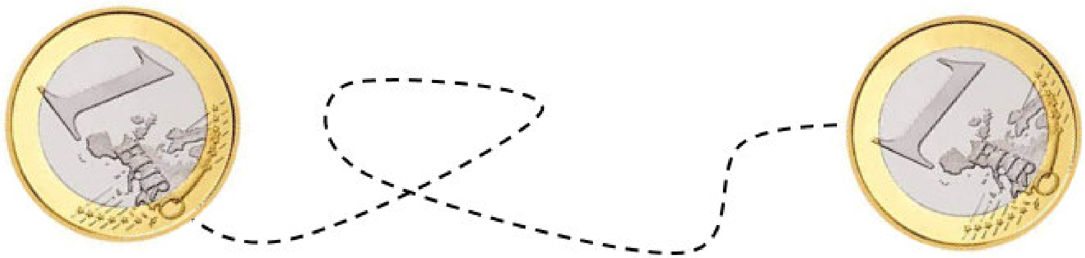
Some Basics of Quantum Computing

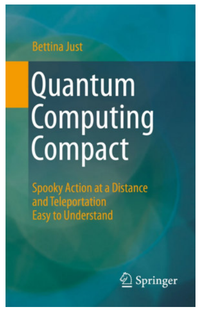


University of Potsdam, Dept. of Mathematics, 2024-04-10

Bettina Just, THM

Bettina Just:

- PhD in Math and Computer Science from Goethe-University Frankfurt/Main;
- Professor for mathematics and computer science at THM since 2010;
- Book „Quantencomputing kompakt: Spukhafte Fernwirkung und Teleportation endlich verständlich“, Springer 2020, english 2023;
- Since 2021 head of Competence-Center Quantumcomputing at TransMIT;
- More than 5.600 attendes of quantum-computing MOOCs at openHPI Potsdam: https://open.hpi.de/courses/qc-intro-1-2022/
- Aim: Provide an understandable access to quantum computing, although math. model is abstract, and many disciplines are involved ☺

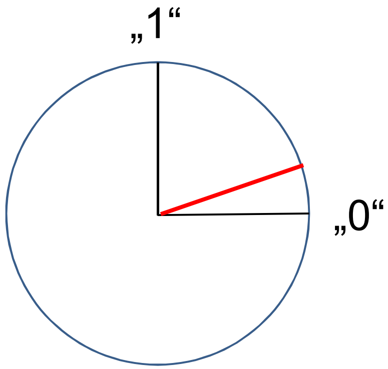


Intro: Comparison between classical bits and quantum bits

Classical bit:

- Object that can take states „0“ or „1“.

- Measurement of a bit does not change ist state („Realism “).



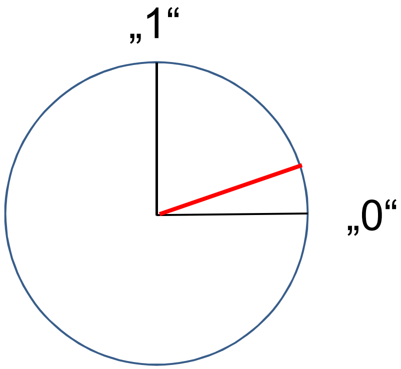
Quantum bit (qubit):

- Object that can take states $|0\rangle$ oder $|1\rangle$
  - or something in between.

- Measurement of a qubit always gives (and puts qubit to) state $|0\rangle$ oder $|1\rangle$.
  Thus if state was „in between“:
  Measurement changes the state of a qubit.

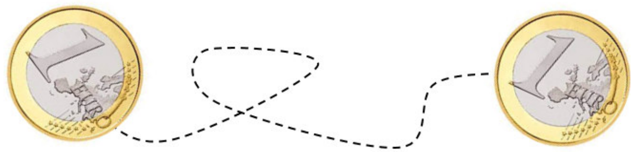
… classical bit:

- Change of one bit does not immediately change the properties of any other bit – takes light propagation time at least („Locality“).

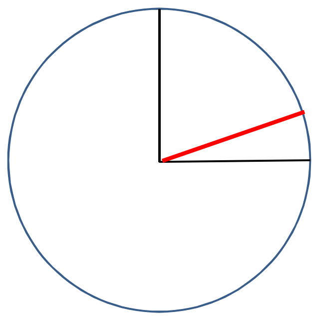


… quantum bit (qubit):

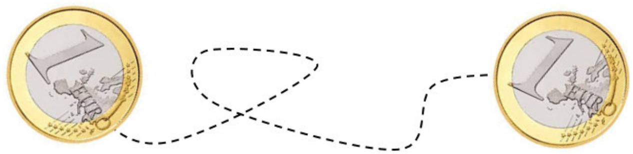
- Change of one qubit can immediately change properties of another qubit– faster than light propagation time, withouth using any known medium
  „Spooky action at a distance“
  „Entanglement“



… classical bit:



… quantum bit (qubit):



- Example of a state for register of n=3 bits: (1,1,0)

State space for register of n bits: $\{0,1\}^n$

- State and state space of a register of n qubits?

State and state space for a register of n=3 qubits

First Idea: Imagine 3 coins, not yet been tossed, able to communicate instantaneously …. they might agree on states:

0	$\sqrt{2/16}$	$\sqrt{1/2}$	0	$\vert 000\rangle$
$\frac{1+i}{2}$	0	0	0	$\vert 001\rangle$
0	$-\sqrt{2/16}$	0	0	$\vert 010\rangle$
0	$-\sqrt{3/16}$	0	0	$\vert 011\rangle$
0	$-\sqrt{1/16}$	0	0	$\vert 100\rangle$
0	$\sqrt{1/16}$	0	0	$\vert 101\rangle$
$\frac{1-i}{2}$	$\sqrt{4/16}$	0	0	$\vert 110\rangle$
0	$\sqrt{3/16}$	$\sqrt{1/2}$	1	$\vert 111\rangle$

State-space could be

$\{(\alpha_0, \dots, \alpha_7) \in \mathbb{R}^8_{\geq 0} : \alpha_0 + \alpha_1 + \alpha_2 = 1\}$?

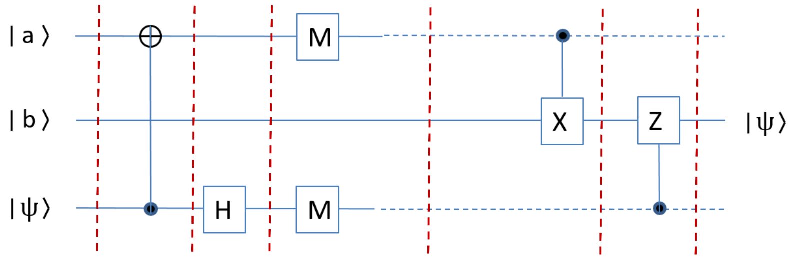
For physical and mathematical reasons: State-space is

$$\{(\alpha_0, \dots, \alpha_7) \in \mathbb{C}^8 : |(\alpha_0, \dots, \alpha_7)| = 1\}$$

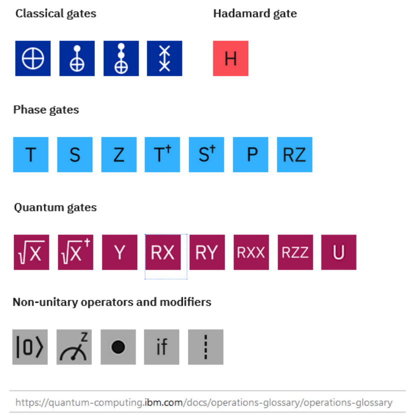
Example of a state:

$$|\psi\rangle = \frac{1}{\sqrt{2}}|000\rangle + \frac{1}{\sqrt{2}}|111\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

Universal model: Gate (circuit) model



Gates used:



Gate transforms system state to a new system state by applying unitary transformation:

$$\begin{array}{rl} & \alpha_0 \cdot |000\rangle \\ + & \alpha_1 \cdot |001\rangle \\ + & \alpha_2 \cdot |010\rangle \\ + & \alpha_3 \cdot |011\rangle \\ + & \alpha_4 \cdot |100\rangle \\ + & \alpha_5 \cdot |101\rangle \\ + & \alpha_6 \cdot |110\rangle \\ + & \alpha_7 \cdot |111\rangle \end{array} \xrightarrow{\text{gate}} \begin{array}{rl} & \alpha'_0 \cdot |000\rangle \\ + & \alpha'_1 \cdot |001\rangle \\ + & \alpha'_2 \cdot |010\rangle \\ + & \alpha'_3 \cdot |011\rangle \\ + & \alpha'_4 \cdot |100\rangle \\ + & \alpha'_5 \cdot |101\rangle \\ + & \alpha'_6 \cdot |110\rangle \\ + & \alpha'_7 \cdot |111\rangle \end{array}$$

where

$$\begin{pmatrix} \\ \text{unitary matrix} \\ \\ \end{pmatrix} \cdot \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \alpha_4 \\ \alpha_5 \\ \alpha_6 \\ \alpha_7 \end{pmatrix} = \begin{pmatrix} \alpha'_0 \\ \alpha'_1 \\ \alpha'_2 \\ \alpha'_3 \\ \alpha'_4 \\ \alpha'_5 \\ \alpha'_6 \\ \alpha'_7 \end{pmatrix}$$

complex vectors, length 1

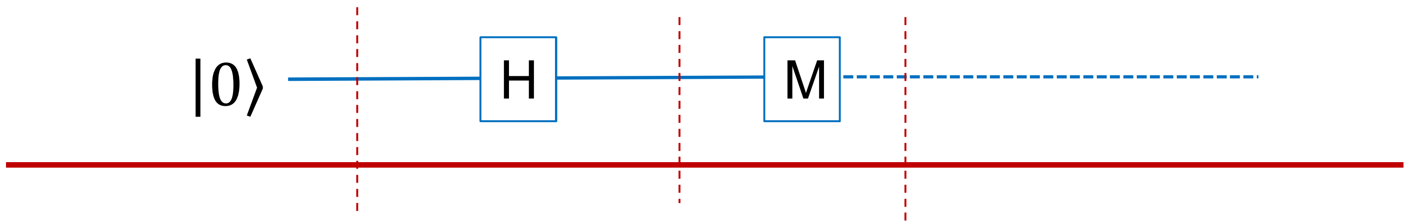
Measurement of a qubit is a projection and renormation to length 1.
Mathematical model of quantum mechanics is upspaced.

Unitaries that are physically possible are allowed.

Examples:

Recall: State of a register of n qubits is (represented by) a vector in $\mathbb{C}^{2^n}$

n=1: State of the „register“ of one qubit is $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ where $|\alpha_0|^2 + |\alpha_1|^2 = 1$.



$1 \cdot |0\rangle + 0 \cdot |1\rangle$

$\frac{1}{\sqrt{2}} \cdot |0\rangle + \frac{1}{\sqrt{2}} \cdot |1\rangle$

- With probability ½, result is $|0\rangle$
- With probability ½, result is $|1\rangle$

true randomness

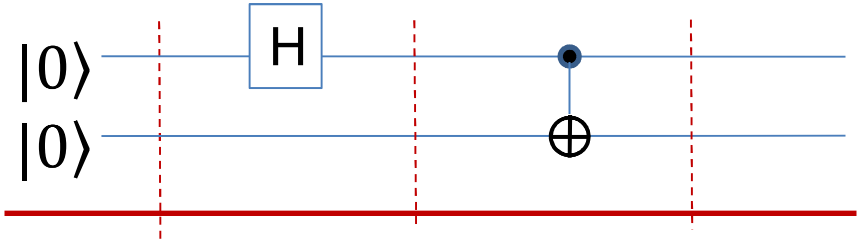
Unitary of Hadamard-Gate $H = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$

Measurement of $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ gives: $\begin{cases} |0\rangle \text{ with probability } |\alpha_0|^2 \\ |1\rangle \text{ with probability } |\alpha_1|^2 \end{cases}$

Examples:

Recall: State of a register of n qubits is (represented by) a vector in $\mathbb{C}^{2^n}$

n=2: State of the „register“ of one qubit is $|\psi\rangle = \alpha_0|00\rangle + \alpha_1|01\rangle + \alpha_2|10\rangle + \alpha_3|11\rangle$



Unitary of H ⊗ Id is $\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 0 & 1 & 0\\ 0 & 1 & 0 & 1\\ 1 & 0 & -1 & 0\\ 0 & 1 & 0 & -1\end{pmatrix}$ Unitary of CNOT-Gate is $\begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{pmatrix}$

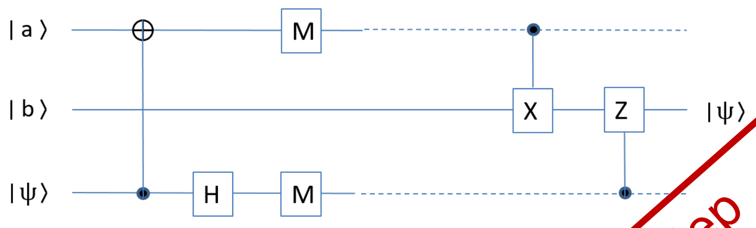
Circuit does $\begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{pmatrix} \cdot \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 0 & 1 & 0\\ 0 & 1 & 0 & 1\\ 1 & 0 & -1 & 0\\ 0 & 1 & 0 & -1\end{pmatrix} \cdot \begin{pmatrix}1\\ 0\\ 0\\ 0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ 0\\ 0\\ 1\end{pmatrix}$

thus $|\psi_{start}\rangle = |00\rangle$, $|\psi_{end}\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$

true randomness, entangled,
used to exchange random bits
cryptographically secure

My contribution: Visualizing quantum-algorithms

Why does teleportation work?



I can follow step by step …
but have no idea what is happening

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;

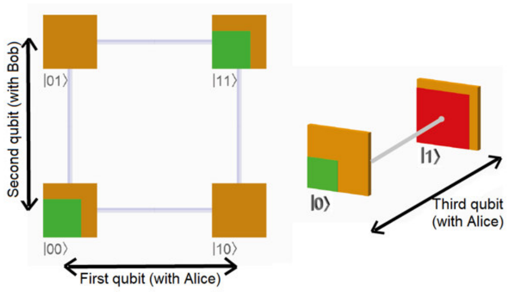
If $|a\rangle = |1\rangle$ (cases $|10\rangle$ and $|11\rangle$), Pauli-X changes Bob's QBit's state to $\alpha|0\rangle + \beta|1\rangle$ or $\alpha|0\rangle - \beta|1\rangle$.

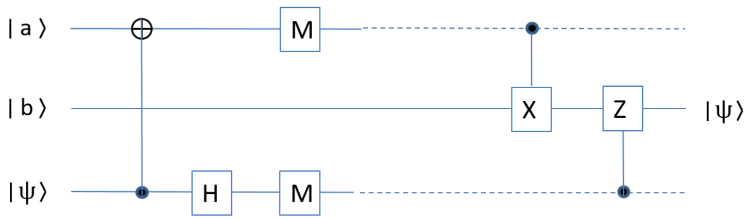
If the third qubit was also measured 1 (cases $|01\rangle$ and $|11\rangle$), Pauli-Z then changes $|b\rangle$ to $\alpha|0\rangle + \beta|1\rangle$. ■

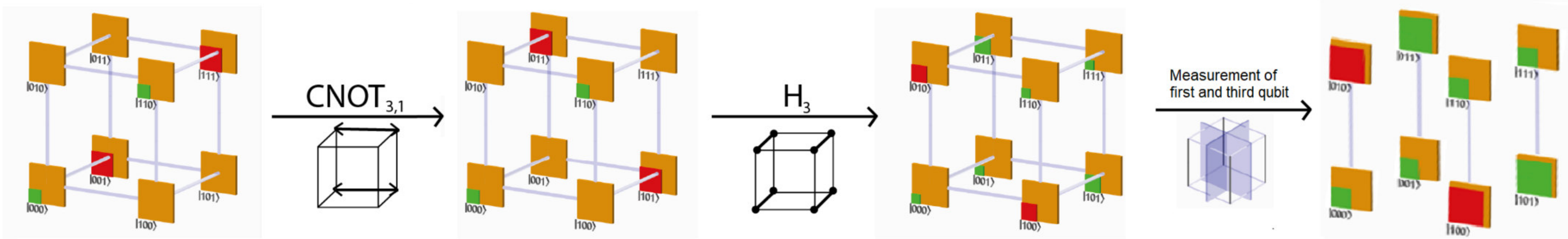
Visualizing states and (some) unitaries

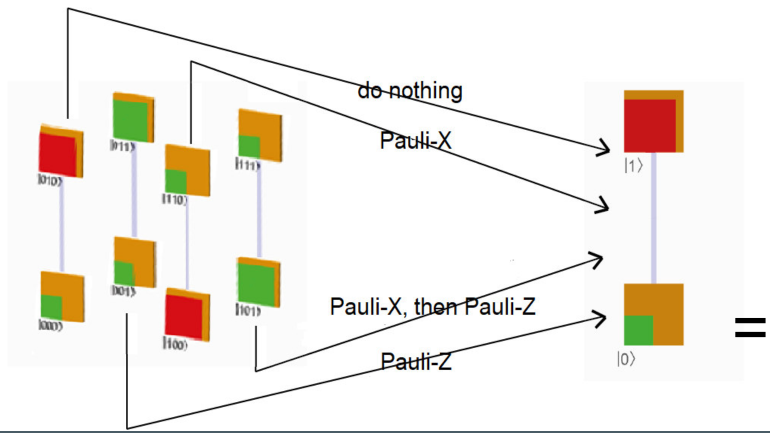
Why does teleportation work?

$|\psi_{start}\rangle =$





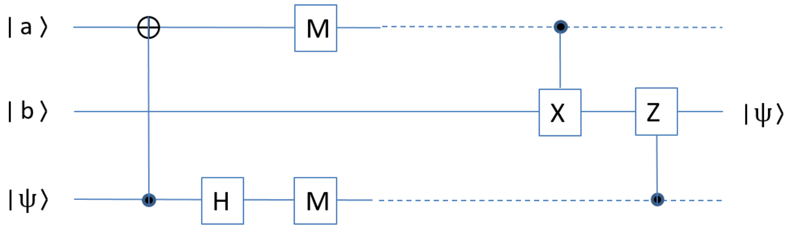




$=|\psi_{end}\rangle$

Quantumcomputing is manipulating SYSTEMS of qubits:

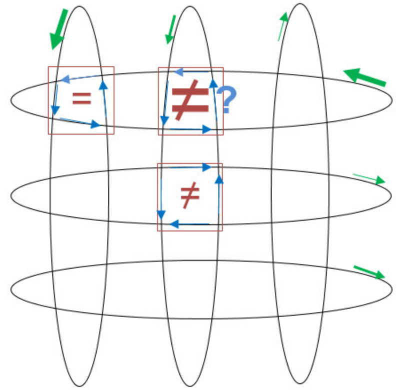
Gate model + quantum circuits (e.g. IBM):



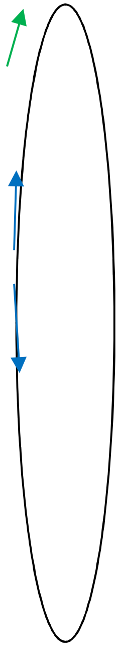
- Universal model in the sense of Feynman-Deutsch computational model;
- Keeps control of every individual qubit (today: ca 20-400 qubits);
- Does classicaly impossible things, e.g. teleportation, or speeds up classical algorithms (famous: Shor's algorithm for factorisation).
- Uses quantum-entanglement.

Quantum simulated annealing (e.g. D-Wave):

- Solves „only“ optimization problems;
- Prepares system, not every individual qubit (today: ca 5000 qubits);
- Cools down and leaves the rest to nature: System minimizes energy and thus solves optimization problem;
- Uses quantum-tunnel-effect.



Quantum simulated annealing (D-Wave):



One qubit: Tiny little loop of wire.

When cooled down to ca absolute zero:
Gets supraconducting: Current flows without resistance
clockwise or counterclockwise. results

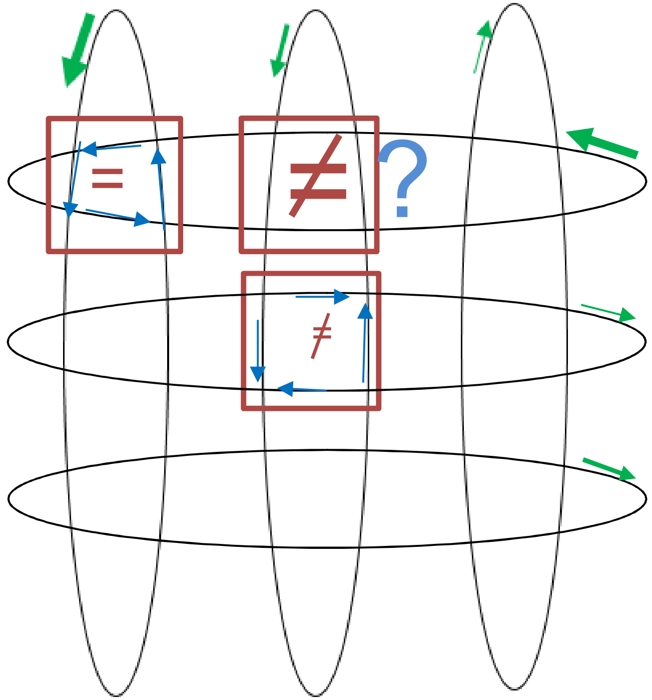
Measuring current flow destroys supraconductance.

Before cooling down, one can put a „weight“ to qubit.
Energy is higher, when current does not flow in
direction of weight.

Qubit „wants“ to minimaze energy, i.e. flow in direction of weight.

If it does: Energetic benefit. Else: Energetic punishment.

System of qubits:



weights, direction of preferred flow

= Coupler, energy lower when both clockwise or both counterclockwise

≠ Coupler, energy lower when one clockwise, the other counterclockwise

Components of solution

Cooling down and minimizing energy,
system solves optimization problem

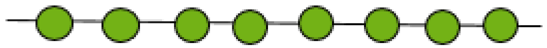
$$\sum_{i} a_i x_i + \sum_{\substack{i,j \\ \text{coupled}}} b_{ij} x_i x_j \rightarrow \min, \qquad x_i, x_j \in \{-1;+1\}$$

The challenge: Transform your optimization problem into that shape.

State of the hardware & application of quantum computing today

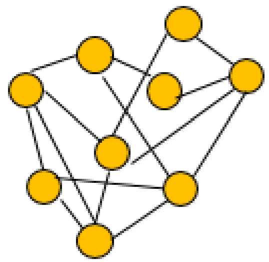
Hardware is the problem.
Qubits are very sensible, faulty when interacting with any kind of something.

Applications with **one qubit after the other:**



- **Telecommunication, cryptography**
- Photons used, fiber optic cables (or vacuum in space) needed
- Practical applications already there, continously increasing.

Applications with **all qubits at the same time:**

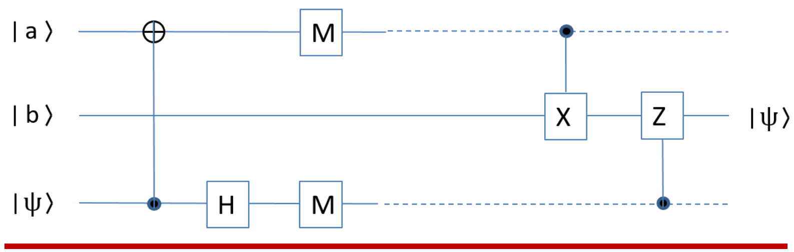


- **Optimization**, simulation, HPC in general
- Supraconductivity, trapped ions are main techniques
- Up to now not capable to solve problems of practical importance (Level today: Factorisation of 6 digit numbers, e.g. 815153 = 887*919)
- When realized, especially in combination with AI, will be game changer.

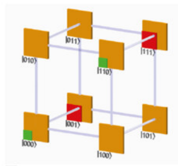
Summary: Quantum computing is manipulating SYSTEMS of qubits:

Gate model + quantum circuits (e.g. IBM):

- Universal model in the sense of Feynman Deutsch computational model;
- Gates are unitary transformations in $\mathbb{C}^{2^n}$
- Measurements are projections.



$$\begin{aligned}&\alpha_0 \cdot |000\rangle\\ +\ &\alpha_1 \cdot |001\rangle\\ +\ &\alpha_2 \cdot |010\rangle\\ +\ &\alpha_3 \cdot |011\rangle\\ +\ &\alpha_4 \cdot |100\rangle\\ +\ &\alpha_5 \cdot |101\rangle\\ +\ &\alpha_6 \cdot |110\rangle\\ +\ &\alpha_7 \cdot |111\rangle\end{aligned} \xrightarrow{\text{gate}} \begin{aligned}&\alpha'_0 \cdot |000\rangle\\ +\ &\alpha'_1 \cdot |001\rangle\\ +\ &\alpha'_2 \cdot |010\rangle\\ +\ &\alpha'_3 \cdot |011\rangle\\ +\ &\alpha'_4 \cdot |100\rangle\\ +\ &\alpha'_5 \cdot |101\rangle\\ +\ &\alpha'_6 \cdot |110\rangle\\ +\ &\alpha'_7 \cdot |111\rangle\end{aligned}$$



$$\begin{pmatrix} & \text{unitary matrix} & \end{pmatrix} \cdot \begin{pmatrix}\alpha_0\\ \alpha_1\\ \alpha_2\\ \alpha_3\\ \alpha_4\\ \alpha_5\\ \alpha_6\\ \alpha_7\end{pmatrix} = \begin{pmatrix}\alpha'_0\\ \alpha'_1\\ \alpha'_2\\ \alpha'_3\\ \alpha'_4\\ \alpha'_5\\ \alpha'_6\\ \alpha'_7\end{pmatrix}$$

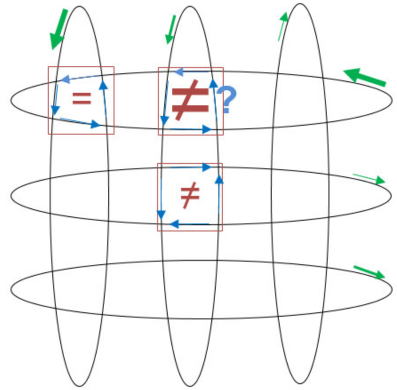
Quantum simulated annealing (e.g. D-Wave):

System solves optimization problem

$$\sum_i a_i x_i + \sum_{\substack{i,j\\ \text{coupled}}} b_{ij} x_i x_j \to \min, \qquad x_i, x_j \in \{-1; +1\}$$

↑ ↓

Challenge: Get your problem to that shape.



Contact

Prof. Dr. Bettina Just, Aktuar (DAV)
THM – FB MNI
Wiesenstraße 14
35390 Gießen

Tel. 0641-309-2454
bettina.just@mni.thm.de