Lab 11: The Shor's Algorithm

Preliminaries

Refer to the teaching materials in Module 11.

Tasks

Run 'jupyter notebook', and create a notebook for this lab. Write your answers for all tasks into this notebook, and then convert it to pdf for submission to vUWS.

1. Suppose the two integers a and N satisfy that $a < N$ and they are co-prime. Use Python code to solve the following tasks.
   1.1 Implement a Python function that takes these two integers as parameters and prints out all the values of $f_{a,\ N}(x) = a^x \bmod N$, where x ranges from 0 to r, the period of $f_{a,\ N}(x)$. Specifically, the output should consist of $r + 1$ lines, with each line containing the value of x and the corresponding value of $f_{a,\ N}(x)$.
   1.2 Use the above function to output the result for $a = 21$ and $N = 391$.
   1.3 Let $r = f_{21,\ 391}(x)$. It should be even. Check if $21^{r/2} + 1$ is a multiple of 391.
   1.4 Calculate $\gcd(21^{\frac{r}{2}} + 1,\ 391)$ and $\gcd(21^{\frac{r}{2}} - 1,\ 391)$. Verify that the product of these two resulting numbers equals 391.
   Hint: According to Euclidean Algorithm,
   $$\gcd\left(21^{\frac{r}{2}} + 1, 391\right) = \gcd\left(21^{\frac{r}{2}}\, mod\, 391 + 1, 391\right)$$
   $$\gcd\left(21^{\frac{r}{2}} - 1, 391\right) = \gcd\left(21^{\frac{r}{2}}\, mod\, 391 - 1, 391\right)$$

2. Consider the 8×8 Vandermonde Matrix as defined in the lecture slides.
   2.1 Use manual calculation to give all entries in its second row.
   2.2 Use manual calculation to give all entries in its third row.

   Note: Each entry should be given in the form of a complex number which can contain radicals but not sin()'s and cos()'s.

3. Suppose we have a signal S, which takes the form of $\cos(\theta) + i\sin(\theta)$, with θ rotating continuously from 0 to -2π in a constant speed. Let's assume that, in a certain time interval, S rotates from 0 to -2π exactly once. Thus, S has the frequency of 1 in this time interval. To detect this frequency, we sample 16 values from this signal during that time interval. The samples happen on $\theta = 0, -\frac{\pi}{8}, \ldots, -\frac{15\pi}{8}$, with a step of $-\frac{\pi}{8}$. You should roughly follow the notebook accompanying Lecture 11 to implement a circuit with QFT to detect the frequency of the signal S by processing these sample values.

4. Follow the notebook accompanying Lecture 11 to implement a circuit with Shor class to factor the integer 21.
   4.1 Try $a = 4$ and show it's not successful. Explain this by manually following Shor's algorithm.
   4.2 Try $a = 2$ and show it's successful.