EFFICIENT CLASSICAL SIMULATIONS OF QUANTUM FOURIER TRANSFORMS AND NORMALIZER CIRCUITS OVER ABELIAN GROUPS

Maarten Van den Nest
Max Planck Institute for Quantum Optics, Garching

The quantum Fourier transform (QFT) is sometimes said to be the source of various exponential quantum speed-ups. In this work we introduce a class of quantum circuits, called normalizer circuits, which cannot outperform classical computers even though the QFT constitutes an essential component. A normalizer circuit over a finite Abelian group is any quantum circuit comprising the QFT over the group, gates which compute automorphisms and gates which realize quadratic functions on the group. We prove that all normalizer circuits have polynomial-time classical simulations. The proof uses algorithms for linear diophantine equation solving and the monomial matrix formalism introduced in our earlier work. We subsequently discuss several aspects of normalizer circuits. First we show that our result generalizes the Gottesman-Knill theorem. Furthermore we highlight connections to Shor's factoring algorithm and to the Abelian hidden subgroup problem in general. Finally we prove that quantum factoring cannot be realized as a normalizer circuit owing to its modular exponentiation subroutine.