

Foundations of quantum computing. Part II*

SŁAWOMIR BUGAJSKI, JERZY KLAMKA, STEFAN WĘGRZYN

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

Abstract: In the second part of the introduction to quantum computation we discuss three-qubit gates, quantum adders and the simplest version of the quantum teleportation protocol. We provide also a general description of the process of quantum computation and stress its specific features like quantum parallelism, and reversibility.

1. Introduction

This paper is a continuation of [7], where we have reviewed basic concepts of quantum mechanics necessary for the quantum model of computing, and described the simplest objects of quantum computer science: one- and two-qubit systems, quantum gates, simple quantum circuits. We will assume that the mentioned material is known to the reader, so we will not repeat definitions formulated there; the notation applied here will be consistent with that introduced in [7]. We will discuss some simple three-qubit quantum circuits, including quantum adders. Then we provide a brief description of the phenomenon called "quantum teleportation", and pass to a general discussion of n -qubit circuits. A general scheme of a quantum computation is presented, and some fundamental issues as "quantum parallelism", reversibility, *etc.* are considered.

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

2. Three-qubit systems

According to general rules of quantum mechanics, the quantum description of a three-qubit system $\mathbf{Q}_A + \mathbf{Q}_B + \mathbf{Q}_C$ has to be based on the three-fold tensor product $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$ (if they are not necessary, the subscripts A, B, C referring to particular qubits will be omitted). The canonical base of $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$ consists of all tensor products of vectors constituting canonical bases of the three two-dimensional spaces. Thus the eight vectors of the canonical base are:

$$|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle \quad (1)$$

where $|000\rangle$ denotes $|0\rangle \otimes |0\rangle \otimes |0\rangle$ etc.

2.1. Three-qubit gates

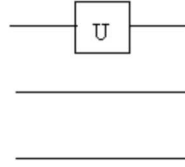
Quantum gates are elementary unitary transformations on the state spaces of one- and two- qubit systems. It is known, see for instance [2], [14], that an arbitrary (but non-trivial in a sense) two-qubit gate together with all one-qubit gates form a universal set: every unitary transformation on every number of qubits can be decomposed into a product of gates of this set. Thus, there is no essential reason to introduce special three-qubit gates, because they can be always implemented as a successive action of one- and two-qubit ones- three-qubit unitary transformations are realized by simple quantum circuits (for an example see Subsection 2.1.4 below). Nevertheless, some three-qubit transformations deserve a special name as well a special attention.

2.1.1. One- and two-qubit gates for three-qubit systems

Like the case of two-qubit systems (see [7], Sect. 3.12), one can extend one- and two-qubit gates to a three-qubit system by tensoring them with unit matrices. Consider, for instance, a one-qubit gate \widehat{U}_A acting on \mathbf{Q}_A . The gate $\widehat{U}_A \otimes \widehat{I}_{B,C}$ (the unit matrix $\widehat{I}_{B,C}$ on $\mathbb{C}_B^2 \otimes \mathbb{C}_C^2$ is simply $\widehat{I}_B \otimes \widehat{I}_C$) acts on any product state $|u\rangle_A \otimes |v\rangle_{B,C}$ as follows:

$$(\widehat{U}_A \otimes \widehat{I}_{B,C}) (|u\rangle_A \otimes |v\rangle_{B,C}) = \widehat{U}_A |u\rangle_A \otimes |v\rangle_{B,C} \quad (2)$$

Thus, $\widehat{U}_A \otimes \widehat{I}_{B,C}$ applied to $|u\rangle_A \otimes |v\rangle_{B,C}$ does not affect the state of the subsystem $\mathbf{Q}_B + \mathbf{Q}_C$, and acts like the gate \widehat{U}_A on the state of \mathbf{Q}_A . That property is the source of the popular (mis)interpretation of $\widehat{U}_A \otimes \widehat{I}_{B,C}$ as a "local" gate acting exclusively on \mathbf{Q}_A , or as a "three-qubit version" of the one-qubit gate \widehat{U}_A . That "local" interpretation is implicit in the rules of design of diagrams for quantum networks. The mentioned gate $\widehat{U}_A \otimes \widehat{I}_{B,C}$ is denoted like



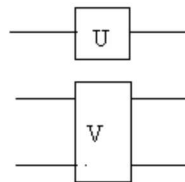
what suggest that the gate \widehat{U} acts on the first qubit without affecting the other two. The "local" interpretation taken literally appears misleading, because the action of $\widehat{U}_A \otimes \widehat{1}_{B,C}$ on entangled states is non-trivial: in spite of its alleged "local" character, the gate $\widehat{U}_A \otimes \widehat{1}_{B,C}$ acting on non-product states changes the reduced state of the subsystem $\mathbf{Q}_B + \mathbf{Q}_C$ as well.

2.1.2. Three-qubit product gates

Two gates, for instance $\widehat{1}_A \otimes \widehat{\square}_{B,C}$ and $\widehat{U}_A \otimes \widehat{1}_{B,C}$, can be applied one after another. It is easy to find (compare [7] 3.12.4) that

$$(\widehat{U}_A \otimes \widehat{1}_{B,C}) (\widehat{1}_A \otimes \widehat{\square}_{B,C}) = \widehat{U}_A \otimes \widehat{\square}_{B,C} \tag{3}$$

so the successive application of two "local" gates $\widehat{1}_A \otimes \widehat{\square}_{B,C}$ and $\widehat{U}_A \otimes \widehat{1}_{B,C}$ is equivalent to a three qubit gate $\widehat{U}_A \otimes \widehat{\square}_{B,C}$. It should be noticed again that the product gate $\widehat{U}_A \otimes \widehat{\square}_{B,C}$ acts in a "local" way on product states $|u\rangle_A \otimes |v\rangle_{B,C}$, but shows "non-local" effects in the case of non-product states of the three-qubitsystem $\mathbf{Q}_A + \mathbf{Q}_B + \mathbf{Q}_C$. The quantum-network diagram for $\widehat{U}_A \otimes \widehat{\square}_{B,C}$ suggests, however, the alleged "local" character of the product gate:



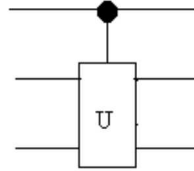
2.1.3. Controlled gates

Any one- or two-qubit gate can be also transformed into a three-qubit gate by considering the other qubit (qubits) as control ones. Thus, for instance, the two-qubit gate $\widehat{U}_{B,C}$ can act in the controlled way as the controlled gate $\widehat{U}_{C \square U}$ defined by

$$\widehat{U}_{C \square U} |0\rangle_A \otimes |u\rangle_{B,C} : = |0\rangle_A \otimes |u\rangle_{B,C} \tag{4}$$

$$\widehat{U}_{C \square U} |1\rangle_A \otimes |u\rangle_{B,C} : = |1\rangle_A \otimes \widehat{U}_{B,C} |u\rangle_{B,C} \tag{5}$$

The diagram for controlled-U gate is



If we take $\hat{U}_{B,C} = \hat{U}_{B,C,C}$, the rule for controlled-U gate leads to the controlled CNOT gate (C²NOT), called the *controlled NOT gate*.

2.1. Toffoli gate

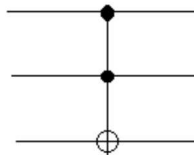
The Toffoli gate is represented by the following unitary matrix in the canonical base of $\mathbb{C}_A^2 \otimes \mathbb{C}_B^2 \otimes \mathbb{C}_C^2$:

$$\hat{U}_{C^2} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \quad (6)$$

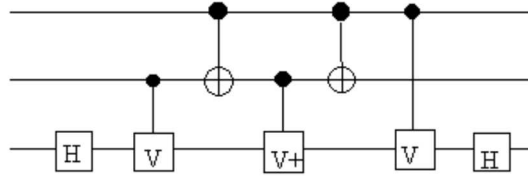
It is easy to check that the C²NOT gate acts on vectors of the canonical base in the following way:

$$\hat{U}_{C^2} |i\rangle |j\rangle |k\rangle = |i\rangle |j\rangle |k \oplus ij\rangle \quad (7)$$

where \oplus is the addition $\text{mod } 2$. The C²NOT gate negates the third (target) qubit only if the first and the second qubits (controls) are in the state $|1\rangle$, otherwise it does not change anything. The graphic representation of C²NOT gate is



The Toffoli gate, like any other three-qubit gate, decomposes into a product of one- and two-qubit gates. One of possible decompositions is the following [1]:



where

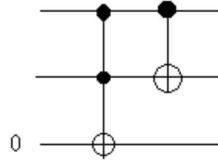
$$\hat{U}_\square = \begin{pmatrix} 1 & 0 \\ 0 & \square \end{pmatrix}, \hat{U}_{\square+} = \begin{pmatrix} 1 & 0 \\ 0 & \square \square \end{pmatrix} \quad (8)$$

2.2. Quantum adders

The addition $\square \square u \square \square 2$ is realized by the quantum CNOT gate (see [7], Sect. 3.12.5) which acts on the canonical base of a two-qubit system in the following way:

$$\hat{U}_{C\square\square\square} |\square \square \rangle = |\square \square \square \rangle \quad (9)$$

A combination of the Toffoli gate and the CNOT gate can act as a $\square u \square ntu \square \square \square \square \square \square e \square$ if only the input state of the third qubit is $|0\rangle$



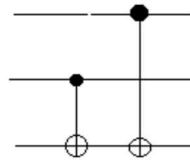
That simple quantum network calculates the sum of the two bits encoded in the input state of the subsystem $\mathbf{Q}_A + \mathbf{Q}_B$, while the output state of \mathbf{Q}_C shows the carry:

$$\hat{U}_{A,B,C\square\square\square} \hat{U}_{A,C,C^2\square\square\square} |\square \square 0\rangle = \hat{U}_{A,B,C\square\square\square} |\square \square \square \rangle = |\square \square \square \square \rangle \quad (10)$$

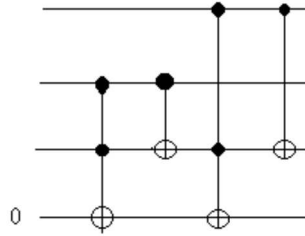
A successive action of two CNOT gates on a three-qubit system realizes the sum of three qubits. Indeed,

$$\hat{U}_{A,C,C\square\square\square} \hat{U}_{B,C,C\square\square\square} |\square \square \square \rangle = \hat{U}_{A,C,C\square\square\square} |\square \square \square \square \rangle = |\square \square \square \square \square \rangle \quad (11)$$

The corresponding diagram is:



A successive action of two quantum half-adders realizes a quantum full adder



Here the input state of the first qubit is the carry c_1 , the output state of the third qubit is the sum $c_2 \oplus a_2 \oplus b_2$, and the output state of the fourth qubit is the new carry $c_3 \oplus c_2 \oplus a_1 \oplus b_1$. The action of the quantum full adder can be summarized as follows:

$$|c_1, a_1, b_1, 0\rangle \rightarrow |c_1, a_1, c_2 \oplus a_2 \oplus b_2, c_3 \oplus c_2 \oplus a_1 \oplus b_1\rangle \tag{12}$$

2.2.1. Quantum parallelism

Notice that quantum adders mentioned above are nothing but a natural extension of the corresponding classical networks. In fact, the action of any such adder on vectors of the canonical base is perfectly analogous to the action of the corresponding "classical" adder. We could expect that the quantum nature of the networks would become manifest when they would act on superpositions of vectors of the canonical base. Take for instance the quantum half-adder. The input state of the third qubit has to be $|0\rangle$, so the most general input state is $\sum_{a_1, b_1} |a_1, b_1, 0\rangle$. The linearity of quantum gates leads to the following output state:

$$\sum_{a_1, b_1} |a_1, b_1, 0\rangle \rightarrow \sum_{a_1, b_1} |a_1, b_1, a_1 \oplus b_1\rangle \tag{13}$$

What we have got is a superposition of all possible results of addition of two bits with the corresponding carry. Thus, apparently the quantum half-adder can do in one computational step what a classical half-adder does in four steps. This surprising feature which is the direct consequence of the linear structure of the state space of qubits is called quantum parallelism. However, it is not obvious how to benefit from quantum parallelism.

Quantum teleportation

The quantum teleportation, discovered by Bennet et al. [3] in 1993, and discussed in many places (see [14]) is often considered as one of the main resources of quantum computers, see e.g. [12]. The process called quantum teleportation is, shortly speaking, a transmission of an unknown quantum state through an "entanglement enhanced" classical channel (comp. [7] 3.14). Assume that there are three qubits Q_{A_1}, Q_{A_2}, Q_B which

constitute quantum composite system; \mathbf{Q}_{A_1} and \mathbf{Q}_{A_2} can be manipulated by Alice, while \mathbf{Q}_B -by Bob. The initial state of the three-qubit system $\mathbf{Q}_{A_1} + \mathbf{Q}_{A_2} + \mathbf{Q}_B$ is assumed to be of the product form: $|v\rangle \otimes |0\rangle \otimes |0\rangle$. The physical interpretation of this state implies that the qubit \mathbf{Q}_{A_1} is in some (unknown) state $|v\rangle$, the qubit \mathbf{Q}_{A_2} is in the state $|0\rangle$, and the qubit \mathbf{Q}_B - in the state $|0\rangle$. It is also assumed that all three qubits are represented by single copies only, so there is not possible to perform a long series of single acts of measurements. If Alice and Bob would have statistical ensembles of their qubits, the unknown state could be identified by Alice, and then reconstructed by Bob. The procedure of teleporting the unknown state $|v\rangle$ of the single copy of \mathbf{Q}_{A_1} from Alice to Bob is performed in several steps.

(1) The following gate is applied:

$$(\widehat{I}_{A_1} \otimes \widehat{U}_{A_2B,C}) (\widehat{I}_{A_1} \otimes \widehat{U}_{A_2} \otimes \widehat{I}_B) \quad (14)$$

it is just the successive application of the Hadamard gate acting on the qubit \mathbf{Q}_{A_2} and the CNOT gate acting on to the qubits \mathbf{Q}_{A_2} and \mathbf{Q}_B . Thus, the gate is simply a three-qubit version of the two-qubit circuit creating entangled states (see [7], Subsection 3.13.2), so the obtained state is

$$|\square\rangle = |v\rangle \otimes |B_1\rangle \quad (15)$$

where

$$|B_1\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \quad (16)$$

is one of the Bell states of the subsystem $\mathbf{Q}_{A_2} + \mathbf{Q}_B$. Thus, the second qubit of Alice and the qubit of Bob became entangled. Decomposing the unknown state $|v\rangle$ in the canonical base:

$$|v\rangle = v_0 |0\rangle + v_1 |1\rangle, \quad (17)$$

we get the decomposition of the state $|\square\rangle$:

$$|\square\rangle = \frac{1}{\sqrt{2}} (v_0 |0\rangle + v_1 |1\rangle) \otimes (|00\rangle + |11\rangle) \quad (18)$$

$$= \frac{1}{\sqrt{2}} (v_0 |000\rangle + v_0 |011\rangle + v_1 |100\rangle + v_1 |111\rangle) \quad (19)$$

(2) Smart Alice realizes that the state $|\square\rangle$ can be decomposed into the superposition of vectors of her Bell base

$$|B_1\rangle \otimes |0\rangle, |B_1\rangle \otimes |1\rangle, |B_2\rangle \otimes |0\rangle, |B_2\rangle \otimes |1\rangle, \quad (20)$$

$$|B_3\rangle \otimes |0\rangle, |B_3\rangle \otimes |1\rangle, |B_4\rangle \otimes |0\rangle, |B_4\rangle \otimes |1\rangle. \quad (21)$$

The decomposition is:

$$|\square\rangle = \frac{1}{2} \left(|B_1\rangle \otimes |v_0\rangle |0\rangle + v_1 |1\rangle \otimes |v_0\rangle |0\rangle + |B_2\rangle \otimes |v_0\rangle |0\rangle + v_1 |1\rangle \otimes |v_0\rangle |0\rangle + |B_3\rangle \otimes |v_1\rangle |0\rangle + v_0 |1\rangle \otimes |v_1\rangle |0\rangle + |B_4\rangle \otimes |v_1\rangle |0\rangle + v_0 |1\rangle \otimes |v_1\rangle |0\rangle \right) \quad (22)$$

Taking this into account, she performs a von Neumann measurement of the Bell observable (comp. [7] 3.14)

$$\widehat{\square} \otimes \widehat{1} = \square_1 |B_1\rangle \langle B_1| + \square_2 |B_2\rangle \langle B_2| + \square_3 |B_3\rangle \langle B_3| + \square_4 |B_4\rangle \langle B_4| \otimes \widehat{1} \quad (23)$$

having four distinct eigenvalues $\square_1, \square_2, \square_3, \square_4$. The measuring apparatus transforms randomly the pre-measurement state $|\square\rangle$ into one of the four possible outcome states:

$$|\square_1\rangle : = c_1 (|B_1\rangle \langle B_1| \otimes \widehat{1}) |\square\rangle = |B_1\rangle \otimes |v_0\rangle |0\rangle + v_1 |1\rangle \otimes |v_0\rangle |0\rangle \quad (24)$$

$$|\square_2\rangle : = c_2 (|B_2\rangle \langle B_2| \otimes \widehat{1}) |\square\rangle = |B_2\rangle \otimes |v_0\rangle |0\rangle + v_1 |1\rangle \otimes |v_0\rangle |0\rangle \quad (25)$$

$$|\square_3\rangle : = c_3 (|B_3\rangle \langle B_3| \otimes \widehat{1}) |\square\rangle = |B_3\rangle \otimes |v_1\rangle |0\rangle + v_0 |1\rangle \otimes |v_1\rangle |0\rangle \quad (26)$$

$$|\square_4\rangle : = c_4 (|B_4\rangle \langle B_4| \otimes \widehat{1}) |\square\rangle = |B_4\rangle \otimes |v_1\rangle |0\rangle + v_0 |1\rangle \otimes |v_1\rangle |0\rangle \quad (27)$$

(c_1, c_2, c_3, c_4 are normalization constants), and at the same time displays one of the corresponding results $\square_1, \square_2, \square_3, \square_4$.

(3) Alice informs Bob on the result of her measurement. She can do that using a classical channel, because she has to send just two classical bits encoding one of the four possible results $\square_1, \square_2, \square_3, \square_4$.

(4) Having got Alice's message, Bob knows the post-measurement state of the three-qubit system: if Alice would send \square_3 the state of $\mathbf{Q}_{A_1} + \mathbf{Q}_{A_2} + \mathbf{Q}_B$ would be $|\square_3\rangle$, $\square = 1, 2, 3, 4$. He applies then one of the four Pauli gates to his qubit according to the message sent by Alice: $\widehat{1}_{A_1} \otimes \widehat{1}_{A_2} \otimes \widehat{1}_B$ if the message was $\square_1, \widehat{1}_{A_1} \otimes \widehat{1}_{A_2} \otimes \widehat{\square}_B$ if the message was $\square_2, \widehat{1}_{A_1} \otimes \widehat{1}_{A_2} \otimes \widehat{\square}_B$ if the message was $\square_3, \widehat{1}_{A_1} \otimes \widehat{1}_{A_2} \otimes \widehat{\square}_B$ if the message was \square_4 . In every of the listed cases Bob's qubit ends up with the state $|v\rangle_B$. Indeed:

$$\widehat{1}_{A_1} \otimes \widehat{1}_{A_2} \otimes \widehat{1}_B |\square_1\rangle = |B_1\rangle \otimes |v\rangle \quad (28)$$

$$\widehat{1}_{A_1} \otimes \widehat{1}_{A_2} \otimes \widehat{\square}_B |\square_2\rangle = |B_2\rangle \otimes |v\rangle \quad (29)$$

$$\widehat{1}_{A_1} \otimes \widehat{1}_{A_2} \otimes \widehat{\square}_B |\square_3\rangle = |B_3\rangle \otimes |v\rangle \quad (30)$$

$$\widehat{1}_{A_1} \otimes \widehat{1}_{A_2} \otimes \widehat{\square}_B |\square_4\rangle = \square |B_4\rangle \otimes |v\rangle \quad (31)$$

(The global phase factor \square in the last line is inessential, see [7] p. 119 - 120.) This completes the teleportation protocol.

Thus, the described procedure transforms in a random way the initial state into one of the listed above states. Independently of which particular final state is obtained, the original unknown state of the first qubit has been faithfully transmitted to the third qubit.

It is commonly assumed that this method of communication, called quantum teleportation, works efficiently even if Alice and Bob are spatially separated. In this case the described protocol would enable sending the unknown quantum state over an arbitrarily large distance with the speed limited only by the speed of light.

Quantum computing

Our exposition was aimed to provide an access to the most popular quantum model of computation, that proposed by Deutsch in 1985 and called the quantum circuit model (also: quantum circuit, quantum network). The Deutsch model consists of two main objects: a quantum register (the memory unit of the quantum computer), which is just an aggregate of a finite number of qubits, and a sequence of quantum gates acting on the register (the computation performed by the quantum computer). Thus, the Deutsch model of computation assumes that logic gates are applied sequentially to a set of qubits. In a standard classical computer, logic gates are localized in fixed points of the circuit board. In a quantum computer, qubits have fixed positions, while quantum gates are interactions which are turned on and off, and act selectively on one or two qubits.

1. Quantum registers

Quantum register is a quantum composite system of n qubits, so its state space \mathcal{H}_n is 2^n -dimensional complex vector space, enhanced with the tensor product structure:

$$\mathcal{H}_n = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \dots \otimes \mathbb{C}^2$$

The canonical base of \mathcal{H}_n consists, like the considered cases of $n = 2$ and $n = 3$, with all tensor products of vectors of canonical bases of the qubits. A typical vector of the canonical base of \mathcal{H}_n is $|i_1\rangle \otimes \dots \otimes |i_n\rangle$ with $i_j = 0, 1$ for all $j = 1, \dots, n$. We use the notation $|i_1, \dots, i_n\rangle$ instead of $|i_1\rangle \otimes \dots \otimes |i_n\rangle$ thus a typical vector of the canonical base of \mathcal{H}_n is $|i\rangle$, where i is an n -element string of zero's and one's. A general state of the register is then represented by the vector

$$\sum_i c_i |i\rangle,$$

with $\sum_i |c_i|^2 = 1$.

2. Quantum computation

The typical quantum computation goes as follows:

- 1) We begin with preparing the starting state of the quantum register, typically $|0, 0, \dots, 0\rangle$. The initial data are usually classical, they can be encoded as a binary string i_1, \dots, i_n ,

so are naturally represented by the vector $|\alpha_1, \dots, \alpha_n\rangle$ belonging to the canonical base of \mathcal{H}_n . Thus, we should transform the starting state $|0, 0, \dots, 0\rangle$ into $|\alpha_1, \dots, \alpha_n\rangle$, this can be done by an appropriate unitary transformation. It is, however, a typical trick of quantum algorithms to transform $|0, 0, \dots, 0\rangle$ into a quantum superposition of all strings the register can represent. This can be achieved by applying the n -fold product of the Hadamard gate

$$\widehat{U}_{n,\alpha} = \frac{1}{\sqrt{2^n}} \widehat{U}_{\alpha_1} \otimes \widehat{U}_{\alpha_2} \otimes \dots \otimes \widehat{U}_{\alpha_n} \quad (32)$$

to the starting state

$$\widehat{U}_{n,\alpha} |0, 0, \dots, 0\rangle = \frac{1}{\sqrt{2^n}} \sum_{\alpha} |\alpha\rangle \quad (33)$$

2) The next step is the computation proper. A computation is then a unitary map

$$\widehat{U} : \mathcal{H}_n \rightarrow \mathcal{H}_n$$

which corresponds to the outcome function of a standard computation. The map \widehat{U} is constructed as an operator product of standard quantum gates (the quantum gate array). Some known quantum algorithms include intermediate non-unitary steps, von Neumann measurements as a rule. It is known, however, that we get the same result with a modified algorithm where all measurements are postponed to the end.

3) The computation is followed by the reading off the obtained result, which is encoded in the final state of the register. Typically, the final state is pure so represented by a vector, say $|\alpha_{out}\rangle \in \mathcal{H}_n$. We are not able to perceive the final state directly, so we have to perform a measurement of some observable on the register in that state. One usually measures, in the von Neumann way, the observable

$$\widehat{\alpha} := \sum_{\alpha} \alpha |\alpha\rangle \langle \alpha| \quad (34)$$

where the summation goes through all 0, 1-strings of length 2^n , and all real numbers α are distinct. The measurement produces the mixture of states of the canonical base, the state $|\alpha\rangle$ would appear with probability $|\langle \alpha | \alpha_{out} \rangle|^2$. Considering the strings α as possible outcomes of the computing, we see that the correct solution appears with a probability less than 1 (if the final state of computing $|\alpha_{out}\rangle$ is not one of vectors of the canonical base). Thus, the quantum computing is a kind of probabilistic computing: we obtain a probability distribution of possibly results α .

4) The fact that the quantum computation is probabilistic forces us to check out the obtained result α . If it does not prove to be a correct solution, we have to repeat the computation.

Reversibility of quantum computation

A physicist entering the area of standard computer science would immediately realize that standard computations are not reversible, so according to basic rules of physics they have to dissipate energy. Because of obvious technical reasons, the dissipation of energy during a computation is not advantageous. It is well known in physics that only a reversible time evolution preserves energy of the evolving system. Hence, the energy loss during computation could be avoided only if the computation would be reversible. A typical classical algorithm defines the outcome function $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$ which transforms the initial data into results of computations. The outcome function is rarely invertible. Nevertheless, we do not lose much if we would consider instead of f the invertible function $F : \{0, 1\}^{n+m} \rightarrow \{0, 1\}^{n+m}$ defined by:

$$F(x, y) := (x, f(x)) \quad (35)$$

where \oplus is the addition mod 2. Indeed, the irreversible algorithm calculating f can be in a polynomial time simulated by a reversible one (calculating F). All that concerns also quantum computers, as unitary transformations which describe quantum calculations (without intermediate measurements) are invertible; that is the reason that all quantum gates considered above are reversible. According to above remarks, the evaluation of a non-invertible function $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$ on a quantum computer has to be performed in the following way. We divide the quantum register into two sub-registers:

$$\mathcal{H}_{n+m} = \underbrace{(\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \dots \otimes \mathbb{C}^2)}_n \otimes \underbrace{(\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \dots \otimes \mathbb{C}^2)}_m$$

Then we encode $\{0, 1\}^{n+m}$ by states of the canonical base:

$$\{0, 1\}^{n+m} \ni (x, y) \mapsto |x\rangle \otimes |y\rangle \quad (36)$$

and extend the map $(x, y) \mapsto (x, f(x))$ to a unitary map $\hat{U} : \mathcal{H}_{n+m} \rightarrow \mathcal{H}_{n+m}$ which acts on both sub-registers.

1. Quantum parallelism again

It is clear that the unitary map $\hat{U} : \mathcal{H}_{n+m} \rightarrow \mathcal{H}_{n+m}$ defined above is a natural quantum extension of the invertible function $F : \{0, 1\}^{n+m} \rightarrow \{0, 1\}^{n+m}$: if we let \hat{U} act on the canonical base of \mathcal{H}_{n+m} we get exactly F . The power of quantum computing appears when we act with \hat{U} on a superposition of vectors of the canonical base, for instance on the equal-coefficient superposition

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0, 1\}^n} |x\rangle \otimes |0, \dots, 0\rangle \quad (37)$$

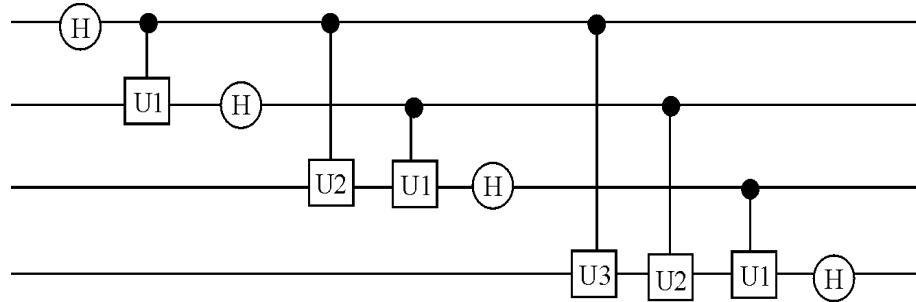
By the linearity of quantum evolution, we get the output superposition

$$\widehat{U} \frac{1}{\sqrt{2^n}} |\alpha\rangle \otimes |0, \dots, 0\rangle = \frac{1}{\sqrt{2^n}} |\alpha\rangle \otimes |\alpha\rangle \quad (3)$$

It is clearly seen that we have computed all values of α by running \widehat{U} just once - this is the phenomenon called the quantum parallelism (a simpler case has been mentioned in Subsection 2.2.1). Quantum parallelism, discovered by Deutsch in 1985, is considered as one of the main resources of quantum computation. We should notice, however, that the output state $\frac{1}{\sqrt{2^n}} |\alpha\rangle \otimes |\alpha\rangle$ is highly entangled, so it is hard to extract from it all the information it contains. Indeed, the quantum state cannot be read off directly; the information encoded in it can be extracted by a measurement (see step 3. of our general scheme of quantum computation, Subsection 4.2). A single run of a von Neumann measurement with respect to the canonical base $|\alpha, \mathbf{y}\rangle$ of \mathcal{H}_{n+n} on the state $\frac{1}{\sqrt{2^n}} |\alpha\rangle \otimes |\alpha\rangle$ produces randomly one of base states $|\alpha, \mathbf{y}\rangle$ with probability $\frac{1}{2^n} |\langle \mathbf{y} | \alpha \rangle|^2$. It is impossible to identify α having only one result of this kind.

Quantum FT on four qubits

Quantum algorithms are discussed in many places. For instance, an elementary presentation of the quantum search algorithm (Grover's algorithm) can be found in [5], the known quantum factorization algorithm of Shor is presented in [11], etc. Here we provide only a simple example showing a quantum circuit implementing the quantum discrete Fourier transform (QFT) on four qubits. (The picture, which appeared in many places, is taken from [13]. For a generalization to n qubits see [9].)



The reader should recognize one-qubit Hadamard gates (see [7]), and controlled unitary gates C-U1, C-U2, C-U3. The one-qubit gates $\widehat{U}_{U1}, \widehat{U}_{U2}, \widehat{U}_{U3}$ are defined as follows:

$$\widehat{U}_{U1} := \begin{pmatrix} 1 & 0 \\ 0 & e^{-\frac{\pi}{2}} \end{pmatrix}, \quad \widehat{U}_{U2} := \begin{pmatrix} 1 & 0 \\ 0 & e^{-\frac{\pi}{4}} \end{pmatrix}, \quad \widehat{U}_{U3} := \begin{pmatrix} 1 & 0 \\ 0 & e^{-\frac{\pi}{8}} \end{pmatrix} \quad (39)$$

An analysis of the action of that circuit should not be hard.

□□ Resources of quantum computation

Let us comment the intriguing question: what is the reason for the extraordinary power of quantum computer □ The "quantum magic tricks" like the quantum dense coding, quantum teleportation, quantum parallelism, have been considered as the main quantum resources. They seem, however, to have the common source: entanglement, which in turn is a direct consequence of the superposition principle □. of the linearity of the state space of a quantum object. That suggests the actually prevailing opinion: entanglement, the mysterious coupling of composite quantum systems, is the property responsible for the "exponential speedup" of quantum computation. It should be noticed, however, that the most successful method of experimental implementation of quantum algorithms, that based on NMR (see [6] for a review), does not use entanglement at all □ That indicates that an explanation of the extraordinary power of quantum computer is still an open question.

□□ Concluding remarks

Both parts of the present paper provide a concise introduction into the new area of theoretical computer science: the quantum theory of computation. Since ten years the quantum computer research develops intensively, almost every month brings new remarkable achievements, so it were impossible to cover all the discussed topics of quantum computing in an introductory paper. A more advanced presentations of the actual state of the quantum computing science could be find in recent reviews like [10], [4], or [1]. The reader is also encouraged to search the Los Alamos preprint archive where all actual research papers are collected together with many interesting reviews, dissertations, and lecture notes.

What can we say about the future of the idea of quantum computer □ The actually developed experimental implementations of quantum algorithms are not very promising because of the scaling problem; their main result is the demonstration that the idea does work at all. Even if a working quantum computer would not be constructed in coming ten or twenty years, it seems sure that the progress in nano-technology will necessarily bring us to the borderline of the quantum world, making inevitable an introduction of quantum aspects into the practical computer science. That should force fundamental changes in theoretical computer science to make it applicable to quantum objects. The actual development of quantum computing theory should be seen as a preliminary stage of the process of constructing the new universal theory of information and computation.

References

- [1] G. Alber, T. Beth, M. Horodecki, R. Horodecki, M. Rotteler, H. Weinfurter, R. Werner, A. Zeilinger (edit.): *Quantum Information* (Springer, Berlin, 2001)
- [2] A. Barenco, C. H. Bennett, R. Cleve, 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.
- [3] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, W. K. Wootters: *Teleporting an unknown quantum state via dual classical and quantum channels*. Physical Review Letters 70 (1993) 1195 - 1199.
- [4] B. Bouwmeester, A. Ekert, A. Zeilinger (Eds.): *The quantum computer and quantum cryptography*. (Springer-Verlag, Berlin, 2000).
- [5] S. Bugajski: *Quantum computing*. Archiwum Informatyki Teoretycznej i Stosowanej vol.13, no. 2, 2001, 143 - 150.
- [6] S. Bugajski, M. Gibas: *Quantum computing* (Polish). To appear in Studia Informatica 22 (2002)
- [7] S. Bugajski, J. Klamka, S. Węgrzyn: *Quantum computing*. Archiwum Informatyki Teoretycznej i Stosowanej vol.13, no. 2 (2001) 97 - 142.
- [8] R. Cleve: *An efficient algorithm for quantum communication*. arXiv:quant-ph/9906111 28 Jun 1999
- [9] T. G. Draper: *Addition on a quantum computer*. arXiv:quant-ph/0008033 v1 7 Aug 2000
- [10] A. Ekert, P. Hayden, H. Inamori: *Basic concepts in quantum computation*. arXiv:quant-ph/0011013 2 Nov 2000
- [11] A. Ekert, R. Jozsa: *Quantum computation and Shor's factoring algorithm*. Reviews of Modern Physics 68 (1996) 733 - 753.
- [12] D. Gottesman, I. L. Chuang: *Quantum teleportation is a universal computational primitive*. arXiv:quant-ph/9908010 v1 2 Aug 1999
- [13] M. Keyl: *Fundamentals of quantum information theory*. arXiv:quant-ph/0202122 v1 21 Feb 2002
- [14] J. Preskill: *Quantum Information and Quantum Computation*. Lecture notes 1998 - 1999. <http://www.theory.caltech.edu/~preskill/ph229>

Podstawy obliczeń kwantowych. Część II.

Streszczenie

W drugiej części opracowania dyskutuje się trójubitowe bramki kwantowe, sumatory kwantowe oraz najprostszą wersję protokołu teleportacji. Podano również ogólną postać procesu obliczeń kwantowych oraz przedyskutowano ich specyfikę a mianowicie równoległość i odwracalność obliczeń.