Lecture Notes for Future Computing Architecture and Programming Paradigms (mod. Quantum Computing Architectures, Programming and Applications) Summer Term 2024

Prof. Dr. D. Kranzlmüller, Tobias Guggemos,
Sophia Grundner-Culemann, Maximilian Höb,
Korbinian Staudacher, Xiao-Ting Michelle To,
Florian Krötz

March 13, 2024

Contents

Chapter 1

Linear Algebra of Qubits

1.1 Quantum Bits (Qubits)

A quantum bit (*qubit*) can described as the linear combination of the states

$$\alpha \cdot |0\rangle + \beta \cdot |1\rangle \, (\alpha, \beta \in \mathbb{C})$$

where α and β are called **amplitudes**. With:

$$|\alpha|^2 + |\beta|^2 = 1$$

In contrast to a classic bit, which only has either the value 0 or 1, a qubit can be in an overlay state, which is also called **superposition**. It is not possible to read this state directly from a qubit. To obtain any information about a qubit it has to be measured, which destroys the superposition. During the measurement, the state $|0\rangle$ is observed with probability $|\alpha|^2$ and the state $|1\rangle$ with probability $|\beta|^2$.
The state of a qubit is considered to be a two-dimensional vector with complex entries. The so-called *state vector* is:

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

This can be specified as a linear combination of the two-dimensional standard basis vectors:

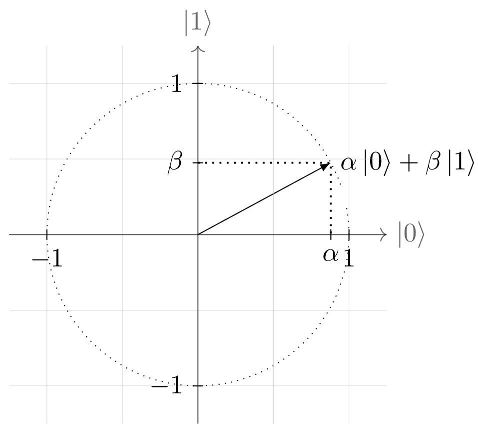
$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \alpha \, |0\rangle + \beta \, |1\rangle$$

The notation $\langle\psi|$ or $|\psi\rangle$ is called **Dirac-** or **Bra-Ket-** notation *(from "bracket")*. If $|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$, then $\langle\psi| = (\alpha^* \;\; \beta^*)$, i.e. the complex conjugate row vector.

1.2 Graphical Representation of a Qubit

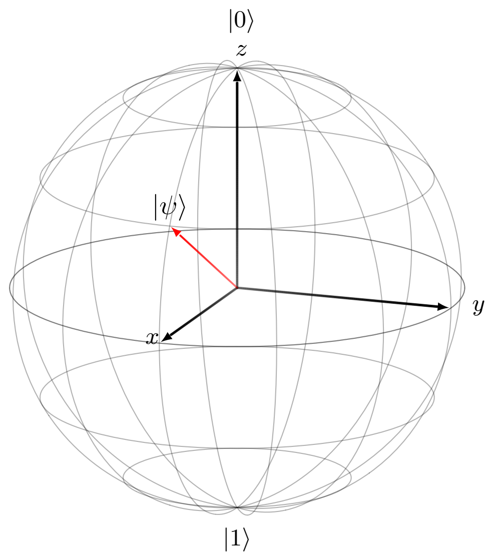
To represent a qubit graphically in its entirety, one would actually need four dimensions, since α and β are two complex numbers, each with a real and imaginary part. However, if we assume that α and β are real numbers, we can represent a qubit as follows[1]:

[1] cf. Aaronson, "Introduction to Quantum Information Science Lecture Notes", Figure 3.1



(1.1)

We enter the value of α on the x-axis and the value of β on the y-axis. As $|\alpha|^2 + |\beta|^2 = 1$, qubits always lie exactly on the dotted circle.
If we want to represent the qubit with complex amplitudes, i.e. $\alpha, \beta \in \mathbb{C}$, we can represent it three-dimensionally on the so-called *Bloch sphere*:



Through transformations (see Appendix A), we can convert the qubit formula from the previous section into the following form:

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + \sin\left(\frac{\theta}{2}\right)e^{i\phi}|1\rangle$$

where $0 \leq \theta \leq \pi$ and $0 \leq \phi \leq 2\pi$.
θ and ϕ are sufficient to completely describe a rotation on the Bloch sphere.[2] ϕ is also called the *(relative) phase* of a qubit.

[2]You can look at the following to illustrate this: https://www.st-andrews.ac.uk/physics/quvis/simulations_html5/sims/blochsphere/blochsphere.html.

1.3 Quantum Gates

Gates are used to convert the state of a qubit into a new state - as in classical computer science. The three so-called *Pauli gates* (also known as *X-, Y- and Z-gates*) and the Hadamard gate are among the most important. Mathematically, the state transition is described with a *unitary matrix*, e.g:

$$U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

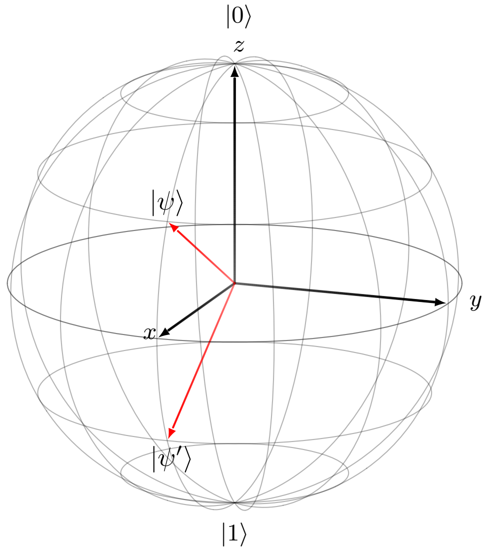
This applies to simple gates on a single qubit as well as in more complex systems with several qubits.
The application of a gate U to a qubit $|\psi\rangle$ is described with

$$|\psi\rangle — \boxed{U} — |\psi'\rangle \, .$$

To calculate the new state, the matrix corresponding to the gate is multiplied from the left by the initial state of the qubit:

$$\boxed{U|\psi\rangle = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} a \cdot \alpha + b \cdot \beta \\ c \cdot \alpha + d \cdot \beta \end{pmatrix} = \begin{pmatrix} \alpha' \\ \beta' \end{pmatrix} = |\psi'\rangle} \tag{1.2}$$

Geometrically, the application of a gate can be seen as a rotation of the state vector in the Bloch sphere.



The vectors drawn show a 180° rotation around the x-axis or a 60° rotation around the y-axis from $|\psi\rangle$ to $|\psi'\rangle$.
The matrix, and thus the effect of a gate, can be calculated using the input and output vectors:

$$U = |\psi'\rangle \langle\psi|$$

If we are searching the matrix of a gate for several input and output vectors, the corresponding matrices are added together:

$$U = \sum_i |\psi_i'\rangle \langle\psi_i|$$

1.3.1 Pauli Gates

Pauli gates describe the rotation of the state vector of a qubit by the angle π (i.e. by 180°) around the respective axis in the Bloch sphere.

1.3.1.1 X Gate

The X gate or NOT gate behaves similarly to a *NOT* gate on a classic bit. In a Bloch sphere, the X gate describes the rotation by the angle π around the x-axis. In a circuit, it is represented as follows:

$$|\psi\rangle — \boxed{X} — |\psi'\rangle$$

The representation as a unitary matrix is

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

Applied to $|0\rangle, |1\rangle$ this results in:

$$\boxed{X|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad X|1\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}} \tag{1.3}$$

In Braket notation, we write:

$$\boxed{X|0\rangle = |1\rangle \qquad X|1\rangle = |0\rangle} \tag{1.4}$$

You can also derive the matrix by correlating the inputs and outputs in Braket notation ($|out\rangle\langle in|$). Therefore we sum the matrices for all possible outputs for the base vectors:

$$\boxed{X = |0\rangle\langle 1| + |1\rangle\langle 0| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}} \tag{1.5}$$

1.3.1.2 Y Gate

In a Bloch sphere, the Y gate describes the rotation by the angle π around the y-axis.
In a circuit, it is represented as follows:

$$|\psi\rangle — \boxed{Y} — |\psi'\rangle$$

The representation as a unitary matrix is:

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

Applied to $|0\rangle, |1\rangle$ this results in:

$$\boxed{Y|0\rangle = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ i \end{pmatrix} \qquad Y|1\rangle = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -i \\ 0 \end{pmatrix}} \tag{1.6}$$

In Braket notation, we write:

$$\boxed{Y|0\rangle = i|1\rangle \qquad Y|1\rangle = -i|0\rangle} \tag{1.7}$$

1.3.1.3 Z gate

In a Bloch sphere, the Z gate describes the rotation by the angle π around the z-axis.
In a circuit, it is represented as follows:

$$|\psi\rangle \text{---} \boxed{Z} \text{---} |\psi'\rangle$$

The representation as a unitary matrix is:

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Applied to $|0\rangle, |1\rangle$ this results in

$$\boxed{Z|0\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad Z|1\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ -1 \end{pmatrix}} \tag{1.8}$$

In Braket notation, we write:

$$\boxed{Z|0\rangle = |0\rangle \qquad Z|1\rangle = -|1\rangle} \tag{1.9}$$

1.3.1.4 Characteristics of the Pauli Gates

Together with the identity matrix, the Pauli gates form a basis of the *4-dimensional complex vector space* of all complex 2×2 matrices. This means that every complex 2×2 matrix can be represented by a linear combination of these four matrices. Further, the three Pauli gates are self-inverse, i.e.

$$XX = I; YY = I; ZZ = I$$

1.3.2 Hadamard Gate

The gate, named after the French mathematician Jacques Hadamard, plays an important role in quantum computing because it can move a qubit from the "classical" state to a *superposition*. For example, an equal superposition is obtained by applying the Hadamard gate to the state $|0\rangle$. Then the amplitudes of $|0\rangle$ and $|1\rangle$ are equal; a measurement would bring the qubit into the state $|0\rangle$ or $|1\rangle$ with 50% probability. In the Bloch sphere, the gate describes a rotation by the angle π around the z-axis, followed by a rotation by the angle $\pi/2$ around the y-axis.
In a circuit, it is represented as follows:

$$|\psi\rangle \text{---} \boxed{H} \text{---} |\psi'\rangle$$

The unitary matrix is given as:

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

Applied to $|0\rangle, |1\rangle$ we get

$$H|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\cdot\begin{pmatrix}1\\0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} \qquad H|1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\cdot\begin{pmatrix}0\\1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix} \tag{1.10}$$

In Braket notation, we write:

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{1.11}$$

Summary:

Gates:	**X**	**Y**	**Z**	**Hadamard**
Rotation:	π by X	π by Y	π by Z	π by Z and $\frac{\pi}{2}$ by Y
Formula:	$X\|0\rangle = \|1\rangle$ $X\|1\rangle = \|0\rangle$	$Y\|0\rangle = i\|1\rangle$ $Y\|1\rangle = -i\|0\rangle$	$Z\|0\rangle = \|0\rangle$ $Z\|1\rangle = -\|1\rangle$	$H\|0\rangle = \frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$ $H\|1\rangle = \frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$
Circuit:	$\|\psi\rangle - \boxed{X} - \|\psi'\rangle$	$\|\psi\rangle - \boxed{Y} - \|\psi'\rangle$	$\|\psi\rangle - \boxed{Z} - \|\psi'\rangle$	$\|\psi\rangle - \boxed{H} - \|\psi'\rangle$
Matrix:	$X = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$	$Y = \begin{pmatrix}0 & -i\\ i & 0\end{pmatrix}$	$Z = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$	$H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$
Braket notation:	$X =$ $\|1\rangle\langle 0\| + \|0\rangle\langle 1\|$	$Y =$ $i\|1\rangle\langle 0\| - i\|0\rangle\langle 1\|$	$Z =$ $\|0\rangle\langle 0\| - \|1\rangle\langle 1\|$	$H =$ $1/\sqrt{2}\,(\|0\rangle + \|1\rangle)\langle 0\| +$ $1/\sqrt{2}\,(\|0\rangle - \|1\rangle)\langle 1\|$

1.3.3 Arbitrary Rotation Gates

Quantum states can also be rotated by any angle in order to "reach" all possible states. There are different sets of so-called basis gates in the literature and in the various libraries. We use the rotation gates $R_x(\theta)$, $R_y(\theta)$ and $R_z(\theta)$, which are defined as follows:

$$R_A(\theta) = e^{-i\frac{\theta}{2}A} = \cos(\theta/2)I - i\cdot\sin(\theta/2)A; \quad A \in \{X, Y, Z\}$$

This results in the rotation matrices:

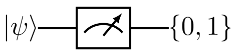
$$\begin{aligned}
R_x(\theta) &= \cos\left(\frac{\theta}{2}\right)I - i\cdot\sin\left(\frac{\theta}{2}\right)X = \begin{pmatrix}\cos\left(\frac{\theta}{2}\right) & -i\sin\left(\frac{\theta}{2}\right)\\ -i\sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right)\end{pmatrix}\\
R_y(\theta) &= \cos\left(\frac{\theta}{2}\right)I - i\cdot\sin\left(\frac{\theta}{2}\right)Y = \begin{pmatrix}\cos\left(\frac{\theta}{2}\right) & -\sin\left(\frac{\theta}{2}\right)\\ \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right)\end{pmatrix}\\
R_z(\theta) &= \cos\left(\frac{\theta}{2}\right)I - i\cdot\sin\left(\frac{\theta}{2}\right)Z = \begin{pmatrix}\cos\left(\frac{\theta}{2}\right) - i\sin\left(\frac{\theta}{2}\right) & 0\\ 0 & \cos\left(\frac{\theta}{2}\right) + i\sin\left(\frac{\theta}{2}\right)\end{pmatrix} = \begin{pmatrix}e^{-i\frac{\theta}{2}} & 0\\ 0 & e^{i\frac{\theta}{2}}\end{pmatrix}
\end{aligned} \tag{1.12}$$

1.3.4 Measurements

When measuring a qubit, the respective (binary) result $|0\rangle$ or $|1\rangle$ is obtained with the probability corresponding to the state of the qubit. This process can also be represented with a gate:

$$|\psi\rangle — \boxed{M} — \{0,1\}$$

or



There is no matrix representation – because measuring is not an operation like any other: It reads a bit of classical information from a qubit. In circuits, a connecting line is therefore sometimes drawn to a classical bit.

1.4 Multi-Qubit Systems

In order to be able to create circuits with several qubits, a state of more than one qubit must first be described. As with the representation with classical bits, the 2^n classical states should be able to be represented with n qubits. This combination is called (as in classical computer science) *register* or *quantum register*. Quantum registers can represent an infinite number of states, but when measured in a certain base, there are only exactly 2^n possible measurement results.

1.4.1 Quantum Register

The combination of two qubits into a register R is the tensor product of the state vectors, $R = |a\rangle \otimes |b\rangle = |a\rangle\,|b\rangle$:

$$\boxed{\begin{aligned} |a\rangle|b\rangle &= \begin{pmatrix}\alpha_0\\ \alpha_1\end{pmatrix} \otimes \begin{pmatrix}\beta_0\\ \beta_1\end{pmatrix} \\ &= \left(\alpha_0 \begin{pmatrix}1\\0\end{pmatrix} + \alpha_1 \begin{pmatrix}0\\1\end{pmatrix}\right) \otimes \left(\beta_0 \begin{pmatrix}1\\0\end{pmatrix} + \beta_1 \begin{pmatrix}0\\1\end{pmatrix}\right) \\ &= (\alpha_0\,|0\rangle + \alpha_1\,|1\rangle) \cdot (\beta_0\,|0\rangle + \beta_1\,|1\rangle) \\ &= \alpha_0\beta_0\,|0\rangle|0\rangle + \alpha_0\beta_1\,|0\rangle|1\rangle + \alpha_1\beta_0\,|1\rangle|0\rangle + \alpha_1\beta_1\,|1\rangle|1\rangle \end{aligned}} \tag{1.13}$$

By multiplying the probabilities α_i and β_j also applies:

$$|\alpha_0\beta_0|^2 + |\alpha_0\beta_1|^2 + |\alpha_1\beta_0|^2 + |\alpha_1\beta_1|^2 = 1$$

To simplify this notation, the amplitudes α_i and β_j are combined to a_{ij}:

$$a_{00}\,|0\rangle|0\rangle + a_{01}\,|0\rangle|1\rangle + a_{10}\,|1\rangle|0\rangle + a_{11}\,|1\rangle|1\rangle$$

In addition, two qubits $|x_0\rangle\,, |x_1\rangle$ can be combined in the Braket notation to $|x_0x_1\rangle$ for further simplification:

$$a_{00}\,|00\rangle + a_{01}\,|01\rangle + a_{10}\,|10\rangle + a_{11}\,|11\rangle$$

If a quantum register is measured, the state $|ij\rangle$ is obtained with probability $|a_{ij}|^2$.
For the formal definition of registers with n qubits, it makes sense to switch from binary to decimal notation:

$$a_0\,|0\rangle + a_1\,|1\rangle + a_2\,|2\rangle + a_3\,|3\rangle$$

Definition 1 *A quantum register with n qubits $R = |x_{n-1}\rangle \dots |x_1\rangle |x_0\rangle = |x_{n-1} \dots x_1 x_0\rangle$ can have 2^n states of the form*

$$\sum_{i=0}^{2^n-1} a_i |i\rangle$$

It holds that:

$$\sum_{i=0}^{2^n-1} |a_i|^2 = 1$$

The measurement of a quantum register therefore results in the state $|i\rangle$ with probability $|a_i|^2$.

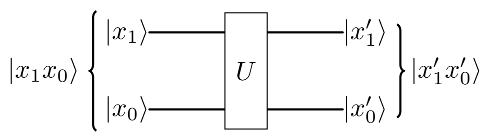
For clarity, the binary representation is preferred in the following, so the basic states of a 2-qubit register are:

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \quad |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

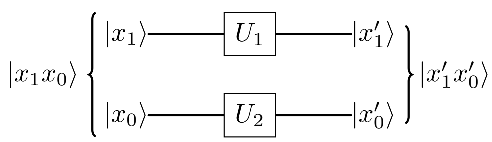
You can see that in the vector representation there is always exactly one 1 at the position (starting from 0) that corresponds to the binary number.

1.4.2 Simple Multi-Qubit Gates

To transfer a quantum register to a new state, gates can be applied to several qubits. In the following circuit, the state $|x_1 x_0\rangle$[3] gets transformed to $|x_1' x_0'\rangle$ using the multi-qubit operation U:



U can be, for instance, a combination of the single qubit gates already presented:



The tensor product of the two 1-qubit matrices then results in the 2-qubit gate, i.e:

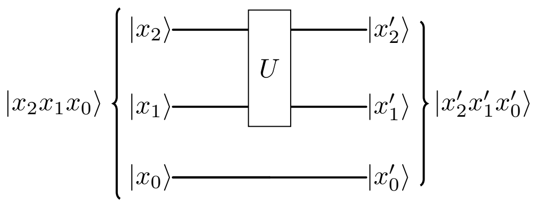
[3] In this lecture, we use this qubit sequence. Please note, however, that the reverse order can also be used, e.g. with IBMQ.

$$U = U_1 \otimes U_2 = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \otimes \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1U_2 & b_1U_2 \\ c_1U_2 & d_1U_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 & a_1b_2 & b_1a_2 & b_1b_2 \\ a_1c_2 & a_1d_2 & b_1c_2 & b_1d_2 \\ c_1a_2 & c_1b_2 & d_1a_2 & d_1b_2 \\ c_1c_2 & c_1d_2 & d_1c_2 & d_1d_2 \end{pmatrix} \tag{1.14}$$

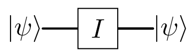
For example, for the X gate, this results in

$$X \otimes X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \tag{1.15}$$

It is also possible to apply multi-qubit gates only to parts of a register. This is illustrated as follows:



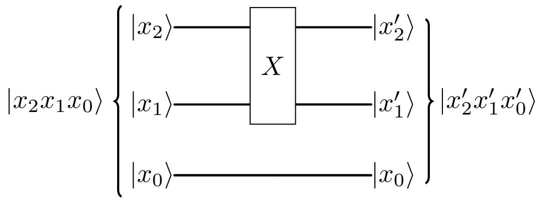
No operation is performed on qubit $|x_0\rangle$, this corresponds to multiplication by the identity matrix I. The identity matrix can also be represented as a gate:



The result of the tensor product is:

$$U_1 \otimes U_2 \otimes I = \begin{pmatrix} a_1a_2 & 0 & a_1b_2 & 0 & b_1a_2 & 0 & b_1b_2 & 0 \\ 0 & a_1a_2 & 0 & a_1b_2 & 0 & b_1a_2 & 0 & b_1b_2 \\ a_1c_2 & 0 & a_1d_2 & 0 & b_1c_2 & 0 & b_1d_2 & 0 \\ 0 & a_1c_2 & 0 & a_1d_2 & 0 & b_1c_2 & 0 & b_1d_2 \\ c_1a_2 & 0 & c_1b_2 & 0 & d_1a_2 & 0 & d_1b_2 & 0 \\ 0 & c_1a_2 & 0 & c_1b_2 & 0 & d_1a_2 & 0 & d_1b_2 \\ c_1c_2 & 0 & c_1d_2 & 0 & d_1c_2 & 0 & d_1d_2 & 0 \\ 0 & c_1c_2 & 0 & c_1d_2 & 0 & d_1c_2 & 0 & d_1d_2 \end{pmatrix}$$

Using the example of the X gate, this is as follows:



And the corresponding matrix is calculated in the same way:

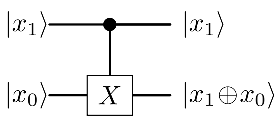
$$X \otimes X \otimes I = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \tag{1.16}$$

If this matrix is applied to a state vector, the desired result is obtained:

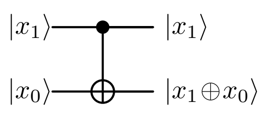
$$(X \otimes X \otimes I)\,|100\rangle = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = |010\rangle \tag{1.17}$$

1.4.3 Controlled Multi-Qubit Gates

There are special multi-qubit gates that require several qubits as input and cannot be represented as a tensor product of individual gates. This means that the state of one qubit can influence the state of another. An example of this is the *Controlled-NOT-* gate, or short *CNOT* gate:



also noted as:



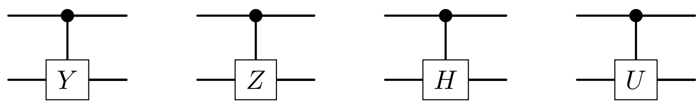
The so-called *control* $|x_1\rangle$ controls the application of the X gate to the *target* $|x_0\rangle$. If the control qubit is $|1\rangle$, the NOT gate is applied to the target qubit. If the control qubit is $|0\rangle$, the target qubit remains unchanged. The state of the control qubit remains unchanged in both cases. The matrix on which the gate is based is :

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

If this matrix is applied to a state vector, the desired result is obtained:

$$\boxed{CNOT\,|11\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = |10\rangle} \tag{1.18}$$

The principle of controlling gates is not limited to the NOT gate, it can be combined with all other gates, e.g:



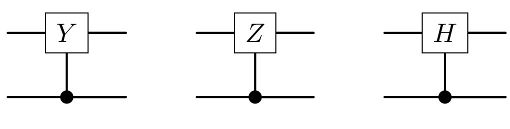
In general, the matrix of a controlled gate U is a state $|x_1 x_0\rangle$ with x_1 as the control qubit and x_0 as the target qubit:

$$\boxed{\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \multicolumn{2}{c}{\multirow{2}{*}{U}} \\ 0 & 0 & & \end{pmatrix}} \tag{1.19}$$

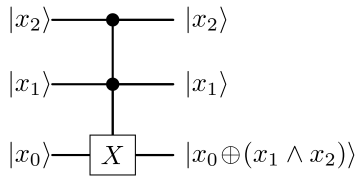
More general in Braket notation a controlled gate U is defined as:

$$\boxed{CU = \underbrace{|0\rangle\langle 0|}_{\text{control}} \otimes \underbrace{I}_{\text{target}} + \underbrace{|1\rangle\langle 1|}_{\text{control}} \otimes \underbrace{U}_{\text{target}}} \tag{1.20}$$

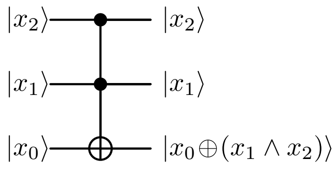
The "direction" of the controlling qubit is not predefined. The following gates are also possible:



The principle of the controlled gate is not limited to two qubits, but can also be used with several qubits, e.g. in the form of the so-called *Controlled CNOT* or *CCNOT* gate, which is also known as the *Toffoli gate* after its inventor.



or:



The NOT gate is only applied to the target qubit if both control qubits are $|1\rangle$. As with the CNOT, the state of the two control qubits remains unchanged.
In general, we can define multi-controlled gates like

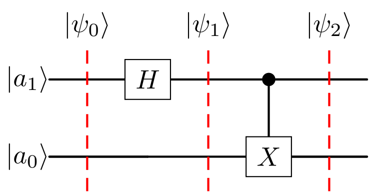
$$\boxed{CCU = \underbrace{|0\rangle\langle 0|}_{\text{control}} \otimes \underbrace{|0\rangle\langle 0|}_{\text{control}} \otimes \underbrace{I}_{\text{target}} + \underbrace{|1\rangle\langle 1|}_{\text{control}} \otimes \underbrace{|1\rangle\langle 1|}_{\text{control}} \otimes \underbrace{U}_{\text{target}}} \tag{1.21}$$

For the CCNOT gate we get the matrix

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

1.5 Entanglement

Another circuit that looks very simple at first glance is the entanglement of two qubits.



If you set $|a_1 a_0\rangle = |00\rangle$, the states in the intermediate steps $|\psi_i\rangle$ are as follows:

$$\boxed{\begin{aligned} |\psi_0\rangle &= |00\rangle \\ |\psi_1\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \\ |\psi_2\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \end{aligned}} \tag{1.22}$$

At the time $|\psi_2\rangle$, the value of both qubits is still completely open and equally probable with 50% each. The state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ also shows that the measurement results of both qubits will be the same in any case. So if you measure $|a_0\rangle$ with $|1\rangle$, the result of a measurement of $|a_1\rangle$ (namely $|1\rangle$) is also fixed. This means that even if you were to separate the two qubits spatially and then measure them independently of each other, you would always get the same result.
This state is named after the Irish physicist John Bell; there are a total of four such states depending on the input register $|a_1 a_0\rangle$:

$$\begin{aligned}
|a_1a_0\rangle = |00\rangle \Rightarrow |\beta_{00}\rangle = \mathbf{\Phi}^+ &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
|a_1a_0\rangle = |10\rangle \Rightarrow |\beta_{10}\rangle = \mathbf{\Phi}^- &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\
|a_1a_0\rangle = |01\rangle \Rightarrow |\beta_{01}\rangle = \mathbf{\Psi}^+ &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\
|a_1a_0\rangle = |11\rangle \Rightarrow |\beta_{11}\rangle = \mathbf{\Psi}^- &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)
\end{aligned} \tag{1.23}$$

The four states differ mainly in that the same result is measured for Φ^+ and Φ^- on both qubits, whereas Ψ^+ and Ψ^- produce opposite measurement results. The two states with positive amplitude Φ^+ and Ψ^+ are also described as *EPR pair*, named after a publication by Einstein, Podolski and Rosen[4].
The Bell states can of course also be calculated using the matrix representation, because $\Phi^+ = CNOT \cdot (H \otimes I)\,|00\rangle$:

$$\begin{aligned}
H \oplus I &= \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix} \\
CNOT \cdot (H \otimes I) &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \cdot \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{pmatrix} \\
|\Phi^+\rangle &= \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}
\end{aligned} \tag{1.24}$$

[4] Einstein, Podolsky, and Rosen, "Can quantum-mechanical description of physical reality be considered complete?"

You can see from this final state that it cannot be a tensor product of individual qubits. This is precisely how entanglement is defined[5]:

Definition 2 (Entanglement) *Let $|\phi\rangle$ be the state of a quantum register of n bits. The state $|\phi\rangle$ is called unentangled if it is the product of the states of the individual bits:*

$$|\phi\rangle = |\phi_{n-1}\rangle \otimes |\phi_{n-2}\rangle \otimes .. \otimes |\phi_0\rangle$$

If there is no such decomposition, the state is called entangled.

A unitary transformation is required for entanglement, which itself cannot be represented as a tensor product on individual qubits. Alongside superposition, entanglement is one of the most powerful tools for quantum computing. These states are extremely difficult to produce and therefore expensive. This is particularly true if they are to be produced over long distances.

1.6 Measuring Qubits

1.6.1 Why Measurement is Important for Qubits

You can only find out something about a qubit in an unknown state by measuring it. During a measurement, the qubit collapses into exactly one of two values. The original state can no longer be reconstructed and you only learn a small part of what there is to know about the state. If $|\phi_0\rangle = \alpha|0\rangle + \beta|1\rangle$ is therefore an unknown state and the measurement result is $|0\rangle$, the only thing that can be said with certainty about $|\phi_0\rangle$ is that $\alpha \neq 0$ must have applied. Further information about $|\phi_0\rangle$ can no longer be obtained, because the qubit has irreversibly lost its state as a result of the measurement and has changed to an unknown subsequent state $|\phi_1\rangle$.

1.6.2 Measurement of Individual Bits in a Register

We have already seen that you can also measure individual bits in a register, as this also has an effect on the measurement result for the other qubits.
How does the state of a register change by measuring a single bit? We know that a register consisting of two qubits $|x\rangle$ and $|y\rangle$ is in the state

$$\boxed{|xy\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle \alpha_{11}|11\rangle} \tag{1.25}$$

for any $\alpha_{00}, \alpha_{01}, \alpha_{10}$ and α_{11}. The probability of measuring $|x\rangle = |0\rangle$ is

$$\boxed{p(|x\rangle = |0\rangle) = |\alpha_{00}|^2 + |\alpha_{01}|^2} \tag{1.26}$$

If we now measure $|x\rangle = |0\rangle$, the register goes into the state

$$\boxed{|0y\rangle = \beta_{00}|00\rangle + \beta_{01}|01\rangle} \tag{1.27}$$

The following applies:

[5] cf. Aaronson, "Introduction to Quantum Information Science Lecture Notes", p.40

$$\boxed{\beta_{0i} = \frac{\alpha_{0i}}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}} \tag{1.28}$$

This means: The amplitudes of $|00\rangle$ and $|01\rangle$ are retained proportionally, but they are normalized so that the measurement probabilities add up to 1 again.

1.6.3 The Result of a Measurement

During a measurement, the qubit collapses into a certain base state, which is obtained as the measurement result. This therefore means:

1. When a qubit is measured, one bit of classical information is obtained.
2. The qubit assumes a subsequent state, which can be a superposition with respect to a base.
3. If you knew the original state, the measurement tells you which subsequent state the qubit is in. This can be used for further calculations.

1.7 No Cloning Theorem

Although it is sometimes possible to copy the state of a qubit to a given qubit, there is no permitted operation that allows this process for any state.
Let a qubit $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ and a target bit $|\sigma\rangle$ in state $|0\rangle$ be given. The register is therefore in the state

$$(\alpha|0\rangle + \beta|1\rangle)|0\rangle$$

and we want to create the state

$$(\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle)$$

with a unitary transformation. For classical states, this works with a CNOT circuit, even reversible: CNOT: $|x\rangle|y\rangle \mapsto |x\rangle|y \oplus x\rangle$ maps $|00\rangle$ to $|00\rangle$ and $|10\rangle$ to $|11\rangle$. However, CNOT does not help in the state described above. From

$$(\alpha|0\rangle + \beta|1\rangle)|0\rangle = \alpha|00\rangle + \beta|10\rangle$$

the application of CNOT yields:

$$\boxed{\alpha|00\rangle + \beta|11\rangle} \tag{1.29}$$

but the desired state would be

$$\boxed{(\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle) = \alpha^2|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta^2|11\rangle} \tag{1.30}$$

This is only true for $\alpha = 0 \vee \beta = 0$. The fact that copying is not possible in general can be seen as follows: Let a target bit $|\sigma\rangle$ be given. If it were possible to copy both state $|\phi\rangle$ and state $|\psi\rangle$ to $|\sigma\rangle$, there would have to be a unitary transformation U so that

$$\forall \quad |x\rangle : U\big(|x\rangle \otimes |\sigma\rangle\big) = |x\rangle \otimes |x\rangle$$

Then the following applies for $|\phi\rangle, |\psi\rangle$:

$$U(|\phi\rangle \otimes |\sigma\rangle) = |\phi\rangle \otimes |\phi\rangle$$

and

$$U(|\psi\rangle \otimes |\sigma\rangle) = |\psi\rangle \otimes |\psi\rangle$$

The following applies to all unitary transformations U and all vectors v, w:

$$\langle Uv|Uw\rangle = \langle v|w\rangle$$

So it must also apply:

$$\boxed{\langle U(|\phi\rangle \otimes |\sigma\rangle)|U(|\psi\rangle \otimes |\sigma\rangle)\rangle = \langle \phi \otimes \sigma|\psi \otimes \sigma\rangle} \tag{1.31}$$

and thus

$$\boxed{\langle \phi \otimes \phi|\psi \otimes \psi\rangle = \langle \phi \otimes \sigma|\psi \otimes \sigma\rangle} \tag{1.32}$$

Because the scalar product of tensors is equal to the product of the individual scalar products, it can be pulled apart:

$$\boxed{\langle \phi|\psi\rangle \langle \phi|\psi\rangle = \langle \phi|\psi\rangle \langle \sigma|\sigma\rangle} \tag{1.33}$$

Since $\langle \sigma|\sigma\rangle = 1$ applies to all qubits, it follows that

$$\boxed{\langle \phi|\psi\rangle^2 = \langle \phi|\psi\rangle} \tag{1.34}$$

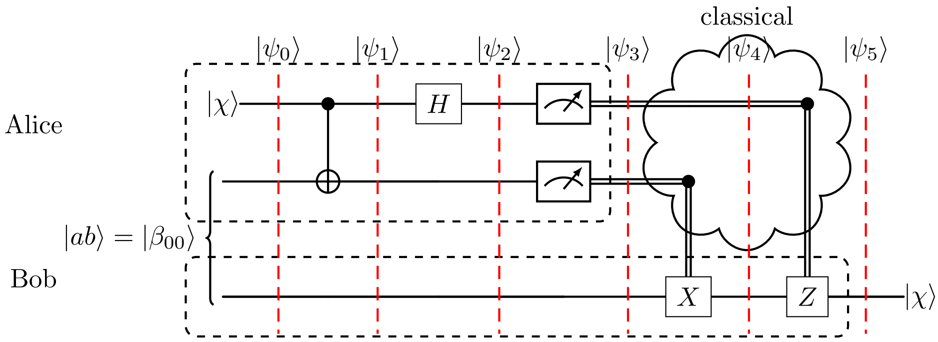
The equation $a^2 = a$ is only valid for $a = 1$ and $a = 0$. $|\phi\rangle$ and $|\psi\rangle$ must therefore be identical or orthogonal and the combination of $|\sigma\rangle$ and U can therefore only be used to copy certain states, but not arbitrary states.

Chapter 2

Applying Entanglement

2.1 Teleportation

Similar to classical computer science, qubits should also be able to be exchanged between several parties. The difficulty lies in transferring the qubit without losing the superposition, while at the same time observing the *No Cloning Theorem*. A qubit can be *teleported* from Alice to Bob if two qubits $|a\rangle$ and $|b\rangle$ were previously entangled and one of them was transported to Alice and Bob respectively. The circuit then looks like this:



The qubits of Alice $|a\rangle$ and Bob $|b\rangle$ are entangled in the Bell state $|\beta_{00}\rangle$. Proof of successful teleportation is shown by using $|\chi\rangle = \chi_0 |0\rangle + \chi_1 |1\rangle$:

$$\begin{aligned}
|\psi_0\rangle = |\chi\rangle |\beta_{00}\rangle &= (\chi_0 |0\rangle + \chi_1 |1\rangle) \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \\
&= \frac{1}{\sqrt{2}} (\chi_0 |000\rangle + \chi_0 |011\rangle + \chi_1 |100\rangle + \chi_1 |111\rangle) \\
&\left(= \frac{\chi_0}{\sqrt{2}} (|000\rangle + |011\rangle) + \frac{\chi_1}{\sqrt{2}} (|100\rangle + |111\rangle)\right)
\end{aligned} \tag{2.1}$$

Now use $|\chi\rangle$ as the control bit to apply CNOT to $|a\rangle$:

$$
\begin{aligned}
CNOT\,|\psi_0\rangle = |\psi_1\rangle = \frac{1}{\sqrt{2}}(\chi_0\,|000\rangle + \chi_0\,|011\rangle + \chi_1\,|110\rangle + \chi_1\,|101\rangle) = \\
\left(= \frac{\chi_0}{\sqrt{2}}(|000\rangle + |011\rangle) + \frac{\chi_1}{\sqrt{2}}(|110\rangle + |101\rangle)\right)
\end{aligned}
\tag{2.2}
$$

Then a Hadamard transformation is applied to $|\chi\rangle$.

$$
\begin{aligned}
|\psi_2\rangle &= (H \otimes I \otimes I)\,|\psi_1\rangle \\
&= \left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right)\frac{\chi_0}{\sqrt{2}}(|00\rangle + |11\rangle) + \left(\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right)\frac{\chi_1}{\sqrt{2}}(|10\rangle + |01\rangle) \\
&= \frac{\chi_0}{2}(|000\rangle + |011\rangle + |100\rangle + |111\rangle) + \frac{\chi_1}{2}(|010\rangle + |001\rangle - |110\rangle - |101\rangle)
\end{aligned}
\tag{2.3}
$$

A transformation makes it easier to read off the result of the measurements:

$$
\begin{aligned}
|\psi_2\rangle = \frac{1}{2}(|00\rangle\,(\chi_0\,|0\rangle + \chi_1\,|1\rangle) + |01\rangle\,(\chi_0\,|1\rangle + \chi_1\,|0\rangle) \\
+ |10\rangle\,(\chi_0\,|0\rangle - \chi_1\,|1\rangle) + |11\rangle\,(\chi_0\,|1\rangle - \chi_1\,|0\rangle))
\end{aligned}
\tag{2.4}
$$

The state of $|\chi\rangle$ is lost as a result of the measurement. The result of the measurement is transmitted from Alice to Bob via a classical channel (classical transmissions are marked as a double bar in the circuit model). Depending on the measurement, the X and/or the Z gate are applied to $|b\rangle$:

(2.5)

Measurement	$\|b\rangle$ at time step $\|\psi_3\rangle$	Operation	Result $\|\psi_5\rangle$ ($\|b\rangle$)
$\|00\rangle$	$\chi_0\,\|0\rangle + \chi_1\,\|1\rangle$	(none)	$\chi_0\,\|0\rangle + \chi_1\,\|1\rangle$
$\|01\rangle$	$\chi_0\,\|1\rangle + \chi_1\,\|0\rangle$	X	$\chi_0\,\|0\rangle + \chi_1\,\|1\rangle$
$\|10\rangle$	$\chi_0\,\|0\rangle - \chi_1\,\|1\rangle$	Z	$\chi_0\,\|0\rangle + \chi_1\,\|1\rangle$
$\|11\rangle$	$\chi_0\,\|1\rangle - \chi_1\,\|0\rangle$	$Z \cdot X$	$\chi_0\,\|0\rangle + \chi_1\,\|1\rangle$

Independent of the measurement, $|b\rangle$ is in the same state as χ was in before the teleportation ($\chi_1\,|0\rangle + \chi_2\,|1\rangle$). The no-cloning theorem is not violated because the state of $|\chi\rangle$ is lost as a result of the measurement.

Appendix

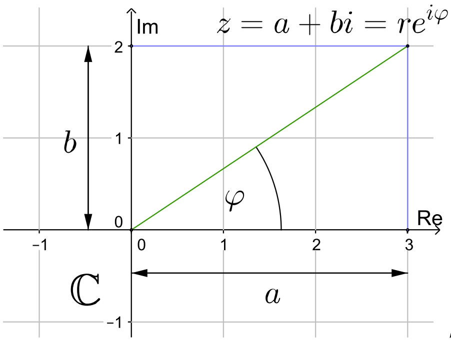
Appendix A

Representation of Qubits on the Bloch Sphere

A qubit has two amplitudes α and β, where $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$. For the 2-dimensional representation of a complex number, we can also use the polar coordinate form $r\dot{e}^{i\phi}$ instead of the Cartesian coordinate form $a + bi$. r and ϕ are calculated as follows from the Cartesian coordinates a, b:

$$r = \sqrt{a^2 + b^2} \tag{A.1}$$

$$\phi = \arctan_2(a, b) \tag{A.2}$$



Source: Wikipedia

This means that we can also define a qubit as

$$|\psi\rangle = r_0 e^{i\phi_0} |0\rangle + r_1 e^{i\phi_1} |1\rangle \, . \tag{A.3}$$

If we now factor out $e^{i\phi_0}$ we get

$$|\psi\rangle = e^{i\phi_0} \left(r_0 |0\rangle + r_1 e^{i(\phi_1 - \phi_0)} |1\rangle \right) . \tag{A.4}$$

As will be shown later in the lecture, $e^{i\phi_0}$ corresponds to a *global phase* whose value has no effect on the measurement result and can therefore be ignored.
If we define $\phi = (\phi_1 - \phi_0)$, we can now describe the qubit with three real variables r_1, r_2, ϕ:

$$|\psi\rangle = r_0 |0\rangle + r_1 e^{i\phi} |1\rangle \tag{A.5}$$

Now we can make a further simplification:
Since $|\alpha|^2 + |\beta|^2 = 1$, $|r_0|^2 + |r_1 e^{i\phi}|^2 = 1$, or $r_0^2 + r_1^2 |e^{i\phi}|^2 = 1$ must also hold. Euler's formula

can be used to show that $|e^{i\phi}|^2 = 1$; this means that $r_0^2 + r_1^2 = 1$. This is the equation for the unit circle and since $cos^2(x) + sin^2(x) = 1$, we can set $r_0 = cos(x)$ and $r_1 = sin(x)$:

$$|\psi\rangle = cos(x)\,|0\rangle + sin(x)e^{i\phi}\,|1\rangle \tag{A.6}$$

We choose $x = \frac{\theta}{2}$ so that the possible angles of rotation θ, ϕ exactly represent the surface of a sphere.

$$|\psi\rangle = cos(\frac{\theta}{2})\,|0\rangle + sin(\frac{\theta}{2})e^{i\phi}\,|1\rangle \tag{A.7}$$

A vector in the Bloch sphere can now be described as:

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} cos(\phi)sin(\theta) \\ sin(\phi)sin(\theta) \\ cos(\theta) \end{pmatrix} \tag{A.8}$$

Bibliography

Aaronson, Scott. "Introduction to Quantum Information Science Lecture Notes". In: (2018). URL: https://www.scottaaronson.com/qclec.pdf.

DiVincenzo, David P. "Topics in quantum computers". In: *Mesoscopic electron transport*. Springer, 1997, pp. 657–677.

Einstein, Albert, Boris Podolsky, and Nathan Rosen. "Can quantum-mechanical description of physical reality be considered complete?" In: *Physical review* 47.10 (1935). https://journals.aps.org/pr/pdf/10.1103/PhysRev.47.777, p. 777.

Newman, Alantha. "Max Cut". In: *Encyclopedia of Algorithms*. Ed. by Kao, Ming-Yang. Boston, MA: Springer US, 2008, pp. 489–492. ISBN: 978-0-387-30162-4. DOI: {10.1007/978-0-387-30162-4_219}. URL: https://doi.org/10.1007/978-0-387-30162-4_219.

Nielsen, Michael A. and Isaac L. Chuang. *Quantum Computation and Quantum Information*. 2010.