2021-2022

Quantum Information and Quantum Computing, Project 7

Teacher : vincenzo.savona@epfl.ch
Assistant : sara.alvesdossantos@epfl.ch, clemens.giuliani@epfl.ch, khurshed.fitter@epfl.ch

Shor's factoring algorithm

We have studied in class *Shor's factoring algorithm.*

The goal of the project is:

1. Read and understand the chapter on Shor's factoring algorithm in Nielsen & Chuang's book, and possibly on other sources, and present to a sufficient level of detail how Shor's algorithms works. Explain in particular how the algorithm relies on the order or period finding problem.

2. Devote part of your presentation to the modular exponentiation, which defines the task to be carried out by the oracle. What may be a systematic way to write a modular exponentiation circuit starting from a classical boolean circuit and using reversible computing? Starting from this result, how much room there is for improvement? You may be interested in this and this article.

3. Implement Shor's algorithm on the IBM-Q Qiskit platform (on the QASM simulator). The specific task is to implement the algorithm for factoring $N = 15$, as seen in class, and then an algorithm for factoring $N = 21$. Use modular exponentiation as introduced in the two articles cited above.

4. Study the performance of the algorithm in presence of (simulated) noise. In particular, what is the statistical error of the $N = 21$ algorithm, compared with the one for $N = 15$ algorithm? Discuss the feasibility of larger factoring tasks on current quantum hardware.