Quantum Computing

I.Quantum bits, gates and circuits

Ivan Bolesta
dept. of Electronics and Computer Technologies
Ivan Franko National university of Lviv
Lviv, Ukraine
bolesta@electronics.lnu.edu.ua

Oleksii Kushnir
dept. of Electronics and Computer Technologies
Ivan Franko National university of Lviv
Lviv, Ukraine
alex.kuschnir@gmail.com

Serhiy Velhosh
dept. of Electronics and Computer Technologies
Ivan Franko National university of Lviv
Lviv, Ukraine
velgosh@electronics.lnu.edu.ua

Yuriy Furgala
dept. of optoelectronics and Information Technologies
Ivan Franko National university of Lviv
Lviv, Ukraine
yuriy.furhala@lnu.edu.ua

Abstract—**Using the formalism of the Boolean algebra, the process of computation in quantum computers is analyzed. The description of quantum bits - qubits - in the Hilbert space is given, quantum logic elements, quantum networks and the structure of an ideal quantum computer are considered. Peculiarities of quantum mechanical calculations related to the superposition principle, the interference of complex amplitudes and the existence of entangled states are discussed.**

Index Terms—**qubits, quantum logic elements, quantum circuits, quantum mechanical calculations, quantum computer.**

I. BITS AND QUBITES

The basic element in the classical computing model is the bit variable, which can only accept two values: "1" and "0" which, in the mathematical description in the context of the Boolean algebra, are called "truth" and "false".

Technically, bits are implemented as transistor-transistor devices that can be localized in two stable states, by which Boolean operations AND, OR and NOT can be expressed.

Development of submicron technologies in the production of integrated circuits at the end of the XX and in the at the beginning of the XXI century, in fact, led physical constraints achieved, since the size of the active elements of integral systems (IC) became commensurate with the characteristic lengths of the physical processes such as the diffusion length of charged carriers, the free path length and the wavelength of the de Broglie carriers that describe the work of the IC.

Physical and technological limitations have led to the creation of quantum informatics, the basic concept of which is a quantum bit - a qubit, which is understood as a quantum mechanical system that can be in two states [1].

In a two-dimensional Hilbert space the state of qubit is described by the vector, which in Dirac's notation is called a ket-vector [2]:

$$|\psi>=\begin{pmatrix} a \\ b \end{pmatrix}=a\,|0>+b\,|1>, \qquad (1)$$

where $|0>=\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1>=\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ are the orthogonal base vectors, and in the general case the complex numbers *a* and *b*, called probability amplitudes, satisfy the condition

$$|a|^2+|b|^2=1. \qquad (2)$$

The equation (1) shows that, unlike the classical bits, which may either be in the state of "0" or in the state "1", the qubit exists in a superposition state, the understanding of which is possible only from the point of view of quantum mechanics [2,3].

In the case of real values of probability amplitudes $a=\cos\varphi$ and $b=\sin\varphi$, condition (2) is performed automatically, and sets the range of the unit radius (Fig. 1a).

At complex values of amplitudes of probabilities $a=e^{i\gamma}\cos\frac{\theta}{2}$, and $b=e^{i\lambda}\sin\frac{\theta}{2}$, the expression (1) can be rewritten as:

$$|\psi>=e^{i\gamma}\left[\cos\frac{\theta}{2}|0>+e^{i\varphi}\sin\frac{\theta}{2}|1>\right], \qquad (3)$$

where $\varphi=\lambda-\gamma$, and θ are real numbers.

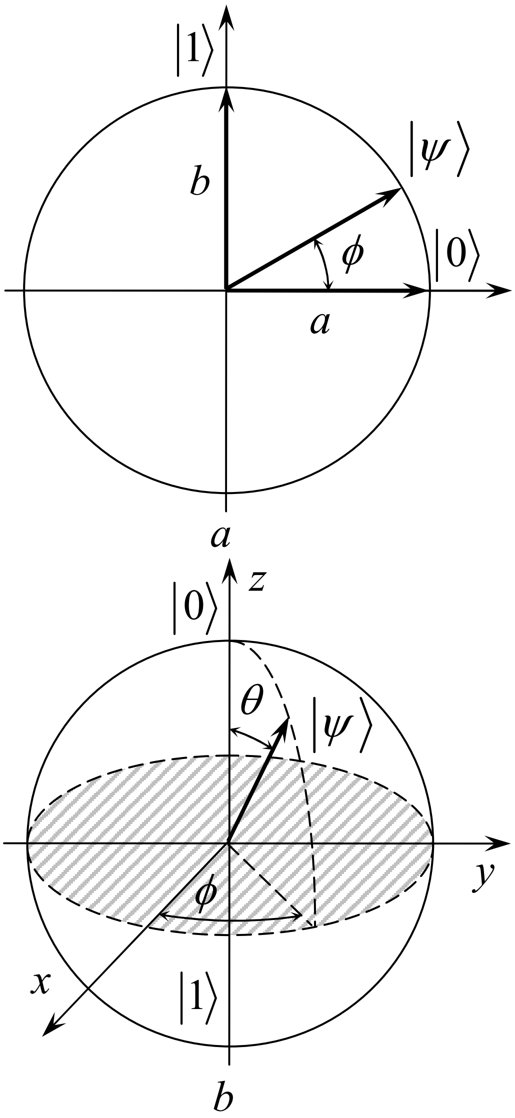

Fig. 1. Geometric representation of qubit in the case of real numbers of probability amplitudes as a point on a unit circle (a) and in the case of complex numbers of probability amplitudes as a point on a Bloch unit sphere (b).

Since the quantum-mechanical states $|\psi\rangle$ and $c|\psi\rangle$ (c – complex constant) are identical [2], the ratio (3) shown, that the state of qubit is determined by two parameters, which can be interpreted as coordinates of the spherical system. So, in this case, the geometric image of the qubit is a point on the sphere of a unite radius - the Bloch unite sphere (fig. 1b) [1].

In a system (register) of several qubits, a superpositional state is formed for the whole system. The basis for such a system is formed as a tensor product of the states of each qubit. In general case the tensor product of the matrices A with dimension $m \times n$ and B with dimension $r \times s$, their tensor product is called the matrix with dimensionality $mr \times ns$ that is obtained according to the rule [1]:

$$A \otimes B = \begin{pmatrix} a_{11}B \; a_{12}B \ldots a_{1n}B \\ a_{21}B \; a_{22}B \ldots a_{2n}B \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1}B \; a_{m2}B \ldots a_{mn}B \end{pmatrix}$$

According to those procedure $2^2 = 4$ basis vectors for the two- qubits system appear to be as follows:

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

They form an orthogonal basis, the state vector $|\psi\rangle$ in this basis is recorded as

$$|\psi\rangle = \sum_{i_1,i_2=\{0,1\}} a_{i_1 i_2} |i_1, i_2\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle,$$

were probability amplitudes satisfy the condition $a_{00}^2 + a_{01}^2 + a_{10}^2 + a_{11}^2 = 1$.

In general case the state vector for the n qubits system is a schedule based on the 2^n basic states of the system $|i_1 \ldots i_n\rangle$, $i_1 \ldots i_n = \{0,1\}$ [3]:

$$|\psi\rangle = \sum_{i_1 \ldots i_n} a_{i_1 \ldots i_n} |i_1 \ldots i_n\rangle. \qquad (4)$$

In other words, the base state $|i_1 \ldots i_n\rangle$ is a n dimensional binary number $|x\rangle$, whose digits coincide with the numbers $i_1 \ldots i_n = \{0,1\}$. In these notation, the state of vector (4) is recorded in the form:

$$|\psi\rangle = \sum_{x=0}^{2^{n-1}} a_x |x\rangle. \qquad (5)$$

II. Quantum gates and sircuits

In classical computers the computational process can be described by the formalism of Boolean algebra:

$$f : \{0,1\}^n \to \{0,1\}^m, \qquad (6)$$

which transforms the state of the n bits in the state of the m bits. Such functions are "constructed" from certain blocks, using schematic approaches, and are called logical elements (LEs) (or values). These functions also form a basis, which is understood as the minimum number of elements through which you can express an arbitrary function.

In a quantum computation model, the state of a qubit $|\psi\rangle$ under the action of a certain physical variable is changing. From the geometric interpretation of the qubit, it follows that the change in the state of the qubit is due to its rotation in the Hilbert space.

It is known [2,3] that quantum mechanics physical quantities are assigned to the matching Hermitian operator, to which in turn, matrix is matched in a Hilbert space. Within this formalism, the qubit rotation can be described by changing the basis, which provides the method for finding the matrices of the corresponding rotation as a product of the ket-vector on the bra-vector: $|i\rangle\langle j|$.

For example, if the operator carries out the following transformation of the basis: $|0> \to |0>$; $|1> \to |1>$, then the matrix of such an operator will be unitary:

$$I = |0><0| + |1><1| = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

The operator X, which carries out the following transformations of the basis: $|0> \to |1>$; $|1> \to |0>$, have the matrixc

$$X : |0><1| + |1><0| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \sigma_x .$$

This unitary operator is an analogue of the classical "NOT": because it rearranges the coefficients *a* and *b* in (1):

$$X|\psi\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} b \\ a \end{pmatrix}.$$

Other important standard single-qubit elements are the *Y* and *Z* elements, whose matrices are Pauli matrices

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

Of great importance is the transformation of Hadamard H, which carries out such a transformation of the basis: $|0> \to \frac{1}{\sqrt{2}}(0> + |1>)$; $|1> \to \frac{1}{\sqrt{2}}(0> - |1>)$.

Its matrix will look like:

$$U_H : \frac{1}{\sqrt{2}}\left[\left(|1><0| + |0><1|\right) + \left(|1><0| - |0><1|\right)\right] = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

This operator is often used in quantum algorithms.

Graphical representation of a one – qubit quantum gate U is depicted as

Gates can be applied to a system of two and more qubits. The most important two-qubites gate is "CNOT" (driven "NOT") (fig, 2a).

Its essence is that when the first - the control cubit in a state $|1>$, then the second - the "controlled"- target - qubit,- changes to the opposite (fig.2b):

$$CNOT|00> = |00>; \; CNOT|01> = |01>;$$

$$CNOT|10> = |11>; \; CNOT|11> = |10>.$$

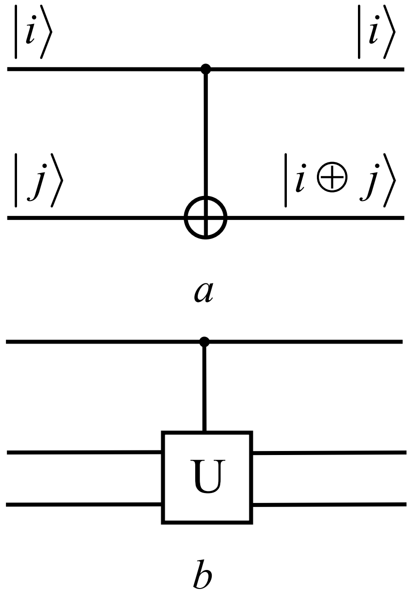

Fig.2 Conditional representation of CNOT gate (a) and CU gate (b)

In the general case, an arbitrary unitary transformation U can be controlled by adding one more qubit, which will depend on whether U transformation is performed:

$$CU\left(|0> \otimes |\varphi>\right) = |0> \otimes |\varphi>;$$

$$CU\left(|1> \otimes |\varphi>\right) = |0> \otimes U|\varphi>.$$

His matrix will look as $CU = \begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix}$, where I - the unit size $2^n \times 2^n$ matrix, n - the number of cubits in the register $|\varphi>$.

Often in quantum algorithms, the so-called oracles are used, which are quantum analogues of black boxes: the corresponding function (6) is called the oracle unitary transformation that calculates this function:

$$U_f : \{0,1\}^{n+m} \to \{0,1\}^{n+m} \qquad (7)$$

The input for calculating the function f is a register x of n qubits. At the output of the oracle, the result of the calculation of the function is added to the module 2 with the auxiliary register y of m qubits (fig. 3).

III. Principles of buildings and work of ideal quantum computer

The above approaches to the formation and management of the state of the system of qubits are described by such a schematic diagram of an ideal quantum computer (Fig. 3)

The register - vector of n qubits (5) - is fed to a device that performs unitary transformation $U\left(2^n \times 2^n\right)$. The calculation process on a quantum computer is the transformation of the input vector $|\psi\rangle_{in}$ into a finite vector $|\psi\rangle_f$ by multiplying it into a unitary matrix of size $2^n \times 2^n$:

$$|\psi\rangle_f = U\left(2^n \times 2^n\right)|\psi\rangle_{in} \tag{8}$$

From equation (8) it follows that the algorithm of the solution of the problem is included in the matrix of unitary transformation.

To implement the necessary conversion, an approach is used, which is called quantum circuitry - diagrams that visualize quantum algorithms. The main task of quantum circuit engineering lies in the synthesis and analysis of quantum circuits, created from quantum elements that form the required computational process. Such schemes are formed on a basic set of quantum logical elements.

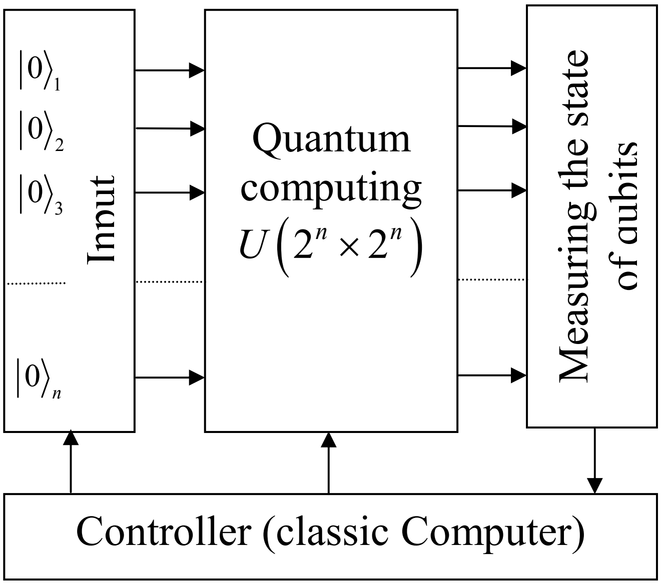
$|0\rangle_1$
$|0\rangle_2$
$|0\rangle_3$
$|0\rangle_n$
Innut
Quantum computing $U\left(2^n \times 2^n\right)$
Measuring the state of qubits
Controller (classic Computer)

Fig. 3. Diagram of ideal quantum computer.

Information about its solution is in the final vector $|\psi\rangle_f$, for which it is necessary to measure its state.

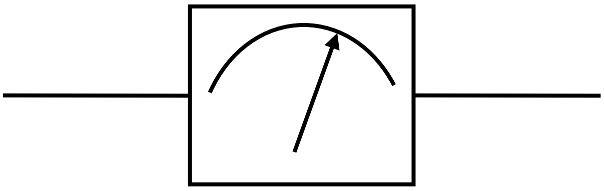

Fig. 4. Conditional designation of measurement operation.

The evolution of the state of the input register with the unitary transformation and measurement of the state of the output qubit is carried out by external classical signals, whose work, in turn, is guided by the classical computer.

The equation (8), which describes the work of an ideal quantum computer, allows us to estimate its computational resources. In particular, from the principle of superposition, which describes the state of the system of qubits, it follows that for quantum computation, multiple 2^n parallelism is realized, since when a state of only one qubit changes, all 2^n projections of a vector are rearranged. Therefore, a relatively small number n of qubits forms an exponentially large 2^n information resource (for comparison, note that the classical register of n bits can only be in one of the 2^n states!).

Since the amplitudes of probabilities in the equation (5) are complex quantities, the quantum amplitudes interference is observed in quantum computations, which, in turn, is used in quantum computing. In particular, quantum algorithms are constructed so that the results of the interference increase the desired result [1].

Significant advantages in quantum computations are obtained by using the entangled quantum states [6]. It is this phenomenon, the nature of which is not completely understandable, which allows to obtain nontrivial results (dense coding, quantum teleportation, etc.)[1,3,5].

.

Referenses

[1] M.A. Nielsen, S.L. Chuang “Quantum Computation and Quantum Information.” Cambridge: Cambridge Univ. Press, 2000.

[2] I.O. Vakarchuk “Quantum Mechanics” 4rd ed, Lviv: Ivan Franko National university of Lviv Press, 2012.

[3] V.M. Tkachuk “The Fundamental Problems of Quantum Mechanics”, Lviv: Ivan Franko National university of Lviv Press, 2011.

[4] A. Barenco, C.H. Bennet, R. Cleve, D.P. DiVincenzo, N, Margolus, P. Shor “Elementary gates for quantum computation,” Phys. Rev. A, 1995, vol. 52, pp. 3457-3467

[5] D. Bouwmeester A.K. Ekert, A. Zeilinger “The Physics of Quantum Information.” Berlin: Springer, 2000.

[6] A. Einstein, B. Podolsky, N. Rosen “Can quantum-mechanical description of physical reality be considered complete?” Phys. Rev., 1935, vol. 49, 195-200.