

MAR15-2015-021018

Abstract for an Invited Paper
for the MAR15 Meeting of
the American Physical Society

Hidden subgroups and hidden polynomials

MIKLOS SANTHA, CNRS, Université Paris Diderot and CQT, National University of Singapore

Efficient solutions for the abelian hidden subgroup problem (HSP) constitute probably the greatest success of quantum computing. As a sequel to these results, various generalizations of the abelian HSP have been investigated, such as the non abelian HSP, hidden symmetry problems, and hidden structures of higher degree. In this talk we review an interesting connection between the HSP in certain semidirect product p -groups of constant nilpotency class and the multi-dimensional univariate hidden polynomial graph problem when the degree of the polynomials is constant. Using that connection, we present an efficient quantum solution for both, based on a new randomized algorithm for solving systems of diagonal polynomial equations in finite fields.

Joint work with Gábor Ivanyos.