Algorithm Analysis and Design (CS1.301)

Monsoon 2021, IIIT Hyderabad
13 November, Saturday (Lecture 18)

Quantum Algorithms

Shor's Algorithm

Shor's Algorithm is a method to find nontrivial divisors in polynomial time. It consists of four parts:

- reducing the divisors problem to finding a nontrivial square root of 1 modulo N (classically)
- reducing the square root problem to finding order of a number modulo N (classically)
- the order of an integer is simply the period of a particular periodic superposition
- the order-finding problem can be solved efficiently by the quantum Fourier transform or QFT

Part 1

We wish to find a nontrivial factor of N. Let us suppose that x is a nontrivial square root of 1 modulo N.

Then let $x^2 = 1 \mod N$ for some $x \notin \{\pm 1\}$, which means that $(x+1)(x-1) = kN$. This means that $x+1$ and $x-1$ have some factor in common with N, and so $\gcd(x+1, N)$ is a nontrivial factor.

Part 2

Now we choose a random x and assume that $\gcd(x, N) = 1$. If this is not true, we are done.

If r, the order of x, is even, then a nontrivial square root of 1 is $x^{\frac{r}{2}}$. Half the numbers in $\mathcal{Z}_N$ have even order.

Part 3

Let us define $f(a) = x^a \mod N$, where x is the number we chose in Part 2. Clearly, f is periodic with period r.
We can also find U_f as the transformation which takes $|x, 0\rangle$ to $|x, f(x)\rangle$. Then, we know that

$$\begin{aligned} U_f\left(\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x,0\rangle\right) &= \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}U_f\left(|x,0\rangle\right) \\ &= \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x,f(x)\rangle\,. \end{aligned}$$

Then we can compute the superposition

$$\sum_{a=0}^{M-1}\frac{1}{\sqrt{M}}\,|a,f(a)\rangle\,,$$

and measure the second register. The system will then collapse to the vectors of only those values of a with the same $f(a)$, *i.e.* the value we measured.

Now, the values of a will be periodic – if say s is the smallest value, then we will have $s, s+r, s+2r, ...$ Thus we can find the period.

Step 4

The Fourier transform of a vector

$$|\alpha\rangle = \sum_{j=0}^{\frac{M}{k}-1}\sqrt{\frac{k}{M}}\,|jk\rangle$$

is

$$|\beta\rangle = \frac{1}{\sqrt{k}}\sum_{j=0}^{k-1}\left|\frac{jM}{k}\right\rangle.$$