Homework 7 8.370/18.435/2.111 Due 11/9

1. Let's look at a piece of the factoring algorithm a little more closely. As an example, let's factor 21. Suppose we use the unitary transformation which acts as:

$$U\,|y \bmod (21)\rangle = |2y \bmod (21)\rangle$$

on binary representations of the numbers between 0 and 20 (for this problem, it's irrelevant what it does outside this range).

For the factoring algorithm, recall that we start with the state $|1 \bmod (21)\rangle$, and use the phase estimation algorithm on the transformation U. If we have an eigenvector with eigenvalue $e^{2\pi i a/b}$, assume that phase estimation combined with continued fractions returns a/b in reduced fraction form with probability 1.

(a) The state $|1 \pmod{21}\rangle$ can be represented as a superposition of eigenvectors of U. What are these eigenvectors? How many of them are there? (You don't have to write them all down; but make sure the grader can tell that you know what they are.)

(b) Suppose the algorithm returns a/b, and if b is even, we compute $2^{b/2}$ and try to use it to factor. What is the probability we get the right factors this way? (If b is odd, count this as a failure.)

Solution:

There are six eigenvectors which have quantum overlap with $|1\rangle$.

We have

$$2^1 = 2, 2^2 \equiv 4, 2^3 \equiv 8, 2^4 \equiv 16, 2^5 \equiv 11, 2^6 \equiv 1 \pmod{21}.$$

Thus, the eigenvectors are

$$\begin{array}{lrrrrrr}
\frac{1}{\sqrt{6}}\big(\,|1\rangle & +e^{\pi i/3}\,|2\rangle & +e^{2\pi i/3}\,|4\rangle & -\,|8\rangle & +e^{4\pi i/3}\,|16\rangle & +e^{5\pi i/3}\,|11\rangle\,\big) \\
\frac{1}{\sqrt{6}}\big(\,|1\rangle & +e^{2\pi i/3}\,|2\rangle & +e^{4\pi i/3}\,|4\rangle & +\,|8\rangle & +e^{2\pi i/3}\,|16\rangle & +e^{4\pi i/3}\,|11\rangle\,\big) \\
\frac{1}{\sqrt{6}}\big(\,|1\rangle & -\,|2\rangle & +\,|4\rangle & -\,|8\rangle & +\,|16\rangle & -\,|11\rangle\,\big) \\
\frac{1}{\sqrt{6}}\big(\,|1\rangle & +e^{4\pi i/3}\,|2\rangle & +e^{2\pi i/3}\,|4\rangle & +\,|8\rangle & +e^{4\pi i/3}\,|16\rangle & +e^{2\pi i/3}\,|11\rangle\,\big) \\
\frac{1}{\sqrt{6}}\big(\,|1\rangle & +e^{5\pi i/3}\,|2\rangle & +e^{4\pi i/3}\,|4\rangle & -\,|8\rangle & +e^{2\pi i/3}\,|16\rangle & +e^{\pi i/3}\,|11\rangle\,\big) \\
\frac{1}{\sqrt{6}}\big(\,|1\rangle & +\,|2\rangle & +\,|4\rangle & +\,|8\rangle & +\,|16\rangle & +\,|11\rangle\,\big)
\end{array}$$

These have eigenvalues $e^{2\pi i(5/6)}$, $e^{2\pi i(2/3)}$, $e^{2\pi i(1/2)}$, $e^{2\pi i(1/3)}$, $e^{2\pi i(1/6)}$, and $e^{2\pi i(0/1)}$, respectively.

The denominator 6 gives $(2^3+1)(2^3-1) = 9 \cdot 7$, and $\gcd(9, 21) = 3$ while $\gcd(7, 21) = 7$.

The denominator 3 doesn't work because 3 is odd.

The denominator 2 gives $(2+1)(2-1)$, and you get that $\gcd(3, 21) = 3$, which is one of the factors, by coincidence—something that I didn't realize when I wrote the problem.

The denominator 1 doesn't work because 1 is odd.

So the probability that we get the right factors this way is either $1/2$ or $1/3$, depending on whether you count the case where you find a factor by coincidence. Either solution should get full credit.

2. In the last problem, we saw that even if the phase estimation and continued fractions pieces of the algorithm work perfectly, and we choose a g in $[1, N-1]$ that is relatively prime to N, use the unitary

$$U : |y \pmod{N}\rangle \rightarrow |gy \pmod{N}\rangle$$

and get the correct period r, the factoring algorithm still has some probability of failing.

(a) How bad is this problem for large N?

Note: You may need the following theorem from number theory: Euler's totient function $\phi(n)$ is the number of positive integers less than or equal to n that are relatively prime to n. For all n, $\phi(n) \geq \frac{Cn}{\ln \ln n}$ for some constant C.

Solution: If the order is r, you will get a denominator r whenever you happen to find an eigenvalue of the form ℓ/r where $\gcd(\ell, r) = 1$. And in these cases you are guaranteed to find a factor. The probability this happens is $\phi(r)/r$. And since $r < N$, this will always happen with probability at least $\frac{C}{\ln \ln N}$.

(b) Can you think of anything to do to make the factoring algorithm somewhat more efficient for large N? (Assume that quantum computation is expensive and classical computation is relatively cheap.)

Solution: Most of the time when you get a fraction ℓ/r with $\gcd(\ell, r) > 1$, $\gcd(\ell, r)$ will be fairly small. So if you end up with fraction a/b, and b doesn't give you a factor, see whether a small multiple of b, like $r = 2b$, $r = 3b$, $r = 4b$, $r = 5b$, gives you a factor.

3. (20 points)

For a prime p and two numbers a, b, with $1 < a, b < p$, consider the quantum state

$$\frac{1}{\sqrt{p}} \sum_{j=0}^{p-1} |j \pmod{p}\rangle \, |aj + b \pmod{p}\rangle$$

(a) Show that if you are given one copy of this quantum state, then with a quantum computer, you can find a with high probability (i.e., with probability going to 1 as p goes to ∞).

(b) Show that you can also find b with high probability (i.e., with probability going to 1 as p goes to ∞).

(c) Show that no quantum algorithm can identify a with probability 1.

Hint: there are two techniques that we've seen in class that you might use to attack parts (a) and (b). One is the quantum Fourier transform and the other is phase estimation. One of these techniques works substantially better than the other.

Solution: Here we apply QFT to both registers, and get

$$\begin{aligned}
&\frac{1}{p^{3/2}} \sum_{j=0}^{p-1} \left(\sum_{k=0}^{p-1} e^{2\pi i jk/p} \, |k\rangle \right) \otimes \left(\sum_{l=0}^{p-1} e^{2\pi i (aj+b)l/p} \, |l\rangle \right) \\
&= \frac{1}{p^{3/2}} \sum_{k,l}^{p-1} \left(\sum_{j=0}^{p-1} \exp\{2\pi i [jk + ajl + bl]/p\} \, |kl\rangle \right) \\
&= \frac{1}{p^{3/2}} \sum_{k,l}^{p-1} e^{2\pi i bl/p} \left(\sum_{j=0}^{p-1} \exp\{2\pi i [k + al]j/p\} \, |kl\rangle \right).
\end{aligned}$$

Note that $\sum_{j=0}^{p-1} \exp\{2\pi i [k + al]j/p\} = 0$ unless $k + al \equiv 0 \bmod p$. Therefore, if we now measure both registers, then as long as k, l are not both zero (which only happens with probability $1/p$), we will get an non-trivial equation $k + al \equiv 0 \bmod p$, from which we can obtain a with certainty.

To find b, we can reduce the problem to part (a). Consider the unitary transform that such that

$$\forall x, U|0\rangle|x\rangle = |0\rangle|x\rangle$$
$$\forall j \neq 0, x, U|j\rangle|x\rangle = \left|j^{-1}\right\rangle\left|j^{-1}x\right\rangle.$$

Here j^{-1} is the unique k such that $0 < k \leq p-1$, $jk \equiv 1 \bmod p$. We see that U is hermitian, and U is its own inverse, which means U is unitary. Now if we apply U to our state in part (a), we get the state

$$\frac{1}{\sqrt{p}}|0\rangle|b\rangle + \frac{1}{\sqrt{p}}\sum_{j=1}^{p-1}\left|j^{-1}\right\rangle\left|a + j^{-1}b\right\rangle = \frac{1}{\sqrt{p}}|0\rangle|b\rangle + \frac{1}{\sqrt{p}}\sum_{j=1}^{p-1}|j\rangle|a+jb\rangle \text{ by renaming.}$$

This is almost like the state $\frac{1}{\sqrt{p}}\sum_{j=0}^{p-1}|j\rangle|a+jb\rangle$, except that when $j=0$ we have the state $|0\rangle|b\rangle$ instead of $|0\rangle|a\rangle$. We will see that the strategy from part (a) still works with high probability, despite this caveat. Applying QFT to both registers, we have

$$\frac{1}{p^{3/2}}\left(\sum_{k=0}^{p-1}|k\rangle\right)\otimes\left(\sum_{l=0}^{p-1}e^{2\pi ibl/p}|l\rangle\right) + \frac{1}{p^{3/2}}\sum_{j=1}^{p-1}\left(\sum_{k=0}^{p-1}e^{2\pi ijk/p}|k\rangle\right)\otimes\left(\sum_{l=0}^{p-1}e^{2\pi i(a+bj)l/p}|l\rangle\right)$$
$$= \frac{1}{p^{3/2}}\sum_{k,l}^{p-1}\exp\{2\pi ibl/p\}|kl\rangle + \frac{1}{p^{3/2}}\sum_{k,l}^{p-1}\left(\sum_{j=1}^{p-1}\exp\{2\pi i[jk+al+bjl]/p\}|kl\rangle\right)$$
$$= \frac{1}{p^{3/2}}\sum_{k,l}^{p-1}\left(e^{2\pi ibl/p} + e^{2\pi ial/p}\sum_{j=1}^{p-1}\exp\{2\pi i[k+bl]j/p\}\right)|kl\rangle.$$

Note that if $k + bl \equiv 0 \bmod p$,then $\sum_{j=1}^{p-1}\exp\{2\pi i[k+al]j/p\} = p-1$; otherwise, the sum equals to -1. Therefore the above state is

$$\frac{1}{p^{3/2}}\sum_{k,l:k+bl=0}^{p-1}\left(e^{2\pi ibl/p} + e^{2\pi ial/p}(p-1)\right)|kl\rangle + \frac{1}{p^{3/2}}\sum_{k,l:k+bl\neq 0}^{p-1}\left(e^{2\pi ibl/p} + e^{2\pi ial/p}\right)|kl\rangle.$$

Since the norm of complex numbers satisfy triangular inequality, the probability that we get any particular k, l with $k + bl \equiv 0 \bmod p$ if we measure this state is

$$\geq p\frac{(p-2)^2}{p^3} \approx 1.$$

Therefore with high probability we can find b as well.

For the last part, suppose for a fixed j, we have $aj + b = a'j + b'$ for some a, a', b, b'. Then the states

$$\frac{1}{\sqrt{p}}\sum_{j=0}^{p-1}|j \pmod p\rangle|aj + b \pmod p\rangle \text{ and } \frac{1}{\sqrt{p}}\sum_{j=0}^{p-1}|j \pmod p\rangle|a'j + b' \pmod p\rangle$$

are not orthogonal, which means there is no quantum algorithms that can tell them apart with certainty.