Shor’s Algorithm

DK Lee, Derek Dang

Steps of Algorithm

1. Take in an input N.
2. Verify that N != p^k, for some prime p, constant k.
3. Choose a random number a from $1 < a < N$. Verify that $gcd(a, N) = 1$.
4. If $gcd = 1$, use an algorithm to find the period r of the certain sequence.
5. If r is odd, or $a^{r/2} = -1 mod N$, pick another a.
6. Find the $gcd(a^{r/2} \pm 1, N)$.
7. Return factor.

How to find the period

- Classical:
  - List out values of x from 0 to 100 (assuming we find a period before then).
  - Use formula:

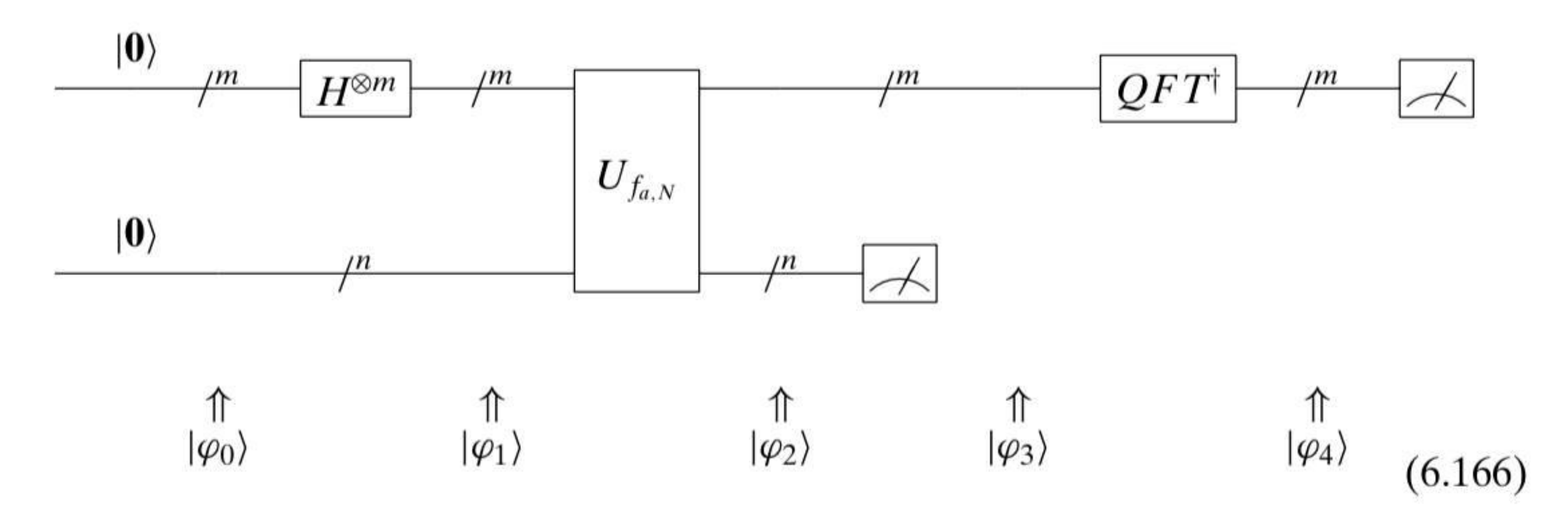
$$f_{a,N}(x) = a^x mod N.$$

  - Look for repeating values. If there is a repeat, the x at that value is the period.

How to find the period

- Quantum
  - Use the dagger of the QFT (or DFT) and multiply it to the superposition of all the measured values ($|\boldsymbol{\varphi}_3\rangle$).
  - Measure the resulting vector and get a value.
  - Use the formula: value = $\lambda * 2^m/r$ and solve for r.

How to find the period



Let’s get a sample of our efforts before our discovery.

$p = 15$ $a = 7$ $n = 4$ $r = 4$

$m = 2n$

$= 4(2) = 8$

x	7^{2x}
0	1
1	7
2	4
3	13
4	1

$r = 4$

7

1

forward → 7

256

128

256/4

$2^8 = 256$

$(w^1)^0$

(w^1)

$(w^{255})^2$

$(w^{255})^{255}$

$2^8 = 256$

64

64

0

$(w^2)^0 + (w^6)^0 \ldots$

$(w^2)^{64} + (w^6)^{64} \ldots$

$= -1 - 1 - 1 \ldots$

2

w^{32} — w^{128}_{-1} $(w^2$ $-w^2$

head_p

struct element

head_p struct element

temp → ele

temp → poi

struct element (

element ;

struct element (* point ;

return

measure $|\varphi_2\rangle$ and get 5:

$|\varphi_2\rangle = [0\ 1\ 0\ 1\ \ldots\ 1\ 0\ 1\ \ldots]$

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ \vdots & \omega & \omega^2 & & \ldots & \omega^{63} \\ \vdots & (\omega^2) & (\omega^2)^2 & & \ldots & (\omega^{2})^{63} \\ \vdots & & & & & \\ & \omega^{63} & & & \ldots & (\omega^{63})^{63} \end{bmatrix} \begin{bmatrix} \cdot \\ \vdots \\ \cdot \\ \vdots \\ \vdots \end{bmatrix} = \begin{bmatrix} 32 \\ 0 \\ \\ 0 \\ \vdots \end{bmatrix}$$

$\cancel{\omega^1} + \cancel{\omega^3} + \cancel{\omega^5} + \omega^7 + \omega^9 + \ldots$
$\cancel{\omega^{33}} + \cancel{\omega^{35}} + \cancel{\omega^{37}} + \ldots\ \omega^{63}$

$\cancel{\omega^2} + \cancel{\omega^6} + \cancel{\omega^{10}} + \cancel{\omega^{14}} + \cancel{\omega^{18}} + \cancel{\omega^{22}} + \cancel{\omega^{26}} + \cancel{\omega^{30}}$
$\cancel{\omega^{34}} + \cancel{\omega^{38}}\ \ \omega^{42}\ \ \cancel{\omega^{46}} + \ldots + \cancel{\omega^{62}} + \cancel{\omega^{66}} + \omega^{70} + \omega^{32}$
$+ \omega^{64}$

rd $\to 1\ \ \omega^{32}\ \ (\omega^{32})^2\ \ (\omega^{32})^3\ \ldots\ \ (\omega^{32})^{63}$

$\omega^{32} + (\omega^{32})^3 + (\omega^{32})^5 + (\omega^{32})^7 + \ldots + (\omega^{32})^{63}$
$-1 - 1 - 1 - 1 - 1 - 1 - 1 \ldots = -32$

$$\begin{array}{c} \\ \\ \\ 32^{\text{nd}} \to \\ \\ \\ \end{array} \begin{bmatrix} 32 \\ 0 \\ 0 \\ 0 \\ \vdots \\ -32 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

No offset : period is $32 = \frac{2^m}{r} = \frac{2^6}{2} = \boxed{32}$ as

expected.

$|\chi_4\rangle$ = has only nonzero entries only at nonzero multiples of

$\frac{2^m}{r} : \lambda \cdot \frac{2^m}{r}$.

$= \frac{1}{\sqrt{2}} \left[1\ 0 \ldots\ 0\ -1\ 0 \ldots\ 0 \right]$