Lecture 14

Shor's algorithm (quantum factoring algorithm)

First, let's review classical factoring algorithm (again, we will factor N=15 but pick different number)

(1) Pick any number y less than 15: y=13.
(2) Calculate $f(n)=y^n \bmod 15$ and find the period r of f(n).

n=1	13		13 mod 15 = **13**
n=2	$13^2=169$	169=15x11+4	13^2 mod 15 = **4**

n=3 shortcut: $13^3 = (15\text{x}11 + 4)\text{x}13=15\text{x}11\text{x}13+\underbrace{4\text{x}13}_{52}$

13^3 mod 15 = 52 mod 15 = **7**

n=4 From the above, we can just calculate (7x13) mod 15 = 91 mod 15 =**1**

Therefore, period r=4.

(3) Let's suppose that period is even: r=2s. Then,

$y^{2s} = 1 \bmod N$ (Remember line $n=4 \Rightarrow y^n \bmod 15 = 1$

$$y^{2s} - 1 = 0 \bmod N \qquad (N=15)$$

$$(y^s - 1)(y^s + 1) = kN$$

There fore, $\gcd(y^s \pm 1, N)$ will give factors of N.

$13^2 - 1 = 168 \qquad \gcd(168, 15) = \gcd(15, 3) = 3$

[since $168 = 15 \times 11 + 3$]

$13^2 + 1 = 170 \qquad \gcd(170, 15) = \gcd(15, 5) = 5$

[since $170 = 15 \times 11 + 5$]

$168 \cdot 170 = 1904 \times 3 \times 5$

Note that we assumed $y^s + 1 \neq 0 \bmod N$
(we know that since s is half period).

If $y^s = -1 \bmod N$ algorithm fails and we need to pick different y.

Therefore, the problem of factoring reduces to the problem of finding **<u>even</u>** periods $r=2s$ for which the term y^s+1 is not equal to 0 (mod N).

<u>The ideas of Shor's algorithm</u>

(1) Evaluate **all values** of periodic function y^n mod N **simultaneously**.

(2) **Adjust the probability amplitudes** to get a value of the period r with high probability. Note: careful with definition of which probability is considering "high". For some purposes, 1/2 is good enough. **How?** The finite Fourier transform can transform cyclic behavior of the periodic function into the enhanced probability amplitudes of some states.

Shor's algorithm for factoring N=15

(1) Chose number of qubits so $2^n \geq N$. In our case, n=4, $2^4>N$
Pick y such as gcd(y,N)=1. For example, we pick y=13.

(2) Initialize two quantum registers of n=4 qubits to state 0

$$|\psi\rangle=|0000\rangle|0000\rangle\equiv|0\rangle|0\rangle$$

four qubits each

(3) Randomize the first register, i.e. make the superposition of states with all possible four-qubit basis set states:

$$|0000\rangle \rightarrow \frac{1}{\sqrt{16}}\{|0000\rangle + |0001\rangle + |0010\rangle + \ldots + |1111\rangle\} = \sum_{k=0}^{15} \frac{1}{\sqrt{16}}|k\rangle$$

$|k\rangle$ states are labeled in the order of binary numbers.

Note on binary numbers:

Binary addition

$0+1 \rightarrow 1$
$1+0 \rightarrow 1$
$1 + 1 \rightarrow 0$, carry 1 (since $1 + 1 = 0 + 1 \times 10$ in binary)

Example:

```
  1 1 1 1 1  (carried digits)
    0 1 1 0 1
+   1 0 1 1 1
-------------
= 1 0 0 1 0 0
```

Therefore, counting in binary we get:

0	0000	8	1000
1	0001	9	1001
2	0010	10	1010
3	0011	11	1011
4	0100	12	1100
5	0101	13	1101
6	0110	14	1110
7	0111	15	1111

Class exercise: demonstrate that application of Hadamard gate to each of the four qubits in |0000> register will randomize it.

Hadamard gate: $|0\rangle \rightarrow \frac{|0\rangle + |1\rangle}{\sqrt{2}} \qquad |1\rangle \rightarrow \frac{|0\rangle - |1\rangle}{\sqrt{2}}$

One qubit $\quad |0\rangle - \boxed{H} - \frac{|0\rangle+|1\rangle}{\sqrt{2}} = \sum_{k=0}^{1} \frac{1}{\sqrt{2}} |k\rangle$

Two qubits

$$\left.\begin{array}{l} \#1 \\ |0\rangle - \boxed{H} - \frac{|0\rangle+|1\rangle}{\sqrt{2}} \\ |0\rangle - \boxed{H} - \frac{|0\rangle+|1\rangle}{\sqrt{2}} \\ \#2 \end{array}\right\} \left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right) =$$

$$= \frac{1}{\sqrt{4}} \left\{ |00\rangle + |01\rangle + |10\rangle + |11\rangle \right\} = \sum_{k=0}^{3} \frac{1}{\sqrt{4}} |k\rangle$$

2^n

Four qubits

$$\underbrace{\begin{array}{l} |0\rangle - \boxed{H} - \\ |0\rangle - \boxed{H} - \\ |0\rangle - \boxed{H} - \\ |0\rangle - \boxed{H} - \end{array}}_{H^{\otimes 4}} \left\} \frac{1}{\sqrt{16}} (|0\rangle + |1\rangle)(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)\right.$$

$$= \frac{1}{\sqrt{16}} \sum_{k=0}^{15} |k\rangle$$

|k>: |0> = |0000>
|1> = |0001>
|2> = |0010>
|3> = |0011>
:
|15>=|1111>

You can think about this step as generating numbers k=0 … 15 to calculate f(k) later.

We use these labels for our 16 basis set states of our four-qubit registers.

The combined wave function of the two registers after this step is:

$$|\psi_1\rangle = \sum_{k=0}^{15} \frac{1}{\sqrt{16}} |k\rangle|0\rangle$$

(4) Compute the function f(k) = 13^k mod (15) on the second register:

$$|\psi_2\rangle = \sum_{k=0}^{15} \frac{1}{\sqrt{16}} |k\rangle|f(k)\rangle = \frac{1}{\sqrt{16}}\left(|0\rangle|f(0)\rangle + |1\rangle|f(1)\rangle + \dots\right)$$

Here is now the function 13^k mod (15) on the second register

Class exercise: write out all 16 terms of the $|\psi_2\rangle$ wave function. Use designations |0> … |15> for both registers.

Hint: we have already calculated the function 13k mod 15 when we discussed the classical algorithm.

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
f(k)	1	13	4	7	1	13	4	7	1	13	4	7	1	13	4	7

Therefore, our state is

$$|\psi_2\rangle = \frac{1}{\sqrt{16}}\Big(|0\rangle|1\rangle + |1\rangle|13\rangle + |2\rangle|4\rangle + |3\rangle|7\rangle$$
$$+ |4\rangle|1\rangle + |5\rangle|13\rangle + |6\rangle|4\rangle + |7\rangle|7\rangle$$
$$+ |8\rangle|1\rangle + |9\rangle|13\rangle + |10\rangle|4\rangle + |11\rangle|7\rangle$$
$$+ |12\rangle|1\rangle + |13\rangle|13\rangle + |14\rangle|4\rangle + |15\rangle|7\rangle \Big)$$

Note that it is done in one operation since due to quantum parallelism we can evaluate all values of f(k) simultaneously.

(5) Operate on first four qubits by the finite Fourier transform F

$$|k\rangle \rightarrow \frac{1}{\sqrt{16}} \sum_{u=0}^{15} e^{\frac{2\pi i u k}{16}} |u\rangle$$

and measure the state of the first register.

Since there are no further operations applied to the second register, we can apply **the principle of implicit measurement** .

Principle of implicit measurement: Without loss of generality, any unterminated quantum wires (qubits which are not yet measured) at the end of the quantum circuit may be assumed to be measured.

Therefore, we can assume that the second register is measured.

Question for the class:

If we measure second register in $|\psi_2\rangle$, what possible results can we get and with what probabilities?

Our wave function is

$$\begin{aligned}|\psi_2\rangle = \frac{1}{\sqrt{16}} \big(& |0\rangle|1\rangle + |1\rangle|13\rangle + |2\rangle|4\rangle + |3\rangle|7\rangle \\ + & |4\rangle|1\rangle + |5\rangle|13\rangle + |6\rangle|4\rangle + |7\rangle|7\rangle \\ + & |8\rangle|1\rangle + |9\rangle|13\rangle + |10\rangle|4\rangle + |11\rangle|7\rangle \\ + & |12\rangle|1\rangle + |13\rangle|13\rangle + |14\rangle|4\rangle + |15\rangle|7\rangle \big).\end{aligned}$$

Therefore, we get a **random** result |1>, |13>, |4>, or |7> (all probabilities are 1/4)

Suppose we get |4>:

$$\begin{aligned}|\psi_2\rangle = \frac{1}{\sqrt{16}} \big(& |0\rangle|1\rangle + |1\rangle|13\rangle + \boxed{|2\rangle|4\rangle} + |3\rangle|7\rangle \\ + & |4\rangle|1\rangle + |5\rangle|13\rangle + \boxed{|6\rangle|4\rangle} + |7\rangle|7\rangle \\ + & |8\rangle|1\rangle + |9\rangle|13\rangle + \boxed{|10\rangle|4\rangle} + |11\rangle|7\rangle \\ + & |12\rangle|1\rangle + |13\rangle|13\rangle + \boxed{|14\rangle|4\rangle} + |15\rangle|7\rangle \big).\end{aligned}$$

superposition will collapse and only these four terms will remain

The input for quantum Fourier transform is

$$|\psi_3\rangle = \sqrt{\frac{4}{16}}\,\left(|2\rangle + |6\rangle + |10\rangle + |14\rangle\right)$$

extra $\sqrt{4}$ since function has to be normalize

$$\text{If} \quad |\psi\rangle = \alpha|00\rangle + \alpha|01\rangle + \alpha|10\rangle + \alpha|11\rangle$$

(equal probabilities) $\quad |4\alpha|^2 = 1$

We now apply quantum Fourier transform (QFT)

$$|k\rangle \rightarrow \frac{1}{\sqrt{16}} \sum_{u=0}^{15} e^{\frac{2\pi i u k}{16}} |u\rangle$$

Let's consider each of four states separately

$$|2\rangle \rightarrow \frac{1}{\sqrt{16}} \sum_{u=0}^{15} e^{\frac{2\pi i u \cdot \overset{k}{2}}{16}} |u\rangle$$

$$|6\rangle \rightarrow \frac{1}{\sqrt{16}} \sum_{u=0}^{15} e^{2\pi i u \overset{k}{6}/16} |u\rangle$$

$$|10\rangle \rightarrow \frac{1}{\sqrt{16}} \sum_{u=0}^{15} e^{2\pi i u \overset{k}{10}/16} |u\rangle$$

$$|14\rangle \rightarrow \frac{1}{\sqrt{16}} \sum_{u=0}^{15} e^{2\pi i u \overset{k}{14}/16} |u\rangle$$

Putting these four terms together, we get

$$|\psi_4\rangle = \underbrace{\sqrt{\frac{4}{16}}\frac{1}{\sqrt{16}}}_{1/8} \sum_{u=0}^{15} |u\rangle \left\{ e^{2\pi i \cdot 2/16} + e^{2\pi i u 6/16} \right.$$

$$\left. + e^{2\pi i u 10/16} + e^{2\pi i u 14/16} \right\} = \frac{1}{8} \sum_{u=0}^{15} |u\rangle A_u$$

The probability of getting result $|u\rangle$ after first register is measured is

$$P_u = \left| \frac{1}{8} A_u \right|^2$$

We use Maple to calculate P_u for all 16 cases. We get $P_0=P_4=P_8=P_{12}=1/4$ and all other probabilities being zero. Therefore, we can get only states |0>, |4>, |8>, and |12> with equal probabilities.

You can check that if we pick other results of the measurement on the second register, i.e. |1>, |13>, or |7>, we still get the same probabilities: $P_0=P_4=P_8=P_{12}=1/4$ and all other probabilities being zero.

Remember, this is the basic idea of the Shor's algorithm:
Adjust the probability amplitudes to get a value of the period r with high probability. In this case, we can prove (by writing Fourier transform sum for all states and splitting the sum into two, over single period and over period cycles) that the probabilities are non-zero only if 16 divides ur, where r is the period, meaning

$$\boxed{ur=16k}$$

SUMMARY:

The result of the Shor's algorithm is one of the states state |0>, |4>, |8>, or |12>, each with equal probability and period r is ur=16k.

So, what is the probability to get correct period from the first try?

|u>=|0> does not give you any information - rerun the algorithm

|u>=|4> gives 4r=16k, lowest k=1: Period is **r=4.**

|u>=|8> gives 8r=16k, r=2, incorrect (easily checked) - rerun the algorithm

|u>=|12> gives 12r=16k, k=3   12r=16x3: Period is **r=4.**

Therefore, the algorithm has 1/2 probability of success from the first run in this case.