Introduction to quantum information and quantum cryptography: Lecture 1

WANTED

DEAD **&** ALIVE

Schrödinger's cat

$$\frac{1}{\sqrt{2}}(|\mathrm{DEAD}\rangle + |\mathrm{ALIVE}\rangle)$$

Quantum information in a nutshell

Quantum information in a nutshell

- storage of information
  - the information is stored in a quantum system
  - where the information is the state of the system

- processing the information (using unitary operators)

- reading out the information (making quantum measurements)

Introduction: quantum bit

As we know, in classical information theory, the basic unit of information is the *bit* whose value can be 0 **or** 1. Its analogue (but not the same(!)) in quantum information theory is the *quantum bit*. From now, we will talk about the latter quantity.

Any two-level quantum system can be regarded as a **quantum bit** (and its state is the information, as we know).

It is natural to ask:
when can a system be regarded as a quantum system?
Unfortunately, it is hard to answer this question adequately (from the perspective of a physicist) to persons who has never been trained in quantum mechanics on a university level.

Introduction: quantum bit

However, from the perspective of an informatician, the question below can be answered with a satisfying precision.

From our perspective, the most important feature of a **quantum system** is that its state is not necessarily defined. What does it mean on the level of bits? While the two possible states of a classical bit (0 and 1) mutually excludes each other, in case of a quantum bit, the *superposition* of these states is also a possible state of the system.

In a *superposition*, both classicaly possible states are included (with some weight) in the state of a quantum bit. The essence of this phenomenon can be summerized expressively in the following way: *events which are mutually exluded by each other in classical physics do not necessarily exlude each other in quantum physics.*

Introduction: quantum bit

Being in a superposition of states titled 0 and 1, a quantum bit *does not "decide"* which state to choose until the readout (which means a quantum measurement or in other word: observation). We must not think that before the measurement / observation, the qubit *is* in one of these states and this information is merely dredged up by the measurement which can give 0 or 1 with some probability!
The truth is that in a state like this, till the readout, even itself the qubit does not "know" if it is in state 0 or state 1. This (the choice of the qubit between 0 and 1) is being "decided" during the interaction of the measurement.
Before the measurement, its state is neither 0 nor 1..... it is *something else*. This "else" is the superposition of them. In case of a superposition only the probability of getting a given state (after measurement) can be predicted exactly.

Introduction: quantum bit

The question naturally arises: what kind of new possibilites are provided by the superposition state of quantum bits?
Using quantum computers in information processing, the input (qubit) state can be also the superposition of classical bit states, hence the quantum computer can process the different input states parallelly.
Using this parallelism quantum computers can solve problems that cannot be solved with classical computers.

Introduction: quantum bit

So far, we have talked about the state of a quantum system, but we have not mentioned how to describe it. The mathematical tool which helps us to feature the state of a quantum system is the: **state vector**.
In the general formalism of quantum mechanics (called Dirac formalism), the state of a system is described with a general infinite dimensional vector. This vector is independent from any coordinate system. Before starting its explanation, I have to emphasize: I will make no effort to be mathematically rigorous restricting myself to give only those informations which we need to know, if we want to understand the topics explained in future lessons.

Introduction: quantum bit

Let us suppose we have a particle (with a mass m) moving in a potential $V(q)$. We try to describe its one dimensional motion in this potential, where q is the coordinate of the particle spread onto the range of $-\infty$ to ∞.
In the Schrödinger formalism of quantum mechanics (called position representation), the state of the particle at a time t is described by its wave function $\psi(q,t)$. If there is no intervening measurement (the particle is not observed), this state evolves from time t_0 (and from a state $\psi(q,t_0)$) according to the Schrödinger equation:

$$\left[-\frac{\hbar^2}{2m}\frac{\partial}{\partial q^2}+V(q)\right]\psi(q,t)=i\hbar\frac{\partial}{\partial t}\psi(q,t).$$

Introduction: quantum bit

From the things explained so far, it follows that there is a strange ambiguity:

- on one hand: if the system is not disturbed by a measurement, its time evolution gives a nice, smooth example of causality.
- on the other and: if there is an intervening measurement, the state of the system falls into one of its classically possible (observable) states and we can predict the probability of a given output only.

For example, if we want to know the position of a particle at a time t, we can make a measurement. The probability of finding the particle between q and $q + dq$ is $|\psi(q, t)|^2 dq$.

Introduction: quantum bit

We have to remark that this state can be described in momentum representation too where the function which features the particle can be written in the following way: $\psi(p,t)$. The two representation are connected by the Fourier transform:

$$\psi(p,t) = \frac{1}{\sqrt{2\pi\hbar}} \int_{-\infty}^{+\infty} \psi(q,t) e^{-\frac{ipq}{\hbar}} dq.$$

Both representations describe the same state. It is just a question of perspective, hence the question naturally arises: is not there a possibility for us to feature a quantum state with a device which is independent from any coordinate system?

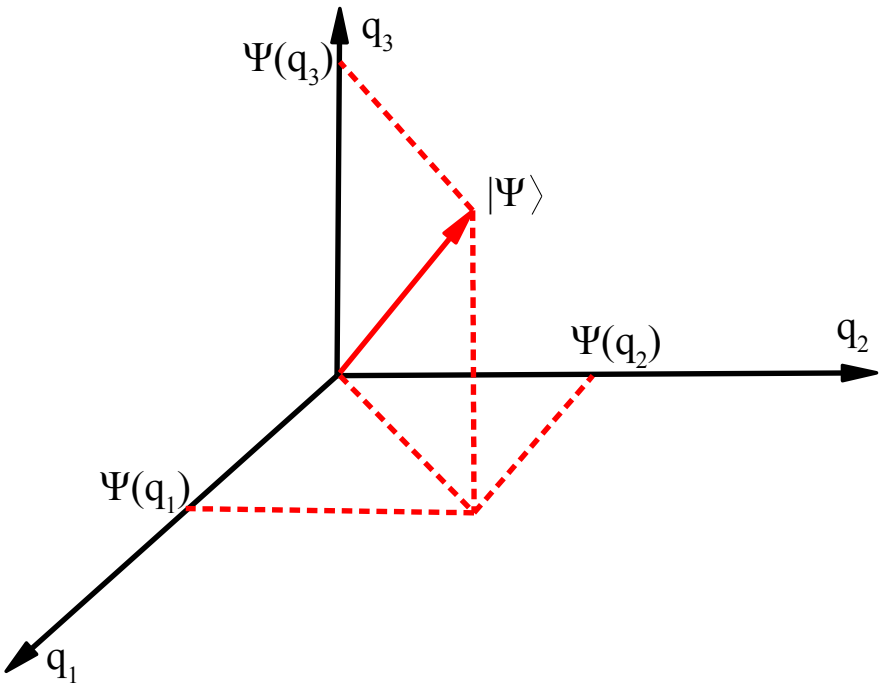
Introduction: quantum bit

The answer is yes. This is aimed by the Dirac formalism. We can understand how a state vector features the quantum state of a system, if we give a geometrical interpretation to the wave function $\psi(q, t)$ at a frozen time t.
We know, coordinate q can have any value from $-\infty$ to ∞. On each place q_1, q_2, q_3.... and so on, the wave function has the value of $\psi(q_1)$, $\psi(q_2)$, $\psi(q_3)$... We can imagine a space with infinite number of dimensions spanned by mutually perpendicular axes. Each axis corresponds to one of the q places.

Introduction: quantum bit

In the system of axes, $\psi(q_1)$ is actually the projection of some vector on axis q_1, $\psi(q_2)$ is the projection of the same vector on axis q_2 and so on. In this case, this vector (as its components too) represents the state of the system, hence we call it **state vector**.This vector is not a simple vector, because its components can be complex numbers. A vector of this kind is denoted by the following symbol (introduced by Dirac) $|\rangle$. The vector whose components are $\psi(q_1)$, $\psi(q_2)$, $\psi(q_3)$... is called ψ ket and denoted by $|\psi\rangle$. The following picture try to show how this vector can be imagined (but we have to keep in mind that a vector like this can be more than three dimensional and its components can have complex values too).

Introduction: quantum bit



Introduction: quantum bit

Each state of a dynamic system is described by a ket vector. We already know that the (linear) superposition of the states of a quantum system is also a possible state of the system. From this it follows that the ket vector space is linear in the following sense: if c_1 and c_2 are complex numbers and $|a\rangle$ and $|b\rangle$ are ket vectors, then their linear combination is also a ket vector

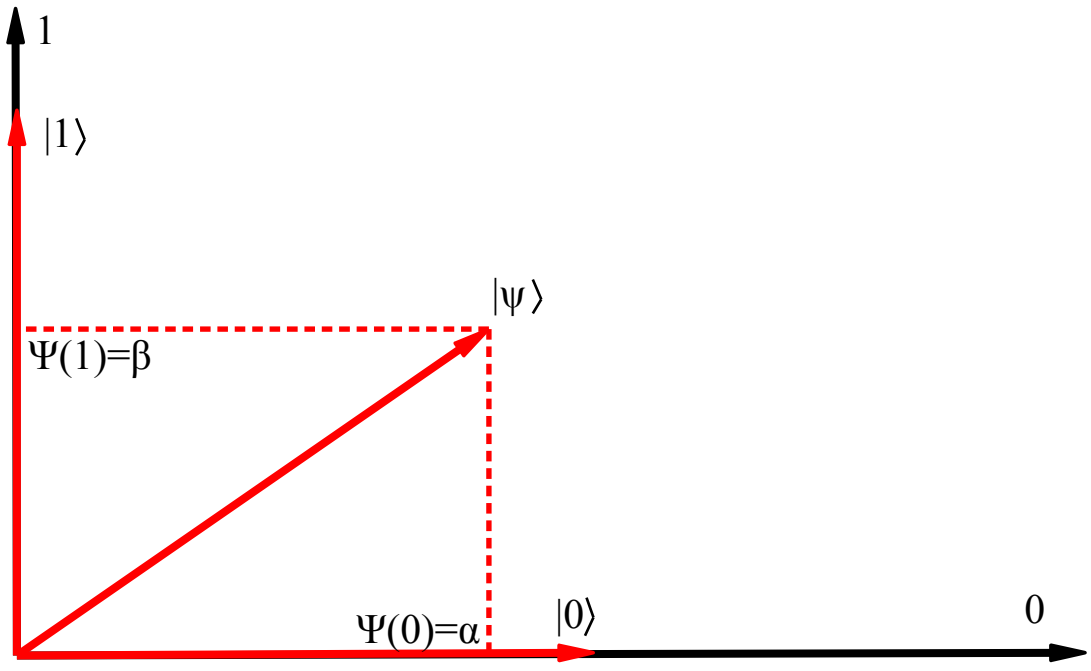
$$|u\rangle = c_1|a\rangle + c_2|b\rangle,$$

because the linear combination of $|a\rangle$ and $|b\rangle$ is also a state of the system. If we have two (or more) ket vectors and none of them can be expressed by the linear combination of the others, they are said to be linearly independent vectors. The number of dimensions of a ket vektor space is defined by the number of its linearly independent kets.

Introduction: quantum bit

The independent states of a quantum system are represented by independent ket vectors, hence the number of dimensions of the vector space (state space) is determined by the number of independent states of the quantum system. Time evolution of the system can be imagined as the rotation of the state vector round the origo.
Returning to the quantum bit: we know any two-level quantum system can be regarded as a quantum bit and the state of the system is the information. In the picture below, we try to show how a qubit (or rather its state vector) can be visualized.

Introduction: quantum bit



Introduction: quantum bit

In the pictuer above, the $|\psi\rangle$ state of the qubit is a superposition of state $|0\rangle$ and state $|1\rangle$, where state $|0\rangle$ is weighted by the value of α and state $|1\rangle$ is weighted by the value of β. These numbers can be complex and using them we can calculate the probability of getting the states $|0\rangle$ and $|1\rangle$ (after measurement). As we mentioned any two level system can be a qubit. Such systems are the polarization of photons or the spin of a particle and so on.

Introduction: quantum bit

We need to know how to calculate with ket vectors on a base spanned by them. Before explaining it, ther is a very important thing we have to know, namely: *the length of a ket vector must be* 1. It is evident that on a base like this, the coordinate of ket $|0\rangle$ on the axis representing bit 0 is 1 and this value is 0 respectively the other axis.
In the case of ket $|0\rangle$, it is evident that these coordinate values are exchanged.

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Introduction: quantum bit

We will need to use also adjoints of ket vectors (adjoint means: transposed and (complex) conjugated). These kind of vectors are named *bra* vectors. In case of having non-complex components, adjoints of kets $|0\rangle$ and $|1\rangle$ (bras $\langle 0|$ and $\langle 1|$) can be written into the form below:

$$\langle 0| = \begin{pmatrix} 1 & 0 \end{pmatrix}, \quad \langle 1| = \begin{pmatrix} 0 & 1 \end{pmatrix}$$

Scalar (or in other word: inner) product of two vectors will also be needed. This multiplication can be achieved in the following way: we have the adjoint of one of the two vectors (in case of non-complex representatives, it is all the same which vector is adjoined), then we multiply this adjoint vector by the other vector. For example scalar product of kets $|0\rangle$ and $|1\rangle$ can be seen below:

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

Introduction: quantum bit

In case of non-complex components, order of factors does not matter, because:

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

but on the other hand, in case of kets $|a\rangle$ and $|b\rangle$ have complex representatives, the following formula is valid:

$$\langle a|b\rangle = \langle b|a\rangle^*$$

Introduction: quantum bit

....and of course, we will need to use also the outer product of vectors. Instead of a number, this kind of product results a matrix. As we can see below, in case of outer product, order of factors is not irrelevant, even in case of non-complex components:

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

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

Introduction: quantum bit

Now, let us return to our quantum bit:

$$|0\rangle, |1\rangle \Longrightarrow |\Psi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

where the following very important requirement has to be satisfied:

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

(This requirement is necessary because of the probability interpretation.)

Introduction: quantum bit

In this phase, we have to enlighten the reasons why we have to know the things treated above. First of all, as we saw, state $|\Psi\rangle$ of a quantum bit is expressed on an orthonormal base which is expanded by kets $|0\rangle$ and $|1\rangle$. States that are represented by kets $|0\rangle$ and $|1\rangle$ are called classically observable states. These orthonormal, *observable*[1] states are the *eigenstates* of the system. If a measurement is made, the measured system falls always into one of its eigenstates (in case of our qubit, into ket $|0\rangle$ or into ket $|1\rangle$) and from that instant, state vector of the system will be the "chosen" eigenstate (or eigenvector).

[1] or in other words: states that are mutually excluded by each other in classical physics

Introduction: quantum bit

Now then! The question is that how can we calculate the probability of finding the system in a certain eigenstate, after making a measurement? We can calculate it via ascertaining the amplitude of projection of state vector $|\Psi\rangle$ on the certain eigenstate[2]. After obtaining this projection (which is a complex number), we have to compute its absolute value, and then we have to square this absolute value. The calculated number will be the value of the sought probability.

[2] obviously *before* making the measurement

Introduction: quantum bit

For example, if we want to know the probability of finding the system of qubit $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ in the state $|0\rangle$, after a measurement, we have to calculate the square of absolute value of α. Square of absolute value of a complex number equals the number itself multyplied by its complex conjugated. In our case, it means: $|\alpha|^2 = \alpha^*\alpha$. Since we will work with vectors with two or far more then two number of dimensions, it is necessary to know how to calculate probabilities that we are interested in. First of all, let us keep in mind that scalar product of two vectors which are perpendicular to each other equals 0, furthermore let us realize that all eigenvectors in the linear combination which builds up state $|\Psi\rangle$ are mutually perpendicular to each other (in our case: $|0\rangle$ and $|1\rangle$). From these two facts it directly follows the way of calculation of probabilities which we are interested in:

Introduction: quantum bit

We have to square the absolute value of scalar product of state $|\Psi\rangle$ and the eigenstate whose materialization-probability we want to know. This method can be understood very easy, if we keep in mind that $|\Psi\rangle$ is a sum of mutually *perpendicular* (eigen)vectors, thus in case of multiplying it by *a member of this sum*, we actually do the following: we multiply all members of the sum by the given member and add the obtained results to each other. Consisting of mutually perpendicular ket vectors, all scalar products which contains different kets results 0. Only the scalar product survives this operation in which the angle between the eigenvector and our ket is equal to 0. There is only one such an eigenvector in the linear combination of $|\Psi\rangle$, namely the one by which $|\Psi\rangle$ was multiplied. Obviously, scalar product between our eigenket and itself equals 1, and this result multiplies the *projection* which we are intersted in (which can be called *probability amplitude*).

Introduction: quantum bit

What is it all about? If we are interested in the value of the projection of $|\Psi\rangle$ on a certain eigenket, all we have to do is to have the scalar product between $|\Psi\rangle$ and the eigenket. Let us consider a very simple example, where we show how to compute the value of probability w_1 of finding the system in state $|1\rangle$ after making a measurement on the base of $(|0\rangle, |1\rangle)$, if the initial state of the system is $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$:

$$w_1 = |\langle 1|\Psi\rangle|^2 = |\langle 1|(\alpha|0\rangle + \beta|1\rangle)|^2 = |\alpha\langle 1|0\rangle + \beta\langle 1|1\rangle|^2 =$$

$$= |\alpha \times 0 + \beta \times 1|^2 = |\beta|^2 = \beta^*\beta$$

...or in matrix representation:

$$w_1 = |\langle 1|\Psi\rangle|^2 = |\begin{pmatrix} 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix}|^2 = |\beta|^2 = \beta^*\beta$$

Introduction: quantum bit

Considering things drawn above, we can understand the reason of the requirement connected with $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$, namely: $|\alpha|^2 + |\beta|^2 = 1$. Since $|\alpha|^2$ is the probability of finding the system in state $|0\rangle$, and $|\beta|^2$ is the probability of materialization of state $|1\rangle$ after a measurement, obviously their sum has to be equal to 1. From this fact, it follows that *the length (or norm) of any statevector has to equal* 1, (because in case of $|\alpha|^2 + |\beta|^2 = 1$, length $\sqrt{|\alpha|^2 + |\beta|^2}$ will be equal to 1). From the foregoing, it is clear how to calculate the norm (length) of an arbitrary vector $|\Psi\rangle$. (By the way, the norm of a vector $|\Psi\rangle$ is denoted by $\|\Psi\|$.)

$$\|\Psi\| = \sqrt{\langle\Psi|\Psi\rangle} = \sqrt{(\alpha^*\langle 0| + \beta^*\langle 1|)(\alpha|0\rangle + \beta|1\rangle)} =$$

$$= \sqrt{|\alpha|^2\langle 0|0\rangle + \alpha^*\beta\langle 0|1\rangle + \beta^*\alpha\langle 1|0\rangle + |\beta|^2\langle 1|1\rangle} =$$

$$= \sqrt{|\alpha|^2 + |\beta|^2}$$

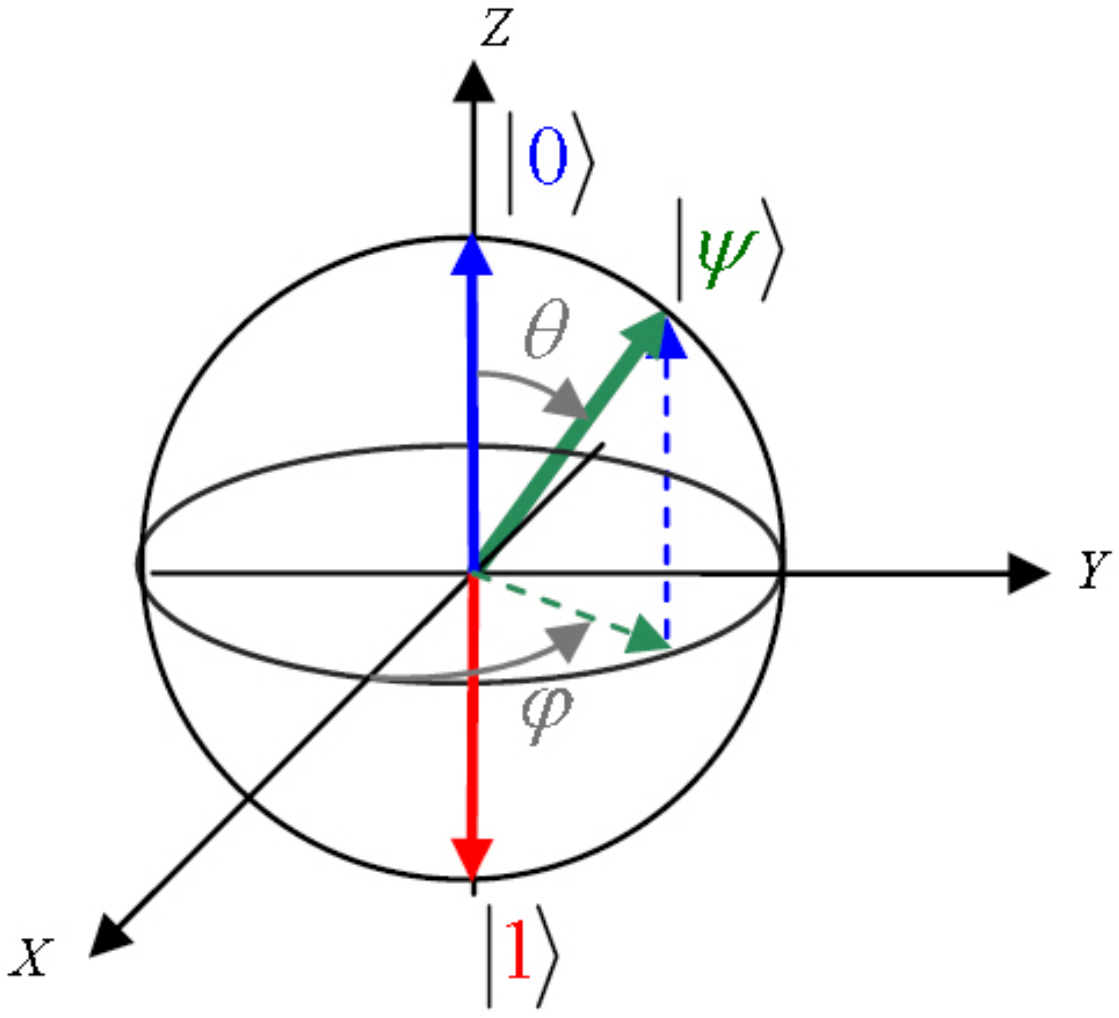
Introduction: quantum bit

...or it can be expressed via matrices:

$$\|\Psi\| = \sqrt{\langle\Psi|\Psi\rangle} = \sqrt{\begin{pmatrix}\alpha^* & \beta^*\end{pmatrix}\begin{pmatrix}\alpha \\ \beta\end{pmatrix}} = \sqrt{|\alpha|^2 + |\beta|^2}$$

Generally, α is a real number and β is a complex one. Besides superposition, phase-freedom is also a newness, in quantum information (from the $e^{j\varphi}$ shape of complex numbers). Phase-freedom makes possible for us to achieve computations via interference. This is related with another kind of visualization of qubits which is represented by the *Bloch-sphere*, as it can be seen in the picture below.

Introduction: quantum bit



Introduction: quantum bit

In this case, the state of the qubits is described by two angles ($0 \leq \theta \leq \pi$ and $0 \leq \varphi \leq 2\pi$), according to the following formula: $|\Psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$. Any point on the surface of the sphere is a possible state $|\Psi\rangle$. In this kind of representation θ is responsible for superposition. If $\theta = 0$, the system is in state $|0\rangle$, and in case of $\theta = \pi$, state of the system is $|1\rangle$. On this surface, orthogonal states are 'over against' each other. Let us remember, in our previous representation, orthogonal states were perpendicular to each other. This is the reason why $\frac{\theta}{2}$ is written into the expression above, instead of θ. Angle φ represents the phase of the complex factor.
Naturally, we will have to work with systems which consist of several qubits, thus we need to know the way of description of their state. This is shown from the following slide.

Introduction: quantum bit

Description of a multi-qubit system

Ensemble of two qubits: In this case the state space of their common system is the tensor product of their state spaces. The base where their state is expressed on is the so called product base, whose elements are the following ones:

$$|0\rangle_1|0\rangle_2 = |00\rangle$$

$$|0\rangle_1|1\rangle_2 = |01\rangle$$

$$|1\rangle_1|0\rangle_2 = |10\rangle$$

$$|1\rangle_1|1\rangle_2 = |11\rangle$$

In our case $|\Psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$, and obviously the following requirement has to be satisfied: $|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$. Generally one of the α-s gets a real value while all the others are complex, hence we get a very large phase-freedom.

Introduction: quantum bit

Description of a multi-qubit system

Let us realize that numbers in the symbols of kets above are actually binary numbers. In decimal system, they correspond to numbers 0, 1, 2, and 3. In case of a system which consists of three qubits, the first base ket of the state space is $|000\rangle$ and the last one is $|111\rangle$, thus numbers from 0 to 7 can be described by base kets. If we have an *n*-qubit system, base elements of its state space are the following ones:

$$|00.....00\rangle$$

$$.$$

$$.$$

$$.$$

$$|11.....11\rangle$$

Description of a multi-qubit system

From this, it follows that general state of an n-qubit system can be written into the following shape:

$$|\Psi\rangle = \sum_{x=0}^{2^n-1} c_x |x\rangle$$

The question naturally arises how can a tensor production of vectors be achieved?[a] Without any explanation we try to show this method below via an example.

[a] For example: how to achieve a production like this $|00\rangle$?

Introduction: quantum bit

Description of a multi-qubit system

$$|a\rangle = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}, \quad |b\rangle = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}, \quad |a\rangle|b\rangle = |ab\rangle = \begin{pmatrix} a_1 b_1 \\ a_1 b_2 \\ a_2 b_1 \\ a_2 b_2 \end{pmatrix}$$

In case we have non column/row matrices:

$$a = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}, b = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}$$

$$a \otimes b = \begin{pmatrix} a_1 b_1 & a_1 b_2 & a_2 b_1 & a_2 b_2 \\ a_1 b_3 & a_1 b_4 & a_2 b_3 & a_2 b_4 \\ a_3 b_1 & a_3 b_2 & a_4 b_1 & a_4 b_2 \\ a_3 b_3 & a_3 b_4 & a_4 b_3 & a_4 b_4 \end{pmatrix}$$

Introduction: quantum bit

Description of a multi-qubit system

Returning to n-qubit systems, we have to mention possibilities given by them: as we have already known numbers and *their superpositions* can be described by two-state quantum systems. What is it all about? As we know $|\Psi\rangle = \sum_{x=0}^{2^n-1} c_x|x\rangle$ is the general state of an n-qubit system, where in each $|x\rangle$, x is binary number consisting of n pieces of digits. In a *superposition* of an n-qubit system, **many numbers** ($2^n - 1$ and 0) can be described **at the same time** via *one* of the states of the system (and of course there is the phase-freedom, as an additional possibility).

Introduction: quantum gates

From the *Schrödinger*-equation an important conservation law can be derive which is related to the current of probability-density. The derived law of conservation represents the conservation of the total probability. It means that any transformation which has an effect on our state vectors (for example in case of their time evolution) must leave the total probability untouched. What does it mean exactly? The thing is that though state vector may rotate around the origo as the state itself is changing, its length has to be left unchanged by the transformation which makes state vector rotate. Why is it equivalent to the conservation of probability? Let us consider the well known two dimensional case, where the norm (length) of the state vector $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ was calculated according to this formula: $\|\Psi\| = \sqrt{\langle\Psi|\Psi\rangle} = \sqrt{|\alpha|^2 + |\beta|^2}$,
where the members under the root-sign are probability values.

Introduction: quantum gates

Any changing of the length of state vector under some transformation would mean that sum of probabilities has changed, or in other words: total probability is not invariant. But - as we know - it cannot happen because of the law of probability-conservation. Since **quantum gates** alter states, matrices which describe transformations made by these gates has to represent operators which satisfy the requirement mentioned above. Operators of this kind are called **unitary operators** (and their matrices are unitary ones). Unitarity is a necessary and sufficient condition which ensures that transformation cannot change the length of (the norm of) a state vector. Operators of such kind of transformations are denoted by the following symbol: $\hat{U}$. But what is the condition of unitarity? A matrix which represents a unitary operator has to satisfy the following requirement: $U^{-1} = U^{\dagger}$, where $U^{\dagger}$ means the adjoint (transposed and complex conjugated) of the matrix.

Introduction: quantum gates

From the fact that length of our state vectors $\sqrt{\langle\Psi|\Psi\rangle} = 1$ (because of the total probability), it follows that $\langle\Psi|\Psi\rangle = 1$. If $|\Psi\rangle$ is subject to a unitary operation of some $\hat{U}$ which alters the original state into a new state of $|\Psi'\rangle$, the following expression has to come true: $\langle\Psi|\Psi\rangle = \langle\Psi'|\Psi'\rangle = 1$. Let us check how unitarity of an operator $\hat{U}$ can ensure it:

$$|\Psi'\rangle = \hat{U}|\Psi\rangle \Longrightarrow \langle\Psi'|\Psi'\rangle = \langle\hat{U}\Psi|\hat{U}\Psi\rangle = \langle\Psi|\hat{U}^{\dagger}\hat{U}|\Psi\rangle$$

We know that according to unitarity $U^{-1} = U^{\dagger}$, furthermore we know U is a square matrix, and in case of a square matrix $UU^{-1} = U^{-1}U = I$. Knowing these facts, we can realize the value of the scalar product (just like the value of the norm) remained the same after the effect of $\hat{U}$. There is another important consequence of unitarity of an operator like $\hat{U}$, namely: transformations described by this kind of operators are *reversible*.

Introduction: quantum gates

This means output state of a quantum gate (or a quantum circuit containing several gates) can be retransformed to its input state by sending back the output state into the gate (or circuit).
Let us consider what it means in case of *one* quantum gate: So, our input sate is $|\Psi\rangle$, and state $|\Psi'\rangle = U|\Psi\rangle$ will appear on the output. (Since henceforward every operator will be represented by matrices, from now $\hat{U} = U$.) This output state will be sent back through the quantum gate, in other words matrix U will have an effect on state $|\Psi'\rangle = U|\Psi\rangle$. In this way, we will get the following state: $UU|\Psi\rangle$.
At this point, it is important to know that from the unitarity of a matrix U, it follows U is a self-adjoint (hermitian) matrix, thus $U^\dagger = U$. Accordingly, $UU|\Psi\rangle = U^\dagger U|\Psi\rangle$. Since - as we know - $U^\dagger = U^{-1}$, our last expression can be altered into the next form: $U^\dagger U|\Psi\rangle = U^{-1}U|\Psi\rangle = |\Psi\rangle$. As we can see, we got back the original input state, thus the transformation is really reversible.

Introduction: quantum gates

From this reversibility, it follows there are classical gates which do not have a quantum analogous. For example such a gate is the AND gate which gives 0 output in case of 00, 01, and 10 inputs. In such a case, input cannot be found out from knowledge of output. On the other hand, NOT gate, which causes a bit-flip ($0 \to 1$, $1 \to 0$), is a reversible one, thus it has a quantum analogous ($|0\rangle \to |1\rangle$, $|1\rangle \to |0\rangle$). Its effect on a general qubit is:

$$\alpha|0\rangle + \beta|1\rangle \to \alpha|1\rangle + \beta|0\rangle$$

Representing the state of the qubit by a two-component column matrix like this

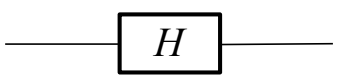
$$\alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix},$$

Introduction: quantum gates

we can describe the effect of NOT gate by use of the matrix below:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix},$$

which is actually one of the three *Pauli* matrices (more on them later) denoted by σ_x. Now, that we know there are classical gates which do not have quantum analogous (for example: AND gate), it is time to mention a quantum gate that does not have classical analogous. Such a gate is the one-bit *Hadamard* gate whose circuit symbol can be seen below:



The left side line of the picture above represents the input quantum bit, and the right side symbolizes the output qubit.

Introduction: quantum gates

It is nice, but we still have not written what happen with qubit crossing through the *Hadamard* gate. Depending on the bit itself, the gate can have two kinds of effect on the qubit:

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

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

(Let us realized that the resulted states span an orthonormal base.)

Introduction: quantum gates

So, after the effect of *Hadamard* gate, a qubit which was originally in one of its eigenstates (in $|0\rangle$ or $|1\rangle$) gets into the superposition of states $|0\rangle$ and $|1\rangle$. It is apparently *impossible in a classical case*. Let us realize that $H^2 = I$:

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

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

Introduction: quantum gates

The matrix of the *Hadamard* gate can be seen below:

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

Naturally, there are two-qubit gates, too. From this kind of gates, C-NOT (Controlled–NOT) gate is the most important one, whose effect can be found below:

$$|00\rangle \rightarrow |00\rangle$$

$$|01\rangle \rightarrow |01\rangle$$

$$|10\rangle \rightarrow |11\rangle$$

$$|11\rangle \rightarrow |10\rangle$$

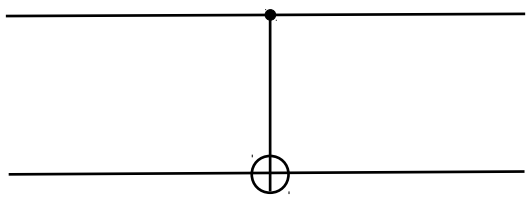
From the rows above, it is clear that C-NOT affects only in case value of first qubit (the control bit) equals 1. In this case second qubit (target bit) is given a reverse value than it had before (a bit flip happens).

Introduction: quantum gates

If we have a little patient, we can easily find out the matrix which represents the effect of C-NOT:

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

Watchful readers can find quickly the NOT gate hiding in the right bottom part of the matrix. Checking of unitarity of C-NOT is a reader's task.
Circuit symbol of C-NOT can be seen below:



Introduction: quantum gates

In the picture above, upper line symbolyzes the controll bit whose value remains untouched by the gate. Only the value of target bit (visualized by the lower line) can change, in case value of control bit equals 1.

Introduction

Quantum circuits

Now we have reached the point, where it is worth introducing the method of modelling quantum computation via quantum circuits. As it can be surmised, in a system of this kind of circuits, qubits are symbolized by lines of the circuit, and quantum gates (which are actually unitary opertors) are denoted by their symbols. There is an important theorem, namely: Any kind of unitary transformation can be constructed by use of one-qubit gates and C-NOT gates. (We set aside from proving this theorem.) This is the reason why we can meet so many C-NOT gates in schemes realizing different kinds of quantum informatical protocols. Below, we show a very simple quantum protocol.

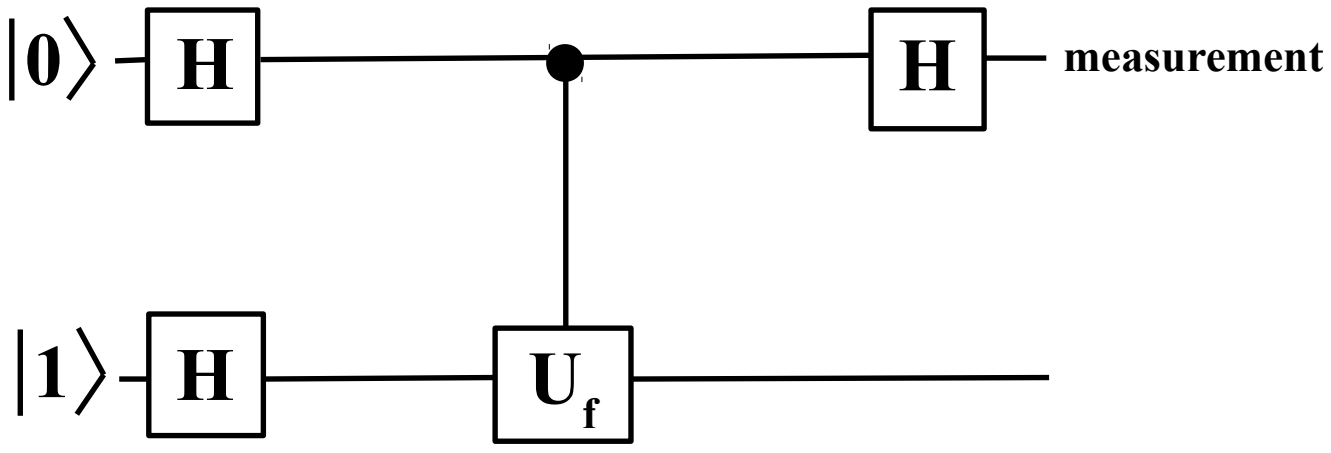
Introduction: Deutsch algorithm

As a tradition, many times *Deutsch* problem is the first treated one in standard textbooks on quantum information to demonstrate how efficient a quantum algorithm can be. The reason which makes writers of these books follow this way can be easily understood, if we realize that though using very few knowledges, this algorithm already shows quantum paralellism in computation, giving students a relatively simple tool that demonstrates how a quantum algorithm can work tipically. Let us follow our great ancestors by beginning with this algorithm.

Introduction: Deutsch algorithm

Let us consider a function f which maps the discreet set of $\{0, 1\}$ onto the set $\{0, 1\}$. In case $f(0) = f(1)$, function f is called constant, and if $f(0) \neq f(1)$ function f is a balanced one. Using some classical method, we have to make *two* evaluations to decide whether function f is a constant or a balanced one. However, using Deutsch algorithm, we can decide it after *one* evaluation. Let us check how it works. First of all, we have to know the quantum circuit which implements *Deutsch*'s algorithm. This circuit is drawn in the figure below.

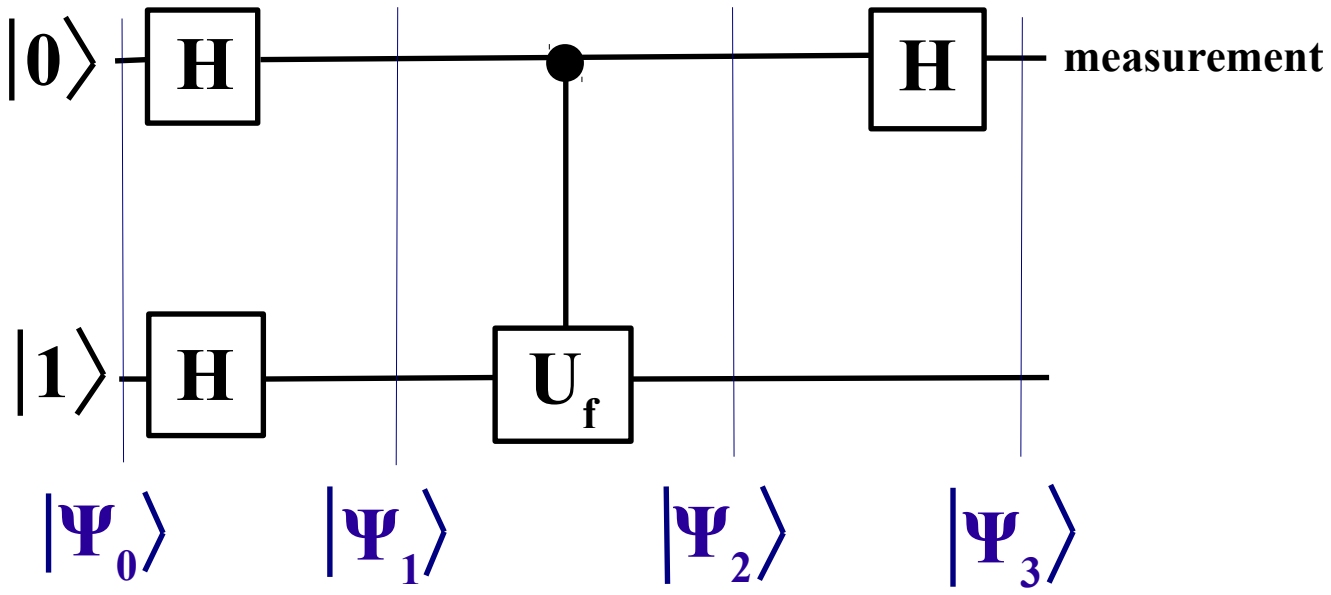
Introduction: Deutsch algorithm



Introduction: Deutsch algorithm

In the picture above, U_f denotes the f-Controlled-NOT gate (or fNOT, CfNOT, or *Deutsch* gate). What does this gate do? In case of denoting the upper bit (which is the control bit) by $|x\rangle$, and the lower bit (target bit) by $|y\rangle$, two-qubit gate U_f has the following effect on the pair of qubits: $|x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$, where $\oplus$ means modulo-2 addition, which is subject to the following connections: $0 + 0 = 0$, $0 + 1 = 1$, $1 + 0 = 1$, $1 + 1 = 0$. In the figure below, different states of the two-qubit system is denoted, correspondently to relevant sections of the circuit.

Introduction: Deutsch algorithm



Introduction: Deutsch algorithm

As it can be seen, input state of the circuit is $|\Psi_0\rangle = |0\rangle|1\rangle$. Due to the effect of first two *Hadamard* gates, this state alters into the state $|\Psi_1\rangle$, as we can see below:

$$|\Psi_1\rangle = H|0\rangle H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) =$$

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

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

Introduction: Deutsch algorithm

Now let us see how this state changes under the effect of *Deutsch* gate:

$$|\Psi_2\rangle = \mathit{CfNOT}|\Psi_1\rangle = \frac{1}{2}\mathit{CfNOT}(|00\rangle - |01\rangle + |10\rangle - |11\rangle) =$$

$$= \frac{1}{2}[|0\rangle|0+f(0)\rangle - |0\rangle|1+f(0)\rangle + |1\rangle|0+f(1)\rangle - |1\rangle|1+f(1)\rangle] =$$

$$= \frac{1}{2}[|0\rangle(|0+f(0)\rangle - |1+f(0)\rangle) + |1\rangle(|0+f(1)\rangle - |1+f(1)\rangle)]$$

Being watchful, we can realize how to simplify the expression above:

- if $f(x) = 0$, then $|0+f(x)\rangle - |1+f(x)\rangle = |0\rangle - |1\rangle$
- on the other hand,
  if $f(x) = 1$, then
  $|0+f(x)\rangle - |1+f(x)\rangle = |1\rangle - |0\rangle = (-1)(|0\rangle - |1\rangle)$
- *thus*: $|0+f(x)\rangle - |1+f(x)\rangle = (-1)^{f(x)}(|0\rangle - |1\rangle)$

Introduction: Deutsch algorithm

From this enumeration, it follows that $|\Psi_2\rangle$ can be written into the shape below:

$$|\Psi_2\rangle = \frac{1}{2}[(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle](|0\rangle - |1\rangle)$$

Before making the measurement (in other word: readout) on the output of the circuit, we have to find out the effect of the last gate on the state of the system. As we can see, in this case a *Hadamard* gate affects on the upper qubit. Let us calculate the resulted state after its action:

$$|\Psi_3\rangle = \frac{1}{2\sqrt{2}}[(-1)^{f(0)}(|0\rangle + |1\rangle) + (-1)^{f(1)}(|0\rangle - |1\rangle)](|0\rangle - |1\rangle) =$$

$$= \frac{1}{2\sqrt{2}}[((-1)^{f(0)} + (-1)^{f(1)})|0\rangle + ((-1)^{f(0)} - (-1)^{f(1)})|1\rangle](|0\rangle - |1\rangle)$$

Introduction: Deutsch algorithm

So, $|\Psi_3\rangle$ is the output state of the circuit, and as it can be seen, there remains no more but to make a measurement on this output state to find out whether function f is a constant or a balanced one. It is natural to ask: how can we decide it based on only one measurement (or in other word: evaluation)? The answer can be easily understood, if we try to imagine what is the output state $|\Psi_3\rangle$ in case of a constant function and in case of a balanced function.

Introduction: Deutsch algorithm

Let us see the result of our imagination:

- if f is a constant function, the resulted state is

$$|\Psi_3\rangle = \pm\frac{1}{\sqrt{2}}(|00\rangle - |01\rangle)$$

- if f is a balanced function, the resulted state is

$$|\Psi_3\rangle = \pm\frac{1}{\sqrt{2}}(|10\rangle - |11\rangle)$$

So, we can draw a conclusion, according to which if f is a constant function, state of the upper qubit will be $|0\rangle$, and if f is a balanced one, upper qubit will be in the state $|1\rangle$.
Thus, making *only one* measurement on the upper qubit, we can decide what sort of function f is.