Lectures on Quantum Measurements

Czech Technical University, Prague, June 2009

By: János Bergou
CUNY Hunter College

Abstract

Measurements are an integral part of quantum information processing. Reading out the quantum information at the end of the processing pipeline is equivalent to learning what final state the system is in at the output since information is encoded in the state. In fact, information is the state itself. Since the only way to determine the state of a system is to perform measurements on it, we need a thorough understanding of the quantum theory (and practice) of measurements. To this end we will begin by a simplified model of a quantum measurement, due essentially to von Neumann, and from this model we will read out the postulates of standard quantum measurement theory. Then, by analyzing the underlying assumptions we will show that some of the postulates can be replaced by more relaxed ones and this will lead us to the concept of generalized measurements (POVMs), which are particularly useful in measurement optimization problems. Next, by invoking Neumark's theorem we will show how to actually implement POVMs experimentally. As illustrations of these general concepts we will study two state discrimination strategies in some detail, namely the unambiguous discrimination and the minimum error discrimination of two quantum states. For an application of these ideas we will analyze the B92 protocol for quantum key distribution (QKD). QKD is the crucial ingredient of most quantum cryptographic protocols and in the B92 proposal all of the concepts of measurement theory come together in a particularly clean and instructive form.