A QUANTUM CHARACTERIZATION OF NP

HUGUE BLIER AND ALAIN TAPP

Abstract. In this article, we introduce a new complexity class called \( \text{PQMA}_{\log(2)} \). Informally, this is the class of languages for which membership has a logarithmic-size quantum proof with perfect completeness and soundness, which is polynomially close to 1 in a context where the verifier is provided a proof with two unentangled parts. We then show that \( \text{PQMA}_{\log(2)} = \text{NP} \). For this to be possible, it is important, when defining the class, not to give too much power to the verifier. This result, when compared to the fact that \( \text{QMA}_{\log} = \text{BQP} \), gives us new insight into the power of quantum information and the impact of entanglement.

Keywords. Quantum complexity, interactive proof.

Subject classification. 68Q15 Complexity classes.

1. Introduction

In classical complexity, the concept of proof is extensively used to define very interesting complexity classes such as \( \text{NP}, \text{MA}, \) and \( \text{IP} \). When allowing the verifier (and the prover) to be quantum mechanical, we obtain complexity classes such as \( \text{QMA} \) and \( \text{QIP} \). Quantum complexity classes can sometimes turn out to have surprising properties. For example, in contrast to the classical case, we know that quantum interactive proofs can be restricted to three messages; that is, \( \text{QIP} = \text{QIP} (3) \) (Kitaev & Watrous 2000).

Because of the probabilistic nature of quantum computation, the most natural quantum generalization of \( \text{NP} \) is \( \text{QMA} \). This is the class of languages having polynomial-size quantum proofs. A quantum proof obviously requires a quantum verifier, but
behave similar to a classical proof with regard to completeness and soundness. Since group non-membership is in QMA (Watrous 2000), but is not known to be in MA (and therefore NP), we have an example of a statement having polynomial-size quantum proofs but no known polynomial-size classical proof.

In this paper, we are interested in logarithmic-size quantum proofs. Classically, when considering a polynomial-time verifier, the concept of logarithmic-size classical proofs is not interesting. Any language having logarithmic-size classical proofs would also be in P, since one can go through every possible logarithmic-size proof in polynomial time.

In the quantum case, very short quantum proofs could still be interesting. Any reasonable classical description of a quantum proof requires a polynomial number of bits, and thus, one cannot try all quantum proofs using a classical simulator. That being said, if the verifier is simple enough, the optimization problem of finding a proof that makes the verifier accept with high enough probability can be turned into a semidefinite programming problem (Alizadeh 1995; Vandenberghe & Boyd 1996) of polynomial size. Thus, if the verifier is simple enough, then the language is in P. Also, if the verifier is in BQP, then one still only obtains BQP (Marriott & Watrous 2004).

Although we just argued that logarithmic-size classical and quantum proofs seem uninteresting, by slightly changing the rules of the game, we get an interesting complexity class. In preliminary work (Blier & Tapp 2008), we showed that $\text{NP} \subseteq \text{QMA}_{\log(2)}$. This class is also defined with the promise that two logarithmic-size unentangled registers are given to the verifier. This promise gives the verifier more leeway to check the proof and limits the prover’s ability to cheat. Therefore, this gives a new perspective on the properties of entanglement.

In parallel with our work, and independently of us, Aaronson et al. (2008) have shown that 3SAT is in $\text{QMA}_{\log(\sqrt{n}\text{polylog}(n))}$ (i.e., with $\sqrt{n}\text{polylog}(n)$ unentangled registers) with constant completeness and soundness. It seems that only two unentangled registers for the certificate are not enough to check the proof with a constant gap between completeness and soundness; we