Shor's algorithm

Dilhan Manawadu

June 23, 2023

Science and Technology Facilities Council
Hartree Centre

Factoring large numbers

- A prime number is a natural number greater than 1 that is divisible by only 1 and itself.
- By multiplying two prime numbers, we can generate composite numbers with two prime factors. For example $21 = 3 \times 7$.
- Given a large composite number, can one devise an algorithm to find its prime factors?
- Shor's algorithm is a quantum algorithm proposed to solve this problem.

Factoring large numbers

- The periodic function $f(x)$ is defined by

$$f(x) = a^x \mod N \tag{1}$$

  where $\mod N$ stands for division modulo N. For example,

$$11 = 3 \mod 4$$

  since $11 \div 4$ returns 3 as the remainder.
- The period of function $f(x)$ is defined as the smallest non-zero integer r such that $f(r) = a^r \mod N = 1$.
- A unique $r > 0$ exists as long as $a < N$, and a and N do not have common factors, i.e., $\gcd(a, N) = 1$

Shor's unitary operator

- Let's define the operator U by

$$U|y\rangle = |ay \mod N\rangle \tag{2}$$

- For example, U for the periodic function $f(x) = 7^x \mod 15$ is given by,

$$U|y\rangle = |7y \mod 15\rangle$$

- Starting with $y = 1$, we get

$$\begin{aligned} U|1\rangle &= |7 \mod 15\rangle = |7\rangle \\ U^2|1\rangle &= U|7\rangle = |49 \mod 15\rangle = |4\rangle \\ U^3|1\rangle &= U|4\rangle = |28 \mod 15\rangle = |13\rangle \\ U^4|1\rangle &= U|13\rangle = |91 \mod 7\rangle = |1\rangle \end{aligned}$$

- Since $U^4|1\rangle = |1\rangle$, U is a unitary operator.
- $\{|7\rangle, |4\rangle, |13\rangle, |1\rangle\}$ forms a basis for U.

Eigenstates of U

- Let's define as $|u_0\rangle$ the state created by symmetric superposition of these basis states.

$$
\begin{aligned}
|u_0\rangle &= \frac{1}{2}\left(|1\rangle + |7\rangle + |4\rangle + |13\rangle\right) \\
U|u_0\rangle &= \frac{1}{2}\left(U|1\rangle + U|7\rangle + U|4\rangle + U|13\rangle\right) \\
U|u_0\rangle &= \frac{1}{2}\left(|7\rangle + |4\rangle + |13\rangle + |1\rangle\right) \\
U|u_0\rangle &= |u_0\rangle
\end{aligned}
$$

$|u_0\rangle$ is an eigenstate of operator U.

Eigenstates of U

- Any state $|u_s\rangle$ defined for $s < r$ by

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left\{\left(-\frac{2\pi i s k}{r}\right)\right\} U^k |1\rangle \tag{3}$$

  is an eigenstate of the operator U,

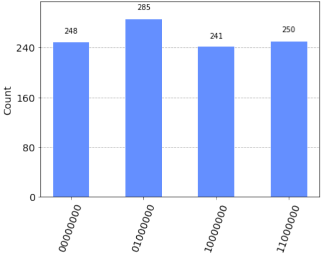
$$U|u_s\rangle = \exp\left\{\left(\frac{2\pi i s}{r}\right)\right\}|u_s\rangle \tag{4}$$

- If we can prepare the state $|u_s\rangle$ on a quantum computer, we can approximate the value of r using the quantum phase estimation (QPE) algorithm.
- We cannot prepare the state $|u_s\rangle$ without knowing r!

Initial state for QPE

- If we sum over states $|u_s\rangle$ for values $0 \leq s < r$, the phases cancel to give
$$\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |u_s\rangle = |1\rangle \tag{5}$$
- Therefore we can use the easy-to-prepare state $|1\rangle$ as the initial target state for QPE.
- As $|1\rangle$ is a symmetric superposition of states $|u_s\rangle$, QPE will measure a phase $\phi = \frac{s}{r}$ where s will be a random integer between 0 and $r-1$ drawn from a uniform distribution.

Example : Finding r of $a^r \mod 15$ using QPE



Register Output (binary)	Decimal	Phase	Fraction
00000000	0	$\frac{0}{256} = 0.00$	0
01000000	64	$\frac{64}{256} = 0.25$	1/**4**
10000000	128	$\frac{128}{256} = 0.50$	1/2
11000000	192	$\frac{192}{256} = 0.75$	3/**4**

- We find the correct period $r = 4$ with 50% accuracy.
- This is a consequence of using $|1\rangle$ instead of $|u_s\rangle$ to initialise the target registry.

Factoring

- Since $r = 4$ is even, we can write

$$\begin{aligned} a^r \mod N &= 1 \\ a^r - 1 &= xN \\ (a^{r/2} - 1)(a^{r/2} + 1) &= xN \end{aligned}$$

- we can see that $a^{r/2} \pm 1$ is highly likely to share a factor with N.
- Therefore, we can guess the greatest common dividers of these two integers with N to be a factor of N.
- If r is odd, we choose a different value for a and perform QPE until an even r is found.