Introduction to Quantum Computing (Lecture 6)

Gerardo Pelosi, Alessandro Barenghi

Dipartimento di Elettronica, Informazione e Bioingegneria - DEIB
Politecnico di Milano

March 23th, 2022

Outline

Quantum Algorithms with superpolynomial speedup

Quantum Phase Estimation

To introduce the idea of phase estimation we note/remark that a n-qubit Hadamard gate applied to a n-qubit computational basis state $x \in \{0,1\}^n$, $\mathtt{H}^{\otimes n} |x\rangle_n$ allows to encode the same information, i.e., x, in the relative phases between the basis states $|00\cdots 0\rangle$ and $|11\cdots 1\rangle$, as follows:

$$\mathtt{H}^{\otimes n} |x\rangle_n = \left(\frac{1}{\sqrt{2}}|0\rangle_1 + \frac{(-1)^x}{\sqrt{2}}|1\rangle_1\right) \otimes \cdots \otimes \left(\frac{1}{\sqrt{2}}|0\rangle_1 + \frac{(-1)^x}{\sqrt{2}}|1\rangle_1\right) =$$

$$= \frac{1}{\sqrt{2^n}} \sum_{z=0}^{2^n-1} (-1)^{x \circ z} |z\rangle_n = \frac{1}{\sqrt{2^n}} \sum_{z \in \{0,1\}^n} (-1)^{x \circ z} |z\rangle_n$$

A second application of the $\mathtt{H}^{\otimes n}$ gate can be thought of as decoding the information carried out in the relative phases of the state $\mathtt{H}^{\otimes n} |x\rangle_n$ into the integer value x (i.e., $|x\rangle_n = \mathtt{H}^{\otimes n}(\mathtt{H}^{\otimes n} |x\rangle_n)$).

can be expressed as a phase factor

- Obs: $(-1)^{x \circ z} = e^{2\pi i \omega} = \left(e^{2\pi i (\frac{x \circ z}{2})}\right)$, with $\omega = \frac{x \circ z}{2} = \pm\frac{1}{2}$, thus the $\mathtt{H}^{\otimes n}$ gate does not allow to decode information encoded in more general ways into the relative phases of a basis state.

Quantum Phase Estimation Problem

Definition

Given the following particular quantum state

$$|\varphi\rangle_n = \frac{1}{\sqrt{2^n}} \sum_{z=0}^{2^n-1} e^{2\pi i\,\omega z} |z\rangle_n\,, \quad \omega \in (0,1) \cap \mathbb{R}$$

find a good estimate of the phase parameter ω

Encoding of the information in ω

since $\omega \in (0,1)$, its (fixed point) binary expansion is:

$$\omega = 0.x_1 x_2 x_3 \cdots x_t \cdots = x_1 2^{-1} + x_2 2^{-2} + x_3 2^{-3} + \cdots + x_t 2^{-t} + \cdots$$

whilst the (fixed point) binary expansion of a power-of-2 multiple of ω is:

$$2^t\,\omega = x_1 x_2 x_3 \cdots x_t . x_{t+1} x_{t+2} x_{t+3} \cdots$$

Quantum Phase Estimation Problem

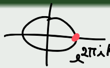
Definition

Given the following particular quantum state

$$|\varphi\rangle_n = \frac{1}{\sqrt{2^n}} \sum_{z=0}^{2^n-1} e^{2\pi i\, \omega z} |z\rangle_n \,, \quad \omega \in (0,1) \cap \mathbb{R}$$

find a good estimate of the phase parameter ω

Encoding of the information in ω

since $e^{2\pi\ i\ k} = 1$ when $k \in \mathbb{Z}$, $\Rightarrow$  $e^{2\pi i k},\ k \in \mathbb{Z}$

$$e^{2\pi\, i\, (2^t\, \omega)} = \underbrace{e^{2\pi\, i\, x_1 x_2 x_3 \cdots x_t}}_{=1} e^{2\pi\, i\, 0.x_{t+1} x_{t+2} x_{t+3} \cdots} = e^{2\pi\, i\, 0.x_{t+1} x_{t+2} x_{t+3} \cdots}$$

Quantum Phase Estimation Problem

Notable identity

The following particular t-qubit quantum state

We are interested on the first t bits of ω.

Finding

$$|\varphi\rangle_t = \frac{1}{\sqrt{2^t}} \sum_{z=0}^{2^t-1} e^{2\pi i\,\omega z}\,|z\rangle_t\,, \quad \omega \in (0,1),\ \omega = 0.x_1 x_2 \cdots x_t x_{t+1} x_{t+2} x_{t+3} \cdots$$

can be re-written highlighting the first t fractional digits of ω via the tensor product of the following t 1-qubit factors:

No

shouldn't it be

$x_1 x_2 \ldots x_{t-1} x_t \cdots$?

$$|\varphi\rangle_t = \frac{|0\rangle + e^{2\pi i\,(2^{t-1}\omega)}\,|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2\pi i\,(2^{t-2}\omega)}\,|1\rangle}{\sqrt{2}} \otimes \cdots \otimes \frac{|0\rangle + e^{2\pi i\,(2^{0}\omega)}\,|1\rangle}{\sqrt{2}} =$$

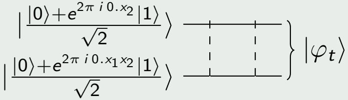
$$= \frac{|0\rangle + e^{2\pi i\,0.x_t x_{t+1}\cdots}\,|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2\pi i\,0.x_{t-1} x_t x_{t+1}\cdots}\,|1\rangle}{\sqrt{2}} \otimes \cdots \otimes \frac{|0\rangle + e^{2\pi i\,0.x_1 x_2 \cdots x_{t-1} x_t x_{t+1}\cdots}\,|1\rangle}{\sqrt{2}}$$

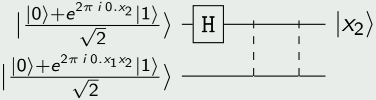
Proof. (... by induction)

Quantum Phase Estimation Problem

A 2-qubit example with $\omega = 0.x_1x_2$ → we want to measure x1 and x2.

$$|\varphi_t\rangle = \frac{1}{\sqrt{2^2}} \sum_{z=0}^{2^2-1} e^{2\pi i\, \omega z}\, |z\rangle_2 = \frac{|0\rangle + e^{2\pi\, i\, 0.x_2}\, |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2\pi\, i\, 0.x_1x_2}\, |1\rangle}{\sqrt{2}}$$





Being the state un-entangled

- the application of a H gate on the leftmost/topmost qubit allows to derive a state coinciding with $|x_2\rangle$. Indeed, $\frac{|0\rangle+e^{2\pi\, i\, 0.x_2}|1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \sum_{z=0}^{1} e^{2\pi\, i\, \frac{x_2}{2} z}\, |z\rangle = \frac{1}{\sqrt{2}} \sum_{z=0}^{1} (-1)^{x_2 z}\, |z\rangle = \mathtt{H}\, |x_2\rangle$
- to determine x_1, we note that if $x_2 = 0$ then it is possible to apply an H gate and get also $|x_1\rangle$ (as we did for x_2). If $x_2 = 1$ we need to do something else...

Quantum Phase Estimation Problem

1-qubit (unitary) phase rotation operator w.r.t. the computational basis

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

↳ Rotation phase operator (gate)

$$R_k^{-1} = \begin{bmatrix} 1 & 0 \\ 0 & e^{-\frac{2\pi\, i}{2^k}} \end{bmatrix} = R_k^{\dagger}$$

$R_k\,|0\rangle = |0\rangle$

$R_k\,|1\rangle = e^{\frac{2\pi\, i}{2^k}}\,|1\rangle = e^{2\pi\, i\, 0.00\cdots0\underbrace{1}_{k\text{th bit}}}|1\rangle$

↳ only the k^{th} bit is $=1$

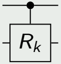
the k-th (fractional) binary digit is equal to 1.

Note: $R_0 = \mathrm{Z}$

$R_k^{-1}\,|0\rangle = |0\rangle$

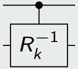
$R_k^{-1}\,|1\rangle = e^{-\frac{2\pi\, i}{2^k}}\,|1\rangle = e^{-2\pi\, i\, 0.00\cdots01}\,|1\rangle$

Controlled-R_k, Controlled-R_k^{-1} gates



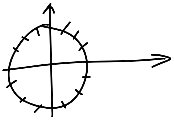
$R_k\,|00\rangle = |00\rangle,\ R_k\,|01\rangle = |01\rangle$

$R_k\,|10\rangle = |10\rangle,\ R_k\,|11\rangle = e^{\frac{2\pi\, i}{2^k}}\,|11\rangle$



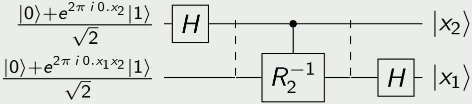
$R_k^{-1}\,|00\rangle = |00\rangle,\ R_k^{-1}\,|01\rangle = |01\rangle$

$R_k^{-1}\,|10\rangle = |10\rangle,\ R_k^{-1}\,|11\rangle = e^{-\frac{2\pi\, i}{2^k}}\,|11\rangle$



A 2-qubit example with $\omega = 0.x_1x_2$

$$\frac{1}{\sqrt{2^2}}\sum_{z=0}^{2^2-1} e^{2\pi i\,\omega z}\,|z\rangle_2$$



when it is $=1$

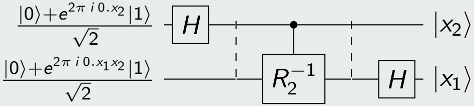
If $x_2 = 1$, the application on $\frac{|0\rangle+e^{2\pi\, i\, 0.x_1x_2}|1\rangle}{\sqrt{2}}$ of R_2^{-1} and then H yields $|x_1\rangle$:

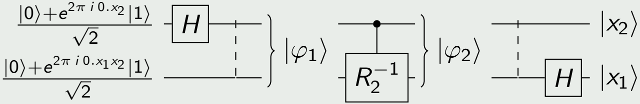
Here we are subtracting the contribution of x_2, in order to be able to isolate the term of x_1 and measure it.

$$\mathrm{H}\left(R_2^{-1}\left(\frac{|0\rangle + e^{2\pi\, i\, 0.x_1x_2}\,|1\rangle}{\sqrt{2}}\right)\right) = \mathrm{H}\left(\frac{|0\rangle + e^{2\pi\, i\,(0.x_1 1 - 0.01)}\,|1\rangle}{\sqrt{2}}\right) = \mathrm{H}\left(\frac{|0\rangle + e^{2\pi\, i\, 0.x_1}\,|1\rangle}{\sqrt{2}}\right) = |x_1\rangle$$

A 2-qubit example with $\omega = 0.x_1x_2$

$$\frac{1}{\sqrt{2^2}} \sum_{z=0}^{2^2-1} e^{2\pi i\,\omega z}\,|z\rangle_2$$





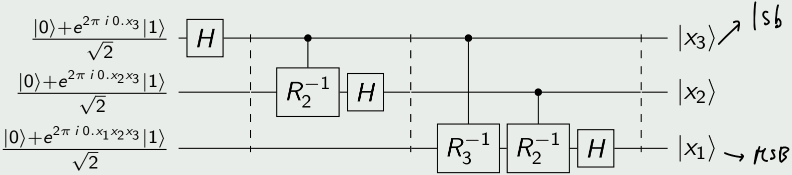
$$|\varphi_1\rangle = |x_2\rangle\left(\frac{|0\rangle + e^{2\pi\, i\, 0.x_1x_2}\,|1\rangle}{\sqrt{2}}\right), \quad |\varphi_2\rangle = |x_2\rangle\left(\frac{|0\rangle + e^{2\pi\, i\, 0.x_1}\,|1\rangle}{\sqrt{2}}\right)$$

Obs: a controlled-R_2^{-1} or a controlled-R_2 is symmetric w.r.t. swapping the control and target bits (...when doing phase estimation it is convenient to think of it as being a controlled phase shift.

Quantum Phase Estimation Problem

A 3-qubit example with $\omega = 0.x_1x_2x_3$

$$\frac{1}{\sqrt{2^3}} \sum_{z=0}^{2^3-1} e^{2\pi i\, \omega z}\, |z\rangle_3$$

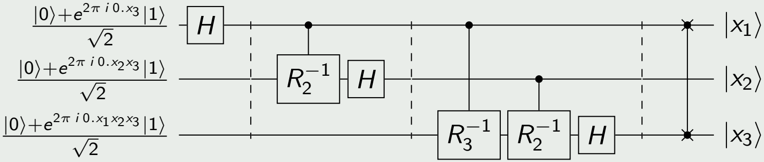


But we want $x_1x_2x_3$

- the classic bit-string in the output state $|x_3x_2x_1\rangle$ when reflected and multiplied by $\frac{1}{2^t}$ equals the binary notation of the positive integer x such that $\omega = \frac{x}{2^t}$ (e.g., with $t = 3$, $\omega = 1/4 + 1/8 = 0.011_{\texttt{bin}} = \frac{3}{8}$, the output register is $|110\rangle$).
- To assess the cost of a t-qubit circuit, consider: H; $R_2^{-1}(H)$; $R_3^{-1}(R_2^{-1}H)$; $R_4^{-1}(R_3^{-1}R_2^{-1}H)$ … $R_t^{-1}(R_{t-1}^{-1} \cdots R_2^{-1}H) \Rightarrow \frac{t(t+1)}{2} \approx t^2$ gates are needed, with a maximum depth of the circuit $= t$.

Example with $\omega = 0.x_1x_2x_3 = \frac{x}{2^3}$, $\quad 0 \leq x < 2^3,\ x = (x_1x_2x_3)_{\texttt{bin}},\quad |x\rangle = |x_1x_2x_3\rangle$

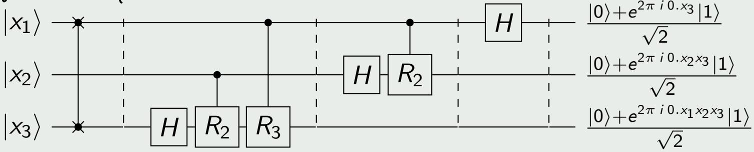
$$\frac{1}{\sqrt{2^3}}\sum_{z=0}^{2^3-1} e^{2\pi i \frac{x}{2^3} z}\,|z\rangle_3 \mapsto |x\rangle_3$$



Inverse QFT (QFT^{-1})

It allows to encode a classical state into a quantum one (?)

$$|x\rangle_3 \mapsto \frac{1}{\sqrt{2^3}}\sum_{z=0}^{2^3-1} e^{-2\pi i \frac{x}{2^3} z}\,|z\rangle_3$$



Quantum Fourier Transform ($\texttt{QFT}$)

information in the relative phases of the output are equivalent to $\frac{x}{2^3}$

Quantum Fourier Transform

$\mathtt{QFT}$ acting on one out of 2^n (computational) basis states

$$\mathtt{QFT}_{2^n} : |x\rangle_n \mapsto \frac{1}{\sqrt{2^n}} \sum_{z=0}^{2^n-1} e^{-2\pi i \frac{x}{2^n} z} |z\rangle_n$$

- it is just the reverse of the circuit employed to solve the phase estimation problem (...when the number of basis states is a power of 2). It is a unitary operator: (see previous slide) $\mathtt{QFT}^\dagger_{2^n}\mathtt{QFT}_{2^n} = \mathtt{I}^{\otimes \mathrm{n}}$ because all the bits are zero → All the R_K gates subtract null contribution of $0.0...x_K$
- Obs: $\mathtt{QFT}_{2^n} |0\rangle_n = \frac{1}{\sqrt{2^n}} \sum_{z=0}^{2^n-1} |z\rangle = \mathtt{H}^{\otimes n} |0\rangle_n$ (seeing the previous circuit, if the controlled gates have no effect, the only active gates are the $\mathtt{H}$ gates)

$\mathtt{QFT}^{-1}$ acting on one out of 2^n (computational) basis states

$$\mathtt{QFT}^{-1}_{2^n} : |x\rangle_n \mapsto \frac{1}{\sqrt{2^n}} \sum_{z=0}^{2^n-1} e^{2\pi i \frac{x}{2^n} z} |z\rangle_n$$

Phase estimation circuit

Error analysis for estimating arbitrary phases via $\texttt{QFT}^{-1}$

↳ How good is the estimation of ω by using n qbits?

Theorem

Let $\tilde{\omega} = \frac{\tilde{x}}{2^n} = 0.x_1 x_2 \cdots x_n$ be some fixed number.
The phase estimation algorithm ($\texttt{QFT}^{-1}_{2^n}$) applied to the input state $|\psi\rangle_n = \frac{1}{\sqrt{2^n}} \sum_{z=0}^{2^n-1} e^{2\pi i \omega z} |z\rangle_n$, outputs the integer $\tilde{x}$ such that $\left|\frac{\tilde{x}}{2^n} - \omega\right| < \frac{1}{2^{n+1}}$, with probability $\geq \frac{4}{\pi^2} \approx 40.5\%$. ⇒ An acceptable approximation of $|\psi\rangle_n$ occurs with probability ≃ 40%

↳ Approximation of the real quantum state $|\psi\rangle_n$

Obs: The probability 40.5% refers to the collection of n exact fractional digits of $\tilde{\omega}$.

Performing the measurement over $n + \Delta$ qubits ($\Delta > 1$) will give you a probability of observing a measurement of the first n-bits with the correct (rounded) bit values, which is equal to:

$$1 - \frac{2}{2^\Delta} + \frac{2}{2^\Delta}\left(\frac{4}{\pi^2}\right)$$

E.g., with $\Delta = 2$, $Pr \geq 70\%$

Periodic States

we have
m qubits and
m·r possible computational basis states

A periodic superimposition of states

The following state of $u = \lceil \log_2(mr+1) \rceil$ qubits obtained as the superimposition of m particular computational states

$$|\phi_{r,b}\rangle_u = \frac{1}{\sqrt{m}} \sum_{z=0}^{m-1} |zr+b\rangle_u, \quad b \in \{0, 1, \ldots, r-1\}$$

is said to be periodic with period r, shift b, and m repetitions. Obs: $|\,|\phi_{r,b}\rangle_u|^2 = m \cdot |\frac{1}{\sqrt{m}}|^2 = 1$

$$|\phi_{r,b}\rangle_u = \frac{1}{\sqrt{m}} \Big(|b\rangle_u + |r+b\rangle_u + |2r+b\rangle_u + \cdots + |(m-1)r+b\rangle_u \Big)$$

- If we measure $|\phi_{r,b}\rangle_u$ in the computational basis, we get $zr+b$ for some $z \in \{0, \ldots, (m-1)\}$ chosen uniformly at random and since also $b \in \{0, 1, \ldots, r-1\}$ is chosen in a uniformly random fashion, the probability of the measurement producing any particular value $x \in \{0, \ldots, mr-1\}$ is $\frac{1}{mr}$; therefore, it gives us no particular information about the period r

↳ We want to find the periodic factor r.

Problem: Given mr and a black box generating $|\phi_{r,b}\rangle_u$, find the period r

$$u = \lceil \log_2(mr+1) \rceil, \quad |\phi_{r,b}\rangle_u = \frac{1}{\sqrt{m}} \sum_{j=0}^{m-1} |jr+b\rangle_u, \quad b \in \{0, 1, \dots, r-1\}$$

If we apply the operator $\mathtt{QFT}_{mr}^{-1}$ to each term $|jr+b\rangle$ in $|\phi_{r,b}\rangle_u$:

It is possible to know when there happens that $z = m \cdot k \Rightarrow$ we can compute $\frac{\cancel{m}k}{\cancel{m}r} = \frac{k}{r}$ $\Leftarrow$ if z != multiple of m $\Rightarrow$ we have the sum of all the possible combination of quantum states

$z \neq m \cdot k$

$$\frac{1}{\sqrt{m}} \left(\mathtt{QFT}_{mr}^{-1} |b\rangle_u + \cdots + \mathtt{QFT}_{mr}^{-1} |(m-1)r+b\rangle_u \right) = \frac{1}{m} \frac{1}{\sqrt{r}} \sum_{z=0}^{mr-1} \left(e^{2\pi\, i\, \frac{b}{mr}\, z} \sum_{j=0}^{m-1} e^{2\pi\, i\, \frac{j}{m}\, z} \right) |z\rangle$$

= the sum will be equal to zero.

Obs. with $k = 0, 1, 2, \dots (r-1)$, if $z \neq mk$ then $\sum_{j=0}^{m-1} e^{2\pi\, i\, \frac{j}{m}\, z} = 0$, otherwise $\sum_{j=0}^{m-1} e^{2\pi\, i\, \frac{j}{m}\, z} = m$.

$$= \frac{1}{m} \frac{1}{\sqrt{r}} \sum_{z=0,\ \text{with}\ z=mk}^{mr-1} \left(e^{2\pi\, i\, \frac{b}{r}\, k} \cdot m \right) |z\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{2\pi\, i\, \frac{b}{r}\, k} |mk\rangle$$

Periodic States

Problem: Given mr and a black box generating $|\phi_{r,b}\rangle_u$, find the period r

$$u = \lceil \log_2(mr+1) \rceil, \quad |\phi_{r,b}\rangle_u = \frac{1}{\sqrt{m}} \sum_{j=0}^{m-1} |jr+b\rangle_u\,, \quad b \in \{0, 1, \ldots, r-1\}$$

After the application of $\mathtt{QFT}^{-1}_{mr}$, we get:

$$\mathtt{QFT}^{-1}_{mr} |\phi_{r,b}\rangle_u = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi\, i\, \frac{b}{r}\, k} |mk\rangle$$

- If we measure this state we will obtain a value $x = mk$ for some random value of $0 \leq k < r-1$. As we know mr, we can compute $\frac{x}{mr} = \frac{mk}{mr} = \frac{k}{r}$ in lowest terms and find out the value of r However, if k and r share a common proper factor, we will find a denominator $\neq r$. The prob. of occurrence of such an event is: $1 - \frac{6}{\pi^2} \approx 40.3\%$ (i.e., 1 - Prob. of k and r being coprime). Thus, runnig the whole circuit several times will allow us to derive r.

Periodic States

New Problem

Given an integer n, $b \in \{0, 1, \ldots, r-1\}$ and a black box generating

$$|\phi_{r,b}\rangle_n = \frac{1}{\sqrt{m_b}} \sum_{z=0 (zr+b<2^n)}^{m_b - 1} |zr + b\rangle_n \,, \text{ with } m_b \approx \frac{2^n}{r} \text{ to make the state being unitary; find } r.$$

If we apply the circuit $\mathtt{QFT}^{-1}$, then with high probability a measurement will give us a value x such that $\frac{x}{2^n}$ is close to $\frac{k}{r}$ for a random k in $\{0, 1, 2, \ldots, r-1\}$.

Periodic States

Theorem (Period value probability)

Let x be the outcome of measuring $\mathtt{QFT}^{-1}\left|\phi_{r,b}\right\rangle_n$. The probability of obtaining x such that $\left|\left(\frac{x}{2^n}-\frac{k}{r}\right)\right| \leq \frac{1}{2m_b r}$ for some integer k, is $\geq \frac{m_b}{2^n}\frac{4}{\pi^2}$.

If $m_b \geq r$ (which implies $2^n \geq 2r^2$) then $\frac{1}{2m_b r} \leq \frac{1}{2r^2}$

Theorem (Period Value Reconstruction)

Let x be the outcome of measuring $\mathtt{QFT}^{-1}\left|\phi_{r,b}\right\rangle_n$. If x is so that $\left|\left(\frac{x}{2^n}-\frac{k}{r}\right)\right| \leq \frac{1}{2r^2}$, the application of the *continued fraction algorithm* fed with $\tilde{\omega}=\frac{x}{2^n}=0.x_1x2x_3\ldots x_n$ allows to derive $\frac{k}{r}$ with a computational effort linear in the number of bits of x.

Augmenting the number of qubits to perform the period estimation from n to $n+\Delta$ ($Delta > 1$), will increase the probability to read an x with the first n fractional binary digits in the correct range beyond 50%: $1-\frac{2}{2^\Delta}+\frac{2}{2^\Delta}\left(\frac{4}{\pi}^2\right)$

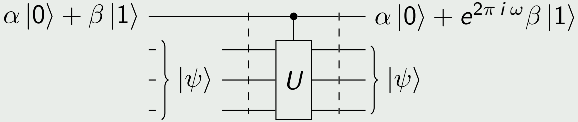
Preliminaries on the Eigenvalue Estimation Problem

Consider a n-qubit (unitary) operator U with eigenvector $|\psi\rangle$ and eigenvalue $e^{2\pi\, i\, \omega}$, and assume we have an efficient quantum circuit realizing U.
Consider a *controlled* $- U$ gate, c-U, and assume that its target register is prepared in the eigenstate $|\psi\rangle$. Consequently,

- $c\text{-}U(|0\rangle\, |\psi\rangle) = |0\rangle\, |\psi\rangle$
- $c\text{-}U(|1\rangle\, |\psi\rangle) = |1\rangle\, U\, |\psi\rangle = |1\rangle \otimes e^{2\pi\, i\, \omega}\, |\psi\rangle = (e^{2\pi\, i\, \omega}\, |1\rangle) \otimes |\psi\rangle$

c-U turns the eigenvalue into a relative phase factor of the control bit superimposition

The action of the controlled-U gate can be considered to have kicked back to the control bit the eigenvalue of the eigenstate prepared in the target register



Eigenvalue Estimation Problem

Definition

Given a quantum circuit implementing an operator U together with one of its eigenstate-eigenvalue pair: $|\psi\rangle$, $e^{2\pi\, i\, \omega}$, find a good estimation for the phase ω.

We now know that if we can devise a quantum circuit able to create the state

$$\frac{1}{\sqrt{2^n}} \sum_{z=0}^{2^n-1} e^{2\pi\, i\, \omega\, z} \left|z\right\rangle_n = \left(\frac{|0\rangle + e^{2\pi\, i\, (2^n \omega)} |1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle + e^{2\pi\, i\, (2^{n-1} \omega)} |1\rangle}{\sqrt{2}}\right) \otimes \cdots \otimes \left(\frac{|0\rangle + e^{2\pi\, i\, \omega} |1\rangle}{\sqrt{2}}\right)$$

the $\texttt{QFT}^{-1}$ circuit would allow us to assess $\omega = \frac{x}{2^n} = 0.x_1 x_2 \cdots x_{n-1} x_n$ by measuring its output x in multiple runs.

Eigenvalue Estimation Problem

1st step: Creation of the state

$$\frac{1}{\sqrt{2^n}} \sum_{z=0}^{2^n-1} e^{2\pi\, i\, \omega\, z} |z\rangle_n = \left(\frac{|0\rangle + e^{2\pi\, i\, (2^n \omega)} |1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle + e^{2\pi\, i\, (2^{n-1} \omega)} |1\rangle}{\sqrt{2}}\right) \otimes \cdots \otimes \left(\frac{|0\rangle + e^{2\pi\, i\, \omega} |1\rangle}{\sqrt{2}}\right)$$

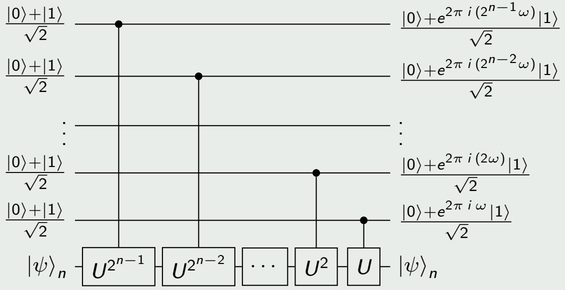
starting from U with eigenvalue $e^{2\pi\, i\, \omega}$ and eigenvector $|\psi\rangle$

Observations

- $|\psi\rangle$, $e^{2\pi\, i\ \ \omega}$ are an eigenstate-eigenvalue pair of U
- $|\psi\rangle$, $e^{2\pi\, i\, k\, \omega}$ are an eigenstate-eigenvalue pair of U^k
- using a $c\text{-}U^{2^j}$ with the target register prepared as the eigenvector $|\psi\rangle$ of U and with the control qubit prepared as $\mathtt{H}\,|0\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, it is easy to see that:

$$c\text{-}U^{2^j}\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\,|\psi\rangle\right) = \left(\frac{|0\rangle + e^{2\pi\, i\, (2^j \omega)}\,|1\rangle}{\sqrt{2}}\right)|\psi\rangle$$

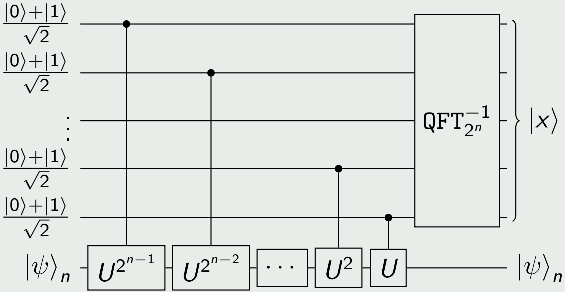
First stage of eigenvalue estimation



Eigenvalue Estimation Problem

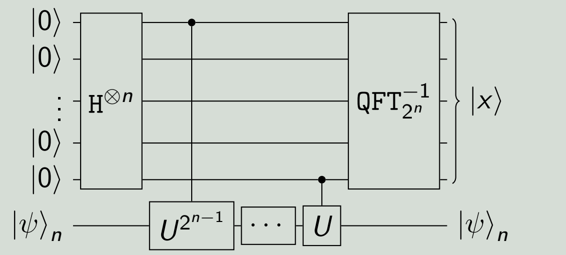
2nd Step: Application of the $\mathtt{QFT}_{2^n}^{-1}$ to measure an output state x so that $\frac{x}{2^n}$ is a good approximation of $\omega = 0.x_1 x_2 \cdots x_n\, x_{n+1} \cdots$

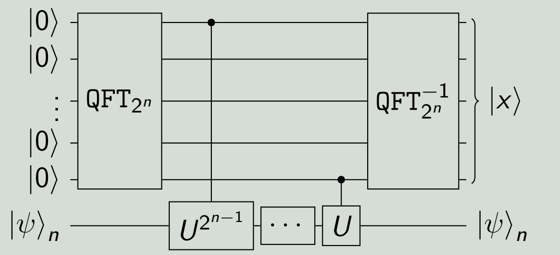
First and Second Stage of the Eigenvalue Estimation



Eigenvalue Estimation Problem

Circuit for the estimation of the eigenvalue of U associated to $|\psi\rangle$: $\tilde{\omega} = 2\pi\, i\, \frac{x}{2^n}$





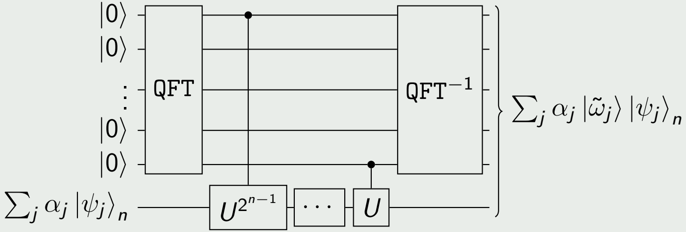
Eigenvalue Estimation Problem

Eigenvalue estimation circuit with the target register initially in an arbitrary state $|\varphi\rangle$

By the Spectral theorem, the eigenvectors of the 2^n-dimensional operator U form a basis.
This means that every state can be written as a linear composition of eigenvectors of U:

$$|\varphi\rangle_n = \sum_{j=0}^{2^n-1} \alpha_j \, |\psi_j\rangle_n \,, \text{ where } |\psi_j\rangle_n \text{ coupled with } e^{2\pi\, i\, \omega_j} \text{ are the eigen-vector/-value pairs of } U$$

- By measuring the control register, the whole output state collapses to $|\tilde{\omega}_j\rangle \, |\psi_j\rangle_n$ with probability $|\alpha_j|^2$



Preliminaries on Rivest Shamir Adleman (RSA) - Cryptoscheme

Greatest common divisor between two integers

The greatest common divisor between two integers a, b, denoted as $gcd(a, b)$, is the largest positive integer d such that $d|a$ and $d|b$. In the case that $a = b = 0$, by definition $\mathtt{gcd}(a, b) = 0$.

Extended Euclidean Algorithm for the computation of the gcd

The computation of the gcd among two integers $a, b \in \{0, \ldots, 2^n - 1\}$ allows to determine a triple of integers ξ, η, d ranging in the same interval such that

$$d = \mathtt{gcd}(a, b) = a \cdot \xi + b \cdot \eta$$

We know that, if $a > b > 0$:

$\Rightarrow gcd(a, b) = gcd(b, a \bmod b)$

Preliminaries on Rivest Shamir Adleman (RSA) - Cryptoscheme

set of element composed
by a . . . — (a w

The multiplicative algebraic group $\mathbb{Z}_N^*$

Given an integer $N > 0$, the support of the group $(\mathbb{Z}_N^*, \cdot)$ is defined as the set of residue classes $\{[0], [1], \dots, [a], \dots, [N-1]\}$, modulo N, where the representative element of a generic class $[a] = \{\cdots, -2N + a, -N + a, a, N + a, 2N + a, \cdots\}$ is chosen to be the integer with the lowest positive value:

$$\mathbb{Z}_N^* = \{0, 1, \dots, a, \dots, N-1\}, \text{where } 0 \leq a < N$$

Being a group, $\mathbb{Z}_N^*$ must contain the neutral element 1, and an inverse for each element into its support. The superscript $*$, in the notation $\mathbb{Z}_N^*$, points out that not all residue classes with representative less than N admits a multiplicative inverse...how many elements are in $\mathbb{Z}_N^*$?

$\mathbb{Z}_N = \{0, \dots, N-1\}$, $N > 0$.

$\phantom{\mathbb{Z}_N = \{} [0] \qquad [N-1]$

dot product in $\mathbb{Z}_N$

$(\mathbb{Z}_N, \cdot) \Rightarrow a, b \in \mathbb{Z}_N \Rightarrow a \cdot b = (a \cdot b) \bmod N$

$\Rightarrow \forall a \in \mathbb{Z}_N \Rightarrow a \cdot 1 = 1 \cdot a = a$

$a \in \mathbb{Z}_N \Rightarrow \bar{a} \cdot a = a \cdot \bar{a} = 1$

Euler Totient Function

Given an integer $N > 0$, the Euler Totient Function evaluated onto N is defined as the cardinality of the set of positive numbers less than N and with no common factors with N.

$$\varphi(N) = |\{m \text{ s.t. } 0 < m < N \text{ and } \gcd(m, N) = 1\}|$$

Closed formula for the Euler Totient Function

Given the factorization of $N = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$, where p_j are distinct prime numbers and $e_j \geq 1$ integers, the Euler Totient function can be computed as:

$$\varphi(N) = \prod_{j=1}^{s} \left(p_j^{e_j} - p_j^{e_j - 1}\right) = \frac{1}{N} \prod_{j=1}^{s} \left(1 - \frac{1}{p_j}\right)$$

$N = 15$

$\Rightarrow \varphi(N) = \left| \{1, 2, 4, 7, 8, 11, 13, 14\} \right| = 8$

we know that $N = 15 = 3 \cdot 5$

$\Rightarrow \varphi(N) = \varphi(3^1 \cdot 5^1) = (3^1 - 3^0)(5^1 - 5^0) = 8$

Preliminaries on Rivest Shamir Adleman (RSA) - Cryptoscheme

Theorem: Given $a \in \mathbb{Z}_N$, $a^{-1} \bmod N$ exists iif $\texttt{gcd}(a, N) = 1$

Two cases are possible:

- $\texttt{gcd}(a, N) = 1$ (the number of values $1 \leq a < N$ satisfying this condition is $\varphi(N)$)
- $\texttt{gcd}(a, N) = d > 1$

In the former case, lifting the value of a in $(\mathbb{Z}, +, \cdot)$, we can apply the Extended Euclid Algorithm to find the coefficients ξ, η s.t.:$1 = a \cdot \xi + N \cdot \eta$. Computing $\bmod N$ at both members, we can derive that

$$1 \bmod N = (a \cdot \xi) \bmod N = ((a \bmod N) \cdot (\xi \bmod N)) \bmod N \Rightarrow a^{-1} = (\xi \bmod N).$$

In the latter case, when $\texttt{gcd}(a, N) = d > 1$, a, does not belong to $(\mathbb{Z}_N^*, \cdot)$.
if $a \in (\mathbb{Z}_N^*, \cdot)$ there should exist an integer z, s.t. $a \cdot z \equiv_N 1 \Leftrightarrow a \cdot z - 1 = N \cdot q$ for a proper q.
Dividing both members of the last equality by d, we write
$\frac{a}{d} \cdot z - \frac{N}{d} \cdot q = \frac{1}{d}$, which is clearly false (...the difference of two integer numbers cannot be equal to $\frac{1}{d}$).

Preliminaries on Rivest Shamir Adleman (RSA) - Cryptoscheme

The multiplicative algebraic group $(\mathbb{Z}_N^*, \cdot)$

Given an integer $N > 0$, the support of the group $(\mathbb{Z}_N^*, \cdot)$ is defined as the set of residue classes modulo N, where the representative element of each class equals the integer with the lowest positive value and is coprime with N.

$$\mathbb{Z}_N^* = \{0, 1, \ldots, a, \ldots, N-1\},\ \gcd(a, N) = 1,\ 0 \leq a < N \qquad |\mathbb{Z}_N^*| = \varphi(N)$$

Order or period of an element $a \in \mathbb{Z}_N^*$

It is the lowest positive integer r such that $a^r = 1 \bmod N$ (or $a^r \equiv_n 1$)

Obs.:
$(\{a, , a^2, a^3, \ldots, a^r\}, \cdot)$ is a subgroup with r elements of $\mathbb{Z}_N^*$ and by the Lagrange Theorem $r|\varphi(N)$.
Given a factor of $\varphi(N)$ (being $\mathbb{Z}_N^*$ abelian) there exist at least one subgroup with the same cardinality.

Rivest Shamir Adleman (RSA) - Cryptoscheme

Public Key: k_{pub}

Let p, q be two prime integers ($p \approx q$) – randomly chosen

$$
\begin{aligned}
\text{RSA public modulus:} \quad & N \leftarrow p \cdot q \\
\text{RSA public exponent:} \quad & e \overset{\text{Random}}{\longleftarrow} \mathbb{Z}^*_{\varphi(N)} \\
& e \in \{1 \leq i \leq \varphi(N) - 1 \text{ s.t. } \gcd(e, \varphi(N)) = 1\}
\end{aligned}
$$

$$k_{pub} = \langle e, N \rangle$$

Private Key: k_{priv}

$$\text{RSA private exponent:} \quad d \leftarrow e^{-1} \mod \varphi(N) \qquad d \in \mathbb{Z}^*_{\varphi(N)}$$

$$k_{priv} = \langle p, q, \varphi(N), d \rangle$$

Rivest Shamir Adleman (RSA) - Cryptoscheme

One-way Function with Trapdoor

Encryption Function

Given a RSA public key $k_{pub} = \langle N, e \rangle$, the message $\mathcal{M}$ and ciphertext $\mathcal{C}$ spaces are defined as elements of $\mathbb{Z}_N$; i.e., $m, c \in \mathbb{Z}_n$

$$c \leftarrow Enc_{k_{pub}}(m) = m^e \bmod N$$

Decryption Function

Given a RSA private key $k_{priv} = \langle p, q, \varphi(N), d \rangle$, and a proper ciphertext $c \in \mathbb{Z}_n$

$$m \leftarrow Dec_{k_{priv}}(m) = c^d \bmod N$$

Rivest Shamir Adleman (RSA) - Cryptoscheme

In order to employ the previous definitions in a full cryptosystem it is necessary to prove:

$$Dec(Enc(m)) = m, \ \forall\, m \in \mathbb{Z}_n$$
$$(m^e)^{d \bmod \varphi(N)} \bmod N \equiv m^{ed \bmod \varphi(N)} \bmod N \stackrel{?}{\equiv} m \bmod N$$

$$Enc(Dec(c)) = c, \ \forall\, c \in \mathbb{Z}_n$$
$$(c^d)^{e \bmod \varphi(N)} \bmod N \equiv c^{ed \bmod \varphi(N)} \bmod N \stackrel{?}{\equiv} c \bmod N$$

- The symmetry of the encryption and decryption functions allows us to restrict the correctness proof only to the encryption transformation.

Rivest Shamir Adleman (RSA) - Cryptoscheme

Given $N = p \cdot q, m \in \mathbb{Z}_N$; $e, d \in \mathbb{Z}^*_{\varphi(N)}$ $(e \cdot d \equiv_{\varphi(N)} 1)$, we need to prove that:

$$(m^e)^{d \bmod \varphi(N)} \bmod N \equiv m \bmod N, \ \forall\, m \in \mathbb{Z}_n$$

we need to distinguish two cases:

1st case: $\gcd(N, m) = 1$

In this case m has a multiplicative inverse in $\mathbb{Z}_N$: $m \in \mathbb{Z}^*_N$, where $|\mathbb{Z}^*_n| = \varphi(N)$ thus, for some integer t, we can write the following:

$$(m^e)^d \equiv_N m^{1+t\varphi(N)} \equiv_N m \cdot (m^{\varphi(N)})^t \equiv_N m$$

Therefore,

$$(m^e)^{d \bmod \varphi(N)} \bmod N \equiv m^{ed \bmod \varphi(N)} \bmod N \equiv m \bmod N \qquad \text{(cvd.)}$$

2nd case: $\gcd(N, m) \neq 1$

Being $\gcd(N, m) \neq 1$ we can write (without loss of generality) that $\gcd(N, m) = p$, that is, we can assume $\mathbf{m} = \mathbf{u} \cdot \mathbf{p}$, for some integer u.

Consider that:

$$
\begin{aligned}
&m^{\varphi(q)} \bmod q \equiv m^{q-1} \bmod q \equiv 1 \bmod q \qquad (obs. : \gcd(q, m) = 1) \\
&(m^{\varphi(N)})^t \bmod q \equiv (m^{(q-1)})^{(p-1)t} \bmod q \equiv 1 \bmod q \\
&(\mathbf{m}^{\varphi(\mathbf{N})})^{\mathbf{t}} = \mathbf{1} + \mathbf{s}\,\mathbf{q}, \text{for some integers } \mathbf{s} \text{ and } \mathbf{t}.
\end{aligned}
$$

Thus,

$$
\begin{aligned}
&(\mathbf{m}^{\mathbf{e}})^{\mathbf{d}} \equiv_n m^{1+t\varphi(N)} \equiv_N m \cdot (m^{\varphi(N)})^t \equiv_{\mathbf{n}} \mathbf{m} \cdot (\mathbf{1} + \mathbf{s}\,\mathbf{q}) \\
&m \cdot (1 + s\,q) \equiv_n m + \mathbf{m}\,s\,q \equiv_n m + \mathbf{u}\,\mathbf{p}\,s\,q \equiv_n m + (u\,s)\,\mathbf{N} \equiv_{\mathbf{n}} \mathbf{m}
\end{aligned}
$$

Hence:

$$
(m^e)^{d \bmod \varphi(N)} \bmod N \equiv m^{ed \bmod \varphi(N)} \bmod N \equiv m \bmod N \qquad \text{(cvd.)}
$$

Mathematical Security of the RSA cryptoscheme

Observation

Note that the domain of the RSA encryption and decryption transformations (with $N = pq$) is

$$\mathbb{Z}_N = \overbrace{\mathbb{Z}_N^*}^{\text{All the elements less than } n \text{ and coprime with } n} \cup \underbrace{\{p, 2p, 3p, \ldots, (q-1)p\}}_{q-1 \text{ elements}} \cup \underbrace{\{0, q, 2q, 3q, \ldots, (p-1)q\}}_{p \text{ elements}}$$

The cardinalities of the previous sets are: $\varphi(N)$, $q-1$ and p, and the chances to observe a random plaintext/ciphertext value in $\mathbb{Z}_n \setminus \mathbb{Z}_n^*$ are: $\frac{p+q-1}{pq}$ (having N encoded with 2048 bits implies a Pr$\approx \frac{1}{2^{1023}}$).

- If an adversary has the chance to verify (with poly cost via the EEA) that a ciphertext/plaintext message has a factor in common with the public modulus N, e.g., $gcd(c, N) = p$, then he can factor the RSA public modulus and also break the RSA problem.
- Chances that this actually happen are negligible in the length of the public modulus ! (Nobody in practice makes the aforementioned check)

Mathematical Security of the RSA cryptoscheme

Factoring Problem (FP)

Given a positive integer N, find $p_1, p_2, \ldots p_s$, $e_1, e_2, \ldots, e_s$ s.t. $N = \prod_{j=0}^{s} p_j^{e_j}$, where p_js are distinct primes, $e_j > 0$, $s > 0$.

Generally speaking, to make FP actually interesting, N should be odd and include at least two distinct odd prime factors (i.e., $s \geq 2$)

- even factors can be straightforwardly checked
- $N = p^w$ can be checked via no more than $\log_2(N)$ primality tests to $p = 2^{\frac{1}{w}\log_2 N}$, $0 < w < \log_2(N)$

The Security of RSA cryptosystem (where the public modulus N is built as the product of two distinct primes having the same size) is related to the computational complexity of FP because if anyone can factor in poly time the public modulus $N = pq$, then he can also compute $(p-1)(q-1) = \varphi(N)$ and $d = e^{-1} \bmod \varphi(N)$, via the EEA, thus breaking the RSA problem!

Mathematical Security of the RSA cryptoscheme

Splitting an Odd Non-prime-power Integer Problem (SONIP)

Given an odd integer N that has at least two distinct prime factors, find N_1, N_2 s.t. $N = N_1 N_2$, where $1 < N_1 < N$, $1 < N_2 < N$

The FP problem can be reduced to SONIP. Indeed, with a SONIP oracle it is easy to devise a recursive procedure able to determine the prime power factors of N with $O(\log(N))$ primality tests, where each test can be executed with either $O(N^2)$ prob. pol. complexity or $O(N^7)$ deterministic complexity.

Order Finding Problem (OF)

Given two integers $0 < c < N$, s.t. $\texttt{gcd}(c, N) = 1$, find the lowest integer r such that $a^r \equiv_n 1$.

The SONIP can be reduced to the OFP as follows. Given N (with at least two prime factors) and a randomly selected c with $\texttt{gcd}(c, N) = 1$, the OF oracle returns r. The probability of r being even is at least $\frac{1}{2}$, as a consequence, also the following derivation hold with the same chances: $(c^{r/2} - 1)(c^{r/2} + 1) \equiv_n 0 \Leftrightarrow \texttt{gcd}(c^{r/2} - 1, N)$ is a non trivial factor of N.

Mathematical Security of the RSA cryptoscheme

RSA Problem (RSAP)

Given a ciphertext $c = m^e \bmod N \in \mathbb{Z}_N$, where $N = p \cdot q$, $e \in \mathbb{Z}^*_{\varphi(N)}$; find $m \in \mathbb{Z}_N$.

- RSAP is in NP$\cap$coNP, therefore highly likely $\notin$NPC $\Rightarrow$ quantum superpoly speedup is possible!
- Being OFP $\geq$ SONIP $\geq$ FP $\geq$ RSAP, the RSAP is not more difficult than FP, SONIP, OFP.
- There is no algorithm to solve the RSAP directly. Furthermore, it is not known if an algorithm able to solve the RSAP can also solve OFP, FP, SONIP!
  (we do not know if RSAP $\geq$ OFP, i.e., if OFP can be reduced to RSAP , and therefore if RSAP=OFP)

RSA message recovery via order finding (a direct RSAP to OFP reduction)

Given a RSA public key $k_{\text{pub}} = (e, N)$, and a ciphertext c, if an oracle finds the order r of c, then r is also the order of m and $\gcd(e, r) = 1$ because $\gcd(e, \varphi(N)) = 1$ and $r|\varphi(n)$ which, in turn, implies the existence of another integer d' s.t. $e \cdot d' = 1 \bmod r$. It can be computed in poly time via the EEA.

The plaintext m is then recovered without knowing the private key, by computing
$c^{d'} \equiv_N m^{ed'} \equiv_N m^{1+s\cdot r} \equiv_N m \cdot (m^r)^s \equiv_N m$.

Quantum Eigenvalue Estimation Approach to Order Finding

Order Operator U_a

Given $0 < a < N, \texttt{gcd}(a, N) = 1$, let U_a be the operator implemented with n qubits ($2^n > N$) s.t.

$$U_a : |s\rangle \mapsto |sa \bmod N\rangle\,, \text{ when } 0 \leq s < N, \;\; |s\rangle \mapsto |s\rangle \text{ otherwise}$$

We will restrict the action of U_a over the state space spanned by $\{|0\rangle\,, |1\rangle\,, \ldots, |N-1\rangle\}$.

Eigenvalues of U_a

Denoting with r the order (period) of $a \bmod N$, since $a^r \equiv 1 \bmod N$:

$$U_a^r : |s\rangle \mapsto |sa^r \bmod N\rangle = |s\rangle$$

That is, $U_a U_a \cdots U_a = U_a^r$ is the operator having the r-th roots of $\mathtt{I} \bmod N$ as eigenvalues.

- Being U_a unitary, it is also normal and then the spectral theorem applies:
  $U_a = V \Lambda V^\dagger$, $U_a^r = V \Lambda^r V^\dagger$, where $\Lambda^r = \texttt{diag}(\ldots, \lambda_i^r, \ldots)$
  $U_a^r = I \Rightarrow \lambda_i^r = 1 \Rightarrow \lambda_i = e^{2\pi\, i\, \frac{k}{r}}$, $k \in \{0, \ldots, r-1\}$ are the distinct eigenvalues of U_a.

Quantum Eigenvalue Estimation Approach to Order Finding

Eigenvectors of U_a

The following state is one out of r distinct eigenvectors of U_a.

$$|u_k\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{-2\pi\, i\, \frac{k}{r} s} \, |a^s \bmod N\rangle$$

Proof.

$$U_a\,|u_k\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{-2\pi\, i\, \frac{k}{r} s} \, |a^{s+1} \bmod N\rangle = \frac{e^{2\pi\, i\, \frac{k}{r}}}{\sqrt{r}} \sum_{s=0}^{r-1} e^{-2\pi\, i\, \frac{k}{r}(s+1)} \, |a^{s+1} \bmod N\rangle = e^{2\pi\, i\, \frac{k}{r}}\,|u_k\rangle$$

For any value $k \in \{0, \ldots, r-1\}$ if we were given the eigenvector state $|u_k\rangle$ we could apply the eigenvalue estimation circuit and determine the phase of the eigenvalue $e^{2\pi\, i\, \frac{k}{r}}$ as $\frac{x}{2^m} = \frac{k}{r}$ deriving r. Nonetheless, we do not know r and consequently cannot prepare the state $|u_k\rangle$, accordingly;

however

it is possible to find r by preparing a superimposition of all distinct eigenvectors of U_a.

Quantum Eigenvalue Estimation Approach to Order Finding

$$|u_k\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{-2\pi\, i\, \frac{k}{r} s} \left| a^s \bmod N \right\rangle$$

Observation

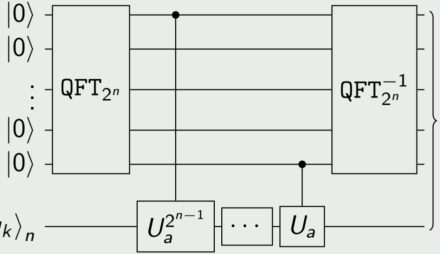
$$\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |u_k\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{-2\pi\, i\, \frac{k}{r} s} \left| a^s \bmod N \right\rangle .$$

Note that $\left| a^s \bmod N \right\rangle = |1\rangle$ when $s \equiv_N 0$, therefore the amplitude of $|1\rangle$ in the above state is $\frac{1}{\sqrt{r}} \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{2\pi\, i\, \frac{k}{r}\, 0} = 1$. The amplitudes of all other computational basis equal 0, and we can conclude that the sum of all distinct eigenvectors of U_a is:

$$\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |u_k\rangle = |1\rangle$$

Quantum Eigenvalue Estimation Approach to Order Finding

Circuit for the estimation of the eigenvalues of U_a associated to the superimposition of its eigenvectors



$$|1\rangle_n = |00\cdots1\rangle_n = \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}|u_k\rangle_n$$

$$\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}|\tilde{\omega}_k\rangle_n|u_k\rangle_n,\ \tilde{\omega}_k = \frac{\tilde{k}}{r}$$

Obs: $c\text{-}U_a^{2^j}$ can be realized computing j squarings ($a^{2^j} \bmod N$) and preparing $c\text{-}U_{a^{2^j}} = c\text{-}U_a^{2^j}$; the circuits we need to prepare other than, $\mathtt{QFT}$ and $\mathtt{QFT}^{-1}$, are the ones equivalent to computing $a^{2^t} \bmod N$ where $1 \leq t < n$

The Eigenvalue estimation algorithm maps

the input state $|0\rangle_n|1\rangle_n = \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}|0\rangle_m|u_k\rangle_n$ to the output state: $\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}|\tilde{\omega_k}\rangle_n|u_k\rangle_n$

Quantum Order Finding Algorithm (to find the order r of a mod N, $\mathtt{gcd}(a, N) = 1$)

1. Choose an integer n so that $2^n \geq 2r^2$. As $r|\varphi(N)$ and $\varphi(N) \approx N$, $n = \lceil 2 \log N \rceil$ will suffice.
2. Initialize an n-qubit register to $|0\rangle_n = |0\rangle_1^{\otimes n}$ (call it *control register*)
3. Initialize an n-qubit register to $|1\rangle_n = |0\rangle_1^{\otimes n-1} |1\rangle_1$ (call it *target register*)
4. Apply the $\mathtt{QFT}_{2^n}$ to the control register (in this case $\equiv \mathtt{H}^{\otimes n}$)
5. Apply the series of c-$U_a^{2^j}$ gates to both control and target registers
6. Apply the $\mathtt{QFT}_{2^n}^{-1}$ to the control register
7. Measure the control register and obtain $\bar{x}$ (... and $\frac{\bar{x}}{2^n}$ as an estimate for a random multiple of $\frac{1}{r}$)
8. Apply the "continued fraction algorithm" to find c_1, r_1 such that $\left|\frac{\bar{x}}{2^n} - \frac{c_1}{r_1}\right| < \frac{1}{2^{n+1}}$ otherwise "FAIL". Repeat steps 1–7 to get another measurement $\tilde{x}$ and apply the "continued fraction algorithm" to find c_2, r_2 such that $\left|\frac{\tilde{x}}{2^n} - \frac{c_2}{r_2}\right| < \frac{1}{2^{n+1}}$ otherwise "FAIL"
9. Compute r as the least common multiple between $r = \mathtt{lcm}(r_1, r_2) = \frac{r_1 \cdot r_2}{\mathtt{gcd}(r_1, r_2)}$ (proof next slide)
10. If $a^r = 1$ mod N then outputs r. Otherwise, output "FAIL".

Finding r, given $\frac{k}{r}$ for random $k \in \{0, 1, \ldots, r-1\}$

Theorem

Suppose the integers k_1, k_2 are selected independently and uniformly at random from $\{0, 1, \ldots, r-1\}$. Let r_1, r_2, c_1, c_2 be integers satisfying $\mathtt{gcd}(r_1, c_1) = \mathtt{gcd}(r_2, c_2) = 1$ and $\frac{k_1}{r} = \frac{c_1}{r_1}$ and $\frac{k_2}{r} = \frac{c_2}{r_2}$. Then $\mathtt{Pr}(\mathtt{lcm}(r_1, r_2) = r) \geq \frac{6}{\pi^2} \approx 60.7\%$

Proof.

$r = r_1\mathtt{gcd}(k_1, r)$, $r = r_2\mathtt{gcd}(k_2, r)$
If we assume $\mathtt{gcd}(k_1, r)$ and $\mathtt{gcd}(k_2, r)$ with no common factor, (such an event has Prob.$\geq \frac{6}{\pi^2} \approx 60.7\%$ to occur), the following equalities hold.
$\mathtt{gcd}(k_1, r) | r_2 \Rightarrow r_2 = \alpha\mathtt{gcd}(k_1, r)$
$\mathtt{gcd}(k_2, r) | r_1 \Rightarrow r_1 = \beta\mathtt{gcd}(k_2, r)$

Being $r = r_1\mathtt{gcd}(k_1, r) = \beta\mathtt{gcd}(k_2, r)\mathtt{gcd}(k_1, r)$ and $r = r_2\mathtt{gcd}(k_2, r) = \alpha\mathtt{gcd}(k_1, r)\mathtt{gcd}(k_2, r)$ it is easy to infer that $\alpha = \beta$, therefore $\mathtt{gcd}(r_1, r_2) = \alpha$.

$$\mathtt{lcm}(r_1, r_2) = \frac{r_1 \cdot r_2}{\mathtt{gcd}(r_1, r_2)} = \frac{\alpha^2 \cdot \mathtt{gcd}(k_1, r)\mathtt{gcd}(k_2, r)}{\alpha} = r$$

Quantum Order Finding Algorithm (the order r of a mod N)

Cost of the order finding circuit

Each one of the $c\text{-}U_a^{2^j}$ operators $j = 0, 1, \ldots, n-1$ requires a quantum circuit able to mimic the classical multiplication of an integer s by the integer a^t mod N for proper values of t (i.e., s.t. $a^{2^j} \equiv a^t \bmod N$).
Each $c\text{-}U_a^{2^j}$ circuit can be implemented employing $O((\log N) \log\log(N) \log\log\log(N))$ gates.

- The series of $c\text{-}U_a^{2^j}$ circuit requires $O((\log N)^2 \log\log(N) \log\log\log(N))$
- the $\mathtt{QFT}_{2^n}$ requires $O((\log N)^2$ gates

Total Quantum Cost: $O((\log N)^2 \log\log(N) \log\log\log(N))$; with a constant number of runs.
Total Classical cost: $O\left(\exp\left((\log N)^{\frac{1}{3}} (\log\log(N))^{\frac{2}{3}}\right)\right)$

Shor's Approach to Estimating a random multiple of $\frac{1}{r}$

Shor's approach can be listed in four steps. It employes exactly the same circuit we have already studied but the state of the system is now analyzed in the computational basis instead of using the eigenvector basis.

Step 1

Create the state

$$|\psi_0\rangle = \sum_{x=0}^{2^n-1} \frac{1}{\sqrt{2^n}} |x\rangle |a^x \bmod N\rangle = U_a^x(\mathrm{H}^{\otimes n} |0\rangle_n |1\rangle_n), \text{with } U_a^x : |x\rangle |y\rangle \mapsto |x\rangle |ya^x \bmod N\rangle$$

Obs. each x can be decomposed in a quotient and a remainder of the division by r obtaining:

$$|\psi_0\rangle = \sum_{b=0}^{r-1} \left(\sum_{z=0}^{m_b-1} \frac{1}{\sqrt{2^n}} |zr + b\rangle \right) |a^b \bmod N\rangle$$

where m_b is the largest integer s.t. $(m_b - 1)r + b < 2^n$

Shor's Approach to Estimating a random multiple of $\frac{1}{r}$

Step 2

Measure the second register. We will get a value $a^b \bmod N$ for b chosen almost uniformly at random in $\{0, 1, \ldots, r-1\}$. The first register will be left in the following superimposition

$$\frac{1}{\sqrt{m_b}} \sum_{z=0}^{m_b-1} |zr + b\rangle \, .$$

If we were able to implement $\mathtt{QFT}^{-1}_{m_b r}$ and apply it to the above state, then we would produce the superimposition

$$\sum_{j=0}^{r-1} e^{2\pi\, i\, \frac{k}{r} j} \, |mj\rangle \, .$$

In other word, we will only measure x such that $\frac{x}{rm_b} = \frac{j}{r}$ for some integer j. However, since we do not know what m_b and r are, we use $\mathtt{QFT}^{-1}_{2^n}$

Shor's Approach to Estimating a random multiple of $\frac{1}{r}$

Step 3

Apply $\mathtt{QFT}_{2^n}^{-1}$ to the first register, and then measure. Let x be the measured value.

Step 4

Output $\frac{x}{2^n}$

Theorem

The Shor's algorithm outputs an integer x, $0 \leq x < 2^n$, such that for each $j \in \{0, 1, \ldots, r-1\}$ with probability at least $\frac{4}{r\pi^2}$ we have: $|\frac{x}{2^n} - \frac{j}{r}| < \frac{1}{2^{n+1}}$.

Textbook references

- N. D. Mermin Chapter 3