A Very Very Very Very^k Short Introduction to Quantum Mechanics for Quantum Computing choose arbitrary $k \in \mathbb{N}$ adapted to your knowledge

Benjamin Maier*

June 10, 2012

1 Introduction on the Introduction

In order to understand the computational model of quantum computing, it is recommended to get a first intuition in quantum mechanics (QM), respectively quantum many-body systems. However, QM is a wide field, therefore one can easily get lost in the vast descriptions of the phenomena, without aiming to the essentials for the model of computation. To see the beauty of quantum parallel computing, it is rather important to understand the physical meaning and mathematical description of so-called “qubits” than the basic calculations with “wave-like” particles or “particle-like” waves.

Thus, I will not start this introduction with the Schrödinger equation like other authors, but rather try to create a physical intuition of quantum systems by means of linear algebra.

To this end, I start with introducing quantum states as vectors and operators as matrices in Sec. 2. Afterwards, in Sec. 3, I start to introduce qubits and give a first motivation for quantum computing. While reading, you will notice that I also present two exercises. Of course nothing is mandatory, however, I think that solving the exercises will help you to obtain an intuition for the calculations. Furthermore I will perform similar things in my talk on Tuesday. The solutions are attached in Sec. 4.

2 Quantum States and Linear Algebra

2.1 States and Vectors

Consider the following system: a particle is caught in a one-dimensional box (say, a line), s.t. it can move inside the box, but cannot get out. The dimensions are such, that QM has to be used to describe the situation properly. The laws of QM tell us that the particle’s states are discrete, that means, it cannot have an arbitrary energy, but is restricted to certain states of energy. These states are vectors in a so-called “Hilbert space” and are enumerated.

On the lowest level of energy, the state is called $|0\rangle$. The state of the next greater energy is called $|1\rangle$ and so forth (we will see soon enough, why we are using the strange notation $|\cdot\rangle$, which is the “ket” part of the so-called “bra-ket notation”). In case of the particle in a box, one can see eventually that there are infinitely (but countable) many states. Thus, the Hilbert space is infinite-dimensional. As I already said, the states can be represented as vectors in the Hilbert space. Note that they have to be orthonormal. One representation

*e-mail: `bfmaier@physik.hu-berlin.de`

could then be

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ \vdots \end{pmatrix}, \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ \vdots \end{pmatrix}, \qquad |2\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ \vdots \end{pmatrix}, \qquad \dots \tag{1}$$

Note, that the vectors can be complex (e.g. replace the 1's with $e^{i\phi}$, where $i^2 = -1$ and ϕ is an arbitrary real number) and be scaled with complex scalars). To build scalar products as well as matrices, we need a dual space, where the "bra"-vectors are located. We denote these vectors with the notation $\langle \cdot |$, e.g. $\langle 2|$ and gain them by the hermitian conjugation $\langle n| = (|n\rangle)^\dagger$. This operation produces the complex conjugate transposition of the input and can be used for an arbitrary matrix. As an example, take the matrix A with complex entries

$$A = \begin{pmatrix} a & 0 & e^{-ib} \\ 0 & 1 & c \end{pmatrix}, \tag{2}$$

then the hermitian conjugation would yield

$$A^\dagger = \begin{pmatrix} a^* & 0 \\ 0 & 1 \\ e^{ib} & c^* \end{pmatrix}. \tag{3}$$

As you can see, the operation is its own inverse.

Correspondingly to the bra-notation in QM, in Linear Algebra we would write

$$\langle 0| = (1, 0, 0, \dots), \qquad \langle 1| = (0, 1, 0, \dots), \qquad \dots \tag{4}$$

Now, we can build scalar products

$$\langle 0|0\rangle = 1, \qquad \langle 0|1\rangle = 0, \qquad \langle 1|2\rangle = 0, \qquad \dots, \tag{5}$$

which is equivalent to

$$\langle 0|0\rangle = (1, 0, \dots) \cdot \begin{pmatrix} 1 \\ 0 \\ \vdots \end{pmatrix} = 1 \cdot 1 + 0 \cdot 0 + \dots = 1. \tag{6}$$

Since the states are orthonormal base vectors, they fulfill the condition $\langle m|n\rangle = \delta_{mn}$ with the Kronecker-delta

$$\delta_{mn} = \begin{cases} 1, & m = n \\ 0, & m \neq n \end{cases}, \qquad m, n \in \mathbf{N}. \tag{7}$$

Exercise 1

From a special orthonormal base, take the vector

$$|0\rangle = \begin{pmatrix} e^{ia} \\ 0 \\ 0 \\ \vdots \end{pmatrix}. \tag{8}$$

Build the corresponding vector in the dual space, $\langle 0|$. Build the scalar product $\langle 0|0\rangle$.

What else can we do with vectors? We can, for example, build linear combinations! To do this, let us first specify how states are scaled with scalars. As an example, take the state $|\phi\rangle = \alpha|0\rangle$. The dual vector is $(|\phi\rangle)^\dagger = \alpha^*\langle 0|$. Now, building a linear combination means we can prepare a state for our particle (let's stay with the example above), which is a superposition of some of the states. Let's call our state $|\psi\rangle$ and prepare it as follows

$$|\psi\rangle = \alpha|0\rangle + \beta|3\rangle + \gamma|8\rangle, \tag{9}$$

where α,β and γ are complex numbers and are called the "probability amplitudes". Why are they attached with such a strange name? To answer this question, we have to know about the probabilistic nature of QM.

As you may have heard, measurements with respect to QM are often random processes (supposed we measure superpositions of states), which means that we cannot always predict the outcome of the measurements but only make assumptions based on probabilities.

Suppose, we measure a system in the quantum state $|\psi\rangle$. Then, the probability $P_\psi(0)$ that the outcome is state $|0\rangle$ is $|\alpha|^2 = \alpha\alpha^*$, where α^* is the complex conjugate of α. The probability for $|3\rangle$ is $|\beta|^2$ and the probability for $|8\rangle$ is $|\gamma|^2$. All the probabilities for other states are 0. In other words, we can connect the scalar product of states to the probability amplitudes and probabilities of the measurement outcomes

$$\begin{aligned}
\langle 0|\psi\rangle &= \alpha \underbrace{\langle 0|0\rangle}_{=1} + \beta \underbrace{\langle 0|3\rangle}_{=0} + \gamma \underbrace{\langle 0|8\rangle}_{=0} = \alpha & P_\psi(0) &= |\langle 0|\psi\rangle|^2 = |\alpha|^2, \\
\langle 3|\psi\rangle &= \beta, & P_\psi(3) &= |\langle 3|\psi\rangle|^2 = |\beta|^2, \\
\langle 8|\psi\rangle &= \gamma, & P_\psi(8) &= |\langle 8|\psi\rangle|^2 = |\gamma|^2, \\
& & P_\psi\big(x \in \mathbf{N}\backslash\{0,3,8\}\big) &= 0.
\end{aligned}$$

Since the probability that we measure any of the states has to be normed to 1, we find

$$\begin{aligned}
\langle\psi|\psi\rangle = \quad & \alpha^*\alpha\,\langle 0|0\rangle + \alpha^*\beta\,\langle 0|3\rangle + \alpha^*\gamma\,\langle 0|8\rangle + & (10)\\
& + \beta^*\alpha\,\langle 3|0\rangle + \beta^*\beta\,\langle 3|3\rangle + \beta^*\gamma\,\langle 3|8\rangle + & (11)\\
& + \gamma^*\alpha\,\langle 8|0\rangle + \gamma^*\beta\,\langle 8|3\rangle + \gamma^*\gamma\,\langle 8|8\rangle & (12)\\
& = |\alpha|^2 + |\beta|^2 + |\gamma|^2 & (13)\\
& \overset{!}{=} 1 & (14)\\
& = |\langle\psi|\psi\rangle|^2 . & (15)
\end{aligned}$$

In general, we can state that for two quantum states $|\phi\rangle$ and $|\psi\rangle$, the probability that $|\psi\rangle$ "collapses to" $|\phi\rangle$ is $|\langle\phi|\psi\rangle|^2$, meaning that when measuring $|\psi\rangle$ with a system that $|\phi\rangle$ is part of, $|\langle\phi|\psi\rangle|^2$ is the probability we obtain $|\phi\rangle$ as a result.

Exercise 2

For a quantum system take the states

$$|\varphi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle \tag{16}$$

$$|\theta\rangle = \beta|0\rangle - \frac{e^{ia}}{\sqrt{2}}|1\rangle, \tag{17}$$

with $\alpha_0, \alpha_1, \beta \in \mathbf{C}$, $a \in \mathbf{R}$ and $|\alpha_0|^2 + |\alpha_1|^2 = 1$.

a) What is the probability to measure $|\varphi\rangle$ to be $|0\rangle$?

b) What is the probability to measure $|\theta\rangle$ to be $|1\rangle$?

c) Calculate $|\beta|^2$.

d) Build $\langle\theta|$.

e) What is the probability to find $|\varphi\rangle$ to be in the state $|\theta\rangle$ (i.e. to measure the state $|\theta\rangle$)?

2.2 Operators and Matrices

Now, it is time to lose a word or two on operators. Operators are called like this, because they act on states and modify them. In QM, all operators are of linear kind. The easiest operators are, for example, the zero operator $\mathbf{0}$ and the identity $\mathbf{1}$. Acting on an arbitrary state $|\phi\rangle$, we obtain

$$\mathbf{0} \cdot |\phi\rangle = 0, \qquad \mathbf{1} \cdot |\phi\rangle = |\phi\rangle. \tag{18}$$

As we can see, the zero operator "kills" the state, s.t. no operation is possible anymore afterwards, while the identity just gives the same state. Maybe you already noticed - since operators are acting on states, correspondingly in Linear Algebra they are acting on vectors. Now the question is, linear objects, acting on vectors, producing outcome in the same vector space, what kind of objects can that be? Of course, the answer is "matrices" (well, we could say that scalars do that, too, but scalars are just special cases of matrices). In the case of the former defined operators, the matrix representations would be

$$\mathbf{1} = \begin{pmatrix} 1 & 0 & \dots \\ 0 & 1 & \\ \vdots & & \ddots \end{pmatrix}, \qquad \mathbf{0} = \begin{pmatrix} 0 & 0 & \dots \\ 0 & 0 & \\ \vdots & & \ddots \end{pmatrix}. \tag{19}$$

Note that for the zero operator you mostly will read the scalar 0.

Now, how can we build matrices from the "bra-ket"-notation? The answer is, kind of the same like in Linear Algebra, as in the following:

$$|0\rangle\langle 0| = \begin{pmatrix} 1 \\ 0 \\ \vdots \end{pmatrix} \times (1, 0, \dots) = \begin{pmatrix} 1 & 0 & \dots \\ 0 & 0 & \\ \vdots & & \ddots \end{pmatrix}, \qquad |0\rangle\langle 1| = \begin{pmatrix} 1 \\ 0 \\ \vdots \end{pmatrix} \times (0, 1, \dots) = \begin{pmatrix} 0 & 1 & \dots \\ 0 & 0 & \\ \vdots & & \ddots \end{pmatrix}, \tag{20}$$

$$|1\rangle\langle 2| = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \end{pmatrix} \times (0, 0, 1 \dots) = \begin{pmatrix} 0 & 0 & 0 & \dots \\ 0 & 0 & 1 & \\ 0 & 0 & 0 & \\ \vdots & & & \ddots \end{pmatrix}. \tag{21}$$

And of course, we are able to build linear combinations to create operators. Let me introduce a few operators

$$P_0 = |0\rangle\langle 0|, \qquad \text{(Projection to state } |0\rangle) \tag{22}$$
$$P_1 = |1\rangle\langle 1|, \qquad \text{(Projection to state } |1\rangle) \tag{23}$$
$$P_n = |n\rangle\langle n|, \qquad \text{(Projection to state } |n\rangle) \tag{24}$$
$$N_{01} = |0\rangle\langle 1| + |1\rangle\langle 0|, \qquad \text{(exchange } |0\rangle \text{ with } |1\rangle \text{ and vice versa, kill all other states).} \tag{25}$$

How are these operators acting? Take the state $|\psi\rangle$ of the last section and the following examples

$$P_0|\psi\rangle = |0\rangle\langle 0| \Big(\alpha|0\rangle + \beta|3\rangle + \gamma|8\rangle\Big) \tag{26}$$
$$= \alpha|0\rangle \underbrace{\langle 0|0\rangle}_{=1} + \beta|0\rangle \underbrace{\langle 0|3\rangle}_{=0} + \gamma|0\rangle \underbrace{\langle 0|8\rangle}_{=0} \tag{27}$$
$$= \alpha|0\rangle \tag{28}$$
$$N_{03}|\psi\rangle = \Big(|0\rangle\langle 3| + |3\rangle\langle 0|\Big)\Big(\alpha|0\rangle + \beta|3\rangle + \gamma|8\rangle\Big) \tag{29}$$
$$= \alpha|3\rangle + \beta|0\rangle. \tag{30}$$

As you can see from the matrix representations and the examples above, the identity operator would just be a linear combination of projection operators, thus

$$\mathbf{1} = \sum_{n=0}^{\infty} P_n = \sum_{n=0}^{\infty} |n\rangle\langle n|. \tag{31}$$

Operators can also act one after another to form new operators, e.g.

$$N_{03}P_3 = \Big(|0\rangle\langle 3| + |3\rangle\langle 0|\Big)|3\rangle\langle 3| \tag{32}$$
$$= |0\rangle \langle 3|3\rangle \langle 3| + |3\rangle \langle 0|3\rangle \langle 3| \tag{33}$$
$$= |0\rangle\langle 3|. \tag{34}$$

Note that when we hermitian conjugate an operator, we transform the corresponding vectors to their dual space. Meaning formally: $\big(|n\rangle\langle m|\big)^\dagger = |m\rangle\langle n|$. Furthermore, for a chain of operators, their order changes: $(ABC)^\dagger = C^\dagger B^\dagger A^\dagger$. For the example above we obtain

$$(N_{03}P_3)^\dagger = P_3^\dagger N_{03}^\dagger \tag{35}$$
$$= |3\rangle\langle 3|\Big(|0\rangle\langle 3| + |3\rangle\langle 0|\Big) \tag{36}$$
$$= |3\rangle\langle 0|, \tag{37}$$

which is the same as if we just would have calculated $\big(|0\rangle\langle 3|\big)^\dagger$.

The most important operators for physics are hermitian. What does that mean? Well, first it means that when you transpose the matrix and complex conjugate all its entries, you get the same matrix. In formal, an operator A is hermitian when it suffices $A = A^\dagger$. Second, the operator has real eigenvalues, which is important since these are the values we can really measure (therefore we call the corresponding operators "observables").

Other important operators are unitary operators. We say, U is unitary when it fulfills $UU^\dagger = \mathbf{1}$. That means, U is invertible (or reversible, which is important for computing) and we find its inverse U^{-1} by hermitian conjugation.

3 First steps for quantum computing

3.1 Two-State Systems

I feel like I should come to an end soon, therefore let me just quickly lose some words on the whole meaning for quantum computers. For quantum computers, most books and papers are working with two state systems, which means, the particle "lives" in a Hilbert space $\mathcal{H}_2$. An example for that could be the spin of an electron ("up" or "down") or the polarization of a photon ("horizontal" or "vertical"). That means explicitly, that we are acting in a system with the only states

$$|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}, \qquad \text{and} \qquad |1\rangle = \begin{pmatrix}0\\1\end{pmatrix}. \tag{38}$$

These states are the mysterious "qubits". Important operators are the creation operator

$$a^\dagger = |1\rangle\langle 0| = \begin{pmatrix}0 & 0\\1 & 0\end{pmatrix} \tag{39}$$

and the annihilation operator

$$a = |0\rangle\langle 1| = \begin{pmatrix}0 & 1\\0 & 0\end{pmatrix}. \tag{40}$$

They are called like that, because $a^\dagger$ creates a higher state acting on $|0\rangle$, meaning $a^\dagger|0\rangle = |1\rangle$, respectively a annihilates $|1\rangle$ to $|0\rangle$, meaning $a|1\rangle = |0\rangle$. Furthermore, they can destroy the whole state. Since there is no state lower than $|0\rangle$, a acting on $|0\rangle$ yields 0 ($a|0\rangle = 0$), while there is no state greater than $|1\rangle$, as well, s.t. $a^\dagger|1\rangle = 0$. You can see these relations by explicit matrix multiplication or the use of the bra-ket-notation. With these operators, it is easy to define all important operators, such as one important boolean operator, namely the "NOT", which I will refer to as N in the following. N is defined as

$$N = a + a^\dagger, \tag{41}$$

one of the term always destroys the state on which N acts on, the other term flips the state. Note, that N is hermitian and unitary, i.e. reversible.

3.2 Many-Body Systems

Of course, one bit is not enough to perform a computation. Therefore, physicists use quantum many-body systems to express storage. In these systems, we consider n particles interacting with each other. Each of them can either be in state $|0\rangle$ or $|1\rangle$. Hence, we can construct a state by a so-called tensor product $\otimes$. For example, take a three qubit system. One state ψ is then part of the Hilbert space $\mathcal{H}_2^{(1)} \otimes \mathcal{H}_2^{(2)} \otimes \mathcal{H}_2^{(3)}$, and could look like this

$$|\psi\rangle = |0\rangle^{(1)} \otimes |1\rangle^{(2)} \otimes |0\rangle^{(3)} \tag{42}$$

with the superscript enumerating the qubits. However, physicists are lazy. Therefore we will just write

$$|\psi\rangle = |010\rangle \tag{43}$$

and keep the order fixed. But we have to take care of operations. As soon as we perform one, it has to be clear on which qubit the operation is performed. Thus, I will keep the superscript notation in my talk.

Note that the whole state is destroyed as soon as one of the qubits becomes 0 by an operation (such as annihilating a $|0\rangle$, for example).

3.3 What is so Cool about Quantum Computing?

You may now have a first impression on how we prepare a state, call it a storage and perform a computation on it. But how is it different from real computing? The answer to that lies in the linear combinations. It is possible (not only theoretically but also experimentally), to create superpositions and entangled states for many-body systems. Take, for example, the state

$$|\psi\rangle = \frac{1}{\sqrt{2}}\Big(|001\rangle + |010\rangle\Big). \tag{44}$$

Mathematically, this is easy. Physically, this means that the second and the third qubit represent $|0\rangle$ and $|1\rangle$ at the same time. Welcome to the puzzling world of quantum mechanics (by the way, this could be the kind of superposition that Schrödinger suggests for his cat)! Performing operations on this state yields a natural parallel computation on both inputs. However, in the end, we can only measure one of the outputs, can't we? Well, we can use little tricks. But I will give hints about that in my talk!

4 Solutions to Exercises

4.1 Exercise 1

As indicated, the dual vector is obtained from first transposing, then complex conjugating the inital vector (where transposition and complex conjugation are interchangeable).

$$\langle 0| = (|0\rangle)^\dagger = \Big((|0\rangle)^T\Big)^* = \left(e^{ia}, 0, 0, \ldots\right)^* = \left(e^{-ia}, 0, 0, \ldots\right). \tag{45}$$

Then, the scalar product is

$$\langle 0|0\rangle = \left(e^{-ia}, 0, 0, \ldots\right) \cdot \begin{pmatrix} e^{ia} \\ 0 \\ 0 \\ \vdots \end{pmatrix} = e^{-ia}e^{ia} + 0\cdot 0 + 0 \cdot 0 + \cdots = 1. \tag{46}$$

4.2 Exercise 2

a)

$$P_\varphi(0) = |\langle 0|\varphi\rangle|^2 = \left|\alpha_0 \underbrace{\langle 0|0\rangle}_{=1} + \alpha_1 \underbrace{\langle 0|1\rangle}_{=0}\right|^2 = |\alpha_0|^2. \tag{47}$$

$$\tag{48}$$

b)

$$P_\theta(1) = |\langle 1|\theta\rangle|^2 = \left|\beta \underbrace{\langle 1|0\rangle}_{=0} - \frac{e^{ia}}{\sqrt{2}} \underbrace{\langle 1|1\rangle}_{=1}\right|^2 = \frac{e^{ia}e^{-ia}}{\sqrt{2}\sqrt{2}} = \frac{1}{2} \tag{49}$$

c) $|\beta|^2 + \left|\frac{e^{ia}}{\sqrt{2}}\right|^2 = 1 \Leftrightarrow |\beta|^2 = \frac{1}{2}$

d) $\langle\theta| = \beta^* \langle 0| - \frac{e^{-ia}}{\sqrt{2}} \langle 1|$

e)

$$\langle\theta|\varphi\rangle = \alpha_0\beta^* \langle 0|0\rangle - \alpha_0 \frac{e^{-ia}}{\sqrt{2}} \langle 1|0\rangle + \alpha_1\beta^* \langle 0|1\rangle - \frac{\alpha_1 e^{-ia}}{\sqrt{2}} \langle 1|1\rangle = \alpha_0\beta^* - \frac{\alpha_1 e^{-ia}}{\sqrt{2}} \tag{50}$$

$$P_\varphi(\theta) = |\langle\theta|\psi\rangle|^2 = |\alpha_0\beta^*|^2 + \frac{|\alpha_1|^2}{2} - \frac{1}{\sqrt{2}} \operatorname{Re}\left(\alpha_0\beta^*\alpha_1 e^{-ia}\right) \tag{51}$$