BQP After 28 Years

Scott Aaronson
University of Texas, Austin, TX, USA

Abstract

I will discuss the now-ancient question of where BQP, Bounded-Error Quantum Polynomial-Time, fits in among classical complexity classes. After reviewing some basics from the 90s, I will discuss the Forrelation problem that I introduced in 2009 to yield an oracle separation between BQP and PH, and the dramatic completion of that program by Ran Raz and Avishay Tal in 2018. I will then discuss very recent work, with William Kretschmer and DeVon Ingram, which leverages the Raz-Tal theorem, along with a new "quantum-aware" random restriction method, to obtain results that illustrate just how differently BQP can behave from BPP. These include oracles relative to which $\mathsf{NP}^{\mathsf{BQP}} \not\subset \mathsf{BQP}^{\mathsf{PH}}$ – solving a 2005 open problem of Lance Fortnow – and conversely, relative to which $\mathsf{BQP}^{\mathsf{NP}} \not\subset \mathsf{PH}^{\mathsf{BQP}}$; an oracle relative to which $\mathsf{P} = \mathsf{NP}$ and yet $\mathsf{BQP} \neq \mathsf{QCMA}$; an oracle relative to which $\mathsf{NP} \subseteq \mathsf{BQP}$ yet PH is infinite; an oracle relative to which $\mathsf{P} = \mathsf{NP} \neq \mathsf{BQP} = \mathsf{PP}$; and an oracle relative to which $\mathsf{PP} = \mathsf{PostBQP} \not\subset \mathsf{QMA}^{\mathsf{QMA}^{\cdots}}$. By popular demand, I will also speculate about the status of BQP in the unrelativized world.

2012 ACM Subject Classification Theory of computation → Quantum complexity theory

Keywords and phrases quantum computing, complexity theory, oracle separations, circuit lower bounds

Digital Object Identifier 10.4230/LIPIcs.FSTTCS.2021.1

Category Invited Talk

41st IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2021).
Editors: Mikołaj Bojańczyk and Chandra Chekuri; Article No. 1; pp. 1:1–1:1
Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany