Is fault-tolerant quantum computation really possible?

M. I. Dyakonov Université Montpellier II, France

The answer that the quantum computing community currently gives to this question is a definitive "yes". The so-called "threshold" theorem says that, once the error rate per qubit per gate is below a certain value, estimated as 10^{-4} – 10^{-6} , indefinitely long quantum computations are feasible, even if all of the 10^3 – 10^6 qubits involved are subject to relaxation processes, and all the manipulations with qubits are not exact. By active intervention, errors caused by decoherence can be detected and corrected during the computation. Though today we may be several orders of magnitude below the required threshold, quantum engineers may achieve it tomorrow (or in a thousand years), making large-scale quantum computation possible *in principle*.

The purpose of this talk is to explain these ideas and to examine in some detail the technical prescription for fault-tolerant quantum computing, first put forward by Shor and elaborated by other mathematicians. Special care will be taken to reveal the hidden assumptions on which it is based. It seems that the mathematics behind the threshold theorem is somewhat detached from the physical reality. This raises serious doubts on the possibility (even as a matter of principle) of quantum computing on times exceeding the typical relaxation time.