Shor's algorithm

Period finding

- The goal is to factorize the number N

1. Choose a random number m

such that:
- $m < N$
- m should be coprime with N

$\Downarrow$

m and N don't have any common factor bet^n them

$g.c.d\,(m, N) = 1$

2. Find various pairs of m corresponding to N

Define function $f : N \rightarrow N$ such that

$$F_N(a) = m^a \bmod N$$

The smallest value of $a\ (= p)$ for which

$$m^p = 1 \bmod N$$

is called the period of this function.

Say $N = 21$

1. Choose $m = 2$ ✓

2.
$2^1 = 2$

$2^2 = 4$

$2^3 = 8$

$2^4 = 16 = 16 \bmod 21$

$2^5 = 32 = 11 \bmod 21$

$2^6 = 64 = 1 \bmod 21$

period = 6

We choosing $m = 2$ find the period for $N = 21$ $p = 6$

- Find the period for $N = 55$ choosing $m = 13$

$13^1 = 13$

$13^2 = 169 = 4 \bmod 55$

$13^3 = 52 \bmod 55$

$\vdots$

$13^{20} = 1 \bmod 55$

$13^1 = 13$	$13^5 = 43$	$13^9 = 28$	$13^{13} = 8$	$13^{17} = 18$
$13^2 = 4$	$13^6 = 9$	$13^{10} = 34$	$13^{14} = 49$	$13^{18} = 14$
$13^3 = 52$	$13^7 = 7$	$13^{11} = 2$	$13^{15} = 32$	$13^{19} = 17$
$13^4 = 16$	$13^8 = 26$	$13^{12} = 26$	$13^{16} = 31$	$13^{20} = 1$

Period = 20

$m^p = 1 \bmod N$

Say $x^2 = 1 \bmod N \rightarrow (1)$

case1 If N is an odd prime, then we can show that Eq. (1) has only a trivial solution

$x = \pm 1 \rightarrow (2)$

case2 If N is a composite number, then in addition to the trivial solution (2), we have a non-trivial solution

$$x = \pm a \bmod N \quad \Rightarrow \quad x = kN \pm a$$

$\rightarrow (3)$

$x^2 = 1 \bmod 41$

As 41 is odd prime $x = \pm 1$

$x^2 = 1 \bmod 55$

It has the trivial solution

$x = \pm 1$

$x = \pm 21$ (claim) is a non-trivial solution

$x^2 = 441 = 1 \bmod 440$

Because $440 = 8 \times 55$

$$x^2 = 1 \bmod 55$$

$m^P = 1 \bmod N$

choose $x = m^{P/2}$

then $m^P = 1 \bmod N$

$\Rightarrow x^2 = 1 \bmod N$

We can do it only if P is even

So one of the requirement of Shor's algorithm is that "P" has to be even.

If "P" is odd, the algorithm fails.

Then, choose a different 'm' and redo the process.

If P is even:

$$(m^{P/2} + 1)(m^{P/2} - 1) = 0 \bmod N$$

$\left(\Rightarrow (m^{P/2}+1)(m^{P/2}-1) = kN+0\right)$

$m^{P/2} - 1 \neq 0 \mod N \Rightarrow m^{P/2} = kN + 1$

$m^{P/2} + 1 = kN$

If $\boxed{(m^{P/2}+1) \neq 0 \mod N}$

Then $(m^{P/2}+1)(m^{P/2}-1) = 0 \mod N$

contains the factors of N

- P must be even
- $m^{P/2} + 1 \neq 0 \mod N$

$N = 21$

$m = 2, \quad P = 6$

$(2^3+1)(2^3-1) = 0 \mod 21$

$2^3+1 = 9$ contains 3

$2^3-1 = 7$

$N = 35, \quad m = 13$

$13^1 = 13$

$13^2 = 169 = 29 \mod 35$

$13^3 = \_\_$

$13^4 = 28561 = 35 \times 816 + 1$

$= 1 \mod 35$

$P = 4$

$(13^2 + 1)$ $(13^2 - 1)$

170 168

factors factors

Implementation of Shor's algorithm

1. Take a ℓ qubit register

ℓ should be such that

$$N^2 < 2^\ell < 2N^2 \quad / \quad 2N^2 < 2^\ell < 3N^2$$

Say $Q = 2^\ell$

2. Initialize two ℓ-qubit registers to null state

$$|\psi_0\rangle = |0\rangle \otimes |0\rangle$$

3. Prepare the first register in a uniform linear superposition of basis states $\{|0\rangle\}$ through a set of H-gates.

4. $$|\psi_1\rangle = \frac{1}{\sqrt{Q}} \sum_{x=0}^{Q-1} |x\rangle |0\rangle$$

5. choose a random number

$m < N$

6. Now apply Quantum oracle to compute

$m^a \bmod N$ and store the result in the second register

$N = 55$

$13^{20} = 1 \bmod 55$ ✓

$13^1 = 13$	$13^5 = 43$	$13^9 = 28$	$13^{13} = 8$	$13^{17} = 18$
$13^2 = 4$	$13^6 = 9$	$13^{10} = 34$	$13^{14} = 49$	$13^{18} = 14$
$13^3 = 52$	$13^7 = 7$	$13^{11} = 2$	$13^{15} = 32$	$13^{19} = 17$
$13^4 = 16$	$13^8 = 26$	$13^{12} = 26$	$13^{16} = 31$	$13^{20} = 1$

Period = 20

$m = 13$

1. choose ℓ such that

$$55^2 < 2^\ell < 2 \times 55^2$$

$$= 3025 < 2^\ell < 6050$$

$$Q = 2^{12} = 4096$$

$\Rightarrow$ Take 12 qubit register

2. $$|\psi_1\rangle = \frac{1}{\sqrt{4096}} \left[|0, 0\rangle + |1, 0\rangle + \cdots + |4095, 0\rangle \right]$$

3. choose $m = 13$

4. compute various powers of m and store the result in 2nd register

5. $$|\psi_2\rangle = \frac{1}{\sqrt{4096}} \left[|0, 1\rangle + |0, 13\rangle + |2, 13^2 = 4 \bmod 55\rangle + \cdots + |20, 13^{20} = 1 \bmod 55\rangle \right]$$

4095

$$+ \cdots + |4095, 13\rangle = 32\rangle$$

6. Now measure the second register
We will get any random value between 1 to 32

7. Say you get, after measuring the 2nd register, $\underline{\underline{9}}$ and it corresponds to 13^6

$\Rightarrow$ The first register would be in state
$6, 26, 46, 66, \cdots$

we can immediately have a rough count, we will obtain

204 states

$204 \times 20 = 4080$,

However, Total = 205 as 9 will appear once more in the remaining 16 states

$$|\psi_3\rangle = \frac{1}{\sqrt{205}} \left[|6, \underline{\underline{9}}\rangle + |26, 9\rangle + |46, 9\rangle + \cdots + |4086, 9\rangle \right]$$

$x_0 = 6$, $d = 0$, $p = 20$

$x_0 = 6$, $d = 1$, $p = 20$

In general

$$|\psi_3\rangle = \frac{1}{\sqrt{M}} \sum_{d=0}^{M-1} |x_0 + d.P, K\rangle$$

Period

msmt in the 2nd register

number of states in the 1st register corresponding to a given value of 2nd register

Starting point of the 1st register

position in the period

8. Now apply QFT on the 1st register

$$|\psi_3\rangle = \frac{1}{\sqrt{M}} \sum_{d=0}^{M-1} |x_0 + d.P, K\rangle$$

9. $|\psi_4\rangle = QFT\ |\psi_3\rangle$

$$= \frac{1}{\sqrt{Q}} \frac{1}{\sqrt{M}} \sum_{y=0}^{Q-1} \sum_{d=0}^{M-1} e^{2\pi i y (x_0 + dP)/Q} |y, K\rangle$$

$$= \frac{1}{\sqrt{QM}} \sum_{y=0}^{Q-1} e^{2\pi i y x_0/Q} \sum_{d} e^{2\pi i y dP/Q} |y, K\rangle$$

$$= \frac{1}{\sqrt{QM}} \sum_{y=0}^{Q-1} e^{2\pi i y x_0/Q} \left(\sum_{d} z^d \right) |y, K\rangle$$

where $z = e^{2\pi i y P/Q}$

The probability to get a particular value of $|y\rangle$ after measuring the 1st register is

$$\frac{1}{QM}\left|\sum_{d=0}^{M-1} z^d\right|^2$$

$$\sum_{d=0}^{M-1} z^d = \frac{1-z^M}{1-z}, \quad z = e^{2\pi i P y/Q}$$

$$\left|\sum_{d=0}^{M-1} z^d\right| = \left|\frac{\sin(\pi y PM/Q)}{\sin(\pi y P/Q)}\right|$$

The probability that we get a particular $|y\rangle$ will be:

$$P(y_i) = \frac{1}{QM}\left(\frac{\sin(\pi y_i PM/Q)}{\sin(\pi y_i P/Q)}\right)^2$$

Note that $\lim_{x\to 0} \frac{\sin^2 \alpha x}{\sin^2 x} = \alpha^2$

When, $\frac{y_i P}{Q} = n$, an integer

$\frac{yP}{Q} = n$ gives significant probability

$$P(y) = \frac{M^2}{QM} = \frac{M}{Q}$$

The probability at which y_i are most likely to come out

In our example $P(y) = \frac{205}{4096} = .05 \Rightarrow 5\%$

$$\frac{yP}{Q} = n \Rightarrow \frac{y}{Q} = \frac{n}{P}$$

This is what we want! We need to have a smart way for determining what should be the value of P corresponding to a given m, with Q known. Having known what are the values of y which are likely to be projected out, when we measure the first register we can find out P.

Continued fraction

$$\frac{17}{47} = 0 + \frac{1}{47/17} = 0 + \frac{1}{2 + \frac{13}{17}}$$

$$= 0 + \frac{1}{2 + \frac{1}{17/13}}$$

$$= 0 + \frac{1}{2 + \frac{1}{1 + \frac{4}{13}}}$$

$$= 0 + \frac{1}{2 + \frac{1}{1 + \frac{1}{3 + \frac{1}{4}}}}$$

$$\frac{17}{47} = [0, 2, 1, 3, 4]$$

$$x = [a_0, a_1, \cdots a_M]$$

Let us stop at a_j

$$x = [a_0\ a_1 \cdots a_j]$$

j^{th} convergent of x

$$\frac{y}{Q} = \frac{n}{P}$$

Express $\frac{y}{Q}$ as continued fraction and look at various convergent of it. Then approximate that fraction for which the denominator starts exceeding the original number N.

$N = 55$

$$y = 408$$

$$\frac{408}{4096} = \frac{1}{10 + \frac{2}{51}}$$

$$= \frac{1}{10 + \frac{1}{25 + \frac{1}{2}}}$$

$$\frac{408}{4096} = [0, 10, 25, 2]$$

First convergent: $\frac{1}{10}$ $\quad 10 < 55$

2nd convergent $\quad \frac{1}{10 + \frac{1}{25}} = \frac{25}{251}$

$$251 > 55$$

Stop at first convergent, i.e. at $\frac{1}{10}$

$$\frac{408}{4096} \approx \frac{n}{P} = \frac{1}{10}$$

$\Rightarrow \quad p = 10n$

Period possibilities are 10, 20, 30, 40, 50

m^p

10, 20, 30, ...

13^{10} $\quad$ 13^{20}

$13^{20} = 1 \bmod 55$

1. Factorizing 77 using Shor's algorithm

$m = 5$

$p = 30$

$l = 13$ i.e. 13 qubit register is used

$N^2 < 2^l < 2N^2$

What would be the intensity of the peak?

$$\frac{M}{Q} = \frac{Q/p}{Q} = \frac{1}{p} = \frac{1}{30}$$

$$= 0.033$$

3.3%

Factorizing

$N = 15$, choosen $m = 7$

$N^2 < 2^l < 2N^2$

Say msmt. of the 2nd register yield 7. Now apply QFT to the first register. And msmt. of the ... gives the state $|128\rangle$

first register gives ...

What is the probability of obtaining this outcome ?

$$7^1 = 7 \mod 15$$
$$7^2 = 4 \mod 15$$
$$7^3 = 13 \mod 15$$
$$7^4 = 1 \mod 15$$

period $P = 4$

$$\frac{1}{P} = \frac{1}{4} = 0.25$$