Phase Estimation and Order Finding Cheatsheet

1 Phase Estimation

1.1 Task

Given: Unitary operator U, with an eigenvector $|\psi\rangle$, and eigenvalue $e^{2\pi i\phi}$
Determine: ϕ

The defining equation of an eigenvector $|\psi\rangle$ and eigenvalue $e^{2\pi i\phi}$:

$$U|\psi\rangle = e^{2\pi i\phi}|\psi\rangle$$

1.2 Algorithm

1. Create two registers: first one with t qubits and the second one with a number of qubits that can store $|\psi\rangle$;
2. Set the first register to $|0\rangle$ and the second register to $|\psi\rangle$;
3. Apply Hadamard gates to the first register;
4. Apply CU^{2j}, where $t-j$ is the control for $j = 0, ..., t-1$;
5. Apply the inverse QFT to the first register;
6. Measure the first register;

2 Order Finding

2.1 Task

Given: Positive integers x and N, where $x < N$ with no common factors
Determine: The least positive integer r such that $x^r = 1 \,(\mathrm{mod} N)$

2.2 Algorithm

1. Create two registers: first one with $t = 2L + 1\lceil \log(2 + \frac{1}{2\epsilon}) \rceil$ qubits and the second one with L qubits;
2. Set the first register to $|0\rangle$ and the second register to $|1\rangle$;
3. Apply QPE;
4. Find r from $\frac{s}{r}$ using continued fractions;