
Quantum Information and Quantum Computing, Problem set 7

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

Problem 1 : Shor's code for factoring $N = 15$

Our goal is to implement on Qiskit the simplest instance of the period-finding code, so to factor the number $N = 15$. Assume that in step 3 of Shor's algorithm we have randomly chosen $x = 4$ among the co-prime numbers of N , i.e. such that $\gcd(x, N) = 1$.

1. Devise a quantum circuit that executes the modular exponentiation $f(z) = x^z \bmod 15$, with $x = 4$. We will assume that z is a 2-qubit number. This means that we choose $t = 2$ as the number of qubits in the first register of the quantum period finding algorithm. This assumption is justified if we expect to find a small period, which is the case here.
2. Implement on Qiskit the period-finding algorithm with the modular exponentiation code that you just found. Show that it finds a factor of $N = 15$.