Shor's Algorithm

as taught by Seth Lloyd, notes by Aaron Vontell
(Dated: November 15, 2016)

These are notes on the second lecture about Shor's Algorithm, as taught by Seth Lloyd in 8.370 Quantum Computation at MIT during Fall 2016. A more in-depth coverage of the material can be found at `https://en.wikipedia.org/wiki/Shors_algorithm`

I. INTRODUCTION

A. Review of Shor's Algorithm

From last time, we have a number N which is the product of primes p and q. We reduce the problem of finding p and q to the discrete logarithm problem.

We pick some X and find the smallest r such that

$$x^r \equiv 1 \bmod N$$

where r is the **order** of X mod N. This implies the following:

$$(x^{r/2}+1)(x^{r/2}-1) = bN$$

for some b. We then find the GCD of $(x^{r/2}+1), (x^{r/2}-1)$, and N, to reveal p and q with high probability.

B. Using the Quantum Computer

We can use a quantum computer to compute r. We do this with the following steps:

1. We pick an n such that $N^2 < 2^n < 2N^2$.

2. Construct the state

$$\frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} |k\rangle \otimes |X^k \bmod N\rangle$$

   using modular exponentiation, which takes $O(n^3)$, or with fancy methods, $O(n^2 \log n \log(\log n))$. This also makes use of **quantum parallelism**, which takes a superposition of states, and with one gate computes $f(x)$ for each component.

3. We now have this state where $X^k \bmod N$ is periodic with period r. We can finally compute the QFT on the first register to compute the period, and therefore obtain

$$\frac{1}{2^n} \sum_{j,k=0}^{2^n-1} e^{2\pi jk/2^n} |j\rangle \otimes |X^k \bmod N\rangle$$

4. We measure the first register, and get a value of j such that jr is (very) close to some multiple of 2^n. This is due to positive interference. This implies that $\frac{j}{2^n} \approx \frac{s}{r}$.
5. We expand $j/2^n$ and find s, r by expanding until the continued fraction converges, which is the order of x. *Note that* $r < N < 2^{n/2+1}$

HW Problem 9.1: We have that $N = 91 = 7 * 13$ and $X = 4$. a) Computer the order of $X = 4$, mod N (in other words, find he smallest r such that $4^r = 1$ mod 91. b) Show that $x^{r/2} - 1 \equiv 63$ mod 91. *Note that the GCD of 63 and 91 is 7*!

HW Problem 9.2: We have that $N = 15$, $X = 7$, and $n = 10$. We therefore have

$$\frac{1}{2^4} \sum_{k=0}^{2^10-1} |k\rangle \otimes |7^k \bmod N\rangle$$

which is equal to

$$\frac{1}{2^4}(|0\rangle\otimes|1\rangle - |1\rangle\otimes|7\rangle + |2\rangle\otimes|4\rangle + |3\rangle\otimes|13\rangle + |4\rangle\otimes|1\rangle + |5\rangle\otimes|7\rangle + ...)$$

This means that $r = 4$ from seeing the period in the second register. *We would then take the QFT of the first register to obtain some j. Suppose when you measure, you get* 768/1024 *for* $j/2^n$. Compute this using Shor's method, and then find the continued fraction for 768/1024 to show that $s = 3$ and $r = 4$.

HW Problem 9.3: Go through all of the steps of Shor's algorithm for $N = 21$. Pick an X so that the GCD of X and N is greater than 1 and not N. Go through the modular exponentiation (such that you find r). Then write down the QFT, find values of j such that $j/2^n = s/r$, and verify that the continued fraction expansion gives you r. Do it again for another value of X, finding an r even.

C. Example

Following from homework problem 9.3, what if we get that $j = 769$? Then we still get the correct answer.