Quantum Computation

oliverobrien111

July 2021

1 Lecture 1

1.1 Review of Shor's algoirthm/quantum period finding algorithm

Polynomial time hierarchy:// Computation with input of size n, and we are interested in the number of steps/gates (classical or quantum). When we say $O(poly(n))$ steps we regard this as an "efficent computation".

Shor's algorithm solves the factoring problem:
Given an integer N needing $O(logN)$ bits, we want to find a non-trival factor in $O(polyn)$ time.

The best known classical algorithm (number sieve): $e^{O(n^{\frac{1}{3}}(\log n)^{\frac{1}{3}})}$
Shor's alogrithm takes $O(n^3)$

1.1.1 Quantum factoring algorithm (summary)

1. First, convert factoring into periodicity determination. Given N, choose $a < N$ s.t. a is coprime (this is easy classically can be seen in part II lecture notes). Consider $f : \mathbb{Z} \to \mathbb{Z}_N$ $f(x) = a^x \mod N$. **Euler's Theorem**: if f is periodic with period r, then it is called 'order of $a \mod N$'.
2. In order to find r we need a quantum implementation of f. We are always workingon finite size registers so restricting $x \in \mathbb{Z}$ to $x \in \mathbb{Z}_M$ (for some large enough M): $f : \mathbb{Z}_M \to \mathbb{Z}_N$. f will no longer be exactly preriodic but this would have neglible effect if M is sufficently large e.g. $M = O(N^2)$
3. Using the classical theory of continued fractions. Define Hilbert spaces $\mathcal{H}_M \to \{|i\rangle\}_{i\in\mathbb{Z}_M}, \mathcal{H}_N \to \{|i\rangle\}_{i\in\mathbb{Z}_N}$.
4. $|x\rangle \to |f(x)\rangle$ is not generally a valid quantum operator, so we make it a unitary operation which can be implemented:

$$U_f : \mathcal{H}_M \otimes \mathcal{H}_N \to \mathbb{H}_M \otimes \mathbb{H}_N$$

$$U_f : |i\rangle |k\rangle \to |i\rangle |k + f(i)\rangle$$

5. if $x \to f(x)$ can be classically computed in $O(poly(m))$ time ($m = \log M$)), then U_f can be implemented in poly(m) time quantumly too

6. We will sometimes view U_f as a black box/oracle and we will count the number of times the algorithm invokes the oracle.

7. Back to facotoring to get r we'll use the quantum algorithm for periodicity determination:

8. Given an oracle U_f with the promise that f is periodic of some unknown period $r \in \mathbb{Z}_N$ so that $f(x + r) = f(x)$ and f is one-to-one in this period (for all $0 \leq x_1 < x_2 < r f(x_1) \neq f(x_2)$)

9. To find r in $O(polyn)$ with any persecribed success probability $1 - \epsilon$ we use the following alogirthm:

   - Step 1: Create the state
   $$\frac{1}{\sqrt{M}} \sum_{i=0}^{M-1} |i\rangle |0\rangle$$
   - Step 2: Apply U_f to get
   $$\frac{1}{\sqrt{M}} \sum_{i=0}^{M-1} |i\rangle |f(i)\rangle$$
   - Step 3: Measure the 2nd register to get y. By the born rule the first register collapses to all those i: $f(i) = y$ i.e. $i = x_0, x_0 + r, x_o + 2r, ..., x_0 + (A - 1)r$, $0 \leq x_0 < r$.

     Discard the second register to get the following state:
   $$|per\rangle = \frac{1}{\sqrt{A}} \sum_{j=0}^{A-1} |x_0 + jr\rangle$$
     If we measure $|per\rangle$ in computation basis we will get a value of one of these states $x_0 + jr$ for uniformly random j. This only gives us a random element of $\mathbb{Z}_M$ with no information about r.
   - Step 4: Apply quantum fourier transform mod M (QFT). Lets recap what QFT does:
   $$|x\rangle \to \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} \omega^{xy} |y\rangle, \forall x \in \mathbb{Z}_M, \omega = e^{2\pi i/M}$$

This can be implement in $O(m^2)$ time and gives state:

$$QFT\,|per\rangle = \frac{1}{\sqrt{MA}} \sum_{j=0}^{A-1} \sum_{y=0}^{M-1} \omega^{(x_0+jr)y}\,|y\rangle = \frac{1}{\sqrt{MA}} \sum_{y=0}^{M-1} \omega^{x_0 y} \left[\sum_{j=0}^{A-1} \omega^{jry}\,|y\rangle \right]$$

The square brackets will be:

$$\begin{cases} A & \text{if } y = KA = k\frac{M}{r}, x = 0, 1, ..., r-1 \\ 0 & \text{otherwise} \end{cases}$$

So gives final state:

$$QFT\,|per\rangle = \sqrt{\frac{A}{M}} \sum_{k=0}^{A-1} \omega^{x_0 k \frac{N}{r}}\,|k\frac{M}{r}\rangle$$

Now the random shift x_0 only appears in the phase not in the ket labels. So now the measurement probabilities will be indepedant of x_0. When we measure this we get some value $c = \frac{k_0 M}{r}$ with k_0 uniformly random in range $0 \leq k_0 < r$

$$\frac{k_0}{r} = \frac{c}{M}$$

As c and M are known, and k_0 is unknown but random in the given range. We want to find r and so we recall several classical facts.

Co-primality Theorem: The number of integers less than r that are coprime to r grows with $O(\frac{r}{\log\log r})$

Therefore, the probability of k_0 being coprime to r is $O(\frac{1}{\log\log r})$.

Lemma: If a single trial has success probability P then if one repeats it M^* times, for any $0 < 1-\epsilon < 1$. We get probability of at least one success in M^* trails is greater than $1-\epsilon$ if $M^* = \frac{-\log\epsilon}{p}$

10. From learning the period r we can use number theory to find a factor of N