When will we have a quantum computer?

Michel I. Dyakonov
Laboratoire Charles Coulomb, Université Montpellier, France

A *classical* computer with *N* bits (transistors), has 2^N possible states, and the computation process consists in switching *on* or *off* certain transistors according to a prescribed program. In contrast, the *quantum* computer with *N qubits* (spins) is characterized by 2^N quantum amplitudes, which are *continuous* complex variables.

Thus, a toy quantum computer with, say, 50 qubits will be characterized at any given moment by $2^{50} = 1125899906842624$ continuous parameters, which we should be able to manipulate at will. However the number of qubits needed to have a *useful* machine (*i.e.* one that can compete with your laptop in factoring very large numbers) is estimated to be 10^3–10^5. The number of continuous variables describing the state of such an apparatus at any given moment is at least 2^{1000} ($\sim 10^{300}$) which is much, much greater than the number of particles in the entire Universe (only $\sim 10^{80}$)!

Thus the answer to the question in the title is: As soon as the physicists and engineers will learn to control this quantity of continuous parameters!

In recent years the trend is to advertise as quantum computers circuits made from truly quantum devices based on Josephson junctions at liquid helium temperatures, an approach that was initially started by the D-wave company, followed and developed by IBM, Google, Microsoft, and others. This is *not* going to be the quantum computer everyone was talking about during the last 20 years, as it will *not* be able to factor large numbers by Shor's algorithm. It will not and cannot compute anything at all, except its own ground state, a process labeled as "*quantum annealing*".

After initial preparation, any system, whether classical or quantum, at low temperature will relax to its ground state. Calculating the ground state of a more or less complex quantum system, either analytically or numerically, is usually impossible – this is what originally inspired Feynman's idea of quantum computing. However, we can measure *some* properties of this ground state. (The full characterization of the ground state requires measuring 2^N parameters).

It is not entirely clear what will be the possible practical use of such systems. However, such modeling might provide some additional knowledge on the behavior of large and complicated quantum systems.