Quantum Computing: from Basics to the cutting Edge - Notes

Benjamin Köhler

Contents

Part I

Quantum Computing: Less Formulas - more understanding

This part is based on my notes taken in the lecture of the same name by Dr. Sergey Sysoev. If you have the opportunity, you should try to find videos of his lecture and listen to those. His style of presentation is much beyond my ability to write down this outstanding lecturer's wonderful humour and insightful remarks.
In this part, a very shallow overview over the field of quantum computing is given. It should enable you the reader to appreciate the beauty of quantum computing and understand its working principle without too much mathematical exposure.
I begin by introducing the basic notions of quantum mechanics and the most important physical phenomena that can be used for computation. Furthermore, I give you a overview on the mathematics and show you the limitations and opportunities arising from quantum mechanics. Also I give examples of quantum circuits that realise quantum algorithms. At the end, I discuss two quantum cryptography protocols.
This part should enable you to join in conversations about quantum computing without embarrassing yourself too soon. You will also be able to understand popular books written by the pioneers of quantum computing. I recommend the Feynman lectures on computation and the books by David Deutsch. I hope you enjoy this short part and feel motivated to dive deeper into the field and will read the other three parts that are more rigorous and will enhance your understanding and allow you to read more advanced literature and become a true expert in the field.

Chapter 1

Basic notions

There are three essential demands on a quantum computer:

1. continuum of states
2. true randomness
3. interference

We explore all three aspects of this in the next sections and point out that only when all three properties are fulfilled, the resulting computer is superior to a regular computer. A side effect of these considerations is that we encounter and introduce many useful concepts and notations from quantum mechanics that are necessary to understand all main principles of quantum computing.

1.1 The state space

A **qubit** has a continuum of possible states in contrast to a bit (which is either 0 or 1) as it can be a superposition of $|0\rangle$ and $|1\rangle$. A quantum bit can, therefore, store an infinite number of information/values, e.g. as a point on the unit circle[1]

$$|\Phi\rangle = \cos\phi|0\rangle + \sin\phi|1\rangle. \tag{1.1}$$

Theoretically a classical pendulum can represent an infinite number of states/a point on the unit circle too. A quantum bit is **much more**!

1.2 True randomness

This property of a quantum computer is often underestimated. A coin toss is not truly random (Laplace demon). **True randomness** means that the universe can not predict the outcome. The double slit experiment shows that this is possible, i.e. there are true random processes. A qubit state is a superposition of many base states. The measurement destroys this superposition. Random behaviours enable one to get many more outcomes by the same input. Many quantum computers do the same task, but are differently successful. A pendulum will always be in only one state and is, therefore, not truly random.
Imagine the following function that takes one bit as input

$$f(x) = \begin{cases} f(|0\rangle) = f_0 \\ f(|1\rangle) = f_1 \end{cases} \tag{1.2}$$

The state

$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \tag{1.3}$$

[1] We later demonstrate that the actual state space is much larger as $|\Phi\rangle = \frac{1}{\sqrt{2}}\phi|0\rangle + \frac{\mathrm{i}}{\sqrt{2}}|1\rangle$ is also a valid state which, however, does not lie on the unit circle.

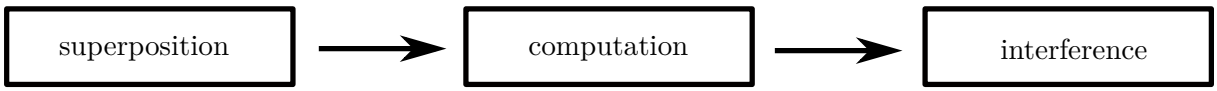


Figure 1.1: Basic principle of quantum computing. The last step allows to extract the quantum nature of a qubit.

can be the one of a qubit and passed to the function, but this state can not be represented by the pendulum. A qubit can be in infinitely many states **and** have two values **simultaneously**. The pendulum can only store one value at a time.

1.3 Interference

An observer makes the wave function collapse and measures only one of the two possible values in equation (1.2), i.e. after the measurement, every consecutive measurement returns the same value as was obtained in the initial measurement. After the measurement, the state is either $|0\rangle$ or $|1\rangle$ and no longer a superposition. In the multiverse interpretation one considers the universe to split into two versions where in one $|0\rangle$ and in the other $|1\rangle$ was observed. The observer **entangles** himself with the qubit.
We want to use both outcomes for our calculations. **Interference** makes this possible. Here, the result of the observation is a superposition of the base states (interference pattern in the double slit experiment), i.e. there is an interaction of the base states:

$$f(x)|+\rangle = \frac{f(x)}{\sqrt{2}}\left[|0\rangle + |1\rangle\right] = \frac{1}{\sqrt{2}}\left[f_0|0\rangle + f_1|1\rangle\right] \neq \begin{cases} f_0|0\rangle \\ f_1|1\rangle \end{cases} . \tag{1.4}$$

The basic principle of quantum computations is illustrated in Figure 1.1. The last step allows to extract the quantum nature of the qubit. For quantum computations to be reliable, there **must** be no other interaction destroying the interference. Therefore, the computation process must be:

1. fast
2. cold
3. isolated (probably the hardest)

1.4 Classical and quantum particles

The double slit experiment can be used to distinguish classical (bullet-like) and quantum (wave-like) particles:

- For **classical particles** the resulting pattern is the sum of two one-slit experiments
- For **quantum particles** the resulting pattern is the superposition of of the two one-slit experiment's intensities (amplitudes squared)
- Heavier particles have a smaller wavelength, i.e. more concentrated wave functions
- The intensity of the wave function is the probability to observe the particle in a particular state

The wave-function needs to be square-integrable ($\mathcal{L}^2$) and non-zero.

Chapter 2

Mathematical background and physical notions of quantum mechanics

Mathematically wave functions form a vector space, i.e. if $\mathbb{F}$ is a linear vector space then

$$
\begin{aligned}
&A, B \in \mathbb{F},\ \alpha, \beta \in \mathbb{C} \\
&1.\ \alpha A \in \mathbb{F} \\
&2.\ A + B \in \mathbb{F} \\
&\Rightarrow f(x) : \int f^2(x)\mathrm{d}x < \infty \\
&\quad g(x) = af(x) \Rightarrow \int g^2(x)\mathrm{d}x = a^2 \int f^2(x)\mathrm{d}x < \infty \\
&\quad (f+g)(x) = f(x) + g(x) \in \mathbb{F}
\end{aligned}
$$

The dimensionality of square-integrable functions is infinite, i.e. there will be infinitely many basis functions. Measurements make the wave function collapse and entangle the observer with a basis function of the measurement. Dirac-delta functions form the basis of the vector space $\mathcal{L}^2$-function strictly speaking (δ-distribution are orthonormal basis functions). Measurements transform the wave function composition into one (**randomly selected**) vector of that composition:

$$x = \sum_{i=1}^{n} x_i \boldsymbol{e}_i \to \boldsymbol{e}_i \qquad \text{(measurement)} \tag{2.1}$$

$$P(\boldsymbol{e}_a) = x_a^2 \qquad \text{(probability)} \tag{2.2}$$

$$f(x) = \int_{-\infty}^{\infty} f(a)\delta(x-a)\,\mathrm{d}a \;\to\; \delta(x-a) \qquad \text{(measurement with probability } f(a)\text{)} \tag{2.3}$$

The last integral is a **Lebesque integral**.

2.1 State space

The **state space** is a isomorphism of a general vector

$$x = \sum_{i=1}^{N} x_i \boldsymbol{e}_i = \begin{pmatrix} x_1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ x_2 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \cdots + \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ x_N \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_N \end{pmatrix}. \tag{2.4}$$

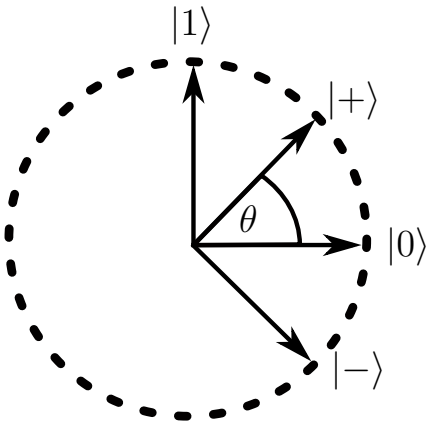


Figure 2.1: The rotation of the polarisation filter also rotates the basis of possible outcomes of the measurement. By rotating the filter, the basis can be manipulated.

This reduces the dimensionality of the state. Such a finite representation and in particular the **two-state-representation** is most interesting for quantum computing. The latter is realised, e.g. by the polarisation of light which is the plane of oscillation of electro-magnetic waves (light). Polarisation filter are composed of dipol ordered atoms. These block out one polarisation (all other polarised waves interfere destructively). A **single** photon can either pass or not through the filter. This is the measurement of the photon's polarisation. The reflected light will have the opposite polarisation. The photon polariser has a state space of dimension 2. This is the so called **qubit-realisation**.
With the polariser at $\theta = \frac{\pi}{4}$ the basis is

$$|+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$$
$$|-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$

which is also illustrated in Figure 2.1. By rotating the polariser, the measurement can be tuned/the basis be manipulated.
The polarisation of light oscillates with period T or frequency ω

$$|P(t)\rangle = \frac{1}{\sqrt{2}}\left[\cos(\omega t)|0\rangle + \sin(\omega t)|1\rangle\right] = |+\rangle(t) \qquad \text{(clockwise rotation)} \tag{2.5}$$
$$|-\rangle = \frac{1}{\sqrt{2}}\left[\cos(\omega t)|0\rangle - \sin(\omega t)|1\rangle\right] \qquad \text{(anti-clockwise rotation)} \tag{2.6}$$
$$|+\rangle = \frac{1}{\sqrt{2}}\left[\mathrm{e}^{\mathrm{i}\omega t}|0\rangle + \mathrm{i}\mathrm{e}^{\mathrm{i}\omega t}|1\rangle\right] = |+\rangle(t) \tag{2.7}$$
$$|-\rangle = \frac{1}{\sqrt{2}}\left[\mathrm{e}^{\mathrm{i}\omega t}|0\rangle - \mathrm{i}\mathrm{e}^{\mathrm{i}\omega t}|1\rangle\right] = |+\rangle(t). \tag{2.8}$$

As phases do not matter, we can cancel the time dependence:

$$|+\rangle = \frac{1}{\sqrt{2}}\left[|0\rangle + \mathrm{i}|1\rangle\right] \tag{2.9}$$
$$|-\rangle = \frac{1}{\sqrt{2}}\left[|0\rangle - \mathrm{i}|1\rangle\right] \tag{2.10}$$

or alternatively

$$|+\rangle = \frac{\mathrm{e}^{\mathrm{i}\omega t}}{\sqrt{2}}\left[|0\rangle + |1\rangle\right] \tag{2.11}$$
$$|-\rangle = \frac{\mathrm{e}^{-\mathrm{i}\omega t}}{\sqrt{2}}\left[|0\rangle + |1\rangle\right]. \tag{2.12}$$

2.2 Bloch sphere

The general two-qubit state can be expressed as

$$|\Psi\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}e^{i\phi}|1\rangle \tag{2.13}$$

where the argument of the trigonometric functions is to ensure that $|0\rangle$ and $|1\rangle$ are on opposite on the so called **Bloch sphere** which is illustrated in Figure 2.2. With these two angles, six special states for quantum computing applications are defined:

$\theta = 0, \quad \phi = 0 : \quad |\Psi\rangle = |0\rangle,$
$\theta = \pi/2, \quad \phi = 0 : \quad |\Psi\rangle = |+\rangle,$
$\theta = \pi, \quad \phi = 0 : \quad |\Psi\rangle = |1\rangle,$
$\theta = 3\pi/2, \quad \phi = 0 : \quad |\Psi\rangle = |-\rangle,$
$\theta = \pi/2, \quad \phi = \pi/2 : \quad |\Psi\rangle = |\circlearrowleft\rangle,$
$\theta = -\pi/2, \phi = \pi/2 : \quad |\Psi\rangle = |\circlearrowright\rangle.$

The Bloch sphere is applicable to any two state systems, e.g. the Stern Gerlach experiment[1].

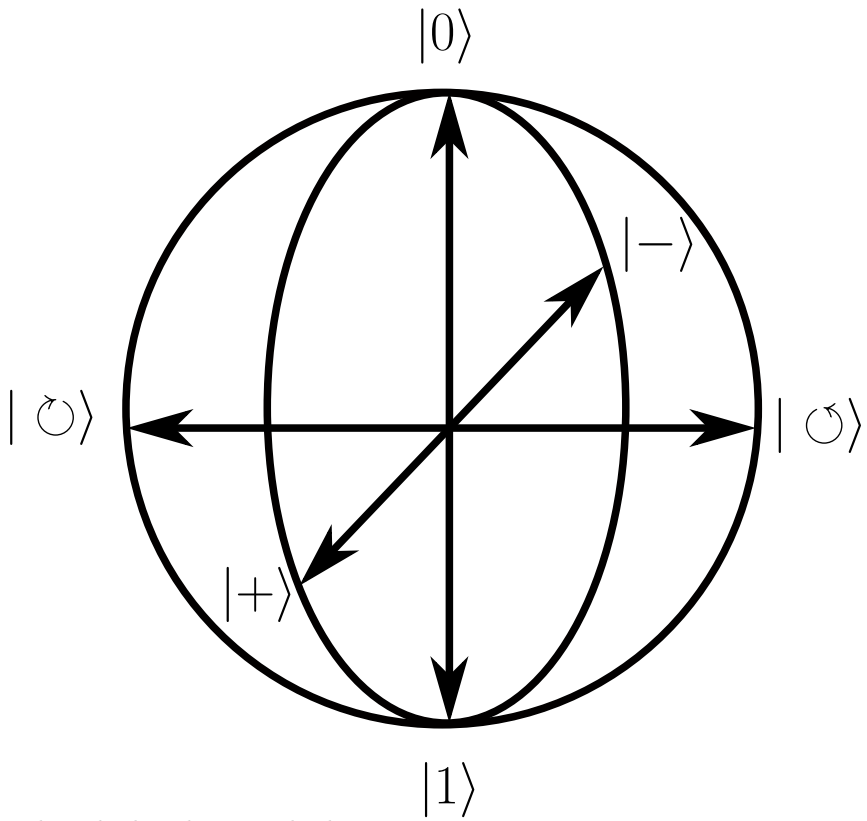


Figure 2.2: The Bloch sphere with the six most important states in quantum computing

[1] Silver atoms in a magnetic field, deflection to north or south because of the electron spin

2.3 Entanglement

One qubit is not enough for quantum computing. There is no problem with creating more qubits, e.g. by having many atoms, photons, or spins, **but** they need to be **entangled** to truly be powerful tools in quantum computing. Else, the qubits do not depend on one another and calculations need to collapse the wavefunctions (normal qubit). For example the so called **conditional NOT (CNOT)**-gate flips the state of a qubit if another qubit is in state $|1\rangle$ and leaves it as it is if the other qubit is in state $|0\rangle$. The wavefunctions do not collapse in this process. The state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle$ is transformed into the state $\frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$[2]. In this state, both qubits are indistinguishably entangled. As of now (2022) entangling is a complicated process and the basis of any practicable application of quantum computations.

2.4 Systems with many qubits

For two qubits, there are four possible basis states: $|0\rangle|0\rangle$, $|0\rangle|1\rangle$, $|1\rangle|0\rangle$ and $|1\rangle|1\rangle$. There are states that can be expressed as results of tensor products of two states

$$(\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle) = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle \tag{2.14}$$

and states like

$$\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right). \tag{2.15}$$

Both types of states can exist physically. The notation we use here is

$$|\alpha\beta\rangle = \begin{pmatrix}\alpha_0\\ \alpha_1\end{pmatrix} \otimes \begin{pmatrix}\beta_0\\ \beta_1\end{pmatrix} = \begin{pmatrix}\alpha_0\begin{pmatrix}\beta_0\\ \beta_1\end{pmatrix}\\ \\ \alpha_1\begin{pmatrix}\beta_0\\ \beta_1\end{pmatrix}\end{pmatrix} = \begin{pmatrix}\begin{pmatrix}\alpha_0\beta_0\\ \alpha_0\beta_1\end{pmatrix}\\ \\ \begin{pmatrix}\alpha_1\beta_0\\ \alpha_1\beta_1\end{pmatrix}\end{pmatrix} = \begin{pmatrix}\alpha_0\beta_0\\ \alpha_0\beta_1\\ \alpha_1\beta_0\\ \alpha_1\beta_1\end{pmatrix} \tag{2.16}$$

This scheme generalises to many qubits and the basis notation yields the binary representation of numbers. The dimension of the basis is 2^n where n is the number of qubits in the system.

2.5 Mathematics of quantum computing

- **inner products**

$$\begin{aligned}&\cdot : \mathcal{H} \times \mathcal{H} \to \mathbb{C}\\ &\quad \boldsymbol{x}, \boldsymbol{y} \in \mathcal{H}, \alpha \in \mathbb{C}\\ &1.\ \boldsymbol{x}\cdot\boldsymbol{y} = \overline{\boldsymbol{y}\cdot\boldsymbol{x}}\\ &2.\ \boldsymbol{x}\cdot(\alpha\boldsymbol{y}) = \alpha(\boldsymbol{x}\cdot\boldsymbol{y}) \quad \text{(only second component!!!)}\\ &3.\ \boldsymbol{x}\cdot\boldsymbol{x} \geq 0 \ \ (\boldsymbol{x}\cdot\boldsymbol{x} = 0 \Leftrightarrow \boldsymbol{x} = \boldsymbol{0})\end{aligned}$$

$$\text{in Hilbert space: } \boldsymbol{x}\cdot\boldsymbol{y} = \sum_{i=1}^{n} x_i^* y_i, \ \ f\cdot g = \int f^*(x)g(x)\,\mathrm{d}x$$

- **conjugate space**

$$\boldsymbol{x} \in \mathcal{H}, \ f_{\boldsymbol{x}} : \boldsymbol{y} \to \boldsymbol{x}\cdot\boldsymbol{y} \ \forall \boldsymbol{y} \in \mathcal{H}, \ f - x \in \mathcal{H}^*$$

$$\left.\begin{aligned}|x\rangle &\in \mathcal{H}\\ \langle x| &\in \mathcal{H}^*\end{aligned}\right\} \text{Bra-Ket notation}$$

$$f_{\boldsymbol{x}} = \langle x|$$

$$\langle x|y\rangle = \boldsymbol{x}\cdot\boldsymbol{y}$$

[2] This is one of the Bell states which we encounter later

- **representations**

$$|x\rangle = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \qquad \langle x| = \Big(x_1^*, \ldots, x_n^*\Big)$$

- **hermitian conjugation**

$$\alpha^* = \overline{\alpha}, \quad |x\rangle^* = \langle x|, \quad \langle x|^* = |x\rangle$$

- **linear operators**

  ...are the tool to to manipulate the states or qubits

$$\begin{aligned} A &: \mathcal{H} \to \mathcal{H} \\ & A(\alpha|x\rangle + \beta|y\rangle) = \alpha A|x\rangle + \beta A|y\rangle \end{aligned}$$

  A are operators represented by matrices.

$$A|x\rangle = A_{ij}|x\rangle_j \quad \text{(Einstein summation)}$$

$$A_{ij} = (A|j\rangle)_i \quad \text{where } |j\rangle = \begin{pmatrix} 0 \\ \vdots \\ 1 \leftarrow \text{j'th position} \\ 0 \\ \vdots \\ 0 \end{pmatrix} \ldots \text{ j'th basis vector}$$

  In general, two operators do not commute and, therefore, the order of multiplication is important. The commutator

$$[A, B] = AB - BA \tag{2.17}$$

  is very important.

- **hermitian operators**

  ...are operators with the following property:

$$\begin{aligned} \langle y|A|x\rangle = \langle y|\Big(A|x\rangle\Big) &= \Big(\langle y|A\Big)|x\rangle \\ &= \langle y|\Big(A^*|x\rangle\Big), \end{aligned}$$

  i.e. $A = A^*$ or $\big(\langle\phi|A\big)^* = A^*|\phi\rangle$.

- **hermitian conjugation**

  ...is defined as

$$\big(\alpha|a\rangle\langle b|\langle c|ABC|d\rangle\big)^* = \overline{\alpha}\langle d|C^*B^*A^*|c\rangle|b\rangle\langle a|.$$

  Hermitian operators represent observables. They have real eigenvalues and orthogonal eigenstates.

- **eigenvalue equation**

  ...is

$$A|\Phi\rangle = \lambda|\Phi\rangle.$$

There are many eigenvalues λ (degeneracy possible) and eigenstates $|\Phi\rangle$ (up to normalisation), but[3] the same amount.

The eigenvalues of hermitian operators are real because

$$\begin{aligned}\langle x|A|x\rangle &\overset{A=A^*}{=} (\langle x|A)|x\rangle = \lambda^* \|x\| \\ \langle x|A|x\rangle &= \langle x|(A|x\rangle) = \lambda \ \|x\|\end{aligned}$$

and, therefore, $\lambda = \lambda^*$.

The eigenstates are orthogonal, because

$$\begin{aligned}A|x\rangle &= \lambda|x\rangle \\ A|y\rangle &= \mu|y\rangle \\ \langle x|A|y\rangle &= \lambda\langle x < y\rangle \overset{A=A^*}{=} \mu\langle x|y\rangle\end{aligned}$$

and, therefore, $\langle x|y\rangle = 0$[4].

In the language of quantum mechanics,

- the observables are hermitian operators
- the eigenvectors are the states the system ¨collapses¨ to
- the eigenvalues are the measurement outcomes

For degenerate eigenvalues, one can use a complete set of commuting observables **(CSCO)**.

Here are some examples for hermitian operators

◇ **projection operator** $P = |\Phi\rangle\langle\Phi|$
which projects any state collinearly to the state $|\Phi\rangle$ or some (possibly non-complete) set of operators

$$P = \sum_i |\Phi_i\rangle \langle\Phi_i| .$$

The eigenvalues of P_i are

$$\begin{aligned}\lambda_1 &= 1, \quad \text{degeneracy=1} \\ \lambda_2 &= 0, \quad \text{degeneracy=n-1}\end{aligned}$$

◇ **operator** $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

$$\begin{aligned}X|0\rangle &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle \\ X|1\rangle &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle\end{aligned}$$

This is the quantum mechanical analogue of a NOT-operator in classical computing. The eigenvalues and eigenvectors of X are

$$\begin{aligned}X|+\rangle = \frac{1}{2}(X|0\rangle + X|1\rangle) &= \ |+\rangle \ \rightarrow \ \lambda_1^X = \ 1, \ |\Phi_1^X\rangle = |+\rangle \\ X|-\rangle = \frac{1}{2}(X|0\rangle - X|1\rangle) &= -|-\rangle \ \rightarrow \ \lambda_2^X = -1, \ |\Phi_2^X\rangle = |-\rangle\end{aligned}$$

The operator X is the rotation around the vector along the x-axis of the Bloch sphere.

[3] up to degeneracy

[4] Strictly this only goes for non-degenerate eigenvalues ($\lambda \neq \mu$). For the degenerate subspace, one can orthogonalise the eigenstates that span it.

◇ **Pauli-matrices**

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ Y = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix},\ Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

with the additional eigenvalues and -vectors

$$\begin{aligned} \lambda_1^Y = \quad 1: \ |\Phi_1^X\rangle &= |\circlearrowleft\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + \mathrm{i}|1\rangle\right), \\ \lambda_2^Y = -1: \ |\Phi_2^Y\rangle &= |\circlearrowright\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - \mathrm{i}|1\rangle\right), \\ \lambda_1^Z = \quad 1: \ |\Phi_1^Z\rangle &= |0\rangle, \\ \lambda_2^Z = -1: \ |\Phi_2^Z\rangle &= |1\rangle. \end{aligned}$$

◇ **Hadamard transform** $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ (very important for quantum algorithms)

$$\begin{aligned} H|0\rangle = |+\rangle,\ H|+\rangle = |0\rangle, \\ H|1\rangle = |-\rangle,\ H|-\rangle = |1\rangle. \end{aligned}$$

The eigenvalues and eigenvectors are

$$\begin{aligned} \lambda_1^H = \quad 1 : |\Phi_1^H\rangle &= \cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle, \\ \lambda_2^H = -1 : |\Phi_2^H\rangle &= \cos\frac{\pi}{8}|1\rangle - \sin\frac{\pi}{8}|0\rangle. \end{aligned}$$

◇ **conditional NOT (CNOT) operator**

...is another important unitary operator (which was introduced when we talked about entanglement in section 2.3) acting in a two-qubit space

$$\mathrm{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

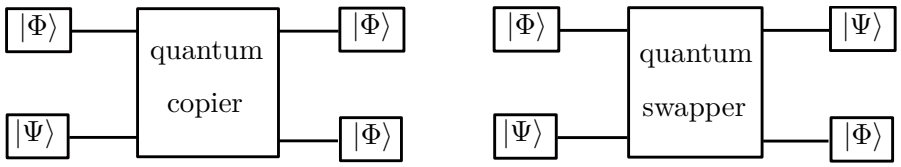
$$\begin{aligned} \mathrm{CNOT}|00\rangle &= |00\rangle \\ \mathrm{CNOT}|01\rangle &= |01\rangle \\ \mathrm{CNOT}|10\rangle &= |11\rangle \\ \mathrm{CNOT}|11\rangle &= |10\rangle \end{aligned}$$

- **evolution of quantum systems**

The basis of a quantum system is changed according to

$$\begin{aligned} |\Phi\rangle = \sum_{i=1}^{n} \alpha_i |\mathrm{e}_i\rangle = \sum_{i=1}^{n} \alpha_i \mathrm{I}|\mathrm{e}_i\rangle = \sum_{i=1}^{n}\sum_{j=1}^{n} \alpha_i |s_j\rangle\langle s_j|\mathrm{e}_i\rangle \\ = \sum_{i=1}^{n} \alpha_i \sum_{j=1}^{n} |s_j\rangle \underbrace{\langle s_j|\mathrm{e}_i\rangle}_{U_{ji}/\alpha_i} = \sum_{j=1}^{n} U_{ij}|s_j\rangle \end{aligned}$$

The matrix U transforms from basis $\{|\mathrm{e}_i\rangle\}$ to $\{|\mathrm{s}_i\rangle\}$. Because $U^{-1} = U^*$, it is a unitary operator. Only unitary transformations can be used for computations (all quantum gates are unitary). All the before encountered operators (X, Y, Z, H) are unitary.



(a) (b)

Figure 2.3: A schematic illustration of a quantum copier that overwrites the state $|\Psi\rangle$ in order to create a copy of $|\Phi\rangle$ in (a) and the quantum swapper that exchanges the states $|\Phi\rangle$ and $|\Psi\rangle$ from one quantum system to the other preserving angles and information in (b).

2.6 No cloning theorem

Can we make a copy of quantum data? Copying is some kind of observation. One can not read a quantum state without altering it. Maybe one can transfer the information to another quantum system without destroying the initial one.
We illustrate quantum algorithms by a special kind of notation. On the left side we write down all the quantum states that are utilised in the algorithm. From left to right we insert quantum gates that operate on those states. Gates on the left act before gates more right of them. The states and gates are connected by lines which indicate that those gates act on these specific states. So called conditional gates, i.e. gates that only act on qubits when other qubits are in particular states (here this is the $|1\rangle$ state), are illustrated with filled dots on the lines of the qubits that determine whether the gates act on the qubits with the gate on their respective line. An example can be seen in the SWAP operator in Figure 2.4 which employs several CNOT-gates. Conditional measurement gates are depicted by open circles like in the quantum teleportation operator in Figure 2.5.
In Figure 2.3(a), we show a schematic of a **quantum copier** that copies the state $|\Phi\rangle$ by overwriting the state $|\Psi\rangle$. Such a quantum copier can not be unitary as the state $|\Psi\rangle$ does not enter the result, i.e. it does not preserve angles. This result is known as the **No cloning theorem** and was proven by J. Park in 1970 and independently by W. Wooster, W. Zurek, and D. Dieks in 1982. An alternative to the quantum copier is the so called **quantum swap** and the **quantum teleportation** operations that can be seen in Figure 2.3(b). Hefig. re the information from one system whose state one wants wants to transfer to another system with a random state one does not care about. This is a weaker copy function which is unitary and can, hence, be implemented by quantum operations.

2.6.1 Quantum swap operator

The quantum SWAP operator is a operator that acts in the two-qubit space in the following way

$$\text{SWAP}|00\rangle = |00\rangle \tag{2.18}$$
$$\text{SWAP}|01\rangle = |10\rangle \tag{2.19}$$
$$\text{SWAP}|10\rangle = |01\rangle \tag{2.20}$$
$$\text{SWAP}|11\rangle = |11\rangle \tag{2.21}$$

and is, therefore, in the above basis represented by

$$\text{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{2.22}$$

It can be realised by the quantum circuit in Figure 2.4 which is the **quantum swap algorithm**.

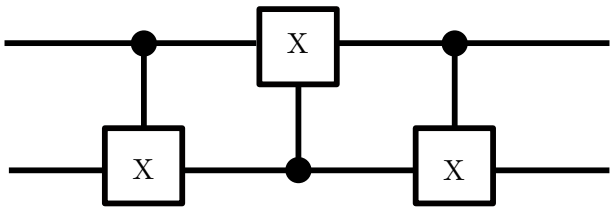


Figure 2.4: Quantum circuit realisation of the SWAP operator using CNOT gates

2.6.2 Quantum teleportation

In the quantum teleportation algorithm, the state of one qubit is transferred into another one by performing a preparation of the **destination qubit** and the **auxiliary qubit** which start of in the $|0\rangle$ state. After this preparation all three qubits are entangled and information can be transferred to the destination state, if one performs certain operations to it which depend on the outcomes of specific measurements on the other two qubits. The **quantum teleportation circuit**[5] is shown in Figure 2.5. In the following, I show the evolution of the states after the application of the respective gates. At the start, the three-qubit state is

$$|\Phi\rangle|0\rangle|0\rangle = (\alpha|0\rangle + \beta|1\rangle)\,|0\rangle|0\rangle, \tag{2.23}$$

because the state $|\Phi\rangle$ is an arbitrary state that we want to transfer. The state after the preparation (before the conditional measurement gates) is

$$\mathrm{H}_1\mathrm{H}_1\mathrm{C}_1\mathrm{Z}_2\mathrm{C}_2\mathrm{X}_3\mathrm{H}_2|\Phi\rangle|0\rangle|0\rangle \tag{2.24}$$

where the subscripts refer to the qubits that they act or on which they depend on, e.g. the gate $\mathrm{C}_1\mathrm{Z}_2$ acts with a Z-gate on the second qubit when the first qubit is in the state $|1\rangle$. The qubits are enumerated from top to bottom, so the full initial state is $|\Phi\rangle_1|0\rangle_2|0\rangle_3$ and I drop the subscripts in the following. Next, I successively let the operators act:

$$\begin{aligned}
\mathrm{H}_1\mathrm{H}_1\mathrm{C}_1\mathrm{Z}_2\mathrm{C}_2\mathrm{X}_3\mathrm{H}_2|\Phi\rangle|0\rangle|0\rangle &= \mathrm{H}_1\mathrm{H}_2\mathrm{C}_1\mathrm{Z}_2\mathrm{C}_2\mathrm{X}_3|\Phi\rangle|+\rangle|0\rangle \\
&= \mathrm{H}_1\mathrm{H}_2\mathrm{C}_1\mathrm{Z}_2\frac{1}{\sqrt{2}}|\Phi\rangle\,(|00\rangle + |11\rangle) \\
&= \mathrm{H}_1\mathrm{H}_2\frac{1}{\sqrt{2}}\,(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle - \beta|111\rangle) \\
&= \frac{1}{\sqrt{2}}\,(\alpha|++0\rangle + \alpha|+-1\rangle + \beta|-+0\rangle - \beta|--1\rangle)\,.
\end{aligned}$$

Now, we can simplify the resulting state further:

$$\begin{aligned}
&\frac{1}{\sqrt{2}}\,(\alpha|++0\rangle + \alpha|+-1\rangle + \beta|-+0\rangle - \beta|--1\rangle) \\
&\quad= \frac{1}{2\sqrt{2}}\Big[(\alpha+\beta)|000\rangle + (\alpha+\beta)|010\rangle + (\alpha-\beta)|100\rangle + (\alpha-\beta)|110\rangle + (\alpha-\beta)|001\rangle \\
&\qquad - (\alpha-\beta)|011\rangle + (\alpha+\beta)|101\rangle - (\alpha+\beta)|111\rangle\Big].
\end{aligned}$$

[5]The Nobel prize in physics was awarded to Anton Zeilinger in the year 2022 for the successful realisation of this algorithm by photons over a distance from the earth's surface to a satellite in the earths orbit.

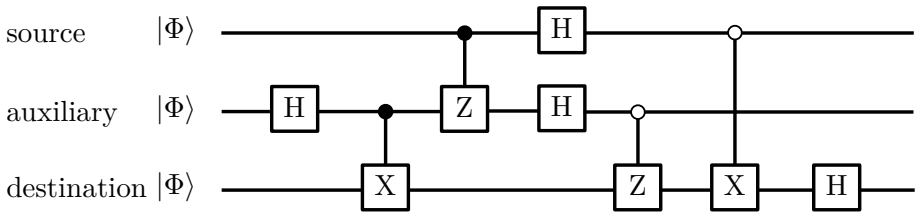


Figure 2.5: The quantum teleportation circuit which transfers the state of an arbitrary qubit $|\Phi\rangle$ into an destination state by appropriate pre- and postprocessing before and after successive measurements on this state and an auxiliary qubit

The measurements entangles the observer to the first two qubits. I indicate this by the subscript obs. It can easily be checked that the state after the measurements is

$$\begin{aligned}\frac{1}{2}\Big[\quad & |00\rangle_{\text{obs}} \left(\frac{\alpha+\beta}{\sqrt{2}}|0\rangle + \frac{\alpha+\beta}{\sqrt{2}}|1\rangle\right) \\ & + |01\rangle_{\text{obs}} \left(\frac{\alpha+\beta}{\sqrt{2}}|0\rangle - \frac{\alpha-\beta}{\sqrt{2}}|1\rangle\right) \\ & + |10\rangle_{\text{obs}} \left(\frac{\alpha-\beta}{\sqrt{2}}|0\rangle + \frac{\alpha+\beta}{\sqrt{2}}|1\rangle\right) \\ & + |11\rangle_{\text{obs}} \left(\frac{\alpha-\beta}{\sqrt{2}}|0\rangle - \frac{\alpha+\beta}{\sqrt{2}}|1\rangle\right) \Big].\end{aligned}$$

The observer can recreate the initial state $|\Phi\rangle$ by applying the operator H_3 to the state in the first line, i.e. when he measured the state $|00\rangle$, the operator $(\mathrm{ZH})_3$ to the state in the second line, i.e. when he measured the state $|01\rangle$, the operator $(\mathrm{XH})_3$, i.e. when he measured the state $|10\rangle$, and the operator $(\mathrm{ZXH}_3$, i.e. when he measured the state $|11\rangle$. This is exactly what can be seen in the quantum teleportation circuit in Figure 2.5. Although the state $|\Phi\rangle$ is transferred into the destination state, this transfer needs the results of the measurement and, therefore, the information does not travel faster than light. The information in the state $|\Phi\rangle$ is destroyed by the measurement.

Chapter 3

Quantum cryptography protocols

The no-cloning theorem from section 2.6 forbids the interception of a quantum state without destroying it. This fact is of utmost importance for cryptography, because it allows for safe exchange of keys. The standard formulation of **quantum cryptography** is that Alice and Bob want to correspond without Eve listening [1]. Alice and Bob have a secret key (shared key). While RSA is a much used classical message transfer system which is considered secure[2], I present the BB84 and the E91 quantum message transfer systems in the following two sections.

3.1 BB84 (C. Bennett, G. Brassard)

In this protocol Alice and Bob follow many steps:

1. Alice and Bob generate long enough sequences (from e.g. photon experiments). Alice needs two sequences A1 and A2 and Bob only needs only one B1.

2. They open a channel of communication (e.g. by exchanging photons)

3. The sequence A1 determines the basis in which Alice sends photon the photon: She sends it in the $\{|0\rangle, |1\rangle\}$ basis if her qubit in A1 is $|0\rangle$, and she transforms her photon into the Hadamard basis, if her photon in A1 is in state $|1\rangle$

4. The sequence A2 determines the value (polarisation) of the photon she sends: If her qubit in A2 is in state $|0\rangle$ she sends it in the state $|0\rangle$ and if her qubit is in state $|1\rangle$ in A2, she sends it in the state $|1\rangle$.

   The photons sent by Alice are random in two senses (basis and value)!!!

5. Bob receives random message B2 by Alice and measures his qubits according to his sequence B1

   $|0\rangle \rightarrow$ Bob measures in $\{|0\rangle, |1\rangle\}$ basis

   $|1\rangle \rightarrow$ Bob measures in Hadamard basis

6. Bob only obtains clear result when the sequences A1 and B1 coincide, else the result is random.

7. Bob saves his results.

8. Bob calls Alice and she gives him A1.

9. Bob returns correctly measured photons but **not** the results of the measurement.

[1] Often the names are shortened to A, B, and E

[2] A procedure we will learn how to break by the Shore quantum algorithms in section **??** and 8.3!

10. They both have a secure code no one else knows (shared secret key).

    If Eve listens, the photons disappear and Alice and Bob will find out if Eve does not send another photon to Bob. Eve can, however, not duplicate the photons because of the no cloning theorem. She can only send the same measured photon, but she does not know the basis she should choose (neither Bob's nor Alice's). Only with probability $P = \frac{1}{2} + (\frac{1}{2})^3 = \frac{5}{8}$ is she correct in one qubit[3]. Hence, the probability of being right in every transferred qubit goes to zero as the number of bits grows.

11. Final Check: they choose a number of bits to exchange and test whether those are still correct (if Eve has not listened or made no mistake, there will be nothing wrong)

12. If something is wrong, they create a new key.

3.2 E91 (A. Eckard)

In this protocol, a third party (C) can help with the initial key creation which does not even need to be trusted. The third party gives Alice and Bob a pair of **entangled** photons (for each bit). Alice gets one and Bob the other. The measurement yields the same for Alice and Bob, (because the state is $|\Psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$). C does not know the result of the measurement, though! If Eve infiltrates C and sends photons in the non-entangled states $|00\rangle$ and $|11\rangle$, Alice and Bob can still communicate securely. Alice and Bob must agree beforehand for each photon pair whether they measure in the σ_Z or the Hadamard basis. This information can be shared by any insecure line. In the Hadamard basis, the result is just $|++\rangle$ or $|--\rangle$ when the entangled state is sent and Alice and Bob should receive the same result. This is not true when the non-entangled states are sent. So Alice and Bob can check whether their communication is secure by randomly checking measurement outcomes in the Hadamard basis and, therefore, discover Eve's intrusion.

[3]She either is correct in her chosen basis and measures the right result or she measures in the wrong basis, but by chance she measures the correct state and by chance Bob's measurement yields the correct result.

Part II

Physical basics of quantum computing

Chapter 4

Introduction

The **qubit** is the unit amount of information in quantum computing. It has two orthonormal basis states $|0\rangle$ and $|1\rangle$ and can exist in a superposition of both states

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle,\ \alpha, \beta \in \mathbb{C},\ |\alpha|^2 + |\beta|^2 = 1.$$

4.1 Di Vincenzo criteria

The **Di Vincenzo criteria** list the minimal conditions on a system to realise a good basis for quantum computations:

1. A quantum physical system on which a qubit is realised must have two **distinguishable** orthogonal basis quantum states.

2. It must be **possible to prepare the system in any of these two quantum states**.

3. There must be a **procedure for measuring the qubit** (macroscopical distinguishability of the basis states).

4. One must be able to create a**universal set of quantum logic gates** (gates) for the qubit.

5. The **decoherence time** must be longer than the operating time of the quantum logic elements.

There is an additional condition to make the system useful for practical applications: The qubits and gates must be scalable, i.e. it must be possible to realise an arbitrary number of qubits and quantum gates.
Here are some examples:

- Polarisation of a photon

- Two level atoms (ground state and first excited state are energetically well-separated to all other excited states)

- Spin 1/2 systems

- Stern-Gerlach spin 1/2 systems

4.2 The Bloch sphere

A classical bit can store the information of a two-state object and n bits can store the information of a 2^n state system. The information capacity of a qubit can be seen in the **Bloch sphere**:

$$
\begin{aligned}
|\Psi\rangle &= \alpha|0\rangle + \beta|1\rangle \\
&\left.\begin{aligned} \alpha &= a\,\mathrm{e}^{\mathrm{i}\varphi} \\ \beta &= b\,\mathrm{e}^{\mathrm{i}\vartheta} \\ a^2+b^2 &= 1 \end{aligned}\right\} \; a,b,\varphi,\vartheta \in \mathbb{R} \\
|\Psi\rangle &= \underbrace{\cos\frac{\theta}{2}}_{a}\,\mathrm{e}^{\mathrm{i}\varphi}|0\rangle + \underbrace{\sin\frac{\theta}{2}}_{b}\,\mathrm{e}^{\mathrm{i}\vartheta}|1\rangle \\
&= \mathrm{e}^{\mathrm{i}\varphi}\left(\cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}\mathrm{e}^{\mathrm{i}(\vartheta-\varphi)}|1\rangle\right) \\
&\simeq \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}\mathrm{e}^{\mathrm{i}\gamma}|1\rangle.
\end{aligned}
$$

To express the value/state of a qubit one needs only two real numbers θ and $\gamma(=\vartheta-\varphi)$.

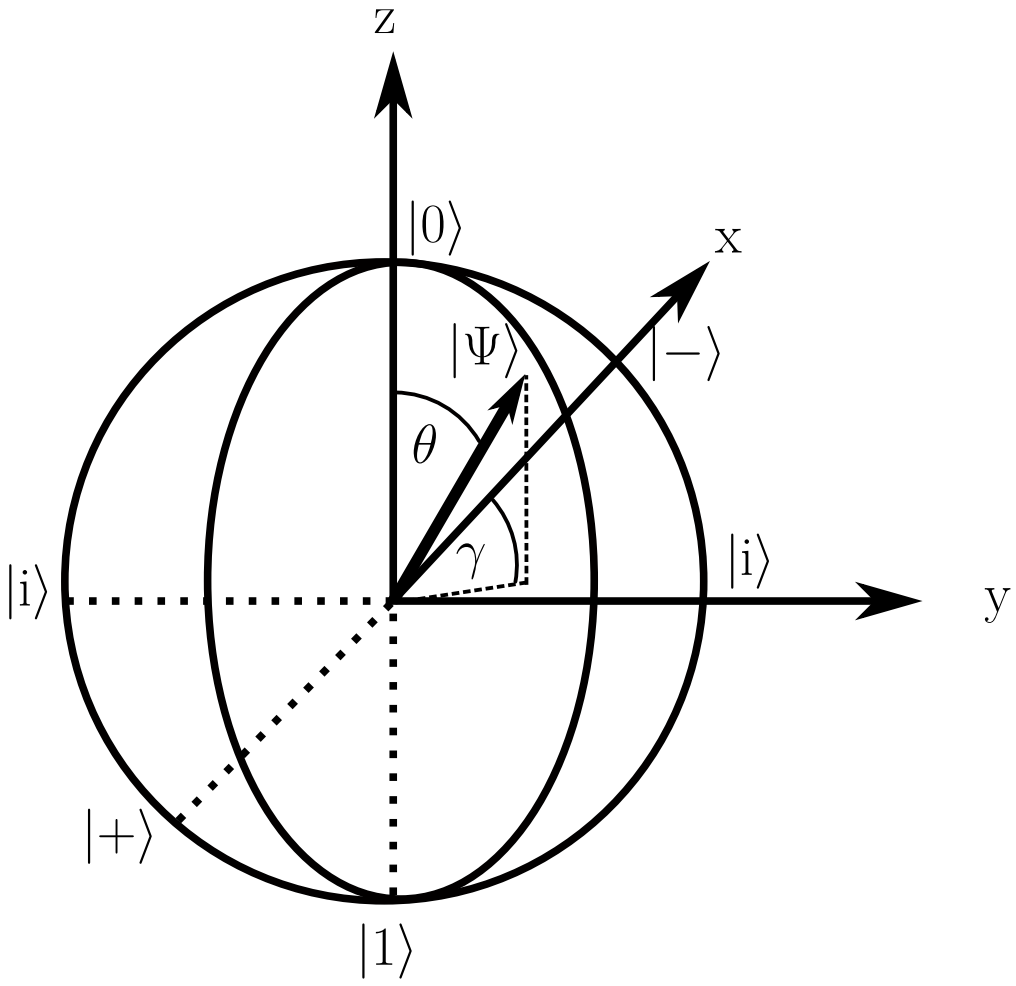


Figure 4.1: The Bloch sphere with the six most important basis states and the two angles γ (angle between state and z-axis) and θ (polar angle in the x-y axis) necessary to describe a general state $|\Psi\rangle$

The six states shown in Figure 4.1 are

$$\begin{aligned}
&|0\rangle,\ |1\rangle \text{ basis states belongs to z-axis,}\\
&|+\rangle\ = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right),\ |-\ \rangle\ = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)\ \text{ belongs to x-axis,}\\
&|\mathrm{i}\rangle\ \ = \frac{1}{\sqrt{2}}\left(|0\rangle + \mathrm{i}|1\rangle\right),\ |-\mathrm{i}\rangle\ = \frac{1}{\sqrt{2}}\left(|0\rangle - \mathrm{i}|1\rangle\right)\ \text{ belongs to y-axis.}
\end{aligned}$$

For the case of a photon, the Bloch sphere is called a **Poincare sphere** and the states have a clear physical interpretation:

$$\begin{aligned}
|0\rangle &\mathrel{\hat{=}} \text{polarisation along y-axis,}\\
|1\rangle &\mathrel{\hat{=}} \text{polarisation along z-axis,}\\
|+\rangle &\mathrel{\hat{=}} \text{polarisation } \frac{\pi}{4} \text{ to z-axis (and lying in the y-z plane),}\\
|-\rangle &\mathrel{\hat{=}} \text{polarisation } \frac{\pi}{2} \text{ to z-axis (and lying in the y-z plane),}\\
|\ \ \mathrm{i}\rangle &\mathrel{\hat{=}} \text{right-hand circular polarised light,}\\
|-\mathrm{i}\rangle &\mathrel{\hat{=}} \text{left-hand circular polarised light.}
\end{aligned}$$

An infinite number of information can be encoded into one qubit, **BUT** one measurement will only give one of the two basis values. By measuring an ensemble of qubits in the same quantum state, one is able to know the **true** quantum state in the ensemble and, therefore, the encoded information. The full power of quantum computing can only be realised through the use of **entanglement** and **superposition**.

4.3 Quantum statistics of qubits

There are two kinds of states of a qubit system that need to be distinguished:

1. **pure states:** These states can be expressed as a superposition of basis states in a Hilbert space. A superposition of pure states is also a pure state:

$$|\Psi\rangle = c_1|\psi_1\rangle + c_2|\psi_2\rangle + \cdots + c_N|\psi_N\rangle \tag{4.1}$$

   the c_i are the probability amplitudes to observe the state $\psi_i\rangle$ after a measurement of the quantum system.

2. **mixed states:** These states are a statistical ensemble of pure states $\left\{\{|\Psi_1\rangle, w_1\}, \{|\Psi_2\rangle, w_1\}, \ldots, \{|\Psi_N\rangle, w_N\}\right\}$ with a classical probability w_k to be in state $\Psi_i\rangle$. Such states can **not** be expressed a superposition of pure states or a single ket vector. One uses the density matrix ϱ to describe the mixed states:

$$\varrho = \sum_{i=1}^{n} w_i|\Psi_i\rangle\langle\Psi_i|. \tag{4.2}$$

   For a pure state $\varrho = |\Psi\rangle\langle\Psi|$.

4.3.1 Properties of the density matrix

- **positive semi-definiteness:** $\langle\Psi|\varrho|\Psi\rangle \geq 0\ \forall\ \Psi \in \mathcal{H}$
- **self-adjoint:** $\varrho = \varrho^\dagger$

- **trace one:** $\mathrm{Tr}(\varrho) = 1$

  proof:

  $$\mathrm{Tr}(\varrho) = \sum_i \langle n_i|\varrho|n_i\rangle = \sum_{i,j} w_j \langle n_i|\Psi_j\rangle\langle\Psi_j|n_i\rangle = \sum_j \langle\Psi| \sum_i |n_i\rangle\langle n_i|\Psi_j\rangle w_j = \sum_j w_j \langle\Psi_j|\mathrm{I}|\Psi_i\rangle = 1$$

- **averaging property:**

  $$\langle A\rangle = \mathrm{Tr}(\varrho A) = \sum_i \langle n_i|\varrho A|n_i\rangle = \sum_{i,j} w_j \langle n_i|\Psi_j\rangle\langle\Psi_j|A|n_i\rangle = \sum_j w_j \langle\Psi_j|A \underbrace{\sum_i |n_i\rangle\langle n_i|}_{\mathrm{I}} \Psi_j\rangle$$

  $$= \sum_j w_j \langle\Psi_j|A|\Psi_j\rangle = \underline{\underline{\langle A\rangle}}$$

If a closed quantum system is in a mixed state and is described by a density matrix ϱ, then its evolution is described using the Liouville quantum equation (von Neumann equation):

$$\mathrm{i}\hbar\frac{\partial}{\partial t}\varrho = [H, \varrho]. \tag{4.3}$$

The implementation of a quantum computer requires a physical system consisting of a large number of qubits. The Hilbert space of a physical system consisting of two qubits with Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$, is a tensor product $\mathcal{H}^4 = \mathcal{H}_1^2 \otimes \mathcal{H}_2^2$. If $\left\{|\Psi_1\rangle, |\Psi_2\rangle\right\}$ is a basis in $\mathcal{H}_1^2$ and $\left\{|\Phi_1\rangle, |\Phi_2\rangle\right\}$ is a basis in $\mathcal{H}_2^2$, then the basis in $\mathcal{H}^4$ is a set $\left\{|\Psi_i\rangle\otimes|\Phi_j\rangle\right\}_{i,j=1}^{2}$ $\left(\text{or } \left\{|\Psi_i\Phi_j\rangle\right\}_{i,j=1}^{2}\right)$.
The same goes for operators, **but be careful**: $A \otimes B \neq B \otimes A$!
For states with more than one qubit, entangled states arise.
A two qubit state $|\zeta\rangle = \sum_{i=1}^{2}\sum_{j=1}^{2} c_{ij}|\psi_i\rangle \otimes |\phi\rangle$ is pure if $|\zeta\rangle = |\zeta_1\rangle + |\zeta_2\rangle$ with $|\zeta_1\rangle \in \mathcal{H}_1, |\zeta_2\rangle \in \mathcal{H}_2$.
Such states are called **separable** and otherwise the state is **entangled** (or **inseparable**). A similar definition holds for mixed states and the density matrix, i.e. $\varrho = \varrho_1 \otimes \varrho_2$ is called separable and $\varrho \neq \varrho_1 \otimes \varrho_2$ is inseparable.

4.3.2 Reduced density matrix

If a system consists of two subsystems A and B which is described by a density operator ϱ_{AB}, then one can define so-called **reduced density operators** of the subsystems $\varrho_{\mathrm{A/B}}$ with expectation values of operators $L_{\mathrm{A/B}}$ in the subsystems

$$\langle L_\mathrm{A}\rangle_\mathrm{A} = \mathrm{Tr}(L_\mathrm{A}\varrho_\mathrm{A}) \quad \text{with } \varrho_\mathrm{A} = \mathrm{Tr}_\mathrm{B}(\varrho_\mathrm{AB}) \tag{4.4}$$

$$\varrho_\mathrm{A} = \sum_{j=1}^{M} \left(\mathrm{I}_\mathrm{A}^{N\times N} \otimes \langle\xi_j|\right) \varrho_\mathrm{AB} \left(\mathrm{I}_\mathrm{A}^{N\times N} \otimes |\xi_j\rangle\right) \tag{4.5}$$

$$\varrho_\mathrm{B} = \sum_{j=1}^{N} \left(\langle\zeta_j| \otimes \mathrm{I}_\mathrm{B}^{M\times M}\right) \varrho_\mathrm{AB} \left(|\zeta_j\rangle \otimes \mathrm{I}_\mathrm{B}^{M\times M}\right) \tag{4.6}$$

here $\mathrm{Tr}_{\mathrm{A/B}}(\dots)$ is the trace over the basis in the respective subsystem, e.g.
$\mathrm{Tr}_\mathrm{A}(\dots) = \sum_i \langle\Psi_\mathrm{A}| \otimes \mathrm{I}_\mathrm{B}(\dots)|\Psi_\mathrm{A}\rangle \otimes \mathrm{I}_\mathrm{B}$. These reduced density matrices have the following properties:

- **self-conjugation** $\varrho_\mathrm{A} = \varrho_\mathrm{A}^\dagger,\ \varrho_\mathrm{B} = \varrho_\mathrm{B}^\dagger$
- **positive definiteness**

  $\langle\Psi_\mathrm{A}|\varrho_\mathrm{A}|\Psi_\mathrm{A}\rangle \geq 0 \ \forall\ \Psi_\mathrm{A} \in \mathcal{H}_\mathrm{A}$
  $\langle\Phi_\mathrm{B}|\varrho_\mathrm{B}|\Phi_\mathrm{B}\rangle \geq 0 \ \forall\ \Phi_\mathrm{B} \in \mathcal{H}_\mathrm{B}$

- **equality in retracing**

$$\begin{array}{lcl} \mathrm{Tr_A}(\varrho_{\mathrm{AB}}) & \neq & \mathrm{Tr_B}(\varrho_{\mathrm{AB}}) \\ \mathrm{Tr}(\varrho_{\mathrm{B}}) & = & \mathrm{Tr}(\varrho_{\mathrm{A}}) \end{array}$$

- **equality of determinants**

$$\begin{array}{lcl} \det\left(\mathrm{Tr_A}(\varrho_{\mathrm{AB}})\right) & = & \det\left(\mathrm{Tr_B}(\varrho_{\mathrm{AB}})\right) \\ \det\varrho_{\mathrm{B}} & = & \det\varrho_{\mathrm{A}} \end{array}$$

For a separable system no information is lost in the tracing process over one of the subsystems, but for entangled states some information on the subsystem that is traced out is lost.

4.3.3 Schmidt decomposition

Theorem: For a pure state $|\Psi^{\mathrm{AB}}\rangle$ of a composite quantum system "A+B" there exists a set of orthonormal states $\{|\xi_i^{\mathrm{A}}\rangle\}$ of system "A" and a set of orthonormal states $\{|$
$phi_i^{\mathrm{B}}\rangle\}$ of system "B" such that

$$|\Psi^{\mathrm{AB}}\rangle = \sum_i \sqrt{\lambda_i}|\xi_i^{\mathrm{A}}\rangle \otimes |\phi_i^{\mathrm{B}}$$

with $\{\sqrt{\lambda_i}\}$ being non-negative real numbers such that $\sum_i \lambda_i = 1$. The numbers $\{\sqrt{\lambda_i}\}$ are called the **Schmidt coefficients**. The number of non-zero Schmidt coefficients is called the **Schmidt number**. A pure quantum state is called separable if the Schmidt number is one, i.e. the composite system state vector can be represented as a tensor product of each of the state's vectors:

$$|\Psi^{\mathrm{AB}}\rangle = |\xi^{\mathrm{A}}\rangle \otimes |\phi^{\mathrm{B}}\rangle.$$

A pure state is called entangled if the Schmidt number is greater than one. Therefore, the Schmidt number can be used as a criterion of a state's separability.

4.4 Bell states (EPR pairs)

The most entangled states of two qubits are called **Bell states**. These are the four states

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle\Big)$$
$$|\beta_{01}\rangle = \frac{1}{\sqrt{2}}\Big(|01\rangle + |10\rangle\Big)$$
$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}\Big(|00\rangle - |11\rangle\Big)$$
$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}}\Big(|01\rangle - |10\rangle\Big)$$

All of these states are either totally correlated or anticorrelated. Most entangled means that

$$\varrho_{\mathrm{A}} = \mathrm{Tr}_{\mathrm{B}}\Big(|\beta_{ij}\rangle\langle\beta|\Big) = \frac{1}{2}\mathrm{I}_{\mathrm{A}}$$
$$\varrho_{\mathrm{B}} = \mathrm{Tr}_{\mathrm{A}}\Big(|\beta_{ij}\rangle\langle\beta|\Big) = \frac{1}{2}\mathrm{I}_{\mathrm{B}}$$

for the reduced density matrices, i.e. the result of a measurement is completely random!!!
The four Bell states form an orthonormal basis for a two qubit Hilbert space. Therefore, the measurement of qubits should be proceeded in the appropriate basis. The measurement of a qubit in a Bell state could be done using the scheme (Bell measurements) shown in Figure 4.2 which transform the Bell states in the following way:

$$|\beta_{00}\rangle \to |00\rangle,\ |\beta_{01}\rangle \to |01\rangle,\ |\beta_{10}\rangle \to |10\rangle,\ |\beta_{11}\rangle \to |11\rangle.$$

Entangled states are particularly interesting as they manifest correlations which do not have any classical analogues. The intrinsic feature of the correlation is their **nonlocality**. To entangle a pair of quantum systems one should bring them into interaction with each other (directly or via a auxiliary system), i.e. one should perform a **collective unitary** transformation on the composed system. Bell states are widely used in quantum informatics and quantum telecommunication, e.g. in superdense coding and quantum teleportation which we will discuss soon!

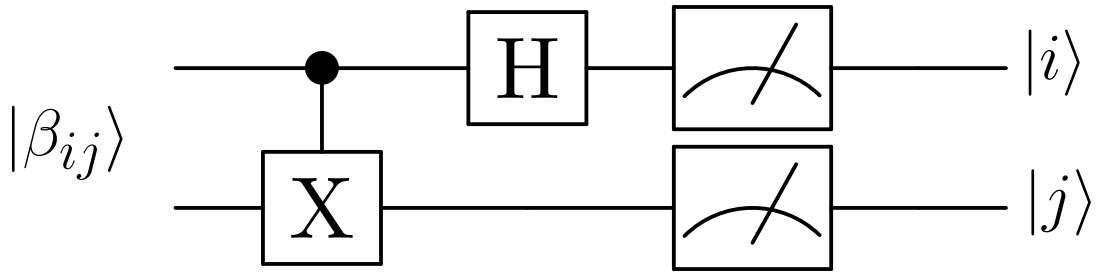


Figure 4.2: The quantum circuit for a Bell measurement. The input $|\beta_{ij}\rangle$ is one of the Bell state and the result is a certain measurement of the separable state $|i\rangle \otimes |j\rangle$.

4.4.1 Bell inequalities

The theory of hidden variables is contrary to quantum mechanics. Bell inequalities are a set of experiments which allow one to compare the predictions of hidden variables conception and quantum mechanics predictions: A quantum system composed of two subsystems "A+B" with observables L_{A} and L'_{A} in system A and observables M_{B} and M'_{B} in system B with a simple spectrum $\{-1,1\}$ for each observable. If these observables are physical reality, i.e. their eigenvalues are possible, there should exist a spectrum $\{l_i^{\mathrm{A}}, l_j'^{\mathrm{A}}, m_k^{\mathrm{B}}, m_n'^{\mathrm{B}}\}_{i,j,k,n=1,2}$ which could have been obtained. This gives rise to 16 states/possibilities/sets defined by the observable

$$s_{ijkn} = \Big(l_i^{\mathrm{A}} + l_j'^{\mathrm{A}}\Big)m_k^{\mathrm{B}} + \Big(-l_i^{\mathrm{A}} + l_j'^{\mathrm{A}}\Big)m_n'^{\mathrm{B}}.$$

Obviously, $|s_{ijkn}| \leq 2$, so when taking the ensemble average ($N \gg 1$), we get

$$|\langle S\rangle| = \frac{1}{N}\Big|\sum_{i,j,k,n} s_{ijkn} \underbrace{N_{ijkn}}_{\text{number of results with } s_{ijkn}}\Big| = \Big|\sum_{i,j,k,n} s_{ijkn} \underbrace{p_{ijkn}}_{\text{probability of } s_{ijkn}}\Big| \leq 2\Big|\sum_{i,j,k,n} p_{ijkn}\Big| = 2.$$

Therefore, $|\langle S\rangle| \leq 2$ or in other words by using the definition of S

$$|\langle S\rangle| = \Big|\langle L_{\mathrm{A}}M_{\mathrm{B}}\rangle - \langle L_{\mathrm{A}}M'_{\mathrm{B}}\rangle + \langle L'_{\mathrm{A}}M_{\mathrm{B}}\rangle + \langle L'_{\mathrm{A}}M'_{\mathrm{B}}\rangle\Big| \leq 2.$$

These are the famous **Bell inequalities**.
In the quantum version

$$[L_{\mathrm{A}}, L'_{\mathrm{A}}] \neq 0 \text{ and } [M_{\mathrm{A}}, M'_{\mathrm{A}}] \neq 0.$$

Because of the spectrum of all operators

$$L_{\mathrm{A}}^2 = L_{\mathrm{A}}'^2 = M_{\mathrm{B}}^2 = M_{\mathrm{B}}'^2 = \mathrm{I}$$

We can define the operator $\hat{S}$ analogues to the classical S

$$\hat{S} = L_{\mathrm{A}}M_{\mathrm{B}} - L_{\mathrm{A}}M'_{\mathrm{B}} + L'_{\mathrm{A}}M_{\mathrm{B}} + L'_{\mathrm{A}}M'_{\mathrm{B}}.$$

The **Tsirelson bound** for $|\hat{S}|$ is

$$\begin{aligned} 2\sqrt{2}\mathrm{I} - \hat{S} &= \frac{2\sqrt{2}}{4}\Big(L_{\mathrm{A}}^2 + L_{\mathrm{A}}'^2 + M_{\mathrm{B}}^2 + M'^2\Big) - \hat{S} \\ &= \frac{1}{\sqrt{2}}\Big(L'_{\mathrm{A}} - \frac{M_{\mathrm{B}} + M'_{\mathrm{B}}}{\sqrt{2}}\Big)^2 + \Big(L_{\mathrm{A}} - \frac{M_{\mathrm{B}} - M'_{\mathrm{B}}}{\sqrt{2}}\Big)^2 \Rightarrow \underline{\underline{0 \leq 2\sqrt{2}\langle \mathrm{I}\rangle - \langle \hat{S}\rangle}} \end{aligned}$$

and therefore $\langle \hat{S}\rangle \leq 2\sqrt{2}$ and analogously one shows $\langle \hat{S}\rangle \geq -2\sqrt{2}$ and, hence, for the quantum system $|\langle \hat{S}\rangle| \leq 2\sqrt{2}$. When the Tsirelson bound is reached in an experiment, then the Bell inequalities are violated and quantum theory can be considered to be correct.

Chapter 5

General principles of classical computations

According to the **Church-Turing thesis**, the computational problem can be solved on some physically reliable computer only if it is solvable on the simplest abstract "machine" called the **Turing machine** (see Figure 5.1). A Turing machine is equivalent to the **circuit computational model** (see Figure 5.2). In the following, we discuss the most important logical gates.

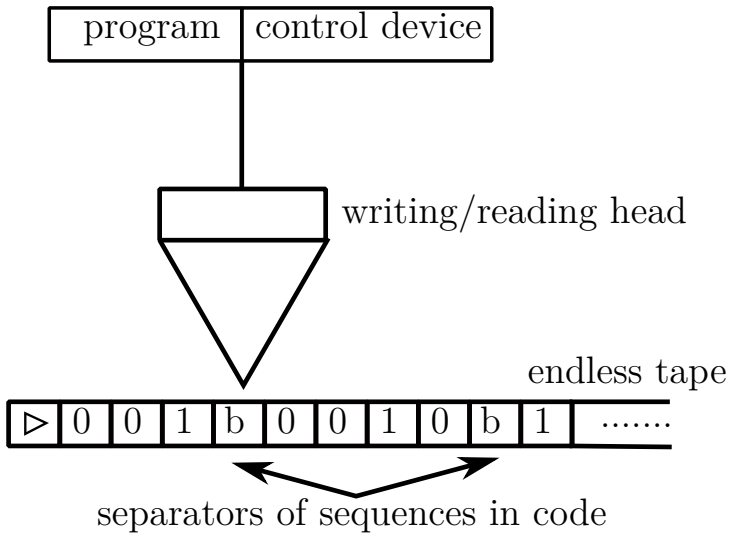


Figure 5.1: Sketch of the Turing machine

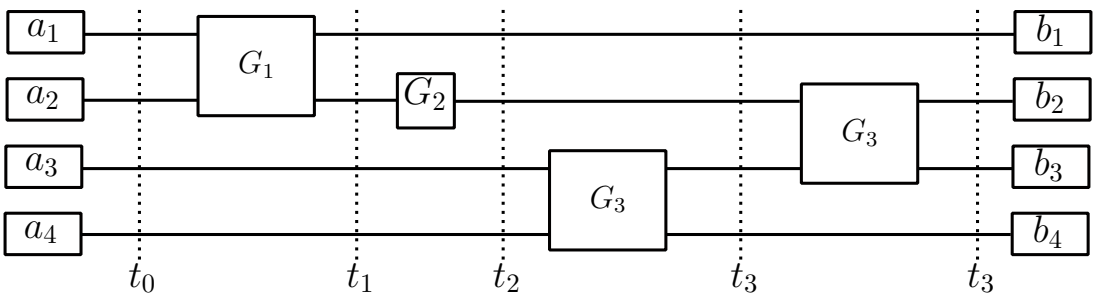
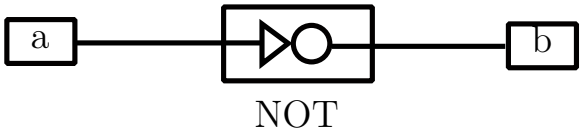


Figure 5.2: Sketch of the circuit computational model. Here G_i are logical gates applied at times t_i that take the bits from their initial state a_j into their final state b_j.

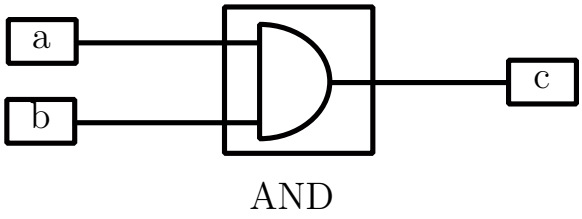
5.1 elementary logic gates

- **NOT element:** the NOT element (negation) changes the value of a bit to the opposite: $b = a \oplus_2 1 = \mathrm{mod}_2(a+1) = (a+1)\%2$



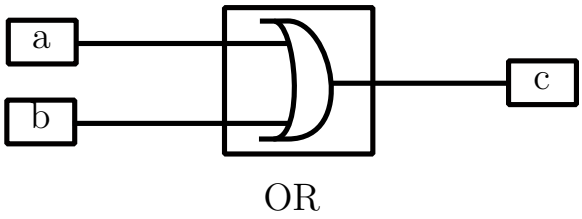
a	b
0	1
1	0

- **AND element:** the AND element (conjugation) produces a logical multiplication: $c = a \cdot b = \min(a, b)$



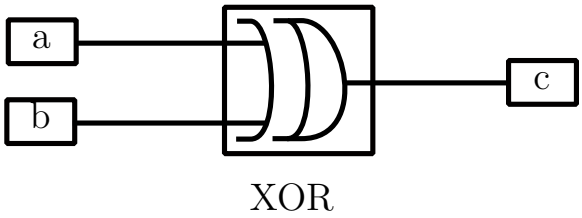
a	b	c
0	0	0
0	1	0
1	0	0
1	1	1

- **OR element:** the OR element (disjunction) returns the largest value: $c = a + b - a \cdot b = \max(a, b)$



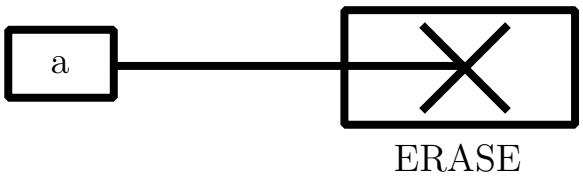
a	b	c
0	0	0
0	1	1
1	0	1
1	1	1

- **XOR element:** the XOR element (strict disjunction) is addition modulo two: $c = (a + b)\%2 = a \otimes_2 b = \max(a, b) - \min(a, b)$



a	b	c
0	0	0
0	1	1
1	0	1
1	1	0

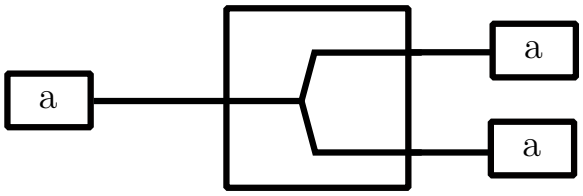
- **ERASE element:** the ERASE element removes a bit



ERASE

a	b
0	-
1	-

- **FANOUT element:** the FANOUT element duplicates a bit

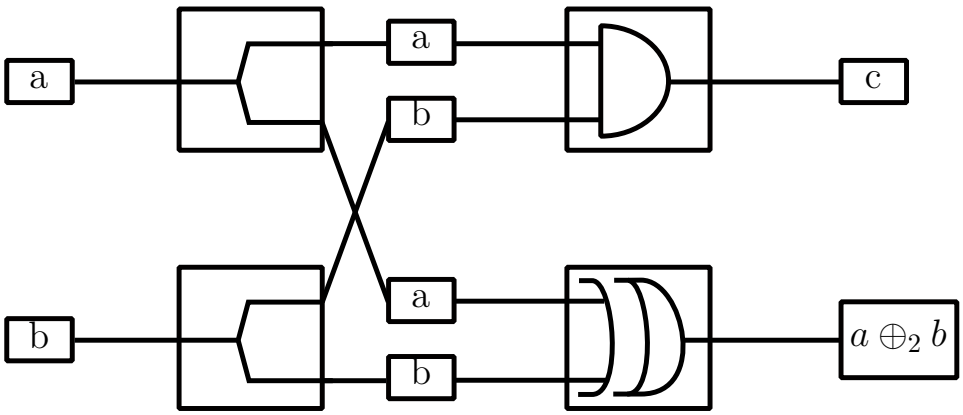


FANOUT

a	b	c
0	0	0
1	1	1

5.2 The simplest classical computations

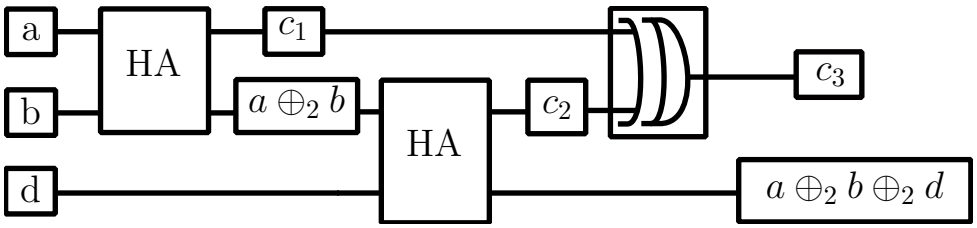
5.2.1 Half-adder



a	b	c	$a \oplus_2 b$	R_2	R_{10}
0	0	0	0	00	0
0	1	0	1	01	1
1	0	0	1	01	1
1	1	1	0	10	2

The half-adder is insufficient for adding more than two single bits (two in and outputs).

5.2.2 Full-adder



a	b	d	c_1	$a \oplus_2 b$	d	c_1	c_2	$a \oplus_2 b \oplus_2 d$	c_3	$a \oplus_2 b \oplus_2 d$
0	0	0	0	0	0	0	0	0	0	0
0	1	0	0	1	0	0	0	1	0	1
1	0	0	0	1	0	0	0	1	0	1
1	1	0	1	0	0	1	0	0	1	0
0	0	1	0	0	1	0	0	1	0	1
0	1	1	0	1	1	0	1	0	1	0
1	0	1	0	1	1	0	1	0	1	0
1	1	1	1	0	1	1	0	1	1	1

For adding multi-digit numbers, one needs a cascade of half- and full-adders.

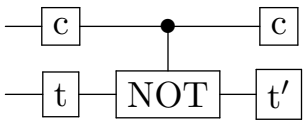
5.3 Landauer principle/reversible gates

AND, OR, and XOR gates are irreversible logic elements, i.e. one can not recover the full information of the two input bits from the one output bit (in all cases). All logic gates that use irreversible elements for their switches are also irreversible, e.g. half-adder and full-adder. The Landauer principle states the following:

- demolition of information is a dissipative process, i.e. it can not be reversed
- loss (destruction) of one bit of information, therefore, leads to the release of energy (heat) $W = k_{\mathrm{B}}T \log 2$
- it is not important for classical computations but plays a very crucial role in quantum computing → any heating can lead to decoherence
- Landauer found that any computation can be performed using **only reversible logic operations (gates)**

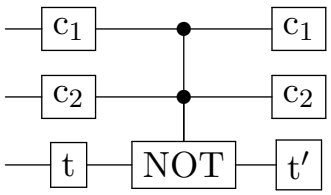
The NOT element is a reversible logic element. The following logic elements are very important:

- **CNOT element:** the CNOT element (controlled negation) changes the value of a bit to the opposite for a certain value of the control bit (1). The resulting truth table is the same as for XOR. It copies the target bit t if the control bit c is given as 0 to the CNOT gate.



t	c	t'
0	0	0
0	1	1
1	0	1
1	1	0

- **CCNOT element:** the CCNOT element (Toffoli element) changes the value of a bit to the opposite for certain values of the two control bits (1). The resulting truth table is the same as for XOR. It copies the target bit t if the control bit c is given as 0 to the CNOT gate. For choosing $t = 0$ one gets the AND gate for the other two bits with result t' (XOR for $c_1 = 1$ or $c_2 = 1$), a OR gate for $a = 0$ and $c_1 \rightarrow \mathrm{NOT}(c_1)$,$c_2 \rightarrow \mathrm{NOT}(c_2)$, a NOT gate for $c_1 = c_2 = 1$ and a FANOUT is realised for $c_2 = 1, a = 0$. Applying CCNOT another time to the result reverses the effect.



c_1	c_2	t	t'
0	0	0	0
0	1	0	0
1	0	0	0
1	1	0	1
0	0	1	1
0	1	1	1
1	0	1	1
1	1	1	0

With these two gates we can build the a reversible version of the half- and of the full-adder as shown in Figures 5.3 and 5.4.

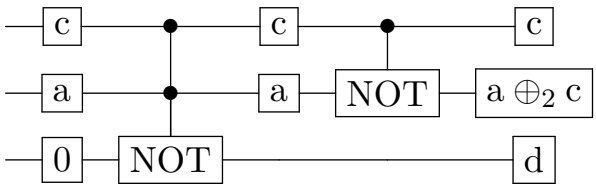


Figure 5.3: scheme of the reversible half-adder

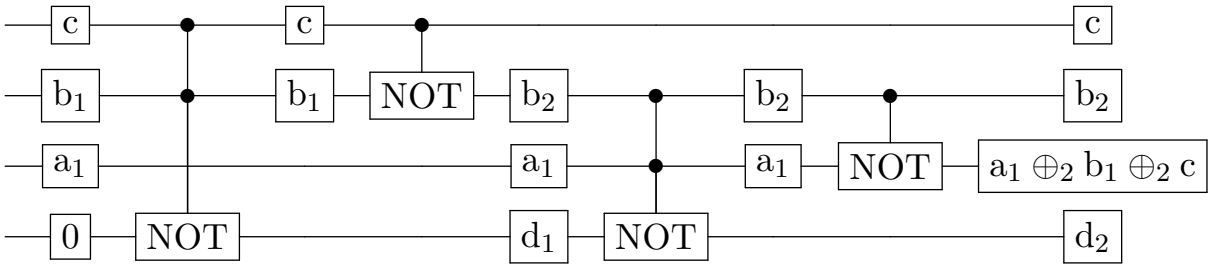


Figure 5.4: scheme of the reversible full-adder

Chapter 6

General principles of quantum computations

6.1 Pauli matrices

The three Pauli matrices are

$$X = \sigma_x = \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \sigma_y = \sigma_2 = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}, \quad Z = \sigma_z = \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Properties:

- They form the basis of all 2×2 hermitian matrices with zero trace and together with the identity matrix they form the basis of all hermitian 2×2 matrices, i.e. any hermitian operator A acting on $\mathcal{H}^2$ can be represented as a linear combination of the Pauli matrices:

  $$A = c_0 \mathrm{I}_2 + \sum_{i=1}^{3} c_i \sigma_i$$

  and any operator function of the Pauli matrices can be represented as a linear combination of the Pauli matrices:

  $$f(\{\sigma_i\}_{i=1,2,3}) = a_0 \mathrm{I}_2 + \sum_{i=1}^{3} a_i \sigma_i.$$

  In particular, the rotation operators $R_{\boldsymbol{n}}(\varphi)$ which rotate the system around the axis directed along $\boldsymbol{n}$ by the angle φ are

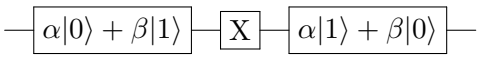
  $$R_{\boldsymbol{n}}(\varphi) = \mathrm{I}_2 \cos\frac{\varphi}{2} - \mathrm{i}(\boldsymbol{\sigma} \cdot \boldsymbol{n}) \sin\frac{\varphi}{2}.$$

- Their squares yield the identity matrix $\sigma_i^2 = \mathrm{I}_2$
- They have trace zero $\mathrm{Tr}\sigma_i = 0$
- Their determinant is -1 $\det\sigma_i = -1$
- Their commutator $[\sigma_i, \sigma_j]_- = 2\mathrm{i}\epsilon_{ijk}\sigma_k$
- Because of $\sigma_i\sigma_j = \mathrm{i}\epsilon_{ijk}\sigma_k$, their anticommutator is zero

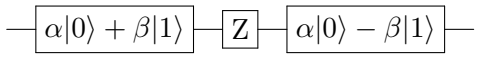
6.2 Single-qubit gates

Like classical computations, quantum computations can be represented by quantum switching boards (quantum circuit computation models). Quantum information theory operates with logical elements whose actions can be described using certain **unitary** quantum transformations, i.e. their actions are **reversible**[1].

- **X element:** In the σ_z-basis this operation is represented by σ_x. It realises a NOT operation.



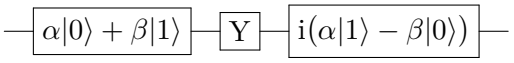
- **Z element:** In the σ_z-basis this operation is represented by σ_z. It shifts the relative phase of a superposition



  It is the NOT element in the **Hadamard** basis:

$$Z|+\rangle = Z\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |-\rangle, \quad Z|-\rangle = Z\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |+\rangle$$

- **Y element:** In the σ_z-basis this operation is represented by σ_y. It realises a NOT operation and a phase shift



The X,Y,Z elements rotate the states around the respective axes of the Bloch sphere (by π).

- **Hadamard or Hadamard-Walsh element:** H performs the transition from one basis to another (computational to Hadamard and Hadamard to the computational basis)

$$H|0\rangle = |+\rangle, \quad H|1\rangle = |-\rangle, \quad H|+\rangle = |0\rangle, \quad H|-\rangle = |1\rangle$$

  In the z-basis $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and $H^2 = \mathrm{I}_2$.

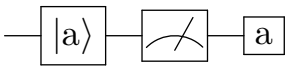
- $\pi/8$ **phase element T:**

$$T\left(\alpha|0\rangle + \beta|1\rangle\right) = \alpha|0\rangle + \mathrm{e}^{\mathrm{i}\pi/4}\beta|1\rangle$$

  In the z-basis $T = \begin{pmatrix} \mathrm{e}^{-\mathrm{i}\pi/8} & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\pi/8} \end{pmatrix} \simeq \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\pi/4} \end{pmatrix}$.

A set of unitary elements is called **universal** for single-qubit elements, if any other single-qubit unitary element can be obtained through a quantum circuit built only on elements from this set. The sets $\{H, T\}$ and $\{I, X, Y, Z\}$ are universal sets for single-qubit elements.

- **The measurement element:** It turns a state into a result of the calculation (the state is destroyed and a real number obtained) → the qubit is destroyed.

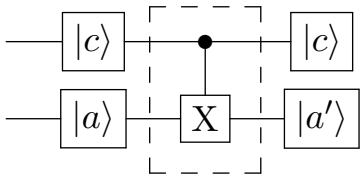


[1] This ensures that the quantum computer does not heat up and results are lost due to decoherence

6.3 Controlled quantum logic gates

To perform quantum computations one needs controlled quantum elements that act on several qubits at once in addition to single-qubit logic elements. Qubits are divided into **control** and **target** qubits as in classical computations. A logical operation on the target qubits is determined by the state of the control qubits. If the control qubits are in a superposition of states, each term of the superposition must be considered separately.

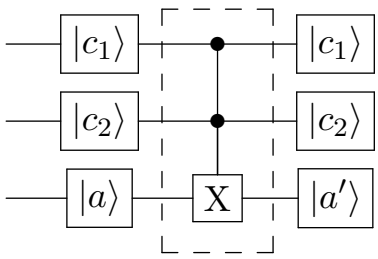
- **CNOT element (CX):** The CNOT element is a controlled ¨NOT". It changes the value of the qubit $|a\rangle$ to the opposite if the control qubit $|c\rangle = |1\rangle$ and it does not change the state $|a\rangle$.



$$|c\rangle = \alpha|0\rangle + \beta|1\rangle, \quad |a\rangle = \gamma|0\rangle + \delta|1\rangle$$
$$|c\rangle \otimes |a\rangle = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle$$
$$C_1X_2|c\rangle \otimes |a\rangle = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|11\rangle + \beta\delta|10\rangle$$

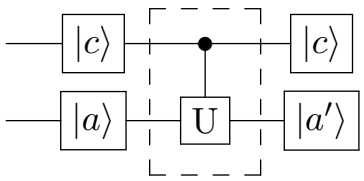
For $\delta = 0, \gamma = 1$ the states are entangled after the CX $\alpha|00\rangle + \beta|11\rangle$!

- **CCNOT element (CCX):** The CCX is the quantum Toffoli element. It changes the state of the target element $|a\rangle$ to the opposite if both qubits are in the states $|c_i\rangle = |1\rangle$ and does not change it if either is in the state $|c_i\rangle = |0\rangle$



$$|c_1\rangle = \alpha|0\rangle + \beta|1\rangle,\ |c_2\rangle = \gamma|0\rangle + \delta|1\rangle,\ |a\rangle = \epsilon|0\rangle + \phi|1\rangle$$
$$\begin{aligned}|c_1\rangle \otimes |c_2\rangle \otimes |a\rangle &= \alpha\gamma\epsilon 000\rangle + \alpha\gamma\phi|001\rangle + \alpha\delta\epsilon|010\rangle \\ &+ \alpha\delta\phi|011\rangle + \beta\gamma\epsilon|100\rangle + \beta\gamma\phi|101\rangle \\ &+ \beta\delta\epsilon|110\rangle + \beta\delta\phi|111\rangle \\ C_1C_2X_3|c_1\rangle \otimes |c_2\rangle \otimes |a\rangle &= \alpha\gamma\epsilon 000\rangle + \alpha\gamma\phi|001\rangle + \alpha\delta\epsilon|010\rangle \\ &+ \alpha\delta\phi|011\rangle + \beta\gamma\epsilon|100\rangle + \beta\gamma\phi|101\rangle \\ &+ \beta\delta\epsilon|111\rangle + \beta\delta\phi|110\rangle\end{aligned}$$

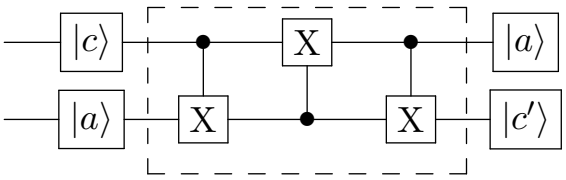
- **CU element:** The CU element changes the state of the qubit $|a\rangle$ to $U|a\rangle$ if the qubit $|c\rangle = |1\rangle$ and leaves it as it is otherwise.



$$|c\rangle \otimes |a\rangle = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle$$
$$C_1U_2|c\rangle \otimes |a\rangle = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|1\rangle U|0\rangle + \beta\delta|1\rangle U|1\rangle$$

The set of elements $\{H, T, CX\}$ is a **universal** set for any unitary element, i.e. a quantum computation circuit of arbitrary complexity can be constructed from these and only these elements.

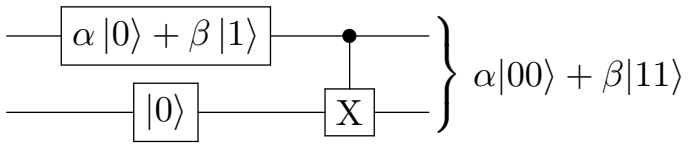
The SWAP circuit changes the order of the input qubits



$$
\begin{aligned}
|c\rangle \otimes |a\rangle &= \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle \\
C_1X_2|c\rangle \otimes |a\rangle &= \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|11\rangle + \beta\delta|10\rangle \\
C_2X_1C_1X_2|c\rangle \otimes |a\rangle &= \alpha\gamma|00\rangle + \alpha\delta|11\rangle + \beta\gamma|01\rangle + \beta\delta|10\rangle \\
C_1X_2C_2X_1C_1X_2|c\rangle \otimes |a\rangle &= \alpha\gamma|00\rangle + \alpha\delta|10\rangle + \beta\gamma|01\rangle + \beta\delta|11\rangle \\
&= (\gamma|0\rangle + \delta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle) \\
&= |a\rangle \otimes |c\rangle
\end{aligned}
$$

6.4 No-cloning theorem

There is no quantum realisation of the classical FANOUT gate. This is known as the **No-cloning theorem**. The naive approach inspired by the classical gate might be



For a general state as the target, we get

$$(\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \epsilon|1\rangle) \stackrel{?}{=} \alpha|00\rangle + \beta|11\rangle$$

Unfortunately, this is only true for an eigenstate. This means that an eigenstate can be copied but not a general state. One can proof that there is no unitary operation that does copy an arbitrary state into another one.

Proof:

$$
\begin{aligned}
U|\Psi\rangle|\Xi\rangle|\text{in}\rangle &\to |\Psi\rangle|\Psi\rangle|\text{out}_\Psi\rangle \\
U|\xi\rangle|\Xi\rangle|\text{in}\rangle &\to |\Xi\rangle|\Psi\rangle|\text{out}_\Xi\rangle \\
\langle\text{out}_\Psi|\text{out}_\Xi\rangle &\neq 1 \\
U^\dagger = U^{-1} &\Rightarrow U^\dagger U = \mathrm{I}
\end{aligned}
$$

Multiplying the upper left state with the down left state:

$$
\begin{aligned}
\langle\Psi|\langle\Xi|\langle\text{in}|U^\dagger U|\Xi\rangle|\Xi\rangle|\text{in}\rangle &\underset{\text{equations}}{\overset{\text{right}}{=}} \big(\langle\Psi|\langle\Psi|\langle\text{out}_\Psi|\big)|\Xi\rangle|\Xi\rangle|\text{out}_\Xi\rangle \\
&= \big|\big(\langle\Psi|\Xi\rangle\big)\big|^2\langle\text{out}_\Psi|\text{out}_\Xi\rangle
\end{aligned}
$$

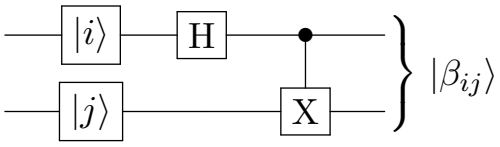
Because of the normalisation

$$
\begin{aligned}
\langle\Psi|\Xi\rangle &= \big(\langle\Psi|\Xi\rangle\big)^2\langle\text{out}_\Psi|\text{out}_\Xi\rangle \\
\mathrm{I} &= \langle\Psi|\Xi\rangle\langle\text{out}_\Psi|\text{out}_\Xi\rangle
\end{aligned}
$$

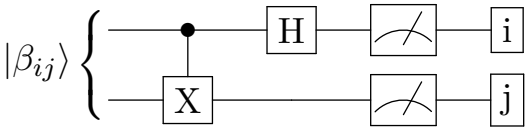
As $\big|\langle\Psi|\Xi\rangle\big| < 1$ and $\langle\text{out}_\Psi|\text{out}_\Xi\rangle \leq 1$ the above equality is a contradiction. Therefore, only eigenstates can be copied and all logical operations and calculations need to be carried out before a measurement, i.e. obtaining an result. **This is bad for quantum computing, but very good for quantum cryptography**.

6.5 Superdense coding

One first generates a Bell state[2]



The reverse scheme is used for the measurement of the Bell state[3]



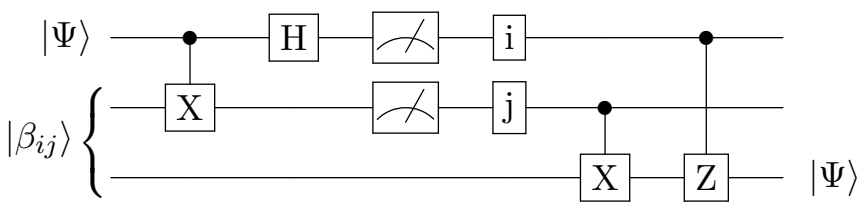
The quantum entanglement between two qubits allows one to encode information using the qubits' **relative phase** and **not only** the qubits' **values**. One can transfer two classical bits of information using only a single qubit via the **superdense coding** protocol:

1. A specific Bell state is prepared, e.g. $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
2. Alice gets the first qubit (photon) of the Bel state and performs a operation I to encode the information "00", the operation X to encode "01", the operation Z to encode "10" or the operation ZX to encode the information "11"
3. Alice sends her photon to Bob
4. Bob performs a Bell measurement

By only operations to one qubit, a two bit message can be encoded.

6.6 Quantum teleportation

Quantum teleportation is a way to transfer a quantum state over long distances using spatially separated entangled EPR/Bell state pair and a classical communication channel. By this way of transferring information, the quantum state of one physical system is **destroyed** at the transmission point during the measurement and **recreated** at the reception point on the other physical system.
Protocol



[2]This procedure is not used in practice to obtain a Bell state as it is much easier to obtain them through actual physical processes.
[3]The calculation was carried out in I

For $|\beta_{00}\rangle$:
At the beginning the state is

$$|\Psi\rangle|\beta_{00}\rangle = \frac{1}{\sqrt{2}}[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)]$$

After C_1X_2:

$$= \frac{1}{\sqrt{2}}[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle)]$$

After H_1:

$$= \frac{1}{2}[\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)]$$
$$= \frac{1}{2}[|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)]$$

After the two control gates, the final state is

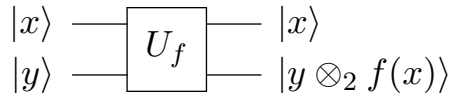
$$\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle) = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \otimes |\Psi\rangle.$$

The state $|\Psi\rangle$ has been successfully copied into the state of the Bell state's second qubit, but has been destroyed in the initial qubit through the measurement. One can use quantum teleportation to perform quantum logical operations.

6.7 Quantum parallelism

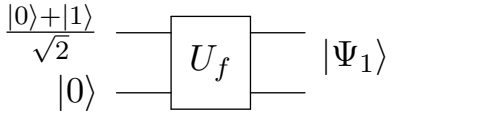
Quantum parallelism is a fundamental property of any quantum algorithm based on the quantum superposition principle. In quantum computational devices it allows one to obtain several values of a certain function $f(x)$ in points $\{x_1, x_2, \ldots, x_n\}$ simultaneously. It means that only **one** unitary logical operation $U_f : \{x_1, x_2, \ldots, x_n\} \to \{f(x_1), f(x_2), \ldots, f(x_n)\}$ is needed. A typical logical transformation (black box) is e.g. $f : \{0, 1\} \to \{0, 1\}$.

$$U_f : |x, y\rangle \to |x, y \otimes_2 f(x)\rangle.$$



The first register (x) is called the **data register** and the second register (y and $y \otimes_2 f(x)$) is called the value register.
Simultaneous computation of two values of $f(x)$:

$$U_f : \tfrac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \to \tfrac{1}{\sqrt{2}}(|0, f(0)\rangle + |1f(1)\rangle)$$



After the U_f transformation, every superposition term keeps information on **different** required function values. In contrast to classical computations, because of quantum parallelism one only needs one logical operation for calculating the values of $f(x)$. Like for the classical computer, one only obtains one value when measuring the superposition state $f(0)$ or $f(1)$. To get more practical benefits from quantum computations, we have to learn how to extract more information from the superposition $\frac{1}{\sqrt{2}}(|0, f(0)\rangle + |1f(1)\rangle)$. In the next chapter, we will look at different **quantum algorithms** that give recipes for how this can be done. All obtained results can be generalised to a multidimensional case.

Chapter 7

Quantum algorithms

Chapter 8

Quantum error correction

8.1 Features of classical error correction

8.2 Features of quantum error correction

Part III

Introduction to quantum computing

8.3 Shor-algorithm

Part IV

One-way quantum computation