QUANTUM COMPUTING 2.

Jozef Gruska

Faculty of Informatics
Brno
Czech Republik

March 25, 2000

2. QUBITS and QUANTUM REGISTERS

In this chapter basic concepts concerning quantum qubits and quantum registers are presented and explored. Main quantum resources such as superposition, parallelism and entanglement are analysed. No-cloning theorem is formulated and proven.

CLASSICAL versus QUANTUM COMPUTING

The essence of the difference
between
classical computers and **quantum computers**

is in the way information is stored and processed.

In **classical computers**, information is represented on **macroscopic level** by **bits**, which can take one of the two values

$$0 \quad \text{or} \quad 1$$

In **quantum computers**, information is represented on **microscopic level** using **qubits**, which can take on any from uncountable many values

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

where α, β are arbitrary complex numbers such that

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

QUBITS

A **qubit** is a quantum state in H_2

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

where $\alpha, \beta \in \mathbf{C}$ are such that $|\alpha|^2 + |\beta|^2 = 1$ and

$$\{|0\rangle, |1\rangle\} \quad \text{is a } \textbf{(standard) basis} \text{ of } \; H_2$$

EXAMPLE: Representation of qubits by

(a) electron in a Hydrogen atom

(b) a spin-$\frac{1}{2}$ particle

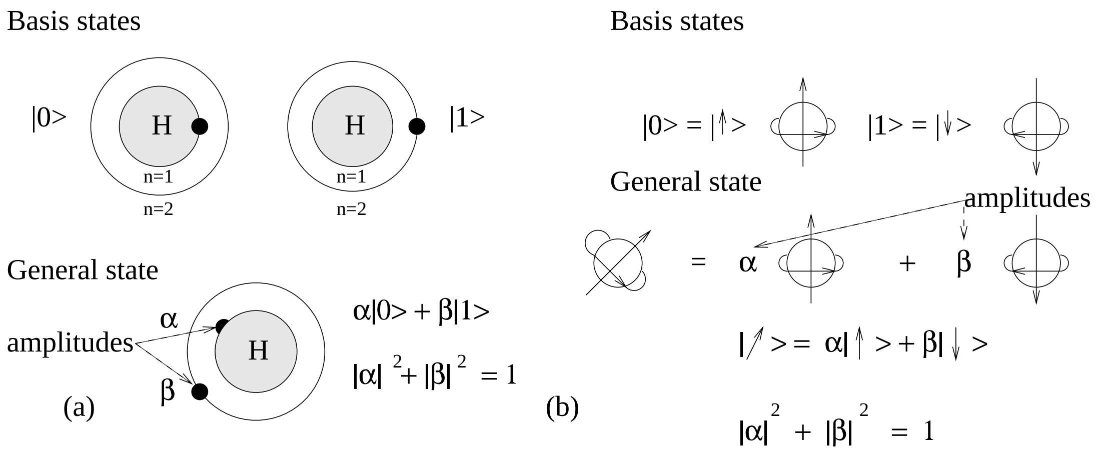


Figure 1: Qubit representations by energy levels of an electron in a hydrogen atom and by a spin-$\frac{1}{2}$ particle. The condition $|\alpha|^2 + |\beta|^2 = 1$ is a legal one if $|\alpha|^2$ and $|\beta|^2$ are to be the probabilities of being in one of two basis states (of electrons or photons).

HILBERT SPACE H_2

STANDARD BASIS

$|0\rangle, |1\rangle$

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

DUAL BASIS

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

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

Hadamard matrix

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

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

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

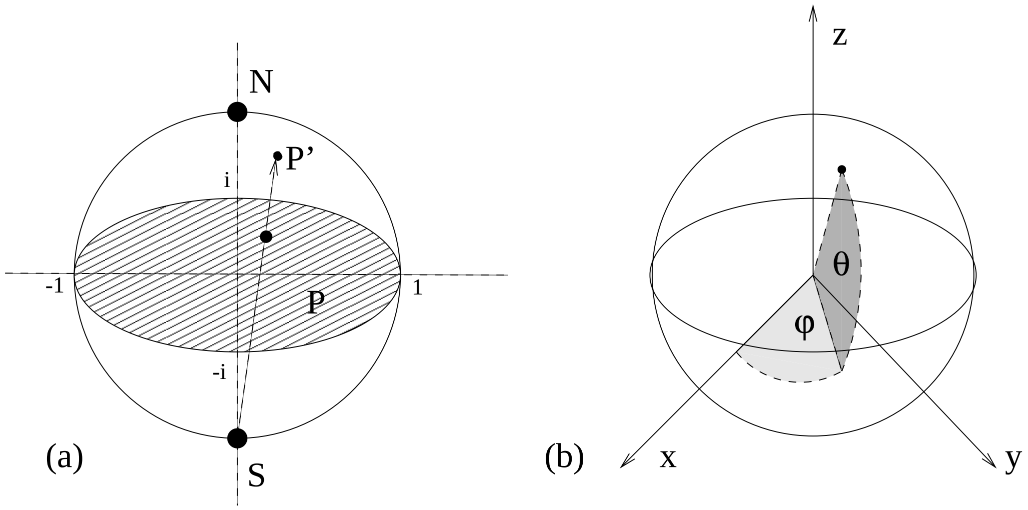
transforms
one of the basis into another one.

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 (that correspond to 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 centre 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).

MYSTERIOUS WARNING

A quantum system is a useful abstraction which frequently appears in the literature, but does not really exists in nature.

A. Peres (1993)

Some scientists are happy with the view that quantum theory provides only calculaton procedures for computing probabilities and not an objective picture of the physical world.

QUANTUM MEASUREMENT

of a qubit state

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

By a **measurement** of the qubit state

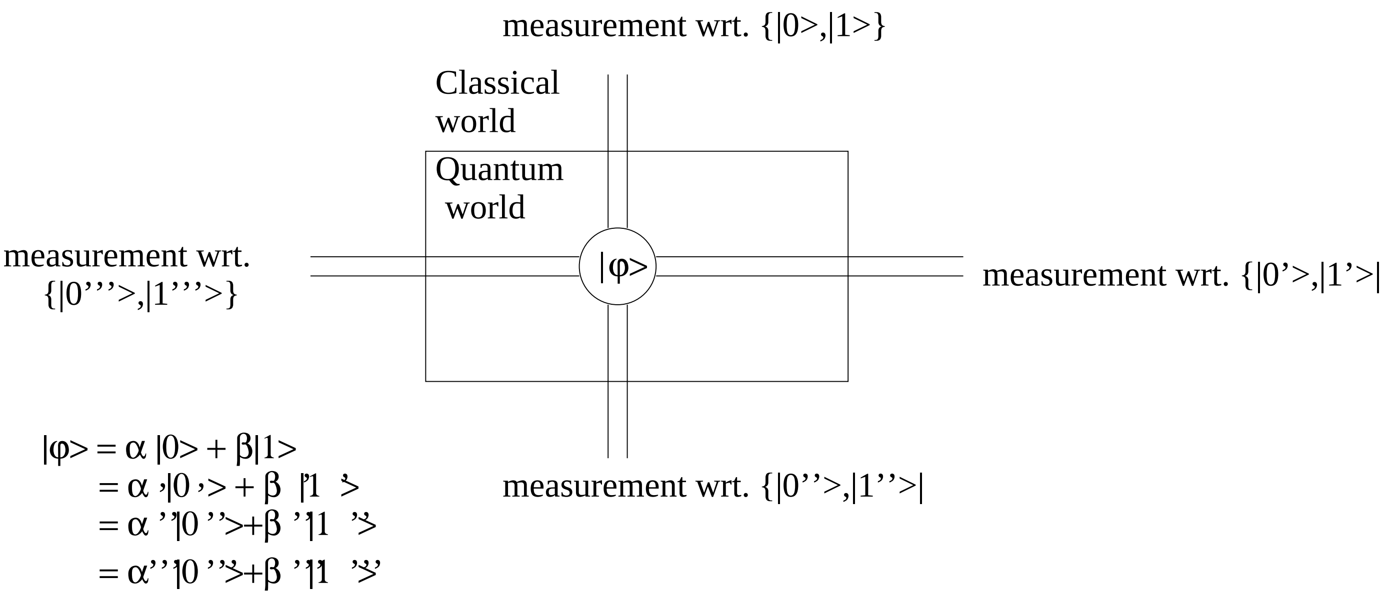
$$\alpha|0\rangle + \beta|1\rangle$$

with respect to the basis

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

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

$$0 \text{ with probability } |\alpha|^2$$
$$1 \text{ with probability } |\beta|^2$$



EXAMPLE 1

If the state

$$|0\rangle$$

is measured with respect to the standard 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 $\frac{1}{2}$ 1 with probability $\frac{1}{2}$

and the state collapses into

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

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

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

or

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

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

$$0 \text{ with probability } \tfrac{1}{2}|\alpha+\beta|^2$$

alebo

$$1 \text{ with probability } \tfrac{1}{2}|\alpha-\beta|^2$$

MEASUREMENT in CLASSICAL and 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.

QUANTUM 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.

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

An important unitary matrix of degree 4, to transform states of 2-qubit registers:

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

It holds:

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

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

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

BELL STATES

States

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

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

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.

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

   RESULTS:

   $$\begin{array}{ll} 00 & \text{with probability} \;\; |\alpha_{00}|^2 \\ 01 & \text{with probability} \;\; |\alpha_{01}|^2 \\ 10 & \text{with probability} \;\; |\alpha_{10}|^2 \\ 11 & \text{with probability} \;\; |\alpha_{11}|^2 \end{array}$$

2. Measurement of particular qubits:

   By measuring the first qubit we get

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

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

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

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

QUANTUM n-qubit REGISTER

General state of an n-qubit register has the form:

$$|\phi\rangle = \sum_{i=0}^{2^n-1} \alpha_i|i\rangle = \sum_{i\in\{0,1\}^n} \alpha_i|i\rangle, \quad \text{where} \quad \sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1$$

and $|\phi\rangle$ is a vector in H_{2^n}.

Operators on n-qubits registers are unitary matrices of degree 2^n.

Is it difficult to create a superposition of an exponential large number of basis states?

In general yes, in some important special cases not. For example, if n-qubit **Hadamard transformation**

$$H_n = \bigotimes_{i=1}^{n} H.$$

is used then

$$H_n|0^{(n)}\rangle = \bigotimes_{i=1}^{n} H|0\rangle = \bigotimes_{i=1}^{n} |0'\rangle = |0'^{(n)}\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle$$

and, in general, for $x \in \{0,1\}^n$

$$H_n|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} (-1)^{x\cdot y}|y\rangle.^{2} \tag{1}$$

[2] The dot product is defined as follows: $x \cdot y = \bigoplus_{i=1}^{n} x_i y_i$.

CAT STATES

Of importance in various areas of quantum information processing are the so-called

$$\textbf{cat states} \quad \frac{1}{\sqrt{2}}(|0^{(n)}\rangle + |1^{(n)}\rangle).$$

In the case $n = 2$ we have one of the Bell states, and in the case $n = 3$ one of the **GHZ states** (where GHZ stands for Greenberg, Horne and Zeilinger, 1998a).

In general there are eight GHZ states of the form

$$\frac{1}{\sqrt{2}}(|abc\rangle \pm |\bar{a}\bar{b}\bar{c}\rangle),$$

where $a, b, c \in \{0, 1\}$ and at most one of a, b, c is one.

PROPERTIES of n-QUBIT REGISTERS

- The number of basis states grows exponentially with n.
- In order to store an integer n one needs $\lceil \lg(n+1) \rceil$ qubits and one has to work in a Hilbert space of dimension $2^{\lceil \lg(n+1) \rceil} \geq n$.
- In spite of the fact that there are exponentially many basis states, there is a fast, linear time, access from one basis state to another.
- n-qubit register seems to be able to store exponential amount of information. However, according to the so-called **Holevo theorem**, n is the maximum number of bits that can be stored in an n-qubit register and then faithfully retrieved.

INVERSION ABOUT THE AVERAGE

This transformation will play the key role at quantum search algorithms in Chapter 6.

Example 0.1 (Inversion about the average) *The unitary transformation*

$$D_n : \sum_{i=0}^{2^n-1} a_i|\phi_i\rangle \rightarrow \sum_{i=0}^{2^n-1} (2E - a_i)|\phi_i\rangle,$$

where E is the average of $\{a_i \,|\, 0 \leq i < 2^n\}$, can be performed by the matrix[3]

$$D_n = \begin{pmatrix} -1 + \frac{2}{2^n} & \frac{2}{2^n} & \dots & \frac{2}{2^n} \\ \frac{2}{2^n} & -1 + \frac{2}{2^n} & \ddots & \frac{2}{2^n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{2}{2^n} & \frac{2}{2^n} & \dots & -1 + \frac{2}{2^n} \end{pmatrix}.$$

The matrix D_n is clearly unitary and it can be shown to have the form

$$D_n = -H_n R_n^1 H_n,$$

where

$$R_n^1[i,j] = 0 \text{ if } i \neq j, R_n^1[1,1] = -1, \text{ and } R_n^1[i,i] = 1 \text{ if } 1 < i \leq n.$$

[3]The name of the operation comes from the fact that $2E - x = E + E - x$ and therefore the new value is as much above (below) the average as it was initially below (above) the average—which is precisely the inversion about the average.

QUANTUM MEASUREMENT of STATES in H_{2^n}

If the state $|\phi\rangle$ of an n-qubit register is measured with respect to the standard basis we get as the outcome n bits, each n-tuples of bits with a pre-calculated probability, and the state $|\phi\rangle$, in the (potential) superposition of 2^n basis states, collapses to just one of the basis states.

Let us now consider a measurement of the jth qubit only.

The corresponding observable is $\mathcal{B}_j = \{E_j^0, E_j^1\}$, where E_j^0 (E_j^1) is the subspace of the 2^n-dimensional Hilbert space spanned by all basic vectors having 0 (1) in the jth component.

The measurement of the jth qubit gives

$$0 \text{ with probability } \sum_{i \,|\, i_j = 0} |\alpha_i|^2,$$

and

$$1 \text{ with probability } \sum_{i \,|\, i_j = 1} |\alpha_i|^2,$$

where i_j denotes the jth bit in the binary representation of i.

QUANTUM PARALLELISM

If

$$f : \{0, 1, \ldots, 2^n - 1\} \Longrightarrow \{0, 1, \ldots, 2^n - 1\}$$

then the mapping

$$f' : (x, 0) \Longrightarrow (x, f(x))$$

is one-to-one and therefore there is a unitary transformation U_f such that.

$$U_f(|x\rangle|0\rangle) \Longrightarrow |x\rangle|f(x)\rangle$$

Let

$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle|0\rangle$$

With a **single application** of the mapping U_f we get

$$U_f|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle|f(i)\rangle$$

IN A SINGLE COMPUTATIONAL STEP 2^n VALUES OF f ARE COMPUTED!

$\boxed{\text{QUANTUM PARALLELISM}}$

A quantum register with

200 QUBITS

can be at the same time
in a superposition of

2^{200} classical states

and with a single operation can compute
2^{200} values of a function

CONSTRUCTIVE and DESTRUCTIVE INTERFERENCE

In one computation step one can much increase or decrease the probability that by performing a projection measurement one gets a *desirable* result.

The first phenomenon is called **constructive interference** and the second is called **destructive interference**.

For example, let us consider as desirable for an n-qubit register those basis state that have at least half of ones.

By applying the Hadamard ¡transformation H_n to the state $|(0^{(n)}\rangle$ we get the state

$$|\phi\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$$

and therefore the probability of getting a desirable state, by the projection measurement, with respect to the standard basis, has increased from 0 to $\frac{1}{2}$.

On the other side, by applying to the state $|\psi\rangle$ again the Hadamard transformation H_n we get again the state $|0^{(n)}\rangle$ and therefore the probability that by projection measurement, with respect to the standard observable, we get a desirable state has decreased from $\frac{1}{2}$ to 0.

IN WHAT LIES POWER OF QUANTUM COMPUTING?

In quantum interference or in quantum parallelism?

NO

in QUANTUM ENTANGLEMENT

Let

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

be a (global) state of two
very distant particles,
for example
on two planets

QUANTUM ENTANGLEMENT

A pure state $|\phi\rangle$ of a tensor product of Hilbert spaces $H_1 \otimes \ldots \otimes H_n$ is called **entangled** if it cannot be decomposed in the form

$$|\phi\rangle = |\phi_1\rangle \otimes \ldots \otimes |\phi_n\rangle$$

where $|\phi_i\rangle$ is a pure state of H_i.

A mixed state ρ of n qubits is called (fully) **separable** if it can be decomposed as

$$\rho = \sum_i p_i \rho_i^{(1)} \otimes \ldots \otimes \rho_i^{(m)}$$

where $\sum_i p_i = 1$ and $\rho_i^{(j)}$ is a density matrix of j-th qubit for any j.

Otherwise, ρ is called **inseparable** or **entangled**.

LOCAL OPERATIONS + CLASSICAL COMMUNICATIONS

In order to manipulate entangled states several types of operations play a special role.

LOCC — local unitary operations and (two-way) classical communication.

LQCC — local quantum operations (any, including superoperators and POVM measurements) and (two-way) classical communications.[4,5]

ELQCC — entanglement-assisted local (general) quantum operations and classical communication — communicating parties are allowed, in addition to features offered by LQCC, first to "borrow" some entanglement, and then to use it for local operations and classical communication, but without consuming it.

[4] All these operations can be composed from the following ones: (a) appending an ancilla (an auxiliary quantum system), not entangled with the other subsystem; (b) unitary operations; (c) projection measurements; (d) tracing out a subsystem.

[5] Mathematically, we can represent these operations by multilocal superoperators — completely positive linear maps that do not increase trace and can be implemented locally, with classical coordination among the parties.

PARADOXICAL NATURE of ENTANGLEMENT

The source of various paradoxes related to entangled states is the fact that particles of a pair of particles in an entangled state can be much physically separated.

Each measurement on one particle of such an entangled pair "immediately determines" the state of another one, no matter how far apart they are.

A measurement of an entangled particle exhibits therefore the so-called "**non-local effect**", something that cannot happen from the point of view of classical physics without an instantaneous communication among the particles.

The concept of an entangled state is an excellent example of a difference between thinking in terms of Hilbert space constructs and dealing with real quantum systems.

Mathematically the concept of entanglement is a trivial one. Physically the existence of entangled states of distant particles is one of the most puzzling phenomena.

It was a very challenging experimental task to show experimentally entanglement of even 2 qubits.

HOW TO CREATE ENTANGLEMENT

Physically

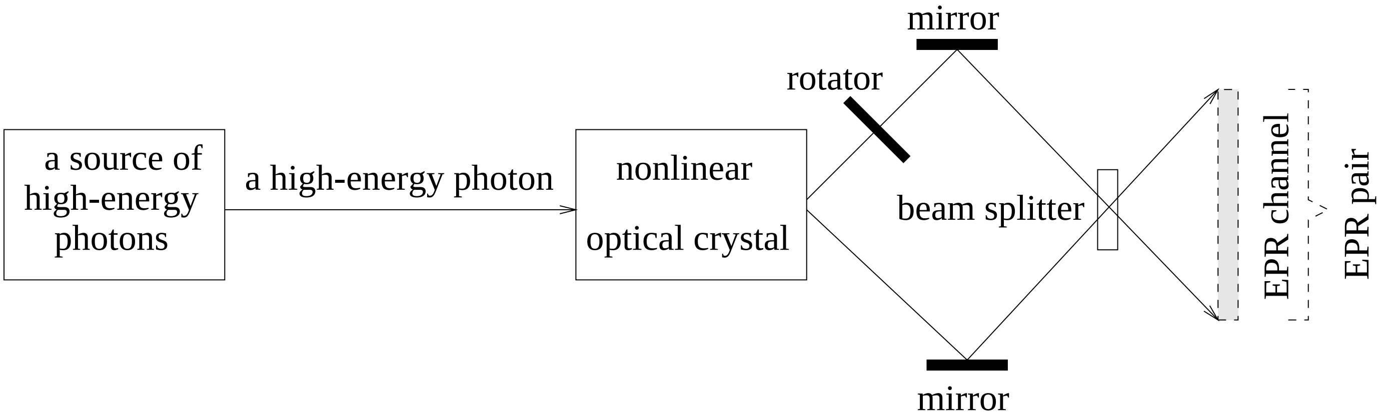


Figure 2: Generation of an EPR pair of polarized photons and an EPR-channel, adopted from Glanz (1995).

By a quantum operation

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

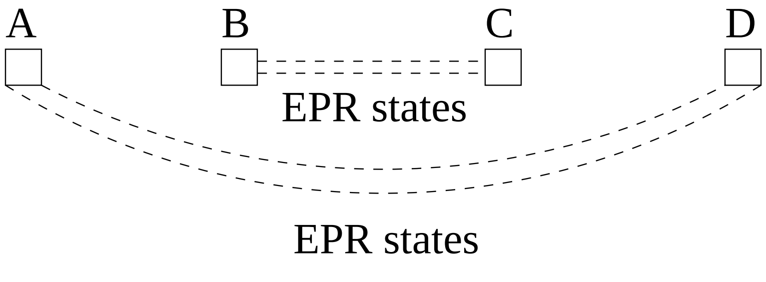
By a quantum measurement

ENTANGLEMENT SWAPPING

Entanglement swapping is a method to make, by measurement, entangled particles that have never interacted before.

Let particles A and B as well as particles C and D are in the EPR state.

In the case ons states of particles B and C Bell measurement is performed the particles B aand C as well as particles A and D get entangled.



FIDELITY

(Similarity of quantum states.)

For pure states $|\phi\rangle$a and $|\psi\rangle$:

$$F(\phi, \psi) = |\langle\phi \mid \psi\rangle|^2.$$

If $|\phi\rangle$ is a pure state and ρ is a mixed state, then

$$F(\phi, \rho) = |\langle\phi \mid \rho\phi\rangle|^2.$$

Transmission fidelity, for the case that a quantum channel produces on each pure state $|\phi_i\rangle$, produced with probability p_i an output mixed state ρ_i, is

$$F = \sum_i p_i \langle\phi_i|\rho_i\phi_i\rangle.$$

$\boxed{\text{EXTRAS}}$

SUBSTITUTING ENTANGLEMENT for COMMUNICATION

One of the surprising applications of entanglement was discovered in the area of multiparty communications. For example, by sharing entangled particles communicating parties can reduce the amount of bits they need to broadcast in order to compute together a function whose input data are distributed among the parties.

There are k parties $P_1, \ldots, P_k$ and a k-variable function f whose inputs are n-bit strings $x_1, \ldots, x_k$. The party P_j holds only the string x_j. All parties want to compute together $f(x_1, \ldots, x_k)$. To achieve that parties have to communicate.

The average number of bits the parties have to broadcast if they work with classical information only, for valid inputs of length n, is called the communication complexity of f and denoted by $C(f, n, k)$.

For the case where the parties can work also with quantum information, the corresponding communication complexity is denoted by $QC(f, n, k)$.

We show an example of functions $f_k, k = 1, 2, \ldots$ such that $QC(f_k, n, k)$ is asymptotically smaller, with respect to k, than $C(f_k, n, k)$.

EXAMPLE

An input $(x_1, \ldots, x_k) \in \{0, \ldots, 2^n - 1\}^k$ is defined to be **valid** if

$$\left(\sum_{i=1}^{k} x_i\right) \bmod 2^{n-1} = 0.$$

Denote by $f_k : \{0, \ldots, 2^n - 1\}^k \to \{0, 1\}$, the Boolean function defined, on valid inputs only, by

$$f_k(x_1, \ldots, x_k) = \left(\frac{1}{2^{n-1}} \sum_{i=1}^{k} x_i\right) \bmod 2.$$

Clearly, $f_k(x_1, \ldots, x_k) \in \{0, 1\}$ for all valid inputs.

We show that $QC(f_k, n, k) = k$ provided k communicating parties share k entangled qubits, each party one. The book contains a proof that $C(f_k, n, k) \geq k \lg k - k$ for $n \geq \lg k$.

Let us assume that k parties share k qubits, the party P_i the qubit q_i and together these qubits are in the entangled state

$$|q_1 \ldots q_k\rangle = \frac{1}{\sqrt{2}}(|0^{(k)}\rangle + |1^{(k)}\rangle).$$

Let each party P_j, independently, apply on its qubit q_j the following procedure.

1. A phase-changing transformation

$$|0\rangle \to |0\rangle, \quad |1\rangle \to e^{\frac{2\pi i x_j}{2^n}}|1\rangle.$$

2. Hadamard transformation.

3. A measurement of the jth qubit q_j, with respect to the standard observable $\{|0\rangle, |1\rangle\}$, providing an output $b_j \in \{0, 1\}$.

After the first step the resulting state is

$$\frac{1}{\sqrt{2}}\left(|0^{(k)}\rangle + (e^{\frac{2\pi i}{2^n}\sum_{j=1}^{k}x_j})|1^{(k)}\rangle\right).$$

(Observe that for a valid input $e^{\frac{2\pi i}{2^n}\sum_{j=1}^{k}x_j}$ equals 1 or -1.) After the second step the resulting state is

$$\frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2^k}}\sum_{j=0}^{2^k-1}|j\rangle + e^{\frac{2\pi i}{2^n}\sum_{j=1}^{k}x_j}\frac{1}{\sqrt{2^k}}\sum_{j=0}^{2^k-1}(-1)^{parity(j)}|j\rangle\right),$$

where $parity(j) = 0$ if j is even and 1, otherwise.

Since

$$e^{\frac{2\pi i}{2^n}\sum_{j=1}^{k}x_j} = (-1)^{f_k(x_1,\ldots,x_k)}$$

we see that the resulting state is

$$\frac{1}{\sqrt{2^{k-1}}}\sum_{parity(j)=f_k(x_1,\ldots,x_n)}|j\rangle.$$

It is now easy to determine that

$$b_1 \oplus b_2 \oplus \ldots \oplus b_k = f_k(x_1,\ldots,x_k),$$

no matter in which order parties perform their measurements.