Introduction to Quantum Proof Systems and Applications

Liam Salt - APMA 990

April 3, 2022

Contents

Abstract

In this paper, we introduce quantum interactive proof systems, demonstrate their advantages over classical systems, and showcase their utility by using them to prove certain properties of finite groups. A quantum proof is a state which, along with some quantum computations, can be used to solve problems in Quantum MA (QMA), a class of decision problems analogous to NP. Using the notion of a black box group, a type of oracle, we exemplify the power of quantum proof systems by considering such problems as group non-membership. We show that this problem is solvable (up to some error) in polynomial time, which is impossible classically. Efficient solving and verification of group non-membership also allows us to approach other group theoretical problems such as: finding the maximal normal subgroup, and whether an integer N divides the order of a group.

1 Introduction

1.1 Computer Science Background

Before we can begin to define a quantum proof system, we first must introduce some classical computing formalism and terminology. In classical computing, an *interactive proof system* is a Turing machine that encapsulates the mathematical idea of a proof. It models a proof as a sequence of communications between two actors: a potentially dishonest *prover*, and a skeptical, honest verifier. Through various *rounds* of communication, the prover attempts to convince the verifier to accept their proof. The default convention is to assume the verifier is constrained to be a deterministic polynomial-time TM, whereas we make no constraints to the prover's computational power. Additionally, an interactive proof system is assumed to satisfy both *completeness* and *soundess*, defined below:

Definition. *An interactive proof system is said to be* <u>*complete*</u> *or to satisfy completeness if for any true statement, the prover can always convince the verifier of its validity.*

Definition. *An interactive proof system is said to be* <u>*sound*</u> *if for any false statement, the prover can only with negligible probability convince the verifier of its validity.*

Remark. *Often, many of these conditions are loosened in various ways, e.g. the prover only needing to convince the verifier up to some probability.*

Now we can more formally define an interactive proof system.

We say that a formal language L has a k-round interactive proof system with error probability ε with prover verifier pair (P, V) if:

1. (P, V) either accepts or rejects any input after k rounds
2. $\forall x \in L, (P, V)$ accepts x with probability 1
3. $\forall x \notin L, (P, V)$ accepts x with probability ε

Given this definition, a familiar, degenerate example is to show that any language in **NP** has a $1-$round interactive proof system with error probability 0. We recall that one definition of **NP** is as the set of decision problems whose positive answers can be verified in polynomial time by a deterministic Turing machine. Accordingly, if a problem is in **NP**, then by definition our prover can produce a polynomial-sized certificate that can be verified in polynomial-time.

1.2 Arthur-Merlin Protocol

d

2 Quantum Complexity Classes

d

2.1 Relationship Between QMA and PP

d

3 Group Theoretic Applications

d

3.1 Group Non-Membership

d

3.2 Other Applications/Open Problems

j