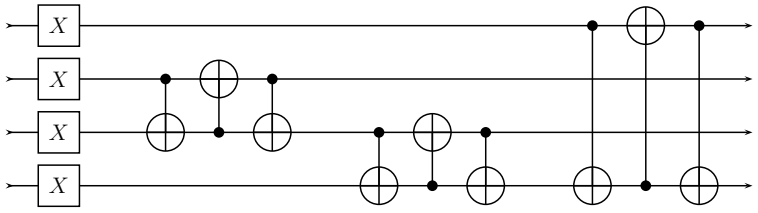
33-658 Quantum Computing and Quantum Information Homework 9

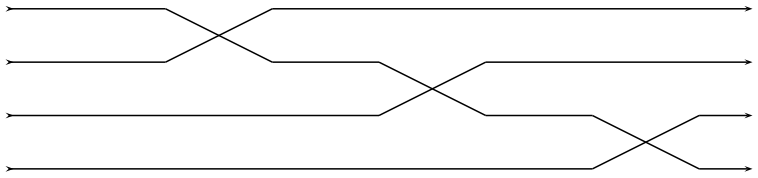
1. Read the paper "Demonstration of Shor's factoring algorithm for $N = 21$ on IBM quantum processors" by Skosana and Tame (2021). List the elements of the modular group G_{21}. Identify the subgroup generated by $a = 4$ and determine the order of a. Explain the operation of U^1, U^2, and U^4 in their circuit (Fig. 2). Run the algorithm on the IBM quantum system. Print out he histogram of states, and use it to discover the factors of N. Note that you will need to use continued fractions (see Mermin Appendix K).

2. Consider the circuit below that executes the operation $|x\rangle \rightarrow |y\rangle = |7x \ mod \ 15\rangle$.



(a) Explain how the initial `NOT` gates map $|x\rangle \rightarrow |-x \ mod \ 15\rangle$.

(b) Identify groups of three `cNOT` gates that execute swap operations. You should find three such sets that taken together execute a right-rotate as shown below. Explain that this operation generates a multiplication $|y\rangle \rightarrow |z\rangle = |8y \ mod \ 15\rangle$.



(c) The combination of *(a)* and *(b)* transforms $|x\rangle \rightarrow |-8x \ mod \ 15\rangle$. How does this relate to $|7x \ mod \ 15\rangle$?

3. Grover search

(a) Let $|\phi\rangle = (1/\sqrt{2^n}) \sum_x |x\rangle$ and let $|a\rangle$ be $|x\rangle$ for some value of x. In the Grover Search algorithm the angle between $(WV)^m|\phi\rangle$ and $|a\rangle$ varies with the number of iterations m. Does this violate unitarity (preservation of inner products)? Explain why or why not.

(b) Show that $Y = -W = (2|\phi\rangle\langle\phi| - 1)$ (with $|\phi\rangle$ as given above) acting on a state $|\psi\rangle = \sum_k \alpha_k |k\rangle$ (with k ranging over n-bit integers) yields

$$Y|\psi\rangle = \sum_k \left(-\alpha_k + 2\langle\alpha\rangle\right)|k\rangle$$

where $\langle\alpha\rangle = (1/2^n) \sum_k \alpha_k$ is the mean. Y is called inversion about the mean.