Shor's factoring algorithm: quantum Fourier transform

Yipeng Huang

Rutgers University

October 13, 2021

Table of contents

The classical part: converting factoring to order finding / period finding

General strategy for the classical part

1. Factoring
2. Modular square root
3. Discrete logarithm
4. Order finding
5. Period finding

The fact that a quantum algorithm can support all these primitives leads to additional ways that future quantum computing can be useful / threatening to existing cryptography.

Order finding

Our discrete log problem is equivalent to order finding.

	$a^1 \mod 15$	$a^2 \mod 15$	$a^3 \mod 15$	$a^4 \mod 15$
a=2	2	4	8	1
a=4	4	1	4	1
a=7	7	4	13	1
a=8	8	4	2	1
a=11	11	1	11	1
a=13	13	4	7	1
a=14	14	1	14	1

Find smallest r such that $a^r \equiv 1 \mod N$

Period finding

In other words, the problem by now can also be phrased as finding the period of a function.

$$f(x) = f(x+r)$$

Where

$$f(x) = a^x = a^{x+r} \mod N$$

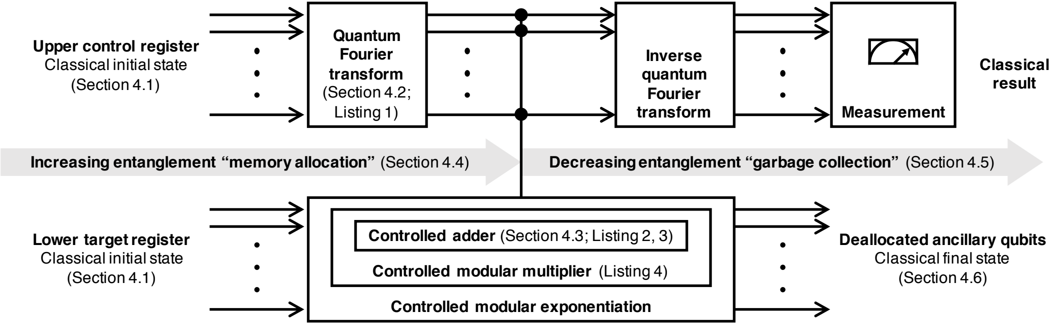
Find r.

Table of contents

The quantum part: period finding using quantum Fourier transform

- After picking a value for a, use quantum parallelism to calculate modular exponentiation: $a^x \mod N$ for all $0 \leq x \leq 2^n - 1$ simultaneously.
- Use interference to find a global property, such as the period r.

Calculate modular exponentiation



- Image source: Huang and Martonosi, Statistical assertions for validating patterns and finding bugs in quantum programs, 2019.
- A good source on how to build the controlled adder, controlled multiplier, and controlled exponentiation is in Beauregard, Circuit for Shor's algorithm using 2n+3 qubits, 2002.

Calculate modular exponentiation

- State after applying modular exponentiation circuit is

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle |f(x)\rangle$$

- Concretely, using our running example of $N = 15$, need $n = 4$ qubits to encode, and suppose we picked $a = 2$, the state would be

$$\frac{1}{4} \sum_{x=0}^{15} |x\rangle |2^x \mod 15\rangle$$

Measurement of target (bottom, ancillary) qubit register

- We then measure the target qubit register, collapsing it to a definite value. The state of the upper register would then be limited to:

$$\frac{1}{\sqrt{A}}\sum_{a=0}^{A-1}|x_0 + ar\rangle$$

- Concretely, using our running example of $N = 15$, and suppose we picked $a = 2$, and suppose measurement results in 2, the upper register would be a uniform superposition of all $|x\rangle$ such that $2^x \equiv 2 \mod 15$:

$$\frac{|1\rangle}{2} + \frac{|5\rangle}{2} + \frac{|9\rangle}{2} + \frac{|13\rangle}{2}$$

- The key trick now is can we extract the period $r = 4$ from such a quantum state. We do this using the quantum Fourier transform.

Quantum Fourier transform to obtain period

The task now is to use Fourier transform to obtain the period.

$$QFT\left(|x\rangle\right) = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{\frac{2\pi i}{2^n}xy} |y\rangle$$

$$QFT = \frac{1}{\sqrt{2^n}} \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{2^n-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(2^n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{2^n-1} & \omega^{2(2^n-1)} & \cdots & \omega^{(2^n-1)(2^n-1)} \end{bmatrix}$$

Where

$$\omega = e^{\frac{2\pi i}{2^n}}$$

And recall that

$$e^{ix} = \cos x + i \sin x$$

Quantum Fourier transform to obtain period

The task now is to use Fourier transform to obtain the period.

$$QFT\Big(|x\rangle\Big) = \frac{1}{\sqrt{2^n}}\sum_{y=0}^{2^n-1} e^{\frac{2\pi i}{2^n}xy}\,|y\rangle$$

$$\begin{aligned}
&QFT\left(\frac{1}{\sqrt{A}}\sum_{a=0}^{A-1}|x_0+ar\rangle\right) \\
&= \frac{1}{\sqrt{2^n}}\sum_{y=0}^{2^n-1}\left(\frac{1}{\sqrt{A}}\sum_{a=0}^{A-1} e^{\frac{2\pi i}{2^n}(x_0+ar)y}\right)|y\rangle \\
&= \sum_{y=0}^{2^n-1}\left(\frac{1}{\sqrt{2^n A}} e^{\frac{2\pi i}{2^n}x_0 y}\sum_{a=0}^{A-1} e^{\frac{2\pi i}{2^n}ary}\right)|y\rangle
\end{aligned}$$

Quantum Fourier transform to obtain period

$$\mathrm{Prob}(y) = \frac{A}{2^n}\left|\frac{1}{A}e^{\frac{2\pi i}{2^n}x_0 y}\sum_{a=0}^{A-1} e^{\frac{2\pi i}{2^n}ary}\right|^2$$
$$= \frac{A}{2^n}\left|\frac{1}{A}\sum_{a=0}^{A-1} e^{\frac{2\pi i}{2^n}ary}\right|^2$$

- Here, values of y such that $\frac{ry}{2^n}$ is close to an integer will have maximal measurement probability.
- In our case, only $\frac{ry}{2^n} = \frac{4 \cdot 4}{16}$, $|y\rangle = |4\rangle$ will have high measurement probability.
- To get a beautiful explanation of principle of least action, read Feynman, QED.

How to construct the Quantum Fourier transform

- Cost of computing the FFT for functions encoded in n bits: $O(2^n n)$
- Cost of quantum Fourier transform for functions encoded in n qubits: $O(n^2)$ gates.

$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & \exp \frac{2\pi i}{2^k} \end{bmatrix}$$

1. $$R_0 = \begin{bmatrix} 1 & 0 \\ 0 & \exp \frac{2\pi i}{2^0} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$
2. $$R_1 = \begin{bmatrix} 1 & 0 \\ 0 & \exp \frac{2\pi i}{2^1} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = Z$$
3. $$R_2 = \begin{bmatrix} 1 & 0 \\ 0 & \exp \frac{2\pi i}{2^2} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} = S$$
4. $$R_3 = \begin{bmatrix} 1 & 0 \\ 0 & \exp \frac{2\pi i}{2^3} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & \frac{\sqrt{2}}{2} + \frac{\sqrt{2}i}{2} \end{bmatrix} = T$$