2. QUANTUM COMPUTING

Jozef Gruska

Faculty of Informatics
Brno, Czech Republic
gruska@fi.muni.cz, http://www.fi.muni.cz/usr/gruska/vienna07

March 18, 2007

2. BASICS - BASIC CONCEPTS and RESULTS

In the chapter several basic concepts of quantum information processing, as well as several very basic but very important results and methods, are introduced.

QUANTUM STATES and PROJECTION MEASUREMENT

In case an orthonormal basis $\{\beta_i\}_{i=1}^n$ is chosen in $\mathcal{H}_n$, any state $|\phi\rangle \in \mathcal{H}_n$ can be expressed in the form

$$|\phi\rangle = \sum_{i=1}^{n} a_i|\beta_i\rangle, \quad \sum_{i=1}^{n} |a_i|^2 = 1,$$

where

$a_i = \langle\beta_i|\phi\rangle$ are called probability amplitudes

and

their squares provide probabilities

that if the state $|\phi\rangle$ is measured with respect to the basis $\{\beta_i\}_{i=1}^n$, then the state $|\phi\rangle$ collapses into the state $|\beta_i\rangle$ with probability $|a_i|^2$.

The classical “outcome” of a measurement of the state $|\phi\rangle$ with respect to the basis $\{\beta_i\}_{i=1}^n$ is the index i of that state $|\beta_i\rangle$ into which the state $|\phi\rangle$ collapses.

QUANTUM (PROJECTION) MEASUREMENTS

A more general view of the measurement of a quantum state is as observation (measurement) with respect to an **observable** — a decomposition of a given Hilbert space into orthogonal subspaces (such that each vector can be uniquely represented as a sum of vectors of these subspaces).

There are two outcomes of a projection measurement of a state $|\phi\rangle$:

1. Classical information into which subspace projection of $|\phi\rangle$ was made.
2. A new quantum state $|\phi'\rangle$ into which the state $|\phi\rangle$ collapses.

The subspace into which projection is made is chosen **randomly** and the corresponding probability is uniquely determined by the amplitudes at the representation of $|\phi\rangle$ at the basis states of the subspace.

SUPERPOSITION PRINCIPLE

Perhaps the most important principle of quantum pure states is superposition principle that says that any superposition of quantum states is again a quantum state.

Technically, this means that if $|\phi_i\rangle$, $1 \leq i \leq n$, are pure states and $\Sigma_{i=1}^{n} |a_i|^2 = 1$, then also

$$\sum_{i=1}^{n} a_i|\phi_i\rangle$$

is a quantum pure state.

PROBABILISTIC versus QUANTUM SYSTEM

Let us illustrate, on an example, a principal difference between a quantum evolution and a classical probabilistic evolution as well as impacts of quantum superpositions.

If a qubit system develops under the evolution

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

then, after one step of evolution, we observe both $|0\rangle$ and $|1\rangle$ with the probability $\frac{1}{2}$, but after two steps we get

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

and therefore any observation gives $|0\rangle$ with probability 1.

On the other hand, in case of the classical probabilistic evolution

$$[0] \longrightarrow \frac{1}{2}[0] + \frac{1}{2}[1] \quad [1] \longrightarrow \frac{1}{2}[0] + \frac{1}{2}[1]$$

we have after one step of evolution both 0 and 1 with the same probability $\frac{1}{2}$, but after two steps we have again

$$[0] \longrightarrow \frac{1}{2}(\frac{1}{2}[0] + \frac{1}{2}[1]) + \frac{1}{2}[0] + \frac{1}{2}[1]) = \frac{1}{2}[0] + \frac{1}{2}[1]$$

and therefore, after two steps of evolution, we have again both values 0 and 1 with the same probability $\frac{1}{2}$.

In the quantum case, in the second evolution step, amplitudes at $|1\rangle$ cancel each other and we have so-called destructive interference/superposition. At the same time, amplitudes at $|0\rangle$ amplify each other and we have so-called constructive interference/superposition.

WHAT ARE ACTUALLY QUANTUM STATES? - TWO VIEWS

- In so called “relative state interpretation” of quantum mechanics a quantum state is interpreted as an objective real physical object.
- In so called “information view of quantum mechanics” a quantum state is interpreted as a specification of (our knowledge or beliefs) probabilities of all experiments that can be performed with the state - the idea that quantum states describe the reality is therefore abounded.

MEASUREMENT

in CLASSICAL versus QUANTUM physics

BEFORE QUANTUM PHYSICS

it was taken for granted that when physicists measure something, they are gaining knowledge of a pre-existing state — a knowledge of an independent fact about the world.

QUANTUM PHYSICS

says otherwise. Things are not determined except when they are measured, and it is only by being measured that they take on specific values.

A quantum measurement forces a previously indeterminate system to take on a definite value.

QUBITS

A quantum bit, or qubit, is a unit vector

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

in a two dimensional vector (Hilbert) space for which a particular basis , denoted $\{|0\rangle, |1\rangle\}$, has been fixed.

EXAMPLE: Representation of qubits by
(a) electron in a Hydrogen atom (b) a spin-$\frac{1}{2}$ particle

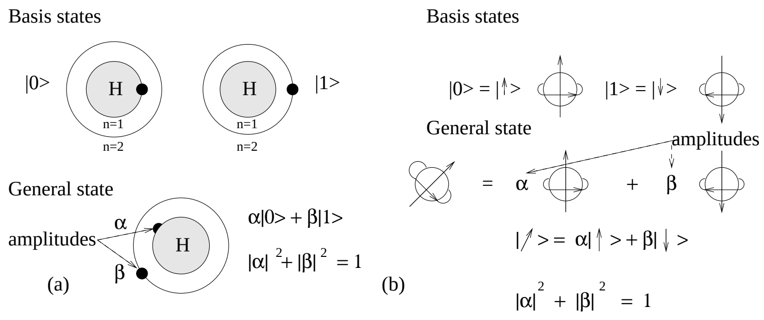


Figure 1: Qubit representations by energy levels of an electron in a hydrogen atom and by a spin-$\frac{1}{2}$ particle. The condition $|\alpha|^2 + |\beta|^2 = 1$ is a legal one if $|\alpha|^2$ and $|\beta|^2$ are to be the probabilities of being in one of two basis states (of electrons or photons).

HILBERT SPACE H_2

STANDARD (COMPUTATIONAL) BASIS — **DUAL BASIS**

$$|0\rangle, |1\rangle \qquad\qquad |0'\rangle, |1'\rangle$$

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad\qquad \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \quad \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix}$$

Hadamard matrix (Hadamard operator in the standard basis)

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

has properties

$$H|0\rangle = |0'\rangle \qquad\qquad H|0'\rangle = |0\rangle$$

$$H|1\rangle = |1'\rangle \qquad\qquad H|1'\rangle = |1\rangle$$

transforms one of the basis into another one.

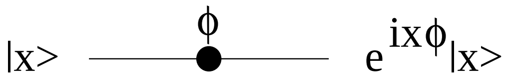
Whener we talk about qubits and quantum computation in general, a choice of a fixed basis (usually computational) is expected with respect to which all statements are made.

UNIVERSAL SET of ONE-QUBIT GATES

Hadamard gate and the following phase shift gate

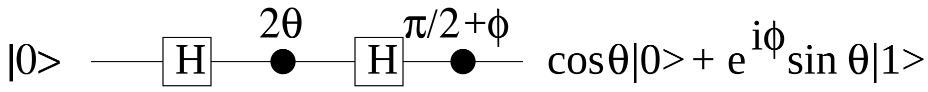
$$\phi = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}$$

with notation



form a universal set of gates for one-qubit gates.

Two Hadamard gates and two phase shift gates can generate the most general pure state of a single qubit

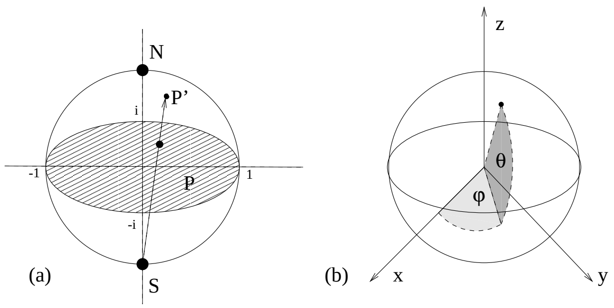


General form of a unitary matrix of degree 2

$$U = e^{i\gamma} \begin{pmatrix} e^{i\alpha} & 0 \\ 0 & e^{-i\alpha} \end{pmatrix} \begin{pmatrix} \cos\theta & i\sin\theta \\ i\sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} e^{i\beta} & 0 \\ 0 & e^{-i\beta} \end{pmatrix}$$

QUBIT REPRESENTATION

There are several ways to represent qubits as points on a unit sphere:



One way to represent states of qubits is as points on the surface of a unit Riemann sphere, where North and South poles correspond to the basis states (bits) (see Figure a).[1]

Qubits can be represented also by points on a Bloch sphere (called also Poincaré sphere), and (see Figure b), using the spherical coordinate system.

This representation is based on the fact that any qubit can be represented as

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

.

A qubit unitary operation = rotation

[1]The Riemann sphere is a sphere of unit radius whose equatorial plane is the complex plane whose center is the origin of the plane. One qubit state $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ can be represented by a point on a Riemann sphere as follows.If $\beta \neq 0$ we mark in the complex plane the point P that represents the number $\frac{\alpha}{\beta}$ and then we project P from the South Pole onto the sphere to get the point P' that then represents $|\phi\rangle$. If $\alpha = 0$ one gets the North Pole this way; if $\beta = 0$ the South Pole is the limit (Penrose, 1994).

QUBIT MEASUREMENT

A qubit state can "contain" unbounded large amount of information. However, a quantum state cannot be fully identified.

By a measurement of the qubit state

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

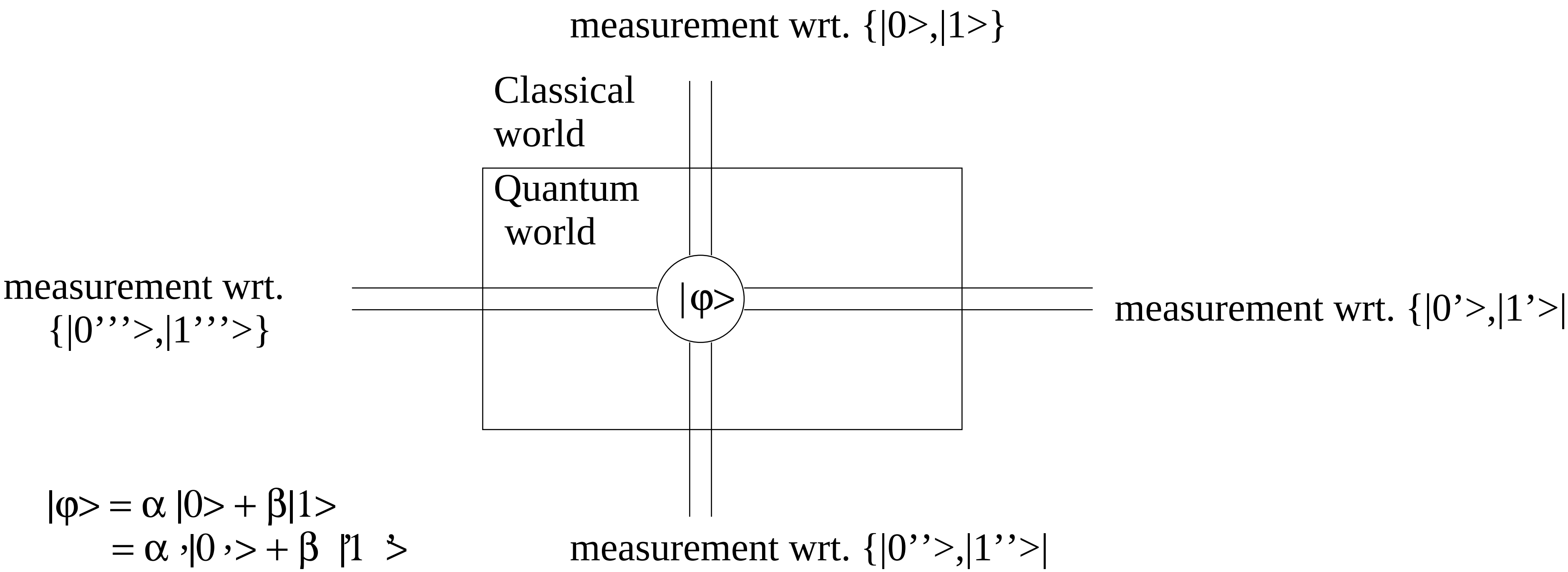
with respect to the basis

$$|0\rangle, |1\rangle$$

we can obtain only classical information and only in the following random way:

$$0 \text{ and } |0\rangle \text{ with probability } |\alpha|^2$$

$$1 \text{ and } |1\rangle \text{ with probability } |\beta|^2$$



$$
\begin{aligned}
|\varphi\rangle &= \alpha\,|0\rangle + \beta|1\rangle \\
&= \alpha'|0'\rangle + \beta'|1'\rangle \\
&= \alpha''|0''\rangle + \beta''|1''\rangle \\
&= \alpha'''|0'''\rangle + \beta'''|1'''\rangle
\end{aligned}
$$

EXAMPLE 1

If the state

$$|0\rangle$$

is measured with respect to the standard (called also Boolean or computational) basis $\{|0\rangle, |1\rangle\}$**, then we get as the outcome**

$$0$$

with probability 1 **and the state collapses**

to itself.

If the state

$$|0\rangle$$

is measured with respect to the dual basis $\{|0'\rangle, |1'\rangle\}$**, then we get as the outcome**

0 **with probability** $\frac{1}{2}$ $\qquad$ 1 **with probability** $\frac{1}{2}$

and the state collapses into the state

$|0'\rangle$ $\qquad$ **or** $\qquad$ $|1'\rangle$

because

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

EXAMPLE 2

If the qubit

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$$

is measured with respect to the standard basis $\{|0\rangle, |1\rangle\}$**, then we get**

$$0 \text{ - } |0\rangle \textbf{ with probability } |\alpha|^2 \quad \textbf{or} \quad 1 \text{ - } |1\rangle \textbf{ with probability } |\beta|^2$$

Let us now try to measure $|\phi\rangle$ **with respect to the dual basis** $\{|0'\rangle, |1'\rangle\}$**. Since**

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

and therefore

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

we have

$$|\phi\rangle = \frac{1}{\sqrt{2}}((\alpha + \beta)|0'\rangle + (\alpha - \beta)|1'\rangle)$$

what implies that measurement of $|\phi\rangle$ **with respect to the dual basis provides**

$$0 - |0'\rangle \textbf{ with probability } \tfrac{1}{2}|\alpha + \beta|^2$$

or

$$1 - |1'\rangle \textbf{ with probability } \tfrac{1}{2}|\alpha - \beta|^2$$

BEAM-SPLITTERS and MACH-ZEHNDER INTERFEROMETER

The following picture illustrate one-particle interference using so-called Mach-Zehnder interferometer.

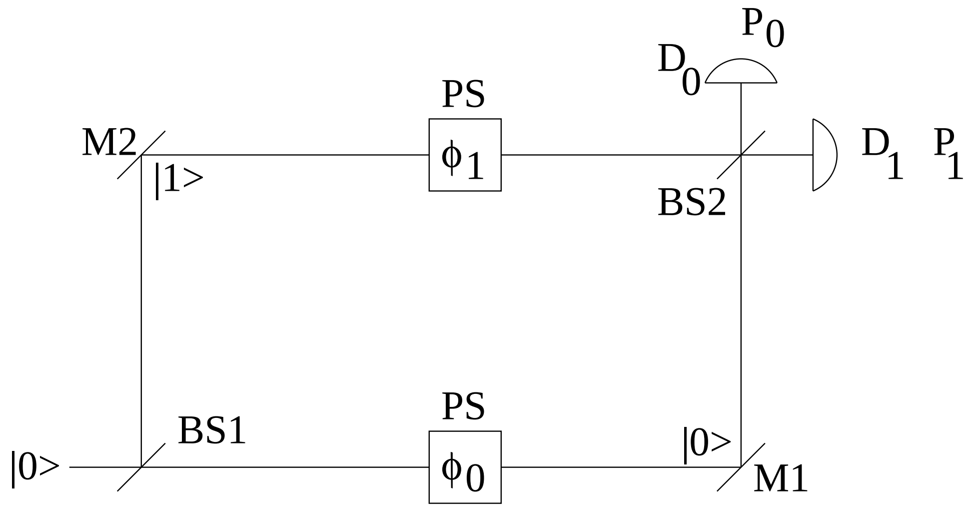


Figure 2: Mach-Zehnder interferometer, BS - beam-splitters, M -mirrors, PS - phase-shifter, D - detectors

Action of a beam-splitter is as that of the Hadamard gate

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

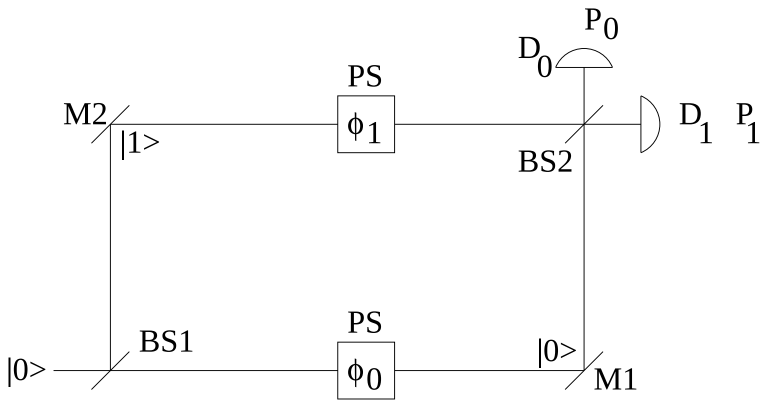


Figure 3: Mach-Zehnder interferometer, BS - beam-splitters, M -mirrors, PS - phase-shifter, D - det ectors

Action of Mach-Zehnder interferometer can be described as follows

$$
\begin{aligned}
|0\rangle &\overset{BS1}{\longrightarrow} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \overset{PS}{\rightarrow} \frac{1}{\sqrt{2}}(e^{i\phi_0}|0\rangle + e^{i\theta_1}|1\rangle) && (1)\\
&= e^{i\frac{\theta_0+\theta_1}{2}}\frac{1}{\sqrt{2}}(e^{i\frac{\theta_0-\theta_1}{2}}|0\rangle + e^{i\frac{-\theta_0+\theta_1}{2}}|1\rangle) && (2)\\
&\overset{BS2}{\longrightarrow} e^{i\frac{\theta_0+\theta_1}{2}}(\cos\frac{1}{2}(\phi_0-\phi_1)|0\rangle + i\sin\frac{1}{2}(\phi_0-\phi_1)|1\rangle) && (3)
\end{aligned}
$$

Two detectors detect a particle with probabilities

$$P_0 = \cos^2\frac{\phi_0-\phi_1}{2} \text{ and } P_1 = \sin^2\frac{\phi_0-\phi_1}{2}$$

and therefore if $\phi_0 = \phi_1$ only the detector D_0 can detect a particle.

OBSERVATION on INTERFERENCE EXPERIMENTS

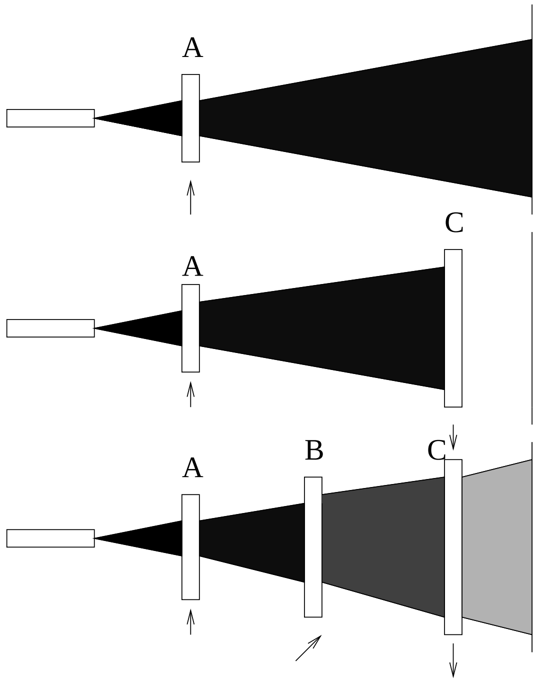
- **Single particle experiments are not restricted to photons.**
- **One can repeat such an experiment with electrons, atoms or even some molecules.**
- **When it comes to atoms both internal and external degrees of freedom can be used**

LIGHT GOING THROUGH FILTERS

In the first experiment if the light goes through filter A polorized up half of that does not get through, half does.

If we add filter C with oposite polarization, no light gets through the filter C.

If we add, between filters A and C another filter with diagonal polaization some of light gets over the filter C.

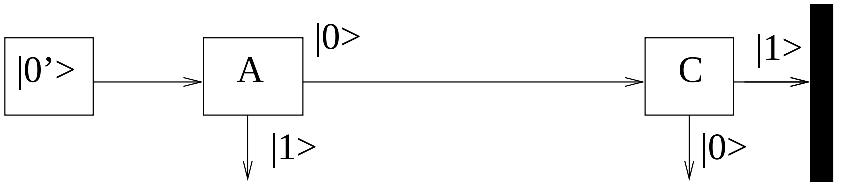


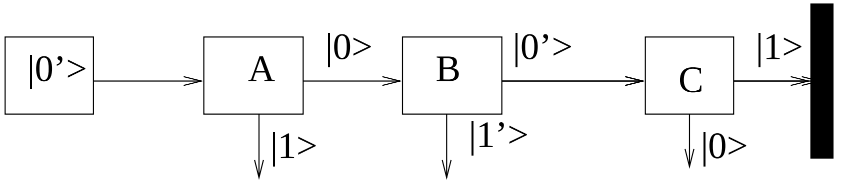
FILTERS as MEASURING DEVICES

In our previous experiment we can see the sourse as produsing the state $|0'\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

Filter A can be seen as produsing measurement in the computational basis with horizontal output corresponding to the state $|1\rangle$. Filter C does the smae but has outputs with opposite orientation.

Filter B should be seen as producing measurement in the dual basis.





PAULI MATRICES

Very important one-qubit unary operators are the following *Pauli operators*, expressed in the standard basis as follows;

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

An application of Pauli matrices to basis states can be expressed also as follows (for $b \in \{0,1\}$:

$$\sigma_x|b\rangle = |b \oplus 1\rangle, \quad \sigma_y|b\rangle = i(-1)^b|b \oplus 1\rangle \quad \sigma_z|b\rangle = (-1)^b|b\rangle.$$

Observe that Pauli matrices transform a qubit state $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ as follows

$$\sigma_x(\alpha|0\rangle + \beta|1\rangle) = \beta|0\rangle + \alpha|1\rangle \quad \sigma_z(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle - \beta|1\rangle$$

and for $\sigma_y' = \sigma_x\sigma_z$ we have

$$\sigma_y'(|\alpha|0\rangle + \beta|1\rangle) = \beta|0\rangle - \alpha|1\rangle.$$

Operators σ_x, σ_z and σ_y' represent therefore a *bit error*, a *sign error* and a *bit-sign error*.

MIXED STATES - DENSITY MATRICES

A probability distribution $\{(p_i, |\phi_i\rangle\}_{i=1}^k$ on pure states is called a mixed state to which it is assigned a density operator

$$\rho = \sum_{i=1}^{k} p_i |\phi_i\rangle\langle\phi_i|.$$

One interpretation of a mixed state $\{p_i, |\phi_i\rangle\}_{i=1}^k$ is that a source X produces the state $|\phi_i\rangle$ with probability p_i.

Any matrix representing a density operator is called density matrix.

To two different mixed states can correspond the same density matrix.

Two mixed states with the same density matrix are physically undistinguishable.

MAXIMALLY MIXED STATES

To the maximally mixed state

$$(\frac{1}{2}, |0\rangle), (\frac{1}{2}, |1\rangle)$$

which represents a random bit corresponds the density matrix

$$\frac{1}{2}\begin{pmatrix}1\\0\end{pmatrix}(1,0)+\frac{1}{2}\begin{pmatrix}0\\1\end{pmatrix}(0,1)=\frac{1}{2}\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}=\frac{1}{2}I_2$$

Surprisingly, many other mixed states have as their density matrix that one of the maximally mixed state.

QUANTUM ONE-TIME PAD CRYPTOSYSTEM

CLASSICAL ONE-TIME PAD cryptosystem

plaintext: an n-bit string p
shared key: an n-bit string k
cryptotext: an n-bit string c
encoding: $c = p \oplus k$
decoding: $p = c \oplus k$

QUANTUM ONE-TIME PAD cryptosystem:

plaintext: an n-qubit string $|p\rangle = |p_1\rangle \dots |p_n\rangle$
shared key: two n-bit strings k, k'
cryptotext: an n-qubit string $|c\rangle = |c_1\rangle \dots |c_n\rangle$
encoding: $|c_i\rangle = \sigma_x^{k_i} \sigma_z^{k'_i} |p_i\rangle$
decoding: $|p_i\rangle = \sigma_z^{k'_i} \sigma_x^{k_i} |c_i\rangle$ where $|p_i\rangle = \begin{pmatrix} a_i \\ b_i \end{pmatrix}$ and $|c_i\rangle = \begin{pmatrix} d_i \\ e_i \end{pmatrix}$ are qubits and

$\sigma_x = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ with $\sigma_z = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ are Pauli matrices.

UNCONDITIONAL SECURITY of QUANTUM ONE-TIME PAD

In the case of encryption of a qubit

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$$

by QUANTUM ONE-TIME PAD cryptosystem what is being transmitted is the mixed state

$$(\frac{1}{4}, |\phi\rangle), (\frac{1}{4}, \sigma_x|\phi\rangle).(\frac{1}{4}, \sigma_z|\phi\rangle), (\frac{1}{4}, \sigma_x\sigma_z|\phi\rangle)$$

whose density matrix is

$$\frac{1}{2}I_2.$$

This density matrix is identical to the density matrix corresponding to that of a random bit, that is to the mixed state

$$(\frac{1}{2}, |0\rangle), (\frac{1}{2}, |1\rangle)$$

SHANNON's THEOREMS

Shannon classical encryption theorem says that n bits are necessary and sufficient to encrypt securely n bits.

Quantum version of Shannon encryption theorem says that $2n$ classical bits are necessary and sufficient to encrypt securely n qubits.

COMPOSED QUANTUM SYSTEMS

Tensor product of vectors

$$(x_1,\dots,x_n)\otimes(y_1,\dots,y_m)=(x_1y_1,\dots,x_1y_m,x_2y_1,\dots,x_2y_m,\dots,x_ny_1,\dots,x_ny_m$$

Tensor product of matrices $$A\otimes B=\begin{pmatrix} a_{11}B & \dots & a_{1n}B \\ \vdots & & \vdots \\ a_{n1}B & \dots & a_{nn}B \end{pmatrix}$$

where $$A=\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \dots & & \dots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}$$

Example

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\otimes\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}=\begin{pmatrix} a_{11} & a_{12} & 0 & 0 \\ a_{21} & a_{22} & 0 & 0 \\ 0 & 0 & a_{11} & a_{12} \\ 0 & 0 & a_{21} & a_{22} \end{pmatrix}$$

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\otimes\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}=\begin{pmatrix} a_{11} & 0 & a_{12} & 0 \\ 0 & a_{11} & 0 & a_{12} \\ a_{21} & 0 & a_{22} & 0 \\ 0 & a_{21} & 0 & a_{22} \end{pmatrix}$$

Tensor product of Hilbert spaces $H_1 \otimes H_2$ is the complex vector space spanned by tensor products of vectors from H_1 and H_2, that corresponds to the quantum system composed of the quantum systems corresponding to Hilbert spaces H_1 and H_2.

If a Hilbert space $\mathcal{H}_n$ has a basis $\{\alpha_i\}_{i=1}^n$ and Hilbert space $\mathcal{H}_m$ has a basis $\{\beta_j\}_{j=1}^m$,

then tensor product $\mathcal{H}_n \otimes \mathcal{H}_m\}$ has as one of the basis $\{\alpha_i \otimes \beta_j\}_{ij}$

An important difference between classical and quantum systems

A state of a compound classical (quantum) system can be (cannot be) always composed from the states of the subsystems.

EXAMPLE

Hilbert space $\mathcal{H}_4$ can be seen as tensor product of two one-qubit Hilbert spaces

$$\mathcal{H}_2 \otimes \mathcal{H}_2$$

and therefore one of its basis consists of the states

$$|0\rangle \otimes |0\rangle, \quad |0\rangle \otimes |1\rangle, \quad |1\rangle \otimes |0\rangle, \quad |1\rangle \otimes |1\rangle$$

that are usually denoted shortly as the states

$$|00\rangle, \quad |01\rangle, \quad |10\rangle, \quad |11\rangle$$

Similarly, the states of the standard/computational n-qubit Hilbert space $\mathcal{H}_{2^n}$ are the states

$$|i_1 i_2 \ldots i_n\rangle = |i_1\rangle \otimes \ldots \otimes |i_n\rangle$$

CARTESIAN PRODUCT versus TENSOR PRODUCT

Individual state spaces of n classical particles combine through the cartesian product. For example, if V and W are two dimensional vector

spaces with bases $\{v_1, v_2\}$ and $\{w_1, w_2\}$, respectively, then $V \times W$ has as the basis union of the basis of components, that is $\{v_1, v_2, w_1.w_2\}$

Individual state spaces of n quantum particles combine through the tensor product.

$V \otimes W$ has as the basis

$$\{v_1 \otimes w_1, v_1 \otimes w_2, v_2 \otimes w_1, v_2 \otimes w_2\}.$$

In case V and W have dimension 3, $V \times W$ has dimension 6 and $V \otimes W$ has dimension 9.

TWO QUBIT REGISTERS

A general state of a 2-qubit register is:

$$|\phi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

where

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$$

and $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ are vectors of the “standard” basis of H_4, i.e.

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

Important unitary matrices of degree 4, to transform states of 2-qubit registers are C-NOT (CNOT) or controlled not matrix:

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

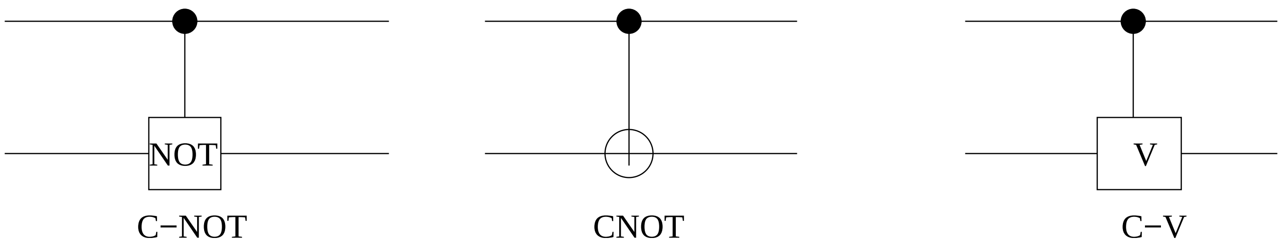
for which it holds:

$$CNOT : |x, y\rangle \Longrightarrow |x, x \oplus y\rangle$$

and C-V, or control V, matrix

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

For the gates corresponding to the above matrices we use notation:



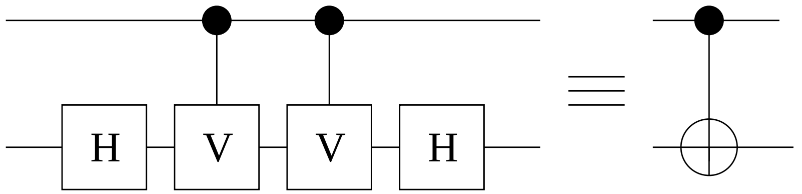
$$V = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

QUANTUM CIRCUITS - EXAMPLES

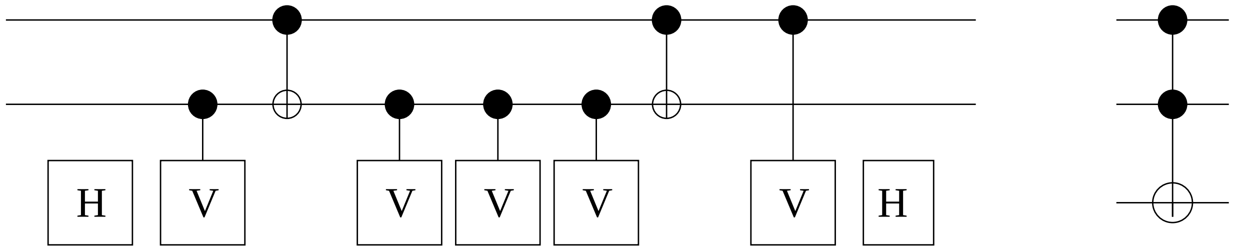
Quantum circuits are defined in a similar way as classical only its gates are either unitary operations or measurements.

Hadamard gate and C-V gate form a universal set of unitary gates - using these gates one can for any unitary operation U and $\varepsilon > 0$ design a quantum circuit C_U that approximates U with precision ε.

Two examples of quantum circuits for the CNOT gate and for Toffoli gate:



CNOT gate

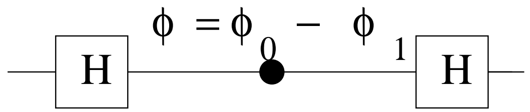


Toffoli gate

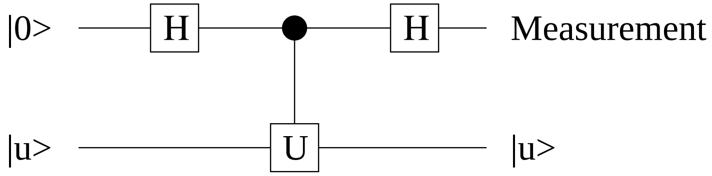
V

GENERALIZATION of MACH-ZEHNDER INTERFEROMETER

Mach-Zehnder interferometer can be represented by the following circuit



Its modification is the following circuit where $|u\rangle$ is eigenvector of U that maps $U|u\rangle = e^{i\phi}|u\rangle$.



This circuit "kick back" eigenvalue $e^{i\phi}$ in the front of the $|1\rangle$-component in the first qubit. The first qubit evolves as follows:

$$|0\rangle|u\rangle \stackrel{H}{\rightarrow} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|u\rangle \stackrel{c-U}{\rightarrow} \frac{1}{\sqrt{2}}(|0\rangle + e^{i\phi}|1\rangle|1\rangle)|u\rangle \stackrel{H}{\rightarrow} (\cos\frac{\phi}{2}|0\rangle + i\sin\frac{\phi}{2}|1\rangle)|u\rangle.$$

SOLVING SCHRÖDINGER EQUATION

For the Hamiltonian

$$H = \frac{\pi\hbar}{2}\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & -1 & 1 \end{pmatrix} = \frac{\pi\hbar}{2}V$$

the Schödinger equation

$$i\hbar\frac{\partial U(t)}{\partial t} = HU(t)$$

has the solution

$$U(t) = e^{-\frac{i}{\hbar}Ht} = \sum_{k=1}^{\infty}\frac{(-\frac{i\pi}{2})^k V^k t^k}{k!} = I + \frac{1}{2}\sum_{k=0}^{\infty}\frac{(-\pi i t)^k}{k!}V$$

and therefore for $t = 1$,

$$e^{-\frac{i\pi}{2}V} = I + \frac{1}{2}(e^{-i\pi} - 1)V = I - V = XOR.$$

A QUANTUM EVOLUTION STEP

A quantum evolution step consists formally of a quantum state (vector) multiplication by a unitary operator. That is

$$A|\phi\rangle = |\psi\rangle$$

For example,

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \end{pmatrix} = \begin{pmatrix} a_{11}b_1 + a_{12}b_2 + a_{13}b_3 + a_{14}b_4 \\ a_{21}b_1 + a_{22}b_2 + a_{23}b_3 + a_{24}b_4 \\ a_{31}b_1 + a_{32}b_2 + a_{33}b_3 + a_{34}b_4 \\ a_{41}b_1 + a_{42}b_2 + a_{43}b_3 + a_{44}b_4 \end{pmatrix}.$$

A better insight into such a process can be obtained using different notation at which it is assumed that all rows and columns are labeled by the states of the standard basis of H_4.

$$\begin{pmatrix} a_{00,00} & a_{00,01} & a_{00,10} & a_{00,11} \\ a_{01,01} & a_{01,01} & a_{01,10} & a_{01,11} \\ a_{10,00} & a_{10,01} & a_{10,10} & a_{10,11} \\ a_{11,00} & a_{11,01} & a_{11,10} & a_{11,11} \end{pmatrix} \begin{pmatrix} b_{00} \\ b_{01} \\ b_{10} \\ b_{11} \end{pmatrix} = \begin{pmatrix} a_{00,00}b_{00} + a_{00,01}b_{01} + a_{00,10}b_{10} + a_{00,11}b_{11} \\ a_{01,00}b_{00} + a_{01,01}b_{01} + a_{01,10}b_{10} + a_{01,11}b_{11} \\ a_{10,00}b_{00} + a_{10,01}b_{01} + a_{10,10}b_{10} + a_{10,11}b_{11} \\ a_{11,00}b_{00} + a_{11,01}b_{01} + a_{11,10}b_{10} + a_{11,11}b_{11} \end{pmatrix} = \begin{pmatrix} d_{00} \\ d_{01} \\ d_{10} \\ d_{11} \end{pmatrix}.$$

NO-CLONING THEOREM

INFORMAL VERSION: Unknown quantum state cannot be cloned.

FORMAL VERSION: There is no unitary transformation U such that for any qubit state $|\psi\rangle$

$$U(|\psi\rangle|0\rangle) = |\psi\rangle|\psi\rangle$$

PROOF: Assume U exists and for two different states $|\alpha\rangle$ and $|\beta\rangle$

$$U(|\alpha\rangle|0\rangle) = |\alpha\rangle|\alpha\rangle \quad U(|\beta\rangle|0\rangle) = |\beta\rangle|\beta\rangle$$

Let

$$|\gamma\rangle = \frac{1}{\sqrt{2}}(|\alpha\rangle + |\beta\rangle)$$

Then

$$U(|\gamma\rangle|0\rangle) = \frac{1}{\sqrt{2}}(|\alpha\rangle|\alpha\rangle + |\beta\rangle|\beta\rangle) \neq |\gamma\rangle|\gamma\rangle = \frac{1}{2}(|\alpha\rangle|\alpha\rangle + |\beta\rangle|\beta\rangle + |\alpha\rangle|\beta\rangle + |\beta\rangle|\alpha\rangle)$$

However, CNOT can make copies of basis states $|0\rangle, |1\rangle$:

$$XOR(|x\rangle|0\rangle) = |x\rangle|x\rangle$$

IMPLICATIONS FOR SECURE TRANSMISSION of QUANTUM STATES

Let us assume that an eavesdropper Eve knows that Alice is sending to Bob one quantum state from a set $\{\phi_1, \phi_2, \ldots, \phi_n\}$ of non-orthogonal quantum states. What she can do?

- Eve cannot make copy of the transmitted state.
- There is no measurement Eve can find out reliably which state is being transmitted.
- She can only measure the state being transmitted, but each such a measurement will, with large probability, destroy the state being transmitted.

Intuitive conclusion There is nothing an eavesdropper can do without having large probability of being detected.

BELL STATES

States

$$|\beta_{00}\rangle = |\Phi^{+}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle, \quad |\beta_{10}\rangle = |\Phi^{-}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$|\beta_{01}\rangle = |\Psi^{+}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle, \quad |\beta_{11}\rangle = |\Psi^{-}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

form an orthogonal (Bell) basis in H_4 and play an important role in quantum computing.

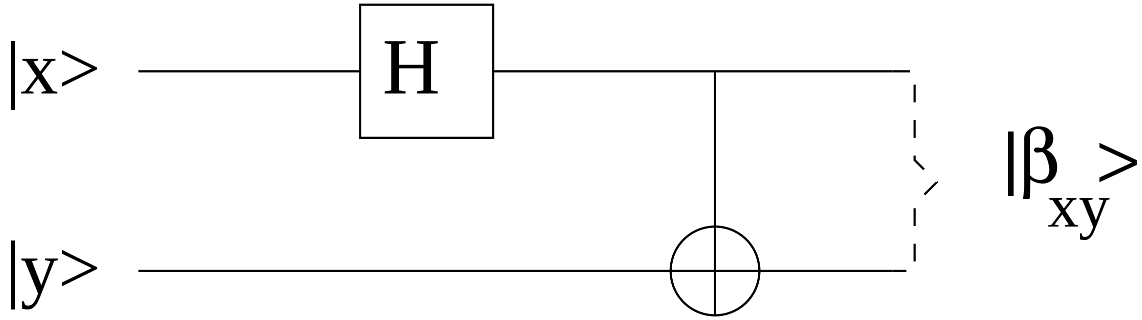
Theoretically, there is an observable for this basis. However, no one has been able to construct a measuring device for Bell measurement using linear elements only.

DESIGN of BELL STATES

Bell states can be defined concisely by formula

$$|\beta_{xy}\rangle = \frac{|0y\rangle + (-1)^x |1\bar{y}\rangle}{\sqrt{2}}.$$

and constructed easily by the circuit



QUANTUM MEASUREMENT

of the states of 2-qubit registers

$$|\phi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

1. Measurement with respect to the basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ provides the results:

$$\begin{array}{llll} 00 & \text{and} & |00\rangle & \text{with probability } |\alpha_{00}|^2 \\ 01 & \text{and} & |01\rangle & \text{with probability } |\alpha_{01}|^2 \\ 10 & \text{and} & |10\rangle & \text{with probability } |\alpha_{10}|^2 \\ 11 & \text{and} & |11\rangle & \text{with probability } |\alpha_{11}|^2 \end{array}$$

2. Measurement of particular qubits provides the results:

By measuring the first qubit we get

$$0 \text{ with probability } |\alpha_{00}|^2 + |\alpha_{01}|^2$$

$$\text{and } |\phi\rangle \text{ is reduced to the vector } \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$$

$$1 \text{ with probability } |\alpha_{10}|^2| + |\alpha_{11}|^2$$

$$\text{and } |\phi\rangle \text{ is reduced to the vector } \frac{\alpha_{10}|10\rangle + \alpha_{11}|11\rangle}{\sqrt{|\alpha_{10}|^2 + |\alpha_{11}|^2}}$$

MEASUREMENT — EXAMPLE

A photon with linear polarization along a direction θ to the vertical axis (to vector $|1\rangle$) is represented by the state

$$|\theta\rangle = \cos\theta|1\rangle + \sin\theta|0\rangle$$

A photon with orthogonal polarization has then the state

$$|\theta^{\perp}\rangle = \sin\theta|1\rangle - \cos\theta|0\rangle$$

From that it follows that:

$$|1\rangle = \cos\theta|\theta\rangle + \sin\theta|\theta^{\perp}\rangle$$

$$|0\rangle = \sin\theta|\theta\rangle - \cos\theta|\theta^{\perp}\rangle$$

If another photon is prepared with linear polarization ϕ, then

$$\begin{aligned} |\phi\rangle &= \cos\phi|1\rangle + \sin\phi|0\rangle && (4)\\ &= \cos\phi[\cos\theta|\theta\rangle + \sin\theta|\theta^{\perp}\rangle] + \sin\phi[\sin\theta|\theta\rangle - \cos\theta|\theta^{\perp}\rangle] && (5)\\ &= \cos(\theta-\phi)|\theta\rangle + \sin(\theta-\phi)|\theta^{\perp}\rangle && (6) \end{aligned}$$

If the above state is measured with respect to the basis $\{\theta\rangle, |\theta^{\perp}\rangle\}$ (or using the calcite crystal oriented with its axis at an angle θ), then the outcome is θ with probability

$$\cos^2(\theta-\phi).$$

MEASUREMENT of TWO PHOTONS

Let us assume that two photons in the state

$$|\psi\rangle = \alpha|10\rangle - \beta|01\rangle$$

are much separated, see Figure, and then one is measured with respect to the polarization θ and the other one with respect to the polarization ϕ.

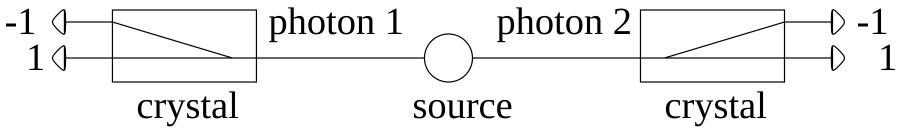


Figure 4: Two entangled photons are measured for orientations θ and ϕ

$$\begin{aligned}
|\psi\rangle &= \alpha|10\rangle - \beta|01\rangle && (7)\\
&= \alpha[\cos\theta|\theta\rangle + \sin\theta|\theta^{\perp}\rangle][\sin\phi|\phi\rangle - \cos\phi|\phi\rangle] - \beta[\sin\theta|\theta\rangle - \cos\theta|\theta^{\perp}\rangle][\cos\phi|\phi\rangle + \sin\phi|\phi^{\perp}\rangle] && (8)\\
&= [\alpha\cos\theta\sin\phi - \beta\sin\theta\cos\phi]|\theta\rangle|\phi\rangle + [\alpha\cos\theta\cos\theta - \beta\sin\theta\sin\phi]|\theta\rangle|\phi^{\perp}\rangle && (9)\\
&+ [\alpha\sin\theta\sin\phi + \beta\cos\theta\cos\phi]|\theta^{\perp}\rangle|\phi\rangle + [-\alpha\sin\theta\cos\phi + \beta\cos\theta\sin\phi]|\theta^{\perp}\rangle|\phi^{\perp}\rangle && (10)
\end{aligned}$$

The probability that the state $|\psi\rangle$ collapses into the state $|\theta\rangle|\phi^{\perp}\rangle$ is therefore

$$|\alpha\cos\theta\cos\phi - \beta\sin\theta\sin\phi|^2.$$

QUANTUM ENTANGLEMENT I

The concept of entanglement is primarily concerned with states of multipartite systems.

For a bipartite quantum system $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$, we say that its state $|\Phi\rangle$ is *an entangled state* if it cannot be decomposed into a tensor product of a state from $\mathcal{H}_A$ and a state from $\mathcal{H}_B$.

For example, it is easy to verify that a two-qubit state

$$|\phi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle,$$

is not entangled, that is

$$|\phi\rangle = (x_1|0\rangle + y_1|1\rangle) \otimes (x_2|0\rangle + y_2|1\rangle)$$

if and only if $\frac{a}{b} = \frac{x_2}{y_2} = \frac{c}{d}$, that is if

$$ad - bc = 0.$$

Therefore, all Bell states are entangled, and they are important examples of entangled states.

QUANTUM ENTANGLEMENT - BASIC DEFINITIONS

The concept of entanglement is primarily concerned with the states of multipartite systems.

For a bipartite quantum system $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$, a pure state $|\Phi\rangle$ is called entangled if it cannot be decomposed into a tensor product of a state from $\mathcal{H}_A$ and a state from $\mathcal{H}_B$.

A mixed state (density matrix) ρ of $\mathcal{H}$ is called entangled if ρ cannot be written in the form

$$\rho = \sum_{i=1}^{k} p_i \rho_{A,i} \otimes \rho_{B,i}$$

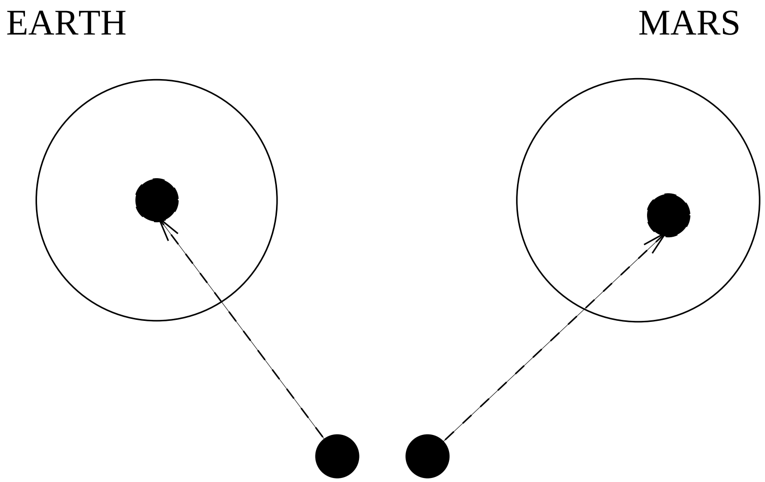
where $\rho_{A,i}$ ($\rho_{B,i}$) are density matrices in $\mathcal{H}_A$ (in $\mathcal{H}_B$) and $\Sigma_{i=1}^{k} p_i = 1$, $p_i > 0$.

Basic importance of entanglement comes from the following facts demonstrating that entanglement implies the existence of non-local correlations.

Let two particles originally in the EPR-state

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

move far from each other



then measurement of any one of these particles makes the EPR-state to collapse, randomly, either to one of the states $|00\rangle$ or $|11\rangle$. As the classical outcomes both parties get at their measurements, no matter when they make them, the same outcomes.

Einstein called this phenomenon "spooky action at a distance" because measurement in one place seems to have an instantaneous (non-local) effect at the other (very distant) place.

CREATION of ENTANGLED STATES

Entangled states are gold mine for QIPC, but their creation is very difficult. This is natural because particles in an entangled states should exhibit non-local correlations no matter how far they are.

Basic methods to create entangled states:

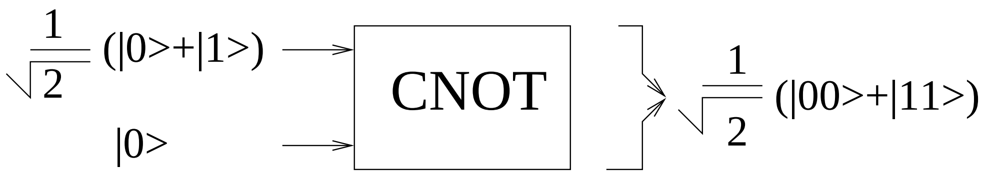
- Using special physical processes, for example parametric down-conversion. (Nowadays one can create in one second million maximally entangled states with 99% "precision" (fidelity)).
- Using "entangling" quantum operations. For example

$$\text{CNOT}((\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)) \otimes |0\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

- Using entanglement swapping.

HOW TO CREATE ENTANGLED STATES?

$$\mathbf{CNOT}\left(\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\otimes|0\rangle\right) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\right)$$



ENTANGLEMENT SWAPPING

If particles P_1 and P_2 are in the EPR-state and so are particles P_3 and P_4, then Bell measurement of particles P_2 and P_3, makes particles P_1 and P_4, that have never interacted before, to be in the maximally entangled EPR-state:

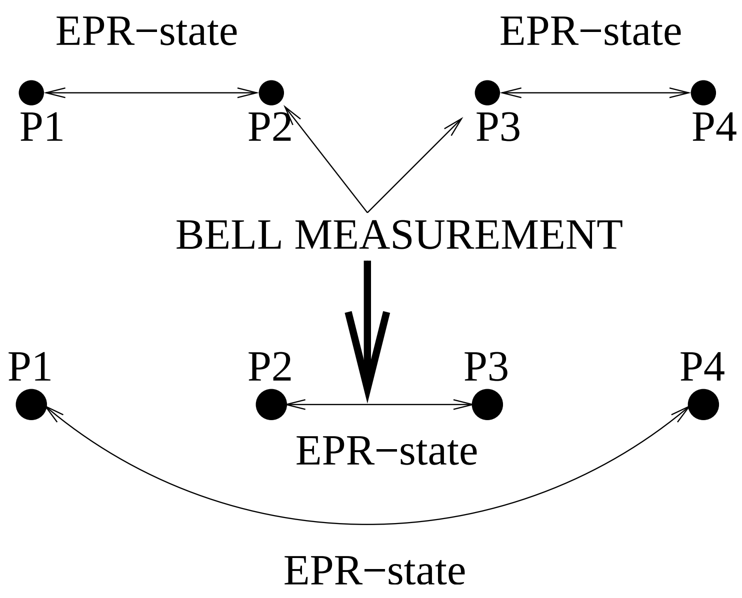


Figure 5: Entanglement swapping

QUANTUM NON-LOCALITY

- Physics was non-local since Newton's time, with exception of the period 1915-1925.
- Newton has fully realized counterintuitive consequences of the non-locality his theory implied.
- Einstein has realized the non-locality quantum mechanics imply, but it does not seem that he realized that entanglement based non-locality does not violate no-signaling assumption.
- Recently, attempts started to study stronger non-signaling non-locality than the one quantum mechanics allows.

NON-LOCALITY in NEWTON's THEORY

Newton realized that his theory concerning gravity allows non-local effect. Namely, that

> **if a stone is moved on the moon, then weight of all of us, here on the earth, is immediately modified.**

NEWTON's words

The *consequences of current theory that implies that* gravity should be innate, inherent and essential to Matter, so that any Body may act upon another at a Distance throw a Vacuum, without the mediation of any thing else, by and through which their Action and Force may be conveyed from one to another, is to me so great an Absurdity, that I believe no Man who has in philosophical Matters a competent Faculty of thinking, can ever fall unto it.

Gravity must be caused by an Agent acting constantly according certain Laws, but whether this Agent be material or immaterial, I have left to the Consideration of my Readers.

POWER of ENTANGLEMENT

After its discovery, entanglement and its non-locality impacts have been seen as a peculiarity of the existing quantum theory that needs some modification to get rid of them, as a source of all kind mysteries and counterintuitive consequences.

Currently, after the discovery of quantum teleportation and of such powerful quantum algorithms as Shor's factorization algorithm, entanglement is seen and explored as a new and powerful quantum resource that allows

- to perform tasks that are not possible otherwise;
- to speed-up much some computations and to economize (even exponentially) some communications;
- to increase capacity of (quantum) communication channels;
- to implement perfectly secure information transmissions;
- to develop a new, better, information based, understanding of the key quantum phenomena and by that, a deeper, information processing based, understanding of Nature.

DIFFERENCES between ONE and TWO-QUBIT states

It is just quantum entanglement which prevents realization of quantum computation using just classical waves (that also exhibit superposition).

Indeed, all possible states of one qubit can be realized by the polarization states of classical light beam – using one half-wave and two quarter-wave plates. As a consequence a single qubit has a classical analogue.

On the other hand, the entangled states of two qubits have no classical counterpart.

CLASSICAL TELEPORTATION

The so called *No-teleportation theorem*, one of the fundamental laws of quantum mechanics, says that *(classical) teleportation* is impossible.

This means that there is no way to use classical channels to transmit faithfully quantum information.[2]

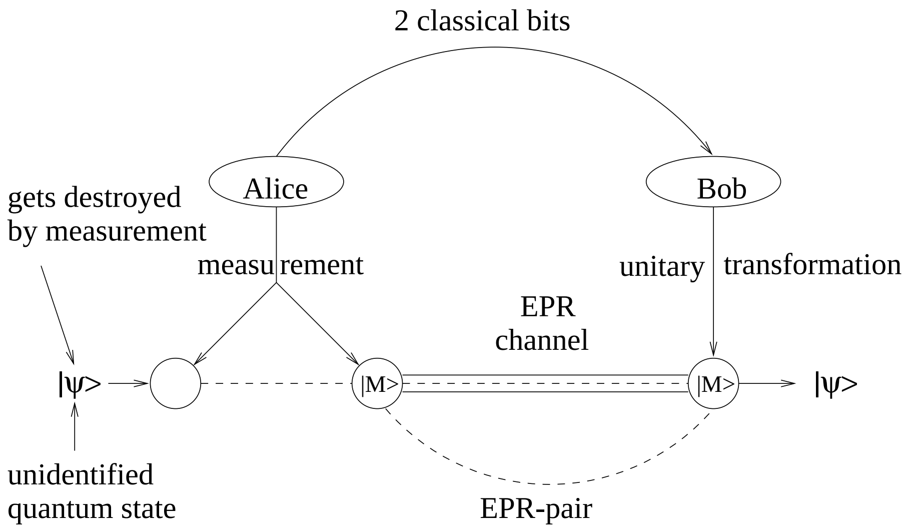
In more technical terms, there is no possibility to measure, in general, a single copy of quantum state in such a way that the classical outcomes of the measurement would be sufficiently to reconstruct faithfully the state.

Indeed, the classical teleportation would imply that *quantum cloning is possible* and this would imply that *super-luminal communication* is possible.

[2] I looked to several dictionaries for term teleportation. Webster 's New World Dictionary of the American Language says *Teleportation is theoretical transportation of matter through space by converting it into energy and then converting it at the terminal point*;

QUANTUM TELEPORTATION

Quantum teleportation allows to transmit unknown quantum information to a very distant place in spite of impossibility to measure or to broadcast information to be transmitted.



$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad |EPR-pair\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Total state

$$|\psi\rangle|EPR-pair\rangle = \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle)$$

Measurement of the first two qubits is then done with respect to the “Bell basis”.

BELL BASES

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \qquad |\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \qquad |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

QUANTUM TELEPORTATION I

Total state of three particles:

$$|\psi\rangle|EPR - state\rangle = \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle)$$

can be expressed as follows:

$$\begin{aligned}|\psi\rangle|EPR - state\rangle \; = \; & \frac{1}{2}|\Phi^+\rangle(\alpha|0\rangle + \beta|1\rangle) + \frac{1}{2}|\Psi^+\rangle(\alpha|1\rangle + \beta|0\rangle) \\ & + \frac{1}{2}|\Phi^-\rangle(\alpha|0\rangle - \beta|1\rangle) + \frac{1}{2}|\Psi^-\rangle(\alpha|1\rangle - \beta|0\rangle)\end{aligned}$$

and therefore the measurement of the first two particles projects the state of the Bob's particle into a "small modification " $|\psi_1\rangle$ of the unknown state $|\psi\rangle = \frac{1}{\sqrt{2}}(\alpha|0\rangle + \beta|1\rangle)$.

The unknown state $|\psi\rangle$ can therefore be obtained from $|\psi_1\rangle$ by applying one of the four operations

$$\sigma_x, \sigma_x\sigma_z, \sigma_z, I$$

and the result of the Bell measurement provides two bits specifying which of the above four operations should be applied.

These four bits Alice needs to send to Bob using a classical channel (by email, for example).

QUANTUM TELEPORTATION II

If the first two particles of the state

$$\begin{aligned} |\psi\rangle|EPR-state\rangle &= \frac{1}{2}|\Phi^+\rangle(\alpha|0\rangle+\beta|1\rangle)+\frac{1}{2}|\Psi^+\rangle(\alpha|1\rangle+\beta|0\rangle) \\ &+\frac{1}{2}|\Phi^-\rangle(\alpha|0\rangle-\beta|1\rangle)+\frac{1}{2}|\Psi^-\rangle(\alpha|1\rangle-\beta|0\rangle) \end{aligned}$$

are measured with respect to the Bell basis then Bob's particle gets into the mixed state

$$(\frac{1}{4},\alpha|0\rangle+\beta|1\rangle)\oplus(\frac{1}{4},\alpha|0\rangle-\beta|1\rangle)\oplus(\frac{1}{4},\beta|0\rangle+\alpha|1\rangle)\oplus(\frac{1}{4},\beta|0\rangle-\alpha|1\rangle)$$

to which corresponds the density matrix

$$\frac{1}{4}\begin{pmatrix}\alpha\\ \beta*\end{pmatrix}(\alpha^*,\beta^*)+\frac{1}{4}\begin{pmatrix}\alpha\\ -\beta\end{pmatrix}(\alpha^*,-\beta^*)+\frac{1}{4}\begin{pmatrix}\beta\\ \alpha\end{pmatrix}(\beta^*,\alpha^*)+\frac{1}{4}\begin{pmatrix}\beta\\ -\alpha\end{pmatrix}(\beta^*,-\alpha^*)=\frac{1}{2}.I$$

The resulting density matrix is identical to the density matrix for the mixed state corresponding to the random bit:

$$(\frac{1}{2},|0\rangle)\oplus(\frac{1}{2},|1\rangle).$$

Indeed, the density matrix for the last mixed state has the form:

$$\frac{1}{2}\begin{pmatrix}1\\ 0\end{pmatrix}(1,0)+\frac{1}{2}\begin{pmatrix}0\\ 1\end{pmatrix}(0,1)=\frac{1}{2}I.$$

QUANTUM TELEPORTATION — COMMENTS

- **Alice can be seen as dividing information contained in $|\psi\rangle$ into**

  quantum information - transmitted through EPR channel

  and

  classical information - transmitted through a classical channel

- **In a quantum teleportation an unknown quantum state $|\phi\rangle$ can be disassembled into, and later reconstructed from, two classical bit-states and an maximally entangled pure quantum state.**

- **Using quantum teleportation an unknown quantum state can be *teleported* from one place to another by a sender who does not need to know — for teleportation itself — neither the state to be teleported nor the location of the intended receiver.**

- **One can also see quantum teleportation as a protocol that allows one to teleport all characteristics of an object, embedded in some matter and energy, and localized at one place to another piece of energy and matter located at a distance.**

- **The teleportation procedure cannot be used to transmit information faster than light**

  but

  it can be argued that quantum information presented in unknown state is transmitted instantaneously (except two random bits to be transmitted at the speed of light at most).
- **EPR channel is irreversibly destroyed during the teleportation process.**
- **One can also see quantum teleportation as a protocol that allows one to teleport all characteristics of an object embedded in some matter and energy localized at one place to another piece of energy and matter located at a distance.**

QUANTUM SUPER DENSE CODING

A process inverse to teleportation, in which one qubit is used to send two bits, is called **superdense quantum coding**.

Assume again that Alice and Bob share two particles in the EPR-state: If now Alice wants to send to Bob bits $b_1 b_2$, she performs on her particle a Pauli operations according to the columns 1 and 2 of the following table 6:

Alice's bits	Pauli's rotations	Alice's particle: new state	$\rightarrow$	Bob's XOR transformation	Bob's bases $\mathcal{D}, \mathcal{B}$	Bob's bits
00	I	$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$		$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)\|0\rangle$	00	00
01	σ_x	$\frac{1}{\sqrt{2}}(\|10\rangle + \|01\rangle)$		$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)\|1\rangle$	01	01
11	σ'_y	$\frac{1}{\sqrt{2}}(-\|10\rangle + \|01\rangle)$		$\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)\|1\rangle$	11	11
10	σ_z	$\frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$		$\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)\|0\rangle$	10	10

Figure 6: Superdense coding steps

The overall state of two particles is then depicted in column 3. If Alice sends then her particle to Bob (we say that she sends one qubit) and Bob performs on his, now two, particles the XOR operation, then his two particles get into the state shown in column 4. If now Bob measures his old particle in the standard basis and the newly obtained particle in the dual basis, he can determine, see columns 5 and 6, the two bits Alice tried to send him.

Observe, that in both examples it was the EPR state that allowed extraordinary powerful transmission of quantum or classical information.

QUANTUM PSEUDO-TELEPATHY

Using entangled states various effects can be produced that resemble telepathy.

Example - Stage telepathy

Two players, Alice and Bob, are on a stage, see Figure 7, very far from each other (so far that they cannot communicate), and they are simultaneously, but independently and randomly asked again and again, by a moderator, either a “food question” or a “color question”.

- **FOOD question**: What is your favorite meal?

  ANSWER has to be either **carrot** or **peas**.

- **COLOR question**: What is your favorite color?

  ANSWER has to be either **green** or **red**.

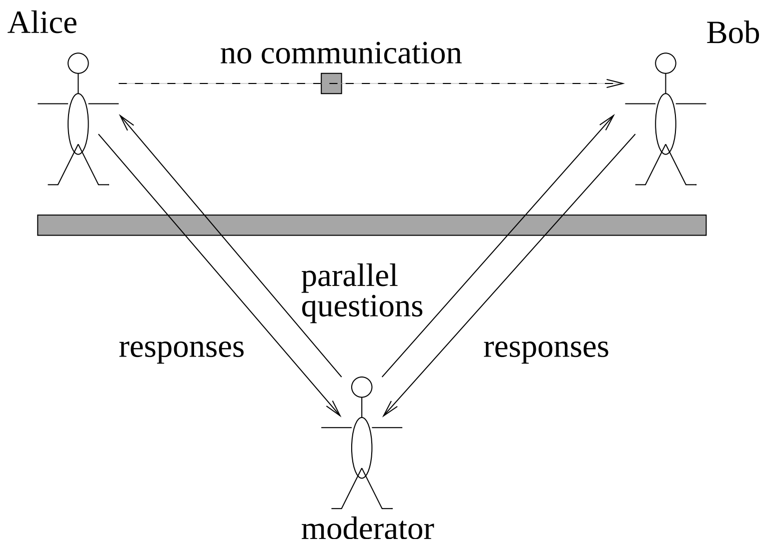


Figure 7: Setting for “colour-food” game

The audience observes that their answers satisfy the following conditions:

- If both players are asked color-questions then in about 9% of cases they answer **green**.
- If one of the players is asked the color-question and answers **green** and the other is asked the food-question, then (s)he answers **peas**.
- If both are asked food-questions they never both answer **peas**.

It is not difficult to show that within the classical physics there is no way that Alice and Bob could invent a strategy for their answers, before they went to the stage, in such a way that the above mentioned behavior of them would be observed. However, there is a quantum solution, and actually quite a simple one.

SOLUTION

Let $|p\rangle$ and $|c\rangle$ be two arbitrary orthogonal states in the two-dimensional Hilbert space H_2, and let

$$|r\rangle = a|p\rangle + b|c\rangle,$$
$$|g\rangle = b|p\rangle - a|c\rangle$$

be two new (orthogonal) states.

Let Alice and Bob, at the very beginning, before they go to the stage, create a large number of pairs of particles in the state

$$|\psi\rangle = N(|r\rangle|r\rangle - a^2|p\rangle|p\rangle),$$

where N is a normalization factor, and let later each of them takes his/her particle from each pair with him/her to the stage.

If any of them is asked the color-question, then (s)he measures his/her particle with respect to the $\{|r\rangle, |g\rangle\}$-basis and answers in accordance with the result of measurement.

If any of them is asked the food-question (s)he measures his/her particle with respect to the $\{|p\rangle, |c\rangle\}$-basis and responds in accordance with the result of measurement.

It is a not difficult exercise to show that in this way Alice's and Bob's responses follow the rules described above (9% comes from an optimization in one case).

ANSWER YOUR QUESTION PUZZLE — SOLUTION—PROOF

Case 1. Both are asked colour question. By substitution we get.

$$|\psi\rangle = N(|r\rangle|r\rangle - a^2(a|r\rangle + b|g\rangle)(a|r\rangle + b|g\rangle))$$

The coefficient at $|g\rangle|g\rangle$ is Na^2b^2 with maximum at about 9%.

Case 2. Alice is asked colour-question, Bob is asked food question.

$$|\psi\rangle = N(|r\rangle(a|p\rangle + b|c\rangle) - a^2(a|r\rangle + b|g\rangle)|p\rangle$$

There is no $|g\rangle|c\rangle$ term. This implies that probability that Alice answers green and Bob carrot is 0.

Case 3. Alice is asked colour-question, Bob is asked food question.

Solution is as above, due to the symmetry of the cases.

Case4 4. Both are asked food questions. By substitution we get

$$|\psi\rangle = N((a|p\rangle + b|c\rangle 0(a|p\rangle + b|c\rangle) - a^2|p\rangle|p\rangle)$$

Since $|p\rangle|p\rangle$ terms cancel the probability is 0 that both answers **peas**.

QUANTUM ERROR CORRECTION I

In the quantum case, information processing evolutions are far more under the negative impact of their environment, called in general *decoherence*, than in the classical computing.

The impact of decoherence is actually in all known technologies so strong, and grows exponentially in time, that till 1995 there have been strong doubts whether a powerful quantum information processing is possible at all.

A strong reason for pessimism was a belief (understanding) that in the quantum case one cannot use some quantum modification of so powerful classical error-correcting code approach.

There were several physical reasons for such a pessimism.

One of them was that in order to determine an error, we would need to measure the erroneous state, but that would irreversibly modify/destroy the erroneous state and we would have nothing to correct. Fortunately, it has turned out that there is a way out and quantum error correction can work well. The example presented in this section demonstrates the basic steps how such an error correction process can work, in principle.

QECC — EXAMPLE

Example of a qubit communication process through a noisy channel using a 3-qubit bit-error correction code.

Alice: encoding. Alice encodes the qubit $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ by a network of two XOR gates and two additional qubits in the ancilla state $|00\rangle$ into the entangled state $\alpha|000\rangle + \beta|111\rangle$, see Figure.

Noisy channel. A bit error is assumed to occur with probability $p < \frac{1}{2}$ on any qubit and results in one of the states shown bellow:

resulting state	its probability
$\alpha\|000\rangle + \beta\|111\rangle$	$(1-p)^3$
$\alpha\|100\rangle + \beta\|011\rangle$	$p(1-p)^2$
$\alpha\|010\rangle + \beta\|101\rangle$	$p(1-p)^2$
$\alpha\|001\rangle + \beta\|110\rangle$	$p(1-p)^2$
$\alpha\|110\rangle + \beta\|001\rangle$	$p^2(1-p)$
$\alpha\|101\rangle + \beta\|010\rangle$	$p^2(1-p)$
$\alpha\|011\rangle + \beta\|100\rangle$	$p^2(1-p)$
$\alpha\|111\rangle + \beta\|000\rangle$	p^3

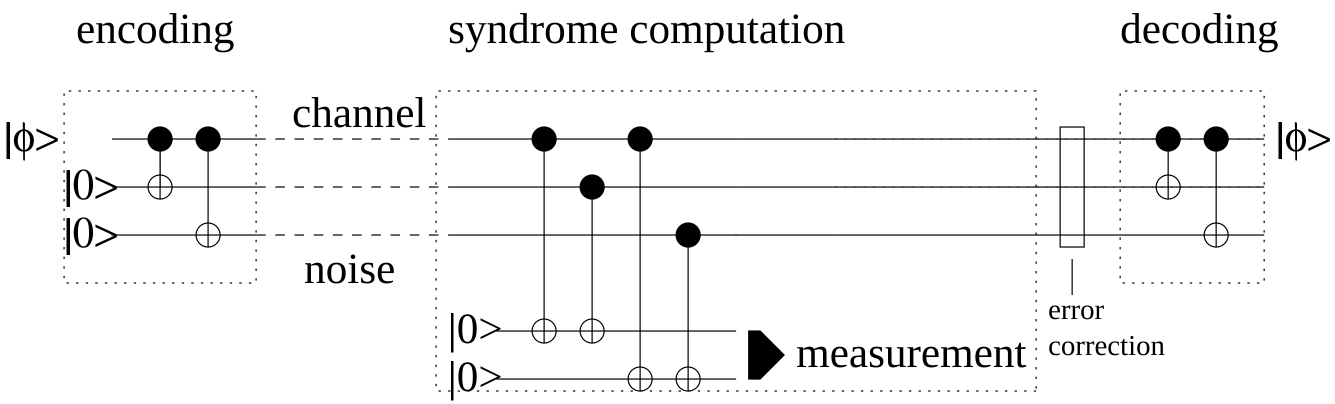
BOB: Syndrome computation process: By using two additional ancilla qubits in state $|00\rangle$ and four XOR operations syndromes of errors can be computed as shown in the following table

resulting state	its probability
$(\alpha\|000\rangle + \beta\|111\rangle)\|00\rangle$	$(1-p)^3$
$(\alpha\|100\rangle + \beta\|011\rangle)\|11\rangle$	$p(1-p)^2$
$(\alpha\|010\rangle + \beta\|101\rangle)\|10\rangle$	$p(1-p)^2$
$(\alpha\|001\rangle + \beta\|110\rangle)\|01\rangle$	$p(1-p)^2$
$(\alpha\|110\rangle + \beta\|001\rangle)\|01\rangle$	$p^2(1-p)$
$(\alpha\|101\rangle + \beta\|010\rangle)\|10\rangle$	$p^2(1-p)$
$(\alpha\|011\rangle + \beta\|100\rangle)\|11\rangle$	$p^2(1-p)$
$(\alpha\|111\rangle + \beta\|000\rangle)\|00\rangle$	p^3

Error correction. Bob does nothing if syndrome is 00 and performs σ_x operation

on third qubit if syndrome is 01
on second qubit if syndrome is 10
on first qubit if syndrome is 11

Resulting state is either $\alpha|000\rangle + \beta|111\rangle$ or $\beta|000\rangle + \alpha|111\rangle$.
Final decoding provides either the state $\alpha|0\rangle + \beta|1\rangle$ or the state $\beta|0\rangle + |1\rangle$.


encoding
syndrome computation
decoding
|ϕ>
|0>
|0>
channel
noise
|0>
|0>
measurement
error
correction
|ϕ>

BELL THEOREM

de Broglie (1927) and Bohm (1952) developed a hidden variable interpretation (theory)[3] of quantum mechanics. Einstein rejected it because it was inherently non-local.

Bell theorem, proved by Bell,says that each hidden variable theory of quantum mechanics has to be non-local.

Bell proved his theorem using a Gedanken experiment at which locally separated particles were measured and has shown that the average values of certain variables have then to satisfy certain inequalities, called in general *Bell inequalities*, provided a non-local theory of hidden variables holds and that these inequalities should be violated in case quantum mechanics with non-local effects hold.

As discussed later, various experiments confirmed violations of various Bell inequalities. This will be dealt with in more details in some of other chapters.

[3] Such a theory is often described as a theory in which individual quantum systems are described by classical parameters and they are responsible for randomness that appears in quantum experiments.

BELL THEOREM without BELL INEQUALITIES

there is a way to prove Bell theorem, one of the main outcome of quantum mechanics, also without Bell inequalities.

Let us assume that three photons are created in the state

$$\frac{1}{2}(|000\rangle - |011\rangle - |101\rangle - |110\rangle)$$

and photons move in three different directions where they are measured with respect to the standard ($\mathcal{B}$) or the dual basis ($\mathcal{D}$).

If we take results of the measurement as being 1 for $|0\rangle$ or $|0'\rangle$ and -1 for $|1\rangle$ or $|1'\rangle$ and $A(.,\lambda)$, $B(.,\lambda)$ and $C(.,\lambda)$ denotes the results of the measurement of the first, second and third photon in the appropriate basis submitted for the first parameter (with λ standing again for hidden variables), then it is easy to see that the product of the values of A,, B and C at different measurements have the following values

$$A(\mathcal{B},\lambda)B(\mathcal{B},\lambda)C(\mathcal{B},\lambda) = +1$$

$$A(\mathcal{B},\lambda)B(\mathcal{D},\lambda)C(\mathcal{D},\lambda) = -1$$

$$A(\mathcal{D},\lambda)B(\mathcal{B},\lambda)C(\mathcal{D},\lambda) = -1$$

$$A(\mathcal{D},\lambda)B(\mathcal{D},\lambda)C(\mathcal{B},\lambda) = -1$$

In the case there are no nonlocal influences the result of one measurement cannot influence the other two and therefore we can assume that values of variables A, B and C appearing in different equations for the same basis are the same. We can then multiply the left and the right sides of all four equalities. However, the product of the left sides gives the value 1 because each value appears there twice and the product of the right sides gives the value -1. A contradiction.