Quantum Information Processing: An Emerging Field

Simona Caraiman

Computer Engineering Department, Technical University of Iasi, Romania

Quantum computation and quantum information systems have recently received a lot of attention due to their spectacular perspectives especially regarding performance speedup and secure communication. Moreover, it seems that soon the binary unit of information, the bit, will be implemented at subatomic scale. Thus, the extrapolation of Moore's Law recommends quantum systems as the natural choice for implementing future computing systems. In the last two decades, scientists have found that the necessary reformulation of information processing in accordance with quantum physics (or Quantum Information Processing) is a tremendously powerful concept for information processing and communication. This is due to the immense computing power provided by a quantum machine compared to that of a classical one. It comes as a direct consequence of the principles of quantum physics that translate into three remarkable quantum resources: quantum parallelism, quantum interference and entanglement of quantum states.

Quantum computers promise to solve complex problems that are currently impossible on even the world's largest supercomputers. Thus, the remarkable properties of quantum systems have led to the emergence of innovative ideas in all major fields of computing. Efficient quantum algorithms have been formulated allowing for significantly faster calculations than on classical computers. Nevertheless, there are fundamental differences between the algorithms that can be run on quantum computers and those run on classical computers. Consequently, a major challenge in quantum computation is to develop efficient quantum algorithms. These differences come from the probabilistic nature of quantum mechanics which stems from the act of measurement: even though a quantum computer can do exponentially many computations in parallel, a measurement of the resulting quantum state yields a random outcome which is not necessarily the particular outcome searched for. The common approach to cope with this behavior is to create constructive interference among the computational paths that lead to 'right' answers and thus high probability of observing those answers.

At present, quantum computation may seem unachievable, but small quantum computers have already been built and larger machines are being developed. The development of efficient quantum algorithms for practical problems would help in justifying the immense efforts required for building a working quantum computer as it represents a very challenging task that requires spending a huge amount of resources.