

CONFERENCES AND SYMPOSIA PACS number: 01.10.Tt

Scientific session of the Division of General Physics and Astronomy of the Russian Academy of Sciences (27 January 1999)

A scientific session of the Division of General Physics and Astronomy of the Russian Academy of Sciences (RAS) was held on 27 January 1999 at the P L Kapitza Institute for Physical Problems, RAS.

Two papers were presented at this session:

(1) **Valiev K A** (Institute of Physics and Technology, RAS, Moscow) "Quantum computers: can they be made 'large'?";

(2) **Molotkov S N** (P N Lebedev Physics Institute, RAS, Moscow) "Quantum cryptography".

An abridge version of the first paper is given below.

PACS number: 03.67.Lx

Quantum computers: can they be made 'large'?

K A Valiev

The idea of the quantum computer goes back to Feynman's work in 1982 – 1986 [1 – 3] when, concerned with using the computer to simulate the evolution of a quantum system, he found this 'incompatible' in the sense that classical machines have insufficient memory and speed for solving quantum problems. For example, a system of n two-state quantum particles (of spin 1/2) offers 2^n basis states, implying that for the system to be described 2^n state amplitudes should be specified and stored in the computer. It was this negative result which led R Feynman to conjecture that probably the 'quantum computer' will have suitable properties for quantum problems to be dealt with [1 – 3].

'Classical' computers are built up of transistor circuits having their input and output voltages related in a nonlinear fashion. These are, in fact, bistable elements: for example, for a low input voltage (logical '0') the output voltage is high (logical '1'), and vice versa.

In the quantum world, one can associate with such a bistable transistor circuit a two-level quantum particle if one assigns to the state E_0, $|\Psi_0\rangle$ the value of logical '0'$\equiv|0\rangle$ and to the state $|\Psi_1\rangle$, $E_1 > E_0$, the value of logical '1'$\equiv|1\rangle$. To the transitions '0' $\rightarrow$ '1' in such a bistable transistor circuit there will correspond level-to-level transitions, i.e. $|0\rangle \leftrightarrow |1\rangle \equiv E_0 \leftrightarrow E_1$. However, compared with its classical counterpart, the quantum bistable element (which came to be known as the qubit) possesses a new property, namely that of the superposition of states, meaning that it may be in any state $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where α, β are complex numbers, and $|\alpha|^2 + |\beta|^2 = 1$. The states of a quantum system of n two-level particles are generally superpositions of the form $|\Psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i|\Psi_i\rangle$ of 2^n basis states $|\Psi_i\rangle = |i_1 i_2 \ldots i_n\rangle$, $i_k = 0, 1$. Essentially, it is the quantum principle of superposition which imparts to the quantum computer its fundamentally new 'abilities'.

It has been proved that it takes only two elements (gates) to build a quantum computer, a one-qubit element $Q(\theta, \varphi)$ and a two-qubit element 'controlled NOT' (CNOT). The 2×2 matrix of the $Q(\theta, \varphi)$ element is of the form

$$Q(\theta, \varphi) = \begin{pmatrix} \cos\dfrac{\theta}{2} & -\mathrm{i}\exp(-\mathrm{i}\varphi)\sin\dfrac{\theta}{2} \\ -\mathrm{i}\exp(\mathrm{i}\varphi)\sin\dfrac{\theta}{2} & \cos\dfrac{\theta}{2} \end{pmatrix}. \quad (1)$$

The $Q(\theta, \varphi)$ gate describes a rotation of the qubit state vector from the axis z to the polar axis specified by angles θ, φ. If the numbers θ, φ are irrational, then by repeatedly applying $Q(\theta, \varphi)$ the state vector may be given any preassigned orientation — a feature which makes the one-qubit gate (1) 'universal'. In the special case $\theta = \pi/2$, $\varphi = 0$ we have a one-qubit logical element NOT: $\mathrm{NOT}|0\rangle = |1\rangle$, $\mathrm{NOT}|1\rangle = |0\rangle$. To realize NOT physically requires a quantum particle (qubit) to be subjected to an external pulse whose role is to transfer the qubit from one state to another. A controlled NOT gate is established by acting on two qubits with a coupling between them, the coupling allowing one qubit to control the evolution of the other. Transitions caused by external pulses are well known in pulsed magnetoresonance spectroscopy. The NOT gate corresponds to the spin flip $I_z \leftrightarrow -I_z$ due to pulse $Y(\pi)$ (the magnetization vector rotates about the axis Y through an angle π). A CNOT gate is set up by two 1/2 spins with the Hamiltonian $H = \omega_i I_{zi} + A_{ij} I_{zi} I_{zj} + H'_{\mathrm{imp}}(t)$ (spin I_j controlling I_i) and proceeds in three stages: a pulse $Y_i(\pi/2)$, free precession for a time $\tau = \pi/A_{ij}$, and finally a pulse $X_i(\pi/2)$. If $I_{zj} = 1/2$ (the controlling qubit in the state $|0\rangle$), the above influences cause the controlled qubit to perform the transitions $I_{zi} \rightarrow I_{xi} \rightarrow I_{yi} \rightarrow I_{zi}$ (or $-I_{zi} \rightarrow -I_{xi} \rightarrow -I_{yi} \rightarrow -I_{zi}$). If, on the other hand, $I_{zj} = -1/2$ (the controlling qubit in the state $|1\rangle$), the evolution of the controlled qubit has a different result: $I_{zi} \rightarrow I_{xi} \rightarrow -I_{yi} \rightarrow -I_{zi}$ $(-I_{zi} \rightarrow -I_{xi} \rightarrow I_{yi} \rightarrow I_{zi})$. Thus, the spin I_i evolves differently for $I_{zj} = 1/2$ and $I_{zj} = -1/2$: $|00\rangle \rightarrow |00\rangle$, $|01\rangle \rightarrow |01\rangle$, $|10\rangle \rightarrow |11\rangle$, $|11\rangle \rightarrow |10\rangle$; here i_1 in $|i_1 i_2\rangle$ is the state of the controlling qubit.

In discussing various quantum systems as candidates for a quantum computer, it is the realizability and properties of the elementary gates NOT and CNOT which should be considered first.

For later use, it is convenient to introduce the Hadamard one-qubit transformation

$$\mathrm{H}|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right), \quad \mathrm{H}|1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right).$$

Uspekhi Fizicheskikh Nauk **169** (6) 691 – 694 (1999)
Translated by E G Strel'chenko; edited by A Radzig

In the magnetic resonance technique, these gates are realized by the pulses $\pi/2$:

$$Y\left(\frac{\pi}{2}\right)I_z \to I_x\,, \quad Y\left(\frac{\pi}{2}\right)(-I_z) \to -I_x\,.$$

A flow chart of a quantum computer is shown in Fig. 1. Before starting the computer, all the qubits (quantum particles) must be brought to the state $|0\rangle$, i.e. to their ground state. This is not a trivial condition in itself because to fulfil it, either deep cooling (to millikelvin temperatures) or polarization techniques are needed. A system of n qubits in the state $|00\ldots0\rangle$ can be regarded as a memory register prepared for recording input data and performing computations. Apart from this register, additional (auxiliary) registers for recording intermediate computation results are generally assumed to exist. To record data, some kind of influence is exerted on each computer qubit. Suppose, for example, that each register qubit is subject to the Hadamard transformation

$$\begin{aligned}&\mathrm{H}_n\otimes\mathrm{H}_{n-1}\otimes\ldots\otimes\mathrm{H}_1|0_1 0_2\ldots 0_n\rangle\\ &\quad= 2^{-n/2}\prod\left(|0\rangle_1+|1\rangle_1\right)\ldots\left(|0\rangle_n+|1\rangle_n\right)\\ &\quad= 2^{-n/2}\sum_{x=0}^{2^n-1}|x\rangle = |\Psi_1\rangle\,.\end{aligned} \tag{2}$$

As a result, the system goes over to a state superposed of 2^n basis states with an amplitude of $2^{-n/2}$. Each basis state comprises a binary number x, from $x=0(|00\ldots0\rangle)$ to $x=2^n-1(|11\ldots1\rangle)$. Notice that the horizontal lines in the figure represent time axes.

The algorithm $f(x)$ proceeds by subjecting the superposition $|\Psi_1\rangle$ to the unitary transformation U_f represented by a unitary $2^n\times 2^n$ matrix. In the external pulse scheme, the matrix $U_f(2^n)$ must be represented as a vector product of the matrices of size 2 $(U(2))$ and 2^2 $(U(2^2))$. These latter can be performed by successively acting on single qubits $(U(2))$ or qubit pairs $(U(2^2))$:

$$U_f = U_k\otimes U_{k-1}\otimes\ldots\otimes U_0\,, \tag{3}$$

the number of cofactors in the expansion determining the time required for and the complexity involved in calculating $f(x)$. All the U_l in Eqn (3) are performed by applying the operations NOT, CNOT, H or varieties of them.

Remarkably, the linear unitary operator U_f simultaneously acts on all the terms $|x\rangle$ in the superposition $|\Psi_1\rangle = 2^{-n/2}\sum_{x=0}^{2^n-1}|x\rangle$:

$$U_f|\Psi_1\rangle|0\rangle = 2^{-n/2}\sum_{x=0}^{2^n-1}U_f|x\rangle|0\rangle = 2^{-n/2}\sum_{x=0}^{2^n-1}|x\rangle|f(x)\rangle\,. \tag{4}$$

The calculated $|f(x)\rangle$ is stored in a stand-by register, which had been in the state $|0\rangle$ before U_f was applied. One run of the computational process gives us the necessary magnitudes of the desired function f for all values of the argument $x=0,\ldots,2^n-1$. This phenomenon has come to be known as quantum parallelism.

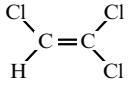
To measure the result of the calculations simply requires that the superposition vector in Eqn (4) be projected onto the vector of one of the basis states $|x\rangle$:

$$\mathrm{R}2^{-n/2}\sum_{x=0}^{2^n-1}|x\rangle|f(x)\rangle = 2^{-n/2}|x\rangle|f(x)\rangle\,. \tag{5}$$

We see here one of the weaknesses of the quantum computer: the number $|x\rangle$ 'appears' at random in the process of measurement. In order to find $f(x^*)$ for a given x^*, computations and measurements must be performed many times until $|x^*\rangle|f(x^*)\rangle$ appears in this random way. If input data are structured such that the amplitude c_{x^*} of the vector $|x^*\rangle$ in $|\Psi_1\rangle=\sum_{x=0}^{2^n-1}c_x|x\rangle$ may be close to 1, then the measurement will at once yield the state $|x^*\rangle|f(x^*)\rangle$ with probability $|c_{x^*}|^2\sim 1$. If x^* is not known in advance and the input data cannot be structured, special operations can be introduced into the algorithm, which will determine the required superposition term and, via the iteration process, will increase its amplitude to ~ 1. An example is Grover's algorithm to search for a certain object in an unstructured database [4].

The analysis of the unitary evolution of a computing quantum system highlights the importance of the interference type physical processes: unitary transformations are performed in the space of complex numbers whose phases produce an interference effect when added. It turns out that the Fourier transform, known to be so fruitful in interference phenomena and spectroscopy, is also ever-present in quantum algorithms. The Hadamard transform is in fact the simplest possible discrete Fourier transform. The NOT and CNOT gates may be established directly with the Mach–Sehnder interferometer by using the photon interference effect and rotations of the photon polarization vector [5].

Various approaches to the realization of quantum computers are currently being studied. In particular, quantum computing models using a pulsed NMR spectrometer have been tested [6–10], in which two or three spins (qubits), for example, two spins of ^{13}C nuclei and one proton spin in the trichlorethylene molecule [10]



were employed. However, the quantum computer involved in these experiments was of the 'ensemble' type in that its output signal was in fact a sum of signals from a large number ($\sim 10^{20}$) of liquid solution molecules.

By now, a number of systems have been suggested as quantum computer candidates, including trapped ions and molecules in vacuum [11]; nuclear spins in liquids (see above); nuclear spins of ^{31}P atoms in crystalline silicon [12]; electron spins in quantum dots produced in the 2D electron gas of the

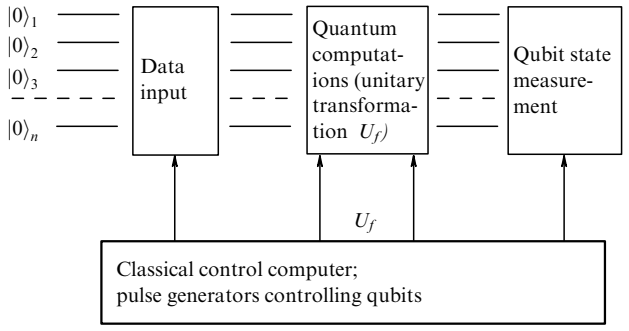


Figure 1. Flow chart of a quantum computer.

GaAs heterostructure [13], and the Josephson junctions [14]. We see that, in principle, atomic particles in vacuum and liquids as well as in crystals are suitable for building up a quantum computer. Although in each particular case certain obstacles are to be overcome, some of these are common due to the common principles of operation of qubits in a quantum computer. Suppose we set ourselves the task of constructing a full-scale, say, 10^3 qubits, quantum computer (even though an $n = 100$ quantum computer may be useful enough). This implies the following.

(1) Techniques are to be found with which to put computer qubits in the initial state $|0 \dots 0\rangle$. For a spin system in a crystal this clearly requires ultralow temperatures and superstrong magnetic fields. For cooling and high fields combined, spin polarization by pumping may prove useful.

For vacuum trap ions, laser methods are used to achieve superlow cooling of ions (atoms) and of course a cold and ultrahigh vacuum is also necessary.

(2) Technology is needed to apply pulses selectively to any chosen qubit. For the radio-frequency range and spin resonances, this implies that (in spectroscopic resolution terms) each spin should have its own resonance frequency. Resonance frequency differences between spins in molecules are due to chemical shifts for spins of one isotope and one element; the required frequency differences exist for nuclear spins of dissimilar elements. Common sense suggests, however, that these nature-provided frequency differences are hardly sufficient to work with 10^3 spins.

More promising approaches are those allowing the resonance frequency of each individual qubit to be externally controlled. In the silicon quantum computer concept, the nuclear spin of an impurity atom ^{31}P acts as a qubit, the resonance frequency being determined by the constant A of the hyperfine nuclear-electron spin interaction $H_{IS} = A\mathbf{I} \times \mathbf{S}$ in the ^{31}P atom. The electric field at the nanoelectrode above the ^{31}P atom polarizes this latter and changes the constant A (and hence the resonance frequency of the nuclear spin). Thus, the presence of the electrode makes the qubit a part of the electronic circuit and tunes its resonance frequency.

(3) To perform a CNOT_{ij} (controlled NOT) operation requires that there be a coupling of the form $A_{ij}I_{zi}I_{zj}$ between qubits i and j. Such a coupling occurs between nuclear spins in a molecule if nuclei i and j are separated through a single chemical bond between them. In principle, it is necessary to be able to perform the CNOT_{ij} operation for any pair of qubits with $i \neq j$. In a natural environment, since the qubit-qubit coupling is hardly expected to be of the all-with-all type and of the same order of magnitude for each qubit pair, it is clearly necessary that the medium in-between the qubits be tuned from outside by means of controlled-potential electrodes introduced for the purpose. In this way, for example, an overlap of electron wave functions between neighboring quantum dots and a coupling of the form $J(V)S_i \times S_j$ between the electron spins [13] can be achieved. The overlap between the electron wave functions of the neighboring ^{31}P atoms gives rise to the coupling $A_{ij}\mathbf{I}_i \times \mathbf{I}_j$ between nuclear spins [12].

In order to perform the operation CNOT_{ij}, where i and j are far-apart qubits with no $A_{ij}\mathbf{I}_i \times \mathbf{I}_j$ coupling between them, it is necessary that the computer performs the state exchange operation along the chain $j \to l \to k \to \dots \to p$, in which case $A_{ip}I_iI_p$ secures CNOT_{ij} because the state I_p is the same as I_j.

(4) Since computer qubits are affected by the environment in the course of performing a unitary transformation corresponding to the selected algorithm, the amplitudes and phases of the qubit state vector undergo random changes, i.e. decoherence. In fact, decoherence is the relaxation of those degrees of freedom of the particle, which are employed in the qubit, and the time of decoherence τ_d is equal to the relaxation time. For a nuclear magnetic resonance in liquids, the relaxation times T_1 and T_2 range between 1 and 10 s. For ions in traps with optical transitions between the levels E_0 and E_1, the decoherence times are the time of spontaneous emission and the collision time for residual atoms. Clearly, decoherence is a serious obstacle to quantum computing in that the computation process acquires some elements of randomness when a period of time equal to the decoherence time passes after its start.

However, the stability of the quantum computation process can be maintained for an arbitrarily long tome $\tau \gg \tau_d$ by systematically applying the methods of quantum encoding and (phase and amplitude) error correction [15]. It has been proved that, for relatively mild requirements on the failure rate of elementary operations NOT and CNOT (error probability within 10^{-5}), quantum error correction (QEC) methods secure a stable operation of a quantum computer.

Alternatively, the decoherence process can be suppressed by periodically performing measurements on the system of qubits. With a large probability, a measurement will find the particle to be in a 'regular' state, whereas small random changes of the state vector will collapse during the measurement (Zenon quantum effect [16, 17]). As yet, however, the utility of this approach is difficult to assess because measurements like this may themselves affect — and destroy — the computing process.

(5) To see the result of the computation, the states of the qubits must be measured after the computing process is over. Although today no technology is up to the job, the obvious way it should be sought is by using amplification methods when performing the quantum measurement. For example, the state of the nuclear spin I is transferred to the electron spin S, this latter determines the orbital wave function, and the knowledge of this function may in turn be used to perform a charge transfer (ionization); using classical electrometrical methods [12, 13], the presence or absence of a single electron charge may be detected. In measurements like this, force-microscopy probe techniques are likely to be employed.

Quantum algorithms that speed up computations exponentially relative to classical computers have been discovered. One example is Shor's algorithm for factoring large (multidigit) numbers [18]. This purely mathematical problem has serious implications for human society because the 'non-computability' of such factors is currently at the heart of many cryptographic systems — hence the sensation caused by Shor's discovery. For physicists, it is important that quantum problems (in particular, the Schrödinger equation for many-particle systems) may be solved exponentially faster with a quantum computer [19].

Finally, it is important that in the course of quantum computing studies, the basic problems of quantum physics — in particular, locality, reality, complementarity, hidden parameters, and wave function collapse — come again under the scrutiny of both theoreticians and experimentalists.

The concepts of quantum computing and quantum communications came to the fore a hundred years after the advent of quantum mechanics. Both theoretical and experimental studies have demonstrated the viability of the quantum computer idea. Quantum physics is 'sufficient' as a

tool for designing quantum computers on various 'elemental bases.' If blessed with success, quantum computers will be a XXI century technique. For their fabrication, technology issues at nanometer and atomic size levels will have to be resolved — a task for decades of work, perhaps. Another illustration of the principle of the inexhaustibility of nature, quantum computers would show that Mother Nature has enough means to solve whatever problem a human may correctly formulate. In conclusion, these reviews on quantum computing [20 – 22] are recommended for further reading.

References

1. Feynman R P *Int. J. Theor. Phys.* **21** 467 (1982)
2. Feynman R P *Opt. News* (Feb.) 11 (1985)
3. Feynman R P *Found. Phys.* **16** (6) 507 (1986)
4. Grover L K *Phys. Rev. Lett.* **79** 325 (1997)
5. Adami C, Cerf N J, quant-ph/9806048 (14 June 1998)
6. Chuang I L et al. *Nature* (London) **393** 143 (1998)
7. Chuang I L et al. *Proc. R. Soc. London Ser. A* **454** 447 (1998)
8. Cory D G et al. *Proc. Natl. Acad. Sci. USA* **94** 1634 (1997)
9. Jones J A et al. *Nature* (London) **393** 344 (1998)
10. Cory D G et al., quant-ph/9802018 (6 February 1998); *Phys. Rev. Lett.* **81** 2152 (1998)
11. Cirac J I, Zoller P *Phys. Rev. Lett.* **74** 4091 (1995)
12. Kane B E *Nature* (London) **393** 133 (1998)
13. Loss D, Di Vincenzo D P *Phys. Rev. A* **57** 120 (1998)
14. Shnirman A et al. *Phys. Rev. Lett.* **79** 2371 (1997); Schön G, Shnirman A, Makhlin Yu, cond-mat/9811029 (3 November 1998)
15. Preskill J, quant-ph/9705031, v3 (26 August 1997)
16. Khalfin L A *Usp. Fiz. Nauk* **160** 185 (1990) [*Sov. Phys. Usp.* **36** 868 (1990)]
17. Braunstein S L, Smolin J A, quant-ph/9604036, v2 (22 October 1996)
18. Shor P, in *Proc. 35th Annual Symposium on Foundations of Computer Science* (Los Alamitos, Calif.: IEEE Computer Soc. Press, 1994) p. 124
19. Zalka C *Proc. R. Soc. London Ser. A* **454** 313 (1998)
20. Steane A, quant-ph/9708022, v2 (24 September 1997); *Rep. Prog. Phys.* **61** 117 (1998)
21. Rieffel E G, Polak W, quant-ph/9809016 (8 September 1998)
22. Aharonov D, quant-ph/9812037 (15 December 1998); in *Annual Reviews of Computational Physics* (Ed. D Stauffer) Vol. 6 (Singapore: World Scientific, 1998)