Quantum Side Information: Uncertainty Relations, Extractors, Channel Simulations

A dissertation submitted to

ETH ZURICH

for the degree of
Doctor of Sciences

presented by

Mario Andrea Berta
Dipl. Phys. ETH

born April 27, 1985, in Winterthur
citizen of Selma, GR, Switzerland

accepted on the recommendation of

Prof. Dr. Matthias Christandl, examiner
Prof. Dr. Patrick Hayden, co-examiner
Prof. Dr. Renato Renner, co-examiner

2013
Abstract

Any theory of information processing always depends on an underlying physical theory. Information theory based on classical physics is known as classical information theory, and information theory based on quantum mechanics is called quantum information theory. It is the aim of this thesis to improve our understanding of the similarities and differences between classical and quantum information theory by discussing various information theoretic problems from the perspective of an observer with the ability to perform quantum operations. This thesis is divided into four parts, each is self contained and can also be read separately.

In the first part, we discuss the algebraic approach to classical and quantum physics and develop information theoretic concepts within this setup. This approach has the advantage of being mathematically very general, and with this, allows to describe virtually all classical and quantum mechanical systems. Moreover, it enables us to include physical situations with infinitely many degrees of freedom involved.

In the second part, we discuss the uncertainty principle in quantum mechanics. The principle states that even if we have full classical information about the state of a quantum system, it is impossible to deterministically predict the outcomes of all possible measurements. In comparison, the perspective of a quantum observer allows to have quantum information about the state of a quantum system. This then leads to an interplay between uncertainty and quantum correlations. It turns out that even in the presence of this additional information, we exhibit nontrivial bounds on the uncertainty contained in the measurements of complementary observables. We provide an information theoretic analysis by discussing so-called entropic uncertainty relations with quantum side information.

In the third part, we discuss the concept of randomness extractors. Classical and quantum randomness are an essential resource in information theory, cryptography, and computation. However, most sources of randomness exhibit only weak forms of unpredictability, and the goal of randomness extraction is to convert such weak randomness into (almost) perfect randomness. We discuss various constructions for classical and quantum randomness extractors, and we examine especially the performance of these constructions relative to an observer with quantum side information.
In the fourth part, we discuss channel simulations. Shannon’s noisy channel theorem determines the capacity of classical channels to transmit classical information, and it can be understood as the use of a noisy channel to simulate a noiseless one. Channel simulations as we want to consider them here are about the reverse problem: simulating noisy channels from noiseless ones. Starting from the purely classical case (the classical reverse Shannon theorem), we develop various kinds of quantum channel simulation results. We achieve this by exploiting quantum correlations, and using classical and quantum randomness extractors that also work with respect to quantum side information. Finally, we discuss implications to channel coding theory, quantum physics, and quantum cryptography.
Zusammenfassung

Jede Theorie über Information und deren Verarbeitung basiert auf einer zugrundeliegenden physikalischen Theorie. Informationstheorie basierend auf klassischer Physik bezeichnet man als klassische Informationstheorie und Informationstheorie basierend auf Quantenmechanik heisst Quanteninformationstheorie. Das Ziel dieser Doktorarbeit ist es, die Gemeinsamkeiten und Unterschiede von klassischer Informationstheorie und Quanteninformationstheorie zu verdeutlichen. Zu diesem Zweck diskutieren wir verschiedene informationstheoretische Probleme aus der Perspektive eines quantenmechanischen Beobachters. Die Doktorarbeit besteht aus vier Teilen, welche je auch einzeln gelesen werden können.

Im ersten Teil diskutieren wir die algebraische Herangehensweise an die klassische Physik und die Quantenphysik und entwickeln informationstheoretische Konzepte in diesem Formalismus. Dies erlaubt uns, mathematisch sehr allgemein zu sein und damit praktisch alle klassischen und quantenmechanischen Systeme zu beschreiben.

Im zweiten Teil besprechen wir das Unschärfeprinzip der Quantenmechanik. Dieses Prinzip besagt, dass auch bei Vorliegen vollständiger klassischer Information über den Zustand eines quantenmechanischen Systems, es nicht möglich ist, die Ausgänge aller möglichen Messungen vorherzusagen. Die Perspektive eines quantenmechanischen Beobachters erlaubt es nun aber, quantenmechanische Information über das Quantensystem zu haben. Dies führt zu einem Wechselspiel zwischen Unschärfe und quantenmechanischen Korrelationen. Wir beschreiben eine informationstheoretische Analyse dieses erweiterten Unschärfeprinzips mit Hilfe von sogenannten entropischen Unschärfereaktionen mit zusätzlicher quantenmechanischer Information.

Im dritten Teil diskutieren wir Zufallsextraktoren. Klassische und quantenmechanische Zufallszahlen sind eine fundamentale Ressource in der Informationstheorie, der Kryptographie und der theoretischen Informatik. Allerdings sind die meisten Quellen nicht perfekt zufällig und die Idee von Zufallsextraktoren ist es, auch aus solchen Quellen (fast) perfekte Zufallszahlen zu generieren. Wir diskutieren verschiedene klassische und quantenmechanische Zufallsextraktoren und untersuchen insbesondere, ob die Konstruktionen auch aus der Perspektive eines quantenmechanischen Beobachters funktionieren.
Im vierten Teil diskutieren wir Kanalsimulationen. Das Kanalcodierungs- 
theorem von Shannon bestimmt die Kapazität von klassischen Kanälen zur 
Übertragung von klassischer Information, indem es beschreibt, wie man 
mit gestörten Kanälen perfekte Kanäle simuliert. Hier schauen wir uns das 
umgekehrte Problem an; wir wollen mit perfekten Kanälen gestörte Kanäle 
simulieren. Ausgehend von klassischen Resultaten (dem invertierten Shan-
non Kanalcodierungstheorem) entwickeln wir verschiedene quantenmech-
anische Kanalsimulationen. Zu diesem Zweck nutzen wir quantenmecha-
nische Korrelationen und verwenden klassische und quantenmechanische 
Zufallsextraktoren, welche auch aus der Perspektive eines quantenmecha-
nischen Beobachters funktionieren. Zum Schluss diskutieren wir Anwen-
dungen in der Codierungstheorie, Quantenphysik und Quantenkryptogra-
phie.