# Quantum Information and Quantum Computing, Project 6

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

## *Grover and quantum counting algorithms*

We have studied the *Grover search algorithm* in class. In particular, we have shown that one should ideally know the number of target entries in the searched database in order to apply Grover's algorithm optimally, and have discussed how this number can be estimated using the *quantum counting algorithm*.

The goal of the project is:

1. Read and understand the chapter on Grover's search algorithm in Nielsen & Chuang's book, and possibly on other sources, and present to a sufficient level of detail both Grover's and the quantum counting algorithms.
2. Devote part of your presentation to a clear analysis of the importance of Grover's search in the context of the theory of quantum computational complexity, in particular with respect to the limitations to the quantum speedup of problems in the NP complexity class.
3. Implement Grover's algorithm on the IBM-Q Qiskit platform (on the QASM simulator). The specific task is to create an oracle based on a function $f(x): \{0,1\}^n \to \{0,1\}$, where the $m$ target bitsets that the algorithm must find, are those for which $f(x) = 1$. Try to write an oracle for $m = 1$ or $m = 2$ (no matter which bitsets are the actual targets) for various values of $n$. You may use ancilla qubits and Toffoli gates, similar to Fig. 4.10 of Nielsen and Chuang. Can you write an oracle that doesn't make use of ancilla qubits?
4. Study the performance of the algorithm in the presence of (simulated) noise. In particular, when the Grover angle $\theta/2 \sim \sqrt{m/n}$ is small, you need a correspondingly large number of applications of the Grover iteration, and the Grover oracle is correspondingly deeper. With this in mind, see how large can you make $n$ before noise dominates the outcome of the algorithm.