Available online at www.sciencedirect.com

SCIENCE DIRECT®

Information and Computation 200 (2005) 1–34

Information and Computation

www.elsevier.com/locate/ic

Quantum and classical complexity classes: Separations, collapses, and closure properties ☆

Holger Spakowski [a,1], Mayur Thakur [b,2], Rahul Tripathi [c,*]

[a] *Institut für Informatik, Heinrich-Heine-Universität Düsseldorf, Düsseldorf 40225, Germany*
[b] *Department of Computer Science, University of Missouri–Rolla, Rolla, MO 65409, USA*
[c] *Department of Computer Science, University of Rochester, Rochester, NY 14627, USA*

Received 12 December 2003
Available online 10 May 2005

Abstract

We study the complexity of quantum complexity classes such as EQP, BQP, and NQP (quantum analogs of P, BPP, and NP, respectively) using classical complexity classes such as ZPP, WPP, and $C_=P$. The contributions of this paper are threefold. First, via oracle constructions, we show that no relativizable proof technique can improve the best known classical upper bound for BQP (BQP⊆AWPP [Journal of Computer and System Sciences 59(2) (1999) 240]) to BQP⊆WPP and the best known classical lower bound for EQP (P⊆EQP) to ZPP⊆EQP. Second, we prove that there are oracles A and B such that, relative to A, coRP is immune to NQP and relative to B, BQP is immune to $P^{C_=P}$. Extending a result of de Graaf and Valiant [Technical Report quant-ph/0211179, Quantum Physics (2002)], we construct a relativized world where EQP is immune to $MOD_{p^k}P$. Third, motivated by the fact that counting classes (e.g., LWPP, AWPP, etc.) are the best known classical upper bounds on quantum complexity classes, we study properties of these counting classes. We

☆ A preliminary version of this paper was presented at the 23rd Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS '03). Research supported in part by Grant NSF-INT-9815095/DAAD-315-PPP-gü-ab, a grant from the DAAD, and by DFG project RO 1202/9-1.

* Corresponding author.
E-mail addressess: spakowsk@cs.uni-duesseldorf.de (H. Spakowski), thakurk@umr.edu (M. Thakur), rahult@cs.rochester.edu (R. Tripathi).
[1] This work was done in part while visiting the University of Rochester.
[2] This work was done in part while the author was affiliated with the University of Rochester.

doi:10.1016/j.ic.2004.10.009

prove that WPP is closed under polynomial-time truth-table reductions, while we construct an oracle relative to which WPP is not closed under polynomial-time Turing reductions. The latter result implies that proving the equality of the similar appearing classes LWPP and WPP would require nonrelativizable proof techniques. We also prove that both AWPP and APP are closed under $\leqslant_T^{\mathrm{UP}}$ reductions. We use closure properties of WPP and AWPP to prove interesting consequences, in terms of the complexity of the polynomial-hierarchy, of the following hypotheses: NQP⊆BQP and EQP=NQP.

Keywords: Computational complexity; Quantum complexity classes; Gap-definable counting classes; Relativization theory; Reduction closure properties

1. Introduction

Quantum complexity classes such as EQP, BQP [8] (quantum analogs, respectively, of P and BPP [24]), and NQP [1] (quantum analog of NP) are defined using quantum Turing machines [8], the quantum analog of classical Turing machines. EQP is the class of languages L accepted by a quantum Turing machine M running in polynomial time such that, for each $x \in \Sigma^*$, if $x \in L$, then the probability that $M(x)$ accepts is 1, and if $x \notin L$, then the probability that $M(x)$ accepts is 0. BQP is the class of languages L accepted by a quantum Turing machine M running in polynomial time such that, for each $x \in \Sigma^*$, if $x \in L$, then the probability that $M(x)$ accepts is at least $2/3$, and if $x \notin L$, then the probability that $M(x)$ accepts is at most $1/3$. NQP is the class of languages L accepted by a quantum Turing machine M running in polynomial time such that, for each $x \in \Sigma^*$, $x \in L$ if and only if the probability that $M(x)$ accepts is nonzero.

Quantum complexity classes represent the computational power of quantum computers. Some fundamental computational problems—for example, factoring, discrete logarithm [42], Pell's equation, and the principal ideal problem [30]—are not believed to be in BPP, and yet have been shown to be in BQP. One of the key issues in quantum complexity theory is studying the relationship between classical and quantum complexity classes. The inclusion relationships of BQP with some natural classical complexity classes are known. Bernstein and Vazirani [8] showed that BPP $\subseteq$ BQP $\subseteq$ $\mathrm{P}^{\#\mathrm{P}}$. Adleman et al. [1] improved that to BQP $\subseteq$ PP. Fortnow and Rogers [23] showed that the investigation of counting classes can give us insights into the classical complexity of quantum complexity classes. In particular, they studied the complexity of BQP using gap-definable counting classes [19]. (See Section 2 for definitions of complexity classes not defined in this section.) Loosely speaking, gap-definable counting classes capture the power of computing via counting the gap (i.e., difference) between the number of accepting and rejecting paths in a nondeterministic polynomial-time Turing machine. Fortnow and Rogers proved that BQP $\subseteq$ AWPP, where AWPP is a gap-definable counting class. Since AWPP $\subseteq$ PP, this gives a better upper bound for BQP than that of Adleman et al. Thus, the best known lower and upper bounds for BQP in terms of classical complexity classes are, respectively, BPP and AWPP: BPP $\subseteq$ BQP $\subseteq$ AWPP $\subseteq$ PP. Similarly, the best known classical lower and upper bounds for EQP are, respectively, P and LWPP: P $\subseteq$ EQP $\subseteq$ LWPP $\subseteq$ AWPP $\subseteq$ PP. The quantum complexity class NQP coincides with $\mathrm{coC_{=}P}$ [21,54].

In light of these connections between quantum and counting complexity classes, it is natural to ask if there are counting (or other classical) complexity classes that give better lower (or upper) bounds