

## Foundations of quantum computing. Part I\*

SŁAWOMIR BUGAJSKI, JERZY KLAMKA, STEFAN WĘGRZYN

Institute of Theoretical and Applied Computer Science  
Polish Academy of Sciences  
44-100 Gliwice, Bałtycka 5, Poland

**Abstract:** The paper presents fundamental properties of quantum-mechanical systems essential for quantum computations. The following concepts are described in details: qubit, superposition of states, measurement, entanglement, quantum gate, quantum circuit, quantum information channel, dense coding, and others. The typical single-qubit and two-qubit gates are considered, as well as simple examples of quantum circuits.

### 1. Why quantum computers ?

Physics and information theory developed almost independently one of the other up to 80'ths of XX century, with exception of rather marginal areas of common interests like: connections between entropy and information in physics, the problem of energy spent on computation together with the related problem of reversible computation, and others. On the other hand, it seems evident now that every information-processing machine has to be a physical system operating according to laws of physics, and that every time evolution of a physical system can be considered as an information processing. Among physical systems are these which, like atoms and molecules, belong to the realm of quantum theory, so quantum computers are simply hypothetical machines that use principles of quantum mechanics for their basic operations. Thus, the idea of quantum computer appears to be a natural consequence of a theoretical reflection.

---

\*This research was supported by KBN Project no. 7 T11C 017 21

Actually, the most evident practical motivation for studying and developing the idea of quantum computation is the technological progress in producing microprocessors. Modern lithographic techniques can draw logic gates less than a micron ( $10^{-6}m$ ) on the surface of a silicon chip, while a typical size of an atom would be about  $10^{-10}m$ ; one can expect that we reach the point where logic gates will consist of only a few atoms each. Then we would enter the area governed by the laws of quantum mechanics. Thus, if computers are to continue to become faster, and therefore smaller, new quantum technology must replace what we have now. Another important motivation comes from the modern theory of information processing in living systems.

As the date of birth of the quantum computer one can assume year 1985, when D. Deutsch published his seminal paper [2] on quantum computing, and simultaneously R. P. Feynman (a Nobel Prize winner) raised similar ideas [5]. In 1989 Deutsch introduced a quantum computing model that made full use of quantum superpositions - the quantum gate array (called also the quantum circuit) [3]. The Deutsch model is not the only mathematical model for quantum computation; it is the most popular now because of its simplicity. Essentially, the Deutsch model describes quantum register as a (quantum) composite system consisting of elementary components called qubits. Quantum gate arrays became soon an object of extensive studies, nevertheless the idea remained pure speculation until 1994 when Shor invented the quantum factoring algorithm (see [4] for a review) - the discovery which initiated the recent activity in quantum computation research.

We explain here the basic concepts of quantum computing like qubit, superposition of states, measurement, two-qubit system, entanglement, quantum gate, quantum gate array, quantum information channel, dense coding, *etc.* The paper does not need any preliminary knowledge of quantum mechanics, it should be comprehensible to a reader familiar with complex vector spaces and matrices.

## 2. Qubit

The most striking difference between classical and quantum mechanics is that the former represents states of a pertinent physical object by points of some set (a phase space), whereas the latter describes them as vectors of a complex linear space. Thus, states of a quantum system "are" vectors of a suitable complex space: in the general case this is the abstract (infinitely dimensional) Hilbert space. The linear structure of the space of states of a quantum system is commonly referred to as the *superposition principle*, and considered to be one of the basic features of the theory. In fact, all the peculiar features of quantum

mechanics result from the superposition principle.

It should be stressed that the numerous peculiarities and "paradoxes" of the quantum mechanical world do not indicate that the theory itself is wrong or incomplete. Quantum mechanics is the greatest achievement of science of the last century, it lays foundations for all the modern physics, while its predictions are confirmed by numerous experiments with an astonishing accuracy. The counter-intuitive character of quantum mechanics should be seen as a result of the fact that we have no direct insight into the area of reality the theory refers to.

### 2.1. State space

Qubit is the simplest quantum system; its states are vectors of 2-dimensional complex linear space, so the vectors of  $\mathbb{C}^2$ . Strictly speaking, every quantum mechanical physical system needs for its full description the infinitely dimensional Hilbert space. It is feasible, however, that we are interested only in some particular properties of the quantum physical object; in such a case a "smaller" vector space can be sufficient. There are various physical properties which quantum mechanics describes by means of the 2-dimensional space  $\mathbb{C}^2$ , the most popular one is called *spin*  $\frac{1}{2}$ . Hence qubits are often called "spins" or "spin-half systems".

The *canonical base* of the linear space  $\mathbb{C}^2$  consists of the two orthogonal vectors  $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$  and  $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ ; quantum mechanics traditionally applies the so-called *bra and ket notation*, so the two vectors will be denoted  $|0\rangle$  and  $|1\rangle$  respectively. Clearly, any vector  $|v\rangle$  of  $\mathbb{C}^2$  is a linear superposition of the base vectors  $|0\rangle$  and  $|1\rangle$ :

$$|v\rangle = v_0 |0\rangle + v_1 |1\rangle,$$

so is represented by the pair of its components arranged into the column  $\begin{pmatrix} v_0 \\ v_1 \end{pmatrix}$ .

The inner product of two vectors  $|v\rangle$  and  $|w\rangle$  is denoted  $\langle v|w\rangle$ , and defined by

$$\langle v|w\rangle := \begin{pmatrix} v_0^* & v_1^* \end{pmatrix} \begin{pmatrix} w_0 \\ w_1 \end{pmatrix} = v_0^* w_0 + v_1^* w_1,$$

where star means complex conjugation. Hence, coefficients of the decomposition  $|v\rangle = v_0 |0\rangle + v_1 |1\rangle$  are inner products:

$$v_0 = \langle 0|v\rangle, \quad v_1 = \langle 1|v\rangle.$$

Vectors of  $\mathbb{C}^2$  can represent, according to general rules of quantum mechanics, states of the quantum object. (States and the corresponding vectors are identified.) Accordingly, the two-dimensional complex linear space  $\mathbb{C}^2$  is called the

state space of the qubit. The two-dimensionality of the state space of qubit makes some authors to call qubit a "two-state quantum system".

We will need also the concept of an *operator* on  $\mathbb{C}^2$ . An operator on  $\mathbb{C}^2$  (in fact, a linear operator) is a linear map  $\widehat{O} : \mathbb{C}^2 \rightarrow \mathbb{C}^2$ . Any complex  $2 \times 2$  matrix  $\widehat{M}$  defines an operator on  $\mathbb{C}^2$  : an arbitrary vector  $|v\rangle \in \mathbb{C}^2$  is transformed into

$$\begin{aligned}\widehat{M}|v\rangle &= \begin{pmatrix} M_{00} & M_{01} \\ M_{10} & M_{11} \end{pmatrix} \begin{pmatrix} v_0 \\ v_1 \end{pmatrix} \\ &= \begin{pmatrix} M_{00}v_0 + M_{01}v_1 \\ M_{10}v_0 + M_{11}v_1 \end{pmatrix} \in \mathbb{C}^2.\end{aligned}$$

The matrix elements of  $\widehat{M}$  can be expressed as:

$$M_{00} = \langle 0 | \widehat{M} | 0 \rangle, \quad M_{01} = \langle 0 | \widehat{M} | 1 \rangle, \quad \text{etc.}$$

If we fix the canonical base, we do not need to distinguish between operators on  $\mathbb{C}^2$  and complex  $2 \times 2$  matrices.

The bra-ket notation provides a convenient description for some operators: the symbol  $|u\rangle\langle v|$  is understood as the operator acting on an arbitrary vector  $|w\rangle$  in the following way:

$$|u\rangle\langle v| |w\rangle := \langle v | w \rangle |u\rangle.$$

It is easy to find that the operator  $|v\rangle\langle v|$  for a normalized vector  $|v\rangle$  is simply the orthogonal projection onto the one-dimensional subspace determined by  $|v\rangle$ .

In particular:

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

## 2.2. Observables of a qubit

Experimentally measurable properties of a quantum-mechanical object are traditionally called *observables*. In the considered case of a qubit they are represented by self-adjoint operators on the state space  $\mathbb{C}^2$ , *i.e.* by  $2 \times 2$  complex self-adjoint matrices. An operator

$$\widehat{Q} = \begin{pmatrix} Q_{00} & Q_{01} \\ Q_{10} & Q_{11} \end{pmatrix}$$

is called *self-adjoint* if it satisfies the condition:

$$\widehat{Q} = \widehat{Q}^*,$$

or equivalently, if:

$$\begin{aligned} Q_{00}^* &= Q_{00}, \\ Q_{11}^* &= Q_{11}, \\ Q_{01}^* &= Q_{10}. \end{aligned}$$

Notice that  $Q_{00}^*$  is the complex conjugate of the complex number  $Q_{00}$ , while  $\widehat{Q}^*$  is the matrix adjoint to  $\widehat{Q}$  (*i.e.* transposed and complex conjugated). Physicists agree that any self-adjoint operator on  $\mathbb{C}^2$  represents a measurable physical property of the qubit.

Crucial for the physical interpretation of self-adjoint operators are their eigenvectors and eigenvalues. A vector  $|w\rangle$  of  $\mathbb{C}^2$  is an *eigenvector* of a self-adjoint operator  $\widehat{Q}$  if it satisfies the equation

$$\widehat{Q}|w\rangle = q|w\rangle$$

for an appropriate number  $q$ , which is called an *eigenvalue* of  $\widehat{Q}$  corresponding to the eigenvector  $|w\rangle$ . It is a common convention that an eigenvector corresponding to the eigenvalue  $q$  is denoted  $|q\rangle$ , so the last equation should have the form:

$$\widehat{Q}|q\rangle = q|q\rangle$$

It is easy to check that a self-adjoint matrix  $2 \times 2$  always has two eigenvalues (which could be equal).

It should be stressed that eigenvalues of a self-adjoint operator are always real numbers. Eigenvectors corresponding to different eigenvalues have to be orthogonal:

$$q_1 \neq q_2 \Rightarrow \langle q_1 | q_2 \rangle = 0.$$

If  $q_1 = q_2 = q$ , then  $\widehat{Q}$  is proportional to the identity operator (the unit matrix):

$$\widehat{Q} = q \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = q\widehat{1},$$

so every vector of  $\mathbb{C}^2$  is an eigenvector of such a particular operator; then one says that the eigenvalue  $q$  is *degenerate*.

The mentioned above projection operator  $|v\rangle\langle v|$  is self-adjoint. Its eigenvalues are 0 and 1, the eigenvector corresponding to 1 is just  $|v\rangle$ .

### 2.3. The minimal interpretation

The connection between the abstract algebra of operators and vectors, and results of physical experiments is provided by the following rule (which is a single-qubit version of the so called *minimal interpretation* of quantum mechanics):

Given a vector  $|v\rangle \in \mathbb{C}^2$  which represents a state of a qubit, and a self-adjoint operator  $\widehat{Q}$  representing a physical quantity (an observable) relevant to the qubit. Eigenvalues  $q_1, q_2$  of  $\widehat{Q}$  are the values of the physical quantity, while  $|\langle q_1|v\rangle|^2$  and  $|\langle q_2|v\rangle|^2$ , where  $|q_1\rangle, |q_2\rangle$  are the eigenvectors corresponding to  $q_1, q_2$ , are probabilities for outcomes  $q_1, q_2$  to occur if a measurement of the observable  $\widehat{Q}$  is performed on the object in the state  $|v\rangle$ .

The minimal interpretation has profound consequences. Probabilities in physics emerge as limits of relative frequencies of results of single trials. Thus, they are to be calculated from a long series of such single trials, which constitutes the proper measurement of the physical quantity in question. One should be aware that the two concepts:

- a single act of measurement (a trial) which results randomly in one of eigenvalues, and
  - a proper measurement (a long series of single trials) which provides probabilities of obtaining the particular eigenvalues,
- are often mixed together and / or misinterpreted.

Thus, a measurement of the observable  $\widehat{Q}$ , performed on the object in the state  $|v\rangle$  consists of a long series (a long run) of single acts of measurement (trials). Every single trial should result in one of the eigenvalues of  $\widehat{Q}$ , because the eigenvalues of  $\widehat{Q}$  are the values the physical quantity (represented by  $\widehat{Q}$ ) can have; therefore a quantum object described in  $\mathbb{C}^2$  (a qubit) can have only two-valued physical properties.

The outcomes of single trials appear at random. If the two eigenvalues of  $\widehat{Q}$  are distinct,  $q_1 \neq q_2$ , then the probability of obtaining  $q_i$  in a single trial is  $|\langle q_i|v\rangle|^2$ ,  $i = 1, 2$ . It can happen that the pre-measurement state  $|v\rangle$  is just one of the eigenstates of the measured observable, say  $|q_1\rangle$ . Then the results of single trials are always  $q_1$ , because  $\langle q_1|q_1\rangle = 1$  and  $\langle q_2|q_1\rangle = 0$ .

### 2.4. Probabilities

The interpretation of numbers  $|\langle q_i|v\rangle|^2$  as probabilities is possible only if they satisfy the condition

$$|\langle q_1|v\rangle|^2 + |\langle q_2|v\rangle|^2 = 1.$$

A validity of this condition is assured in quantum mechanics by the special assumption of normalization, which for a qubit has the form: a vector  $|v\rangle$  represents a state if it satisfies the *normalization condition*:

$$|\langle v|v\rangle|^2 = 1,$$

or in the explicit form:

$$|v_1|^2 + |v_2|^2 = 1.$$

Vectors satisfying the normalization condition are called *normalized*.

Thus, the numbers  $|\langle q_1|v\rangle|^2, |\langle q_2|v\rangle|^2$  would be correct probabilities if the two eigenvectors  $|q_1\rangle, |q_2\rangle$ , and the vector  $|v\rangle$  are normalized. Every non-zero vector can be transformed into a normalized one simply by multiplying it by an appropriate complex number. Since now on, all the vectors considered will be assumed normalized. The inner products  $\langle q_1|v\rangle, \langle q_2|v\rangle$  are called *probability amplitudes*, because their relation to probabilities  $|\langle q_1|v\rangle|^2, |\langle q_2|v\rangle|^2$  resembles the relation between Schrödinger wave function and the corresponding probability density.

The *mean value* (the expectation) of the observable  $\widehat{Q}$  is defined by:

$$\langle \widehat{Q} \rangle := q_1 |\langle q_1|v\rangle|^2 + q_2 |\langle q_2|v\rangle|^2.$$

The mean value can be also calculated in another way:

$$\begin{aligned} \langle \widehat{Q} \rangle &= \langle v|\widehat{Q}|v\rangle := \begin{pmatrix} v_0^* & v_1^* \end{pmatrix} \begin{pmatrix} Q_{00} & Q_{01} \\ Q_{10} & Q_{11} \end{pmatrix} \begin{pmatrix} v_0 \\ v_1 \end{pmatrix} \\ &= Q_{00}v_0^*v_0 + Q_{01}v_0^*v_1 + Q_{10}v_1^*v_0 + Q_{11}v_1^*v_1. \end{aligned}$$

## 2.5. States and ensembles

Recall that the minimal interpretation implies the following picture of quantum measurement: a measurement of the observable  $\widehat{Q}$ , performed on the object in the state  $|v\rangle$  consists of a long series of single acts of measurement (trials). A short consideration shows that this should also imply a specific concept of quantum state.

In order to execute a long series of single acts of measurement, we should have an appropriate collection of single samples of the quantum object under investigation; the samples (copies) should be mutually independent one of the other and all prepared in the same manner.. Such a collection is called in physics a *statistical ensemble*. Thus, a state of a quantum object is present in any measurement as a statistical ensemble of identically prepared and mutually independent copies.

This leads to an identification of states and ensembles: quantum state can be understood just as a statistical ensemble. This ensemble interpretation of quantum states, which seems to be a direct consequence of the minimal interpretation, will be assumed from now on.

Clearly, all single copies belonging to the same ensemble "are" in the same state. Thus, if we say that a single copy of a quantum object "is" in some state, we mean that this copy is, or can be a member of a statistical ensemble corresponding to this state.

## 2.6. Post-measurement states

Thus, a measurement of an observable  $\hat{Q}$ , performed on the spin-half object in a state  $|v\rangle$  provides the two probabilities  $|\langle q_1|v\rangle|^2$ ,  $|\langle q_2|v\rangle|^2$  which tell us how often the values  $q_1$ ,  $q_2$  appear in single trials. What happens then to the original spin-half object ?

Typically, the pre-measurement ensemble is destroyed during the process of measurement, so that all its single members are absorbed or scattered-off by the measuring apparatus in an uncontrolled way. However, the most popular formal model of the process of measurement, proposed by J. von Neumann in 1932 [6], assumes that all members of the pre-measurement ensemble survive the interaction with the measuring apparatus. In the *von Neumann measurement* (called also the standard measurement), all single copies of the quantum object which form the pre-measurement statistical ensemble are transformed randomly from the original state  $|v\rangle$  into one of the two eigen-states  $|q_1\rangle$  or  $|q_2\rangle$ , with probability  $|\langle q_1|v\rangle|^2$  or  $|\langle q_2|v\rangle|^2$  respectively. This is the reason why the numbers  $|\langle q_1|v\rangle|^2$ ,  $|\langle q_2|v\rangle|^2$  are often called *transition probabilities*. Notice that in the case of  $|v\rangle = |q_1\rangle$ , the post-measurement state in the von Neumann-type measurement is again  $|q_1\rangle$ ; this observation will appear essential below. In the case of degeneracy  $q_1 = q_2$ , the von Neumann measurement does not change  $|v\rangle$ .

Thus, the von Neumann measurement would in general transform the pre-measurement state  $|v\rangle$  into the statistical mixture of the two eigenstates with probabilities  $|\langle q_1|v\rangle|^2$  and  $|\langle q_2|v\rangle|^2$ ; statistical mixtures of states like that are called *mixed states*. One should be aware that the von Neumann model is often considered in an exaggerated manner as a paradigm for any quantum measurement; in fact it is merely a highly idealized formal model applicable to measurements of a very special kind.



### 2.7. Superpositions and probability amplitudes

Notice, that the two orthogonal and normalized eigenstates  $|q_1\rangle$  and  $|q_2\rangle$  of a self-adjoint operator  $\hat{Q}$  form a new base in  $\mathbb{C}^2$ . Any (normalized) vector  $|v\rangle$  decomposes then into the superposition (the linear combination) of  $|q_1\rangle$  and  $|q_2\rangle$  :

$$|v\rangle = z_1 |q_1\rangle + z_2 |q_2\rangle ;$$

it is easy to find that the coefficients of the superposition are probability amplitudes:

$$z_1 = \langle q_1 | v \rangle, \quad z_2 = \langle q_2 | v \rangle ;$$

thus their square moduluses are equal to transition probabilities. This suggests a connection with the von Neumann measurement, and is the source of the popular interpretation of the superposition: the quantum object in the state

$$|v\rangle = \langle q_1 | v \rangle |q_1\rangle + \langle q_2 | v \rangle |q_2\rangle$$

is told to be "in  $|q_1\rangle$  and in  $|q_2\rangle$  at the same time", what is one of so called "weird" features of quantum objects.

Our discussion indicates that the mentioned interpretation is unfounded. What we are allowed to say is merely this: if the qubit would be in the state  $|v\rangle$  which is a superposition of eigenstates  $|q_1\rangle, |q_2\rangle$  of an observable  $\hat{Q}$ , and we would perform a von Neumann-type measurement of  $\hat{Q}$ , then single samples would leave the measuring apparatus randomly in states  $|q_1\rangle$  or  $|q_2\rangle$  with probabilities  $|\langle q_1 | v \rangle|^2, |\langle q_2 | v \rangle|^2$  respectively. It is natural to consider the measurement interaction as the physical cause of the transition from  $|v\rangle$  to the statistical mixture of  $|q_1\rangle$  and  $|q_2\rangle$ , so there is no reason to claim that the qubit prior to a von Neumann measurement of  $\hat{Q}$  "was" in the two states  $|q_1\rangle$  and  $|q_2\rangle$  simultaneously.

### 2.8. Some simple observables of a spin-half system

We will illustrate the introduced concepts on the basic observables of a spin-half object.

The two base vectors  $|0\rangle, |1\rangle$  can be considered as the two eigenvectors of some observable. A physically meaningful choice is the operator

$$\hat{S}_z = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

(we take, for the sake of simplicity, the Planck constant  $\hbar = 1$ ), the physical quantity represented by  $\hat{S}_z$  is called the *z-th component* of the spin half. Now,

$|0\rangle$  is the eigenstate of  $\widehat{S}_z$  corresponding to the eigenvalue  $\frac{1}{2}$ , while  $|1\rangle$  is the eigenstate of  $\widehat{S}_z$  corresponding to the eigenvalue  $-\frac{1}{2}$ . Hence, if we would measure the  $z$ -th component of the spin half on the object prepared in the state  $|0\rangle$ , we would get the final probability distribution concentrated at  $\frac{1}{2}$ . This explains why physicists call  $|0\rangle$  the *spin-up state*, for similar reason  $|1\rangle$  is called the *spin-down state*.

Notice that the quantum observable  $\widehat{S}_z$  equals (up to a factor) the third one of the *Pauli matrices*:

$$\widehat{\sigma}_x := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \widehat{\sigma}_y := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \widehat{\sigma}_z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \widehat{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Pauli matrices  $\widehat{\sigma}_x, \widehat{\sigma}_y$  represent other components of spin half:

$$\widehat{S}_x = \frac{1}{2} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \widehat{S}_y = \frac{1}{2} \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}.$$

An immediate calculation shows that

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

are eigenstates of  $\widehat{S}_x$  corresponding to eigen-values  $\frac{1}{2}$  and  $-\frac{1}{2}$  respectively.

Mean values of  $\widehat{S}_x$  and of  $\widehat{S}_y$  in the state  $|0\rangle$  are:

$$\langle 0 | \widehat{S}_x | 0 \rangle = 0, \quad \langle 0 | \widehat{S}_y | 0 \rangle = 0,$$

in a full agreement with our "macroscopic" intuition expressed in the term "the spin-up state". Nevertheless, we should be aware that under a measurement of, say the  $x$ -th component of spin on the state  $|0\rangle$ , outcomes of all single trials are  $\frac{1}{2}$  or  $-\frac{1}{2}$ ; what has no satisfactory "macroscopic" interpretation.

For a general spin-half state  $|v\rangle$ , the von Neumann measurement of the  $z$ -th component of spin-half results in the probability distribution on the two-element set  $\{\frac{1}{2}, -\frac{1}{2}\}$  of eigenvalues of  $\widehat{S}_z$ : the probability of outcome  $\frac{1}{2}$  of a single trial is  $|v_0|^2$ , while the probability of  $-\frac{1}{2}$  is  $|v_1|^2$ . The final state of the spin-half object would be then the statistical mixture of spin-up and spin-down states with statistical weights  $|v_0|^2$  and  $|v_1|^2$  respectively.

## 2.9. Single-qubit information channel

Here we meet for the first time Alice and Bob - beloved, though enigmatic, heroes of the quantum-computer folk. Alice's never-ending ingenious attempts to send

a message to Bob, an indefatigable struggle of Alice and Bob against a crafty enemy Eve, Alice's secret sharing with Bob and his young friend Charlie - all that, and many other is carefully and in details described in hundreds of research papers on quantum information processing. Almost every day brings new reports on their doings. One of the simplest stories to tell about them is the following.

Suppose that Alice wants to send a one-bit message to Bob, and that she prefers to do that in a quantum way. In order to perform successfully that task, Alice should be connected to Bob by a (noiseless) *quantum information channel*, which - like any classical information channel - should contain three main parts: the encoding apparatus, the transmitting device (the transmission channel proper), and the decoding apparatus.

A typical implementation of a quantum information channel would be as follows. Alice should have to her disposal a state-preparing apparatus, which produces  $|0\rangle$  if she wants to send 0, and  $|1\rangle$  if she wants to send 1. Thus, she encodes her one-bit message by means of two states of the canonical base of a qubit. Then she sends the qubit in the suitable state to Bob through the channel; it is assumed that the state of the qubit does not change during the transmission. Bob, who is equipped with an apparatus measuring the observable  $\hat{S}_z$  in the von Neumann way, performs a measurement of  $\hat{S}_z$  on the received qubit and finds its state. Knowing the state prepared by Alice, Bob finally decodes the message.

Our previous discussion indicates that a measurement has to be performed on a statistical ensemble of identically prepared qubits. Hence, Alice should apparently send a large number of qubits to make Bob's measurement possible. However, in the considered case, just one qubit is enough: a single trial of the  $\hat{S}_z$ -measurement suffices to distinguish between  $|0\rangle$  and  $|1\rangle$ .

The described "single-qubit channel" is merely an academic example. In fact, Alice gained nothing by using the quantum channel instead of a classical one: she sends one classical bit of information with each qubit. We will see in Subsection 3.14 below that entanglement makes it possible to send two bits of information through a single-qubit channel.

### 2.10. Time evolution of a qubit

The time evolution of a quantum object (so also of a qubit) is described by a *dynamical group*, *i.e.* by a family  $\{\hat{U}_t | t \in \mathbb{R}\}$  of unitary operators on  $\mathbb{C}^2$  satisfying the group conditions:

$$\hat{U}_{t_1} \hat{U}_{t_2} = \hat{U}_{t_1+t_2}, \quad \hat{U}_0 = \hat{1},$$

for each  $t_1, t_2 \in \mathbb{R}$ .

An operator

$$\hat{U} = \begin{pmatrix} U_{00} & U_{01} \\ U_{10} & U_{11} \end{pmatrix}$$

is called *unitary* if it satisfies the condition:

$$\hat{U}\hat{U}^* = \hat{1},$$

or equivalently, if:

$$\begin{aligned} |U_{00}|^2 + |U_{01}|^2 &= 1, \\ |U_{11}|^2 + |U_{10}|^2 &= 1, \\ U_{00}U_{10}^* + U_{01}U_{11}^* &= 0. \end{aligned}$$

Thus, a  $2 \times 2$  matrix is unitary if its rows (or columns) can be considered as normalized mutually orthogonal vectors of  $\mathbb{C}^2$  (the same applies to matrices  $n \times n$ ). Crucial for the physical interpretation is that a unitary operator preserves the inner product: for any two vectors  $|v\rangle, |w\rangle$ , and any unitary operator  $\hat{U}$  we have

$$\langle v | w \rangle = \langle \hat{U}v | \hat{U}w \rangle.$$

This implies that the unitary operator  $\hat{U}$  has to be one-to-one, and that it does not change the norm of vectors (so transforms states into states).

The dynamical group  $\{\hat{U}_t | t \in \mathbb{R}\}$  of a quantum object represents a particular way of time evolution. This means that if  $|v\rangle$  is the state of the object at time 0, then  $\hat{U}_t|v\rangle$  is the state of the object at time  $t$ . The traditional description by means of the Schrödinger equation is completely equivalent to the one provided by a dynamical group. The former is the differential form, while the latter - the integrated form of the same time evolution.

It should be stressed that the unitary time evolution of a quantum object, represented by a dynamical group or by the equivalent Schrödinger equation, can be performed by quantum objects which are either completely isolated or influenced from outside in a very special way; such quantum objects are called relatively isolated, or conservative. In a general case, there is no Schrödinger equation nor a dynamical group. The time evolution of a quantum object coupled to its surroundings is governed by more general laws of reduced dynamics; an example of such a time evolution is the transformation of a pre-measurement state into the post-measurement one caused by a von Neumann measurement (the measuring apparatus is there the surroundings).

### 2.11. Single qubit gates

The unitary operators which are useful for quantum computing are called *single qubit gates*. We list some of them. It should be noticed that there are an infinite number of quantum single-qubit gates, in contrast to the classical case where only two logic gates are possible for a single bit.

#### 2.11.1. The trivial gate

The unit operator

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

is the simplest unitary operator. Its "action" does not change any state, hence  $\hat{1}$  is not considered as a logical gate, but rather as a "wire". The trivial gate becomes essential for systems consisting of many qubits, where one usually acts on some of them and do nothing to others.

#### 2.11.2. NOT gate

The only non-trivial single bit gate in classical computer science is the NOT gate. Its quantum counterpart is the unitary operator

$$\begin{aligned} \hat{U}_{\text{NOT}} &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ &= |0\rangle\langle 1| + |1\rangle\langle 0| = \sigma_x, \end{aligned}$$

because its action on the canonical base states  $|0\rangle, |1\rangle$  is:

$$\hat{U}_{\text{NOT}}|0\rangle = |1\rangle, \quad \hat{U}_{\text{NOT}}|1\rangle = |0\rangle.$$

The quantum NOT gate (called also the *flip gate*) is the only single qubit gate which permutes the canonical base. Other gates transform base vectors  $|0\rangle, |1\rangle$  into superpositions of them, what is considered to be a "truly quantum" action.

#### 2.11.3. Hadamard gate

The *Hadamard gate* is the unitary operator

$$\begin{aligned} \hat{U}_{\text{H}} &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \\ &= \frac{1}{\sqrt{2}} (|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|) = \frac{1}{\sqrt{2}} (\sigma_x + \sigma_z). \end{aligned}$$

It transforms the base states  $|0\rangle, |1\rangle$  into superpositions of base states:

$$\hat{U}_H |0\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle), \quad \hat{U}_H |1\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle).$$

#### 2.11.4. Square root of NOT

Deutsch introduced in [3] the series of quantum gates which he calls *powers of NOT*:

$$\hat{U}_{(\text{NOT})^\alpha} := \frac{1}{2} \begin{pmatrix} 1 + e^{i\pi\alpha} & 1 - e^{i\pi\alpha} \\ 1 - e^{i\pi\alpha} & 1 + e^{i\pi\alpha} \end{pmatrix},$$

where  $\alpha$  is an arbitrary real number. It is clear that for an integer  $\alpha$  we get either the unit matrix  $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$  or the quantum NOT gate. For other values of  $\alpha$  we obtain genuine quantum gates, for instance the case of  $\alpha = \frac{1}{2}$  is the *square root of NOT*:

$$\hat{U}_{\sqrt{\text{NOT}}} = \frac{1}{2} \begin{pmatrix} 1 + i & 1 - i \\ 1 - i & 1 + i \end{pmatrix}.$$

Some authors use the picturesque term "square root of NOT" to denote the following single qubit gate

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

which is not equal to Deutsch's  $\hat{U}_{\sqrt{\text{NOT}}}$ .

#### 2.11.5. Rotations and phase shifts

The three unitary operators

$$\begin{aligned} \hat{U}_{R_x}(\theta) &:= \begin{pmatrix} \cos\frac{\theta}{2} & i\sin\frac{\theta}{2} \\ i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}, \\ \hat{U}_{R_y}(\theta) &:= \begin{pmatrix} \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ -\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}, \\ \hat{U}_{R_z}(\theta) &:= \begin{pmatrix} e^{i\frac{\theta}{2}} & 0 \\ 0 & e^{-i\frac{\theta}{2}} \end{pmatrix} \end{aligned}$$

are called *rotations* by  $\theta$  around the  $x$ -, the  $y$ -, and the  $z$ -axis respectively. The name is suggested by the known mapping between the group  $SU(2)$  of unitary

$2 \times 2$  matrices with unity determinant, and the group  $SO(3)$  of orthogonal  $3 \times 3$  matrices with unity determinant (rotations of  $\mathbb{R}^3$ ).

Clearly, the particular cases of rotations are proportional to Pauli matrices:

$$\sigma_x := i\widehat{U}_{R_x}(\pi), \quad \sigma_y := -i\widehat{U}_{R_y}(\pi), \quad \sigma_z := i\widehat{U}_{R_z}(\pi).$$

The unitary operator

$$\widehat{U}_{\text{Ph}}(\varphi) := \begin{pmatrix} e^{i\varphi} & 0 \\ 0 & e^{i\varphi} \end{pmatrix}$$

is called the *phase shift* with respect to  $\varphi$ ; the name is explained by the fact that the action of  $\widehat{U}_{\text{Ph}}(\varphi)$  on an arbitrary vector  $|v\rangle$  of  $\mathbb{C}^2$  causes only the change of the overall phase factor:

$$\widehat{U}_{\text{Ph}}(\varphi)|v\rangle = e^{i\varphi}|v\rangle.$$

It is known (see [1] for more details and a proof) that every unitary operator on  $\mathbb{C}^2$  can be expressed as the product of three rotations and a phase shift

$$\widehat{U} = \widehat{U}_{\text{Ph}}(\varphi)\widehat{U}_{R_z}(\theta_3)\widehat{U}_{R_y}(\theta_2)\widehat{U}_{R_z}(\theta_1)$$

with the appropriate choice of the real parameters  $\theta_1, \theta_2, \theta_3, \varphi$ .

For instance, the unitary operator

$$\widehat{U}_{2\text{Ph}}(\varphi_1, \varphi_2) := \begin{pmatrix} e^{i\varphi_1} & 0 \\ 0 & e^{i\varphi_2} \end{pmatrix}$$

which changes phases of both components of a vector independently:

$$\widehat{U}_{2\text{Ph}}(\varphi_1, \varphi_2) \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} e^{i\varphi_1}v_1 \\ e^{i\varphi_2}v_2 \end{pmatrix},$$

decomposes into

$$\widehat{U}_{2\text{Ph}}(\varphi_1, \varphi_2) = \widehat{U}_{\text{Ph}}\left(\frac{\varphi_1 + \varphi_2}{2}\right)\widehat{U}_{R_z}\left(\frac{\varphi_1 - \varphi_2}{2}\right).$$

### 3. Two-qubit system

*Much that is weird and wonderful about quantum mechanics can be appreciated by considering the properties of the quantum states of two qubits. J. Preskill [8]*

### 3.1. Tensor product of state spaces of two qubits

Consider two qubits, say  $\mathbf{Q}_A$  and  $\mathbf{Q}_B$  (A for Alice, B for Bob - see Subsection 2.9). Their state spaces are  $\mathbb{C}_A^2$  and  $\mathbb{C}_B^2$  respectively. Assume that the two qubits form together a joint quantum system  $\mathbf{Q}_A + \mathbf{Q}_B$ . The quantum system  $\mathbf{Q}_A + \mathbf{Q}_B$  has to be described according to general rules of quantum mechanics; in particular, its states should be represented by vectors of a complex linear space  $\mathbb{C}^n$ . The composite character of the two-qubit system implies that any pair of states  $|v\rangle_A \in \mathbb{C}_A^2$ ,  $|w\rangle_B \in \mathbb{C}_B^2$  should determine a state of  $\mathbf{Q}_A + \mathbf{Q}_B$ , which is denoted  $|v\rangle_A \otimes |w\rangle_B$  (the tensor product of vectors  $|v\rangle_A$  and  $|w\rangle_B$ ). The tensor product  $|v\rangle_A \otimes |w\rangle_B$  is also denoted  $|v, w\rangle$  (we will use both notations). Formally, we should have a one-to-one map

$$\Phi : \mathbb{C}_A^2 \times \mathbb{C}_B^2 \rightarrow \mathbb{C}^4$$

which with every pair  $|v\rangle_A \in \mathbb{C}_A^2$ ,  $|w\rangle_B \in \mathbb{C}_B^2$  associates the vector

$$\Phi(|v\rangle_A, |w\rangle_B) := |v\rangle_A \otimes |w\rangle_B \in \mathbb{C}^4.$$

The map  $\Phi$  has to be bilinear:

$$\begin{aligned} (z_1 |u\rangle_A + z_2 |v\rangle_A) \otimes |w\rangle_B &= z_1 |u, w\rangle + z_2 |v, w\rangle, \\ |u\rangle_A \otimes (z_1 |v\rangle_B + z_2 |w\rangle_B) &= z_1 |u, v\rangle + z_2 |u, w\rangle; \end{aligned}$$

it should also satisfy the important condition:

$$\langle u, w | v, x \rangle = \langle u | v \rangle_A \langle w | x \rangle_B,$$

where the left-side inner product is defined in  $\mathbb{C}^4$ , while the right-side inner products refer to  $\mathbb{C}_A^2$  and  $\mathbb{C}_B^2$  respectively.

It is easy to realize now that four vectors

$$|0\rangle_A \otimes |0\rangle_B, |0\rangle_A \otimes |1\rangle_B, |1\rangle_A \otimes |0\rangle_B, |1\rangle_A \otimes |1\rangle_B$$

(we will denote them  $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ ), are mutually orthogonal and normalized. A simple calculation shows that any vector  $|v\rangle_A \otimes |w\rangle_B$  decomposes into a linear combination of these four vectors:

$$\begin{aligned} |v\rangle_A \otimes |w\rangle_B &= \langle 00 | v, w \rangle |0, 0\rangle + \langle 01 | v, w \rangle |01\rangle + \langle 10 | v, w \rangle |10\rangle + \langle 11 | v, w \rangle |11\rangle \\ &= v_0 w_0 |00\rangle + v_0 w_1 |01\rangle + v_1 w_0 |10\rangle + v_1 w_1 |11\rangle, \end{aligned}$$



or in the column notation

$$\begin{pmatrix} v_0 \\ v_1 \end{pmatrix} \otimes \begin{pmatrix} w_0 \\ w_1 \end{pmatrix} = \begin{pmatrix} v_0 w_0 \\ v_0 w_1 \\ v_1 w_0 \\ v_1 w_1 \end{pmatrix}.$$

It means that all states of the composite qubit  $\mathbf{Q}_A + \mathbf{Q}_B$  having the form  $|v\rangle_A \otimes |w\rangle_B$ , so all states which can be completely described by saying that  $\mathbf{Q}_A$  is in the state  $|v\rangle_A$  and  $\mathbf{Q}_B$  is in the state  $|w\rangle_B$ , belong to the four-dimensional space  $\mathbb{C}^4$  determined by the vectors  $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ . This indicates that the state space of the two-qubit system should be four-dimensional.

The composite character of  $\mathbf{Q}_A + \mathbf{Q}_B$  is formally expressed by the map  $\Phi : \mathbb{C}_A^2 \times \mathbb{C}_B^2 \rightarrow \mathbb{C}^4$  having the mentioned properties. The space  $\mathbb{C}^4$  enhanced with the map  $\Phi$  is called the *tensor product* (or the Kronecker product) of  $\mathbb{C}_A^2$  and  $\mathbb{C}_B^2$ , and denoted  $\mathbb{C}_A^2 \otimes \mathbb{C}_B^2$ .

The four vectors  $|00\rangle, |01\rangle, |10\rangle, |11\rangle$  form the *canonical base* of  $\mathbb{C}_A^2 \otimes \mathbb{C}_B^2$ . As they are indexed by the pair of indices, the components of vectors with respect to the canonical base are also indexed by pairs of indices:

$$\begin{aligned} |v\rangle &= \langle v | 00\rangle |00\rangle + \langle v | 01\rangle |01\rangle + \langle v | 10\rangle |10\rangle + \langle v | 11\rangle |11\rangle \\ &= v_{00} |00\rangle + v_{01} |01\rangle + v_{10} |10\rangle + v_{11} |11\rangle, \end{aligned}$$

the same in the standard column notation is:

$$\begin{aligned} \begin{pmatrix} v_{00} \\ v_{01} \\ v_{10} \\ v_{11} \end{pmatrix} &= v_{00} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} + v_{01} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ &+ v_{10} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} + v_{11} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ &= v_{00} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + v_{01} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + v_{10} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + v_{11} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}. \end{aligned}$$

Similar convention applies to the matrices representing operators: the matrix element  $\langle 00 | \hat{R} | 00\rangle$  of an operator  $\hat{R}$  will be denoted  $R_{00,00}$ , *etc.*

### 3.2. Entangled states

It is important to notice that the two products  $\mathbb{C}_A^2 \times \mathbb{C}_B^2$  and  $\mathbb{C}_A^2 \otimes \mathbb{C}_B^2$  are not identical. The first is the Cartesian product, so it is simply the collection of all pairs of vectors  $|v\rangle_A, |w\rangle_B$  without any overall linear structure. The second is the complex linear space  $\mathbb{C}^4$  equipped with the additional structure imposed by the one-to-one map  $\Phi : \mathbb{C}_A^2 \times \mathbb{C}_B^2 \rightarrow \mathbb{C}^4$ . Having that in mind, one easily realizes that the image of  $\mathbb{C}_A^2 \times \mathbb{C}_B^2$  under the map  $\Phi$  is not the entire space  $\mathbb{C}^4$ : every pair  $|v\rangle_A, |w\rangle_B$  is transformed by  $\Phi$  into the tensor product vector  $|v\rangle_A \otimes |w\rangle_B \in \mathbb{C}_A^2 \otimes \mathbb{C}_B^2$ , whereas  $\mathbb{C}_A^2 \otimes \mathbb{C}_B^2$  contains also various superpositions of such product vectors, like *e.g.*  $|u\rangle_A \otimes |w\rangle_B + |v\rangle_A \otimes |x\rangle_B$ , which are not of the tensor product form.

Every vector of  $\mathbb{C}_A^2 \otimes \mathbb{C}_B^2$  which does not belong to the image of  $\mathbb{C}_A^2 \times \mathbb{C}_B^2$  under  $\Phi$  is called *entangled*. To the class of entangled vectors belong, for instance, the following four combinations of vectors of the canonical base:

$$\begin{aligned} |B_1\rangle &= \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}, & |B_2\rangle &= \frac{1}{\sqrt{2}} (|00\rangle - |11\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix}, \\ |B_3\rangle &= \frac{1}{\sqrt{2}} (|01\rangle + |10\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}, & |B_4\rangle &= \frac{1}{\sqrt{2}} (|01\rangle - |10\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix}. \end{aligned}$$

They are normalized and mutually orthogonal, so form a particular base of  $\mathbb{C}_A^2 \otimes \mathbb{C}_B^2$  called sometimes the *Bell base*. States of the Bell base are paradigmatic examples of entangled states.

It should be noticed that the linear structure of  $\mathbb{C}_A^2 \otimes \mathbb{C}_B^2$  causes some problems with distinguishing entangled and non-entangled vectors. Indeed, every vector of  $\mathbb{C}_A^2 \otimes \mathbb{C}_B^2$  must decompose into a superposition of vectors of a given base, in particular of the canonical base  $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ ; it concerns also product vectors. Take an arbitrary vector  $|u\rangle_A \otimes |w\rangle_B$  with  $|u\rangle_A = u_0|0\rangle_A + u_1|1\rangle_A$ , and  $|w\rangle_B = w_0|0\rangle_B + w_1|1\rangle_B$ ; then

$$|u\rangle_A \otimes |w\rangle_B = u_0w_0|00\rangle + u_0w_1|01\rangle + u_1w_0|10\rangle + u_1w_1|11\rangle,$$

so the non-entangled vector  $|u\rangle_A \otimes |w\rangle_B$  looks like an entangled one. A criterion which discriminates between entangled and non-entangled states will be provided below (Subsection 3.8).

Some peculiar properties of entangled states are essential for quantum information processing; we will discuss them later on. Nevertheless, one can immediately see why entangled states are so special. The physical interpretation we attributed to product vectors of  $\mathbb{C}_A^2 \otimes \mathbb{C}_B^2$  says that the two qubits  $\mathbf{Q}_A$  and  $\mathbf{Q}_B$  are in well defined states  $|u\rangle_A, |w\rangle_B$  if and only if the state of the composite system  $\mathbf{Q}_A + \mathbf{Q}_B$  is  $|u\rangle_A \otimes |w\rangle_B$ . Hence, if the joint system  $\mathbf{Q}_A + \mathbf{Q}_B$  was in an entangled state, the qubits  $\mathbf{Q}_A$  and  $\mathbf{Q}_B$  would had no definite states - a situation which could never happen in the classical physics.

### 3.3. Observables

Physical quantities (observables) relevant to a quantum system having a four-dimensional state space  $\mathbb{C}^4$  are to be represented, according to general rules of quantum mechanics, by self-adjoint operators on  $\mathbb{C}^4$ . The self-adjointness condition is a direct generalizations of that listed in Subsection 2.2: an operator

$$\widehat{Q} = (Q_{ij,kl}),$$

where  $Q_{ij,kl}$  are matrix elements of  $\widehat{Q}$  in the canonical base, is called self-adjoint if

$$\widehat{Q} = \widehat{Q}^*,$$

or equivalently, if:

$$Q_{ij,kl} = Q_{kl,ij}^*$$

for every  $i, j, k, l = 0, 1$ .

Like the two-dimensional case, eigenvalues of self-adjoint operators are real numbers. It is easy to show that all eigenvectors corresponding to the same eigenvalue form a linear subspace of  $\mathbb{C}^4$  called an *eigensubspace*; if an eigensubspace is of dimension  $d \geq 2$ , the corresponding eigenvalue is called *d-fold degenerate*. Eigensubspaces of a self-adjoint operator  $\widehat{Q}$  corresponding to different eigenvalues are mutually orthogonal, this property enables us to construct bases of  $\mathbb{C}^4$  from eigenvectors of  $\widehat{Q}$ .

An *orthonormal base* of a subspace is any set of mutually orthogonal and normalized vectors, such that every vector belonging to the subspace decomposes into a linear combination of them. It is clear that any subspace of dimension 2 or more has many orthonormal bases. If we than pick up one orthonormal base for every eigensubspace of a self-adjoint operator  $\widehat{Q}$ , we get a base of the whole space  $\mathbb{C}^4$  which consists of eigenvectors of  $\widehat{Q}$ , and is called a  $\widehat{Q}$ -eigenbase (of  $\mathbb{C}^4$ ). If some of eigenvalues of  $\widehat{Q}$  are degenerate, there are many different eigenbases defined by  $\widehat{Q}$ .

Among self-adjoint operators on  $\mathbb{C}^4$  one distinguishes a special class of *projection operators*. An operator  $\hat{P} : \mathbb{C}^4 \rightarrow \mathbb{C}^4$  is a projection operator if it is idempotent:

$$\hat{P}^2 = \hat{P},$$

what means that if we apply it twice, we get the same as we would apply it only once. To the class of projection operators belong the unit operator  $\hat{1}$  and the null operator  $\hat{0}$ , the latter described by the matrix having all entries equal null. Every non-trivial (*i.e.* except  $\hat{1}$  and  $\hat{0}$ ) projection operator has exactly two eigenvalues: 0 and 1.

The vector  $\hat{P}|v\rangle$  for an arbitrary  $|v\rangle \in \mathbb{C}^4$  is simply the orthogonal projection of  $|v\rangle$  onto the eigensubspace of  $\hat{P}$  corresponding to the eigenvalue 1, hence this subspace is the image of  $\mathbb{C}^4$  under the action of the projection operator  $\hat{P}$ . The two eigenvalues of a projection operator  $\hat{P}$  are usually degenerate; if the eigenvalue 1 is non-degenerate, then the corresponding eigensubspace is one-dimensional, the traditional notation for  $\hat{P}$  is then  $|v\rangle\langle v|$  (see Subsection 2.2), where  $|v\rangle$  is a normalized vector belonging to the one-dimensional eigensubspace.

The geometrical interpretation exposed above implies that every projection operator is uniquely characterized by its eigensubspace corresponding to 1. Conversely, with every subspace of  $\mathbb{C}^4$  we can associate the unique projection operator which orthogonally projects all vectors on it. That establishes the natural one-to-one correspondence between projection operators and subspaces of  $\mathbb{C}^4$ .

### 3.4. Spectral decomposition and measurements

Projection operators, called also *elementary observables*, occupy a very special position in the formal structure of quantum mechanics. The reason is that every self-adjoint operator decomposes into projection operators.

According to considerations of the last Subsection, with every self-adjoint operator  $\hat{Q}$  on  $\mathbb{C}^4$  one associates the set of its eigenvalues  $\{q_1, \dots, q_k\}$ ,  $k \leq 4$ , (called the *spectrum* of  $\hat{Q}$ ) and the set of corresponding eigensubspaces  $\{V_1, \dots, V_k\}$ . In turn, with every eigensubspace  $V_j$  we associate the corresponding projection operator  $\hat{P}_j$ . The operator  $\hat{Q}$  can be expressed as a combination of these projection operators:

$$\hat{Q} = q_1\hat{P}_1 + \dots + q_k\hat{P}_k$$

with  $k \leq 4$ , this formula is called the *spectral decomposition* of a self-adjoint operator.

The spectral decomposition is crucial for the minimal interpretation of quantum mechanics, as well as for the quantum theory of measurement. In both cases

considerations of Section 2. should be appropriately generalized to absorb the possible degeneracy of eigenvalues.

The interpretation rule called the *minimal interpretation* formulated in Subsection 2.3 takes now the following form:

Given a vector  $|v\rangle \in \mathbb{C}^4$  representing a state of a quantum object, and a self-adjoint operator  $\widehat{Q}$  representing a physical quantity relevant to the object. Eigenvalues  $q_1, \dots, q_k$  of  $\widehat{Q}$  are the possible values of the physical quantity, while  $\langle v | \widehat{P}_j | v \rangle$ , where  $\widehat{P}_j$  is the projection operator corresponding to the eigenvalue  $q_j$ , is the probability for the outcome  $q_j$  to occur if a measurement of the observable  $\widehat{Q}$  is performed on the object in the state  $|v\rangle$ .

The provided formulation of the minimal interpretation applies to a general state space  $\mathbb{C}^n$  (but not to the infinitely-dimensional Hilbert space !).

The concept of a measurement of a quantum observable, formulated in Section 2 as a long run of single trials is of a general validity. Thus, like the single qubit case, the spectrum  $\{q_1, \dots, q_k\}$  of a self-adjoint operator  $\widehat{Q}$  is the set of all possible outcomes of single trials, whereas the probability of occurrence of a particular value  $q_j$  equals  $\langle v | \widehat{P}_j | v \rangle$  according to the minimal interpretation.

If the measurement is of the von Neumann type, the post-measurement ensemble should be a statistical mixture of eigenstates

$$\langle v | \widehat{P}_j | v \rangle^{-\frac{1}{2}} \widehat{P}_j | v \rangle, \quad j = 1, \dots, k$$

with weights  $\langle v | \widehat{P}_j | v \rangle$ .

### 3.5. Density operators

With any state  $|v\rangle \in \mathbb{C}^4$  one can associate the projection operator  $\widehat{P}_v$  which projects all vectors of  $\mathbb{C}^4$  onto the 1-dimensional subspace spanned by  $|v\rangle$  :

$$\widehat{P}_v |w\rangle := \langle v | w \rangle |v\rangle.$$

In the bra - ket notation

$$\widehat{P}_v = |v\rangle \langle v| \quad ;$$

while the matrix representation (in the canonical base) of  $\widehat{P}_v$  for

$$|v\rangle = \begin{pmatrix} v_{00} \\ v_{01} \\ v_{10} \\ v_{11} \end{pmatrix}$$

is

$$\hat{P}_v = \begin{pmatrix} v_{00}v_{00}^* & v_{00}v_{01}^* & v_{00}v_{10}^* & v_{00}v_{11}^* \\ v_{01}v_{00}^* & v_{01}v_{01}^* & v_{01}v_{10}^* & v_{01}v_{11}^* \\ v_{10}v_{00}^* & v_{10}v_{01}^* & v_{10}v_{10}^* & v_{10}v_{11}^* \\ v_{11}v_{00}^* & v_{11}v_{01}^* & v_{11}v_{10}^* & v_{11}v_{11}^* \end{pmatrix}.$$

The operator  $\hat{P}_v$  provides an alternative description of the state represented by the vector  $|v\rangle$ .

We define the *trace* of an operator,  $\text{Tr } \hat{R}$ , as the sum of its diagonal matrix elements in an arbitrary base. Thus, in the canonical base we have:

$$\begin{aligned} \text{Tr } \hat{R} &:= \sum_{ij=0,1} \langle ij | \hat{R} | ij \rangle \\ &= \langle 00 | \hat{R} | 00 \rangle + \langle 01 | \hat{R} | 01 \rangle + \langle 10 | \hat{R} | 10 \rangle + \langle 11 | \hat{R} | 11 \rangle. \end{aligned}$$

The trace of an operator does not depend on the base, and is linear with respect to sums of operators. Now, the transition probability between two states can be expressed as

$$|\langle v | w \rangle|^2 = \text{Tr} \left( \hat{P}_v \hat{P}_w \right),$$

and the mean value of an observable  $\hat{Q}$  is

$$\langle \hat{Q} \rangle = \langle v | \hat{Q} | v \rangle = \text{Tr} \left( \hat{Q} \hat{P}_v \right).$$

The representation of states by means of corresponding projection operators leads to a concise representation of the statistical mixtures of states which we have met above. Indeed, consider a statistical mixture of two mutually orthogonal states  $|v_1\rangle, |v_2\rangle$  with weights  $\lambda_1, \lambda_2$ . The mean value of an observable  $\hat{Q}$  measured on such a mixed ensemble has to be

$$\begin{aligned} \langle \hat{Q} \rangle &= \lambda_1 \langle v_1 | \hat{Q} | v_1 \rangle + \lambda_2 \langle v_2 | \hat{Q} | v_2 \rangle = \lambda_1 \text{Tr} \left( \hat{Q} \hat{P}_{v_1} \right) + \lambda_2 \text{Tr} \left( \hat{Q} \hat{P}_{v_2} \right) \\ &= \text{Tr} \left( \hat{Q} \left( \lambda_1 \hat{P}_{v_1} + \lambda_2 \hat{P}_{v_2} \right) \right). \end{aligned}$$

The operator in brackets represents the statistical mixture in question, its traditional name is *density operator*. Thus, having the density operator corresponding to a statistical mixture, we can calculate the mean value of any observable at the corresponding ensemble. A deeper analysis shows that the knowledge of all mean values of all observables at some statistical ensemble suffices for an identification of that statistical ensemble. Accordingly, the density operator provides the exhaustive description of the statistical mixture of states.

Formally, the name density operator refers to any operator  $\hat{\rho}$  satisfying the two conditions: all eigenvalues of  $\hat{\rho}$  are to be non-negative (what implies that  $\hat{\rho}$  should be self-adjoint), and its trace must equal 1:

$$\text{Tr } \hat{\rho} = 1.$$

Notice, that any one-dimensional projection operator  $|v\rangle\langle v|$  meets both conditions, so the class of density operators contains all one-dimensional projections (other projection operators are not density operators). The set of all one-dimensional projections is in a sense fundamental for the class of density operators: every density operator decomposes into a linear combination of one-dimensional projections, what has the simple physical interpretation: every statistical ensemble is a statistical mixture of pure ensembles.

If the operator  $|v\rangle\langle v|$  is done in the matrix form, it is not evident that it is a projection operator. It can be proved that a density operator  $\hat{\rho}$  is a one-dimensional projection if and only if

$$\text{Tr } \hat{\rho}^2 = 1,$$

otherwise

$$\text{Tr } \hat{\rho}^2 < 1.$$

In quantum mechanics it is assumed that any density operator describes a general state of a quantum object. If the density operator satisfies the condition  $\text{Tr } \hat{\rho}^2 = 1$ , then it describes a *pure state* (called also a vector state), so just a state represented by a normalized vector of a complex linear space. If  $\text{Tr } \hat{\rho}^2 < 1$ , then  $\hat{\rho}$  describes a *mixed state*. Till now, pure states were called states, while mixed states were called statistical mixtures of states.

We have to notice now some important point. The description of states by means of density operators implies that pure states, represented up to now by normalized vectors  $|v\rangle$ , are represented by projection operators  $|v\rangle\langle v|$ . This new representation of pure states ignores their phase factors: two vectors  $|u\rangle$ , and  $|v\rangle = e^{i\varphi}|u\rangle$  are surely different elements of  $\mathbb{C}^4$ , nevertheless they define the same projection operator because

$$\hat{P}_v |w\rangle = e^{-i\varphi} e^{i\varphi} \langle u | w \rangle |u\rangle = \langle u | w \rangle |u\rangle = \hat{P}_u |w\rangle$$

for arbitrary vector  $|w\rangle \in \mathbb{C}^4$ . We see that the two ways of representing quantum pure states: by means of normalized vectors, and by means of projection operators of one-dimensional range, are not equivalent - the former is more "subtle". It is commonly assumed that the latter representation is adequate, so that the

proper representation of pure states is provided by the projection operators of one-dimensional range. Thus, we have to keep in mind that vectors represent states in an ambiguous way: two vectors which differ only in a phase factor, like  $|u\rangle$  and  $e^{i\varphi}|u\rangle$ , represent the same state.

We encountered mixed states as the post-measurement statistical mixtures generated by a von Neumann-type measurement. Assume that we perform a von Neumann measurement of an observable having the spectral decomposition

$$\widehat{Q} = q_1 \widehat{P}_1 + \dots + q_k \widehat{P}_k, \quad k \leq 4,$$

on a pure state  $|v\rangle$ . The post-measurement ensemble is then (see the previous Subsection) the statistical mixture of eigenstates of  $\widehat{Q}$ :

$$\langle v | \widehat{P}_j | v \rangle^{-\frac{1}{2}} \widehat{P}_j | v \rangle, \quad j = 1, \dots, k$$

with weights  $\langle v | \widehat{P}_j | v \rangle$ . The corresponding density operator is:

$$\widehat{\rho}_{out} = \sum_{j=1}^k \langle v | \widehat{P}_j | v \rangle \frac{1}{\langle v | \widehat{P}_j | v \rangle} |\widehat{P}_j v\rangle \langle \widehat{P}_j v| = \sum_{j=1}^k |\widehat{P}_j v\rangle \langle \widehat{P}_j v|,$$

where  $|\widehat{P}_j v\rangle \langle \widehat{P}_j v|$  denotes the projection operator defined by the (non-normalized!) vector  $\widehat{P}_j | v \rangle$ .

### 3.6. Tensor products of operators

Let us return to the case  $\mathbb{C}^4 = \mathbb{C}_A^2 \otimes \mathbb{C}_B^2$ , what means that the four-dimensional vector space in question is the state space of a two-qubit system  $\mathbf{Q}_A + \mathbf{Q}_B$ .

The tensor-product structure of  $\mathbb{C}^4$  leads to the tensor product of operators. Let  $\widehat{R}_A$  and  $\widehat{R}_B$  be operators on  $\mathbb{C}_A^2$  and  $\mathbb{C}_B^2$  respectively. Having  $\widehat{R}_A$  and  $\widehat{R}_B$ , we can construct an operator

$$\widehat{R} : \mathbb{C}_A^2 \otimes \mathbb{C}_B^2 \rightarrow \mathbb{C}_A^2 \otimes \mathbb{C}_B^2,$$

as follows. We begin with defining the action of  $\widehat{R}$  on vectors of the canonical base:

$$\begin{aligned} \widehat{R} |00\rangle &:= \widehat{R}_A |0\rangle_A \otimes \widehat{R}_B |0\rangle_B, \\ \widehat{R} |01\rangle &:= \widehat{R}_A |0\rangle_A \otimes \widehat{R}_B |1\rangle_B, \\ \widehat{R} |10\rangle &:= \widehat{R}_A |1\rangle_A \otimes \widehat{R}_B |0\rangle_B, \\ \widehat{R} |11\rangle &:= \widehat{R}_A |1\rangle_A \otimes \widehat{R}_B |1\rangle_B. \end{aligned}$$



Then we take into account that every vector  $|v\rangle \in \mathbb{C}_A^2 \otimes \mathbb{C}_B^2$  decomposes in the canonical base:

$$|v\rangle = \langle 00 | v \rangle |00\rangle + \langle 01 | v \rangle |01\rangle + \langle 10 | v \rangle |10\rangle + \langle 11 | v \rangle |11\rangle ,$$

so we can define

$$\widehat{R}|v\rangle := \langle 00 | v \rangle \widehat{R}|00\rangle + \langle 01 | v \rangle \widehat{R}|01\rangle + \langle 10 | v \rangle \widehat{R}|10\rangle + \langle 11 | v \rangle \widehat{R}|11\rangle .$$

The operator  $\widehat{R}$  constructed in this way is denoted  $\widehat{R}_A \otimes \widehat{R}_B$  and called the *tensor product of operators*  $\widehat{R}_A$  and  $\widehat{R}_B$  ; its matrix elements are:

$$\begin{aligned} R_{00,00} &= \langle 00 | \widehat{R} | 00 \rangle = \langle 0 | \widehat{R}_A | 0 \rangle_A \langle 0 | \widehat{R}_B | 0 \rangle_B = R_{A,00} R_{B,00} , \\ R_{00,01} &= \langle 00 | \widehat{R} | 01 \rangle = \langle 0 | \widehat{R}_A | 0 \rangle_A \langle 0 | \widehat{R}_B | 1 \rangle_B = R_{A,00} R_{B,01} , \\ &etc, \end{aligned}$$

hence its matrix form in the canonical base is:

$$\widehat{R}_A \otimes \widehat{R}_B = \begin{pmatrix} R_{A,00} R_{B,00} & R_{A,00} R_{B,01} & R_{A,01} R_{B,00} & R_{A,01} R_{B,01} \\ R_{A,00} R_{B,10} & R_{A,00} R_{B,11} & R_{A,01} R_{B,10} & R_{A,01} R_{B,11} \\ R_{A,10} R_{B,00} & R_{A,10} R_{B,01} & R_{A,11} R_{B,00} & R_{A,11} R_{B,01} \\ R_{A,10} R_{B,10} & R_{A,10} R_{B,11} & R_{A,11} R_{B,10} & R_{A,11} R_{B,11} \end{pmatrix}$$

It is easy to see the following useful properties of the tensor product of operators:

- if both  $\widehat{R}_A$  and  $\widehat{R}_B$  are self-adjoint, then  $\widehat{R}_A \otimes \widehat{R}_B$  is self-adjoint,
- if both  $\widehat{R}_A$  and  $\widehat{R}_B$  are projection operators, then  $\widehat{R}_A \otimes \widehat{R}_B$  is a projection operator,
- if both  $\widehat{R}_A$  and  $\widehat{R}_B$  are projection operators of one-dimensional ranges, then  $\widehat{R}_A \otimes \widehat{R}_B$  is a projection operator of one-dimensional range,
- if both  $\widehat{R}_A$  and  $\widehat{R}_B$  are unitary, then  $\widehat{R}_A \otimes \widehat{R}_B$  is unitary,
- if both  $\widehat{R}_A$  and  $\widehat{R}_B$  are density operators, then  $\widehat{R}_A \otimes \widehat{R}_B$  is a density operator.

A short calculation leads to the important equality:

$$\widehat{R}_A \otimes \widehat{R}_B |v, w\rangle := \widehat{R}_A |v\rangle_A \otimes \widehat{R}_B |w\rangle_B ,$$

which shows how the operator  $\widehat{R}_A \otimes \widehat{R}_B$  acts on product states. An easy consequence of that is:

$$\begin{aligned} \langle u, v | \widehat{R}_A \otimes \widehat{R}_B |w, x\rangle &= \langle u, v | \left( \widehat{R}_A |w\rangle_A \otimes \widehat{R}_B |x\rangle_B \right) \\ &= \langle u | \widehat{R}_A |w\rangle_A \langle v | \widehat{R}_B |x\rangle_B . \end{aligned}$$

If we take two self-adjoint operators  $\widehat{Q}_A$  and  $\widehat{Q}_B$  and two eigen-states  $|q\rangle_A, |r\rangle_B$  :

$$\widehat{Q}_A |q\rangle_A = q |q\rangle_A, \quad \widehat{Q}_B |r\rangle_B = r |r\rangle_B,$$

then

$$\begin{aligned} \widehat{Q}_A \otimes \widehat{Q}_B |q, r\rangle &:= \widehat{Q}_A |q\rangle_A \otimes \widehat{Q}_B |r\rangle_B \\ &= qr |q, r\rangle, \end{aligned}$$

what shows that products of eigen-values of  $\widehat{Q}_A$  and  $\widehat{Q}_B$  are eigen-values of  $\widehat{Q}_A \otimes \widehat{Q}_B$ , and tensor products of eigen-vectors of  $\widehat{Q}_A$  and  $\widehat{Q}_B$  are eigen-vectors of  $\widehat{Q}_A \otimes \widehat{Q}_B$ .

The above conclusion enables a calculation of the spectral decomposition of  $\widehat{Q}_A \otimes \widehat{Q}_B$ : if

$$\widehat{Q}_A = q_1 \widehat{P}_{A,1} + q_2 \widehat{P}_{A,2}, \quad \widehat{Q}_B = r_1 \widehat{P}_{B,1} + r_2 \widehat{P}_{B,2},$$

then

$$\widehat{Q}_A \otimes \widehat{Q}_B = \sum q_i r_j \widehat{P}_{A,i} \otimes \widehat{P}_{B,j}.$$

### 3.7. Observables of subsystems

Applying the last result of the foregoing Subsection to the operator  $\widehat{Q}_A \otimes \widehat{1}_B$ , where  $\widehat{Q}_A$  is a self-adjoint operator on  $\mathbb{C}_A^2$ , and  $\widehat{1}_B$  is the identity operator on  $\mathbb{C}_B^2$ , one finds that the spectrum of  $\widehat{Q}_A \otimes \widehat{1}_B$  is the same as the spectrum of  $\widehat{Q}_A$ . Given the spectral decomposition of the observable  $\widehat{Q}_A$ ,

$$\widehat{Q}_A = q_1 \widehat{P}_{A,1} + q_2 \widehat{P}_{A,2},$$

we easily find that the spectral decomposition of  $\widehat{Q}_A \otimes \widehat{1}_B$  is simply:

$$\widehat{Q}_A \otimes \widehat{1}_B = q_1 \widehat{P}_{A,1} \otimes \widehat{1}_B + q_2 \widehat{P}_{A,2} \otimes \widehat{1}_B.$$

As an example we provide spectral decompositions of the spin-component observables of a subsystem:

$$\begin{aligned} \widehat{S}_{A,z} \otimes \widehat{1}_B &= \frac{1}{2} |0\rangle \langle 0|_A \otimes \widehat{1}_B - \frac{1}{2} |1\rangle \langle 1|_A \otimes \widehat{1}_B \\ &= \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \otimes \widehat{1}_B - \frac{1}{2} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \otimes \widehat{1}_B, \\ \widehat{S}_{A,x} \otimes \widehat{1}_B &= \frac{1}{2} |0_x\rangle \langle 0_x|_A \otimes \widehat{1}_B - \frac{1}{2} |1_x\rangle \langle 1_x|_A \otimes \widehat{1}_B \\ &= \frac{1}{4} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes \widehat{1}_B - \frac{1}{4} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes \widehat{1}_B. \end{aligned}$$

According to the minimal interpretation, if we perform a measurement of the observable  $\widehat{Q}_A \otimes \widehat{I}_B$  on a product state  $|v\rangle_A \otimes |w\rangle_B$ , then particular values  $q_1, q_2$  of the observable  $\widehat{Q}_A \otimes \widehat{I}_B$  should occur in single trials with probabilities  $\langle v, w | \widehat{P}_{A,1} \otimes \widehat{I}_B | v, w \rangle$ ,  $\langle v, w | \widehat{P}_{A,2} \otimes \widehat{I}_B | v, w \rangle$  respectively. However,

$$\begin{aligned} \langle v, w | \widehat{P}_{A,j} \otimes \widehat{I}_B | v, w \rangle &= \langle v | \widehat{P}_{A,j} | v \rangle_A \langle w | w \rangle_B \\ &= \langle v | \widehat{P}_{A,j} | v \rangle_A, \end{aligned}$$

for  $j = 1, 2$ . Thus, any measurement of  $\widehat{Q}_A \otimes \widehat{I}_B$  on a product state  $|v\rangle_A \otimes |w\rangle_B$  should show the same values with the same probabilities as a measurement of  $\widehat{Q}_A$  on the state  $|v\rangle_A$ .

All that make physicists to believe that  $\widehat{Q}_A \otimes \widehat{I}_B$  is the observable of the two-qubit system  $\mathbf{Q}_A + \mathbf{Q}_B$  which represents exactly the same physical property of  $\mathbf{Q}_A$  as the single-qubit observable  $\widehat{Q}_A$  does. In this way we obtain the representation of physical quantities relevant to the subsystem  $\mathbf{Q}_A$  by means of observables of the joint system  $\mathbf{Q}_A + \mathbf{Q}_B$ . Clearly, the same concerns observables of the form  $\widehat{I}_A \otimes \widehat{Q}_B$ . Observables of both kinds,  $\widehat{Q}_A \otimes \widehat{I}_B$  and  $\widehat{I}_A \otimes \widehat{Q}_B$ , are called *subsystem observables*.

Nevertheless, there is an obvious difference between a measurement of  $\widehat{Q}_A \otimes \widehat{I}_B$  and a measurement of  $\widehat{Q}_A$ : the former should be performed on the composite system  $\mathbf{Q}_A + \mathbf{Q}_B$ , so in the presence of both subsystems  $\mathbf{Q}_A$  and  $\mathbf{Q}_B$ , while the latter - on the system  $\mathbf{Q}_A$  alone. Consider, for instance, the von Neumann measurement of  $\widehat{Q}_A \otimes \widehat{I}_B$  on a product pure state  $|v\rangle_A \otimes |w\rangle_B$ , assume that the eigenvalues  $q_1, q_2$  are non-degenerate. The post-measurement state should be

$$\widehat{\rho} = \langle v | \widehat{P}_{A,1} | v \rangle_A |q_1, w\rangle \langle q_1, w| + \langle v | \widehat{P}_{A,2} | v \rangle_A |q_2, w\rangle \langle q_2, w|,$$

where  $|q_1\rangle_A, |q_2\rangle_A$  are the eigenstates of  $\widehat{Q}_A$ . Clearly,  $\widehat{\rho}$  describes the statistical mixture of product states  $|q_j\rangle_A \otimes |w\rangle_B$  with weights  $\langle v | \widehat{P}_{A,j} | v \rangle_A$ ,  $j = 1, 2$ , thus the state  $|w\rangle_B$  of the second subsystem, even if in a passive way, contributes to the measurement process.

### 3.8. States of subsystems

Up to now we were concerned with the problem of describing pure states of the joint system  $\mathbf{Q}_A + \mathbf{Q}_B$  knowing pure states of the subsystems. That problem can be generalized in view of our generalization of the concept of state: describe the state of the joint system  $\mathbf{Q}_A + \mathbf{Q}_B$  knowing states (pure or mixed) of the subsystems. The solution to this problem is simple: if  $\mathbf{Q}_A$  and  $\mathbf{Q}_B$  are in states

$\hat{\rho}_A$  and  $\hat{\rho}_B$ , then the joint system  $\mathbf{Q}_A + \mathbf{Q}_B$  is in the state  $\hat{\rho}_A \otimes \hat{\rho}_B$ . It is easy to see that if  $\hat{\rho}_A$  and  $\hat{\rho}_B$  are pure, then  $\hat{\rho}_A \otimes \hat{\rho}_B$  is also pure and is the projection operator on the product vector  $|v\rangle_A \otimes |w\rangle_B$ , with  $|v\rangle_A$  corresponding to  $\hat{\rho}_A$  and  $|w\rangle_B$  corresponding to  $\hat{\rho}_B$ .

One can also formulate the reverse problem: find states (pure or mixed) of subsystems  $\mathbf{Q}_A$  and  $\mathbf{Q}_B$  knowing a state (pure or mixed) of the joint system  $\mathbf{Q}_A + \mathbf{Q}_B$ .

The presence of subsystem observables provides a surprisingly rich information about states of subsystems. Indeed, let  $|w\rangle \in \mathbb{C}_A^2 \otimes \mathbb{C}_B^2$  be a general (possibly entangled) pure state of the composite system; the decomposition of  $|w\rangle$  in the canonical base is the following:

$$|w\rangle = w_{00} |00\rangle + w_{01} |01\rangle + w_{10} |10\rangle + w_{11} |11\rangle .$$

Take then an arbitrary observable relevant to  $\mathbf{Q}_A$  :

$$\hat{Q}_A \otimes \hat{1}_B = q_1 \hat{P}_{A,1} \otimes \hat{1}_B + q_2 \hat{P}_{A,2} \otimes \hat{1}_B .$$

The mean value  $\langle w | \hat{Q}_A \otimes \hat{1}_B | w \rangle$  of  $\hat{Q}_A \otimes \hat{1}_B$  on the state  $|w\rangle$  can be expressed as the mean value of  $\hat{Q}_A$  on a (possibly mixed) state  $\hat{\rho}_A$ . We will calculate it in the canonical base:

$$\begin{aligned} \langle w | \hat{Q}_A \otimes \hat{1}_B | w \rangle &= \sum_{ij,kl} w_{ij}^* w_{kl} \langle ij | \hat{Q}_A \otimes \hat{1}_B | kl \rangle \\ &= \sum_{ij,kl} w_{ij}^* w_{kl} \langle i | \hat{Q}_A | k \rangle_A \langle j | \hat{1}_B | l \rangle_B \\ &= \sum_{ij,k} w_{ij}^* w_{kj} \langle i | \hat{Q}_A | k \rangle \\ &= \text{Tr} \left( \hat{Q}_A \hat{\rho}_A \right) , \end{aligned}$$

where  $\hat{\rho}_A$  is an operator on  $\mathbb{C}_A^2$  defined by:

$$\hat{\rho}_A = \sum_{ijk} w_{ij}^* w_{kj} |k\rangle \langle i| .$$

The matrix form (in the canonical base of  $\mathbb{C}_A^2$ ) of the obtained operator is:

$$\hat{\rho}_A = \begin{pmatrix} w_{00}w_{00}^* + w_{01}w_{01}^* & w_{00}w_{10}^* + w_{01}w_{11}^* \\ w_{10}w_{00}^* + w_{11}w_{01}^* & w_{10}w_{10}^* + w_{11}w_{11}^* \end{pmatrix} .$$

It is easy to find that  $\hat{\rho}_A$  is a density operator (the trace condition  $\text{Tr } \hat{\rho}_A = 1$  is here equivalent to the normalization condition  $|\langle w | w \rangle|^2 = 1$ ), so describes a state (mixed, in general) of the subsystem  $\mathbf{Q}_A$ . Then, the final formula  $\text{Tr} (\hat{Q}_A \hat{\rho}_A)$  can be interpreted as the mean value of the observable  $\hat{Q}_A$  in the state  $\hat{\rho}_A$ . Taking into account that the definition of  $\hat{\rho}_A$  does not depend on the subsystem observable, we conclude that  $\hat{\rho}_A$  is the state (called the *reduced state*) of the subsystem  $\mathbf{Q}_A$ , provided the joint system  $\mathbf{Q}_A + \mathbf{Q}_B$  is in the pure state  $|w\rangle$ . The reduced state  $\hat{\rho}_A$  is completely determined by the property:

$$\langle w | \hat{Q}_A \otimes \hat{1}_B | w \rangle = \text{Tr } \hat{Q}_A \hat{\rho}_A$$

for every observable  $\hat{Q}_A$  of the subsystem  $\mathbf{Q}_A$ , so that the mean value of arbitrary observable  $\hat{Q}_A$  of the subsystem at  $\hat{\rho}_A$  is the same as the mean value of the corresponding "global" observable  $\hat{Q}_A \otimes \hat{1}_B$  at the corresponding "global" state  $|w\rangle$  of the joint system.

The obtained result is consistent with the assumption made earlier: one can prove that the reduced state  $\hat{\rho}_A$  obtained from a pure state  $|w\rangle \in \mathbb{C}_A^2 \otimes \mathbb{C}_B^2$  in the way described above is a pure state (*i.e.*  $\text{Tr } \hat{\rho}_A^2 = 1$ ) if and only if the original pure state  $|w\rangle$  is of the product form  $|v\rangle_A \otimes |u\rangle_B$ . Thus we have solved the problem of defining the state of subsystem if the state of the joint system is pure.

The procedure of extracting  $\hat{\rho}_A$  from a given pure state  $|w\rangle \in \mathbb{C}_A^2 \otimes \mathbb{C}_B^2$  is called the *partial trace* over indexes of the subsystem  $\mathbf{Q}_B$ , or the *state reduction*; the former emphasizes the formal aspect, while the latter refers to the physical interpretation.

If one compares the matrix form of the density operator  $|w\rangle \langle w|$  describing the state  $|w\rangle$ :

$$|w\rangle \langle w| = \begin{pmatrix} w_{00}w_{00}^* & w_{00}w_{01}^* & w_{00}w_{10}^* & w_{00}w_{11}^* \\ w_{01}w_{00}^* & w_{01}w_{01}^* & w_{01}w_{10}^* & w_{01}w_{11}^* \\ w_{10}w_{00}^* & w_{10}w_{01}^* & w_{10}w_{10}^* & w_{10}w_{11}^* \\ w_{11}w_{00}^* & w_{11}w_{01}^* & w_{11}w_{10}^* & w_{11}w_{11}^* \end{pmatrix}$$

with the provided above matrix form of the reduced density operator, the name *partial trace* becomes clear:  $\hat{\rho}_A$  is obtained by summing up over indices referring to  $\mathbb{C}_B^2$ . This is reflected in the suggestive notation:

$$\hat{\rho}_A := \text{Tr}_B |w\rangle \langle w|.$$

The same method can be applied to define the reduced state of the second subsystem  $\mathbf{Q}_B$ , we obtain:

$$\hat{\rho}_B = \begin{pmatrix} w_{00}w_{00}^* + w_{10}w_{10}^* & w_{00}w_{01}^* + w_{10}w_{11}^* \\ w_{10}w_{00}^* + w_{11}w_{01}^* & w_{01}w_{01}^* + w_{11}w_{11}^* \end{pmatrix},$$

and write

$$\hat{\rho}_B = \text{Tr}_A |w\rangle \langle w|.$$

The reduction procedure which, by means of the partial traces, generates  $\hat{\rho}_A$  and  $\hat{\rho}_B$  from the density operator  $|w\rangle \langle w|$  of the pure state, extends easily over general density operators on  $\mathbb{C}_A^2 \otimes \mathbb{C}_B^2$ . We provide for further references the appropriate formulas: given a density operator in the canonical base

$$\hat{\rho} = \begin{pmatrix} \rho_{00,00} & \rho_{00,01} & \rho_{00,10} & \rho_{00,11} \\ \rho_{01,00} & \rho_{01,01} & \rho_{01,10} & \rho_{01,11} \\ \rho_{10,00} & \rho_{10,01} & \rho_{10,10} & \rho_{10,11} \\ \rho_{11,00} & \rho_{11,01} & \rho_{11,10} & \rho_{11,11} \end{pmatrix},$$

the reduced density operators are:

$$\begin{aligned} \hat{\rho}_A &= \text{Tr}_B \hat{\rho} = \begin{pmatrix} \rho_{00,00} + \rho_{01,01} & \rho_{00,10} + \rho_{01,11} \\ \rho_{10,00} + \rho_{11,01} & \rho_{10,10} + \rho_{11,11} \end{pmatrix}, \\ \hat{\rho}_B &= \text{Tr}_A \hat{\rho} = \begin{pmatrix} \rho_{00,00} + \rho_{10,10} & \rho_{00,01} + \rho_{10,11} \\ \rho_{01,00} + \rho_{11,10} & \rho_{01,01} + \rho_{11,11} \end{pmatrix}. \end{aligned}$$

Owing to the above formulas, one can easily calculate reduced states. For instance, the reductions of four states of the Bell base are:

$$\text{Tr}_B |B_k\rangle \langle B_k| = \frac{1}{2} \hat{1}_A, \quad \text{Tr}_A |B_k\rangle \langle B_k| = \frac{1}{2} \hat{1}_B,$$

for every  $k = 1, 2, 3, 4$ . Thus, all states of the Bell base have exactly the same reductions to both subsystems. By the way, we observe another peculiarity of the quantum mechanical description of composite systems: states of subsystems (the reduced states) do not determine the state of the whole system.

We conclude this Subsection with the announced earlier *criterion of entanglement*, which enables one to distinguish non-entangled pure states among all states of  $\mathbf{Q}_A + \mathbf{Q}_B$ : it should be clear now that a pure state of the joint system  $\mathbf{Q}_A + \mathbf{Q}_B$  is non-entangled if and only if its reduction to  $\mathbf{Q}_A$  (so also to  $\mathbf{Q}_B$ ) is a pure state, otherwise it is entangled. (The concept of entanglement for mixed states is too complicated to be discussed here.)

### 3.9. The time evolution of subsystems

It is a general rule of quantum mechanics to represent the time evolution of a conservative quantum system by means of a dynamical group of unitary maps; such a group is always equivalent to some particular Schrödinger equation. The definition of a unitary operator provided in Subsection 2.10 is generally valid, so operators which are components of a dynamical group of a quantum system should satisfy the condition:

$$\widehat{U}\widehat{U}^* = \widehat{1}.$$

That rule applies in particular to a two-qubit system; therefore the time evolution of a two-qubit system as a whole looks like the time evolution of any other quantum object. What is both peculiar and important here is the fact that a time evolution of a two-qubit system does not define, in a general case, any time evolution of the two qubits.

Let us begin with a formal problem. Take a unitary operator  $\widehat{U}_t$  which belongs to a dynamical group acting on a complex linear space  $\mathbb{C}^n$ . The action of  $\widehat{U}_t$  describes the time evolution from the instant 0 to the instant  $t$ : if  $|v\rangle$  is the state of a quantum system at time 0, then  $\widehat{U}_t|v\rangle$  is the state of the system at time  $t$ . That refers to pure states only; we should know how general states change in time, so how  $\widehat{U}_t$  acts on density operators. The density operator describing the pure state represented otherwise by the vector  $|v\rangle$  is the projection operator  $\widehat{P}_v = |v\rangle\langle v|$ . The projection operator corresponding to the pure state  $\widehat{U}_t|v\rangle$  is

$$\widehat{U}_t|v\rangle\langle v|\widehat{U}_t^* = \widehat{U}_t\widehat{P}_v\widehat{U}_t^*.$$

Taking into account that any density operator can be decomposed into a linear combination of projection operators (see Subsection 3.5), we conclude that the initial mixed state  $\widehat{\rho}$  of a quantum system should evolve under  $\widehat{U}_t$  into  $\widehat{U}_t\widehat{\rho}\widehat{U}_t^*$ ,

$$\widehat{\rho} \rightarrow \widehat{U}_t\widehat{\rho}\widehat{U}_t^*.$$

Returning to considered case of two-qubit systems, take a unitary operator  $\widehat{U}_t$  on  $\mathbb{C}_A^2 \otimes \mathbb{C}_B^2$ . If the initial (*i.e.* at the instant 0) state of the composite system  $\mathbf{Q}_A + \mathbf{Q}_B$  is represented by the density operator  $\widehat{\rho}$ , then the state at  $t$  is represented by  $\widehat{U}_t\widehat{\rho}\widehat{U}_t^*$ . Accordingly, the initial state of the subsystem  $\mathbf{Q}_A$  should be  $\text{Tr}_B\widehat{\rho}$  while the state at  $t$  -  $\text{Tr}_B\left(\widehat{U}_t\widehat{\rho}\widehat{U}_t^*\right)$ . The time evolution of the subsystem  $\mathbf{Q}_A$  induced by the time evolution of the composite system  $\mathbf{Q}_A + \mathbf{Q}_B$  is:

$$\text{Tr}_B\widehat{\rho} \rightarrow \text{Tr}_B\left(\widehat{U}_t\widehat{\rho}\widehat{U}_t^*\right).$$

The obtained "reduced dynamics", contrary to our expectations, is not of the unitary type: it can, for instance, transform the initial pure state into a mixed one (see an example in 3.12.5), while a unitary operator always transforms pure states into pure states. The situation is even worse: it can happen that

$$\mathrm{Tr}_B \hat{\rho}_1 = \mathrm{Tr}_B \hat{\rho}_2$$

for some density operators  $\hat{\rho}_1, \hat{\rho}_2$  on  $\mathbb{C}_A^2 \otimes \mathbb{C}_B^2$ , while

$$\mathrm{Tr}_B \left( \hat{U}_t \hat{\rho}_1 \hat{U}_t^* \right) \neq \mathrm{Tr}_B \left( \hat{U}_t \hat{\rho}_2 \hat{U}_t^* \right) ,$$

so that the a state of  $\mathbf{Q}_A$  would evolve into two different states - that means that "reduced dynamics" does not define any map on the set of density operators on  $\mathbb{C}_A^2$ .

Subsystems of a two-qubit system  $\mathbf{Q}_A + \mathbf{Q}_B$  evolve in a unitary way if and only if the dynamical group  $\left\{ \hat{U}_t \mid t \in \mathbb{R} \right\}$  on  $\mathbb{C}_A^2 \otimes \mathbb{C}_B^2$  preserves the tensor product structure of  $\mathbb{C}_A^2 \otimes \mathbb{C}_B^2$ , *i.e.* if and only if every  $\hat{U}_t$  maps tensor products into tensor products:

$$\hat{U}_t |v\rangle_A \otimes |w\rangle_B = |v'\rangle_A \otimes |w'\rangle_B$$

for every  $t \in \mathbb{R}$ ,  $|v\rangle_A \in \mathbb{C}_A^2$ , and  $|w\rangle_B \in \mathbb{C}_B^2$ . One can prove that in such a case there are two dynamical groups:  $\left\{ \hat{U}_{A,t} \mid t \in \mathbb{R} \right\}$  on  $\mathbb{C}_A^2$ , and  $\left\{ \hat{U}_{B,t} \mid t \in \mathbb{R} \right\}$  on  $\mathbb{C}_B^2$ , such that

$$\hat{U}_t = \hat{U}_{A,t} \otimes \hat{U}_{B,t}$$

for every  $t \in \mathbb{R}$ . There are sound physical reasons to believe that the obtained special "tensor product" time evolution of the composite system can occur only if there is no interaction between the two subsystems.

The fact that a general unitary map on  $\mathbb{C}_A^2 \otimes \mathbb{C}_B^2$  does not preserve the product structure of pure states leads to the paradoxes of entanglement, as a conservative evolution of  $\mathbf{Q}_A + \mathbf{Q}_B$  can transform  $|u\rangle_A \otimes |v\rangle_B$  into an entangled state.

### 3.10. Entanglement

The first demonstration of strange properties of non-product states of quantum composite systems was the Einstein, Podolsky, and Rosen (EPR) thought experiment (1935). The word *entanglement* is a free translation of the German term *Verschränkung*, introduced by Schrödinger (1936) in his throughout discussion of the EPR paper. The EPR example refers to a general, infinite-dimensional



Hilbert space. Its simplest finitely dimensional analogue involves the so called singlet state of the quantum system of two spin-half objects:

$$|B_4\rangle := \frac{1}{\sqrt{2}} (|01\rangle - |10\rangle),$$

which is one of states of the Bell base (see above). In fact, any other state of the Bell base would do equally well.

The corresponding density operator in the canonical base of  $\mathbb{C}_A^2 \otimes \mathbb{C}_B^2$  is:

$$|B_4\rangle\langle B_4| = \frac{1}{2} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

so the two reduced states are:

$$\begin{aligned} \text{Tr}_B |B_4\rangle\langle B_4| &= \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{2} \hat{1}_A, \\ \text{Tr}_A |B_4\rangle\langle B_4| &= \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{2} \hat{1}_B. \end{aligned}$$

Clearly, both obtained density operators (states of subsystems) are mixtures of the two states of canonical bases of  $\mathbb{C}_A^2$  and of  $\mathbb{C}_B^2$  respectively:

$$\begin{aligned} \text{Tr}_B |B_4\rangle\langle B_4| &= \frac{1}{2} (|0\rangle\langle 0|_A + |1\rangle\langle 1|_A), \\ \text{Tr}_A |B_4\rangle\langle B_4| &= \frac{1}{2} (|0\rangle\langle 0|_B + |1\rangle\langle 1|_B). \end{aligned}$$

Thus, we have proved that the EPR state  $|B_4\rangle$  of the two-qubit system is an entangled state.

Consider now the spin-component observables  $\hat{S}_{A,z} \otimes \hat{1}_B$ ,  $\hat{S}_{A,x} \otimes \hat{1}_B$  of the subsystem  $A$ , their spectral decompositions are:

$$\begin{aligned} \hat{S}_{A,z} \otimes \hat{1}_B &= \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \otimes \hat{1}_B - \frac{1}{2} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \otimes \hat{1}_B, \\ \hat{S}_{A,x} \otimes \hat{1}_B &= \frac{1}{2} \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes \hat{1}_B - \frac{1}{2} \frac{1}{2} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes \hat{1}_B, \end{aligned}$$

A von Neumann measurement of  $\widehat{S}_{A,z} \otimes \widehat{1}_B$  on  $|B_4\rangle$  should transform the original state into the statistical mixture of eigen-states which, according to the last formula of Subsection 3.5, is represented by the density operator

$$\widehat{\rho}_z = \left| \widehat{P}_{z,0} B_4 \right\rangle \left\langle \widehat{P}_{z,0} B_4 \right| + \left| \widehat{P}_{z,1} B_4 \right\rangle \left\langle \widehat{P}_{z,1} B_4 \right| ,$$

where

$$\widehat{P}_{z,0} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \otimes \widehat{1}_B , \quad \widehat{P}_{z,1} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \otimes \widehat{1}_B ,$$

and  $\left| \widehat{P}_j B_4 \right\rangle \left\langle \widehat{P}_j B_4 \right|$  denotes the projection operator defined by the vector  $\widehat{P}_j |B_4\rangle$ . It is easy to calculate that the post-measurement density operator is:

$$\widehat{\rho}_z = \frac{1}{2} |0, 1\rangle \langle 0, 1| + \frac{1}{2} |1, 0\rangle \langle 1, 0| = \frac{1}{2} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} .$$

Thus, according to what one could expect, the von Neumann measurement of the  $z$ -the component of spin of the subsystem  $A$  on the entangled state  $|B_4\rangle$  transforms the composite system into the mixed state of two states  $|0, 1\rangle$  and  $|1, 0\rangle$  with statistical weights  $\frac{1}{2}$ . Notice that the subsystem  $B$  after a single trial should be in one of the states  $|1\rangle_B$  or  $|0\rangle_B$  with probability  $\frac{1}{2}$ , so apparently should have its spin oriented along the  $z$ -the axis.

What happens if we would measure the  $x$ -th component of spin of the subsystem  $A$ ? Like above, a von Neumann measurement of  $\widehat{S}_{A,x} \otimes \widehat{1}_B$  on  $|B_4\rangle$  should transform the original state into the statistical mixture

$$\widehat{\rho}_x = \left| \widehat{P}_{x,0} B_4 \right\rangle \left\langle \widehat{P}_{x,0} B_4 \right| + \left| \widehat{P}_{x,1} B_4 \right\rangle \left\langle \widehat{P}_{x,1} B_4 \right| ,$$

where

$$\widehat{P}_{x,0} = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes \widehat{1}_B , \quad \widehat{P}_{x,1} = \frac{1}{2} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes \widehat{1}_B .$$

The post-measurement state is now

$$\widehat{\rho}_x = \frac{1}{2} |0_x, 1_x\rangle \langle 0_x, 1_x| + \frac{1}{2} |1_x, 0_x\rangle \langle 1_x, 0_x| = \frac{1}{4} \begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & -1 & 0 \\ 0 & -1 & 1 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix} .$$

We see that the von Neumann measurement of the  $x$ -the component of spin of the subsystem  $A$  on the entangled state  $|B_4\rangle$  transforms the composite system

into the mixed state of  $|0_x, 1_x\rangle$  and  $|1_x, 0_x\rangle$  with statistical weights  $\frac{1}{2}$ . Now, the subsystem  $B$  after a single trial should be in one of the states  $|1_x\rangle_B$  or  $|0_x\rangle_B$  with probability  $\frac{1}{2}$ , so apparently should have its spin oriented along the  $x$ -th axis !

A popular interpretation is the following: if the composite system is in the entangled state  $|B_4\rangle$ , spins of the two subsystems are strongly correlated in a mysterious way such that a von Neumann measurement of any spin component of the subsystem  $A$  change the direction of spin of the subsystem  $B$ . That is the alleged non-local effect discovered by EPR, and called the entanglement. A careful consideration shows (see the next Subsection) that this interpretation is unfounded.

Irrespective of the interpretation we assume, properties of entangled states are basic for quantum teleportation, quantum error correction, quantum dense coding, quantum cryptography, *etc.*

### 3.11. Bell's telephone

As an example of paradoxical properties of the EPR correlations we discuss briefly the following idea.

Many copies of the two-qubit system  $\mathbf{Q}_A + \mathbf{Q}_B$  are prepared in the state  $|B_4\rangle$  and then they are spatially separated: the ensemble of  $\mathbf{Q}_A$  is sent to Alice, while the ensemble of  $\mathbf{Q}_B$  to Bob. Now, if Alice wants to send a one-bit message to Bob, she chooses to measure (in the von Neumann way) either  $\widehat{S}_{A,z} \otimes \widehat{1}_B$  or  $\widehat{S}_{A,x} \otimes \widehat{1}_B$  for all samples of  $\mathbf{Q}_A$  she has. Her action prepares Bob's qubit  $\mathbf{Q}_B$  in the mixed state  $\frac{1}{2} |0\rangle \langle 0|_B + \frac{1}{2} |1\rangle \langle 1|_B$  (all spins along the  $z$ -th axis), or in  $\frac{1}{2} |0_x\rangle \langle 0_x|_B + \frac{1}{2} |1_x\rangle \langle 1_x|_B$  (all spins along the  $x$ -th axis). That suggests a mechanism for a faster-than-light communication, called the "Bell telephone".

A more careful discussion shows, however, a flaw in that scheme. It has been demonstrated above that Alice's measurement transforms the original state  $|B_4\rangle$  of  $\mathbf{Q}_A + \mathbf{Q}_B$  into  $\frac{1}{2} |0, 1\rangle \langle 0, 1| + \frac{1}{2} |1, 0\rangle \langle 1, 0|$  (if she decided to measure  $\widehat{S}_{A,z} \otimes \widehat{1}_B$ ), or into  $\frac{1}{2} |0_x, 1_x\rangle \langle 0_x, 1_x| + \frac{1}{2} |1_x, 0_x\rangle \langle 1_x, 0_x|$  (if she decided to measure  $\widehat{S}_{A,x} \otimes \widehat{1}_B$ ). What Bob can observe is the state of the subsystem  $\mathbf{Q}_B$ , which we calculate applying the reduction procedure of Subsection 3.8 to the post-measurement states. We obtain

$$\begin{aligned} \text{Tr}_A \left( \frac{1}{2} |0, 1\rangle \langle 0, 1| + \frac{1}{2} |1, 0\rangle \langle 1, 0| \right) &= \frac{1}{2} |0\rangle \langle 0|_B + \frac{1}{2} |1\rangle \langle 1|_B \\ &= \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{2} \widehat{1}_B \end{aligned}$$

when Alice measured  $\widehat{S}_{A,z} \otimes \widehat{1}_B$ , and

$$\begin{aligned}\mathrm{Tr}_A \left( \frac{1}{2} |0_x, 1_x\rangle \langle 0_x, 1_x| + \frac{1}{2} |1_x, 0_x\rangle \langle 1_x, 0_x| \right) &= \frac{1}{2} |0_x\rangle \langle 0_x|_B + \frac{1}{2} |1_x\rangle \langle 1_x|_B \\ &= \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{2} \widehat{1}_B\end{aligned}$$

when Alice measured  $\widehat{S}_{A,x} \otimes \widehat{1}_B$ . Thus, the two apparently different formulas,  $\frac{1}{2} |0\rangle \langle 0|_B + \frac{1}{2} |1\rangle \langle 1|_B$  and  $\frac{1}{2} |0_x\rangle \langle 0_x|_B + \frac{1}{2} |1_x\rangle \langle 1_x|_B$ , describe in fact the same state of  $\mathbf{Q}_B$ , so the message sent by Alice is unreadable for Bob. Bob, observing the subsystem  $\mathbf{Q}_B$ , is not able to distinguish between the two actions Alice can perform.

Moreover, the state of  $\mathbf{Q}_B$  after any of Alice's measurements is exactly the same as before: we have shown above that

$$\mathrm{Tr}_A |B_4\rangle \langle B_4| = \frac{1}{2} \widehat{1}_B.$$

Thus, Alice changes the state of the whole two-qubit system, but she does not change the state of Bob's qubit: Bob is even not aware that Alice has done something to her qubit! The same concerns Alice's qubit: her measurements do not change the reduced state of  $\mathbf{Q}_A$ , what can be calculated in the same way as above.

### 3.12. Two-qubit gates

Some unitary operators on the state space  $\mathbb{C}_A^2 \otimes \mathbb{C}_B^2$  of a two-qubit system are of particular importance for quantum computing, they are called *two-qubit gates*. Clearly, any pair of unitary operators  $\widehat{U}_A : \mathbb{C}_A^2 \rightarrow \mathbb{C}_A^2$ ,  $\widehat{U}_B : \mathbb{C}_B^2 \rightarrow \mathbb{C}_B^2$  defines the unitary operator  $\widehat{U}_A \otimes \widehat{U}_B$  on  $\mathbb{C}_A^2 \otimes \mathbb{C}_B^2$  (see Subsection 3.6), but there are also less trivial unitary operators on  $\mathbb{C}_A^2 \otimes \mathbb{C}_B^2$ .

#### 3.12.1. One-qubit gates for two-qubit systems

Let  $\widehat{U}_A : \mathbb{C}_A^2 \rightarrow \mathbb{C}_A^2$  be an arbitrary unitary map on the state space of the qubit  $\mathbf{Q}_A$ , in particular  $\widehat{U}_A$  can be one of the single-qubit gates mentioned above. The product  $\widehat{U}_A \otimes \widehat{1}_B$  is a unitary operator on  $\mathbb{C}_A^2 \otimes \mathbb{C}_B^2$ , in the canonical base

$$\begin{aligned}\widehat{U}_A \otimes \widehat{1}_B &= \begin{pmatrix} U_{A,00} & 0 & U_{A,01} & 0 \\ 0 & U_{A,00} & 0 & U_{A,01} \\ U_{A,10} & 0 & U_{A,11} & 0 \\ 0 & U_{A,10} & 0 & U_{A,11} \end{pmatrix} \\ &= \widehat{U}_A \otimes |0\rangle\langle 0|_B + \widehat{U}_A \otimes |1\rangle\langle 1|_B.\end{aligned}$$

The operator  $\widehat{U}_A \otimes \widehat{1}_B$  acting on a product state does not change the second factor:

$$\left(\widehat{U}_A \otimes \widehat{1}_B\right)(|v\rangle_A \otimes |w\rangle_B) = \left(\widehat{U}_A |v\rangle_A\right) \otimes |w\rangle_B,$$

while its action on the first factor is just the action of  $\widehat{U}_A$ . That explains the common interpretation of a gate like  $\widehat{U}_A \otimes \widehat{1}_B$  as the single-qubit gate  $\widehat{U}_A$  acting on a two-qubit system  $\mathbf{Q}_A + \mathbf{Q}_B$ . The gate  $\widehat{U}_A \otimes \widehat{1}_B$  is usually denoted  $\widehat{U}_A$ .

As an example we show that Pauli matrices considered as operators on  $\mathbb{C}_A^2 \otimes \mathbb{C}_B^2$  transform  $|B_4\rangle$  into vectors of the Bell basis (we will need this below, see Subsection 3.14):

$$\begin{aligned}\sigma_{x,A} \otimes \widehat{1}_B |B_4\rangle &= \frac{1}{\sqrt{2}} (\sigma_{x,A} |0\rangle_A \otimes |1\rangle_B - \sigma_{x,A} |1\rangle_A \otimes |0\rangle_B) \\ &= \frac{1}{\sqrt{2}} (|11\rangle - |00\rangle) = -|B_2\rangle \\ \sigma_{y,A} \otimes \widehat{1}_B |B_4\rangle &= \frac{1}{\sqrt{2}} (\sigma_{y,A} |0\rangle_A \otimes |1\rangle_B - \sigma_{y,A} |1\rangle_A \otimes |0\rangle_B) \\ &= \frac{i}{\sqrt{2}} (|11\rangle + |00\rangle) = i|B_1\rangle, \\ \sigma_{z,A} \otimes \widehat{1}_B |B_4\rangle &= \frac{1}{\sqrt{2}} (\sigma_{z,A} |0\rangle_A \otimes |1\rangle_B - \sigma_{z,A} |1\rangle_A \otimes |0\rangle_B) \\ &= \frac{1}{\sqrt{2}} (|01\rangle + |10\rangle) = |B_3\rangle, \\ \widehat{1}_A \otimes \widehat{1}_B |B_4\rangle &= \widehat{1} |B_4\rangle = |B_4\rangle.\end{aligned}$$

### 3.12.2. Two-qubit NOT gate

The *two-qubit NOT gate* is the two-qubit gate which flips the state of every qubit. It is simply the tensor product of two single-qubit NOT gates:

$$\widehat{U}_{\text{NOT}} := \widehat{U}_{\text{NOT},A} \otimes \widehat{U}_{\text{NOT},B} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix},$$

acting independently on both qubits:

$$\begin{aligned} \widehat{U}_{\text{NOT}} |00\rangle &= |11\rangle, & \widehat{U}_{\text{NOT}} |01\rangle &= |10\rangle, \\ \widehat{U}_{\text{NOT}} |10\rangle &= |01\rangle, & \widehat{U}_{\text{NOT}} |11\rangle &= |00\rangle. \end{aligned}$$

The two-qubit NOT gate is usually called just NOT gate, because the context implies that it acts on two qubits.

It is interesting to note that vectors of the Bell base are eigenstates of the two-qubit NOT gate:

$$\begin{aligned} \widehat{U}_{\text{NOT}} |B_1\rangle &= |B_1\rangle, & \widehat{U}_{\text{NOT}} |B_2\rangle &= -|B_2\rangle, \\ \widehat{U}_{\text{NOT}} |B_3\rangle &= |B_3\rangle, & \widehat{U}_{\text{NOT}} |B_4\rangle &= -|B_4\rangle. \end{aligned}$$

### 3.12.3. Two-qubit Hadamard gate

The tensor product of two Hadamard gates  $\widehat{U}_{A,H} \otimes \widehat{U}_{B,H}$  performs the Hadamard transform on every of the two qubits separately. The matrix form of the *two-qubit Hadamard gate*  $\widehat{U}_H$  is:

$$\begin{aligned} \widehat{U}_H &:= \widehat{U}_{A,H} \otimes \widehat{U}_{B,H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \\ &= \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \end{aligned}$$

The two-qubit Hadamard gate acting on vectors of the canonical base produces superpositions of all vectors of the canonical base which, however, are not entangled. For instance:

$$\begin{aligned} \widehat{U}_H |00\rangle &= \widehat{U}_{A,H} |0\rangle_A \otimes \widehat{U}_{B,H} |0\rangle_B \\ &= \frac{1}{\sqrt{2}} (|0\rangle_A + |1\rangle_A) \otimes \frac{1}{\sqrt{2}} (|0\rangle_B + |1\rangle_B) \\ &= \frac{1}{2} (|00\rangle + |01\rangle + |10\rangle + |11\rangle). \end{aligned}$$

### 3.12.4. Two-qubit product gates and one-qubit gates

A direct calculation demonstrates that

$$\left(\widehat{U}_A \otimes \widehat{1}_B\right) \left(\widehat{1}_A \otimes \widehat{U}_B\right) = \widehat{U}_A \otimes \widehat{U}_B$$

for any two unitary operators  $\widehat{U}_A, \widehat{U}_B$ . It means that the action of  $\widehat{1}_A \otimes \widehat{U}_B$  followed by  $\widehat{U}_A \otimes \widehat{1}_B$  is the same as the simultaneous action of both  $\widehat{U}_A$  and  $\widehat{U}_B$  on the respective qubits. Thus, in particular, the two-qubit Hadamard gate  $\widehat{U}_H = \widehat{U}_{A,H} \otimes \widehat{U}_{B,H}$  can be realized as the successive action  $\left(\widehat{U}_{A,H} \otimes \widehat{1}_B\right) \left(\widehat{1}_A \otimes \widehat{U}_{B,H}\right)$  of two one-qubit Hadamard gates.

### 3.12.5. CNOT gate

The *controlled-NOT gate* (the CNOT gate) is represented in the canonical base by the  $4 \times 4$  unitary matrix

$$\begin{aligned} \widehat{U}_{\text{CNOT}} &:= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \\ &= |0\rangle \langle 0|_A \otimes \widehat{1}_B + |1\rangle \langle 1|_A \otimes \widehat{U}_{B,\text{NOT}}. \end{aligned}$$

The action of  $\widehat{U}_{\text{CNOT}}$  on vectors of the canonical base of  $\mathbb{C}_A^2 \otimes \mathbb{C}_B^2$  is:

$$\begin{aligned} \widehat{U}_{\text{CNOT}} |00\rangle &= |00\rangle, & \widehat{U}_{\text{CNOT}} |01\rangle &= |01\rangle, \\ \widehat{U}_{\text{CNOT}} |10\rangle &= |11\rangle, & \widehat{U}_{\text{CNOT}} |11\rangle &= |10\rangle. \end{aligned}$$

Thus, if the qubit  $\mathbf{Q}_A$  is in the state  $|0\rangle_A$ , then  $\widehat{U}_{\text{CNOT}}$  does not change the state of the qubit  $\mathbf{Q}_B$ , while if  $\mathbf{Q}_A$  is in the state  $|1\rangle_A$ , then  $\widehat{U}_{\text{CNOT}}$  flips the state of  $\mathbf{Q}_B$ . Because of that,  $\mathbf{Q}_A$  is called the *control* qubit, while  $\mathbf{Q}_B$  - the *target* qubit.

The name "control qubit" is misleading as it suggests that no state of  $\mathbf{Q}_A$  is changed by the CNOT gate. It is not true: if, for instance,  $\widehat{U}_{\text{CNOT}}$  acts on  $\frac{1}{\sqrt{2}}(|0\rangle_A + |1\rangle_A) \otimes |0\rangle_B$ , we obtain

$$\begin{aligned} \widehat{U}_{\text{CNOT}} \frac{1}{\sqrt{2}} (|0\rangle_A + |1\rangle_A) \otimes |0\rangle_B &= \frac{1}{\sqrt{2}} \widehat{U}_{\text{CNOT}} |00\rangle + \frac{1}{\sqrt{2}} \widehat{U}_{\text{CNOT}} |10\rangle \\ &= \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) = |B_1\rangle, \end{aligned}$$

so  $\widehat{U}_{\text{CNOT}}$  transforms the original pure state  $\frac{1}{\sqrt{2}}(|0\rangle_A + |1\rangle_A)$  of  $\mathbf{Q}_A$  into the mixed state

$$\text{Tr}_B |B_1\rangle \langle B_1| = \frac{1}{2} \widehat{1}_A,$$

comp. Subsection 3.8. By the way, we get an example illustrating the statement of Subsection 3.9 that the reduced dynamics is able to transform pure states into mixed.

The action of two CNOT gates one after the other does not change anything:

$$\widehat{U}_{\text{CNOT}} \widehat{U}_{\text{CNOT}} = \widehat{1},$$

what is easy to check. That means that the second CNOT gate nullifies what the first one has done. In particular, applying this to the last example we get:

$$\begin{aligned} \widehat{U}_{\text{CNOT}} \widehat{U}_{\text{CNOT}} \frac{1}{\sqrt{2}} (|0\rangle_A + |1\rangle_A) \otimes |0\rangle_B &= \widehat{U}_{\text{CNOT}} \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \\ &= \frac{1}{\sqrt{2}} (|0\rangle_A + |1\rangle_A) \otimes |0\rangle_B, \end{aligned}$$

what shows that  $\widehat{U}_{\text{CNOT}}$  can transform some entangled states into non-entangled ones. Such a transformation of an entangled state into a non-entangled one is called *disentanglement*.

The CNOT gate is also called the *quantum XOR gate*, because its action on vectors of the canonical base can be briefly summarized as:

$$\widehat{U}_{\text{CNOT}} |ij\rangle = |i, i \oplus j\rangle,$$

where  $i, j = 0, 1$ , and  $\oplus$  denotes the addition modulo 2.

It should be noticed that one can change the role of qubits and take  $\mathbf{Q}_A$  to be the target qubit, and  $\mathbf{Q}_B$  - to be the control one. Such modified CNOT gate  $\widehat{U}'_{\text{CNOT}}$  acts on the canonical base in the following way:

$$\widehat{U}'_{\text{CNOT}} |ij\rangle = |i \oplus j, j\rangle.$$

The matrix form of  $\widehat{U}'_{\text{CNOT}}$  is:

$$\widehat{U}'_{\text{CNOT}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

The CNOT gate is probably the simplest two-qubit gate which does not decompose into a tensor product of single-qubit gates, hence its action can produce



entangled states. It became very popular since the discovery [1] that every (multi-qubit) quantum gate can be decomposed into a sequence of one-qubit rotations and two-qubit CNOT gates.

### 3.12.6. Controlled-U gate

The CNOT gate admits a natural generalization: if  $\widehat{U}_B$  is an arbitrary single-qubit gate acting on  $\mathbf{Q}_B$ ,

$$\widehat{U}_B = \begin{pmatrix} U_{B,00} & U_{B,01} \\ U_{B,10} & U_{B,11} \end{pmatrix},$$

then the  $4 \times 4$  matrix

$$\begin{aligned} \widehat{U}_{C-U} &:= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & U_{B,00} & U_{B,01} \\ 0 & 0 & U_{B,10} & U_{B,11} \end{pmatrix} \\ &= |0\rangle\langle 0|_A \otimes \widehat{1}_B + |1\rangle\langle 1|_A \otimes \widehat{U}_B \end{aligned}$$

acts on the canonical base in the way generalizing the action of CNOT gate:

$$\begin{aligned} \widehat{U}_{C-U} |00\rangle &= |00\rangle, & \widehat{U}_{C-U} |01\rangle &= |01\rangle, \\ \widehat{U}_{C-U} |10\rangle &= |1\rangle_A \otimes \widehat{U}_B |0\rangle_B, \\ \widehat{U}_{C-U} |11\rangle &= |1\rangle_A \otimes \widehat{U}_B |1\rangle_B. \end{aligned}$$

Such a gate is called the *controlled-U gate*.

### 3.12.7. Two-qubit quantum Fourier transform

The  $n$ -qubit gate called *quantum Fourier transform* is an important ingredient of the Shor factorization algorithm. In the considered case of two qubits, the quantum Fourier transform is described by the matrix:

$$\widehat{U}_F = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}.$$

### 3.13. Simple quantum circuits

#### 3.13.1. Diagrams for quantum circuits

A quantum algorithm consists of a sequence of quantum gates acting one after another, such a sequence is called a *quantum gate array* or a *quantum circuit*. In the traditional quantum-mechanical notation, a quantum gate array is described simply as the sequence of corresponding unitary operators. For instance,

$$\hat{U}_H \hat{U}_{\text{CNOT}} |w\rangle$$

means that the CNOT gate acts on the two-qubit state  $|w\rangle$ , and then the two-qubit Hadamard gate acts on the resulting state. However, if the number of involved operators increases, formulas of that kind become obscure.

A more convenient notation is provided by special diagrams, called sometimes *quantum networks*. General rules of drawing such diagrams are:

- qubits are denoted by horizontal lines symbolizing their time evolution, time flows from left to right,
- initial/final state of a qubit is denoted by a symbol placed at the left/right end of the corresponding line,
- particular one-qubit gates are denoted by symbols placed on the corresponding lines,
- particular two-qubit gates are denoted by symbols on two corresponding lines connected by a vertical line,
- general gates are denoted by vertical rectangles overlapping the lines corresponding to the qubits they act on.

There are also more specific rules introduced *ad hoc* by various authors. We provide below simple examples of quantum circuits for two qubits.

#### 3.13.2. Quantum circuit creating entangled states

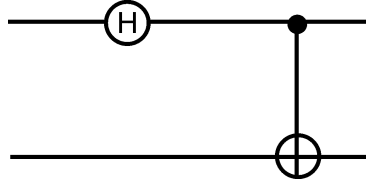
Let us recall that the Hadamard gate transforms vectors of the canonical base of  $\mathbf{Q}_A$  into their superpositions:

$$\hat{U}_{A,H} |0\rangle_A = \frac{1}{\sqrt{2}} (|0\rangle_A + |1\rangle_A), \quad \hat{U}_{A,H} |1\rangle_A = \frac{1}{\sqrt{2}} (|0\rangle_A - |1\rangle_A).$$

Hence, the successive application of  $\hat{U}_{A,H}$  to  $|0\rangle_A$ , and then of  $\hat{U}_{\text{CNOT}}$  to  $(\hat{U}_{A,H} |0\rangle_A) \otimes |0\rangle_B$  produces an entangled state:

$$\begin{aligned}
\hat{U}_{\text{CNOT}} (\hat{U}_{A,H} \otimes \hat{1}_B) |00\rangle &= \hat{U}_{\text{CNOT}} \frac{1}{\sqrt{2}} (|0\rangle_A + |1\rangle_A) \otimes |0\rangle_B \\
&= \hat{U}_{\text{CNOT}} \frac{1}{\sqrt{2}} (|00\rangle + |10\rangle) \\
&= \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)
\end{aligned}$$

The two gates acting one after another provide a simple example of a quantum gate array. The corresponding diagram is:

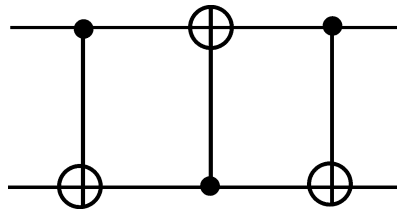


It is easy to check that the above defined circuit transforms vectors of the canonical base into vectors of the Bell base:

$$\begin{aligned}
\hat{U}_{\text{CNOT}} \hat{U}_{A,H} |00\rangle &= \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) = |B_1\rangle, \\
\hat{U}_{\text{CNOT}} \hat{U}_{A,H} |01\rangle &= \frac{1}{\sqrt{2}} (|01\rangle + |10\rangle) = |B_3\rangle, \\
\hat{U}_{\text{CNOT}} \hat{U}_{A,H} |10\rangle &= \frac{1}{\sqrt{2}} (|00\rangle - |11\rangle) = |B_2\rangle, \\
\hat{U}_{\text{CNOT}} \hat{U}_{A,H} |11\rangle &= \frac{1}{\sqrt{2}} (|01\rangle - |10\rangle) = |B_4\rangle.
\end{aligned}$$

### 3.13.3. Swap gate

It appears useful in some circumstances to interchange states of two qubits. This can be achieved by a successive action of three CNOT gates:



Indeed, this simple quantum gate array swaps states of  $\mathbf{Q}_A$  and  $\mathbf{Q}_B$  in the canonical base:

$$\begin{aligned}\widehat{U}_{\text{CNOT}}\widehat{U}'_{\text{CNOT}}\widehat{U}_{\text{CNOT}}|ij\rangle &= \widehat{U}_{\text{CNOT}}\widehat{U}'_{\text{CNOT}}|i, i \oplus j\rangle \\ &= \widehat{U}_{\text{CNOT}}|j, i \oplus j\rangle \\ &= |ji\rangle ,\end{aligned}$$

where  $i, j = 0, 1$ , and  $\widehat{U}'_{\text{CNOT}}$  denotes the CNOT gate with  $\mathbf{Q}_A$  - the target qubit. The matrix form of that circuit:

$$\begin{aligned}\widehat{U}_{\text{CNOT}}\widehat{U}'_{\text{CNOT}}\widehat{U}_{\text{CNOT}} &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} .\end{aligned}$$

An elementary calculation shows that the described circuit, called the *swap gate*, interchanges states of two qubits in arbitrary product state:

$$\widehat{U}_{\text{CNOT}}\widehat{U}'_{\text{CNOT}}\widehat{U}_{\text{CNOT}}|v\rangle_A \otimes |w\rangle_B = |w\rangle_A \otimes |v\rangle_B .$$

### 3.14. Dense coding

The "single-qubit channel" described in Subsection 2.9 becomes more efficient if Alice and Bob would use a pair of entangled qubits. Suppose that the two-qubit system  $\mathbf{Q}_A + \mathbf{Q}_B$  was prepared in the entangled state  $|B_4\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ , and then the qubit  $\mathbf{Q}_A$  was sent to Alice and  $\mathbf{Q}_B$  to Bob. Alice is going to use her qubit to send a two-bit message to Bob. She knows that the four Pauli matrices transform  $|B_4\rangle$  into four mutually orthogonal states of the Bell base (see above):

$$\begin{aligned}\sigma_{x,A} \otimes \widehat{1}_B |B_4\rangle &= -|B_2\rangle \\ \sigma_{y,A} \otimes \widehat{1}_B |B_4\rangle &= i|B_1\rangle , \\ \sigma_{z,A} \otimes \widehat{1}_B |B_4\rangle &= |B_3\rangle , \\ \widehat{1}_A \otimes \widehat{1}_B |B_4\rangle &= |B_4\rangle ,\end{aligned}$$

so she infers that her "local" action on the qubit  $\mathbf{Q}_A$  by means of one of the four Pauli gates will change the state of the two-qubit system  $\mathbf{Q}_A + \mathbf{Q}_B$ .

However, Bob, observing his qubit, is not able to identify Alice's manipulations, as the reductions to  $\mathbf{Q}_B$  of all Bell states are the same:

$$\text{Tr}_A |B_k\rangle \langle B_k| = \frac{1}{2} \hat{1}_B, \quad k = 1, 2, 3, 4$$

(see Subsection 3.8). The situation resembles that of the Bell telephone. What Alice can do is to send her qubit to Bob through the one-qubit channel they are linked up: having both qubits Bob obtains the possibility to control the whole system  $\mathbf{Q}_A + \mathbf{Q}_B$  and to identify its state.

How he could do that? The four states of the Bell base are mutually orthogonal, so we can easily construct a self-adjoint operator which has four non-degenerate eigenvalues, and such that its set of eigenstates is exactly the Bell base. A general form of such an operator is:

$$\hat{Q} = \sum_{k=1}^4 q_k |B_k\rangle \langle B_k|,$$

where  $q_1, \dots, q_4$  are arbitrarily chosen and mutually distinct real numbers. Any of such operators, according to the firm belief of physicists, represents some experimentally measurable quantity (an observable). If then Bob would measure  $\hat{Q}$  on the global state of  $\mathbf{Q}_A + \mathbf{Q}_B$ , the result of a single trial will identify the state of  $\mathbf{Q}_A + \mathbf{Q}_B$ , because the pre-measurement state (prepared by Alice) is one of eigenstates of  $\hat{Q}$ .

The quantum information channel which we just described is in many respects similar to that introduced in Subsection 2.9. The encoding apparatus is here the one which can implement arbitrary one-qubit Pauli gate, while the decoding is provided by a single measurement of an observable  $\hat{Q}$ . What is essentially new, is that both Alice and Bob have to their disposal qubits which together are in an entangled state. Owing to this, the single qubit sent by Alice to Bob was a carrier of two bits of classical information, because Alice's choice of one of four Pauli gates encoded two classical bits.

What is also remarkable in the described "entanglement enhanced one-qubit channel" is that Alice's transmission is perfectly secure against eavesdropping. Eve, the snaky enemy of Alice and Bob, cannot read any information off the qubit sent by Alice, because  $\mathbf{Q}_A$  alone is in the state  $\frac{1}{2} \hat{1}_A$  for every Bell state of  $\mathbf{Q}_A + \mathbf{Q}_B$ . The information Alice sends to Bob is coded in the mutual correlations between  $\mathbf{Q}_A$  and  $\mathbf{Q}_B$ , so can be read off only if one gets both qubits.

#### 4. Concluding remarks

In the second part of this paper we want to describe three-qubit systems, three-qubit gates and three-qubit gate arrays, and the effect called quantum teleportation which appears to be an important resource for quantum computation. We will discuss also the general concept of quantum gate array, provide simple examples of such arrays, and explain the role of quantum parallelism. Finally we are going to present examples of quantum algorithms.

A reader who wants to see the most recent original papers on quantum computing is referred to the Los Alamos e-print archive at <http://arXiv.org>

#### References

- [1] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, H. Weinfurter: *Elementary gates for quantum computation*. Physical Review A 52 (1995) 3457 - 3467.
- [2] D. Deutsch: *Quantum theory, the Church - Turing principle and the universal quantum computer*. Proceedings of the Royal Society London A 400 (1985) 97 - 117.
- [3] D. Deutsch: *Quantum computational networks*. Proceedings of the Royal Society London A 425 (1989) 73 - 90.
- [4] A. Ekert, R. Jozsa: *Quantum computation and Shor's factoring algorithm*. Reviews of Modern Physics 68 (1996) 733 - 753.
- [5] R. P. Feynman: *Quantum mechanical computers*. Optics News 11 (1985) 11 - 20. Reprinted in *Feynman Lectures on Computation*. Edited by A. J. G. Hey, R. W. Allen. (Addison - Wesley Publ. Co., Reading, Mass., 1996).
- [6] J. von Neumann: *Mathematische Grundlagen der Quantenmechanik* (Springer, Berlin, 1932). *Mathematical Foundations of Quantum Mechanics* (Princeton University Press, Princeton, N.J., 1955).
- [7] J. Preskill: *Quantum computing: pro and con*. In: *Proceedings of the ITP Conference on Quantum Coherence and Decoherence*, 17 Dec. 1996.
- [8] J. Preskill: *Quantum Information and Quantum Computation*. Lecture notes 1998 - 1999. <http://www.theory.caltech.edu/~preskill/ph229>

#### Podstawy obliczeń kwantowych. Część I

##### Streszczenie:

Artykuł przedstawia podstawowe własności układów kwantowo-mechanicznych, istotne dla obliczeń kwantowych. Następujące pojęcia są szczegółowo opisane: qubit, superpozycja stanów, pomiar, splątanie, bramka kwantowa, obwód kwantowy, kwantowy kanał informacyjny, gęste kodowanie, i inne. Rozważa się typowe bramki jedno- i dwu-qubitowe, jak również proste przykłady obwodów kwantowych.