Shor's factoring algorithm

Dilip Paneru

Reduction to Order Finding

Classically the most difficult numbers to factor are of the form N=pq where p and q are prime numbers. This problem of factoring can be reduced to the problem of order finding,which can be seen as follows: If x is coprime to N i.e gcd(N,x) = 1, then the order of x is defined as the smallest integer r such that $x^r modN = 1$ if we find r such that $x^r modN = 1$ and r is even then, $(x^{r/2}+1)(x^{r/2}-1)$ mod N=0 and the greatest common divisors of $(x^{r/2}+1)$ and $(x^{r/2}-1)$ with N will give the prime factors.

Period Finding

If we go on evaluating $x^i modN$ for increasing values of i then we find that the values obtained recur with period r. So the problem of order finding is reduced to that of period finding. Period finding can be done in following steps:

1. First we prepare our qubits in the initial state $|0\rangle|0\rangle$ and apply Quantum Fourier Transform to obtain $\frac{1}{\sqrt{M}}\sum_{a=0}^{M-1}|a\rangle|0\rangle$
2. Then we apply the black box function that calculates $x^a modN$, to obtain $\frac{1}{\sqrt{M}}\sum_{a=0}^{M-1}|a\rangle|x^a modN\rangle$ Since the function is periodic we can write the expression as $\sqrt{\frac{r}{M}}\sum_{l=0}^{r-1}\sum_{j=0}^{\frac{M}{r}-1}|jr+l\rangle|x^l modN\rangle$
3. We then measure the second qubit set which collapses the qubits to the state $\sqrt{\frac{r}{M}}\sum_{j=0}^{\frac{M}{r}-1}|jr+l|x^{l_0} modN\rangle$ for a particular value of $l = l_0$. Measuring the first qubit would not be helpful as each time we get a different value of the function.

4. We then apply the Quantum Fourier Transform(QFT) to the first qubit set and we will be left with the superposition of states that are multiple of N/r.We can see why this is true as follows: The resulting state after QFT is $\frac{\sqrt{r}}{M}\sum_{k=0}^{M-1}\sum_{j=0}^{j=\frac{M}{r}-1} e^{\frac{2\pi ik(jr+l_0)}{M}}|k\rangle$

   $= \frac{\sqrt{r}}{M}\sum_{k=0}^{M-1} e^{\frac{2\pi il_0}{M}}\sum_{j=0}^{j=\frac{M}{r}-1} e^{\frac{2\pi ikjr}{M}}|k\rangle$

   If $k = \lambda\frac{M}{r}$ for some λ then all of the terms inside second summation become 1 and since there are $\frac{M}{r}$ of them, the amplitude of $|k\rangle$ becomes, $\frac{\sqrt{r}}{M}\frac{M}{r} = \frac{1}{\sqrt{r}}$ .Since there are r multiples of $\frac{M}{r}$ and the amplitude for each one is $\frac{1}{\sqrt{r}}$ the amplitudes for the states other than the multiples of $\frac{M}{r}$ are zero.

5. The final state therefore is $\frac{1}{\sqrt{r}}\sum_{m=0}^{r-1}|k\rangle$. To obtain the value of $\frac{M}{r}$ we repeat the process and measure the final state as many times as required and then calculate the value of r. If r is even then the prime factors are given by $\gcd(x^{r/2}-1, N)$ and $\gcd(x^{r/2}+1, N)$.

References

[1] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press,New York,2010.

[2] Philip Kaye, Raymond Laflamme and Michele Mosca. *An Introduction to Quantum Computing*. Oxford University Press,New York,2007.

[3] Umesh vazirani: Period Finding and Factoring.
`https://d37djvu3ytnwxt.cloudfront.net/assets/courseware/v1/02762cac43ea5adec`