Theory and Perspectives of Quantum Computers

V. Kupča, T. Rosa

xrosa@fel.cvut.cz

CTU, Faculty of Electrical Engineering, Dept. of Computer Science and Engineering,
Karlovo nám. 13, 121 35 Praha 2

There are basically two reasons, why people interested in the computer science are becoming also interested in the theory of quantum physics. The first reason is due to the increasing effort in the area of miniaturization of elementary blocks used to build up modern computers. Here the theory of quantum physics (in this sense could also be referred to as the theory of micro-world) tells us that we cannot expect to have always the same behavior of these blocks, while their size decreases to the level of atoms. Therefore such pseudoscientific reasoning of the type: "If every atom in the space could compute a partial piece of this problem..." is fatally wrong if we consider that these atoms would behave like contemporary computers do.

The second reason is due to the never fading effort of many scientists to find some brand-new computer architecture, which would be able to solve some of those problems being very hard for contemporary computers in order of magnitude faster. Studying such architectures is very important for the area of complexity theory as it concretes our ideas of what is feasible to compute and what is not. The outcomes of this theory are then very essential for such areas as cryptography, because it strictly relies on the set of assumption of what eventual attackers are able to compute in the reasonable amount of time and what they aren't able to do.

The theory of quantum physics seems to give us the most correct answers to both of the problems illustrated above. It not only tells us, how would building blocks of future computers downsized to the level of atoms behave, it also shows us that such computers (often referred to as *quantum computers*) could be highly effective for solving particular problems which are considered to be very hard yet (we will give an example of such problem later in this text).

Now we will give very brief illustration of the behavior of the quantum computer. In particular we will consider the 2-qubit register. Note that *qubit* is the quantum equivalent of the term "bit" used in contemporary computers. It could be defined as the amount of information held in the quantum system with two possible *eigenstates* (when we measure selected property of this system we can get at most two different results). To represent the state of quantum register we use the elements of Hilbert space ($\boldsymbol{H}$) constructed over the field of complex numbers. Vectors of this space create the set of possible states, while the basis of the space corresponds to the set of possible eigenstates. So n-qubit register corresponds with the Hilbert space of dimension 2^n.

The state of 2-qubit register can be expressed as the following linear combination of basis's vectors:

$$|\Psi\rangle = a_1|00\rangle + a_2|01\rangle + a_3|10\rangle + a_4|11\rangle, \text{ where } a_i \in \mathbb{C}, 1 \le i \le 4$$

Here the vectors (using Dirac's ket-bra notation) |00>, |01>, |10> and |11> form basis of $\boldsymbol{H}$ of dimension four. Until measured, the quantum register stays in the superposition of these eigenstates. The value of $|a_i|^2$ corresponds with the probability that following measure gives the value joined with corresponding base vector. So, although the value obtained by measuring this register can be one of four possible eigenstates, while the computation process run, the register remains in one of infinitely many superpositions of these values. This

phenomenon is referred to as the *quantum superposition* and is one of the key features of the quantum computers.

Another essential property of the quantum computers follows directly from the the quantum superposition. It is referred to as the *quantum paralelism* and it is based on the simple observation, that by altering n-qubits of the quantum register, we are in fact altering 2^n coefficients of the linear superposition describing the new state.

There are of course many other interesting features of quantum systems, including the phenomenon of the *quantum entanglement* (results obtained by measuring different qubits in given register can be correlated). Practical demonstration of the power of (however still theoretical) quantum computers is for example the Shor's algorithm [2]. Given quantum computer with appropriate memory (denoted in qubits) capacity it is able to solve the integer factorization problem or the discrete logarithm problem with the polynomial time complexity. Both of these problems are considered to be NP on contemporary computers.

These problems are very essential for cryptography as the main asymmetric cryptosystems used nowadays (RSA, D-H protocol, DSS, El Gamal) rely heavily on their complexity. The existence of effective algorithms for their solution therefore cryptographers sometimes refer to as *the end of cryptography as we know it*. It follows that the Shor's algorithm has not only theoretical significance, but it has really strong practical impact on the area of computer security when the appropriate quantum computers become the reality.

On the other hand, the quantum theory gives to cryptographers not only the threat in the existence of quantum computers. It also shows how to build new cryptography mechanisms based not on the complexity of selected mathematical problems, but on the possibility/impossibility directly given by nature's laws. The random collapse of quantum state into one of the eigenstates for example can be used to build the quantum version of the key agreement protocol just now. Quantum cryptography exploits directly the laws of the quantum physics, so it doesn't have to wait until powerful quantum computers are built. Thus, the good news for the cryptography is that we will probably have working quantum cryptosystems until the standard ones are discarded by the existence of the quantum computers. Also the existence of the quantum computers doesn't seem to affect the complexity of all mathematical problems. So it would be still possible to design secure "pure" mathematic's cryptosystem. It follows that the quantum computers don't mean the end of the security and privacy in the electronic world.

The diploma thesis [1] tries to give the description of the theory behind the quantum computers for those who are mainly concerned in the area of the theoretical informatics. Its main aim is to give to those people the readable introduction into the problems and benefits joined with this phenomenon.

References:

[1] KUPČA, V.: *Theory and Perspectives of Quantum Computers* Diploma Thesis, CTU-FEE, 2000 in czech.

[2] SHOR, P. W.: *Polynomial time algorithms for prime factorization and discrete logarithms on quantum computer.* SIAM Journal of Computing 1997, pp. 26(5):1484–1509.

[3] STEAN, A. M.: *Quantum Computing* http://xxx.lanl.gov/abs/quant-ph?9708022, 1997.

[4] WILLIAMS, C. P. - CLEARWATER, S. H. *Explorations in QUANTUM COMPUTING* Springer-Verlag 1998.