QUANTUM COMPUTING

Artyom Dmitriyev, *post-graduate student*

Changing the model underlying information and computation from a classical mechanical to a quantum mechanical one yields faster algorithms, novel cryptographic mechanisms, and alternative methods of communication. Quantum algorithms can perform a select set of tasks vastly more efficiently than any classical algorithm, but for many tasks it has been proven that quantum algorithms provide no advantage.

Problems generally get harder as the size of the input increases. The efficiency of an algorithm is quantified in terms of an asymptotic quantity that looks at how the resources used by the algorithm grow with the input. Time and space, generally measured in terms of number of operations and number of bits or qubits, are the resources most often considered. Constant factors are usually ignored, since they depend on fine details of an implementation that often are not known, but can be bounded.

For some problems quantum computation gives efficient results in polynomial time, but for their implementation one needs a quantum computer. Once a quantum computer will be developed a lot of problems such as discrete log or factoring will be sold and this will lead to profoundly understanding of our quantum world.

DiVincenzo developed widely used requirements for a quantum computer. It is relatively easy to obtain N qubits, but it is hard to get them to interact with each other and with control devices, but nothing else. DiVincenzo's criteria are, roughly:

- Scalable physical system with well-characterized qubits
- Ability to initialize the qubits in a simple state
- Robustness to environmental noise
- A set of "universal" gates that approximate all quantum operations
- High efficiency, qubit-specific measurements

There were a lot of efforts but no one could ever build such machine yet. But researches keep trying more progressive techniques.

The breadth of quantum computing applications is still being explored. Major application areas include security and the many fields that would benefit from efficient quantum simulation. The quantum information processing viewpoint provides insight into classical algorithmic issues as well as a deeper understanding of entanglement and other non-classical aspects of quantum physics.

A.M.Dyadechko, *ELA*