Quantum Mastermind

André Souto

LIACC and DCC-FC, U Porto

Abstract

In this paper we give a quantum algorithm based on Grover's search algorithm to solve a generalization of the game Mastermind. Classically, the best result known states that for n positions and k colours where $n \leq k \leq n^2$ it is necessary to query $2n \log k + 4n$ times the Mastermind to determine the secret sequence used and if $k \geq n$ the number of queries necessary is $\lceil \frac{k}{n} \rceil + 2n \log n + 2n + 2$. For the case $k \leq n$ we present an algorithm that determines the secret sequence using $O(\sqrt{k})$ queries and for the case $n \leq k \leq n^2$ we describe a procedure using $O(n)$ queries to determine the secret sequence. We also give prove that the algorithms described are at most a factor of $\sqrt{n}$ away from the best lower bound achieved. Joint work with Harry Buhrman.