An Application of QPE: Order-Finding

Renato Neves

Universidade do Minho

HASLab
HIGH-ASSURANCE
SOFTWARE LABORATORY

Table of Contents

The Problem

A periodic function f. Find its period.

Period-Finding

The Problem

A periodic function f. Find its period.

Problem can be difficult (particularly if f has no obvious structure, such as being trigonometric)

We will see how quantum computation tackles it

Order-Finding

Actually we tackle only a specific case $\Rightarrow$ order-finding

The latter is handled efficiently via QPE

Integer factorisation reduces to it

The only quantum component in Shor's algorithm

Table of Contents

A Handful of Definitions

Definition

We call the integer x a divisor of the integer y if $k \cdot x = y$ for some integer k

Examples

2 is a divisor of 10 and 5 is a divisor of 15. What are the divisors of a prime number?

Definition

For two integers x and y, $gcd(x, y)$ is the greatest divisor common to x and y

Examples

$gcd(8, 12) = 4$ and $gcd(10, 15) = 5$

A Handful of Definitions pt. II

Definition

Two integers x and y are called co-prime if $gcd(x, y) = 1$

Examples

8 and 9 are co-prime and 13 and 15 are co-prime as well. The integers 12 and 15 are not co-prime.

Modular Arithmetic

Definition

Given an integer N the set of integers mod N is $\{0, 1, \ldots, N-1\}$

We can think of this set as a circular circuit with different positions and where the position after $N-1$ is 0

Definition

For two integers x and y we write $x \equiv y \pmod{N}$ if $x \bmod N = y$

Examples

$5 \equiv 0 \pmod{5}$ and $6 \equiv 1 \pmod{5}$

Order-Finding

Definition

For co-prime integers $a < N$ the order of $a \pmod N$ is the smallest integer $r > 0$ s.t. $a^r \equiv 1 \pmod N$

Example

If $N = 5$ the sequence $3^0, 3^1, 3^2, 3^3, 3^4, 3^5, 3^6, \ldots$ leads to the sequence $1, 3, 4, 2, 1, 3, 4, \ldots$

Order of $3 \pmod 5$ is thus 4

Exercise

What is the order of $2 \pmod{11}$?

Table of Contents

Order-Finding

The Problem

Co-prime integers $a < N$

What is the order of $a \pmod{N}$?

Order-Finding

The Problem

Co-prime integers $a < N$

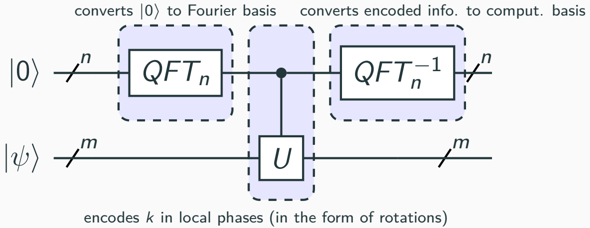
What is the order of $a \pmod N$?

Classically, problem can be difficult for large integers

Quantumly, it can be solved efficiently via QPE

QPE Revisited

Recall the QPE circuit



Need to choose suitable U and $|\psi\rangle$ to disclose the order

Table of Contents

Choosing the Right Unitary

Take co-prime integers $a < N$

Let $m = \lceil \log_2 N \rceil$ and define $U : \mathbb{C}^{2^m} \to \mathbb{C}^{2^m}$

$$U\,|x\rangle = \begin{cases} |xa \pmod N\rangle & \text{if } 0 \le x \le N-1 \\ |x\rangle & \text{otherwise} \end{cases}$$

Exercise

Show that $U\,|a^n \pmod N\rangle = |a^{n+1} \pmod N\rangle$

Choosing the Right Unitary

Take co-prime integers $a < N$

Let $m = \lceil \log_2 N \rceil$ and define $U : \mathbb{C}^{2^m} \to \mathbb{C}^{2^m}$

$$U\,|x\rangle = \begin{cases} |xa \pmod N\rangle & \text{if } 0 \leq x \leq N-1 \\ |x\rangle & \text{otherwise} \end{cases}$$

Exercise

Show that $U\,|a^n \pmod N\rangle = |a^{n+1} \pmod N\rangle$

Next step is to identify suitable eigenvectors

Starting with an Example

Recall: if $N = 5$ sequence $3^0, 3^1, 3^2, 3^3, 3^4, 3^5, 3^6, \ldots$ leads to $\underline{1, 3, 4, 2}, 1, 3, 4, \ldots$

Order r of $3 \pmod 5$ is 4. We then calculate,

$$
\begin{aligned}
&U\Big(\tfrac{1}{\sqrt{r}}(|1\rangle + |3\rangle + |4\rangle + |2\rangle\Big) \\
&= U\Big(\tfrac{1}{\sqrt{r}}\textstyle\sum_{i=0}^{r-1} \left|3^i \pmod 5\right\rangle\Big) \\
&= \tfrac{1}{\sqrt{r}}\textstyle\sum_{i=0}^{r-1} \left|3^{i+1} \pmod 5\right\rangle \\
&= \tfrac{1}{\sqrt{r}}\Big(|3\rangle + |4\rangle + |2\rangle + |1\rangle\Big) \\
&= \tfrac{1}{\sqrt{r}}\Big(|1\rangle + |3\rangle + |4\rangle + |2\rangle\Big)
\end{aligned}
$$

The latter state is therefore an eigenvector of U

A First Approach

Previous example alludes to the equation

$$U\Big(\frac{1}{\sqrt{r}}\sum_{i=0}^{r-1}\left|a^i \pmod N\right\rangle\Big) = \frac{1}{\sqrt{r}}\sum_{i=0}^{r-1}\left|a^i \pmod N\right\rangle$$

Unfortunately, corresponding eigenvalue is $1 = e^{i2\pi 0\frac{1}{2^n}}$

It does not disclose any information about the period r :(

A First Approach

Previous example alludes to the equation

$$U\Big(\tfrac{1}{\sqrt{r}}\textstyle\sum_{i=0}^{r-1}\left|a^i \pmod N\right\rangle\Big) = \tfrac{1}{\sqrt{r}}\textstyle\sum_{i=0}^{r-1}\left|a^i \pmod N\right\rangle$$

Unfortunately, corresponding eigenvalue is $1 = e^{i2\pi 0 \frac{1}{2^n}}$

It does not disclose any information about the period r :(

Need to find eigenvectors with more informative eigenvalues

A Second Approach

Let $\omega = e^{i2\pi\cdot\frac{1}{r}}$ $\underbrace{\text{(division of the unit circle in } r \text{ slices)}}_{\text{a.k.a. the r roots of unity}}$

$$
\begin{aligned}
& U\Big(\tfrac{1}{\sqrt{r}}\textstyle\sum_{i=0}^{r-1}\omega^{-i}\,\left|a^i \pmod N\right\rangle\Big) \\
&= \tfrac{1}{\sqrt{r}}\textstyle\sum_{i=0}^{r-1}\omega^{-i}\,\left|a^{i+1} \pmod N\right\rangle \\
&= \tfrac{1}{\sqrt{r}}\textstyle\sum_{i=0}^{r-1}\omega\omega^{-(i+1)}\,\left|a^{i+1} \pmod N\right\rangle \\
&= \omega\left(\tfrac{1}{\sqrt{r}}\textstyle\sum_{i=0}^{r-1}\omega^{-(i+1)}\,\left|a^{i+1} \pmod N\right\rangle\right) \\
&= \omega\left(\tfrac{1}{\sqrt{r}}\textstyle\sum_{i=0}^{r-1}\omega^{-i}\,\left|a^{i} \pmod N\right\rangle\right)
\end{aligned}
$$

Exercise

Formally justify all the steps in the calculation above

A Second Approach

Let $\omega = e^{i2\pi \cdot \frac{1}{r}}$ and $|\psi_1\rangle = \frac{1}{\sqrt{r}} \sum_{i=0}^{r-1} \omega^{-i} \left| a^i \pmod N \right\rangle$

Previous slide says $U |\psi_1\rangle = \omega |\psi_1\rangle$

So if we feed QPE with U and $|\psi_1\rangle$ we obtain an approximation of $\frac{1}{r}$ with good success probability ($\geq \frac{4}{\pi^2} \approx 0.4$)

A Second Approach

Let $\omega = e^{i2\pi \cdot \frac{1}{r}}$ and $|\psi_1\rangle = \frac{1}{\sqrt{r}} \sum_{i=0}^{r-1} \omega^{-i} \left| a^i \pmod{N} \right\rangle$

Previous slide says $U |\psi_1\rangle = \omega |\psi_1\rangle$

So if we feed QPE with U and $|\psi_1\rangle$ we obtain an approximation of $\frac{1}{r}$ with good success probability ($\geq \frac{4}{\pi^2} \approx 0.4$)

However $|\psi_1\rangle$ is difficult to construct. Can you see why?

A Third Approach

We define a superposition of eigenvectors that is equal to $|1\rangle$:

set $|\psi_k\rangle = \frac{1}{\sqrt{r}} \sum_{i=0}^{r-1} \omega^{-ik} \left| a^i \pmod{N} \right\rangle$ and $|\psi\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |\psi_k\rangle$

Exercise

Then show $U |\psi_k\rangle = \omega^k |\psi_k\rangle$

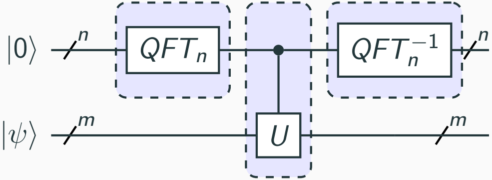
Exercise

Finally show $|\psi\rangle = |1\rangle$ (hint: show $\langle 1|\psi\rangle = 1$ or alternatively use the closed-form formula of geometric series)

A Third Approach

$U|\psi_k\rangle = \omega^k|\psi_k\rangle = e^{i2\pi\frac{k}{r}}|\psi_k\rangle$ and $|\psi\rangle = \frac{1}{\sqrt{r}}\sum_{i=0}^{r-1}|\psi_k\rangle$. Therefore

converts $|0\rangle$ to Fourier basis   converts encoded info. to comput. basis

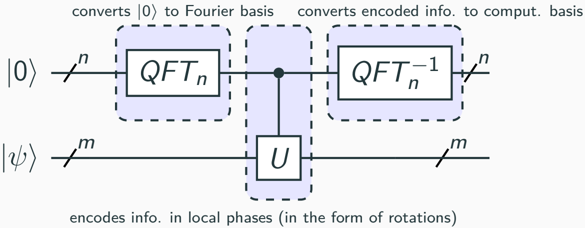


encodes info. in local phases (in the form of rotations)

returns $\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}\left(\left|\tilde{\phi}_k\right\rangle|\psi_k\rangle\right)$ where each $\left|\tilde{\phi}_k\right\rangle$ is the best n-bit approximation of $\frac{k}{r}$ with probability $\geq \frac{4}{\pi^2}$

A Third Approach

$U\,|\psi_k\rangle = \omega^k\,|\psi_k\rangle = e^{i2\pi\frac{k}{r}}\,|\psi_k\rangle$ and $|\psi\rangle = \frac{1}{\sqrt{r}}\sum_{i=0}^{r-1}|\psi_k\rangle$. Therefore



returns $\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}\left(\left|\tilde{\phi}_k\right\rangle|\psi_k\rangle\right)$ where each $\left|\tilde{\phi}_k\right\rangle$ is the best n-bit approximation of $\frac{k}{r}$ with probability $\geq \frac{4}{\pi^2}$

But how to extract r from $\left|\tilde{\phi}_k\right\rangle$?

Extracting the Period

Let φ be the best n-bit approximation of some $\frac{k}{r}$

Theorem

If $\left|\frac{k}{r} - \varphi\right| \leq \frac{1}{2r^2}$ then we can extract $\frac{k}{r}$ in reduced form, and with complexity $O(m^3)$

Proof.

Uses the continued fractions alg. (see Appendix 4, Nielsen and Chuang, *Quantum Computation and Quantum Information*) $\square$

Previous theorem tells we need to use a minimum number n of qubits to represent φ. Particularly,

Extracting the Period

recall: $m = \lceil log_2 N \rceil$

$$2^{n+1} \geq 2r^2$$
$$\Leftarrow 2^{n+1} \geq 2(2^m)^2 \qquad \{r \leq N \leq 2^m\}$$
$$\Leftarrow 22^n \geq 2(2^m)^2$$
$$\Leftarrow 2^n \geq 2^{2m}$$
$$\Leftarrow n \geq 2m$$

Thus the number of qubits to use in the approximation φ should be at least $2m$

Finally...

In order to obtain the order r, proceed with the following steps

1. run QPE + continued fractions alg. twice to obtain two reduced fractions $\frac{k_1}{r_1}$ and $\frac{k_2}{r_2}$
2. if $gcd(k_1, k_2) = 1$ repeat previous step else set $r :=$ least common multiple of r_1 and r_2
3. if $a^r \pmod N \equiv 1$ output r else go back to step 1

Finally...

In order to obtain the order r, proceed with the following steps

1. run QPE + continued fractions alg. twice to obtain two reduced fractions $\frac{k_1}{r_1}$ and $\frac{k_2}{r_2}$
2. if $gcd(k_1, k_2) = 1$ repeat previous step else set $r :=$ least common multiple of r_1 and r_2
3. if $a^r \pmod{N} \equiv 1$ output r else go back to step 1

In step 2, probability of $gcd(k_1, k_2) = 1$ is $\geq \frac{1}{4}$. Hence whole algorithm has constant probability of success

In step 2, computation of gcd and least common multiple has complexity $O(m^2)$. Hence the whole algorithm must be efficient