CS 506: Introduction to Quantum Computing

Determining Periodicity of Functions - Quantum Algorithm

Professor: Bhaskar DasGupta
Scribe: Sanjay Kalaivanan

Lecture Date: October 22, 2025

1 Problem Setup

1.1 Given Function

We have a function $f(x) = f(x + r)$ for all x, which implies the existence of a smallest possible period r.

1.2 Key Observations

- Input x is an n-bit integer: $0 \leq x \leq x^n - 1$
- Value $f(x)$ is an n-bit integer: $0 \leq f(x) \leq x^n - 1$
- $f(x)$ is computable in polynomial time (only in n)
- Period r is also an n-bit integer: $0 \leq r \leq N - 1$

1.3 Notation

$$2^n = N \tag{1}$$

$$n = \log_2 N \tag{2}$$

2 Example: Computing Periodicity

Let $n = 3$, so $N = 2^3 = 8$.

Define: $f(x) = x \bmod 2$

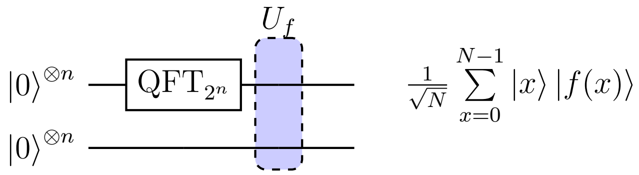
2.1 Computing Function Values

$$\begin{aligned}
x &= (000)_2 = 0 &\Rightarrow\quad & f(0) = 0 \bmod 2 = 0\\
x &= (001)_2 = 1 &\Rightarrow\quad & f(1) = 1 \bmod 2 = 1\\
x &= (010)_2 = 2 &\Rightarrow\quad & f(2) = 2 \bmod 2 = 0\\
x &= (011)_2 = 3 &\Rightarrow\quad & f(3) = 3 \bmod 2 = 1\\
x &= (100)_2 = 4 &\Rightarrow\quad & f(4) = 4 \bmod 2 = 0\\
x &= (101)_2 = 5 &\Rightarrow\quad & f(5) = 5 \bmod 2 = 1\\
x &= (110)_2 = 6 &\Rightarrow\quad & f(6) = 6 \bmod 2 = 0\\
x &= (111)_2 = 7 &\Rightarrow\quad & f(7) = 7 \bmod 2 = 1
\end{aligned}$$

Result: Periodicity $r = 2$ (pattern repeats every 2 values)

3 Quantum Algorithm Approach

3.1 Circuit Diagram



After QFT on first register:

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$$

Final Output:

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle\, |f(x)\rangle$$

$\uparrow$

Observe!

3.2 Quantum Oracle Action

Starting with $|0\rangle$ states, after applying QFT on the first register:

Top register: $\frac{1}{\sqrt{N}} \sum\limits_{x=0}^{N-1} |x\rangle$
Bottom register: $|0\rangle$
After applying U_f:

$$U_f \left(\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \right) |0\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle\, |f(x)\rangle \tag{3}$$

This gives us:

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \, |f(x)\rangle \tag{4}$$

Observe: This creates a superposition over all input-output pairs.

3.3 Example Computation

For the state $|\psi\rangle$ with $N = 8$:

$$\begin{aligned} |\psi\rangle = \frac{1}{\sqrt{8}} \Big(& |0\rangle |f(0)\rangle + |1\rangle |f(1)\rangle + |2\rangle |f(2)\rangle + |3\rangle |f(3)\rangle \\ & + |4\rangle |f(4)\rangle + |5\rangle |f(5)\rangle + |6\rangle |f(6)\rangle + |7\rangle |f(7)\rangle \Big) \end{aligned} \tag{5}$$

Substituting the computed function values:

$$= \frac{1}{\sqrt{8}} \Big[\big(|0\rangle + |2\rangle + |4\rangle + |6\rangle \big) |f(0)\rangle + \big(|1\rangle + |3\rangle + |5\rangle + |7\rangle \big) |f(1)\rangle \Big] \tag{6}$$

Thus we observe either:

$$\frac{1}{2} \big(|0\rangle + |2\rangle + |4\rangle + |6\rangle \big) |f(0)\rangle \tag{7}$$

or

$$\frac{1}{2} \big(|1\rangle + |3\rangle + |5\rangle + |7\rangle \big) |f(1)\rangle \tag{8}$$

Therefore: $m = \frac{8}{2} = 4$

4 General Analysis

4.1 Pattern Recognition

We can write the states in terms of a starting value x_0 and period r:

$$\begin{aligned} f(0) &= x_0 \\ |0\rangle &= x_0 \\ |2\rangle &= x_0 + r \\ |3\rangle &= x_0 + r \\ |4\rangle &= x_0 + 2r \\ |6\rangle &= x_0 + 3r \\ |5\rangle &= x_0 + 2r \\ |7\rangle &= x_0 + 3r \end{aligned}$$

for some $x_0 \in \{0, 1, 2, \ldots, N-1\}$.

4.2 General Superposition Form

The general state can be written as:

$$\frac{1}{\sqrt{m}} \sum_{z=0}^{m-1} |x_0 + zr\rangle \, |f(x_0)\rangle \tag{9}$$

where

$$m = \left\lfloor \frac{N}{r} \right\rfloor \tag{10}$$

Expanding this superposition:

$$= \frac{1}{\sqrt{m}} \big(|x_0\rangle + |x_0 + r\rangle + |x_0 + 2r\rangle + \cdots + |x_0 + (m-1)r\rangle \big) \, |f(x_0)\rangle \tag{11}$$

Ignoring the second register:

$$= \frac{1}{\sqrt{m}} \sum_{z=0}^{m-1} |x_0 + zr\rangle \tag{12}$$

$$= \frac{1}{\sqrt{m}} \big(|x_0\rangle + |x_0 + r\rangle + |x_0 + 2r\rangle + \cdots + |x_0 + (m-1)r\rangle \big) \tag{13}$$

Goal: Now, the problem is to find r.

4.3 Connection to Simon's Problem

Simon's problem uses a similar state:

$$\frac{1}{\sqrt{x}} \big(|x_0\rangle + |x_0 \oplus s\rangle \big) \, |f(x_0)\rangle \tag{14}$$

4.4 Easy Case: Perfect Division

If $\frac{2^n}{r}$ is an integer, then:

$$\frac{2^n}{r} = m \tag{15}$$

$$N = 2^n = mr \tag{16}$$

$$m = \frac{N}{r} \tag{17}$$

$$Nm = m^2 r \tag{18}$$

5 Applying Quantum Fourier Transform

5.1 QFT Application

Starting from:

$$|\psi\rangle = \frac{1}{\sqrt{m}} \sum_{z=0}^{m-1} |x_0 + zr\rangle \tag{19}$$

Apply QFT_{2^n}:

$$|\psi_1\rangle = \mathrm{QFT}_{2^n} |\psi\rangle = \mathrm{QFT}_{2^n} \left(\frac{1}{\sqrt{m}} \sum_{z=0}^{m-1} |x_0 + zr\rangle \right) \tag{20}$$

$$= \frac{1}{\sqrt{m}} \sum_{z=0}^{m-1} \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i (x_0+zr)\frac{y}{2^n}} |y\rangle \tag{21}$$

Rearranging:

$$|\psi_1\rangle = \sum_{y=0}^{2^n-1} \frac{1}{\sqrt{2^n m}} \left(\sum_{z=0}^{m-1} e^{2\pi i (x_0+zr)\frac{y}{2^n}} \right) |y\rangle \tag{22}$$

6 Measurement and Probability Analysis

6.1 Measurement Outcome

Upon measurement, we observe $|y_0\rangle$ for some value $y_0 \in \{0, 1, \ldots, 2^n - 1\}$ with probability:

$$P(y_0) = \left| \frac{1}{\sqrt{2^n m}} \sum_{z=0}^{m-1} e^{2\pi i (x_0+zr)\frac{y_0}{2^n}} \right|^2 \tag{23}$$

$$= \frac{1}{2^n m} \left| \sum_{z=0}^{m-1} e^{2\pi i (x_0+zr)\frac{y_0}{2^n}} \right|^2 \quad \boxed{1} \tag{24}$$

6.2 Simplification

Factor out the x_0 dependence:

$$\left| e^{2\pi i \frac{x_0 y_0}{2^n}} \sum_{z=0}^{m-1} e^{2\pi i \frac{zry_0}{2^n}} \right|^2 \tag{25}$$

Since $|e^{i\alpha}|^2 = 1$:

$$= \left| e^{2\pi i \frac{x_0 y_0}{2^n}} \right|^2 \cdot \left| \sum_{z=0}^{m-1} e^{2\pi i \frac{zry_0}{2^n}} \right|^2 = \left| \sum_{z=0}^{m-1} e^{2\pi i z \frac{ry_0}{2^n}} \right|^2 \tag{26}$$

Since $2^n = mr$ (in the easy case):

$$= \left| \sum_{z=0}^{m-1} e^{2\pi i z \frac{y_0}{m}} \right|^2 \tag{27}$$

Therefore, from $\boxed{1}$:

$$P(y_0) = \frac{1}{2^n m} \left| \sum_{z=0}^{m-1} e^{2\pi i z \frac{y_0}{m}} \right|^2 \tag{28}$$

7 Case Analysis

7.1 Case 1: $y_0 = Km$ for integer K

When $y_0 = Km$ where $K \in \{0, 1, 2, \ldots, r-1\}$:

$$P(Km) = \frac{1}{r}\left|\frac{1}{m}\sum_{z=0}^{m-1} e^{2\pi i z K m/m}\right|^2 = \frac{1}{r}\left|\frac{1}{m}\sum_{z=0}^{m-1} 1\right|^2 \tag{29}$$

$$= \frac{1}{r} \cdot \frac{m}{m} = \frac{1}{r} \tag{30}$$

Result: Each of the values $0, m, 2m, \ldots, (r-1)m$ is observed with probability $\frac{1}{r}$.
Total probability: $r \times \frac{1}{r} = 1$
Conclusion: The probability of observing any other value is 0.