

Quantum Algorithms tutorial 5

Quantum counting and Quantum phase estimation



Casper Gyurik

Leiden Institute of Advanced Computer Science
October 10th, 2019



**Universiteit
Leiden**
The Netherlands

Quantum phase estimation

Quantum Counting

Quantum phase estimation

The problem

Let U be an n -qubit unitary transformation.

- ▶ A vector $|u\rangle$ is an *eigenvector* of U with eigenvalue $\omega_u \in \mathbb{C}$ if

$$U |u\rangle = \omega_u |u\rangle .$$

Quantum phase estimation

The problem

Let U be an n -qubit unitary transformation.

- ▶ A vector $|u\rangle$ is an *eigenvector* of U with eigenvalue $\omega_u \in \mathbb{C}$ if

$$U |u\rangle = \omega_u |u\rangle .$$

- ▶ Turns out that because U is unitary we can write $\omega_u = e^{i2\pi\phi_u}$, for some so-called *eigenphase* $\phi_u \in [0, 1)$.

Quantum phase estimation

The problem

Let U be an n -qubit unitary transformation.

- ▶ A vector $|u\rangle$ is an *eigenvector* of U with eigenvalue $\omega_u \in \mathbb{C}$ if

$$U|u\rangle = \omega_u |u\rangle.$$

- ▶ Turns out that because U is unitary we can write $\omega_u = e^{i2\pi\phi_u}$, for some so-called *eigenphase* $\phi_u \in [0, 1)$.

Phase estimation

Given an eigenvector $|u\rangle$ of U , output a t -bit approximation

$$\bar{\phi} = 0.\phi_1 \dots \phi_t, \phi_j \in \{0, 1\},$$

of the the corresponding eigenphase $\phi_u \in [0, 1)$.

Quantum phase estimation

The problem

Let U be an n -qubit unitary transformation.

- ▶ A vector $|u\rangle$ is an *eigenvector* of U with eigenvalue $\omega_u \in \mathbb{C}$ if

$$U|u\rangle = \omega_u|u\rangle.$$

- ▶ Turns out that because U is unitary we can write $\omega_u = e^{i2\pi\phi_u}$, for some so-called *eigenphase* $\phi_u \in [0, 1)$.

Phase estimation

Given an eigenvector $|u\rangle$ of U , output a t -bit approximation

$$\bar{\phi} = 0.\phi_1 \dots \phi_t, \phi_j \in \{0, 1\},$$

of the the corresponding eigenphase $\phi_u \in [0, 1)$.

Here the t -bit approximation is given by the first t -bits of the binary expansion

$$\phi = \sum_{j=1}^{\infty} \phi_j 2^{-j}.$$

Quantum phase estimation

The problem

Let U be an n -qubit unitary transformation.

- ▶ A vector $|u\rangle$ is an *eigenvector* of U with eigenvalue $\omega_u \in \mathbb{C}$ if

$$U|u\rangle = \omega_u|u\rangle.$$

- ▶ Turns out that because U is unitary we can write $\omega_u = e^{i2\pi\phi_u}$, for some so-called *eigenphase* $\phi_u \in [0, 1)$.

Phase estimation

Given an eigenvector $|u\rangle$ of U , output a t -bit approximation

$$\bar{\phi} = 0.\phi_1 \dots \phi_t, \phi_j \in \{0, 1\},$$

of the the corresponding eigenphase $\phi_u \in [0, 1)$.

Here the t -bit approximation is given by the first t -bits of the binary expansion

$$\phi = \sum_{j=1}^{\infty} \phi_j 2^{-j}.$$

Phase estimation solves not only physically interesting problems, but other interesting problems can be reduced to it (see exercises for an example).

Quantum phase estimation

The algorithm

Turns out that phase estimation can be efficiently solved using the QFT.

The quantum phase estimation (QPE) procedure

1. Start with $|0^t\rangle |u\rangle$.
2. Apply $H^{\otimes n} \otimes I$.
3. Apply the map $|j\rangle |\psi\rangle \mapsto |j\rangle U^j |\psi\rangle$, using controlled- U^j gates.
4. Apply the inverse Fourier transform to the first t qubits and measure result.

Note: the above procedure requires one to prepare (a state related to) $|u\rangle$.

Quantum phase estimation

The algorithm

Turns out that phase estimation can be efficiently solved using the QFT.

The quantum phase estimation (QPE) procedure

1. Start with $|0^t\rangle |u\rangle$.
2. Apply $H^{\otimes n} \otimes I$.
3. Apply the map $|j\rangle |\psi\rangle \mapsto |j\rangle U^j |\psi\rangle$, using controlled- U^j gates.
4. Apply the inverse Fourier transform to the first t qubits and measure result.

Note: the above procedure requires one to prepare (a state related to) $|u\rangle$.
Let us track the state of the quantum computer through the steps.

$$\begin{aligned} |0^t\rangle |u\rangle &\xrightarrow{2.} \frac{1}{\sqrt{2^t}} \sum_{j \in \{0,1\}^t} |j\rangle |u\rangle \xrightarrow{3.} \frac{1}{\sqrt{2^t}} \sum_{j \in \{0,1\}^t} |j\rangle U^j |u\rangle = \frac{1}{\sqrt{2^t}} \sum_{j \in \{0,1\}^t} e^{2\pi i \phi_u \text{dec}(j)} |j\rangle |u\rangle \\ &\xrightarrow{4.} |\bar{\phi}_u\rangle |u\rangle \rightsquigarrow \bar{\phi}_u. \end{aligned}$$

Quantum phase estimation

The algorithm

Turns out that phase estimation can be efficiently solved using the QFT.

The quantum phase estimation (QPE) procedure

1. Start with $|0^t\rangle |u\rangle$.
2. Apply $H^{\otimes n} \otimes I$.
3. Apply the map $|j\rangle |\psi\rangle \mapsto |j\rangle U^j |\psi\rangle$, using controlled- U^j gates.
4. Apply the inverse Fourier transform to the first t qubits and measure result.

Note: the above procedure requires one to prepare (a state related to) $|u\rangle$.
Let us track the state of the quantum computer through the steps.

$$\begin{aligned} |0^t\rangle |u\rangle &\stackrel{2.}{\mapsto} \frac{1}{\sqrt{2^t}} \sum_{j \in \{0,1\}^t} |j\rangle |u\rangle \stackrel{3.}{\mapsto} \frac{1}{\sqrt{2^t}} \sum_{j \in \{0,1\}^t} |j\rangle U^j |u\rangle = \frac{1}{\sqrt{2^t}} \sum_{j \in \{0,1\}^t} e^{2\pi i \phi_u \text{dec}(j)} |j\rangle |u\rangle \\ &\stackrel{4.}{\mapsto} |\bar{\phi}_u\rangle |u\rangle \rightsquigarrow \bar{\phi}_u. \end{aligned}$$

Note: Accuracy determined by size of first register and powers of U in step 3.

Quantum phase estimation

The circuit

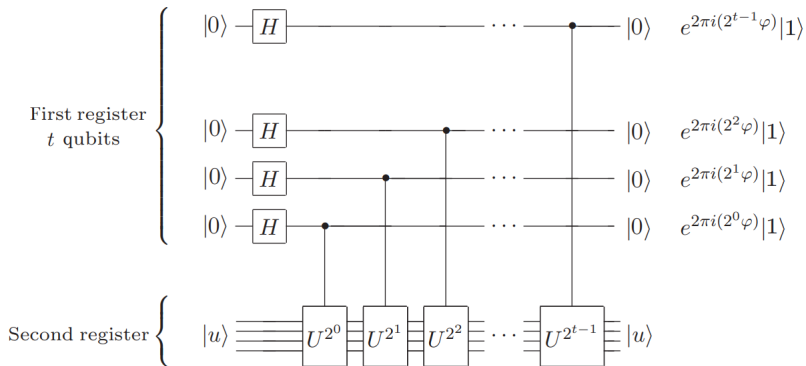


Figure: Taken from Nielsen and Chuang, Section 5.2

Afterwards, the QFT recovers the bits of $\bar{\phi}_u$ from the phases $e^{2\pi i\phi_u 2^k}$.

Quantum counting

The problem

The counting problem

Given oracle access to a function $f : \{0, 1\}^n \rightarrow \{0, 1\}$. Count the number of bitstrings $j \in \{0, 1\}^n$, such that $f(j) = 1$ (these bitstrings are called *solutions*).

Quantum counting

The problem

The counting problem

Given oracle access to a function $f : \{0, 1\}^n \rightarrow \{0, 1\}$. Count the number of bitstrings $j \in \{0, 1\}^n$, such that $f(j) = 1$ (these bitstrings are called *solutions*).

- ▶ Abstraction of counting the number of solutions to a problem.
 - ▶ E.g., f checks whether a bitstring is a clique in an n -vertex graph.

Quantum counting

The problem

The counting problem

Given oracle access to a function $f : \{0, 1\}^n \rightarrow \{0, 1\}$. Count the number of bitstrings $j \in \{0, 1\}^n$, such that $f(j) = 1$ (these bitstrings are called *solutions*).

- ▶ Abstraction of counting the number of solutions to a problem.
 - ▶ E.g., f checks whether a bitstring is a clique in an n -vertex graph.
- ▶ Also allows us to decide whether a solution exists or not.

Quantum counting

The problem

The counting problem

Given oracle access to a function $f : \{0, 1\}^n \rightarrow \{0, 1\}$. Count the number of bitstrings $j \in \{0, 1\}^n$, such that $f(j) = 1$ (these bitstrings are called *solutions*).

- ▶ Abstraction of counting the number of solutions to a problem.
 - ▶ E.g., f checks whether a bitstring is a clique in an n -vertex graph.
- ▶ Also allows us to decide whether a solution exists or not.
- ▶ Classically, it takes $\Theta(N)$ queries to the oracle to solve the problem.

Quantum counting

The problem

The counting problem

Given oracle access to a function $f : \{0, 1\}^n \rightarrow \{0, 1\}$. Count the number of bitstrings $j \in \{0, 1\}^n$, such that $f(j) = 1$ (these bitstrings are called *solutions*).

- ▶ Abstraction of counting the number of solutions to a problem.
 - ▶ E.g., f checks whether a bitstring is a clique in an n -vertex graph.
- ▶ Also allows us to decide whether a solution exists or not.
- ▶ Classically, it takes $\Theta(N)$ queries to the oracle to solve the problem.
- ▶ On a quantum computer this can be done much more quickly by combining *Grover's algorithm* and the *quantum phase estimation procedure*.

Quantum counting

The algorithm

Quantum counting applies phase estimation to estimate the eigenvalues of the previously discussed Grover iterate

$$\mathcal{G} = H^{\otimes n} R H^{\otimes n} O_{f,\pm},$$

where R mapped $|0\rangle \mapsto |0\rangle$ and $|j\rangle \mapsto -|j\rangle$ for $j \neq 0^n$.

Quantum counting

The algorithm

Quantum counting applies phase estimation to estimate the eigenvalues of the previously discussed Grover iterate

$$\mathcal{G} = H^{\otimes n} R H^{\otimes n} O_{f,\pm},$$

where R mapped $|0\rangle \mapsto |0\rangle$ and $|j\rangle \mapsto -|j\rangle$ for $j \neq 0^n$.

- Turns out that $|U\rangle = H^{\otimes n} |0^n\rangle$ can be decomposed into eigenvectors of \mathcal{G} with eigenvalue either $e^{i\theta}$ or $e^{i(2\pi-\theta)}$, where for $M = |f^{-1}(1)|$

$$\sin^2(\theta/2) = M/2^{n+1}. \quad (1)$$

Quantum counting

The algorithm

Quantum counting applies phase estimation to estimate the eigenvalues of the previously discussed Grover iterate

$$\mathcal{G} = H^{\otimes n} R H^{\otimes n} O_{f,\pm},$$

where R mapped $|0\rangle \mapsto |0\rangle$ and $|j\rangle \mapsto -|j\rangle$ for $j \neq 0^n$.

- ▶ Turns out that $|U\rangle = H^{\otimes n} |0^n\rangle$ can be decomposed into eigenvectors of \mathcal{G} with eigenvalue either $e^{i\theta}$ or $e^{i(2\pi-\theta)}$, where for $M = |f^{-1}(1)|$

$$\sin^2(\theta/2) = M/2^{n+1}. \quad (1)$$

- ▶ Therefore, applying the quantum phase procedure to the state $|U\rangle$ will output an estimate of either θ or $2\pi - \theta$.

Quantum counting

The algorithm

Quantum counting applies phase estimation to estimate the eigenvalues of the previously discussed Grover iterate

$$\mathcal{G} = H^{\otimes n} R H^{\otimes n} O_{f,\pm},$$

where R mapped $|0\rangle \mapsto |0\rangle$ and $|j\rangle \mapsto -|j\rangle$ for $j \neq 0^n$.

- ▶ Turns out that $|U\rangle = H^{\otimes n} |0^n\rangle$ can be decomposed into eigenvectors of \mathcal{G} with eigenvalue either $e^{i\theta}$ or $e^{i(2\pi-\theta)}$, where for $M = |f^{-1}(1)|$

$$\sin^2(\theta/2) = M/2^{n+1}. \quad (1)$$

- ▶ Therefore, applying the quantum phase procedure to the state $|U\rangle$ will output an estimate of either θ or $2\pi - \theta$.
- ▶ Combining this estimate with Equation 1 allows us to obtain an estimate of M and even decide whether $M = 0$ or not.

Quantum counting

The algorithm

Quantum counting applies phase estimation to estimate the eigenvalues of the previously discussed Grover iterate

$$\mathcal{G} = H^{\otimes n} R H^{\otimes n} O_{f,\pm},$$

where R mapped $|0\rangle \mapsto |0\rangle$ and $|j\rangle \mapsto -|j\rangle$ for $j \neq 0^n$.

- ▶ Turns out that $|U\rangle = H^{\otimes n} |0^n\rangle$ can be decomposed into eigenvectors of \mathcal{G} with eigenvalue either $e^{i\theta}$ or $e^{i(2\pi-\theta)}$, where for $M = |f^{-1}(1)|$

$$\sin^2(\theta/2) = M/2^{n+1}. \quad (1)$$

- ▶ Therefore, applying the quantum phase procedure to the state $|U\rangle$ will output an estimate of either θ or $2\pi - \theta$.
- ▶ Combining this estimate with Equation 1 allows us to obtain an estimate of M and even decide whether $M = 0$ or not.

Quantum counting

The circuit

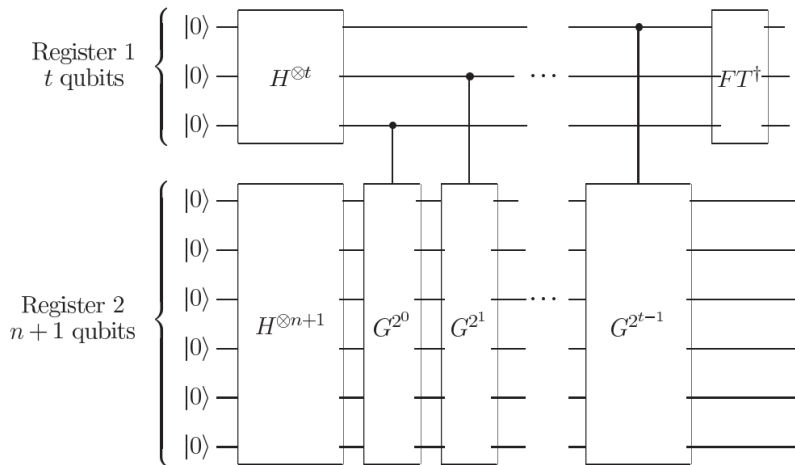


Figure: Taken from Nielsen and Chuang, Section 6.3