Quantum Information and Quantum Computing, Problem set 7

Assistants : sara.alvesdossantos@epfl.ch, david.linteau@epfl.ch, shao.chiew@epfl.ch

Problem 1 : Shor's factoring algorithm and code

Our first 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 $\gcd(x, N) = 1$. After this simple case, you are going to design a quantum circuit for the more complex case $N = 21$.

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 $N = 15$.

3. Now do the same for $N = 21$ and $x = 11$. For this case it is difficult to devise a modular exponentiation circuit. Therefore, we will assume that modular multiplication is available as a primitive and only solve the problem on paper.

   - What is the period of $x = 11$ for $N = 21$? How many qubits t are needed in the phase register to correctly execute Shor's algorithm? How many were necessary in the case $N = 15$, $x = 4$?
   - What is the added algorithmic difficulty of this second factoring case?
   - Write the quantum circuit of Shor's algorithm for $N = 21$ and $x = 11$ using the one-qubit semiclassical QFT (the one with mid-circuit measurements). Assume that you have the controlled modular multiplication operations $c-U_{2^k}$ available as block operations. Here U_{2^k} is the permutation unitary that achieves $|y\rangle \to |yx^{2^k} \bmod N\rangle$. Notice that the U_{2^k} are permutation matrices because x and N are coprimes. Also, remember from class that to correctly define these unitaries for Shor's factoring algorithm, you have to set them to the identity for $y \geq N$.
   - Optional: If you are skilled in Qiskit, define the U_{2^k} and $c - U_{2^k}$ using the Qiskit class `qiskit.circuit.library.PermutationGate` .