Exercise 8

1. Delayed measurement with Clifford only circuits

In general, we can consider quantum circuits with classically-controlled operations: this is when measurements are made throught the circuit, with the outcomes being used to determine what gates are subsequently applied.

Nevertheless, when reasoning about what kind of computations we can do with quantum circuits, it is simplest to consider only circuits of the form represented below.

Here all measurements are deferred to the end, and so there are no classically-controlled operations.

Remarkably, this comes with no loss of generality. This is because all classically-controlled operations (with measurement) can be replaced by fully quantum controlled gates (unitary and without measurement). For example

Any circuit with classically-controlled gates can therefore be replaced by an equivalent one with only fully quantum gates and with all measurements deferred to the end. However, the gate set required for the latter will typically need to be more powerful that the set of unitary gates used in the former.

To show this, consider circuits for which classically-control is allowed, but for which the unitary part of all gates must be Clifford. Show that, in general, the equivalent circuit without classically-controlled gates requires non-Clifford gates.

to prove if $u \in C$ $Cu \notin C$, but $Cu \in U$. Controlled gate: if measurement is 0 then $|\psi\rangle \rightarrow \frac{1}{\sqrt{N_0}} \sum_{\sigma'} c_{0\sigma'} |\sigma'\rangle$ and if measurement is 1, then $|\psi\rangle \rightarrow \frac{1}{\sqrt{N_1}} \sum_{\sigma'} c_{1\sigma'} U|\sigma'\rangle$

2. Unitarity of the order-finding operator

For integers x, N and L with $x < N \leq 2^L - 1$ and $\gcd(x, N) = 1$, consider the following operation,

$$U = \sum_{y=0}^{2^L-1} |\, f(y) \,\rangle \langle\, y \,|, \tag{1}$$

Where $f(y) = x \times y \mod N$ for $0 \leq y < N$ and $f(y) = y$ otherwise. Show that U is unitary.

3. Eigenstates of the order-finding operator

- (a) Show that the following states are eigenstates of U,

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left[\frac{-2\pi i s k}{r}\right] \left|x^k \mod N\right\rangle. \tag{2}$$

Here $0 \leq s \leq r - 1$, where r is the smallest integer such that $x^r = 1 \mod N$. Show also that the corresponding eigenvalues are $u_s = \exp(2\pi i s/r)$.

- (b) There are also many states with eigenvalue 1. What are these?