

Quantum Proof Systems and Entanglement Theory

by

Salman Abolfathe Beikidezfuli

Submitted to the Department of Mathematics
on May 1, 2009, in partial fulfillment of the
requirements for the degree of
DOCTOR OF PHILOSOPHY

Abstract

Quantum complexity theory is important from the point of view of not only theory of computation but also quantum information theory. In particular, quantum multi-prover interactive proof systems are defined based on complexity theory notions, while their characterization can be formulated using LOCC operations. On the other hand, the main resource in quantum information theory is entanglement, which can be considered as a monotonic decreasing quantity under LOCC maps. Indeed, any result in quantum proof systems can be translated to entanglement theory, and vice versa. In this thesis I mostly focus on quantum Merlin-Arthur games as a proof system in quantum complexity theory.

I present a new complete problem for the complexity class QMA. I also show that computing both the Holevo capacity and the minimum output entropy of quantum channels are NP-hard. Then I move to the multiple-Merlin-Arthur games and show that assuming some additivity conjecture for entanglement of formation, we can amplify the gap in QMA(2) protocols. Based on the same assumption, I show that the QMA(k)-hierarchy collapses to QMA(2). I also prove that QMA_{log}(2), which is defined the same as QMA(2) except that the size of witnesses is logarithmic, with the gap $n^{-(3+\epsilon)}$ contains NP. Finally, motivated by the previous results, I show that the positive partial transpose test gives no bound on the trace distance of a given bipartite state from the set of separable states.

Thesis Supervisor: Peter W. Shor

Title: Morss Professor of Applied Mathematics