Quantum Information A Fall 2020 Final Exam

Choose **5 problems** from the 13 alternatives below to solve. Solutions are due in 12 noon on Monday Oct 26. Let me know if you find typos.

All problems except problem 7 are taken from Nielsen-Chuang, look them up from the book. You can use all available sources, but if you happen to find a solution somewhere, do not copy it without understanding every step. Note also that if two students return identical solutions, it will be noticed, and be a problem.

1. Excercise 3.29 from the book.
2. Exercise 4.36 from the book.
3. Exercise 4.41 from the book
4. Exercise 4.42 from the book.
5. Exercise 4.43 from the book.
6. Exercise 4.51 from the book.
7. **Period finding algorithm, simplified example.** If you found the discussion of the period finding algorithm a bit hard to digest in Nielsen-Chuang, you may want to consider working through this (rather straightforward) exercise. It introduces a slightly simplified version of the problem. Consider the function $f : \mathbf{Z}_N \to \mathbf{Z}_M$, where $\mathbf{Z}_N = \{0, 1, 2, \ldots, N-1\}$ with addition modulo N, where N, M are positive integers. We assume that the function satisfies the following properties:

   - f is *periodic*: there exists a positive integer r such that $f(x+r) = f(x)$
   - the period r is a factor of N: $N = nr$ for some non-negative integer n. Thus f has an integer number of periods within $\mathbf{Z}_N$. (This assumption simplifies the algorithm.)
   - f is *one-to-one*: for all pairs (x, y) such that $|x-y| < r$, $f(x) \neq f(y)$.

   We know *a priori* that r is a factor of N, but to determine it precisely we need an algorithm. We start with the discrete Fourier transformation, which we write as the map Q_N:

$$Q_N|x\rangle = \frac{1}{\sqrt{N}} \sum_{y \in \mathbf{Z}_N} \omega_N^{xy} |y\rangle \tag{1}$$

   where $x \in \mathbf{Z}_N$ labels the compuational basis, and $\omega_N \equiv e^{i2\pi/N}$. Thinking of Q_N as a matrix in the computational basis, *e.g.*

$$Q_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \; ; \; Q_3 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & e^{i2\pi/3} & e^{-i2\pi/3} \\ 1 & e^{-i2\pi/3} & e^{i2\pi/3} \end{pmatrix} \tag{2}$$

and so on. One can verify $Q_N^\dagger = Q_N^{-1}$ so that it is unitary. Now let us specify the periodicity determination algorithm. We need a black box gate Q_f that realizes the function f, and two registers, the first of dimension N and the second of dimension M. The steps are (your task is to work out some details):

- Start with the state $|0\rangle|0\rangle$
- Apply Q_N to the first register. Show that the state becomes
$$\frac{1}{\sqrt{N}} \sum_{x \in \mathbf{Z}_N} |x\rangle|0\rangle.$$
- Apply Q_f to the second register, the state becomes
$$\frac{1}{\sqrt{N}} \sum_{x \in \mathbf{Z}_N} |x\rangle|f(x)\rangle.$$
- Measure the second register. Suppose one would recieve the answer $z \in \mathbf{Z}_M$ (we make an implicit measurement, so we do not need to know the answer), with $f(x_0 + jr) = z$ for some x_0 and integers j. Then the state of the first register collapses to
$$\sqrt{\frac{r}{N}} \sum_{j=0}^{(N/r)-1} |x_0 + jr\rangle \ .$$
- Apply Q_N to the first register state (implicitely of the form above). Since r divides N, $N = nr$ for some n. Then $\omega_N^r = e^{i2\pi(r/N)} = \omega_n$. Show that the state of the first register can be written as
$$\frac{\sqrt{r}}{N} \sum_{y \in \mathbf{Z}_N} \omega^{yx_0} \left(\sum_{j=0}^{n-1} \omega_n^{jy} \right) |y\rangle \ .$$
Then, the term in the brackets is a geometric sum, for which we can use
$$\sum_{k=0}^{n-1} \omega^k = \begin{cases} \frac{1-\omega^n}{1-\omega} & \text{if } \omega \neq 1 \\ n & \text{if } \omega = 1 \end{cases}$$
and $\omega_n^{jy} = 1$ if $y \equiv 0 \ (mod\ n)$, in other words if $y = \ell n$ for some ℓ. Thus show that the state of the first register can be rewritten as
$$\frac{1}{\sqrt{r}} \sum_{\ell=0}^{r-1} \omega_N^{\ell x_0 n} |\ell n\rangle \ .$$

- In the end, we measure the first register in the computational basis. **Explain why** from the above state, we can see that the only measurement outcomes with nonvanishing uniform probability are $k \equiv \ell_0 n$ for some $\ell_0 = 0, \ldots, r-1$. We now know N, k, and

$$k = \ell_0 n = \frac{\ell_0 N}{r}\ , \text{ so } \frac{k}{N} = \frac{\ell_0}{r}\ .$$

  Recall that in the end of the day we want to know what is r. If we had luck, the measurement would have yielded an ℓ_0 such that ℓ_0 and r are mutually coprime. Then by canceling out common factors from k/N we would get ℓ_0/r from which we could read off r. What is the probability of obtaining such an ℓ_0? The following fact can be proven:

  > **Fact**. Fix a positive integer r and pick a positive integer ℓ_0 uniformly at random from the integers between 0 and r. Then the probability that ℓ_0 is coprime to r is $\Omega(1/\log\log r)$.

Thus, we keep repeating the algorithm. Every time we get k/N we cancel out common factors and get a candidate for r, which we can test by checking if $f(x+r) = f(x)$. If the test fails, we repeat the algorithm again. The above fact implies that after $O(\log\log r) = O(\log\log N)$ repetitions we have with high probability found the right period r.

Note that if we do not know from the beginning that r must be a factor of N, one of the periods of the function will be incomplete in the domain $\mathbf{Z}_N$. This leads to smearing of the probabilities around ℓ_0 and will lead us to need the continued fractions analysis, as in Nielsen-Chuang.

8. Exercise 5.4 from the book.
9. Exercise 5.5 from the book.
10. Exercise 5.9 from the book.
11. Exercise 5.18 from the book.
12. Problem 5.3 from the book.
13. Exercise 6.3 from the book.