Quantum Computation 101 for Physicists

Home exercise 5

1. Show that the the dagger form of the unitary we found in class for the Fourier transform, $U_{FT}^{\dagger} = (H_3(V_{32}H_2)(V_{31}V_{21}H_1)(V_{30}V_{20}V_{10}H_0)P)^{\dagger}$, implements the inverse Fourier transform.
2. Show that Shor's algorithm is in fact phase estimation:
   (a) Find an operator U for which the operator U_f used in Shor's algorithm can be written as $U_f = \sum_j |j\rangle\langle j| \otimes U^j$, where the $|j\rangle\langle j|$ part acts on the first (input) register and the U^j part acts on the second (output) register. Hint: for the second register, choose a starting state $|y\rangle = |1\rangle_n$.

   (b) Write the eigenstates of U in terms of N, b, r. When you find the eigenstates, write them as $e^i 2\pi\phi$ and find ϕ.

   Hint: start by looking at an example where $N = 13, b = 3$ and note the U divides the Hilbert space into subspaces of size r which are not mixed under the application of U.

   (c) Once you found the relation between the eigenvalues of U and the desired result r, write Shor's algorithm as a phase estimation algorithm.

   - Change the protocol of Shor's algorithm to match reverse rather than regular Fourier transform (or in fact, show that in the specific case there is no difference).
   - Apply the phase estimation algorithm, show how to extract r out of the result and compare to Shor's algorithm steps.