AN INTRODUCTION TO THE PHYSICAL FRAMEWORK OF QUANTUM INFORMATION SCIENCE

Klaus Mølmer
Department of Physics, Aarhus University

The superposition principle of quantum mechanics - physical states are represented as vectors in a Hilbert space - suggests to code different data in different quantum states and to process them all in parallel in a single physical process, and on a single processor unit. The fundamental probabilistic nature of measurements in quantum physics, however, put limitations on what can actually be gained by such quantum information processing.

Information processing capabilities are defined and restricted by the practical properties of the physical systems used and by the general framework of quantum theory. Technologies related to thermal properties, physical motion, electrical conductivity, etc., were over the past centuries developed hand in hand with the basic theories of classical physics, and in the same spirit, the investigation of quantum information concepts contributes new concepts and insights to our understanding of the quantum physical world.

Since the 1994 discovery by Peter Shor, that a quantum computer may factor large numbers more efficiently than any known classical computing strategy, research in quantum computing has been studied by a large number of research communities and its potential has been recognized by a variety of national, international, strategic, and commercial institutions. Quantum computers have to be constructed as physical systems in laboratories, and numerous candidate systems are under current experimental investigation: trapped ions, cold atoms, superconducting circuits, liquid and solid state spin ensembles, etc.

The lecture will introduce the basic concepts of quantum information processing with an emphasis on how our theoretical description must reflects, on the one hand, the specific algebraic properties associated with concrete physical systems and, on the other hand, the fundamental rules of quantum physics, related to, e.g., uncertainty relations and complementarity. We will look at the current status of a few experimental strategies, and we will use these examples to illustrate the theoretical challenges, and sometimes surprising advances, in the development of secure communication, precise gate operations, reliable data storage, and implementation of useful algorithms.