Quantum Algorithms 4/11/2023

Lecture 21: Phase Estimation

Instructor: Dieter van Melkebeek

In this lecture, we talk about the quantum Fourier transform and phase estimation, which is a precursor to eigenvalue estimation, a key ingredient in the algorithm we will later develop for finding the order of an integer modulo another integer. We start by discussing Quantum Fourier transform for the the group $\mathbb{Z}_N, +$ (integers modulo N), where $N = 2^n$. A similar approach can be adapted for the cases where N has prime factors other than 2, but we will mainly use the case where N is a power of 2. Then we talk about phase estimation: the problem statement, an algorithm based on the Quantum Fourier transform over $\mathbb{Z}_N, +$, and its analysis. We end by introducing eigenvalue estimation as an application of phase estimation.

1 Quantum Fourier transform over $\mathbb{Z}_N, +$

In previous lectures, we derived the expression for Quantum Fourier Transform over $\mathbb{Z}_N, +$ as:

$$F\left|x\right\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \exp\left(\frac{2\pi i x y}{N}\right) \left|y\right\rangle . \tag{1}$$

Qualitatively, applying the Fourier transform to a basis state $|x\rangle$ results in a superposition of the basis states $|y\rangle$ where the amplitude for each basis state has absolute value $\frac{1}{\sqrt{N}}$ and the phase is given by $\exp\left(\frac{2\pi i x y}{N}\right)$. Since y here represents an n bit binary number, considering the binary expansion, it can be written as

$$y = \sum_{j=1}^{n} y_j 2^{n-j} \qquad\qquad \text{for } \ y_i \in \{0, 1\}. \tag{2}$$

Thus, we can write $|y\rangle$ as:

$$\left|y\right\rangle = \left|y_1\right\rangle \left|y_2\right\rangle \left|y_3\right\rangle \dots \left|y_n\right\rangle = \left|y_1\right\rangle \otimes \left|y_2\right\rangle \otimes \left|y_3\right\rangle \otimes \cdots \otimes \left|y_n\right\rangle , \tag{3}$$

where y_n is the lowest order bit and y_1 is the highest order bit. We have written $|y\rangle$ as a tensor product on individual qubits, which we can always do for a basis state. We can further use (2) to rewrite the phase term in (1):

$$\exp\left(\frac{2\pi i x y}{N}\right) = \exp\left(\sum_{j=1}^{n} \frac{2\pi i x y_j 2^{n-j}}{2^n}\right) = \prod_{j=1}^{n} \exp\left(\frac{\pi i x y_j}{2^{j-1}}\right). \tag{4}$$

Combining the equations (2), (3) and (4), the overall expression for the Fourier transform can be written as:

$$F\left|x\right\rangle = \frac{1}{\sqrt{N}} \sum_{y_1=0}^{1} \sum_{y_2=0}^{1} ... \sum_{y_n=0}^{1} \exp(\pi i x y_1) \left|y_1\right\rangle \otimes \exp(\pi i y_2/2) \left|y_2\right\rangle \otimes \cdots \otimes \exp(\pi i x y_n/2^{n-1}) \left|y_n\right\rangle . \tag{5}$$

Since the y_i part does not depend on any previous element of the tensor product, we can use distributivity of tensor products over sums to move the sum inside of the tensor product and obtain:

$$F\,|s\rangle = \frac{1}{\sqrt{N}} \sum_{y_1=0}^{1} \exp(\pi i x y_1)\,|y_1\rangle \otimes \sum_{y_2=0}^{1} \exp(\pi i x y_2/2)\,|y_2\rangle \otimes \cdots \otimes \sum_{y_n=0}^{1} \exp\left(\frac{\pi i x y_n}{2^{n-1}}\right)|y_n\rangle\,. \qquad (6)$$

Note that x is an integer between 0 and $N-1$, and each y_j can either be 0 or 1. Focusing on each individual sum of the vector product in (6), we note that for $\sum_{y_j=0}^{1} \exp(\pi i x y_j/2^{j-1})\,|y_j\rangle$, the first term ($y_j = 0$) is always equal to $ket0$. Further, for $y_j = 1$, the product $\exp(\pi i x y_j)$ becomes $\exp(\pi i x/2^{j-1})$. Thus, the sum becomes $|0\rangle + \exp(\pi i x/2^{j-1})|1\rangle$. Re-writing our (6) we get:

$$\frac{1}{\sqrt{2}}(|0\rangle + \exp(\pi i x)|1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + \exp(\pi i x/2)|1\rangle) \otimes ... \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + \exp\left(\frac{\pi i x}{2^{n-1}}\right)|1\rangle\right). \qquad (7)$$

Note that the factor $\frac{1}{\sqrt{N}}$ in (6) is broken down into n factors of $\frac{1}{\sqrt{2}}$ in (7). In summary, we can write the Fourier transform as

$$F\,|x\rangle = |z_1\rangle\,|z_2\rangle \ldots |z_n\rangle\,,$$

where $|z_k\rangle = \frac{1}{\sqrt{2}}(|0\rangle + \exp(\pi i x/2^{k-1})\,|1\rangle)$.

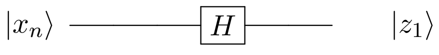
Expressing $|z_j\rangle$ in terms of $|x\rangle$. We now see how we can realize each of these qubits. We start with the simplest case: $|z_1\rangle$. We first note that similar to (2), we can write $x = \sum_{j=1}^{n} x_j 2^{n-j}$, where $x_j \in \{0, 1\}$. Using this, the expression for $|z_1\rangle$ can be written as:

$$|z_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + \exp(\pi i x_n)\,|1\rangle). \qquad (8)$$

Note that the higher order bit in the binary expansion of x do not contribute to the exponential term as they give us a factor of 2 (through the exponent of 2) and $\exp(2\pi i k) = 1$ for any integer k. Thus, for $|z_1\rangle$, only the lowest order bit of x contributes, namely x_n. For $x_n = 0$, $|z_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ whereas for $x_n = 1$ we have $|z_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. In other words, $|z_1\rangle$ can be obtained from $|x_n\rangle$ by application of an Hadamard gate:

$$|z_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + \exp(\pi i x_n)\,|1\rangle) = H\,|x_n\rangle\,, \qquad (9)$$

which can be represented in circuits as:



We can extend this analysis to $|z_2\rangle$. Note here that only the two lowest order bits of x contibute here as the other bits yield a factor of 1 (similar to above). After applying the simplification, the expression can be written as:

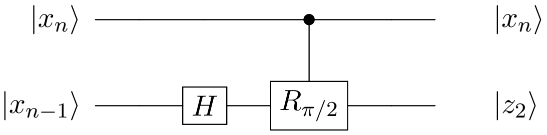
$$|z_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle + \exp(\pi i x_{n-1})\exp(\pi i x_n/2)\,|1\rangle). \qquad (10)$$

This can be realized by applying the Hadamard gate to $|x_{n-1}\rangle$, i.e., $H\,|x_{n-1}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + \exp(\pi i x_{n-1})\,|1\rangle)$, with an additional phase factor on the component $|1\rangle$. The value of the additional phase factor is

1 if $x_n = 0$ and $\exp(i\pi/2)$ for $x_n = 1$. We can write this as a conditional rotation, conditioned on the qubit $|x_n\rangle$ being $|1\rangle$:

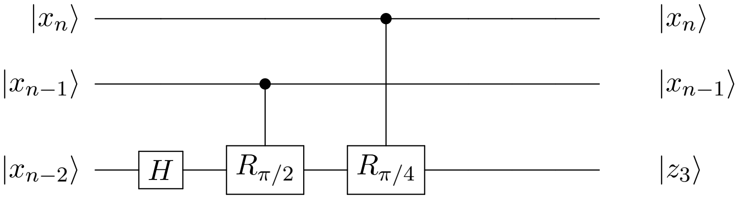
$$CR(\pi/2)\,|x_n\rangle\,H\,|x_{n-1}\rangle = |x_n\rangle|z_2\rangle. \tag{11}$$

In terms of circuits, we have:

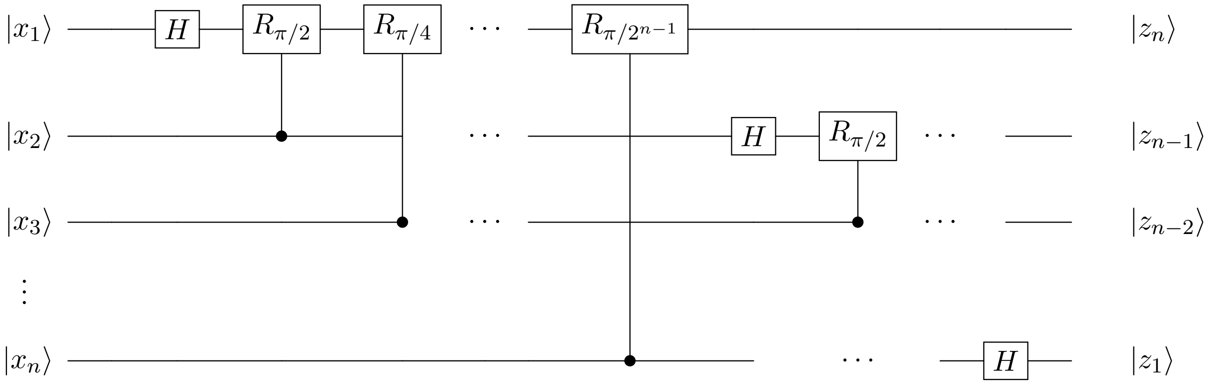


Qualitatively, to obtain $|z_2\rangle$, we first apply the Hadamard gate to $|x_{n-1}\rangle$ and then apply a controlled rotation of $\frac{\pi}{2}$ controlled by qubit $|x_n\rangle$. Note that the order of gates matter here; we cannot swap the Hadamard gate and the controlled rotation. To see this, consider the case when the $|x_{n-1}\rangle$ is in the $|0\rangle$ state. Here, if we apply the rotation first and then the Hadamard gate, the conditional rotation does not have an effect (it only affects the $|1\rangle$ state) and the application of the Hadamard gate results in the final state being $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ (without any additional phase on $|1\rangle$). On the contrary, if we apply the Hadamard first, then the input for the conditional rotation is $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, resulting in the final state $|+\rangle$ if $x_n = 0$ but $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ if $x_n = 1$. Thus, the order of application of gates matters.

Extending the procedure to $|z_3\rangle$, we can construct the following circuit:



Putting it all together. We can extend the pattern to get circuits for $|z_k\rangle$, where we transform the qubit $|x_{n-k+1}\rangle$ into $|z_k\rangle$. In order to calculate the overall Fourier transform, we need the jth bit of x to act as a control on $|x_k\rangle$ for all $k < j$, and thus we cannot change $|x_j\rangle$ until all $|x_k\rangle$ for $k < j$ have been transformed. Due to this, we must compute the $|z_k\rangle$ in descending order, computing $|z_n\rangle$ and then $|z_{n-1}\rangle$, until computing $|z_1\rangle$. This results in the following circuit:



Since the circuits is unitary and works for all basis states $|x\rangle$, it also works for all possible superpositions $|\psi\rangle$. Note that this circuit reverts the order of the output qubits, which can later be reversed using swaps to get the qubits in order. The resulting circuit consists of $n - j + 1$ gates for each x_j, which makes the total gates to be $O(n^2)$.

An important observation here is that many of the further rotations are extremely small, so to compute this transform approximately, we can omit them and still obtain a good approximation of the whole circuit. More precisely:

Exercise 1. *Dropping rotations $R_{\pi/2^j}$ for $j \geq \log(n/\epsilon)$ yields circuit with $O(n \log(n/\epsilon))$ gates that $O(\epsilon)$ approximates F in 2-norm.*

2 Phase estimation

Phase estimation is closely related to the (inverse) Fourier transform over $\mathbb{Z}_N, +$ for $N = 2^n$. We describe both the classical and quantum versions, with the quantum version described as the subroutine output below.

2.1 Problem statement

Input: A pure state on of the form $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \exp(2\pi i \omega x) |x\rangle$, where $\omega \in [0, 1)$ is unknown. We refer to such a state as a harmonic state. Note that the input expression is very similar to the output of the Quantum Fourier Transform. The key difference is that ω can take any value between 0 and 1. The objective is to find ω (or a good approximation of it).

Classical output: ω, or a good approximation of the form y/N for $y \in \mathbb{Z}_N$ such that

$$|\omega - \frac{y}{N}|_{\mathbb{T}} \leq \delta, \tag{12}$$

where we can take δ to be another parameter and $\mathbb{T}$ refers to "modulo 1" (explained below).

Quantum output: Pure state $|\tilde{\omega}\rangle$ on n qubits with total weight of the good y's at least $1 - \epsilon$, where good y's are the ones that satisfy (12).

To obtain the classical output, we can just observe the particular state that the quantum subroutine outputs. It gives us a good y with probability at least $1 - \epsilon$.

As for the approximation requirement (12), note that we cannot expect to find y such that $|\omega - \frac{y}{N}| \leq \delta$ in general, namely in cases where ω is close to 0 or to 1. This is because the input state $|\psi\rangle$ is the same for $\omega = 0$ and for $\omega = 1$. Similarly, the cases with $\omega = \omega_0$ for ω_1 slightly above 0, and $\omega = \omega_1$ for ω_1 slightly below 1 cannot be distinguished efficiently. What we want is that the approximation to ω is to within δ modulo 1. Formally, we can define the distance

$$|\omega_0 - \omega_1|_{\mathbb{T}} = \min_{z \in \mathbb{Z}} |\omega_0 - \omega_1 + z|.$$

We get this metric by "wrapping the interval $[0, 1]$ around on the circle", as shown in Figure 1: ω_0 and ω_1 are close even though ω_1 corresponds to a very small polar angle and ω_1 from a very large polar angle. The distance on the circle captures this. The letter $\mathbb{T}$ in the notation stands for a torus, as a circle is a 1-dimensional torus.

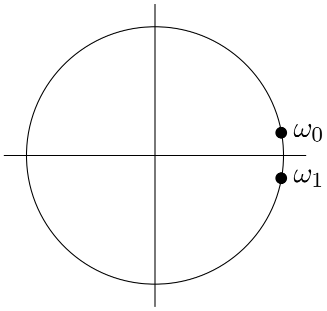


Figure 1: Wrapping the interval $[0,1]$ around on the circle.

2.2 Algorithm

To obtain (an approximation to) the phase value ω, we simply apply the inverse Fourier transform $F^{-1}|\psi\rangle$ over $\mathbb{Z}_N, +$.

In case $\omega = \frac{y^*}{N}$ for $y \in \{0, \ldots, N-1\}$ then we have $| \, |\tilde{\omega}\rangle = |y^*\rangle\rangle$. In this case, measuring the final state always yields a y^*. In this scenario, $|\psi\rangle$ is just the Fourier transform of $|y^*\rangle$.

In the general case, the output $|\tilde{\omega}\rangle$ satisfies the aforementioned requirements for any $\delta > 0$ with $\delta \cdot \epsilon = O(1/N)$. Intuitively, we can understand this as $|\tilde{\omega}\rangle$ has most of its weight on $y \in \mathbb{Z}_N$ with $\frac{y}{N}$ close to ω modulo 1. Measuring the final state yields a good y (i.e, $|\omega - \frac{y}{N}|_{\mathbb{T}} \leq \delta$) with probability at least $1-\epsilon$. There is a trade-off between ϵ and δ. This can be understood intuitively as if we want to be very certain in our measurement (low ϵ) then we would have to increase the error margin on ω. Note that for constant ϵ, it suffices for N to be linear in $\frac{1}{\delta}$, or equivalently, for n to be the number bits of accuracy required plus some constant.

2.3 Analysis

We have that $F^{-1}|x\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \exp\left(-\frac{2\pi i x y}{N}\right) |y\rangle$. We apply this to the superposition $|\psi\rangle$ that we began with, $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \exp(2\pi i \omega x) |x\rangle$. This gives the equation:

$$F^{-1}|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \exp(2\pi i \omega x) \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \exp\left(-\frac{2\pi i x y}{N}\right) |y\rangle = \sum_{y=0}^{N-1} \alpha_y |y\rangle \,,$$

where $\alpha_y = \frac{1}{N} \sum_{x=0}^{N-1} \exp(2\pi i \omega x) \exp\left(-\frac{2\pi i x y}{N}\right)$. We can simplify the expression for α_y using the product properties of exponentials:

$$\begin{aligned} \alpha_y &= \frac{1}{N} \sum_{x=0}^{N-1} \exp(2\pi i \Delta x) \quad \text{where} \quad \Delta \doteq |\omega - \frac{y}{N}|_{\mathbb{T}} \\ &= \frac{1}{N} \sum_{x=0}^{N-1} r^x \quad \text{where} \quad r \doteq \exp(2\pi i \Delta). \end{aligned} \tag{13}$$

If $r = 1$, then the right-hand side of (13) is an arithmetic and equals 1. Since $\Delta \in [0, 1/2]$, we have that $r = 1$ iff $\Delta = 0$ iff $\omega = \frac{y^*}{N}$ for some $y^* \in \mathbb{Z}_N$. In this case, $\alpha_{y^*} = 1$, and we are guaranteed to

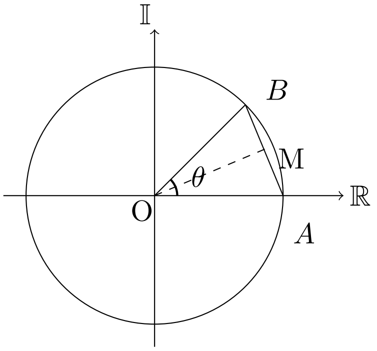


Figure 2: Geometric interpretation of $|A - B|$ where $A = 1$ and $B = \exp(i\theta)$.

observe y^*. Otherwise, we have a geometric sum with ratio $r \neq 1$ and

$$\alpha_y = \frac{1}{N} \cdot \frac{1 - r^N}{1 - r} = \frac{1}{N} \cdot \frac{1 - \exp(2\pi i \Delta N)}{1 - \exp(2\pi i \Delta)}.$$

Our goal is now to show that the weight of the bad y's is small, i.e. $\sum_{\text{bad } y} |\alpha_y|^2$ is small, where a y is considered bad if $|\omega - \frac{y}{N}|_{\mathbb{T}} > \delta$. Recall the double angle identity: $\cos(\theta) = \cos^2(\theta/2) - \sin^2(\theta/2) = 1 - 2\sin^2(\theta/2)$. We have:

$$\begin{aligned} |1 - \exp(i\theta)| &= |1 - \cos(\theta) - i\sin(\theta)| \\ &= \sqrt{(1 - \cos(\theta))^2 + \sin^2(\theta)} \\ &= \sqrt{1 - 2\cos(\theta) + \cos^2(\theta) + \sin^2(\theta)} \\ &= \sqrt{2(1 - \cos(\theta))} \\ &= \sqrt{4\sin^2(\theta/2)} && \text{[double angle identity]} \\ &= 2|\sin(\theta/2)|. \end{aligned}$$

Geometrically, we can obtain the result as follows: In Figure 2, $|1 - \exp(i\theta)|$ is given by the distance of the line segment AB. To compute this distance, we can draw a perpendicular to the segment of the circle. This perpendicular line makes an angle $\theta/2$ with the x-axis and intersects the segment at the midpoint M. In the right-triangle OMB, the side MB is given by $\sin(\theta/2)$. This gives us the length of AB as $2\sin(\theta/2)$. Therefore $|1 - \exp(i\theta)| = 2|\sin(\theta/2)|$.

Thus, we have that

$$|\alpha_y| = \frac{1}{N} \cdot \frac{|\sin(\pi \Delta N)|}{|\sin(\pi \Delta)|}.$$

We now want to bound from below the weight $|\alpha_{y^*}|^2$ of y^*, where y^*/N is the best approximation of ω, and bound from above the total weight of the bad y's. Before doing so, we bound $\sin(\theta)$ from above and below using the convexity of the sine function on the interval $[0, \pi]$.

- For the upper bound, we note that the tangent always stays above a convex function. In particular, $\sin(\theta) \leq \theta$ for all $\theta \in [0, \pi]$.

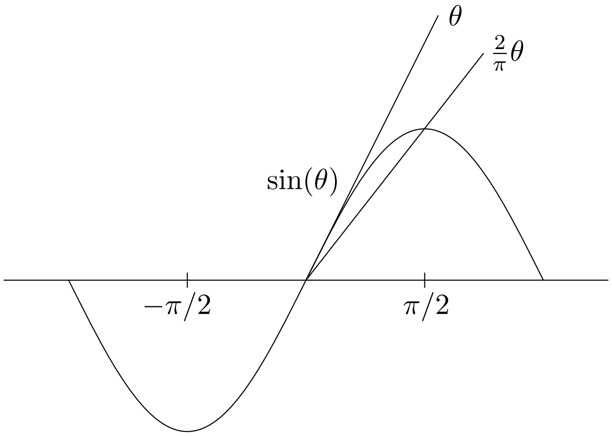


Figure 3: Plot for bounding $\sin(\theta)$.

- For the lower bound, we note that a chord always stays below a convex function. In particular, $\sin(\theta) \geq \frac{2}{\pi}\theta$ for all $\theta \in [0, \frac{\pi}{2}]$, as can be seen in Figure 3. The equation of the chord ($y = \frac{2}{\pi}\theta$) is the equation of line connecting the origin and $\theta = \sin\frac{\pi}{2}$.

Bounding weight of optimal y from below. We use these bounds for the sine function to get lower bounds for $|\alpha_{y^*}|_{\mathbb{T}}$, where y^* is the best approximation of ω. We obtain our lower bound by combining the lower bound for the sine of the numerator with the upper bound for the sine of the denominator. Note that there has to exist an integer y such that $|\omega - \frac{y}{N}| \leq \frac{1}{2N}$. It follows that $\Delta \doteq |\omega - \frac{y^*}{N}|_{\mathbb{T}} \leq \frac{1}{2N}$, so our lower bound for $\sin(\theta)$ applies to $\theta = \pi\Delta N \in [0, \pi/2]$. The argument $\pi\Delta$ for the upper bound certainly is in the allowed range $[0, \pi]$. We obtain:

$$|\alpha_{y^*}| \geq \frac{1}{N} \cdot \frac{2\pi\Delta N/\pi}{\pi\Delta} = \frac{2}{\pi}.$$

Note that α_{y^*} is the amplitude to observe y^* when we measure $\tilde{\omega}$. Thus, the probability of observing the optimal y^* is at least $|\alpha_{y^*}|^2 \geq \left(\frac{2}{\pi}\right)^2 = \frac{4}{\pi^2}$, which is about 40%. We also note that there could be two values that achieve this bound. Due to this, we cannot hope to have the probability of observing a particular y^* to exceed 50%.

Bounding total weight of bad y from above. For any y we have

$$|\alpha_y| = \frac{1}{N} \cdot \frac{|\sin(\pi\Delta N)|}{|\sin(\pi\Delta)|} \leq \frac{1}{N} \cdot \frac{1}{|\sin(\pi\Delta)|} \leq \frac{1}{N} \cdot \frac{1}{2\Delta} = \frac{1}{2\Delta N},$$

where the last inequality holds by our lower bound for sine applied to the angle $\theta = \pi\Delta$, which is in the allowed range $[0, \pi/2]$. Bad y's are the ones for which $\Delta \geq \delta$, or equivalently, $|\omega N - y|_{\mathbb{T}} \doteq \Delta N \geq \delta N$. The range of those y's can be split based on whether $\frac{y}{N}$ is closer to ω or to $\omega \pm 1$. In either range, the values of ΔN all differ by at least 1 and are at least δN. It follows that

$$\sum_{\text{bad } y} |\alpha_y|^2 \leq \sum_{\text{bad } y} \frac{1}{(2\Delta N)^2} \leq 2 \sum_{k \geq \lceil \delta N \rceil} \frac{1}{(2k)^2} = \frac{1}{2} \sum_{k \geq \lceil \delta N \rceil} \frac{1}{k^2}.$$

The series can in turn be bounded from above by an integral:

$$\sum_{k \geq \lceil \delta N \rceil} \frac{1}{k^2} \leq \int_{\delta N - 1}^{\infty} \frac{1}{x^2} dx = \frac{1}{\delta N - 1} = O(1/(\delta N)).$$

We conclude that $\epsilon = O(1/(\delta N))$, or equivalently, $\epsilon\delta = O(1/N)$, where ϵ is the odds of observing a bad y, which is what we wanted to prove.

Putting all of this together, we have:

Theorem 1. *If $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_0^{N-1} \exp(2\pi i \omega x) |x\rangle$ for unknown ω, then the odds of observing y^* for $|\frac{y^*}{N} - \omega|_{\mathbb{T}}$ minimal is at least $\frac{4}{\pi^2}$, and the odds of observing some y such that $|\frac{y}{N} - \omega|_{\mathbb{T}} \geq \delta$ for some specified δ is at most $\frac{1}{2(\delta N - 1)} = O(1/\delta N)$.*

3 Eigenvalue estimation

Eigenvalue estimation is a special case of phase estimation, where the phase derives from the eigenvalue of a unitary operator U. Note that all eigenvalues λ of U have absolute value 1 and can therefore be written as $\lambda = \exp(2\pi i \omega)$ for some $\omega \in [0, 1)$. We discuss the general problem of eigenvalue estimation in this lecture and develop some interesting applications next lecture.

3.1 Problem statement

We start by defining the problem. Like for phase estimation, the output could be either classical or a quantum superposition.

Input: A unitary operation U on n qubits, e.g., in the form of a unitary circuit, and an eigenstate $|\phi\rangle$ of U, i.e., a state such that $U|\phi\rangle = \lambda|\phi\rangle$, where $\lambda = \exp(2\pi i \omega)$ for some $\omega \in [0, 1)$. Also an accuracy parameter $\delta > 0$.

Classical output: A good approximation to ω, namely $\tilde{\omega}$ such that $|\omega - \tilde{\omega}|_{\mathbb{T}} \leq \delta$.

Quantum output: Pure state $|\tilde{\omega}\rangle$ with "most" weight on good approximations to ω.

This is very similar to phase estimation, except that we are given an eigenstate $|\phi\rangle$ rather than a harmonic state.

3.2 Algorithm

Our algorithm consists of creating a harmonic state $|\psi\rangle$ with the same phase as the eigenvalue of λ and then apply phase estimation to $|\psi\rangle$.

As n is already in use for the number of qubits of the eigenvector $|\phi\rangle$, we use m to denote the number of qubits of the harmonic state $|\psi\rangle$. We create $|\psi\rangle$ as follows:

- Initialize the register for $|\psi\rangle$ to $|0^m\rangle$. The initial state of the combined system is $|0^m\rangle|\phi\rangle$.
- Apply $H^{\otimes m}$ to the first register to put it in a uniform superposition: $\frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |x\rangle|\phi\rangle$.
- Use the first register as a control to apply U a number of times to the second register: $\frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |x\rangle U^x |\phi\rangle$

In summary, we have the following process:

$$|0^m\rangle\,|\phi\rangle \to \frac{1}{\sqrt{M}}\sum_{x=0}^{M-1}|x\rangle\,|\phi\rangle \to \frac{1}{\sqrt{M}}\sum_{x=0}^{M-1}|x\rangle\,U^x\,|\phi\rangle$$

For the rationale behind this, we observe that applying U x times to $|\phi\rangle$ is, as $|\phi\rangle$ is an eigenstate, equivalent to a phase shift of $\lambda^x = \exp(2\pi i\omega x)$. This gives us:

$$\frac{1}{\sqrt{M}}\sum_{x=0}^{M-1}\exp(2\pi i\omega x)\,|x\rangle\,|\phi\rangle \doteq |\psi\rangle\,|\phi\rangle\,.$$

Ignoring the $|\phi\rangle$ yields a harmonic state with frequency ω. Wen then apply phase estimation to $|\psi\rangle$: $|\psi\rangle\,|\phi\rangle \to |\tilde{\omega}\rangle\,|\phi\rangle$

Note that $|\phi\rangle$ has not been affected and works as a catalyst in this process. The final state we get is equivalent to the tensor product of $|\tilde{\omega}\rangle$ and $|\phi\rangle$. There is no entanglement between the two registers.

Here is the circuit obtained:

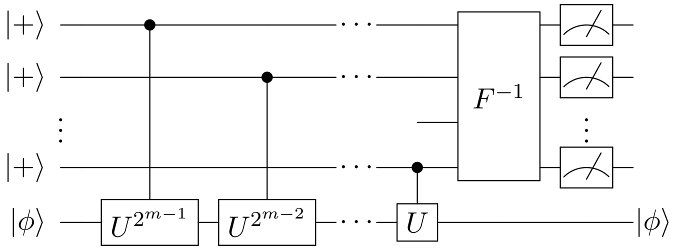


Figure 4: Eigenvalue estimation circuit. The i^{th} highest order bit controls $U^{2^{m-i}}$.

3.3 Analysis

Our analysis of phase estimation yields the following in terms of accuracy:

- The weight of the $y^* \in \mathbb{Z}_m$ with $|\omega - \frac{y^*}{M}|_{\mathbb{T}} \leq \frac{1}{2M}$ is at least $\frac{4}{\pi^2}$.
- The total weight of the $y \in \mathbb{Z}_m$ with $|\omega - \frac{y}{M}|_{\mathbb{T}} \geq \delta$ is $O(\frac{1}{\delta M})$. As such, we can get roughly m bits of accuracy with constant probability.

If the confidence level is not sufficient, we can boost it by increasing M or by running the process multiple times with the same M, and then select the median or, as we know the the best approximation occurs with probability above 40%, the result that appears most often, Running the process multiple times is possible because after measuring register $|\tilde{\omega}\rangle$, the register $|\phi\rangle$ remains intact, so we can reuse it in subsequent runs for boosting the confidence.

In terms of efficiency, we can apply a Fourier transform in time $\operatorname{poly}\log(M)$ (i.e., polynomial in m). Applying high powers (up to M) of U can be more time consuming, and the efficiency of the whole process is typically dictated by this part (computing powers of U).

Applying the process to an arbitrary state. In the problem statement of eigenvalue estimation, we are directly given an eigenstate of U, namely $|\phi\rangle$. What if we apply our algorithm to an arbitrary input state $|\varphi\rangle$?

Since U is a unary operator, it has a full orthonormal basis of eigenstates: $|\varphi\rangle = \sum_j \alpha_j |\phi_j\rangle$ where $U|\phi_j\rangle = \exp(2\pi i\omega_j)||\phi_j\rangle$ for $\omega_j \in [0, 1)$. We can write $|\varphi\rangle$ as a linear combination of the eigenstates: $|\varphi\rangle = \sum_j \alpha_j |\phi_j\rangle$. Note that we may not know the coefficients α_j, but they must exist and can be used for analysis purposes. By linearity of the underlying unitary quantum circuit:

$$|0^m\rangle |\varphi\rangle = \sum_j \alpha_j |0^m\rangle |\phi_j\rangle \to \sum_j \alpha_j |\tilde{\omega}_j\rangle |\phi_j\rangle .$$

Measuring the first register of the two-register system in state $\sum_j \alpha_j |\tilde{\omega}_j\rangle |\phi_j\rangle$ has the same distribution as picking j with probability $|\alpha_j|^2$ and then measuring $|\tilde{\omega}_j\rangle$. Next lecture we will see how we can use samples from this distribution.