuit on n qubits are alway deducted from the unitary transformations of the quantum gates.

Quantum gates on 1 qubit: .

i.) **Identity** Representation in the circuit (if representation is necessary):



Transformation of basis states:
$|0\rangle \mapsto |0\rangle$
$|1\rangle \mapsto |1\rangle$
Unitary matrix: $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

The identity leaves $|q\rangle$ unchanged, but plays an important accompanying role if transformations are carried out on other bits of the circuit at the same time.

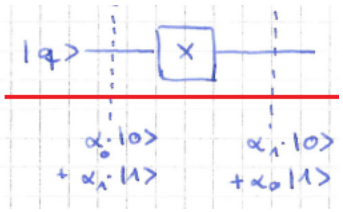
ii.) **Pauli-X** transformation (the NOT in quantum computing)

Representation in the circuit:

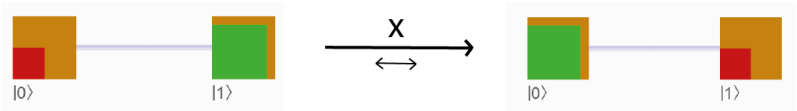
Transformation of basis states:
$|0\rangle \mapsto |1\rangle$
$|1\rangle \mapsto |0\rangle$

Unitary matrix: $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

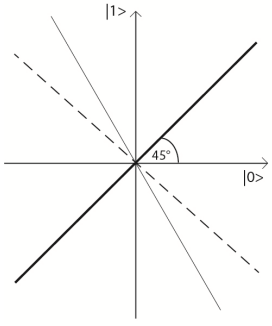
Transformation of arbitrary state: $\alpha_0|0\rangle + \alpha_1|1\rangle \quad \mapsto \quad \alpha_1|0\rangle + \alpha_0|1\rangle$



Graphical illustration / example:



Technical implementation: Reflection of the qubit at the bisector of the 1st quadrant



Pauli-X

Exercise in the lecture: What is the unitary matrix if X is applied to the first qubit of a register made up of two qubits?
How can one graphically imagine the effect on the quantum register?

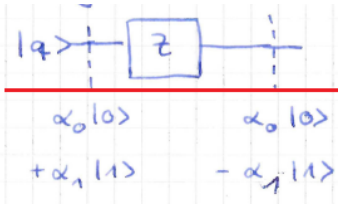
iii.) **Pauli-Z** transformation

Representation in the circuit:

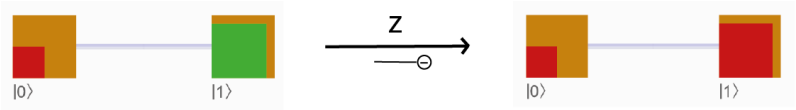
Tansformation of basis states:
$|0\rangle \mapsto |0\rangle$
$|1\rangle \mapsto -|1\rangle$

Unitary matrix: $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

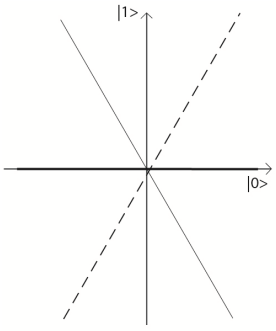
Transformation of arbitrary state: $\alpha_0|0\rangle + \alpha_1|1\rangle \quad \mapsto \quad \alpha_0|0\rangle - \alpha_1|1\rangle$



Graphic illustration / example:



Technical implementation: Reflection of the qubit on the $|0\rangle$ axis



Pauli-Z

Exercise in the lecture: What is the unitary matrix if Z is applied to the second qubit of a register of three qubits?
How can one graphically imagine the effect on the quantum register?

iv.) **Hadamard** transformation

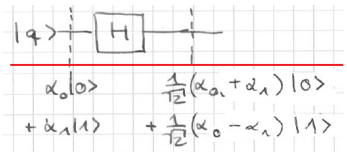
Representation in the circuit:

Transformation of basis states:

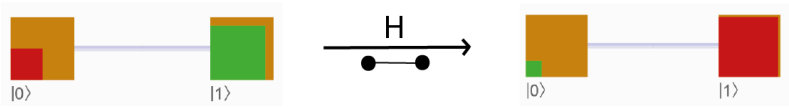
$$|0\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$|1\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Unitary matrix: $\frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

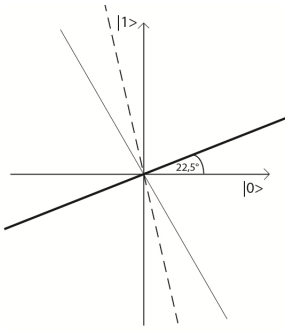
Transformation of arbitrary state:
$\alpha_0|0\rangle + \alpha_1|1\rangle \quad \mapsto \quad \frac{1}{\sqrt{2}}(\alpha_0 + \alpha_1)|0\rangle \; + \; \frac{1}{\sqrt{2}}(\alpha_0 - \alpha_1)|1\rangle$



Graphical illustration / example:



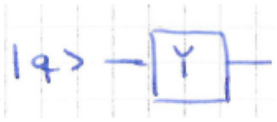
Technical implementation: Reflection of the qubit on the 22.5° axis



Hadamard

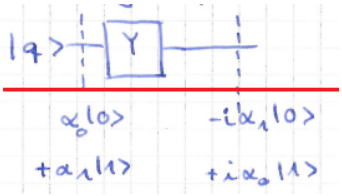
Exercise in the lecture: What is the unitary matrix if H is applied to the second qubit of a register made up of two qubits?
How can one graphically imagine the effect on the quantum register?

v.) **Pauli-Y** transformation (uses $\mathbb{C}$)



Transforamtion of basis states:
$|0\rangle \mapsto i|1\rangle$
$|1\rangle \mapsto -i|0\rangle$
unitary matrix: $\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$

Transformation of arbitrary state: $\alpha_0|0\rangle + \alpha_1|1\rangle \quad \mapsto \quad -i\alpha_1|0\rangle + i\alpha_0|1\rangle$



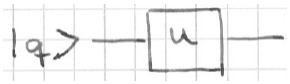
vi.) **General unitary transformation of a qubit**:

Proposition: Every real unitary 2×2 matrix has the form

$$\begin{pmatrix} u & v \\ -v & u \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} u & v \\ v & -u \end{pmatrix}$$

with $u, v \in \mathbb{R}$, $|u|^2 + |v|^2 = 1$.

Proof: The proof is an exercise

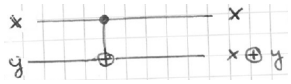


Remark: Please verify that all of the aforementioned transformations have this shape.

Quantum gate on 2 qubits:

i.) **CNOT** (Controlled not, controlled negation):
Meaning: The target bit is negated if and only if the control bit has the value 1.

Representation in the circuit:



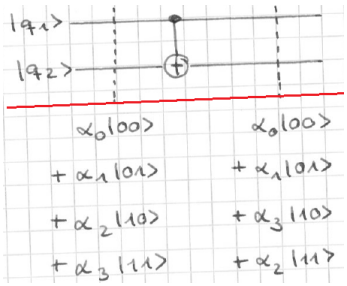
Transformation of basis states:

$$|00\rangle \mapsto |00\rangle$$
$$|01\rangle \mapsto |01\rangle$$
$$|10\rangle \mapsto |11\rangle$$
$$|11\rangle \mapsto |10\rangle$$

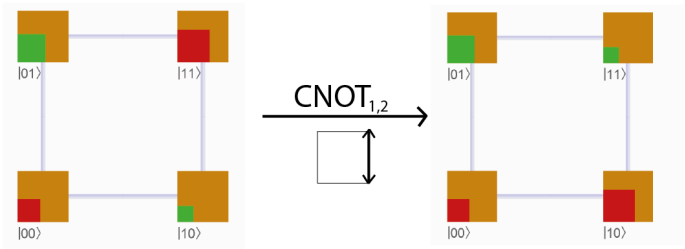
Unitary matrix:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Transformation of arbitrary state:



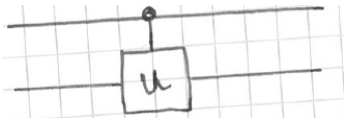
Graphical illustration / example:



Technical implementation: Challenging and not very stable yet. The control bit is brought close to an atom so this is excited. Next, the target qubit is brought close to the atom and is changed by the excitation of the atom (very handwaving).

Exercise in the lecture: What is the unitary matrix if H is applied to the third qubit as a control bit and the first as the destination bit of a register made up of three qubits?
How can one graphically imagine the effect on the quantum register?

ii.) **Controlled U** (one way of generalizing CNOT)



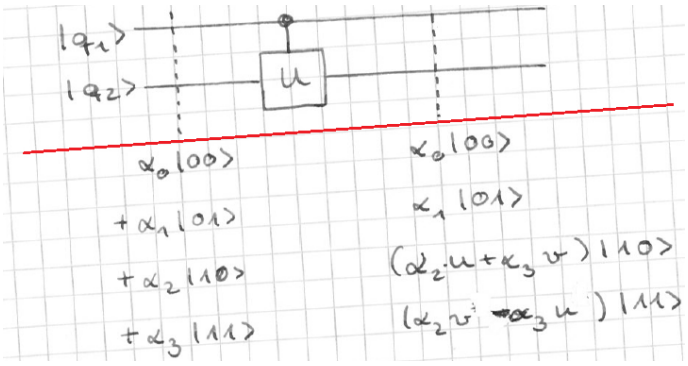
Meaning: The unitary transformation U is applied to the target bit if the control bit has the value 1.
Transformation of basis states:

$$\begin{aligned} |00\rangle &\mapsto |00\rangle \\ |01\rangle &\mapsto |01\rangle \\ |10\rangle &\mapsto |1\rangle \cdot U(|0\rangle) \\ |11\rangle &\mapsto |1\rangle \cdot U(|1\rangle) \end{aligned}$$

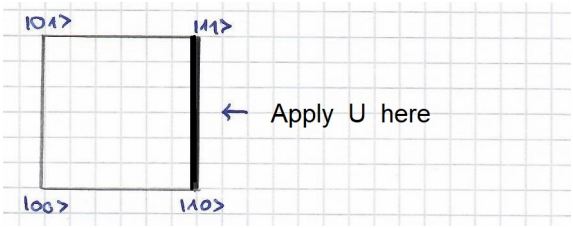
Unitary matrix:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & & \\ 0 & 0 & & \mathrm{U} \end{pmatrix}$$

Trasformation of arbitrary staes:
Only case U = $\begin{pmatrix} u & v \\ -v & u \end{pmatrix}$

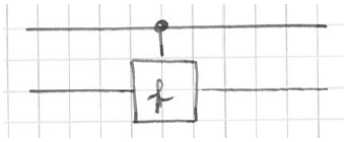


Graphic illustration:



Remark: CNOT is controlled U for U = Pauli-X.

iii.) **Quantum oracle** (another way of generalizing CNOT)



for any (not necessarily bijective) function $f : \{0,1\} \to \{0,1\}$.

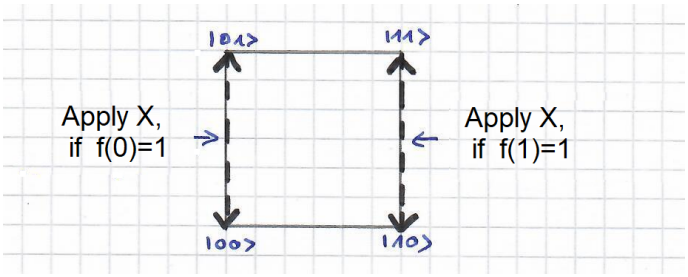
Meaning: Target bit is negated if and only if $f(\text{controlbit}) = 1$.

Transformation of basis states:

$|00\rangle \mapsto |0\rangle|f(0)\rangle$
$|01\rangle \mapsto |0\rangle|1 \oplus f(0)\rangle$
$\downarrow$
$f(0) = 1 \Leftrightarrow$ Order reversed

$|10\rangle \mapsto |1\rangle|f(1)\rangle$
$|11\rangle \mapsto |1\rangle|1 \oplus f(0)\rangle$
$\downarrow$
$f(1) = 1 \Leftrightarrow$ Order reversed

Tansformation of an arbitrary state, for the 4 possible functions is an exercise.
Graphical illustration:



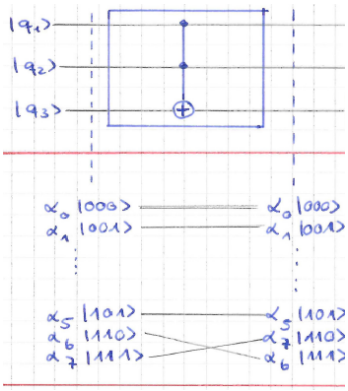
Remark: CNOT is controlled U for $U = \text{Id}$.

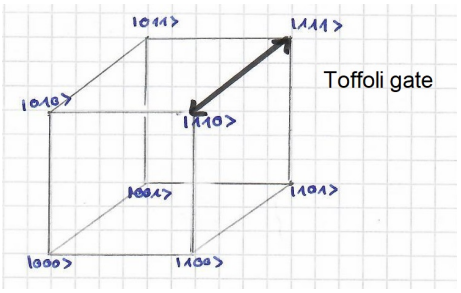
Exercise in the lecture: The function $f(0) = 1, \quad f(1) = 0$ is considered. What is the unitary matrix of its quantum oracle if it is applied to the first qubit as a control bit and the second as the target bit of a register made up of three qubits?
How can one graphically imagine the effect on the quantum register?

Quantum gate on 3 qubits: Only Toffoli gate, has already been dealt with:

Meaning: 3rd bit is negated exactly when the other two are 1.

Transformation of basis states and graphical illustration:





Effect on basic conditions:

$$
\begin{aligned}
|000\rangle &\mapsto |000\rangle \\
|001\rangle &\mapsto |001\rangle \\
|010\rangle &\mapsto |011\rangle \\
|011\rangle &\mapsto |010\rangle \\
|100\rangle &\mapsto |100\rangle \\
|101\rangle &\mapsto |101\rangle \\
|110\rangle &\mapsto |111\rangle \\
|111\rangle &\mapsto |110\rangle
\end{aligned}
$$

Unitary matrix:

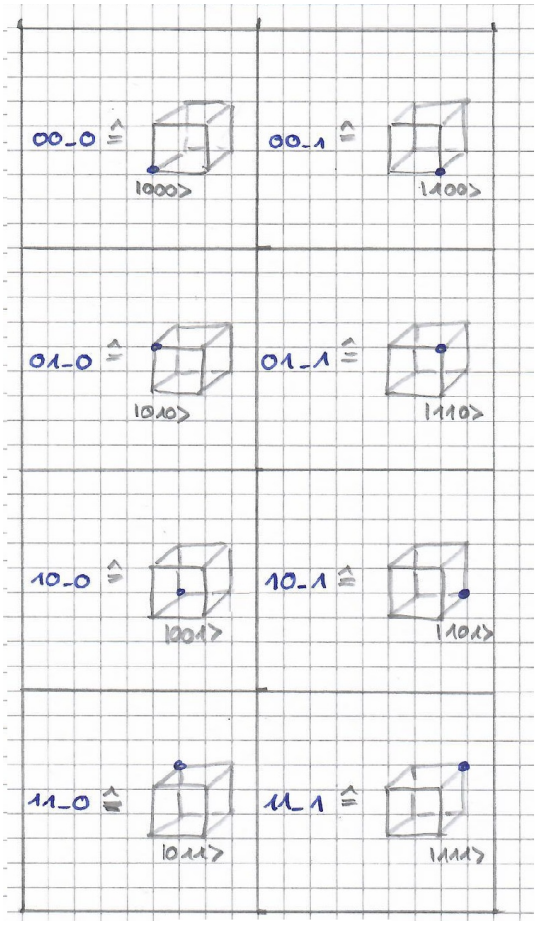
$$
\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0
\end{pmatrix}
$$

These are the main gates for this lecture.
In the online tool quirk at algassert.com you can find many other quantum gates that require the complex numbers in most cases.

A quantum register is represented in reverse order by algassert.
Instead of $|q_1\ q_2\ q_3\rangle$ it is $|q_1\ q_1\ q_0\rangle$. At first glance, this is more difficult to visualize, but corresponds better to the binary representation $|i\rangle$.

Here is a conversion table for a quantum register made up of three qubits:

Which algassert field corresponds to which field in the cube?



Algassert: $|i\rangle = |q_2 q_1 q_0\rangle$

Cube of Qurakel: $|q_1 q_2 q_3\rangle$

2.3 Mathematics: Unitary transformations and tensor product

Learning outcomes:

1.) Knowing about the reversibility of quantum circuits (as long as there is no measurement- so no information is lost, unlike e.g. with classic AND).

2.) Being able to form the tensor product of matrices and vectors.

3.) Know about the following applications of tensor products in quantum circuits:

i.) Multiplication of unentangled quantum states to get a single register state;

ii.) Finding the unitary transformation if parallel gates are used in one step (e.g. CNOT on the first and second qubit, simultaneously Pauli-X on the third);

iii.) Combination of i.) and ii.).

4.) Playing around with Matlab, Algassert, Qurakel and IBM-Q.

This both theoretical and programming issues will provide you with all basics needed to understand the algrihtms of the next chapters :).

Definition: A complex $N \times N$ matrix U is called unitary if $U^{-1} = U^{*T}$.
The corresponding linear mapping is called unitary transformation.

Proposition: Unitary transformations are rotations, reflections and combinations of both. They preserve angles (more precisely: the scalar product) and lengths.

Proof: (not necessarily in the lecture)
Let $x, y \in \mathbb{C}^N, x = \begin{pmatrix} x_1 \\ \vdots \\ x_6 \end{pmatrix}, y = \begin{pmatrix} y_1 \\ \vdots \\ y_6 \end{pmatrix}$. The inner product $\langle x|y\rangle$ of x and y is defined as

$$\langle x|y\rangle = \sum_{i=1}^{n} x_i^* y_i$$

(written as a matrix: $\langle x|y\rangle = x^{*T} y$), the norm (or length) of x is $\sqrt{\langle x|x\rangle}$. Now let U be unitary. Then (in matrix notation, and because $U^{*T} = U^{-1}$):

$$\begin{aligned} \langle Ux|Uy\rangle &= (Ux)^{*T} * Uy \\ &= (U^* x^*)^T * Uy \\ &= x^{*T} \cdot U^{*T} \cdot Uy \\ &= x^{*T} \cdot y \\ &= \langle x|y\rangle \end{aligned}$$

Proposition: (Proof exercise for those with a mathematician's heart)
Unitary $N \times N$ -matrices form a group (with matrix multiplication).

Conclusion: (follows from both propositions)

1. Unitary transformations with composition form a group.
2. A unitary transformation converts a state of a quantum register to another state of the quantum register.
   Tis holds, since a quantum register state is a vector of $\mathbb{R}^{2^n}$ of length 1, and lenghts are preserved by unitary transformations.
3. Every unitary transformation can be reversed (by applying the inverse transformation).
   Reversing a transformation applied to a quantum register yields the state previous to the transformation.
   Therefore: In quantum circuits, no information is lost by using the quantum gates as long as no measurements are made (in contrast to the use of classical binary gates such as AND. If $a \wedge b = 0$, the values of a and b can no longer be reconstructed).

Now, what is the tensor product?

Definition: Let $A = (a_{ij})$, $B = (b_{ij})$ matrices of arbitrary size (not necessarily quadratic): A is a $r \times n$ matrix, B is a $s \times m$ matrix. Then the tensor product $A \otimes B$ is the following $r \cdot s \times n \cdot m$ matrix.

$$\begin{pmatrix} a_{11}B & \dots & a_{1n}B \\ \vdots & & \vdots \\ a_{r1}B & \dots & a_{rn}B \end{pmatrix}$$

Example: Find an example on your own :).

Definition: Let $v \in \mathbb{R}^n$(oder $\mathbb{C}^n$), $w \in \mathbb{R}^m$(oder $\mathbb{C}^m$), then $v \otimes w$ is the vector obtained by writing both vecotrs as columns and forming their (matrix) tensor product. It is a (column) vector with $n \cdot m$ entries.

Proposition: (without proof)

1. Tensor product and matrix multiplication are compatible: Let A, B, v, w be as above, so is
   $$(A \cdot v) \otimes (B \cdot w) = (A \otimes B) \cdot (v \otimes w)$$
2. Tensor products of unitary matrices are unitary.

Exercise:

- On part 1. of the proposition: Please make sure that the dimensions of the matrices at the left and the right side of the eqaution are the same.
- On part 2. of the proposition: Please verify that the tensor product of square matrices is again a square matrix, even if both have different formats.

Note: (not necessarily in the lecture)
Usually the tensor product is introduced for vector spaces: Let V_1, V_2 be vector spaces with bases $e_1, \cdots, e_n$ and $f_1, \cdots, f_m$ respectively, then the tensor product $V_1 \otimes V_2$ is the vector space with bases $\{e_i f_j : i = 1 \cdots n, j = 1 \cdots m\}$. The tensor product of two vectors $v = \sum v_i e_i \in V_1$ and $w = \sum w_j f_j \in V_2$ is then defined as $\sum_{i,j} v_i w_j e_i \otimes f_j$.
In this sense, the state space of a quantum register (as a vector space) is element of the tensor product of the state spaces of the individual qubits.

Note: Not every vector in the tensor product can be represented as a tensor product of vectors of the spaces involved (for instance, with the notations of the note, the vector $e_1 f_1 + e_n f_m$ cannot be represented as tensor product single vectors).

Application of the tensor product to quantum circuits:

1. Calculate the state of a quantum register with unentangled qubits:

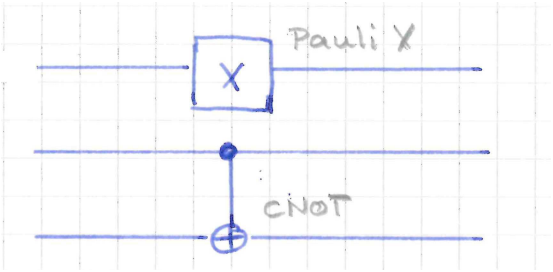
$$\begin{aligned} |q_1\rangle &= \beta_0|0\rangle + \beta_1|1\rangle \\ |q_2 q_3\rangle &= \alpha_0|00\rangle + \alpha_1|01\rangle + \alpha_2|10\rangle + \alpha_3|11\rangle \\ \Rightarrow |q_1 q_2 q_3\rangle &= \sum_{i=0}^{7} \gamma_i |i\rangle \end{aligned}$$

Then

$$\begin{pmatrix} \gamma_0 \\ \vdots \\ \gamma_7 \end{pmatrix} = \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix} \otimes \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix} = \begin{pmatrix} \beta_0\alpha_0 \\ \beta_0\alpha_1 \\ \beta_0\alpha_2 \\ \beta_0\alpha_3 \\ \beta_1\alpha_0 \\ \beta_1\alpha_1 \\ \beta_1\alpha_2 \\ \beta_1\alpha_3 \end{pmatrix}$$

(This is also obtained by multiplying
$(\beta_0|0\rangle + \beta_1|1\rangle) \cdot (\alpha_0|00\rangle + \alpha_1|01\rangle + \alpha_2|10\rangle + \alpha_3|11\rangle)$

2. Matrix of the unitary transformation if gates are used in one step in parallel: E.g:



The associated unitary matrix is

$$U = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} & 0 & & \\ & & & \\ & & & \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

3. (Combination of 1. and 2.) Application of parallel gates to non-entangled sub-registers. Example: Take a quantum register in the state 1., and apply the circuit of 2. to it. This turns the state of the register to

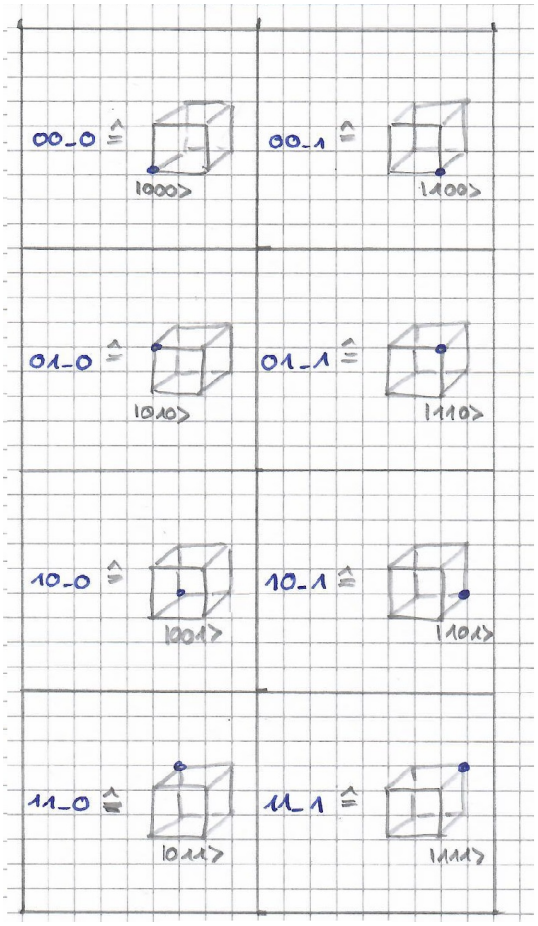
$$\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix} \right) \otimes \left(\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix} \right)$$

$$= \begin{pmatrix} \beta_1 \\ \beta_0 \end{pmatrix} \otimes \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_3 \\ \alpha_2 \end{pmatrix} = \begin{pmatrix} \beta_1\alpha_0 \\ \beta_1\alpha_1 \\ \beta_1\alpha_3 \\ \beta_1\alpha_2 \\ \beta_0\alpha_0 \\ \beta_0\alpha_1 \\ \beta_0\alpha_3 \\ \beta_0\alpha_2 \end{pmatrix}$$

Note: Tensor procduct can only be applied to circuits with parallel transformations applied to successive qubits. So it is possible, if in a circuit of three qubits CNOT ia applied to the first and second, and Pauli-X on the third, or in the circuit above. It is not possible, however, when CNOT is applied to the first and third qubit, and Pauli-X to the second. There is an exercise for this.

Exercise: Please play with Matlab, Algassert, Qurakel and IBM-Q.

Here is the rule for converting the basic states' descriptions of Algassert and Qurakel:



Algassert: $|i\rangle = |q_2 q_1 q_0\rangle$

Cube of Qurakel: $|q_1 q_2 q_3\rangle$

3 Basic Quantum Algorithms

Learning outcomes:

1.) Understand how to simulate a classical circuit with m gates by a quantum circuit with $O(m)$ quantum gates. (Conculsion: Every computational problem can be solved by quantum algorithms at least as quickly as by classical algorithms).

2.) Have seen the following algorithms and understand the way they work:

i.) Generation of random bits;

ii.) Teleportation;

iii.) Key exchange (BB84 protocol)

iv.) Dense coding;

v.) Decryption of quantum oracles (algorithms of Deutsch, Deutsch-Josza and Vazirani).

3.) Know three ways of how to analyse quantum algorithms. There are three options for analysis, their application depends on the situation:

i.) Most complete, but also most complex: Analysis using the unitary transformations.

ii.) If the input is given and has a simple form, e.g. a basic state: Step-by-step calculation of the register states during the calculation.

iii.) For circuits with up to three QBits: Graphic illustration on the "cube".

3.1 Classical Boolean Functions

We want to show that quantum circuits can compute all classical Boolean functions $f : \{0,1\}^n \to \{0,1\}$. This will be shown explicitly for all 16 Boolean functions on $n = 2$ qubits.

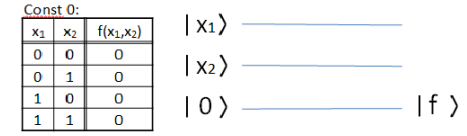
For larger n then all functions can be implemented via their disjunctive normal form DNF. For this, auxiliary qubits will be used, the so called "garbage-qubits".

At the end of the section it will be demonstrated how this method can also be applied to simulate any classical circuit with m gates (on 1 or two classical bits each) by quantum circuits with a maximum of $5m$ quantum gates.

Proposition: The following quantum circuits calculate the 16 different classical Boolean functions on 2 input bits:

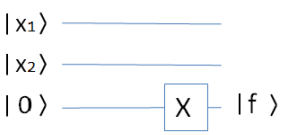
Const 0:

x_1	x_2	$f(x_1,x_2)$
0	0	0
0	1	0
1	0	0
1	1	0



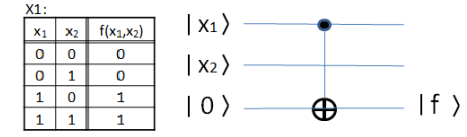
Const 1:

x_1	x_2	$f(x_1,x_2)$
0	0	1
0	1	1
1	0	1
1	1	1



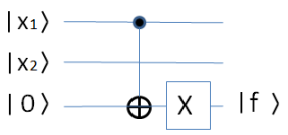
X1:

x_1	x_2	$f(x_1,x_2)$
0	0	0
0	1	0
1	0	1
1	1	1



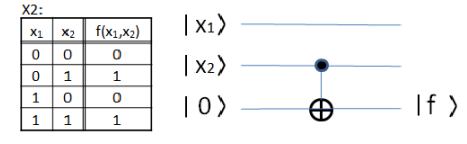
Not X1:

x_1	x_2	$f(x_1,x_2)$
0	0	1
0	1	1
1	0	0
1	1	0



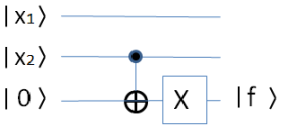
X2:

x_1	x_2	$f(x_1,x_2)$
0	0	0
0	1	1
1	0	0
1	1	1



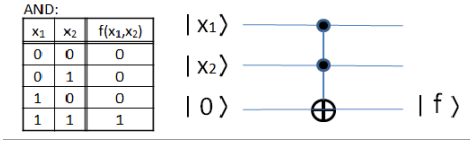
Not X2:

x_1	x_2	$f(x_1,x_2)$
0	0	1
0	1	0
1	0	1
1	1	0



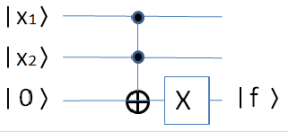
AND:

x_1	x_2	$f(x_1,x_2)$
0	0	0
0	1	0
1	0	0
1	1	1



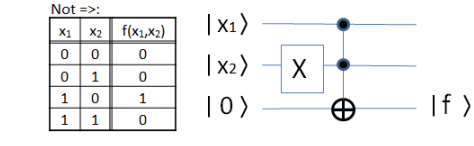
Not AND:

x_1	x_2	$f(x_1,x_2)$
0	0	0
0	1	0
1	0	0
1	1	1



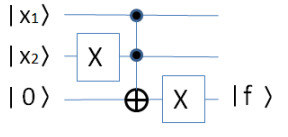
Not =>:

x_1	x_2	$f(x_1,x_2)$
0	0	0
0	1	0
1	0	1
1	1	0



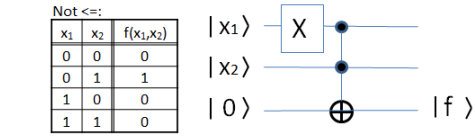
=>:

x_1	x_2	$f(x_1,x_2)$
0	0	1
0	1	1
1	0	0
1	1	1



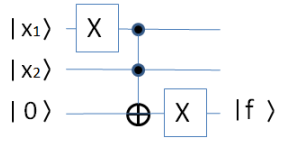
Not <=:

x_1	x_2	$f(x_1,x_2)$
0	0	0
0	1	1
1	0	0
1	1	0



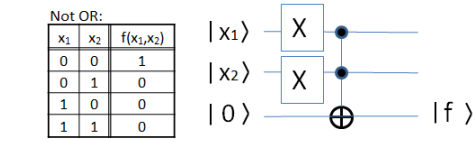
<=:

x_1	x_2	$f(x_1,x_2)$
0	0	1
0	1	0
1	0	1
1	1	1



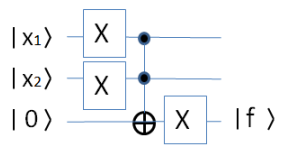
Not OR:

x_1	x_2	$f(x_1,x_2)$
0	0	1
0	1	0
1	0	0
1	1	0



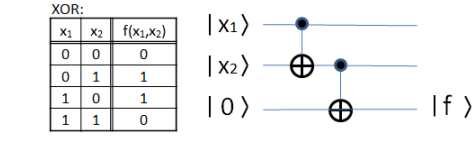
OR:

x_1	x_2	$f(x_1,x_2)$
0	0	0
0	1	1
1	0	1
1	1	1



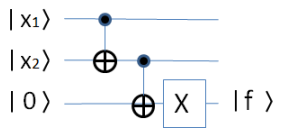
XOR:

x_1	x_2	$f(x_1,x_2)$
0	0	0
0	1	1
1	0	1
1	1	0



⇔:

x_1	x_2	$f(x_1,x_2)$
0	0	1
0	1	0
1	0	0
1	1	1



Proof: Please convince yourself for every single function, it is an exercise.

Exercise in the lecture: Test all three analysis methods for one of the functions. (Unitary transformations, circuit gate by gate, and the cube to visualize the circuits).

We now show an explaining example on how a function of $n > 2$ input bits can be computed by a quantum circuit, using the disjunctive normal form of the function and using a sufficient number of "garbage-qubits". It is an example with $n = 3$ input bits.

Example: The following function is calculated by the quantum circuit below:

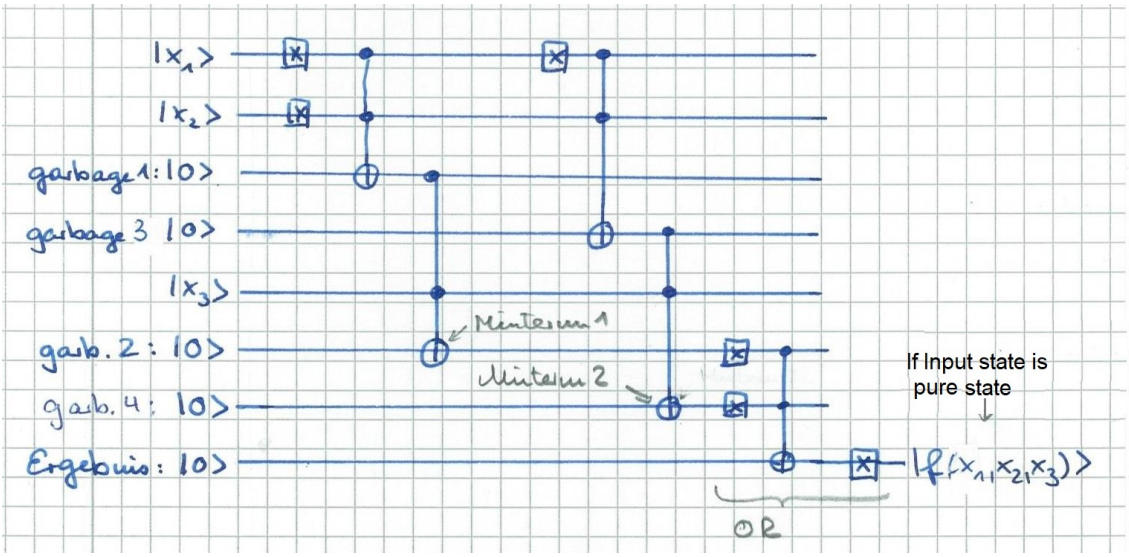
Function:

x_1	x_2	x_3	$f(x_1,x_2,x_3)$
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	0

DNF:

$$f(x_1,x_2,x_3) = (\neg x_1 \wedge \neg x_2 \wedge x_3) \vee (x_1 \wedge \neg x_2 \wedge \neg x_3)$$

Quantum circuit:



Theorem: Every $f : \{0,1\}^n \to \{0,1\}$ can be calculated by a quantum circuit. The circuit yields the value of the function, if the input is a pure state, and yields the superposition of the values, if the input is a superposition. The calculation can be done with $n-1$ garbage qubits for every minterm, and with #Minterme $-$ 2 further garbage qubits for the OR at the end.

Proof: There is no formal proof, the intuition should be clear according to the example.

Remark: The quantum circuits for calculating the $f : \{0,1\}^n \to \{0,1\}$ repeatedly access to the input bits. That works, since by input of a pure state, every qubit at any point of the computation has a unique value $|0\rangle$ or $|1\rangle$. Proof: With an input Q-bit only two different things happen during the calculation:

i.) A number of Pauli X transformations are used, and

ii.) It is used to control Toffoli and CNOT gates.

Induction on the number of operations shows that each qubit actually has a unique state during the entire calculation.
Note: This would not be the case if the Hadamard transformation was applied in between. Applying H, a system is moved from a pure state to a superposition state.

Proposition: Every classical circuit with m gates (on one or two classical input bits each) can be simulated by a quantum circuit with at most $4m$ quantum gates.
"Simulation" means: The quantum circuit delivers the same output on the pure states as the classical circuit does.

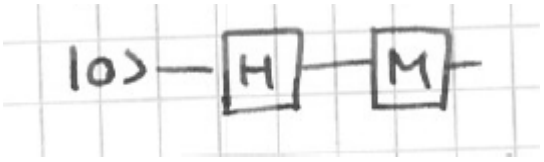
Proof: Similar to the proof of the DNF-simulation with quantum circuits. Please verify: Every classical gate can be simulated by at most 4 quantum gates.

3.2 Random number generators

Generation of true randomness is not possible on classic computers, since these are deterministic. Deterministic maschines are able only to compute pseudo random numbers. With pseudo random numbers, anyone who knows the algorithm and knows an initial seed, can recalculate the numbers already produced, and can predict the future ones.

QBits are truely random (which Einstein didn't like; he claims "God doesn not throw dice.").

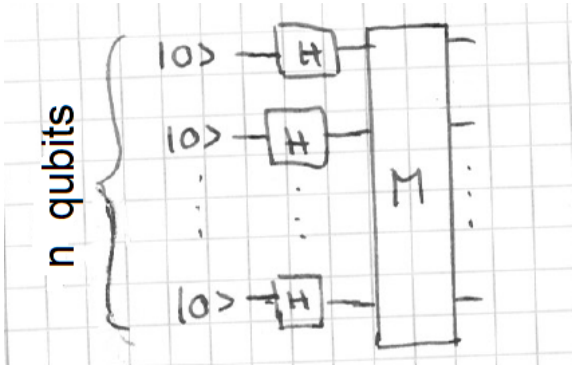
Propositione: The following quantum circuit generates a random bit:



Proof.: After applying H the bit is in the state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.
Measuring delivers the output $|0\rangle$ or $|1\rangle$ with probability $\frac{1}{2}$.

Note: Hardware for quantum random bits can be bought for around 3,000 Eur. Here are pictures of IBM-qrbg121 and of Quantis QRNG PCIe - USB:

Proposition: The following quantum circuit produces n independent real random bits, $n \in \mathbb{N}$:



Proof: After applying the Hadamard transformations the register is in the state

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \cdot \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \cdot \ldots \cdot (|0\rangle + |1\rangle) = \frac{1}{\sqrt{2^n}} \cdot \sum_{i=0}^{2^n-1} |i\rangle.$$

Measuring therefore yields every base state $|i\rangle$ with equal probability.

3.3 Teleportation

One of the most spectacular applications of quantum computing:

1997 Zeilinger's group in Vienna: First teleportation in the laboratory.

2003 Gisin's group in Geneve: Teleportation over 55m, for the first time outside of laboratory;

2004 Zeilinger's group: Teleportation over a distance of 600m, from one bank of the Danube river to its other bank;

2010 Xian Min Lin's group in Shanghai: Teleportation over 16 km;

2012 Chinese University of Science and Technology with Pan Jian-Wei: Teleportation over a distance of 97 km;

2012 Zeilinger's working group: Teleportation over a distance of 143 km between La Palma and Tenerife;

2017 International working group, i.a. with the participation of Zeilinger and Pan Jian-Wei: Teleportation over 1400 km from Earth to the Chinese quantum satellite Micius;

2017 same working group: 7600 km between Austria and China.

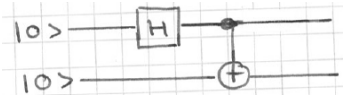
Recent research: Bridging ultra-small distances instead of particularly large ones, for use inside of the computer itself.

Background: Legendary: "' Scotty, beam me up, there is no intelligent life down here "'.

Preparation: Highly entangled quBits, so-called EPR pairs, named after Einstein-Podolsky-Rosen, are used. How are they created?

Answer of a physicist: E.g .: A light particle is sent through an entanglement crystal.

Answer of a computer scientist:



System state after applying Hadamard:

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \cdot |0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$$

System state after applying CNOT:

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Creation of entangled QBits completed (in sense of Computer science - quantum circiuit).

Now we are ready for the teleprotation algorithm. Observation: No matter ist teleported, but properties of a qubit, i.e. information.

Teleportation: (Algorihtm Bennet et al 1993, first physical realization 1997)

Situation and problem: A (Alice) and B (Bob) each own one qubit of an EPR pair, $|a\rangle$ and $|b\rangle$.
Alice also has another qubit $|\psi\rangle$. She wants to send this qubit (more precisely: the state of this qubit) to Bob.
But for Teleportation, there is no way of transporting a qubit from Alice to Bob (no "quantum channel"). There is just a classical channel (telephone).
Please realize, that Alice cannot measure $|\psi\rangle$, that would change the state of $|\psi\rangle$.
So how is $|b\rangle$ changed into $|\psi\rangle$?

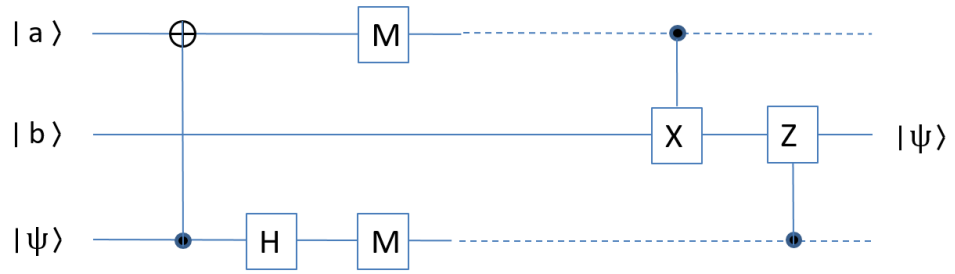
Idea: Entangling $|\psi\rangle$ and $|a\rangle$ distributes information of $|x\rangle$ „between the qubits "of the register; Measuring $|\psi\rangle$ leaves the information completely between $|a\rangle$ and $|b\rangle$ ($\rightarrow$ exercise)

Comparison: Some say, it is like in everyday life: Marriage distributes capital (at least in Germany). If further owner goes bankrupt, there are possibilities of saving the capital "parking it" at the other one.

Procedure in plain text: (see Homeister, "Quatum Computing vertehen", Springer)

1. Alice applies a CNOT gate: $|\psi\rangle|a\rangle \leftarrow |\psi\rangle|a \oplus \psi\rangle$
2. Alice applies the Hadamard transformation to the qubit to be teleporteted: $|\psi\rangle \leftarrow H(\psi)$
3. Alice measures $|\psi\rangle$ and $|a\rangle$ and sends the result to Bob via the classic channel (e.g., telephone).
4. If $|a\rangle = |1\rangle$, Bob applies Pauli-X to $|b\rangle$: $|\psi\rangle \leftarrow X(|b\rangle)$
5. If $|a\rangle = |1\rangle$, Bob applies Pauli-Z to $|b\rangle$: $|b\rangle \leftarrow Z(|b\rangle)$.

Quantum circuit:



"– – –" indicates information via classic channel.

Correctness:

Let $\psi = \alpha|0\rangle + \beta|1\rangle$, where α and β are unknown to Alice and Bob.

State of the quantum register at the beginning:

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \cdot (\alpha|0\rangle + \beta|1\rangle) = \frac{\alpha}{\sqrt{2}}(|000\rangle + |110\rangle) + \frac{\beta}{\sqrt{2}}(|001\rangle + |111\rangle).$$

State after application of CNOT:

$$\frac{\alpha}{\sqrt{2}}(|000\rangle + |110\rangle) + \frac{\beta}{\sqrt{2}}(|101\rangle + |011\rangle) = \frac{\alpha}{\sqrt{2}}(|00\rangle + |11\rangle) \cdot |0\rangle + \frac{\beta}{\sqrt{2}}(|10\rangle + |01\rangle) \cdot |1\rangle.$$

State after application of H:

$$\frac{\alpha}{\sqrt{2}} \cdot \frac{1}{\sqrt{2}} \cdot (|00\rangle + |11\rangle) \cdot (|0\rangle + |1\rangle) + \frac{\beta}{\sqrt{2}} \cdot \frac{1}{\sqrt{2}} \cdot (|10\rangle + |01\rangle) \cdot (|0\rangle - |1\rangle).$$

Rewriting terms (preparation for measuring the first and third QBits):

$$\begin{aligned} & |0\rangle \cdot (\frac{\alpha}{2} \cdot |0\rangle + \frac{\beta}{2} \cdot |1\rangle) \cdot |0\rangle \\ + \; & |0\rangle \cdot (\frac{\alpha}{2} \cdot |0\rangle - \frac{\beta}{2} \cdot |1\rangle) \cdot |1\rangle \\ + \; & |1\rangle \cdot (\frac{\alpha}{2} \cdot |1\rangle + \frac{\beta}{2} \cdot |0\rangle) \cdot |0\rangle \\ + \; & |1\rangle \cdot (\frac{\alpha}{2} \cdot |1\rangle - \frac{\beta}{2} \cdot |0\rangle) \cdot |1\rangle. \end{aligned}$$

Measuring therefore leads to:

- $|00\rangle$ with probability $\frac{1}{4}$; $|b\rangle$ is in state $\alpha|0\rangle + \beta|1\rangle$ in this case;
- $|01\rangle$ with probability $\frac{1}{4}$; $|b\rangle$ is in state $\alpha|1\rangle - \beta|0\rangle$ in this case;
- $|10\rangle$ with probability $\frac{1}{4}$; $|b\rangle$ is in state $\alpha|0\rangle + \beta|1\rangle$ in this case;
- $|11\rangle$ with probability $\frac{1}{4}$; $|b\rangle$ is in state $\alpha|1\rangle - \beta|0\rangle$ in this case;

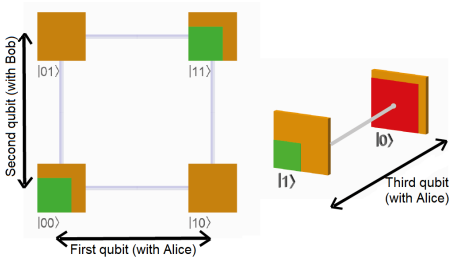
If $|a\rangle = |1\rangle$ (cases $|10\rangle$ and $|11\rangle$), Pauli-X changes Bob's QBit's state to $\alpha|0\rangle + \beta|1\rangle$ or $\alpha|0\rangle - \beta|1\rangle$.

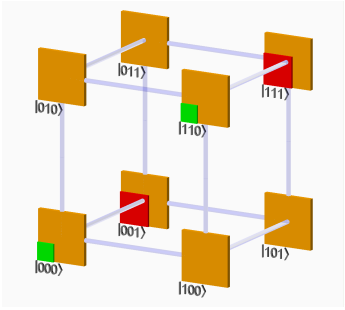
If the third qubit was also measured 1 (cases $|01\rangle$ and $|11\rangle$), Pauli-Z then changes $|b\rangle$ to
$\alpha|0\rangle + \beta|1\rangle$.

Illustration: Consider the example $\psi = 0.5 \cdot |0\rangle - \sqrt{3/4} \cdot |1\rangle$.

Let $\psi = \alpha|0\rangle + \beta|1\rangle$, where α and β are unknown to Alice and Bob.

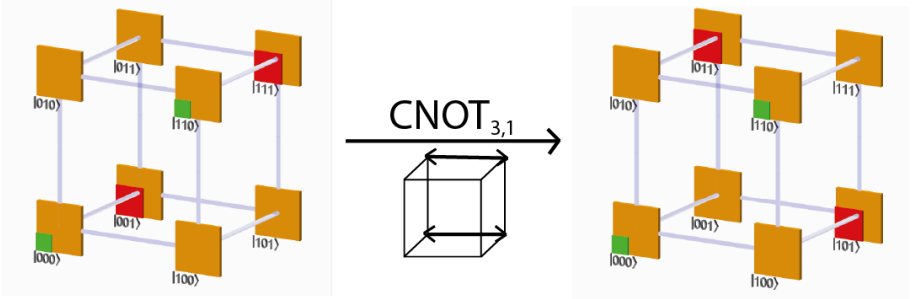
State of the quantum register at the beginning:



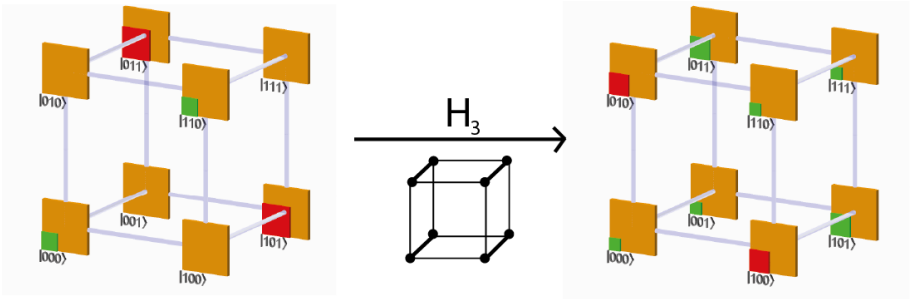
, therefore 

.

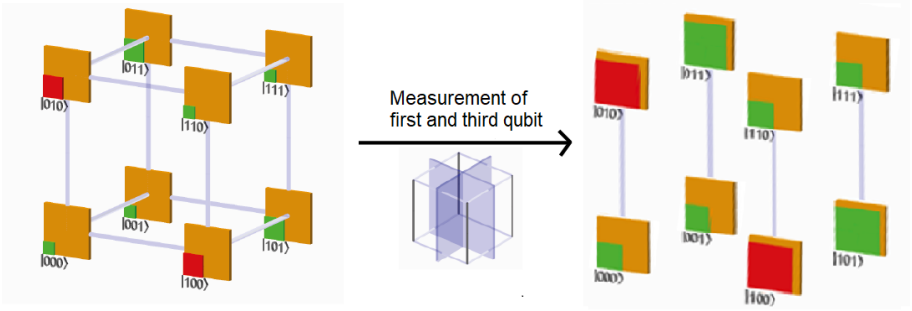
CNOT is applied (control bit third QBit, target bit first QBit):



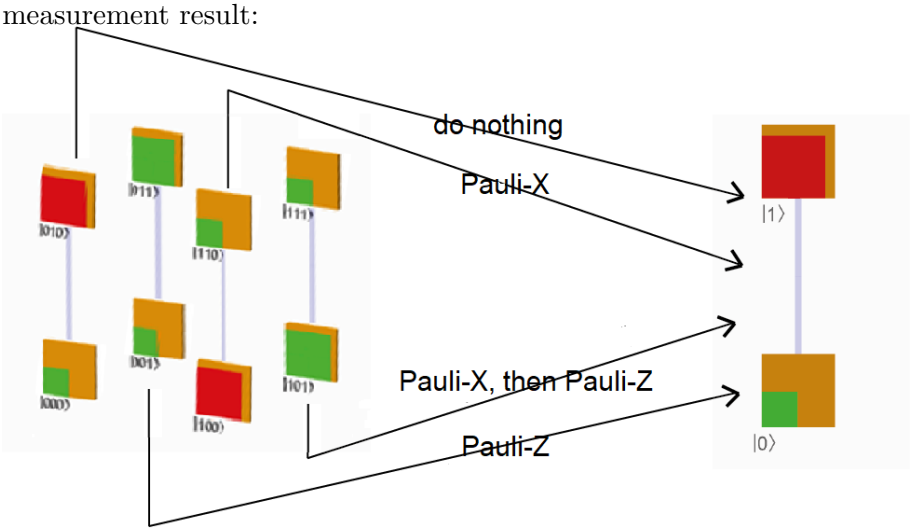
H is applied to the third QBit:



First QBit and third QBit are measured, all results have equal probability of 1/4:



Bob applies Pauli-X and / or Pauli-Z depending on Alice's information on her measurement result:



Note: In cryptography there is always an eavesdropper Eve secretely listening to the communication between Alice and Bob.
Eves doesn't get any information here. She gets just a random pair of bits Alice is given to Bob by means of the classical channel.
The "important" information is transmitted through quantum entanglement, out of reach for Eve.

3.4 BB84 protocol: Cryptography, key exchange

Problem of key exchange:

Alice and Bob want to agree on a series of random classical bits. They need this, for example, to use a common key to encrypt messages.

They have a conventional channel (e.g. telephone) and a quantum channel (e.g. fiber optic cable). Both are however accessible to a possible eavesdropper.

How can they use the properties of qubits to exchange a random key, whereby an eavesdropper should not receive any information about the key and should also be discovered?

Charles H. Bennett and Gilles Brassard found a possibility in 1984.

(Algorithm) BB84 protocol:

i.) Alice starts in state $|0\rangle$ and applies Pauli-X with a probability of 1/2. Now she knows her random bit.

ii.) With probability 1/2 she applies H and sends the qubit to Bob via the quantum channel.

iii.) Bob also applies H with probability 1/2 and measures his qubit. The measurement result is Bob's bit.

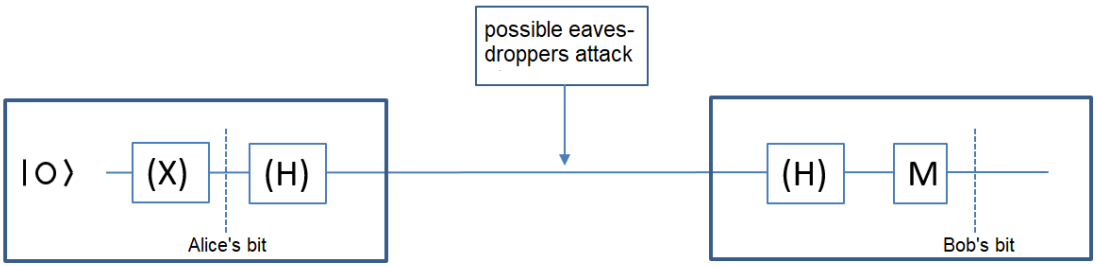
iv.) Alice and Bob connect via the classic channel.

If exactly one of them applied H, the bit is discarded.

Otherwise:

With probability 1/2 they agree to use the bit.

With probability 172 they agree to not use the bit, but compare their bits with probability 1/2 and then discard them.
If their bits are different, this proves the existence of an eavesdropper on the line (or a faulty line).



Analysis:

i.) The method works correctly if there is no eavesdropper "Eve" and the channel is not faulty, because the two H's cancel each other out.

ii.) Because of the no cloning theorem (see below) the eavesdropper cannot clone the qubit and send a copy on to Bob.

iii.) If the eavesdropper does not intervene in the quantum channel, he/she gets only the information which Hadamard transformations Alice and Bob have applied (which are two random bits). He gets no information about the bit itsself.

iv.) For the analysis of the success of eavesdropping attacks, it is sufficient to consider the following four different situations:

		
No comparison of bits		
Comparison of bits		

Reason: A situation is described by the following parameters:

• Information whether $|a\rangle = |0\rangle$ or $|a\rangle = |1\rangle$, where $|a\rangle$ denotes the state of the qubit in Alice after the possible application of Pauli-X;

• Information as to whether Alice applied H;

• Information as to whether Bob applied H;

• Information as to whether Alice and Bob compared their bits (and then discarded them).

These are $2^4 = 16$ situations.

On average every second situation is rejected because Alice and Bob used exactly one Hadamard transformation. These situations do not need to be considered further - they only double the effort, but are not a safety concern.

For the analysis of attacks by an eavesdropper, we o.B.d.A. assume it is $|a\rangle = |0\rangle$. Because the analyzes can be transferred directly to the case $|a\rangle = |1\rangle$.

v.) To analyze a situation, the following questions must be answered:

• Is $|b\rangle = |0\rangle$? That answers whether the key exchange between Alice and Bob was disrupted by Eve's intervention.

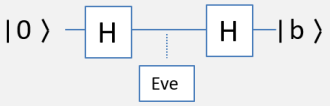
• Is $|e\rangle = |0\rangle$? That answers whether Eve has the right bit in her hands.

• Will Eve be discovered?

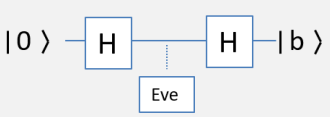
vi.) For every possible attack these three questions must be answered for each of the four fields. Because Eve is in one of the four situations during the eavesdropping attack, that both have applied H or both have not, and that a bit comparison will or will not take place, **but at the time of the attack does not know in which**.

Exercise in the lecture:

a.) Analysis of the CNOT attack (i.e., Eve uses the qubit in the channel as a control bit for her own qubit initialized with $|0\rangle$):

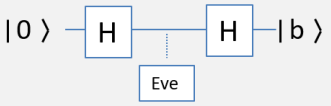
		
No comparison of bits	Is |b> = |0>? Is |e> = |0>? Will Eve be revealed?	Is |b> = |0>? Is |e> = |0>? Will Eve be revealed?
Comparison of bits	Is |b> = |0>? Is |e> = |0>? Will Eve be revealed?	Is |b> = |0>? Is |e> = |0>? Will Eve be revealed?

Result:

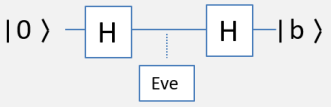
		
No comparison of bits	Is |b> = |0>? Yes Is |e> = |0>? Yes Will Eve be revealed? No	Is |b> = |0>? With probability 1/2 Is |e> = |0>? With probability 1/2 Will Eve be revealed? No
Comparison of bits	Is |b> = |0>? Yes Is |e> = |0>? Yes Will Eve be revealed? No	Is |b> = |0>? With probability 1/2 Is |e> = |0>? With probability 1/2 Will Eve be revealed? With prob. 1/2

.

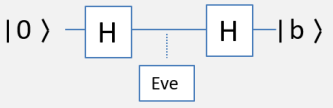
b.) Analysis of the measure-and-forward attack (i.e., Eve measures the qubit in the channel and feeds the measurement result back in):

		
No comparison of bits	Is |b> = |0>? Is |e> = |0>? Will Eve be revealed?	Is |b> = |0>? Is |e> = |0>? Will Eve be revealed?
Comparison of bits	Is |b> = |0>? Is |e> = |0>? Will Eve be revealed?	Is |b> = |0>? Is |e> = |0>? Will Eve be revealed?

Result:

		
No comparison of bits	Is |b> = |0>? Yes Is |e> = |0>? Yes Will Eve be revealed? No	Is |b> = |0>? With probability 1/2 Is |e> = |0>? With probability 1/2 Will Eve be revealed? No
Comparison of bits	Is |b> = |0>? Yes Is |e> = |0>? Yes Will Eve be revealed? No	Is |b> = |0>? With probability 1/2 Is |e> = |0>? With probability 1/2 Will Eve be revealed? With prob. 1/2

c.) Analysis of the H-Measure-H-Forward attack (i.e., Eve applies H to the qubit in the channel, measures, applies H again and forwards the qubit thus obtained to Bob):

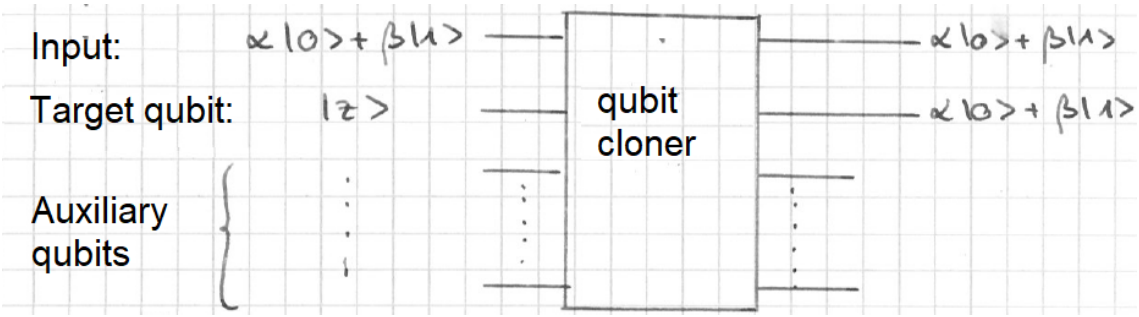
		
No comparison of bits	Is |b> = |0>? Is |e> = |0>? Will Eve be revealed?	Is |b> = |0>? Is |e> = |0>? Will Eve be revealed?
Comparison of bits	Is |b> = |0>? Is |e> = |0>? Will Eve be revealed?	Is |b> = |0>? Is |e> = |0>? Will Eve be revealed?

Note: The situation of the eavesdropper in the BB84 protocol is the reason why it is often written that eavesdroppers are discovered in quantum cryptography.
The exact statement is (for the attacks by Eve considered in this lecture):
• With probability 1/2 Eve has the correct bit and is not discovered (complete success for Eve);
• with probability 1/2 Eve has just a random bit in her hands, does not helpher any further;
• with a probability of 1/4 Bob has just a random bit in his hands after an attack;
• Eve is revealed with a probability of 1/8 (but this means that, for example, with 25 eavesdropping attacks, Eve remains unrevealed only with a probability of $(7/8)^{25} <\approx 0.035$).

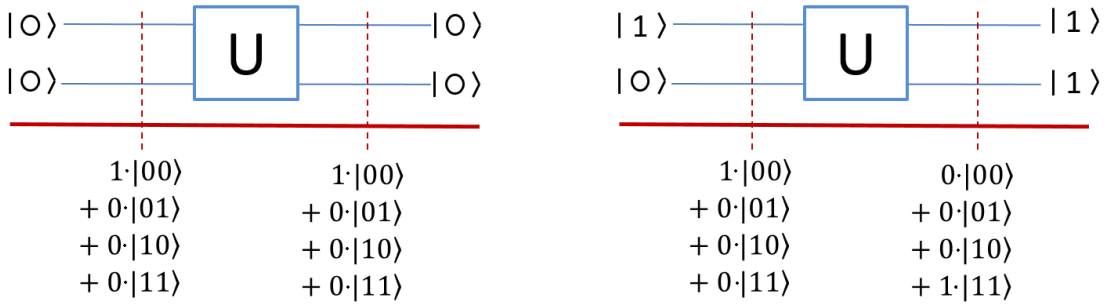
Eve cannot read the qubit sent in the quantum channel without (at least in some cases) changing the qubit Bob receives, since qubits cannot be cloned. This is the subject of the following famous theorem.

Theorem: (No Cloning Theorem)
There is no quantum circuit that clones any qubit to a target bit.

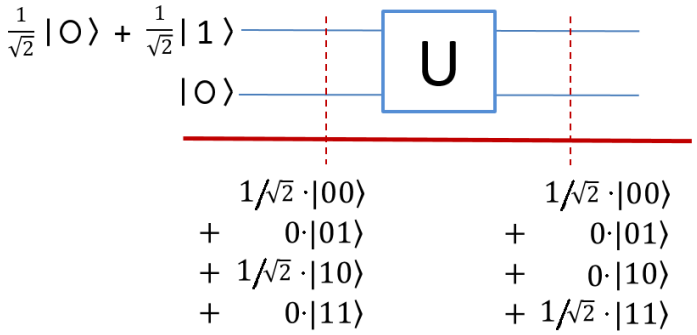
Illustration: There is no such thing:



Idea of proof: Special case: No auxiliary bits, and target bit initialized with $|0\rangle$.
If there was a cloner, than it would perform a unitary transformation U on two qubits, and would clone both the state $|0\rangle$ and the state $|1\rangle$ of the input bit. Thus: $U|00\rangle = |00\rangle$ and $U|10\rangle = |11\rangle$:



Therefore, on input $1/\sqrt{2} \cdot |0\rangle + 1/\sqrt{2} \cdot |1\rangle$ the cloner yields $U(1/\sqrt{2} \cdot |00\rangle + 1/\sqrt{2} \cdot |10\rangle$, which is $1/\sqrt{2}(|00\rangle + |11\rangle)$.



This is not the clone of the input, however. The clone of the input would be the status $0.5 \cdot (|00\rangle + |01\rangle + |10\rangle + |11\rangle)$.

Complete proof: (According to Homeister, "Quantencomputing verstehen", p. 82)
Assume there is a qubits cloner like in the illustration above. Let u be the unitary transformation it performs, and let $|s\rangle$ be the initial state of the target bit and the auxiliary bits. Then the following applies to every state $|q\rangle$ of the input bit:

$$U(|q\rangle \otimes |s\rangle) = |q\rangle \otimes |q\rangle \otimes |s_q\rangle$$

with an input-dependent output state $|s_q\rangle$ of the auxiliary bits.

Applying this to two different input bits $|q_1\rangle$ and $|q_2\rangle$, we get

$$U(|q_1\rangle \otimes |s\rangle) = |q_1\rangle \otimes |q\rangle \otimes |s_{q_1}\rangle \quad \text{and}$$
$$U(|q_2\rangle \otimes |s\rangle) = |q_2\rangle \otimes |q\rangle \otimes |s_{q_2}\rangle$$

Unitary transformations are angle-preserving, so the scalar products of the original images and the images always are the same. Therefore $< Uv|Uw >=< v|w >$ for all vectors v, w. This imlies

$$< q_1 \otimes s \,|\, q_2 \otimes s >=< q_1 \otimes q_1 \otimes s_{q_1} \,|\, q_2 \otimes q_2 \otimes s_{q_2} >$$

Since the inner product and the tensor product are compatible, we can transform:

$$< q_1 \,|\, q_2 >< s \,|\, s >=< q_1 \,|\, q_2 >< q_1 \,|\, q_2 >< s_{q_1} \,|\, s_{q_2} >$$

This equation is fulfilled when $< q_1 \,|\, q_2 >= 0$, ie if q_1 and q_2 are perpendicular.
Otherwise it can be transformed to

$$< s \,|\, s >=< q_1 \,|\, q_2 >< s_{q_1} \,|\, s_{q_2} >$$

so (since $|s\rangle$ is the state of a sub-register and thus $< s \,|\, s >= 1$):

$$1 =< q_1 \,|\, q_2 >< s_{q_1} \,|\, s_{q_2} >$$

Since q_1, q_2, s_{q_1} and s_{q_2} are register states and thus have length 1, their inner products are of absolute value at most 1. The 1 is only achieved in case of parallelism. Thus, the equation can only be fulfilled if q_1 and q_2 are parallel.

Terefore, if a cloner clones the state $|q\rangle$ of one of the qubits correctly, then apart from this state it can only clone parallel or orthogonal qubits. That means there is no cloner able to clone arbitrary qubits. Q.e.d.

3.5 Dense coding

An excursion into information theory: Here we deal with the information (and the redundancies) contained in messages, and the dense, minimum spacerequirering storage of information on bits and qubits.

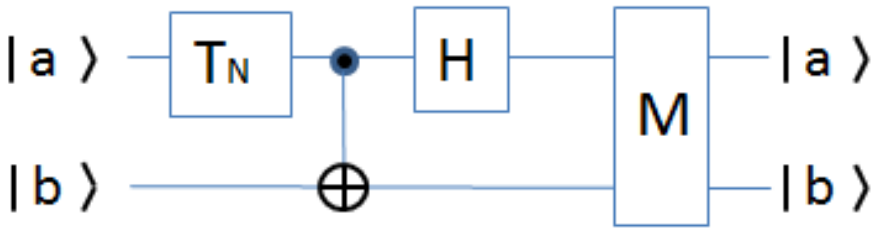
We shall see: It is possible to transport the information of two classic bits transporting only one qubit, if this qubit is part of an EPR pair.

Task: Alice wants to send one of four messages $N = (x, y) \in \{(0,0),(0,1),(1,0),(1,1)\}$ to Bob.
Alice and Bob both have one of two entangled qubits $|a\rangle, |b\rangle$ in the state $|ab\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
Moreover, they have the possibility to send one qubit using a quantum channel.

Solution: Alice selects the transformation T_N that is dependent on the message defined as follows:

$$T_N = \begin{cases} ID, & \text{falls } N = (0,0) \\ X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, & \text{falls } N = (0,1) \\ Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, & \text{falls } N = (1,0) \\ Z \cdot X = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, & \text{falls } N = (1,1) \end{cases}$$

She applies T_N to $|a\rangle$ and sends her qubit to Bob.
Bob applies CNOT to $|ab\rangle$, and measures both bits.
If the result of the measurement is $|xy\rangle$, then $N = (x, y)$, where $x, y \in \{0, 1\}$.



Proposition: The procedure works correctly in all 4 cases.

Proof: Is an exercise, please distinguish between the four possible cases.

Remark: i.) Idea of proof algebraically: The unitary matrix of Bob's transformation is

$$U = (H \otimes Id) * CNOT = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & -1 & 0 \end{pmatrix}$$

Selecting transformation T_N Alice, decides whether the first and last column or the second and third column will be measured, and whether they will be added or subtracted beforehand.

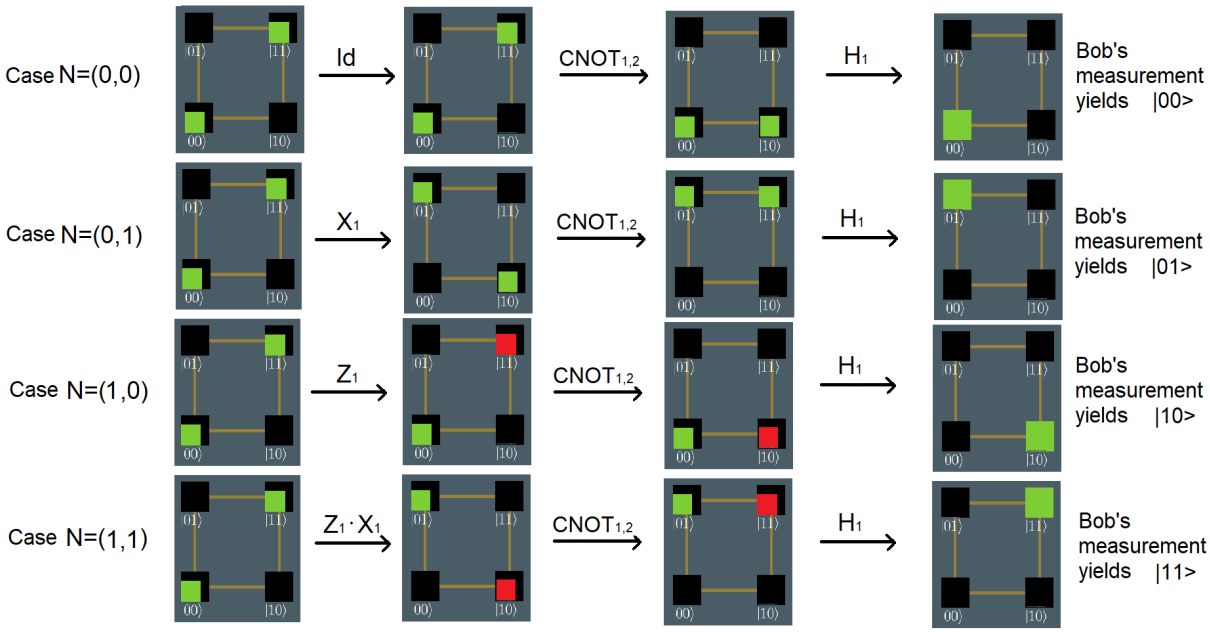
ii.) How does somebody come up with something like that?
The state space of two qubits, a $\mathbb{R}^2 \otimes \mathbb{R}^2$, has the standard basis vectors $|00\rangle, |01\rangle, |10\rangle$ and $|11\rangle$. Every vector in the state space is therefore a linear combination $\sum_{i=0}^{3} \alpha_i |i\rangle$.

The following vectors also form a basis of the state space, the Bell basis formed by Bell states:

$$\Phi^+ = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad , \quad \Phi^- = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \quad ,$$
$$\Psi^+ = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \quad , \quad \Psi^- = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

The Bell basis is quite well known, and the idea of the algorithm is that Alice puts her qubit in one of the four Bell states. Both qubits are then transformed back into one of their 4 basis states by CNOT and Hadamard.

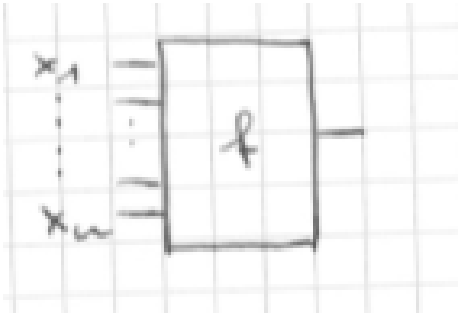
iii.) Graphical illustration of the dense coding, one line per case:



3.6 Decipher quantum oracles

The algorithms of Deutsch, Deutsch-Jozsa and Bernstein-Vazirani

Definition: A (classical) oracle for a function $f : \{0,1\}^n \to \{0,1\}$ is a black box with n input bits and one output bit that calculates the function:

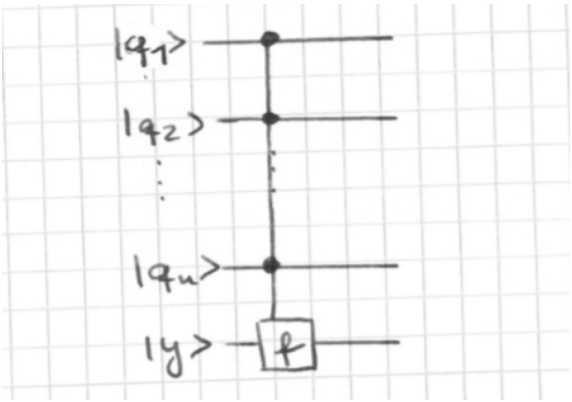


Applications: e.g. Complexity Theory, NP completeness proofs: Here the oracle is a polynomial function verifying whether a given input fulfills the condition of the language.

Remarks: Reverse engineering: Let the oracle be given, search for the function f. What is the complexity of this task?:

- Without further information one has evaluate 2^n inputs, so call the oracle has to be called 2^n times.
- With additional information, you may get by with fewer calls to the oracle. If e.g. $f = const$ is known, one single call of the oracle (with an arbitrary input) is sufficient to determine f.

Definition: A quantum oracle for $f : \{0,1\}^n \to \{0,1\}$ is a quantum gate with $n+1$ inputs



and the following effect on the base states

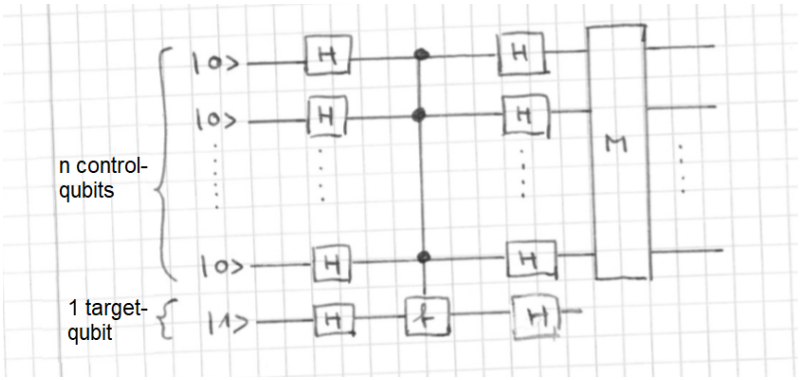
$$|x_1 \cdots x_n y\rangle \mapsto |x_1 \cdots x_n\rangle |y \oplus f(x)\rangle$$

In other words: A binary negation is applyt to the y-qubit, if and only if $f(x_1, \cdots, x_n) = 1$

Task now: Given the quantum oracle for f and additional information that f is either constant (ie either 1 everywhere or 0 everywhere), or balanced (ie, exactly on 2^{n-1} Inputs f is 0, and on the other 2^{n-1} inputs f is 1. Decide whether f is balanced or constant.

Comment: Calls necessary for a classic oracle: In the worst case $2^{n-1}+1$ calls.
It will be shown: One can do it with a single call from the quantum oracle.

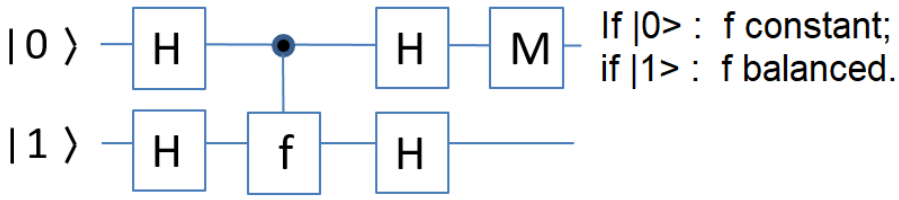
Proposition: (Algorithm of Deutsch-Jozsa, 1992) Let $f : \{0,1\}^n \to \{0,1\}$ be constant or balanced. Then the following quantum circuit delivers the result $|0\cdots 0\rangle$ if and only if f is constant:



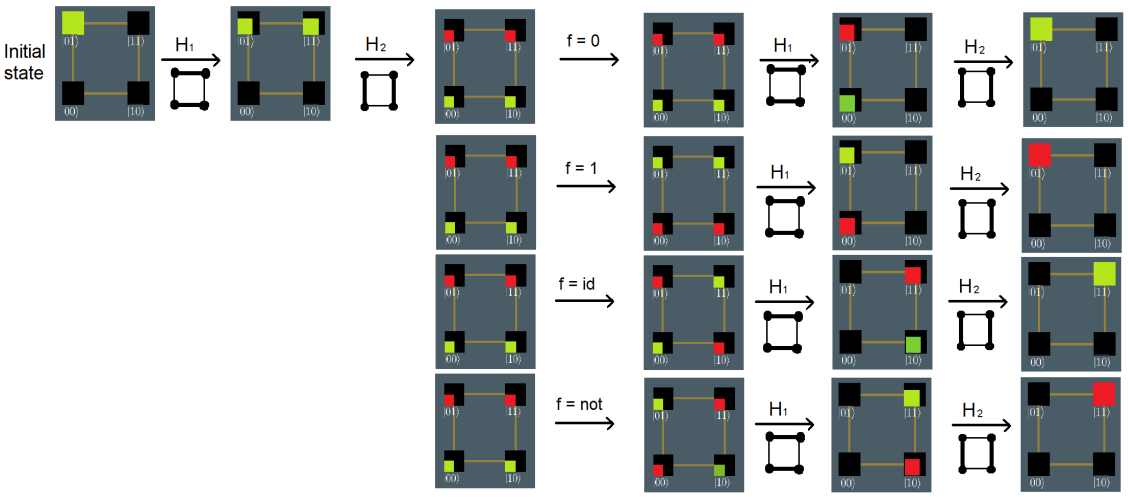
Note:

i.) How can that be: The control bits are transformed, used for control (not measured!). And transformed back, and change their state?
They do so, because the signs of the amplitudes of the basis states $(x_1, \cdots, x_n)$ are altered when the quantum oracle is called and if $f(x_1, ..., x_n) = 1$ applies.

ii.) Illustration for $n = 1$: Circuit:



Graphical analysis:



Measuring the first qubit yields $|0\rangle$ if f was constant, and $|1\rangle$ if f is the identity or the NOT (ie is balanced).

iii.) For $n \geq 2$ the graphical illustration comes to its limits.
Not every function of $n \geq 3$ bits is constant or balanced (which is the case for $n = 2$).
Example: Applying the Deutsch-Josza algorithm to the quantum oracle of the AND function, the final state is:
$0.5 \cdot (|001\rangle + |011\rangle + |101\rangle - |111\rangle)$
(if you want, see for yourself).

Proof: (correctness of the Deutsch-Jozsa for any n)

- After applying the first Hadamard transformations, the register is in the state

$$\frac{1}{\sqrt{2}^{n+1}} \cdot (|0\rangle + |1\rangle)^n \cdot (|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}^{n+1}} \cdot \Big(\sum_{\substack{x \in \{0,1\}^n \\ x = (x_1, \cdots, x_n)}} |x_1 \cdots x_n\rangle \Big) \cdot (|0\rangle - |1\rangle)$$

- After applying the quantum oracle, the register is in the state

$$|\psi\rangle = \frac{1}{\sqrt{2}^{n+1}} \cdot \Big(\sum_{x \in \{0,1\}^n} |x_1 \cdots x_n\rangle \cdot (-1)^{f(x)} \Big) \cdot (|0\rangle - |1\rangle)$$

This holds, since:

If $f(x_1, \cdots, x_n) = 0$, the quantum oracle transfers the state

$$\frac{1}{\sqrt{2}}|x_1 \cdots x_n\rangle \cdot (|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}}(|x_1 \cdots x_n 0\rangle - |x_1 \cdots x_n 1\rangle)$$

in itself, so the new state can also be written as

$$(-1)^{f(x)}|x_1 \cdots x_n\rangle \cdot (|0\rangle - |1\rangle)$$

If $f(x_1, \cdots, x_n) = 1$, the quantum oracle transfers the state

$$\frac{1}{\sqrt{2}}|x_1 \cdots x_n\rangle(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}}(|x_1 \cdots x_n 0\rangle - |x_1 \cdots x_n 1\rangle)$$

to

$$\frac{1}{\sqrt{2}}(|x_1 \cdots x_n 1\rangle - |x_1 \cdots x_n 0\rangle) = \frac{1}{\sqrt{2}}|x_1 \cdots x_n\rangle \cdot (|1\rangle - |0\rangle) = (-1)^{f(x)} \cdot |x_1 \cdots x_n\rangle \cdot (|0\rangle - |1\rangle)$$

- Now let H_n be the n-fold tensor product of the Hadamard matrix $\frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$.

  one can easily verify, that in the first row of of H_n, each entry is the number $\frac{1}{\sqrt{2^n}}$. (Further properties of H_n are an exercise)

  H_n is a unitary transformation (because it is a tensor product of unitary transformations).

  By applying $H_n \otimes H$ ot the state $|\psi\rangle$, it is converted to a state

  $$\Big(\sum_{x \in \{0,1\}^n} \alpha_x \cdot |x_1 \cdots x_n\rangle\Big) \cdot |1\rangle$$

  for certain $\alpha_x \in \mathbb{C}$ with $\sum |\alpha_x|^2 = 1$

  We consider $\alpha_{0\cdots 0}$, the first element of the vector

  $$H_n \cdot \frac{1}{\sqrt{2^n}} \cdot \underbrace{\begin{pmatrix} (-1)^{f((0\cdots 0))} \\ (-1)^{f((0\cdots 01))} \\ \vdots \\ (-1)^{f((1\cdots 1))} \end{pmatrix}}_{:=v}$$

If f is constant, all coefficients of v are identical (+1 or -1), and so we have $\alpha_{0\cdots 0} = \pm\frac{1}{\sqrt{2^n}} \cdot 2^n \cdot \frac{1}{\sqrt{2^n}} = 1$

But then $\alpha_x = 0$ is for all $x \neq (0, \cdots, 0)$, because otherwise it would be $\sum_x |\alpha_x|^2 > 1$.

The measurement therefore yields the state $|0 \cdots 0\rangle$.

If f is balanced, exactly half of the coefficients of v have the value 0, the other half the value 1. So we have
$\alpha_{0\cdots 0} = 0$, and the measurement will never yield the value $|0 \cdots 0\rangle$. Q.e.d.

Exercise: Understand the Deutsch-Jozsa algorithm for $n = 1$ and $n = 3$ explicitely.
(Optional: Also the Bernstein-Vazirani algorithm, below, if you want to read it yourself;)).

The algorithm of Bernstein-Vazirani (1993):

Background: In Deutsch-Jozsa's algorithm, the state $|0 \cdots 0\rangle$ will never be measured for balanced f, but will always be measured for constant f.
Bernstein and Vazirani found in 1993 that other functions f yield other states "completely or not at all". An example is the following algorithm by Bernstein-Vazirani (although the critical reader will already notice that these algorithms were not yet able to bring quantum computing out of its shadowy existence - this was only achieved by Shor's factorization algorithm in 1994).

Input: A quantum oracle for $f : \{0,1\}^n \to \{0,1\}$, for which is known:

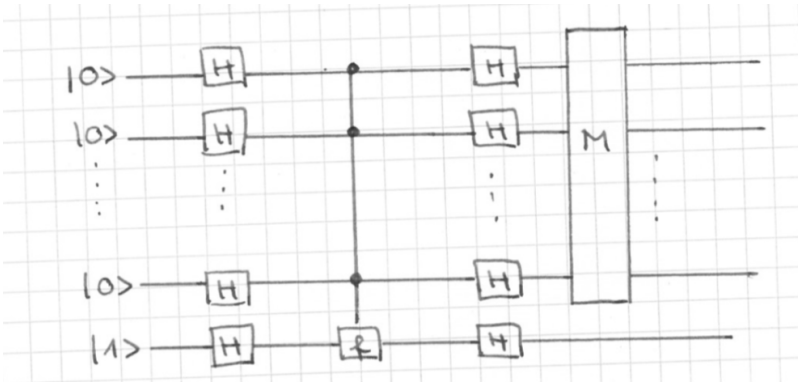
$$f(x_1, \cdots, x_n) = (x_1, \cdots, x_n) * (a_1, \cdots, a_n) \text{for some} a \in \{0,1\}^n \quad ,$$

where * denotes the inner product mod 2.

Output: $a \in \{0,1\}^n$

Procedure:

i.) Apply the quantum circuit of the Deutsch-Jozsa algorithm:



ii.) Output the measurement result $a \in \{0,1\}^n$.

Number of gates: Just one oracle call, $2(n+1)$ Hadamard gates (Remark: $2n+1$ gates are also sufficient, because y at the end needs not to be transformed with H at the end), and one measurement of n qubits.

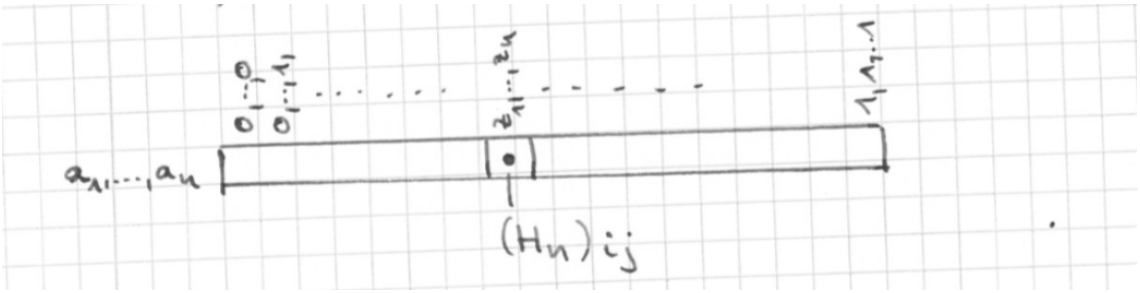
Correctness: As in the analysis of the Deutsch-Jozsa algorithm, one verifies: The state of the quantum register before mesasurement is

$$\left(\sum_{k=0}^{2^k-1} \alpha_k |k\rangle\right) \cdot |1\rangle.$$

Here we denoted

$$\begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{2^n-1} \end{pmatrix} = H_n \cdot \frac{1}{\sqrt{2}^n} \cdot \begin{pmatrix} (-1)^{f(0,\cdots,0,0)} \\ (-1)^{f(0,\cdots,0,1)} \\ (-1)^{f(0,\cdots,1,0)} \\ \vdots \\ (-1)^{f(1,\cdots,1,1)} \end{pmatrix}$$

Let i be the index that belongs to $(a_1, \cdots, a_n)$, i.e. $i = \sum_{k=1}^{n} a_k 2^{n-k}$.
We consider the i-th row of the Hadamard matrix H_n. Let $j \in \{0, \cdots, 2^n - 1\}$ be a column index, $j = \sum_{k=1}^{n} z_k 2^{n-k}$ for some $z_1, \cdots, z_n \in \{0,1\}$.



Then (verifying this is an exercise)

$$(H_n)_{ij} = \frac{1}{\sqrt{2}^2} \cdot (-1)^{(a_1,\cdots,a_n) \cdot (z_1,\cdots,z_n)}$$

Therefore

$$\alpha_i = \frac{1}{2^n} \cdot \sum_{z \in \{0,1\}^n, z=(z_1,\cdots,z_n)} (-1)^{(a_1,\cdots,a_n)*(z_1,\cdots,z_n)} \cdot (-1)^{f(z_1,\cdots,z_n)} = 1$$

since $f(z_1, \cdots, z_n) = (a_1, \cdots, a_n) \cdot (z_1, \cdots, z_n)$.
(Please convince yourself: the -1s meet the -1s, the +1s meet the +1s).
So, since the sum over the amplitudes' squares is 1, we have $\alpha_j = 0$ for all the other $j \in \{0, \cdots, 2^{n-1}\} \setminus \{i\}$.

Measuring the first n bits of the register therefore yields the status $|i\rangle$, ie $|a_1, \cdots, a_n\rangle$. Q.e.d.

4 Quantum Error Correction

Learning outcomes: Given a quantum circuit that maybe changes qubits (due to decoherence of quantum noise).
Have understood that and how an error correction is possible, also though qubits cannot be read without changing them and cannot be cloned either.

4.1 Basic idea of quantum error correction

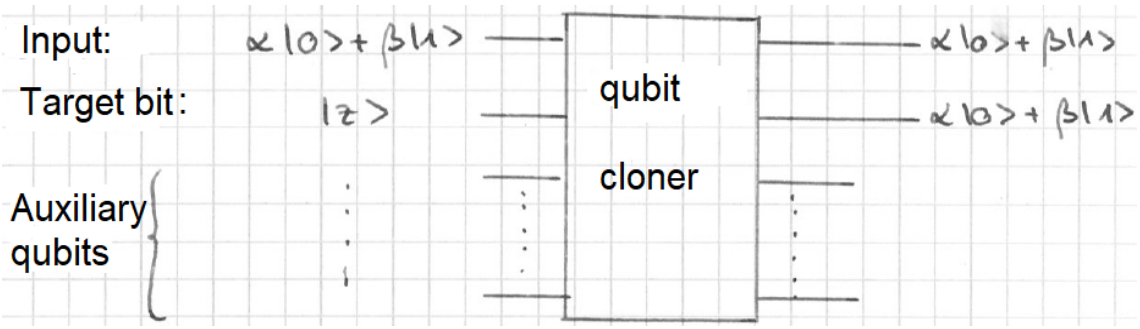
Reminder Classical error correction:

- The bit to be sent is sent three times.
- If the receiver receives unequal bits, an error has occurred.
- The receiver corrects according to "majority decision".
- It works "well", where "well" is the subject of analysis.

Does not work for quantum channels because of the no-cloning theorem (see BB84 protocol, section 3.4, here repeated):

Proposition: (No cloning theorem)
There is no quantum circuit that copies any qubit to a target bit.

Illustration: There is no such thing:



The classic way of detecting and correcting errors therefore does not work with qubits.

Basic idea Quantum error correction:

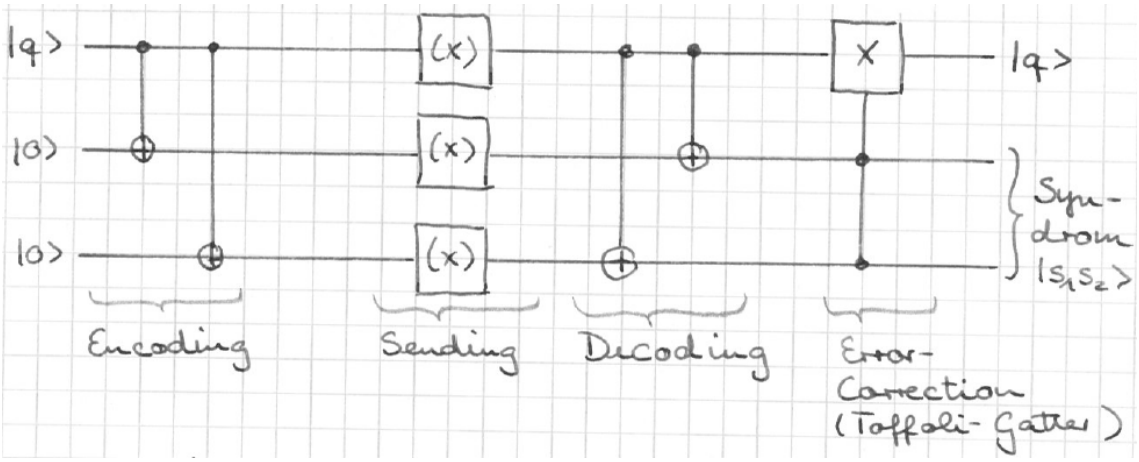
- $|q\rangle = \alpha|0\rangle + \beta|1\rangle$ is the qubit to be sent.
- Generate state $\alpha \cdot |0 \cdots 0\rangle + \beta|1 \cdots 1\rangle$
  (note: $\alpha \cdot |0 \cdots 0\rangle + \beta|1 \cdots 1\rangle \neq (\alpha \cdot |0\rangle + \beta|1\rangle)^n$).
- Send all qubits.
- Measure all of the qubits except the first one.
- correct the first qubit accordingly.

Error types that can change a qubit $|q\rangle = \alpha \cdot |0\rangle + \beta \cdot |1\rangle$ while traveling the channel:

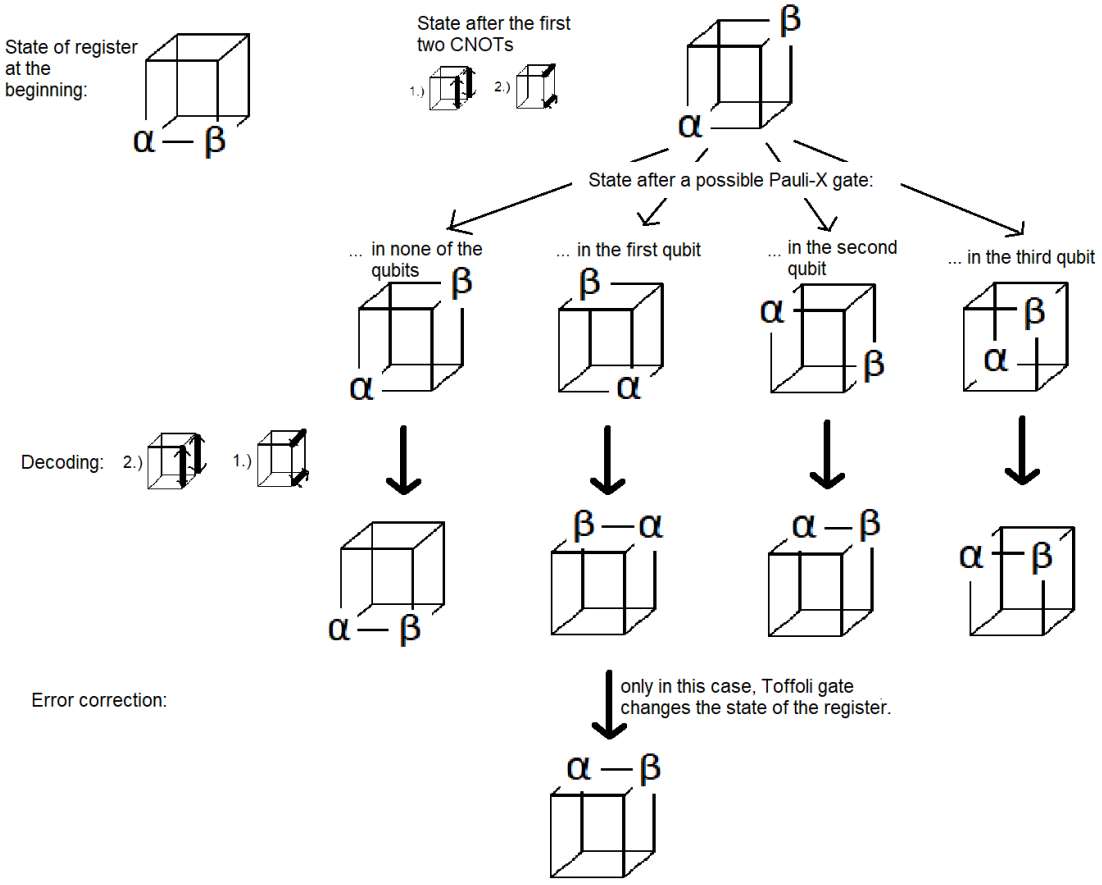
- Bit flip: $\alpha \cdot |0\rangle + \beta \cdot |1\rangle \mapsto \beta \cdot |0\rangle + \alpha \cdot |1\rangle$, thus $|q\rangle \mapsto X|q\rangle$
- Phase flip: $\alpha \cdot |0\rangle + \beta \cdot |1\rangle \mapsto \alpha \cdot |0\rangle - \beta \cdot |1\rangle$, thus $|q\rangle \mapsto Z|q\rangle$
- Combinations:
  $\alpha \cdot |0\rangle + \beta \cdot |1\rangle \mapsto \beta \cdot |0\rangle - \alpha \cdot |1\rangle$, thus $|q\rangle \mapsto ZX|q\rangle$, and
  $\alpha \cdot |0\rangle + \beta \cdot |1\rangle \mapsto -\beta \cdot |0\rangle + \alpha \cdot |1\rangle$, also $|q\rangle \mapsto XZ|q\rangle$
- Any error: $U = \begin{pmatrix} u & v \\ -v & u \end{pmatrix}$ or $U = \begin{pmatrix} u & v \\ v & -u \end{pmatrix}$,
  $\alpha \cdot |0\rangle + \beta \cdot |1\rangle \mapsto (\alpha u + \beta v) \cdot |0\rangle \pm (\alpha u - \beta v) \cdot |1\rangle$, so $|q\rangle \mapsto U|q\rangle$.

4.2 Correction bit flip: (3-qubit) Bit flip code

Proposition: The following circuit outputs the input bit $|q\rangle = \alpha|0\rangle + \beta|1\rangle$, if no qubit or exactly one qubit is flipped in the possibly faulty channel during sending.



Proof: Exercise. Graphical illustration:



Comment:

i.) A measurement of the syndrome does not necessarily have to be carried out. If carried out, it would deliver:
$|s_1 s_2\rangle = |00\rangle \Leftrightarrow$ no transmission error
$|s_1 s_2\rangle = |01\rangle \Leftrightarrow$ Bit flip in the 3rd qubit
$|s_1 s_2\rangle = |10\rangle \Leftrightarrow$ Bit flip in the 2nd qubit
$|s_1 s_2\rangle = |11\rangle \Leftrightarrow$ Bit flip in the 1st qubit.

ii.) Only in the case of the bit flip in the 1st qubit an error correction has to take place (this is exactly when the Toffoli gate acts).

iii.) If two or all three qubits are flipped when sending, the error correction no longer works (as in the classic case).

4.3 Correction phase flip

Phase flip to qubit: application of Pauli Z transformation $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
Effect on qubit: $\alpha_0|0\rangle + \alpha_1|1\rangle \mapsto \alpha_0|0\rangle - \alpha_1|1\rangle$.

Idea for error correction: Return to bit flip.

This works because of the following proposition:

Proposition: Let (as usual) $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.
Then
i.) $H \cdot X \cdot H = Z$ and
ii.) $H \cdot Z \cdot H = X$.

Proof:

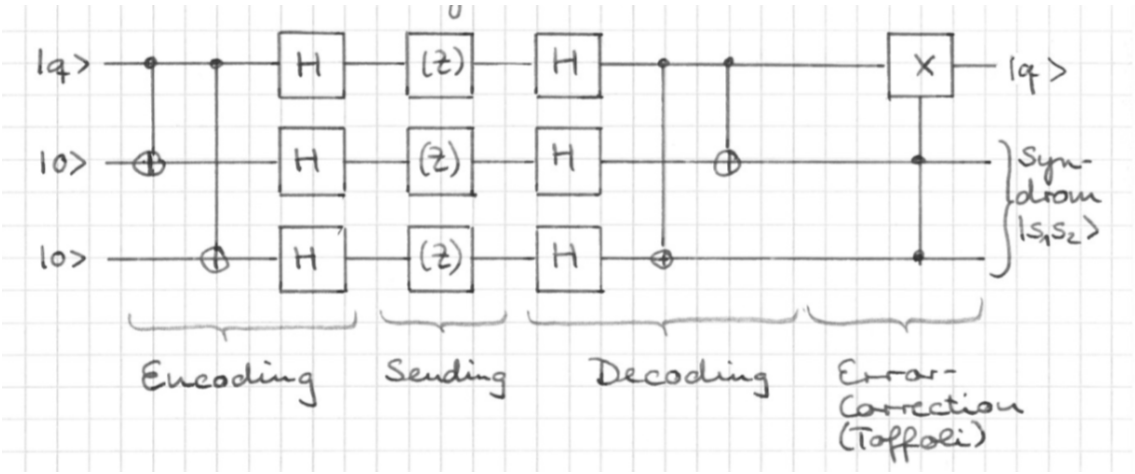
i.) The following can easily be checked:

$$\begin{aligned} H \cdot X \cdot H &= \frac{1}{2} \cdot \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \\ &= \frac{1}{2} \cdot \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \\ &= \frac{1}{2} \cdot \begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix} \\ &= Z \end{aligned}$$

ii.) One can conclude:

$$
\begin{aligned}
& H \cdot X \cdot H = Z && | \cdot \text{H from the left side} \\
\Longrightarrow \quad & H^2 \cdot X \cdot H = H \cdot Z && | \text{ apply } H^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\
\Longrightarrow \quad & X \cdot H = H \cdot Z && | \cdot \text{ H from the right side, and } H^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\
\Longrightarrow \quad & X = H \cdot Z \cdot H
\end{aligned}
$$

Theorem: The following circuit outputs the input qubit $|q\rangle = \alpha \cdot |0\rangle + \beta \cdot |1\rangle$, if a phase flip is applied to none or exactly one of the three qubits in the possibly faulty channel:



Proof: Since $H \cdot (Z) \cdot H = (X)$, the theorem follows from the correctness of the bit flip code.

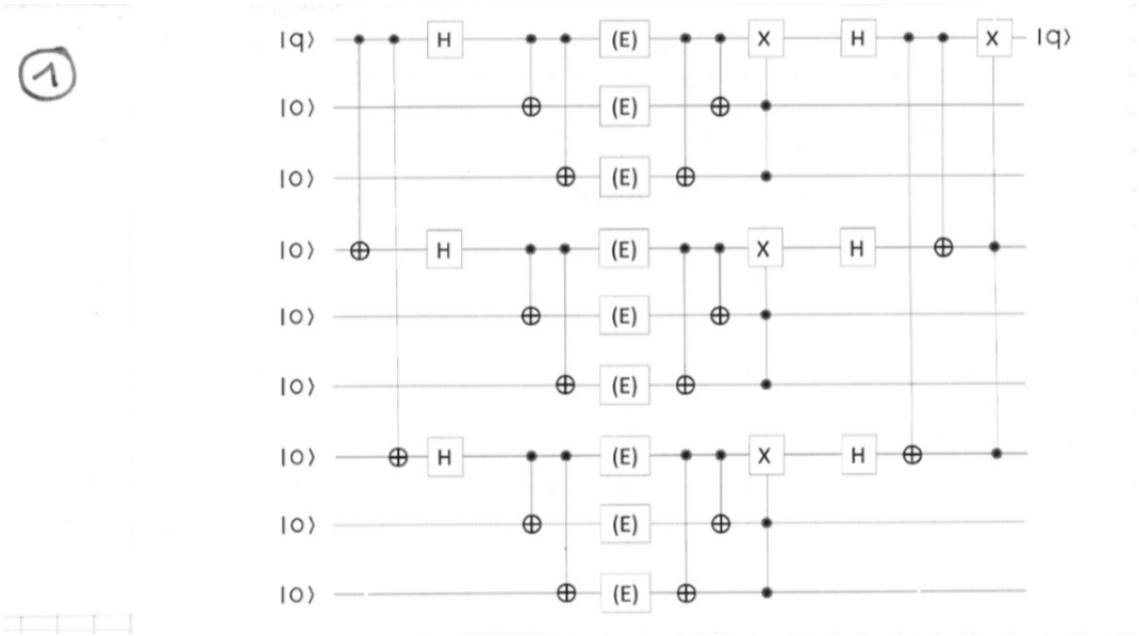
In other words: If a phase flip occurs in the above circuit in the i-th bit ($i \in \{1, 2, 3\}$), the circuit works exactly the way the bit flip code works, when a bit flip is in the i-th bit occurs. In the case of no error occuring, the circuit also works exactly like the bit flip code in the case of no error.

4.4 Correction of the combination of bit flip and phase flip: The Shor Code (1995)

Proposition: The following circuit (1) outputs the input qubit $|q\rangle = \alpha|0\rangle + \beta|1\rangle$ if one of the following transformations (E) is applied to at most one qubit in the possibly faulty channel:

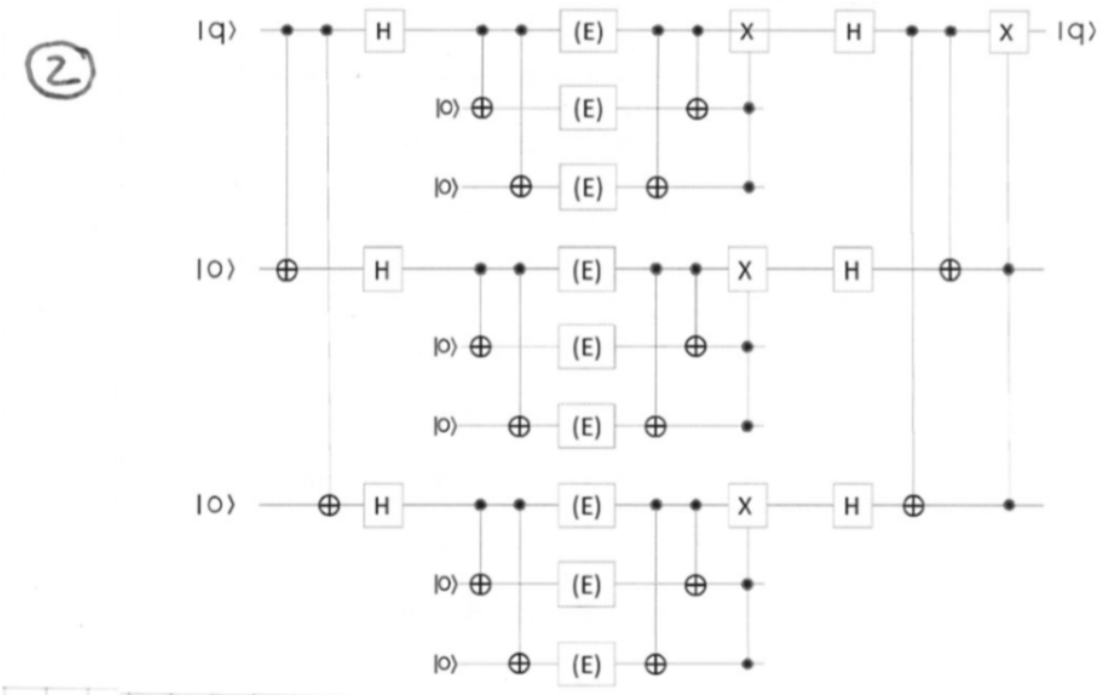
$$\begin{aligned} \text{Pauli X}: &\quad \alpha_0|0\rangle + \alpha_1|1\rangle \mapsto \alpha_0|1\rangle + \alpha_1|0\rangle \\ \text{Pauli Z}: &\quad \alpha_0|0\rangle + \alpha_1|1\rangle \mapsto \alpha_0|0\rangle - \alpha_1|1\rangle \\ \text{ZX}: &\quad \alpha_0|0\rangle + \alpha_1|1\rangle \mapsto \alpha_1|0\rangle - \alpha_0|1\rangle \end{aligned}$$

If XZ is used, i.e. $\alpha_0|0\rangle + \alpha_1|1\rangle \mapsto -\alpha_1|0\rangle + \alpha_0|1\rangle$, it returns $-|q\rangle = -\alpha|0\rangle - \beta|1\rangle$.

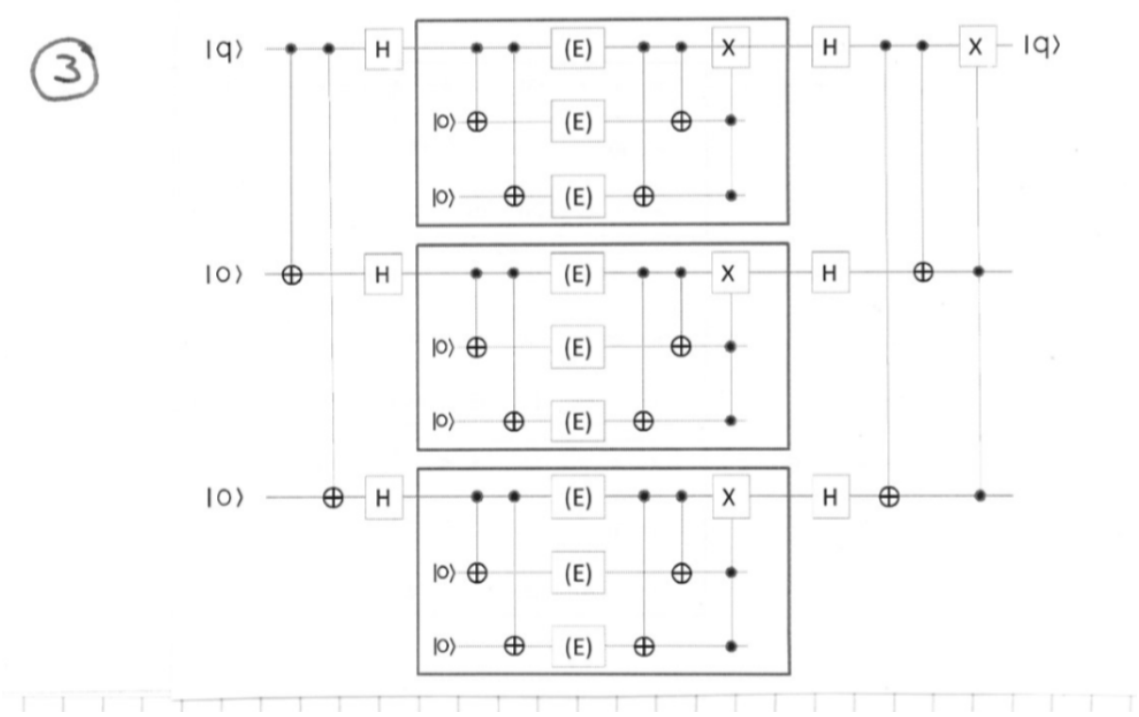


Note: Circuit by Shor (1995), has opened a research field of so-called "stabilizing quantum codes".

Proof: (No, we do not go into the state space of 9 qubits! ....)
Another representation of the circuit is (2):



This is an outer circuit calling the same inner circuit three times:



The inner circuit is the circuit of the 3 qubits flip code.
Completion of the proof is an exercise.

5 Adiabatic Quantum Computing

The company D-Wave in Canada has been propagating for several years that they can build quantum computers with hundreds (as of Octobr 2020: over 5,000) qubits.
The D-Wave computer, however, is not a quantum computer in the sense of the computational model considered so far.

Roughly speaking, the D-Wave computer works as follows: (Cited from german Wikipedia, "Quantum Computer", July 3rd, 2020)

"The idea of the adiabatic quantum computer is to construct a system that has a ground state still unknown in teh beginning of the computiation, and where the gorund state corresponds to the solution of a certain problem, and another /system) whose ground state can easily be prepared experimentally. The system, which is easy to prepare, is then transferred to the system whose ground state one is interested in, and its state is then measured. If the transition has taken place slowly enough, one gets the solution to the problem."

Example: You want to determine the minimum of a function f, you could prepare a system that corresponds to the function $g(x) = x^2$. Here the minimum $x = 0$ is known. Now, if one slowly (adiabatically) converts the function $g(x)$ to f, the minimum $x = 0$ is converted into the minimum of the function f.
The problems solvable by the D-Wave computer are approximation problems. The algorithms usually do not find the optimal solution, but a solution that is up to about 5 percent of the optimum. Good enough for most practical applications :).
So, truely "complex" problems of the future may no longer be the NP-complete problems, but those that have no approximate solutions, like factorization ;).
The physics of the D-Wave computer can no longer be explained with the simple model of a polarized light particle. The energy of the particle, i.e. its frequency (within the plane in which it vibrates) must now also be taken into account.
The model will only be briefly addressed at this event. D-Wave does not publish al lot on hw the computer works. However, since 2020, on can get access via Internet to the D-Wave Computer (make a google for "D-Wave" and "leap".

An interesting article about adiabatic quantum computing can be found in c't issue 12 from 2020. It also describes the problem of HOW to reformulate a given optimization problem into an input for a D-Wave computer.

With the economic stimulus package of June 2020, the German government has made EUR 2 billion available for research on quantum technologies. Germany should - also together in the European network - become globally competitive.

An IBM quantum computer will come to Germany at the beginning of 2021. There is a lot of research performed around the planet. It remains exciting :).