CSE 392: Matrix and Tensor Algorithms for Data

Instructor: Shashanka Ubaru

University of Texas, Austin

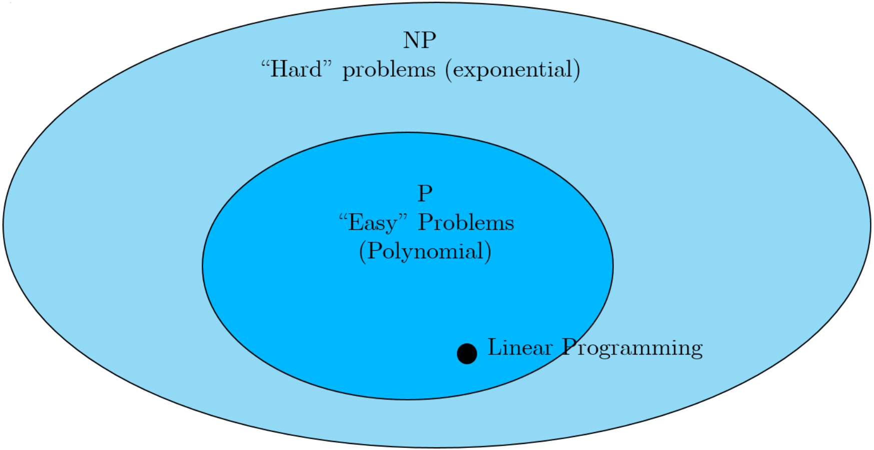
Spring 2024

Lecture 26: Introduction to quantum computing II

Outline

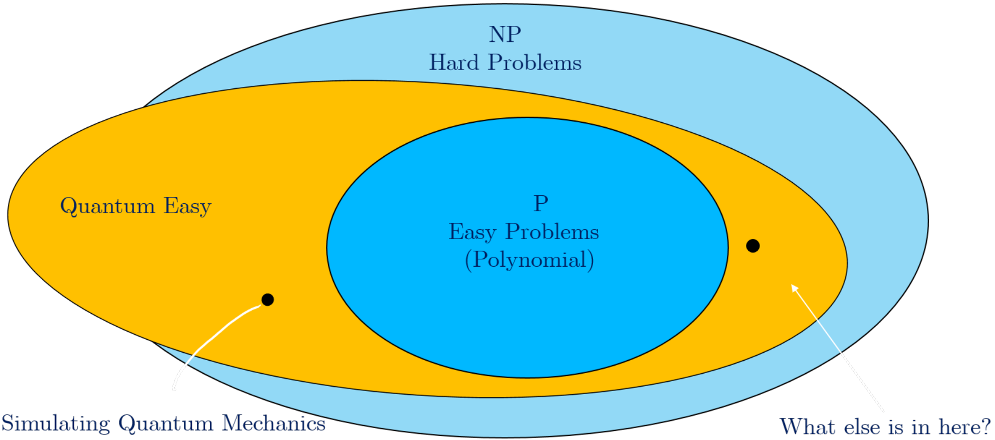
Complexity Classes

- There are many intractable problems where the best known algorithm has runtime that scales exponentially with input size

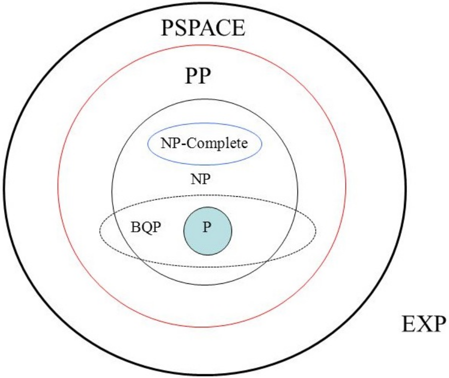


Complexity Classes

- Quantum Computers are the Only Novel Hardware which Changes the Game

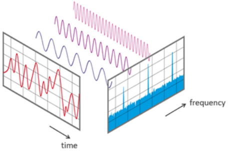


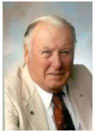
- **Should We Focus on NP-hard Problems ?**
  - Counter to the layman belief, there is a consensus among quantum computing researchers that quantum computing is not likely to exponentially speed-up computation of NP-hard problems [C.H. Bennett, E. Bernstein, G. Brassard, U. Vazirani, Strengths and Weaknesses of Quantum Computing, 1996]

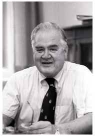


Fourier Transform - Background

- **Fourier Transform: Decomposes** a function or a signal in **one domain** (e.g. time) into its constituent **frequency** representation
- **Instrumental** in signal processing, image analysis, (convolutional) neural networks, etc
- Gilbert Strang described the FFT as **"the most important numerical algorithm of our lifetime"**
- Inducted in **Top** 10 **Algorithms of** 20^{th} **Century by the IEEE journal Computing in Science & Engineering**
- Classically, the Fast Fourier Transform (FFT) can perform the task in $N\log(N)$ run-time [**Cooley** and **Tukey**, 1965]
- Qunatumly, the Quantum Fast Fourier Transform (FFT) is due to [**Coppersmith**, 1994]



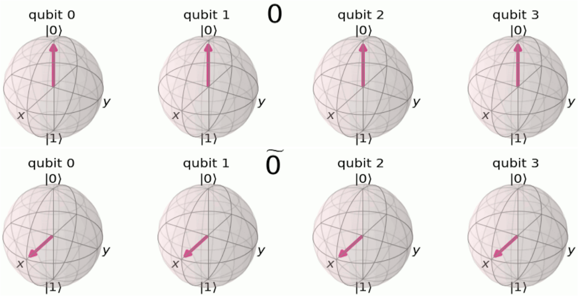




Quantum Fourier Transform

- Similarly to the **classical**, the **quantum Fourier Transform**, (QFT) performs a discrete Fourier transform on the complex valued vector $|\psi\rangle$, yet it can achieve runtime of $\mathcal{O}(n \log n)$
- **Given:** an n-qubit state as a superposition of basis states $|0\rangle, |1\rangle, \ldots, |2^n - 1\rangle$
- **Map** each basis state $|j\rangle$

$$QFT(|j\rangle) = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{\frac{2\pi i j k}{2^n}} |k\rangle$$



Quantum Fourier Transform

- **Notation: Fractional Binary Notation** :

$$[0.x_1 \dots x_m] = \sum_{k=1}^{m} x_k 2^{-k}$$

- For instance, $[0.x_1] = \frac{x_1}{2}$ and $[0.x_1 x_2] = \frac{x_1}{2} + \frac{x_2}{2^2}$
- With this notation, the action of the quantum Fourier transform can be expressed in a compact manner:

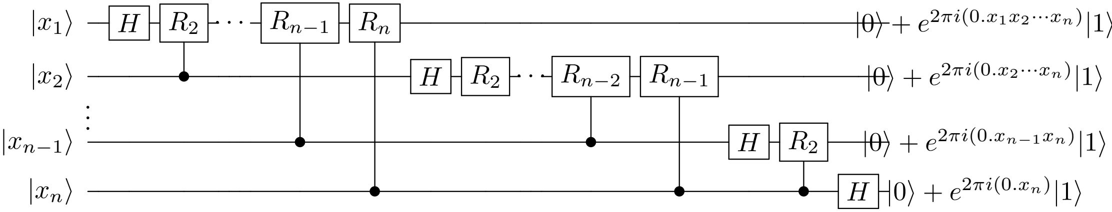
$$QFT(|x_1 x_2 \dots x_n\rangle) =$$
$$\frac{1}{\sqrt{N}} \left(|0\rangle + e^{2\pi i\,[0.x_n]}|1\rangle\right) \otimes \left(|0\rangle + e^{2\pi i\,[0.x_{n-1}x_n]}|1\rangle\right) \otimes \cdots \otimes \left(|0\rangle + e^{2\pi i\,[0.x_1 x_2 \dots x_n]}|1\rangle\right)$$

or

$$QFT(|x_1 x_2 \dots x_n\rangle) = \frac{1}{\sqrt{N}} \left(|0\rangle + \omega_1^x|1\rangle\right) \otimes \left(|0\rangle + \omega_2^x|1\rangle\right) \otimes \cdots \otimes \left(|0\rangle + \omega_n^x|1\rangle\right)$$

Quantum Fourier Transform

- The algorithm effectively takes the 2^n amplitudes of an n-qubit state as a vector of size 2^n and performs a **discrete Fourier Transform** so that the result is encoded in the amplitudes of the output state
- The simplest way to show that the normalized Fourier Transform is a unitary operation is to demonstrate the quantum circuit that performs the QFT



- The input register contains an n-qubit basis state $|x\rangle$ expressed as the tensor product of the individual qubits in its binary expansion:

$$|x\rangle \equiv |x_1 x_2 \cdots x_n\rangle \equiv |x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_n\rangle$$

- The gates labeled R_m represent a series of **single-qubit phase rotations**
- For each integer $m \geq 2$, the gate R_m **shifts the phase** of the $|1\rangle$ component of the input qubit by a factor of $e^{\frac{2\pi i}{2^m}}$, representing the unitary transformation

$$\begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^m}} \end{pmatrix}$$

Quantum Fourier Transform

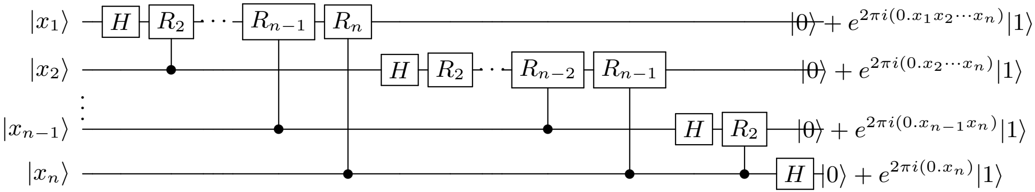
- However, in the QFT circuit, each R^m gate is **controlled** by another qubit (indicated by a large dot connected to the gate by a vertical line)
- Given a two-qubit state, $|\psi_1\rangle|\psi_2\rangle$, composed of the controlling qubit, $|\psi_1\rangle$, and the input qubit, $|\psi_2\rangle$, the **controlled-R^m gate** represents the unitary transformation

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{\frac{2\pi i}{2^m}} \end{pmatrix}$$

Quantum Fourier Transform

- If the controlled-R_m gate is being applied to a **basis state**, $|x_\ell\rangle$, where x_ℓ is either 0 or 1, then depending on the value of x_ℓ, the controlled-R_m gate performs the **identity transformation**, or the R_m **transformation**
- However, we may combine the two and equivalently say that the controlled-R_m gate performs the transformation
$$\begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i x_\ell}{2^m}} \end{pmatrix}$$
on the qubit $|\psi_2\rangle$, effectively performing a **data-dependent phase rotation**

Quantum Fourier Transform - Circuit Analysis



1. After the first Hadamard gate on qubit 1, the state is transformed from the input state to

$$H \otimes I_{n-1}|x_1 x_2 \ldots x_n\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{\frac{2\pi i}{2}x_1}|1\rangle\right) \otimes |x_2 x_3 \ldots x_n\rangle$$

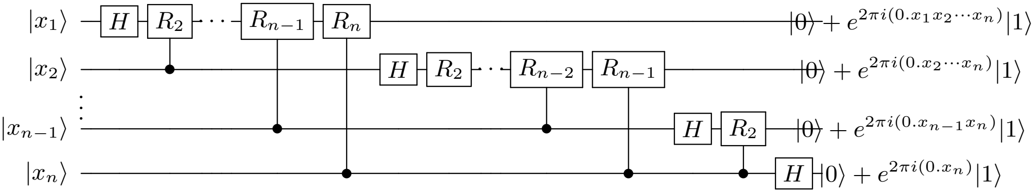
2. Following application of R_2 on qubit 1 controlled by qubit 2, the state becomes

$$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{\frac{2\pi i}{2^2}x_2 + \frac{2\pi i}{2}x_1}|1\rangle\right) \otimes |x_2 x_3 \ldots x_n\rangle$$

3. After the application of the last R_n gate on qubit 1 controlled by qubit n, the state is

$$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{\frac{2\pi i}{2^n}x_n + \frac{2\pi i}{2^{n-1}}x_{n-1} + \cdots + \frac{2\pi i}{2^2}x_2 + \frac{2\pi i}{2}x_1}|1\rangle\right) \otimes |x_2 x_3 \ldots x_n\rangle$$

Quantum Fourier Transform - Circuit Analysis



$$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{\frac{2\pi i}{2^n}x_n + \frac{2\pi i}{2^{n-1}}x_{n-1} + \cdots + \frac{2\pi i}{2^2}x_2 + \frac{2\pi i}{2}x_1}|1\rangle\right) \otimes |x_2x_3\ldots x_n\rangle$$

Since $x = 2^{n-1}x_1 + 2^{n-2}x_2 + \cdots + 2^1x_{n-1} + 2^0x_n$, we can rewrite the state as $\frac{1}{\sqrt{2}}\left(|0\rangle + e^{\frac{2\pi i}{2^n}x}|1\rangle\right) \otimes |x_2x_3\ldots x_n\rangle$

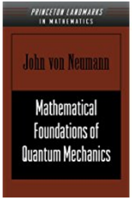
4. Application of a similar sequence of gates for qubits $2\ldots n$, the final state is:

$$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{\frac{2\pi i}{2^n}x}|1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + e^{\frac{2\pi i}{2^{n-1}}x}|1\rangle\right) \otimes \cdots \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + e^{\frac{2\pi i}{2^2}x}|1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + e^{\frac{2\pi i}{2^1}x}|1\rangle\right)$$

which is the QFT of the input state in reversed order

Quantum Phase Estimation

- The **Quantum Phase Estimation** algorithm is one of the most instrumental algorithms in Quantum Computing
- Proposed first in **von Neumman's** Mathematical Foundations of Quantum Mechanics book (aka von Neumann measurement)
- Quantum Computing formulation is due to **Kitaev**
- **Applications** range from factoring, through eigenvalue decomposition, linear system solver and more...



Quantum Phase Estimation

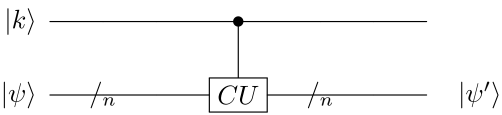
- **Recall : Unitary Eigenvalues** : Let U be a $N \times N$ unitary transformation. U has an **orthonormal basis** of **eigenvectors** $|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_N\rangle$ with **eigenvalues** $\lambda_1, \lambda_2, \ldots, \lambda_N$, where $\lambda_j = e^{2\pi i \theta_j}$ for some θ_j
- **Proof** : U, being **unitary**, **maps unit vectors to unit vectors** and hence all the eigenvalues have **unit magnitude**, i.e. they are of the form $e^{2\pi i \theta}$ for some θ
  - Let $|\psi_j\rangle$ and $|\psi_k\rangle$ be two **distinct** eigenvectors with **distinct** eigenvalues λ_j and λ_k
  - We have that

$$\lambda_j \langle \psi_j, \psi_k \rangle = \langle \lambda_j \psi_j, \psi_k \rangle = \langle U\psi_j, \psi_k \rangle = \langle \psi_j, U\psi_k \rangle = \langle \psi_j, \lambda_k \psi_k \rangle = \lambda_k \langle \psi_j, \psi_k \rangle$$

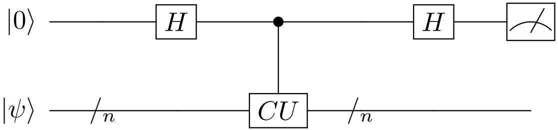
  - Since $\lambda_j \neq \lambda_k$, the inner product $\langle \psi_j, \psi_k \rangle$ is 0, i.e. the eigenvectors $|\psi_j\rangle$ and $|\psi_k\rangle$ are **orthonormal**

Quantum Phase Estimation

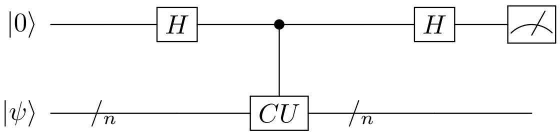
- **Goal: Phase Estimation** : Given a unitary transformation U, and one of its eigenstate $|\psi_j\rangle$
- **Find:** the corresponding eigenvalue $\lambda_j = e^{2\pi i\theta_j}$ (or, equivalently, $\theta_j \in \mathbb{R}$)
- **Reminder : Controlled U** : For any unitary transformation U, the **controlled U gate**, CU, transforms the target register $|\psi\rangle$ to $U|\psi\rangle$ **conditionally** upon the control input qubit



- **Estimation** of the **phase** θ can be performed by the following simple prototype circuit



Quantum Phase Estimation Prototype - Circuit Analysis



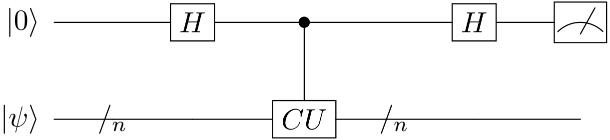
- The application of **H** gate upon the control qubit, transfers the controller into a **uniform superposition** state

$$H \otimes I_n \; |0\rangle|\psi\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + |1\rangle\right) |\psi\rangle$$

- Consequent application of the controlled **CU** entails

$$\begin{aligned} CU \; \frac{1}{\sqrt{2}} \left(|0\rangle + |1\rangle\right) |\psi\rangle &= \frac{1}{\sqrt{2}}|0\rangle|\psi\rangle + \frac{1}{\sqrt{2}}|1\rangle\lambda|\psi\rangle \\ &= \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{\lambda}{\sqrt{2}}|1\rangle\right) \otimes |\psi\rangle \end{aligned}$$

- **Note :** After application of **CU** gate, the **eigenstate**, $|\psi\rangle$ remained **unchanged** while were able to push λ into the **phase** (phase kickback) of the controller qubit

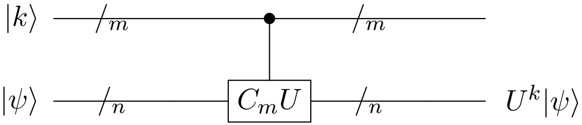


- Application of an additional **Hadamard** gate upon the controller qubit will **transform** the state into a **measurable amplitude** in the Z basis

$$H\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{\lambda}{\sqrt{2}}|1\rangle\right) = \frac{1+\lambda}{2}|0\rangle + \frac{1-\lambda}{2}|1\rangle$$

Quantum Phase Estimation - Circuit Analysis

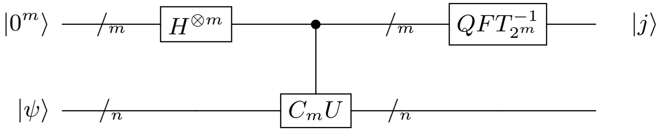
- To perform a (more) **efficient implementation** of the phase estimation algorithm we need to extend the set of **ancillary qubits**
- **Definition: m-Controlled U** : For any unitary transformation U, m-controlled U gate, C_mU, performs the transformation $C_mU\ |k\rangle \otimes |\psi\rangle = |k\rangle \otimes U^k|\psi\rangle$



  where $k \in \{0, 1, ..., 2^m - 1\}$
- Estimation of θ within m bits of **precision** is equivalent to estimating the integer j, where $\frac{j}{2^m}$ is the **closest approximation** to θ

Quantum Phase Estimation - Circuit Analysis

- Let $w_m = e^{\frac{2\pi i}{2^m}}$, the circuit below **estimates** the **phase** efficiently



- The **Hadamard** (over m qubits this time) results in a **uniform superposition**

$$H^{\otimes m} \otimes I_n \; |0^m\rangle|\psi\rangle = \left(\frac{1}{\sqrt{2^m}} \sum_{k=0}^{2^m-1} |k\rangle \right) \otimes |\psi\rangle$$

- Next, application of the m-controlled U gate

$$C_m U \left(\frac{1}{\sqrt{2^m}} \sum_{k=0}^{2^m-1} |k\rangle \right) \otimes |\psi\rangle = \left(\frac{1}{\sqrt{2^m}} \sum_{k=0}^{2^m-1} \lambda^k |k\rangle \right) \otimes |\psi\rangle =$$

$$\left(\frac{1}{\sqrt{2^m}} \sum_{k=0}^{2^m-1} w_m^{jk} |k\rangle \right) \otimes |\psi\rangle$$

Quantum Phase Estimation - Circuit Analysis

- Following the **controlled operation** the ancillary register contains the **Fourier Transform** mod 2^m of j
- How do we retrieve j back ?

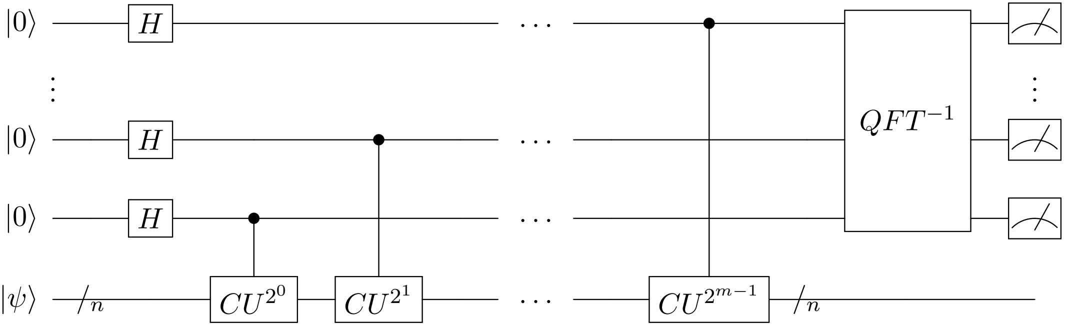
Quantum Phase Estimation - Circuit Analysis

- Following the **controlled operation** the ancillary register contains the **Fourier Transform** mod 2^m of j
- How do we retrieve j back ? Apply the **inverse** of the **Fourier Transform** mod 2^m
- Recall that quantum circuits are **reversible**, thus, following the **inverse QFT** we get back j

$$QFT_{2^m}^{-1} \otimes I_n \left(\frac{1}{\sqrt{2^m}} \sum_{k=0}^{2^m-1} w_m^{jk} |k\rangle \right) \otimes |\psi\rangle = |j\rangle \otimes |\psi\rangle$$

- If $\theta = \frac{j}{2^m}$, then the circuit outputs j
- If $\theta \approx \frac{j}{2^m}$, then the circuit outputs j with high probability

Quantum Phase Estimation - Circuit Description



Linear System of Equations - Problem Definition

- **Given** a matrix A and a vector $|b\rangle$
- **Find** a vector $|x\rangle$ such that $A|x\rangle = |b\rangle$

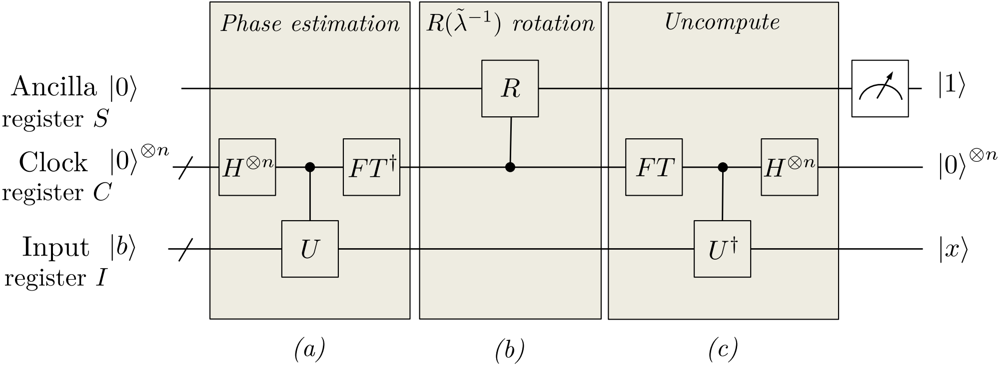
- Solution of linear systems of equations is instrumental across most disciplines of science and engineering

- The study of Harrow, Hassidim and Lloyd (2008) provided algorithmic framework for linear regression with an exponential speed-up

- Note: it is a quantum **algorithm** but not a realizable **quantum computation**. i.e. it does not map classical input to a classical result, but rather manipulates quantum data only

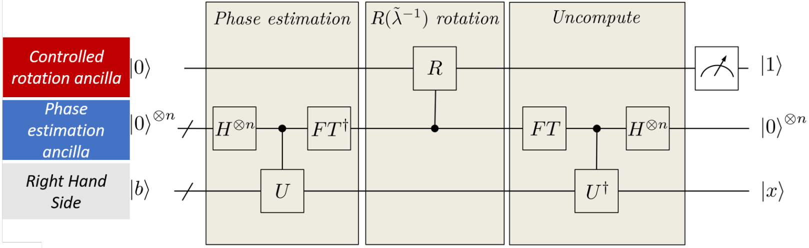
Assumptions and Disclaimers

- The algorithm exemplifies the **gap** between the **desired computation** of providing the system A, and RHS b, and extracting x, **vs. the quantum computation** of $|x\rangle$ given A and $|b\rangle$. This difference is not as subtle as it may appear at first glance
- **Data loading** into the quantum computer, is assumed to be performed in **logarithmic cost** with respect to the **problem size** (an unrealistic assumption for general data), or alternatively the data is (somehow) already stored in a so-called QRAM (quantum RAM)
- **Classical output** is limited to a **low dimensional function** of the **solution** (e.g. an expectation)
- Known approximation of the expectation value of some operator associated with x, e.g., $x^\dagger M x$ for some matrix M
- A is sparse, ($s \ll N$ in entries / row), Hermitian $N \times N$ with condition number κ (this assumption can be avoided)



- **Solve** $Ax = b$, where $|x\rangle$ and $|b\rangle$ are quantum states, and A represents the Hamiltonian

High Level Algorithmic - Steps



1. **State preparation** - prepare the state $|b\rangle$ (amplitude encoding), n ancilla qubits at $|0\rangle$, additional ancillar qubit at $|0\rangle$
2. **Quantum Phase Estimation** - perform phase estimation upon the state $|b\rangle$, using the n ancillar qubits - extract eigenvalues of A - $QPE_A|b\rangle|0\rangle^{\otimes n} = \sum_j \beta_j|\psi_j\rangle|\bar{\lambda_j}\rangle$
3. **Conditional rotation** - performs $\sum \beta_j|\psi_j\rangle|\bar{\lambda_j}\rangle|0\rangle \rightarrow \sum \beta_j|\psi_j\rangle|\bar{\lambda_j}\rangle\left(\sqrt{1-\frac{C^2}{\lambda_j^2}}|0\rangle + \frac{C}{\lambda_j}|1\rangle\right)$
4. **Uncompute QPE** - uncompute eigenvalue register with the **inverted phase** $\sum \beta_j|\psi_j\rangle|0\rangle\left(\sqrt{1-\frac{C^2}{\lambda_j^2}}|0\rangle + \frac{C}{\lambda_j}|1\rangle\right)$
5. **Rejection sampling** - identify cases in which the conditional rotation was successful

Linear System of Equations - Solution Approach

- Assume $A = A^\dagger$
- Otherwise, solve instead

$$\begin{pmatrix} 0 & A \\ A^\dagger & 0 \end{pmatrix} \begin{pmatrix} 0 \\ x \end{pmatrix} = \begin{pmatrix} b \\ 0 \end{pmatrix}$$

  which implies that $Ax = b$ for all A (not necessarily square, can be over-determined or under-determined)
- Per the sparsity assumption upon A, $s \ll N$, $A = A^\dagger$ is local
- Then exponentiation of the operator A (aka Hamiltonian simulation) e^{-iAt} can be performed in time $\mathcal{O}(\log(N))$ [Lloyd 1996]

Linear System of Equations - Solution Approach

- If we know how to diagonalize A, i.e.

$$UAU^\dagger = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_N \end{pmatrix}$$

then inverse is just the inverse of the diagonal elements

$$U^\dagger A^{-1} U = \begin{pmatrix} \lambda_1^{-1} & & 0 \\ & \ddots & \\ 0 & & \lambda_N^{-1} \end{pmatrix}$$

- Based on Kitaev's QPE algorithm for finding eigenpairs, a momentum operator p is used to advance the system $|b\rangle|0\rangle$ by a distance proportional to the eigenvalue of A
- Let the state $|b\rangle$ be represented by an **eigen decomposition** of A, i.e. $|b\rangle = \sum_j \beta_j |\psi_j\rangle$

$$QPE_A|b\rangle|0\rangle = \sum_j \beta_j |\psi_j\rangle|\lambda_j\rangle$$

Linear System of Equations - Solution Approach

- Next, we **pick** the **inverse of the eigenvalues** λ_j and turn them into a **phase**

$$\sum_j \beta_j e^{i\delta\lambda_j^{-1}} |\psi_j\rangle |\lambda_j\rangle$$

  with a small δ
- Next, following the swap of λ and λ^{-1} **undo** the **phase estimation** operation

$$\beta_j e^{i\delta\lambda_j^{-1}} |\psi_j\rangle |0\rangle$$

- The above term is essentially

$$e^{i\delta A^{-1}} |b\rangle |0\rangle$$

Linear System of Equations - Solution Approach

- If δ is small enough

$$e^{i\delta A^{-1}}|b\rangle|0\rangle \approx (I + i\delta A^{-1})|b\rangle|0\rangle = (|b\rangle + i\delta\, \underbrace{A^{-1}|b\rangle}_{|x\rangle})|0\rangle$$

- Thus, within the expression we have the desired $A^{-1}|b\rangle$ which can be extracted with probability of δ^2

Linear Solver - Run-Time Complexity

- The classical algorithms can find x and estimate $x^\dagger M x$ in $\tilde{\mathcal{O}}(N\sqrt{\kappa})$ run time
- For A of condition number, κ, in k steps we get $A^{-1}|b\rangle$ to accuracy of $\mathcal{O}(\frac{\kappa^2 s^2}{\epsilon} logN)$
- This is indeed a remarkable exponential acceleration
- Consequent work improved upon the condition number dependency [A. Childs, R. Kothari and R. Somma, 2015]
- Extension to non-sparse settings and further complexity reduction based on quantum singular value estimation are due to $\mathcal{O}(\sqrt{N} \log N\kappa^2)$ [L. Wossing et al, 2018]

Questions