Abstract

The Hidden Subgroup Problem is one of the most important problems in the theory of quantum computing. Its aim is to find a hidden subgroup H of a given group by evaluating a hiding function that separates cosets of H.

We present an overview of the Hidden Subgroup Problem, along with some efficient quantum algorithms to solve the problem for large classes of groups. In particular, we describe an efficient algorithm for abelian groups, Kuperberg's and Regev's subexponential algorithms for the dihedral group D_N, and Goncalves' algorithm for instances of the semi-direct product group $\mathbb{Z}_N \rtimes \mathbb{Z}_{q^s}$. A reduction of the Shortest Lattice Vector Problem to the Diherdral HSP is outlined as well.

We also provide a brief introduction to the mathematical background of the quantum mechanics making quantum algorithms work.