## Quantum Algorithm for Linear Systems of Equations

Article by:
Aram W. Harrow, Avinatan Hassidim and Seth Lloyd, 2008 Presentation by:
Nir Stiassnie and Shay Kricheli

Quantum Computing, Ben Gurion University

September 2020

## Introduction and Outline

- Algorithm for solving linear equations [1]
- Very common in engineering and science

Outline:

- Problem formulation and definitions
- Runtime comparison with classical algorithms, exponential speedup
- Algorithm sketch - concept and details
- Runtime optimality


## Problem Formulation

Let:

- $A \in \mathbb{C}^{N \times N}$ be an $N \times N$ Hermitian matrix.
- $\vec{b} \in \mathbb{C}^{N}$ be a $N$-dimensional vector.

We would like to find a vector $\vec{x}$ satisfying:

$$
A \vec{x}=\vec{b}
$$

If $A$ is invertible there exists a unique solution which is given by:

$$
\vec{x}=A^{-1} \vec{b}
$$

- Cases in which $A$ is not invertible will be discussed later on.
- For now we will assume that $A$ is invertible.


## Preliminary Definitions

## Definition

Given $s \in \mathbb{N}$, a matrix $A \in \mathbb{C}^{N \times N}$ is called $s$-sparse if each row of $A$ contains at most $s$ non-zero entries.

- For any $N \times N$ matrix $A: s=O(N)$.
- In this algorithm, best performance is achieved when: $s \ll N$.
- More specifically, when: $s$ is poly $(\log N)$.
- As in: $\exists k \in \mathbb{N} ; s=O\left(\log ^{k} N\right)$.


## Definition

Given an Hermitian matrix $A \in \mathbb{C}^{N \times N}$, the condition number of $A$ is given by:

$$
\kappa=\frac{\left|\lambda_{\max }\right|}{\left|\lambda_{\min }\right|}
$$

where $\lambda_{\max }$ and $\lambda_{\min }$ are the maximal and minimal (by moduli) eigenvalues of $A$ respectively.

- $\kappa$ does not necessarily depend on $N$.
- In this algorithm, best performance is achieved when: $\kappa \ll N$.
- More specifically, when: $\kappa$ is poly $(\log N)$.
- $\kappa$ grows $\rightarrow A$ closer to a singular matrix. Such a matrix is said to be "ill-conditioned". If $A$ is not invertible $-\kappa=\infty$.


## Classical Algorithms Runtime

- Solving the problem involves inverting $A$ and multiplying the result by $\vec{b}$.
- Theorem 28.1 in [2] states that the matrix multiplication problem is not harder than the matrix inversion problem and theorem 28.2 states vice versa.
- Thus the runtime of the problem is proportional to that of performing matrix inversion.
- Inverting $A$ can be done by performing Gaussian Elimination.

For inverting a general matrix $A$ :

- Gaussian Elimination algorithm - runs in time $O\left(N^{3}\right)$.
- There are minor improvements, up to about $O\left(N^{2.373}\right)$.
- It is strongly conjured that a tight bound for the matrix multiplication problem given two $N \times N$ matrices is $\Theta\left(N^{2}\right)$.
- Thus the runtime of classical algorithms for matrix inversion is polynomial with high certainty.


## Runtime Improvement Attempts

Assuming that $A$ is $s$-sparse and with condition number $\kappa$ :

- Conjugate Gradient Descent - Runs in $O(N s \kappa)$.
- With the assumptions on $s$ and $\kappa$, we still get a runtime of $O\left(N \log ^{k} N\right)$ for some $k$. At least polynomial in $N$.
Even if $A$ is also positive semi-definite:
- The runtime of Conjugate Gradient Descent reduces to $O(N s \sqrt{\kappa})$.
- We still get a runtime of $O\left(N \log ^{r} N\right)$.
- Positive semi-definiteness is an additional assumption the quantum algorithm does not make.


## Quantum Algorithm Runtime

- Can a quantum algorithm improve the dependence in $N$ to be better than polynomial time?
- Even when the task is done - just reading out the solution takes $O(N)$ time.
- Let $|x\rangle$ be a $n$-qubit quantum state (where $n=\log N$ ) corresponding of the values of $\vec{x}$ up to some error $\varepsilon$.
- In cases where the desired outcome is not $|x\rangle$ itself, but some specific set of functions of $|x\rangle$, the algorithm can perform faster.

Assuming $A$ is $s$-sparse, for some measurement operator $M \in \mathbb{C}^{N \times N}$ such that $M \geq 0$, as in $M$ is positive semi-definite:

- The expression $\langle x| M|x\rangle$ can be calculated efficiently with error $\varepsilon$ - in poly $(\log N, s, \kappa, 1 / \varepsilon)$ time.
- More specifically, a runtime of $O\left(\kappa^{2} s^{2} \log N / \varepsilon\right)$, where $\varepsilon$ is the error achieved in the output state $|x\rangle$.
- This provides exponential improvement over the best known classical algorithm - in terms of $N$.
- The total exponential speedup is present where $\kappa$, s and $1 / \varepsilon$ are poly $(\log N)$.

For example, let $N=10^{12} \approx 2^{40}$ (and when
$\kappa, s, 1 / \varepsilon=O(\log (N))$ :

- The runtime of the classical algorithm will be at least $\Omega\left(2^{40}\right)$.
- The runtime of the quantum algorithm will be $\operatorname{poly}\left(\log \left(2^{40}\right)\right)=\operatorname{poly}(40)$.


## Algorithm Idea

Given an Hermitian matrix $A$ :
(1) Start with a pre-determined initial state.
(2) Performing phase estimation to approximate the the eigenvalues of $A$.
(3) Approximate the inverse of $A$ by inverting its estimated eigenvalues.
(4) Use amplitude amplification to maximize the probability for measuring the desired outcome.
(5) Perform a measurement using $M$ to estimate $\langle x| M|x\rangle$.

## The Non-Hermitian Case

- As the algorithm assumes that $A$ is Hermitian, if $A$ is actually not, then as a preprocess step, we define:

$$
D=\left[\begin{array}{cc}
0 & A \\
A^{\dagger} & 0
\end{array}\right]
$$

As $D$ is Hermitian, using the algorithm we can now solve the equation:

$$
D \tilde{x}=\tilde{b}
$$

for $\tilde{x}$, where:

$$
\tilde{x}=\left[\begin{array}{l}
0 \\
\vec{x}
\end{array}\right] ; \tilde{b}=\left[\begin{array}{l}
\vec{b} \\
0
\end{array}\right]
$$

and then use $\vec{x}$ as explained.

- We want the quantum state $|x\rangle=A^{-1}|b\rangle$.
- We assumed $A$ is invertible. Also Hermitian $\rightarrow$ it is normal.
- Thus its eigenvectors $\left\{\overrightarrow{u_{j}}\right\}_{j=1}^{N}$ corresponding to its eigenvalues $\left\{\lambda_{j}\right\}_{j=1}^{N}$ consist an orthonormal basis.
Let us denote the representation of $|b\rangle$ in that basis:

$$
|b\rangle=\sum_{k=1}^{N} \beta_{k}\left|u_{k}\right\rangle
$$

## Claim

The output state can represented as follows:

$$
|x\rangle=\sum_{j=1}^{N} \lambda_{j}^{-1} \beta_{j}\left|u_{j}\right\rangle
$$

## Proof

By the spectral theorem $f(A)=\sum_{j=1}^{N} f\left(\lambda_{j}\right)\left|u_{j}\right\rangle\left\langle u_{j}\right|$ and thus: $A^{-1}=\sum_{j=1}^{N} \lambda_{j}^{-1}\left|u_{j}\right\rangle\left\langle u_{j}\right|$. We have:

$$
\begin{aligned}
|x\rangle & =A^{-1}|b\rangle=\left(\sum_{j=1}^{N} \lambda_{j}^{-1}\left|u_{j}\right\rangle\left\langle u_{j}\right|\right)\left(\sum_{k=1}^{N} \beta_{k}\left|u_{k}\right\rangle\right) \\
& =\sum_{j=1}^{N} \lambda_{j}^{-1} \beta_{j}\left|u_{j}\right\rangle\left\langle u_{j} \mid u_{j}\right\rangle+\sum_{j=1}^{N} \sum_{\substack{k=1 \\
k \neq j}}^{N} \lambda_{j}^{-1} \beta_{j}\left|u_{j}\right\rangle\left\langle u_{j} \mid u_{k}\right\rangle \\
& =\sum_{j=1}^{N} \lambda_{j}^{-1} \beta_{j}\left|u_{j}\right\rangle
\end{aligned}
$$

since $\left\{\overrightarrow{u_{j}}\right\}_{j=1}^{N}$ consist an orthonormal basis. $\square$

## Algorithm Outline

- Input: Oracle access to the rows of an Hermitian matrix $A$, a method to produce a unit vector $|b\rangle$ and a cutoff value for $\kappa$.
(1) Represent $\vec{b}$ as a quantum state of the form:

$$
|b\rangle=\sum_{i=1}^{N} b_{i}|i\rangle
$$

where: $b_{i}=\vec{b}[i]$.
(2) Next step - produce eigenvalues and eigenvectors of $A$.

- Using a simulation of a section of the phase estimation algorithm.
- Simulate phase estimation $C-U$ section with $U=e^{i A t}$ (which is unitary) via a technique called Hamiltonian Simulation.
- The Fourier Transform is then applied.
- This results in a state proportional to:

$$
\sum_{j=1}^{N} \beta_{j}\left|u_{j}\right\rangle\left|\lambda_{j}\right\rangle
$$

- We now have produced the eigenvalues in the register.
(3) Next step - produce the inverse of the eigenvalues as a scalar. Naive algorithm:
- Apply conditional rotation on ancilla qubit initialized to $|0\rangle$.
- Rotate conditioned on the eigenvalues of $A$ - which are all real since it is Hermitian.
- Let us define the rotation matrix:

$$
\tilde{R}_{\lambda_{j}}=\left[\begin{array}{cc}
\sqrt{1-\frac{1}{\lambda_{j}^{2}}} & -\frac{1}{\lambda_{j}} \\
\frac{1}{\lambda_{j}} & \sqrt{1-\frac{1}{\lambda_{j}^{2}}}
\end{array}\right]
$$

- But, $\tilde{R}_{\lambda_{j}}$ is not necessarily unitary.
- In the case where $\left|\lambda_{j}\right|<1$, we get $\tilde{R}_{\lambda_{j}} \tilde{R}_{\lambda_{j}}^{\dagger} \neq I$.
- This can be fixed using a normalization constant. Let:

$$
R_{\lambda_{j}}=\left[\begin{array}{cc}
\sqrt{1-\frac{C^{2}}{\lambda_{j}^{2}}} & -\frac{C}{\lambda_{j}} \\
\frac{C}{\lambda_{j}} & \sqrt{1-\frac{C^{2}}{\lambda_{j}^{2}}}
\end{array}\right]
$$

- Applying $R_{\lambda_{j}}$ to the ancilla qubit we get the form:

$$
\sum_{j=1}^{N} \beta_{j}\left|u_{j}\right\rangle\left|\lambda_{j}\right\rangle\left(\sqrt{1-\frac{C^{2}}{\lambda_{j}^{2}}}|0\rangle+\frac{C}{\lambda_{j}}|1\rangle\right)
$$

- Conditioned on measuring 1 in the ancilla qubit, we get a state proportional to:

$$
\sum_{j=1}^{N} \beta_{j}\left|u_{j}\right\rangle\left|\lambda_{j}\right\rangle \rightarrow C \sum_{j=1}^{N} \lambda_{j}^{-1} \beta_{j}\left|u_{j}\right\rangle\left|\lambda_{j}\right\rangle
$$

where $C$ is a normalization constant.

- The whole transformation is non-unitary - involves measurement and scaling by a factor $\not \equiv 1$.
- Inverting the eigenvalues is the main challenge solved by the suggested algorithm.
(9) Uncompute the $\left|\lambda_{j}\right\rangle$ register, resulting in a state proportional to:

$$
\sum_{j=1}^{N} \lambda_{j}^{-1} \beta_{j}\left|u_{j}\right\rangle=|x\rangle
$$

where the equivalence is from the proven claim.

## Detailed Algorithm

Let us detail the algorithm operation:
(1) Start with an $n$-qubit register $\mid$ initial $\rangle$.
(2) Produce the state $|b\rangle$. Assume there exists an efficiently implementable unitary operator $B$ such that:

$$
B \mid \text { initial }\rangle=|b\rangle=\sum_{i=1}^{N} b_{i}|i\rangle
$$

possibly along with garbage in ancilla registers. For the discussion of the algorithm, all the errors in $B$ are neglected.
(3) Prepare the unitary operator $e^{i A t}$.

## Definition

A Hermitian $s$-sparse matrix $A \in \mathbb{C}^{N \times N}$, is efficiently row computable if it has at most $s$ nonzero entries per row and given a row index $|i\rangle$, the $i$ 'th row of $A$ can be computed in time $O(s)$.

- Assume $A$ Hermitian, $s$-sparse and efficiently row computable.
- Thus we have an oracle access to the rows of $A$.
- For some time $t \geq 0$ of the evolution, the unitary operator $e^{i A t}$ can be calculated efficiently, as shown in [3].
- In time of approximately $O\left(\log N s^{2} t\right)$.
- Combined with the assumption $s \ll N$, this is where the sparsity of $A$ is in fact used.


## $U_{\text {invert }}$ subroutine

Let us first assume $A$ is well-conditioned.

- Assume the state $\left|\psi_{0}\right\rangle$ can be prepared efficiently, where:

$$
\left|\psi_{0}\right\rangle=\sqrt{\frac{2}{T}} \sum_{\tau=0}^{T-1} \sin \pi\left(\frac{\tau+\frac{1}{2}}{T}\right)|\tau\rangle
$$

for some large $T$ such that $T=O\left(\log N s^{2} t\right)$.

- $\left|\psi_{0}\right\rangle$ are chosen to minimize a loss function of the error.
- Runtime for this operation is $\operatorname{poly}(\log (T / \varepsilon))$.
(4) Define the subroutine of the algorithm $U_{\text {invert }}$ :
- Initiate a register of zeros noted by $L$. Prepare $\left|\psi_{0}\right\rangle$ on register $L$ and adjoin it to $|b\rangle$, to result in:

$$
\left|\psi_{0}\right\rangle \otimes|b\rangle
$$

For phase estimation, apply the next two steps:

- Apply conditional Hamiltonian evolution on $\left|\psi_{0}\right\rangle \otimes|b\rangle$ with:

$$
\sum_{\tau=0}^{T-1}|\tau\rangle\langle\tau| \otimes e^{i A t_{0} \tau / T}
$$

for some chosen $t_{0}$ such that $t_{0}=O(\kappa / \varepsilon)$.

- Apply the Fourier transform to register $L$.

After the Fourier transform, we end up with the state:

$$
\sum_{j=1}^{N} \sum_{k=0}^{T-1} \alpha_{k, j} \beta_{j}|k\rangle\left|u_{j}\right\rangle
$$

where $|k\rangle$ are the Fourier basis states and $\left|\alpha_{k, j}\right|$ is close to 1 if and only if $\lambda_{j} \approx \frac{2 \pi k}{t_{0}}$. Let $\tilde{\lambda_{k}}=\frac{2 \pi k}{t_{0}}$. We can relabel the state to be:

$$
\sum_{j=1}^{N} \sum_{k=0}^{T-1} \alpha_{k, j} \beta_{j}\left|\tilde{\lambda_{k}}\right\rangle\left|u_{j}\right\rangle
$$

To get ${\tilde{\lambda_{k}}}^{-1}$, apply the next non-unitary operation:

- Adjoin a register $S$ in the state:

$$
\left|h\left(\tilde{\lambda_{k}}\right)\right\rangle=\sqrt{1-f\left(\tilde{\lambda_{k}}\right)^{2}}|0\rangle+f\left(\tilde{\lambda_{k}}\right)|1\rangle
$$

where:

- ' 0 ' indicates that the desired matrix inversion hasn't taken place yet.
- ' 1 ' indicates that it has.
- $f$ is called a filter function - used to produce the inverse of the eigenvalues. They adhere certain conditions that we will discuss later.
- This is a generalization of what we saw earlier.

We end up with the following state:

$$
\sum_{j=1}^{N} \sum_{k=0}^{T-1} \alpha_{k, j} \beta_{j}\left|\tilde{\lambda_{k}}\right\rangle\left|u_{j}\right\rangle\left(\sqrt{1-f\left(\tilde{\lambda_{k}}\right)^{2}}|0\rangle+f\left(\tilde{\lambda_{k}}\right)|1\rangle\right)
$$

- To uncompute the $\tilde{\lambda_{k}}$ register, reverse the first three steps to undo phase estimation.
- If the phase estimation was perfect, we would have $\alpha_{k, j}=1$ if $\tilde{\lambda_{k}}=\lambda_{j}$ and 0 otherwise.
- Assuming this is the case, we get the state:

$$
\sum_{j=1}^{N} \beta_{j}\left|u_{j}\right\rangle\left(\sqrt{1-f\left(\tilde{\lambda_{k}}\right)^{2}}|0\rangle+f\left(\tilde{\lambda_{k}}\right)|1\rangle\right)
$$

## Main Loop - Amplitude Amplification

(5) Given the initial state $\left|\phi_{0}\right\rangle=U_{\text {invert }} B \mid$ initial $\rangle$, apply the following repeatedly:

$$
U_{\text {invert }} B R_{\text {init }} B^{\dagger} U_{\text {invert }}^{\dagger} R_{\text {succ }}
$$

- where:

$$
\left.\begin{array}{l}
\text { - } R_{\text {succ }}=I-2|1\rangle\langle 1|\left(\text { reflection over }|1\rangle^{\perp}\right) \\
\text { - } \left.\left.R_{\text {init }}=I-2 \mid \text { initial }\right\rangle\langle\text { initial }| \text { (reflection over } \mid \text { initial }\right\rangle
\end{array}{ }^{\perp}\right)
$$

- Measure register $L$ at the end of the loop until $|1\rangle$ is measured


## Claim

Given $p$ the probability to measure $|1\rangle$ in $\left|\phi_{0}\right\rangle$ - the amplitude amplification procedure makes $O\left(\frac{1}{\sqrt{p}}\right)$ repetitions.

## Proof

For some small $\theta$, the initial state $\left|\phi_{0}\right\rangle$ can be represented as:

$$
\left|\phi_{0}\right\rangle=\cos (\theta)|0\rangle+\sin (\theta)|1\rangle
$$

Thus $p=\sin ^{2}(\theta)$. Since $\theta$ is small and thus $p \approx \theta^{2}$. As with amplitude amplification, each repetition increases the angle by $2 \theta$ (later elaborated). Thus after $n$ repetitions the state becomes:

$$
\left|\phi_{n+1}\right\rangle=\cos ((2 n+1) \theta)|0\rangle+\sin ((2 n+1) \theta)|1\rangle
$$

The amplitude is maxed when the coefficient of $|1\rangle$ is close to 1 , as in:

$$
(2 n+1) \theta \approx \frac{\pi}{2} \rightarrow n \approx \frac{\pi}{4 \theta}=\frac{\pi}{4 \sqrt{p}} \square
$$

( After measuring $|1\rangle$, the state is proportional to:

$$
\sum_{j=1}^{N} \lambda_{j}^{-1} \beta_{j}\left|u_{j}\right\rangle=|x\rangle
$$

(0) Perform a measurement with respect to $\{M, I-M\}$ as the POVM to achieve an estimate of $\langle x| M|x\rangle$ up to error $\varepsilon$.

## Amplitude Amplification Illustration

- We assumed the initial state is $\left|\phi_{0}\right\rangle=\cos (\theta)|0\rangle+\sin (\theta)|1\rangle$.
- Thus the initial angle relative to the $|0\rangle$ axis is $\theta$.
- Let us denote by $\delta$ the angle incurred by the transformation $U_{\text {invert }} B$ and assume w.l.o.g the rotation is counterclockwise.
- Thus the rotation by $B^{\dagger} U_{\text {invert }}^{\dagger}$ is a clockwise rotation by $\delta$.

The initial state $\left|\phi_{0}\right\rangle=U_{\text {invert }} B \mid$ initial $\rangle$ corresponds to a counterclockwise rotation of $\delta$ from $\mid$ initial $\rangle$ :

$33 / 48$

After reflection by $|1\rangle^{\perp}=|0\rangle$ and clockwise rotation by $\delta$ :


After reflection by $\mid$ initial $\rangle^{\perp}$ and counterclockwise rotation by $\delta$ :


Total angle by $|0\rangle$ is $\theta-\delta+2 \theta+\delta=3 \theta$.

## III-Conditioned Case

The algorithm can also handle ill-conditioned matrices.

## Definition

Given a eigenvalue $\lambda$ of a matrix $A \in \mathbb{C}^{N \times N}$, the eigenspace of $\lambda$ is defined as:

$$
E_{\lambda}=\{v \mid(\lambda I-A) v=0\}
$$

Given a Hermitian matrix $A \in \mathbb{C}^{N \times N}$ with condition number $\kappa$, the well-conditioned part of $A$ is defined as:

$$
\operatorname{span}\left(\bigcup_{\lambda \geq 1 / \kappa} E_{\lambda}\right)
$$

III-conditioned part of $A$ is symmetrically defined for $\lambda<1 / \kappa$.

- To handle ill-conditioned matrices, the algorithm inverts only the part of $|b\rangle$ which is in the well-conditioned part of $A$.
- Formally, instead of transforming $|b\rangle=\sum_{j} \beta_{j}\left|u_{j}\right\rangle$ to $|x\rangle=\sum_{j} \lambda_{j}^{-1} \beta_{j}\left|u_{j}\right\rangle$, transform into a state close to:

$$
\sum_{j: \lambda_{j} \geq 1 / \kappa} \lambda_{j}^{-1} \beta_{j}\left|u_{j}\right\rangle|w e l l\rangle+\sum_{j: \lambda_{j}<1 / \kappa} \beta_{j}\left|u_{j}\right\rangle|i l l\rangle
$$

in time $O\left(\kappa^{2}\right)$.

- The last qubit is a flag that enables to estimate the size of the ill-conditioned part.
- Handles cases where $A$ is not invertible and produces the projection of $|b\rangle$ on the well-conditioned part of $A$.


## III-Conditioned $U_{\text {invert }}$

- In the ill-conditioned case, $U_{\text {invert }}$ is changed.
- The $S$ register in step 4 is altered to:

$$
\left|h\left(\tilde{\lambda_{k}}\right)\right\rangle=\sqrt{1-f\left(\tilde{\lambda_{k}}\right)^{2}-g\left(\tilde{\lambda_{k}}\right)^{2}}|0\rangle+f\left(\tilde{\lambda_{k}}\right)|1\rangle+g\left(\tilde{\lambda_{k}}\right)|2\rangle
$$

- $g$ is also a filter function, same as $f$.
- '2' indicates part of $|b\rangle$ is in the ill-conditioned subspace of $A$.


## Filter Functions

- $f$ and $g$ defined earlier are filter functions.
- They set the amplitudes of the basis states of $|h(\lambda)\rangle$.
- Setting $\kappa^{\prime}=2 \kappa$, we define a new range where $f$ and $g$ return values in between their maximal and minimal values.
- $f$ and $g$ adhere the following conditions for some constant $K>1$ :
- $f(\lambda)=\frac{1}{K \lambda}$ for $\lambda \geq \frac{1}{\kappa}$.
- $f^{2}(\lambda)+g^{2}(\lambda) \leq 1$.
- $g(\lambda)=\frac{1}{K}$ for $\lambda \leq \frac{1}{\kappa^{\prime}}$.

Example for a $f$ and $g$ for $K=2$ :

$$
\begin{aligned}
& f(\lambda)= \begin{cases}\frac{1}{2 \lambda} & \lambda \geq 1 \\
\frac{1}{2} \sin \left(\frac{\pi}{2} \cdot \frac{\lambda-\frac{1}{\kappa^{\prime}}}{\frac{1}{\kappa}-\frac{1}{\kappa^{\prime}}}\right) & \frac{1}{\kappa}>\lambda \geq \frac{1}{\kappa^{\prime}} \\
0 & \frac{1}{\kappa^{\prime}}>\lambda\end{cases} \\
& g(\lambda)= \begin{cases}0 & \lambda \geq 1 \\
\frac{1}{2} \cos \left(\frac{\pi}{2} \cdot \frac{\lambda-\frac{1}{\kappa^{\prime}}}{\frac{1}{\kappa}-\frac{1}{\kappa^{\prime}}}\right) & \frac{1}{\kappa}>\lambda \geq \frac{1}{\kappa^{\prime}} \\
\frac{1}{2} & \frac{1}{\kappa^{\prime}}>\lambda\end{cases}
\end{aligned}
$$

## Optimality

- The quantum algorithm run-time is $O\left(\kappa^{2} s^{2} \log N / \varepsilon\right)$.
- Article shows optimality in $\kappa$ and $1 / \varepsilon$.
- It also shows no classical algorithm can run in this time.
- We will discuss optimality in $\kappa$ and with relation to classical algorithms.


## Optimality In $\kappa$

- The runtime dependency in $\kappa$ is polynomial.
- The dependency in $\kappa$ can not be improved to be polylogaritmic.
- Furthermore, it can not be improved to $\kappa^{1-\delta}$ for $\delta>0$.
- The proof of this statement is based on arguments from complexity theory.


## Definition

Let $M I$ denote the set of all algorithms that solve matrix inversion.

## Theorem

Let $M I Q \subset M I$ be the set of all quantum algorithms that solve matrix inversion for a $N \times N$ matrix with condition number $\kappa$. Then if there exists $\mathcal{A} \in M I Q$ that has a error of $\varepsilon$ and runs in $\kappa^{1-\delta}$ poly $(\log N, 1 / \varepsilon)$ time, for some $\delta>0$ then BQP $=$ PSPACE.

- It is highly unlikely that BQP $=$ PSPACE - so this results in optimality.
- The proof is based on a reduction from a general $n$-qubit quantum circuit with $T$ gates to a matrix inversion problem with:
- $N=O\left(T 2^{n}\right)$
- $\kappa=O(T)$


## Proof Outline

- TQBF (quantified SAT problem) problem - known to be PSPACE-complete, solvable for input of size $n$ with $n$ qubits and $T=\Theta\left(2^{2 n}\right)$ gates.
- Using the reduction, we get a matrix inversion problem equivalent to solving TQBF, where $N=O\left(2^{3 n}\right)$. For sufficiently large $n$, the error increases, specifically $\varepsilon \geq 1 / \log (n)$ with runtime:

$$
\kappa^{1-\delta}\left(\frac{\log N}{\varepsilon}\right)^{c_{1}} \leq T^{1-\delta}\left(\frac{3 n}{\varepsilon}\right)^{c_{1}} \leq T^{1-\delta} c_{2}(n \log n)^{c 1}
$$

for some $c_{1}, c_{2}>0$.

- Given a constant $m=\frac{2}{\delta} \frac{\log (2 n)}{\log (\log n)}$
- Iterating the reduction for $l \leq m$ steps repeatedly, for each step $i$ :

$$
\begin{aligned}
& T_{i+1}=T_{i}^{1-\delta} c_{2}(n \log n)^{c 1} \\
& n_{i+1}=n_{i}+\log \left(18 T_{i}\right)
\end{aligned}
$$

- $l=\min \{m, i\}$, where $i$ is the first iteration $T_{i+1}>T_{i}^{1-\delta / 2}$
- Setting $n_{0}=n$, this results in $T_{l}$ is poly $\left(n_{0}\right)$.
- $n_{l}$ is shown to be also poly $\left(n_{0}\right)$.
- Thus a PSPACE computation can be solved in quantum polynomial time.


## Optimality Relating to Classical Algorithms

## Theorem

Let $M I C \subset M I$ be the set of all classical algorithms that solve matrix inversion for a $N \times N$ matrix with condition number $\kappa$. Then if there exists $\mathcal{A} \in M I C$ that runs in poly $(\kappa, \log N)$ time, for some $\delta>0$ then $\mathrm{BPP}=\mathrm{BQP}$.

Proof outline:

- A problem in BQP with $n$ qubits and $T=\operatorname{poly}(n)$ gates is reduced to a inverting a matrix with with $\kappa=\operatorname{poly}(n)$, $N=2^{n}$ poly $(n)$.
- Assuming the specified classical algorithm exists, we get a poly $(n)$ runtime, thus $\mathrm{BPP}=\mathrm{BQP}$.


## Open Questions

- Can we find another quantum algorithm for solving linear systems of equations/matrix inversion using the following formula?

$$
A^{-1}=\frac{1}{\operatorname{det}(A)} \operatorname{adj}(A)
$$

- Can we find similar quantum algorithm providing exponential speedup for other matrix operations such as determinants, adjacent matrix and such?
- Can we improve the dependency in $N$ to be better than $\log N$ ?
- Can we find an efficient quantum algorithm for solving linear systems of equations for non-sparse matrices?


## References

[1] Harrow, Aram W., Avinatan Hassidim, and Seth Lloyd. Quantum Algorithm for Linear Systems of Equations. Physical Review Letters 103.15 (2009): n. pag. Crossref. Web. arXiv:0811.3171.
[2] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest and Clifford Stein. Introduction to Algorithms, Third Edition. MIT Electrical Engineering and Computer Science.
[3] D.W. Berry, G. Ahokas, R. Cleve, and B.C. Sanders. Efficient Quantum Algorithms for Simulating Sparse Hamiltonians. Comm. Math. Phys., 270(2):359-371, 2007. arXiv:quant-ph/0508139.

