# PHYSICS OF QUANTUM COMPUTATION

*V. V. Belokurov, O. A. Khrustalev, V. A. Sadovnichy, O. D. Timofeevskaya*

Lomonosov Moscow State University, Moscow

## INTRODUCTION

As many other significant discoveries in physics, the invention of quantum computer was a result of the battle against thermodynamic laws. It was the middle of the 19th century when Maxwell proposed his demon — a creature with unique perceptivity able to detect every molecule and control its motion. Separating fast and slow molecules of a gas in different parts of a box, Maxwell's demon could have changed the temperature in these parts without producing any work. Thus, the intelligent machine could prevent thermal death.

Later Smoluchowski proved that measuring molecular velocities and storing the information demon would increase entropy. Therefore, the perpetuum mobile of the second type could not be created. It became a common opinion that any physical measurement was irreversible. In the 1950s von Neumann applied these arguments to his computer science. He supposed that the penalty for computer operation was energy scattering with the rate of energy loss $kT \ln 2$ per one step of computation. This estimation was considered as convincing. However at the beginning of the 1960s Landauer proved that energy dissipation in computers was closely related to logical irreversibility of computation. There were no rigorous arguments for correctness of von Neumann's conclusion in the case of reversible computation. A hope appeared that if Maxwell's demon learned to perform reversible computations, the construction of reversible computers would become real. To formulate the latter thesis more precisely, let us recall some definitions.

A function $\mathcal{F}$ is $\mathcal{M}$-computable if a computing machine $\mathcal{M}$ can compute the function $\mathcal{F}$ according to some program.

For each computing machine $\mathcal{M}$ there is a set $\mathcal{C}(\mathcal{M})$ of $\mathcal{M}$-computable functions. Among a great number of machines one can ever imagine there exists the *universal Turing machine* ($\mathcal{T}$) which is able to replace any computer. It follows from the statement (Turing, 1936) that any $\mathcal{M}$-computable function that maps the set of integers $\mathbf{Z}$ to itself belongs to the set $\mathcal{C}(\mathcal{T})$.

It is well known that $\mathcal{C}(\mathcal{T})$ is a numerable set of all recursive functions and it is essentially smaller than the set of all functions that map $\mathbf{Z}$ to $\mathbf{Z}$.

In 1936, Church and Turing independently formulated a hypothesis, the so-called **Church–Turing principle:** *Every function that is considered computable can be computed by the universal Turing machine.*

In 1985, Deutsch [1] proposed a physical version of Church–Turing principle: *«Every finitely realizable physical system can be perfectly simulated by a universal model computing machine operating by finite means.»*

Here, the term «finitely realizable physical system» means any physical object upon which experiment is possible. The «universal computing machine» is an idealized (but theoretically realizable) model. «Finite means» can be defined axiomatically, without restrictive assumptions about the form of physical laws. If we think of a computing machine as proceeding in a sequence of steps whose duration has a nonzero lower bound, then it operates «by finite means» if

(1) only a finite subsystem (though not always the same one) is changed during any step,

(2) a change of a subsystem at any step depends only on a state of a finite number of subsystems, and

(3) a rule of a change of a subsystem is finite in mathematical sense.

The new version of Church–Turing principle is stronger than the original one. Indeed, the demands are so strong that they cannot be satisfied by Turing machine acting according to the laws of classical physics. Owing to continuity of spectra of variables in classical physics, possible states of a classical system form a continuum. But only a numerable set of states can be taken at the input of Turing machine. Consequently, Turing machine cannot perfectly simulate any classical dynamic system. Contrarily to classical systems, quantum systems are compatible with the new version of Church–Turing principle.

Quantum Turing machines are so attractive because their action is controlled by unitary reversible transformations of quantum mechanics. A possible irrevesibility could be introduced only by an input data or by an inappropriate choice of a material of the machine's construction. Configurations of spins seem to be a particularly suitable construction material because these machines would not depend on wave packet spreading. Among the most important early works on the subject, the papers of Benioff [2], Bennett [3] and especially famous Feynman's articles [4] should be mentioned.

However, contemporary science on quantum computation began in 1985 after Deutsch's paper [1].

## 1. QUANTUM TURING MACHINE

Deutch's quantum computer as well as Turing machine consists of two components — a finite *processor* and an infinite *memory*. During calculations always only a finite part is used.

*The processor* is a system, all states of which are eigenstates of a set of observables

$$\hat{P} = \{\hat{n}_i,\ i = 0, 1, \ldots, N-1\},$$

acting in two-dimensional Hilbert spaces.

*The memory* consists of an infinite sequence of observables of the same kind:

$$\hat{M} = \{\hat{m}_i,\ i = 0, 1, \ldots\}.$$

This system corresponds to the infinite memory's tape of Turing machine. The observable $\hat{x}$ corresponds to the head's (cursor's) position at the tape of Turing machine. Its spectrum is a set of integer numbers.

One of the bases in the space of computer's states is a set of eigenvectors of these operators:

$$|x;\ n;\ m\rangle = |x;\ n_0, \ldots, n_{N-1};\ \ldots m_{-1}, m_0, m_1, \ldots\rangle.$$

They are called «computational basis states». The variables $\hat{n}, \hat{m}$ are chosen in such a way that all of them have spectrum $\{0, 1\}$.

The evolution operator $\hat{U}$ for Deutsch computer is defined by its matrix elements

$$\langle x'; n'; m'|\hat{U}|x; n; m\rangle =$$
$$= \{\delta_{x'x+1} U_+(n', m'_x|n, m_x) + \delta_{x'x-1} U_-(n', m'_x|n, m_x)\} \Pi_{y \neq x} \delta_{m_y m_y}.$$

Quantum computer is equivalent to Turing machine if

$$U_\pm(n', m'|n, m) = \frac{1}{2} \delta_{A(n,m),n'} \delta_{B(n,m),m} \{1 \pm C(n, m)\},$$

where $A, B, C$ are some functions with ranges of values $(Z_2)^N$, $Z_2$ and $\{-1, 1\}$, correspondingly.

For operator $\hat{U}$ to be unitary, it is necessary and sufficient to have a bijective mapping:

$$\{n, m\} \Leftrightarrow \{A(n, m), B(n, m), C(n, m)\}.$$

In the rest the functions, $A, B, C$ are arbitrary. They can be chosen such that the constructed computer represents the universal quantum Turing machine $\mathcal{T}$.

## 2. EVALUATION OF FUNCTIONS BY QUANTUM COMPUTER

Suppose the function $f(i) = j$ transforms the set

$$Z_m = \{i = 0, 1, \ldots, m - 1\}$$

into the set

$$Z_n = \{j = 0, 1, \ldots, n - 1\}.$$

Is it possible to associate with it a unitary transformation in some Hilbert space? The answer is positive and the constructions of the space and the transformation are rather transparent.

Let $\mathcal{H}_{mn}$ be a Hilbert space with the dimension $mn$ and

$$e_s \equiv |i, j\rangle, \quad i \in Z_m, \quad j \in Z_n, \quad \langle i, j|i', j'\rangle = \delta_{ii'} \delta_{jj'}$$

be a basis in this space. The transformation

$$U_f|i, j\rangle = |i, j \oplus f(i)\rangle$$

is a unitary one. Symbol $\oplus$ means addition modulo $n$.

A remarkable property of quantum computation is a possibility to define states in which all the values of the function $f$ are considered simultaneously. If

$$\phi = \sum_{i=0}^{m-1} |i, 0\rangle \frac{1}{\sqrt{m}},$$

then

$$\psi = U_f\phi = \sum_{i=0}^{m-1} |i, f(i)\rangle \frac{1}{\sqrt{m}}.$$

In some cases the unitary operator $\hat{S}$ defined by the equation

$$\hat{S}|i,j\rangle = |i,j\rangle(-1)^j$$

appears to be useful. It converts the vector $\psi$ into the vector

$$\theta = \hat{S}\psi = \sum_{i=0}^{m-1} |i, f(i)\rangle \frac{(-1)^{f(i)}}{\sqrt{m}}.$$

In its turn, operator $\hat{U}_f$ transforms the vector $\theta$ into the vector

$$\xi = \hat{U}_f\theta = \sum_{i=0}^{m-1} |i, f(i) \oplus f(i)\rangle \frac{(-1)^{f(i)}}{\sqrt{m}}.$$

If $n = 2$, i.e., the function $f$ has only two values 0 and 1, then $f(i) \oplus f(i) = 0$ and

$$\xi = \sum_{i=0}^{m-1} |i, 0\rangle \frac{(-1)^{f(i)}}{\sqrt{m}}.$$

The scalar product of the initial and the final vectors in this chain is

$$\langle\phi|\xi\rangle = \frac{1}{2m} \sum_{i=0}^{2m-1} (-1)^{f(i)}.$$

An operation of a quantum computer is described by a $d$-dimensional unitary matrix $\hat{T}$ that realizes the evolution operator in a computational basis. It is very essential that the matrix $\hat{T}$ can be represented as a product of $d(2d-1)$ unitary matrices. Each of them corresponds to an operator that acts in a two-dimensional space formed by a pair of vectors of the mentioned basis. Any vector $V$ with the components $(v_1, v_2, \ldots, v_d)$ in the computational basis can be transformed by $d-1$ transformations of indicated form to the vector $W$ that has the components $(1, 0, \ldots, 0)$ in the computational basis:

$$W = \hat{S}_d \cdots \hat{S}_3\hat{S}_2 V.$$

The reverse transformation looks like

$$V = \hat{S}_2^{+} \cdots \hat{S}_{d-1}^{+}\hat{S}_d^{+} W.$$

## 3. QUANTUM FOURIER TRANSFORM

Consider functions defined in $Z_N$. Suppose

$$\omega = \frac{1}{\sqrt{N}} e^{2\pi i/N}.$$

If numbers $a$, $b \in Z_N$, then the numbers $\omega^{ab}$ form a unitary matrix $\hat{F}$:

$$\hat{F}_{ab} = \omega^{ab} = \frac{1}{\sqrt{N}} \exp\left(2\pi i \frac{ab}{N}\right),$$

$$(\hat{F}\hat{F}^{+})_{ab} = \sum_c \omega^{ac}(\omega^*)^{cb} = \frac{1}{N}\sum_c \exp\left(2\pi i \frac{(a-b)c}{N}\right) = \delta_{ab}.$$

The Fourier transform of a function $f(a)$ is given by the equation

$$(\hat{F}f)(a) \equiv \tilde{f}(a) = \sum_c \omega^{ac} f(c).$$

We can define the Fourier operator in the Hilbert space $\mathcal{H}_N$. If a vector $\Psi \in \mathcal{H}_N$ equals

$$\Psi = \sum_{a=0}^{N-1} |a\rangle f(a),$$

then we say that Fourier transform of the vector $\Psi$ is

$$\hat{F}\Psi = \sum_a |a\rangle (\hat{F}f)(a).$$

It is clear that Fourier transform of a basis vector $|a\rangle$ is

$$\hat{F}|a\rangle = \sum_c |c\rangle \omega^{ca}.$$

Further, we suppose that $N = 2^l$. Let $a$ be represented in binary as $a_1 \cdots a_l \in \{0,1\}^l$

$$a = \sum_{i=1}^{l} 2^{l-i} a_i$$

(and similarly $c$). It is possible to represent the computational basis in the form of direct product of the bases in two-dimensional Hilbert spaces

$$|i_1, i_2, \ldots, i_l\rangle = |i_1\rangle \otimes |i_2\rangle \otimes \cdots \otimes |i_l\rangle.$$

The product of the numbers $a$ and $c$ can be written in the form

$$ac = a_l c_l + 2(a_{l-1}c_l + a_l c_{l-1}) + \ldots 2^{l-1}(a_l c_1 + \ldots + a_1 c_l) + O(2^l).$$

Since

$$\frac{ac}{2^l} = \frac{a_l}{2}c_1 + \left(\frac{a_{l-1}}{2} + \frac{a_l}{2^2}\right)c_2 + \ldots + \left(\frac{a_1}{2} + \frac{a_2}{2^2} + \ldots + \frac{a_l}{2^l}\right)c_l + O(2^0),$$

we obtain

$$\exp\left(2\pi i\frac{ac}{2^l}\right) = \mathrm{e}^{2\pi i(0.a_l)c_1}\mathrm{e}^{2\pi i(0.a_{l-1}a_l)c_2}\ldots\mathrm{e}^{2\pi i(0.a_1a_2\cdots a_l)c_l};$$

here,

$$0.a_l = \frac{a_l}{2},\ \cdots 0.a_1\cdots a_l = \frac{a_1}{2} + \frac{a_2}{2^2} + \ldots + \frac{a_l}{2^l}.$$

The Fourier transform of the vector $|a\rangle$ is

$$\hat{F}|a\rangle = \frac{1}{\sqrt{N}}\sum_{\{c\}}|c_1\rangle\,\mathrm{e}^{2\pi i(0.a_l)c_1}\otimes|c_2\rangle\,\mathrm{e}^{2\pi i(0.a_{l-1}a_l)c_2}\otimes\cdots\otimes|c_l\rangle\,\mathrm{e}^{2\pi i(0.a_1a_2\cdots a_l)c_l}.$$

It follows that

$$\hat{F}|a\rangle = \frac{1}{\sqrt{N}}(|0\rangle + |1\rangle\,\mathrm{e}^{2\pi i(0.a_l)})\otimes(|0\rangle + \\ + |1\rangle\,\mathrm{e}^{2\pi i(0.a_{l-1}a_l)})\otimes\cdots\otimes(|0\rangle + |1\rangle\,\mathrm{e}^{2\pi i(0.a_1a_2\cdots a_l)}).$$

The Walsh–Hadamard operator $\hat{R}_j$ acting in a subspace $\mathcal{H}_j$ is given by the formula

$$\hat{R}_j = \frac{1}{\sqrt{2}}(|0_j\rangle\langle 0_j| + |0_j\rangle\langle 1_j| + |1_j\rangle\langle 0_j| - |1_j\rangle\langle 1_j|).$$

The *controlled phase shift* operator $\hat{S}_{jk}$ acts in the join of subspaces $\mathcal{H}_j \cup \mathcal{H}_k$ as:

$$\hat{S}_{jk} = |0_j0_k\rangle\langle 0_k0_j| + |0_j1_k\rangle\langle 1_k0_j| + |1_j0_k\rangle\langle 0_k1_j| + |1_j1_k\rangle\,\mathrm{e}^{i\theta_{jk}}\langle 1_k1_j|.$$

The angle $\theta_{jk}$ is

$$\theta_{jk} = \frac{\pi}{2^{j-k}}.$$

It is easy to prove that the quantum Fourier transform [5] is realized by the following sequence of the operators. First, the operator $\hat{R}_1$ acts. Then the operators $\hat{S}_{2,1}, \hat{S}_{3,1}, \ldots, \hat{S}_{l,1}$ act. Then there is a turn for the operators $\hat{R}_2$, $\hat{S}_{3,2}$ and $\hat{S}_{4,2}$ and so on. In the interval between $\hat{R}_j$ and $\hat{R}_{j+1}$ all operators $\hat{S}_{k,j}$ $(k > j)$ act. The explicit formula is

$$\hat{R}_l\hat{S}_{l,l-1}\hat{R}_{l-1}\hat{S}_{l,l-2}\hat{S}_{l-1,l-2}\hat{R}_{l-2}\hat{S}_{l,l-3}\cdots\hat{S}_{3,2}\hat{R}_2\cdots\hat{S}_{3,1}\hat{S}_{2,1}\hat{R}_1|a_1,\ldots,a_l\rangle = \\ = (|0\rangle + |1\rangle\,\mathrm{e}^{2\pi i(0.a_1\cdots a_l)})(|0\rangle + |1\rangle\,\mathrm{e}^{2\pi i(0.a_2\cdots a_l)})\cdots(|0\rangle + |1\rangle\,\mathrm{e}^{2\pi i(0.a_l)}).$$

This vector differs from the Fourier transform of the vector $|a_1,\ldots,a_l\rangle$ in order of variables $a_i$ only. We use unitary operator $\hat{S}$ that converts basis $|a_1,\ldots,a_l\rangle$ into $|a_l,\ldots,a_1\rangle$. Thus, we get

$$\hat{S}\hat{R}_l\cdots\hat{R}_1 = \hat{F}.$$

In order to understand how important the factorization of the Fourier transform operator is, we recall some general concepts of quantum computation theory.

The minimal quantity of information in the classical theory, **a bit**, is a basic notion of the theory. In the theory of quantum computations the minimal quantity of information (a quantum bit, or **a qubit**) is given by a unit vector in a two-dimensional Hilbert space $\mathcal{H}_2$. In the classical theory a logic gate is a computing machine which has fixed numbers of input and output bits and can produce a fixed operation in a fixed period of time. **A quantum gate** is a device which performs a fixed unitary operation on the selected qubits in a fixed period of time. The quantum gate is an operator that transforms Hilbert space $\mathcal{H}_I$ into $\mathcal{H}_O$. The operators $\hat{R}$ and $\hat{S}_{ij}$, defined above, are gates. The swapping operation is the sequence of gates.

If one quantum gate is one step of computation, then Fourier transform in Hilbert space of $N = 2^l$ dimension requires about

$$N_{\text{qstep}} = O((\lg_2(N))^2)$$

steps. The best known classical algorithm for fast discrete Fourier transform is of size

$$N_{\text{cstep}} = O(N \lg_2(N) \lg_2(\lg_2(N))).$$

## 4. EXPERIMENTAL REALIZATION OF QUANTUM FOURIER TRANSFORMATION

In the paper [6] QFT in two-qubit system is realized by NMR methods. Two qubits were nuclears $A$ and $B$ with spin 1/2 in constant magnetic field. The Hamiltonian for this system can be approximated as

$$\hat{H} = \omega_a \hat{S}_{3a} + \omega_b \hat{S}_{3b} + 2\pi\omega_{ab}\hat{S}_{3a}\hat{S}_{3b} + \hat{H}_{\text{env}},$$

where $\hat{H}_{\text{env}}$ is interaction with environment. In the first approximation it can be ignored. The eigenstates of $\hat{H}$ are the eigenstates of operators $\hat{S}_{3a}$ and $\hat{S}_{3b}$.

In the experiment, they chose $H_2PO_3$ as a sample, labeled $^{31}$P as $A$-qubit and $^{1}$H as $B$-qubit. The observed $J$-coupling between $^{31}$P and $^{1}$H was 647.451 Hz.

First, they produced effective pure state $|00\rangle$ by using «temporal averaging» [7].

To perform QFT on the state $|01\rangle$, we should operate the pulse sequence $\left(\frac{\pi}{2}\right)^H_Y - \frac{1}{2}J - \left(\frac{\pi}{2}\right)^H_X$ on $^{1}$H to obtain the state $|01\rangle$.

Second, we perform Fourier transformation on $|01\rangle$. The list of pulses and spin–spin interaction are as follows:

$$(\pi)^P_X - \left(-\frac{\pi}{2}\right)^P_Y,$$

$$-\left(\frac{\pi}{2}\right)^P_Y \left(\frac{\pi}{2}\right)^H_Y - \left(\frac{\pi}{4}\right)^P_X \left(\frac{\pi}{4}\right)^H_X - \left(-\frac{\pi}{2}\right)^P_Y \left(-\frac{\pi}{2}\right)^H_X - \frac{1}{4J},$$

$$(\pi)^P_X - \left(-\frac{\pi}{2}\right)^H_X.$$

The first and the third lines in this formula are Walsh–Hadamard transformation and the second is phase-shift transformation. After these operations, the initial state $|01\rangle$ is transformed into the state

$$|01\rangle \Longrightarrow \frac{1}{2}(|00\rangle + i|01\rangle - |10\rangle - i|11\rangle) = \frac{1}{2}(|00\rangle + |01\rangle\, \mathrm{e}^{i\pi/2} + |10\rangle\, \mathrm{e}^{i\pi} + |11\rangle\, \mathrm{e}^{i3\pi/2}).$$

The third step is the reversion of qubits. It is well known that this operation is composed of three C-Not gates.

## 5. GEOMETRIC QUANTUM COMPUTATIONS

At present, the geometric quantum computation with NMR on the base of Berry phase [8] is considered as one of the most promising methods. This new approach to quantum gates may be important to the future, as it is naturally resilient to certain types of errors connected with interactions with environment.

If Hamiltonian varies adiabatically through a circuit $C$ in the space of parameters $\mathbf{R}(t)$, then the adiabatic evolution of the system is described by time-dependent Schrödinger equation. According to Berry, solutions have a form

$$\Psi(t) = |n(\mathbf{R}(t))\rangle \,\exp\left\{-\frac{i}{\hbar}\int_0^t dt_1 E_n \mathbf{R}(t_1)\right\} \mathrm{e}^{i\gamma_n(t)}|\mathbf{R}(t)\rangle;$$

here, $|\mathbf{R}(t)\rangle$ is eigenvector of Hamiltonian at the moment $t$ and $\gamma_n(t)$ is *geometric phase* which depends only on the path. For system of two spins 1/2 Berry's phase in the state $|\uparrow,\downarrow\rangle$ is

$$\gamma_{\uparrow,\downarrow} = \mp\pi(1-\cos\theta);$$

here $\theta$ is a solid angle that vector $\mathbf{R}(t)$ sweeps out in the space of parameters. Thus, we get the evolution of state's vector in time $\Psi = |\alpha\rangle\, \mathrm{e}^{i(\delta+\gamma)}$; $\delta$ is dynamical phase which depends on the Hamiltonian. It is well known in NMR that it is possible to eliminate the dynamic phase by the «phase refocusing» procedure. As a result of suitable circuit, the spin state vectors are changed. One gets

$$|\uparrow\rangle \Longrightarrow |\uparrow\rangle\, \mathrm{e}^{i(\delta_\uparrow-\gamma)} \Longrightarrow |\downarrow\rangle\, \mathrm{e}^{i(\delta_\uparrow-\gamma)} \Longrightarrow |\downarrow\rangle\, \mathrm{e}^{i(\delta_\uparrow+\delta_\downarrow-2\gamma)} \Longrightarrow |\uparrow\rangle\, \mathrm{e}^{i(\delta_\uparrow+\delta_\downarrow-2\gamma)},$$
$$|\downarrow\rangle \Longrightarrow |\downarrow\rangle\, \mathrm{e}^{i(\delta_\downarrow+\gamma)} \Longrightarrow |\uparrow\rangle\, \mathrm{e}^{i(\delta_\downarrow+\gamma)} \Longrightarrow |\uparrow\rangle\, \mathrm{e}^{i(\delta_\uparrow+\delta_\downarrow+2\gamma)} \Longrightarrow |\downarrow\rangle\, \mathrm{e}^{i(\delta_\uparrow+\delta_\downarrow+2\gamma)}.$$

The dynamic phases are eliminated and we are left with an exclusively geometric phase difference of $4\gamma = 4\pi\cos\theta$. The conditional Berry phase gates depend only on the geometry of the path. They are completely independent of how the motion is performed, as long as it is adiabatic. Hence, the kind of quantum computation with the help of Berry's phase may be called geometric quantum computation.

These techniques are readily implemented with current technology in quantum optics and have already been demonstrated by some of the authors using NMR [9].

## REFERENCES

1. *Deutsch D.* Quantum theory, the Church–Turing Principle and the Universal Quantum Computer // Proc. Royal. Soc. Lond. A. 1985. V. 400. P. 97–117.

2. *Benioff P.* Quantum Mechanical Hamiltonian Models of Turing Machines // J. Stat. Phys. 1982. V. 29. P. 515–545.

3. *Bennett C. H.* Thermodynamics of Computation // Intern. J. Theor. Phys. 1982. V. 21. P. 219–253.

4. *Feynman R.* Quantum Mechanical Computers // Ibid. Nos. 6/7.

5. *Shor P. W.* Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer // SIAM J. Comput. 1997. V. 26, No. 5. P. 1484–1509.

6. *Fu L. et al.* Experimental Realization of Discrete Fourier Transformation on NMR Quantum Computer. quant-ph/9905083. 1999.

7. *Knill A., Chuang E.* // Phys. Rev. A. 1998. V. 57. P. 3357.

8. *Berry M. V.* Quantum Phase Factor Accompanying Adiabatic Changes // Proc. Royal. Soc. Lond. A. 1984. V. 392. P. 45–57.

9. *Jones J. A., Hansen R. H., Mosca M.* // J. Magn. Reson. 1998. V. 135. P. 353.