**MAT 4930: Quantum Algorithms and Complexity** **Spring 2021**

# Lecture 10: The Quantum Phase Estimation Algorithm

*Lecturer: Jean-François Biasse* *TA: Robert Hart*



## 10.1 The quantum phase estimation problem

**Definition 10.1 (Quantum phase estimation problem)** *Given the input state*

$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2i\pi\omega y} |y\rangle ,$$

*compute the phase $\omega$.*

There are two different cases for this problem:

- $\omega = \frac{x}{2^n}$ for some $x \in \mathbb{Z}$.
- $\omega \in \mathbb{R}$ arbitrary.

The former is easier to deal with than the latter. In this section, we focus on this easy case to introduce the problem, and we defer to Section 10.4 for the case $\omega \in \mathbb{R}$. In the following, we denote by $0.x_1x_2\ldots x_{n-1}$ the phase $\frac{x}{2^n}$ where $x \in \mathbb{Z}_{>0}$ is an $n-1$-bit integer. We can always assume $x < 2^n$, as otherwise the integer part of $\frac{x}{2^n}$ factors out as a global phase. In the simplest case, the phase is of the form $\omega = 0.x_1$. This means that

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + (-1)^{x_1} |1\rangle\right).$$

If we apply the 1-qubit Hadamard gate to $|\psi\rangle$, we get two possible outcomes depending on the value of $x_1 \in \{0, 1\}$:

- $\frac{H}{\sqrt{2}} (|0\rangle + |1\rangle) = |0\rangle$,
- $\frac{H}{\sqrt{2}} (|0\rangle - |1\rangle) = |1\rangle$.

In each case, we have that $H|\psi\rangle = |x_1\rangle$. Thus, after measuring the output qubit, we learn $\omega$.

## 10.2 Controlled rotation gates

Our second example of the resolution of the phase estimation algorithm is when $n = 2$. In this case, $\omega = 0.x_1x_2$ and the input state is

$$|\psi\rangle = \frac{1}{2} \sum_{y=0}^{y=3} e^{2i\pi\omega y} |y\rangle = \underbrace{\left(\frac{|0\rangle + 2^{2\pi i(0.x_2)} |1\rangle}{\sqrt{2}}\right)}_{\text{first qubit}} \otimes \underbrace{\left(\frac{|0\rangle + 2^{2\pi i(0.x_1x_2)} |1\rangle}{\sqrt{2}}\right)}_{\text{second qubit}}.$$

As before, the Hadamard gate on the first qubit, which is in the state $\frac{|0\rangle + 2^{2\pi i(0.x_2)}|1\rangle}{\sqrt{2}}$ directly yields $|x_2\rangle$. Then, to compute $x_1$, we need to consider two cases

1. $x_2 = 0$,
2. $x_2 = 1$.

1) When $x_2 = 0$, then second qubit is in the state $\frac{|0\rangle + 2^{2\pi i(0.x_1)}|1\rangle}{\sqrt{2}}$. Therefore, applying a Hadamard gate yields $|x_1\rangle$.
2) When $x_2 = 1$, we first apply the inverse of the rotation gate defined by

$$R_2 := \begin{pmatrix} 1 & 0 \\ 0 & 2^{\frac{2\pi i}{4}} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i(0.01)} \end{pmatrix}.$$

We can see that $R_2^{-1}\left(\frac{|0\rangle + 2^{2\pi i(0.x_1 1)}|1\rangle}{\sqrt{2}}\right) = \frac{|0\rangle + 2^{2\pi i(0.x_1)}|1\rangle}{\sqrt{2}}$. Then like in 1), the Hadamard gate yields the state $|x_1\rangle$. This is summarized in Figure 10.1

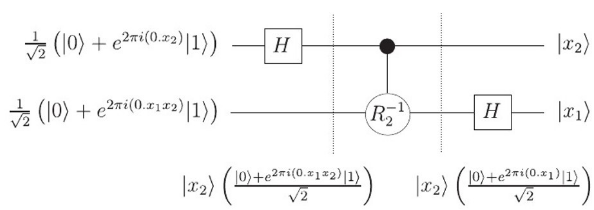



Figure 10.1: 2-qubit quantum phase estimation

The gate $R_2$ is a special of a family of rotation gates that have the form

$$R_z(\theta) = \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix} = e^{-i\theta/2}\begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$

In our case, $R_2 \sim R_z(\pi/2)$ (remember that we use $\sim$ to denote the property "is equal modulo a global phase"). We denote

$$R_k := \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^k}} \end{pmatrix} \sim R_z\left(\frac{2\pi i}{2^k}\right).$$

In general, rotation gates are not part of the Clifford+T gate set, but we know from the Solovay-Kitaev theorem that we can approximate them with an $\varepsilon$ precision by a product of Clifford + T gates of length $\log^c(1/\varepsilon)$ for some constant $c > 0$.

**Example 1 (N. Ross 2014)** *Let* $S = T^4$, *and*

$$\begin{aligned}\hat{U} = {} & HTSHTSHTSHTHTHTHTSHTHTSHTSHTSHTHTHTSHTSHTHTHTSHTHTSHTHT \\ & HTHTHTHTHTSHTSHTSHTHTSHTHTSHTHTHTHTSHTHTHTSHTHTSHTHTHTHTS \\ & HTSHTSHTHTHTSHTSHTSHTSHTHTSHTSHTSHTSHTHTSHTHTSHTSHTHTHTHT \\ & HTSHTHTHTHTSHTSHTSHTHTSHTSHTHTHTSHTHTHTHTHTSHTSHTHTHTHTHT \\ & SHTHTHTHTSHTHTHTHTHTHTH\end{aligned}$$

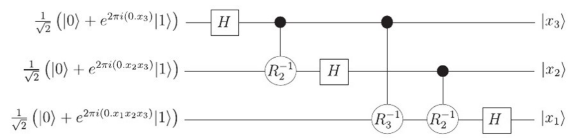
*satisfies* $\|R_z(\pi/128) - \hat{U}\| \leq \frac{1}{10^{-10}}$.

## 10.3 The Quantum Fourier Transform (QFT)

The construction of Section 10.4 to solve the phase estimation problem in cases where $\omega = \frac{x}{2^n}$ for arbitrary $n$. We rely on the fact that

$$\frac{1}{\sqrt{2^n}}\sum_{y=0}^{2^n-1}|y\rangle = \left(\frac{|0\rangle + 2^{2\pi i(0.x_n)}|1\rangle}{\sqrt{2}}\right)\otimes\left(\frac{|0\rangle + 2^{2\pi i(0.x_{n-1}x_n)}|1\rangle}{\sqrt{2}}\right)\otimes\ldots\otimes\left(\frac{|0\rangle + 2^{2\pi i(0.x_1\ldots x_n)}|1\rangle}{\sqrt{2}}\right)$$

**Example 2 (Case $n = 3$)** *The when $\omega = x/8$, we can solve the phase estimation problem with the following circuit:*




The circuit that solves the phase estimation problem when $\omega = x/2^n$ does the following operation:

$$\frac{1}{\sqrt{2^n}}\sum_{y=0}^{2^n-1} e^{\frac{2i\pi xy}{2^n}}|y\rangle \longmapsto |x\rangle\,.$$

**Definition 10.2 (Quantum Fourier Transform (QFT))** *The QFT circuit is the inverse of the circuit that solves the phase estimation problem for $\omega = x/2^n$, i.e. it does:*

$$|x\rangle \longmapsto \frac{1}{\sqrt{2^n}}\sum_{y=0}^{2^n-1} e^{\frac{2i\pi xy}{2^n}}|y\rangle\,.$$

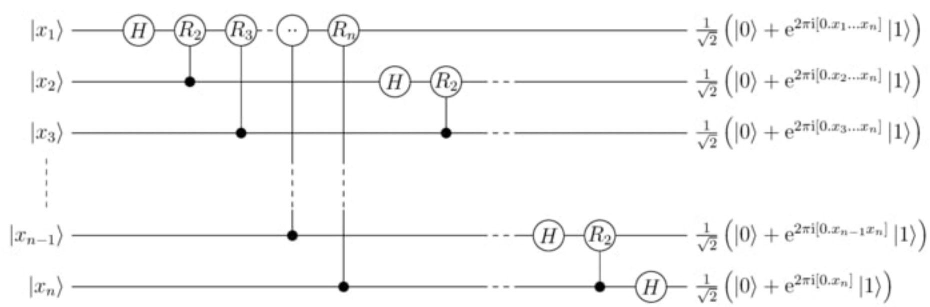



Figure 10.2: Quantum Fourier Transform circuit

**Proposition 10.3** *The action of the inverse of the QFT on basis states is given by*

$$\mathrm{QFT}_m^{-1} : |x\rangle \longmapsto \frac{1}{\sqrt{2^n}}\sum_{y=0}^{2^n-1} e^{-\frac{2i\pi xy}{2^n}}|y\rangle\,.$$

The notion of QFT can be extended to finite groups (in particular $G = \mathbb{Z}/N\mathbb{Z}$). The above would correspond to $G = \mathbb{Z}/2^n\mathbb{Z}$.

## 10.4 Arbitrary phase estimation

In this section, we assume that $\omega$ is not necessarily of the form $\frac{x}{2^n}$. For a given $n$, we want to find $x \in \mathbb{Z}$ such that $\frac{x}{2^n}$ is the closest to $\omega$. Our input state is $|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2i\pi\omega y} |y\rangle$, and the action of the inverse of $\mathrm{QFT}_{2^n}$ is given by

$$\begin{aligned}\mathrm{QFT}_{2^n}^{-1} |\psi\rangle &= \frac{1}{2^n} \sum_{y=0}^{2^n-1} e^{2i\pi\omega y} \left( \sum_{k=0}^{2^n-1} e^{\frac{-2i\pi ky}{2^n}} |k\rangle \right) \\ &= \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{k=0}^{2^n-1} e^{\frac{2i\pi(x-k)y}{2^n}} e^{2i\pi\delta y} |k\rangle ,\end{aligned}$$

where $x = \lfloor 2^n\omega \rceil$ is the nearest integer to $2^n\omega$ and $\delta := \omega - \frac{x}{2^n}$ (which means that $0 \leq |2^n\delta| \leq \frac{1}{2}$). Unless otherwise stated, results regarding measurement probabilities after the action of $\mathrm{QFT}_{2^m}$ (or its inverse) assume that controlled rotation gates are implemented with infinite precision. If needed, we can specify the degree of precision to which $\mathrm{QFT}_{2^m}$ is implemented from the precision to which the rotations are implemented.

**Proposition 10.4** *After applying* $\mathrm{QFT}_{2^n}^{-1}$ *to* $|\psi\rangle$*, the probability of measuring* $x = \lfloor 2^n\omega \rceil$ *is*

- $1$ *if* $\delta = 0$.
- $\frac{1}{2^{2n}} \left| \frac{1-e^{2i\pi 2^n\delta}}{1-2^{2i\pi\delta}} \right|^2$ *otherwise.*

**Proof:** The probability of measuring $x$ is

$$\Pr(\text{Measure } x) = \left| \langle x| \, \mathrm{QFT}_{2^n}^{-1} |\psi\rangle \right|^2 = \frac{1}{2^n} \left| \sum_{y=0}^{2^n-1} 2^{2i\pi\delta y} \right|^2 .$$

If $\delta = 0$, this equals 1, otherwise, it is the sum of the first $2^n$ consecutive terms of a geometric series of ratio $e^{2i\pi\delta}$, hence the result. ■

**Proposition 10.5** *The probability of measuring* $x$ *satisfies*

$$\Pr(\textit{Measure } x) \geq \frac{4}{\pi^2}$$

**Proof:** When $\delta \neq 0$, we have that

$$\Pr(\text{Measure } x) == \frac{1}{2^{2n}} \left| \frac{1 - e^{2i\pi 2^n\delta}}{1 - 2^{2i\pi\delta}} \right|^2 = \frac{1}{2^{2n}} \frac{|\sin(\pi 2^n\delta)|^2}{|\sin(\pi\delta)|^2}.$$

Moreover, $|\delta| \leq \frac{1}{2^{n+1}}$, therefore $|2 \cdot 2^n\delta| \leq |\sin(\pi 2^n\delta)|$ and

$$\Pr(\text{Measure } x) \geq \frac{4}{\pi^2} \geq \frac{1}{2^n} \frac{|2 \cdot 2^n\delta|^2}{|\pi\delta|^2} = \frac{4}{\pi^2}.$$

■

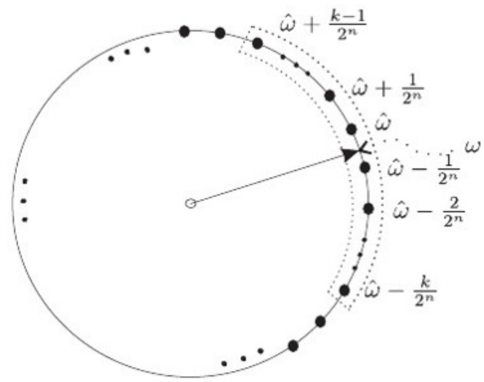



Figure 10.3: Representation of $\omega$ on a circle

This procedure is illustrated in Figure 10.3. To accurately measure the probability of success of the phase estimation algorithm, one needs to take into account the precision to which the controlled-rotations are implemented. From the Solovay-Kitaev result, we know that we can efficiently implemented these gates to an arbitrary degree of precision. Then, given this precision, we need to assess the precision of the resulting approximate QFT over $n$ bits.

**Proposition 10.6** *Let $p$ be a polynomial and assume that the controlled rotation gates are implemented with precision $\varepsilon = \frac{1}{p(n)}$. We denote by $\mathrm{QFT}_n$ the QFT over $n$ bits and by $\widetilde{\mathrm{QFT}}_n$ the approximation resulting from the use of the approximate controlled rotations. Then we have*

$$\max_{|\psi\rangle} \left\| \left( \mathrm{QFT}_n - \widetilde{\mathrm{QFT}}_n \right) |\psi\rangle \right\| \in O\left( \frac{n^2}{p(n)} \right).$$

**Proof:** As a homework assignment. ■

This means that if $p(n)$ has degree at least 3, the resulting approximate QFT is asymptotically precise. This result also applies to inverses.